STAFF REPORT

DATE: January 21, 2025

TO: City Council

FROM: Todd Henry, Police Chief

SUBJECT: Surveillance Technology – Automated License Plate Readers/Public Safety Cameras

---

Recommendation

Informational.

The Police Department is submitting this informational staff report on the consent calendar at least 30 days prior to asking the City Council to hold a public hearing for the Police Department's purchase/use of additional Fixed Public Safety Cameras and Automated License Plate Readers (ALPR). Fixed Public Safety Cameras and Automated License Plate Readers were previously approved by City Council in 2018. This informational staff report has been posted on the City website with the City Council agenda (26.07.030 (c) Davis Municipal Code (DMC)).

Fiscal Impact

The projected purchase cost for the system's initial equipment, installation, hardware, and software is $415,180.00. If approved by Council, the Department intends to apply for a Department of Justice Community Oriented Policing Services (COPS) grant to fund the initial project costs.

The Department of Justice (DOJ), Community Oriented Policing Services (COPS) Office grant program supports law enforcement agencies in implementing community-oriented policing strategies. The COPS Office grants provide funding, resources, and technical assistance to develop and improve these community policing efforts across the United States. The COPS Technology Program focuses on integrating technology into community policing efforts, providing funding for tools that enhance communication, data sharing, and overall effectiveness in policing. The Department intends to submit a funding request for all initial implementation costs associated with the project.

The project will have an annual ongoing cost associated with SIM (cell service) and access to the Motorola Vehicle Management System of ~$17,800.00.

Ongoing costs are anticipated to be funded through the California Supplemental Law Enforcement Services Fund (SLESF). SLESF is a grant fund, and the enabling legislation mandates that each municipality receive funds yearly to be spent on "frontline law enforcement services."

Council Goal(s)

This item is consistent with City Council goal 5, Maintaining High Quality Infrastructure and Services. It is not tied to a specific task.

Commission Involvement

This surveillance impact report and accompanying information regarding the equipment was sent to the Police Accountability Commission for their January 6, 2025, meeting. The Commission's comments and recommendations have been included in this report.

Background and Analysis

An automated license plate reader (ALPR) is a camera that captures images of license plates within its field of view. Fixed cameras are mounted on stationary objects, such as light poles, while mobile cameras are mounted on moving objects, such as patrol cars. Software extracts the license plate numbers from the images and stores the images, plate numbers, dates, times, and locations of the image captured in a searchable database. An ALPR system consists of the cameras, the software that reads and converts images of license plates into data, and the searchable database that stores the data. Although the primary focus of each image is the license plate, the image may also show part of the vehicle itself, including individuals within the vehicle, depending on the camera's position. ALPR technology has existed since the 1970s, yet widespread adoption by U.S. law enforcement agencies began only in the mid-2000s. Law enforcement agencies worldwide consider ALPR technology a vital tool for enhancing public safety.

Once the system collects this information, the automated system can be enabled to check the license plate data against the same State database information police officers use to check vehicle license plates. This includes stolen vehicles, vehicles listed in the database associated with other felony crimes, and missing persons-related vehicles, including those related to Amber Alerts and other at-risk factors. Any license plates matching law enforcement-identified vehicles are relayed to officers and dispatchers monitoring the system as an alert. Time permitting, officers may attempt to locate vehicles related to alerts. Every alert ultimately must be confirmed with the originating agency, and an alert itself would not constitute enough probable cause for an arrest. ALPR technology is objective and unbiased, recording only descriptive license plate details and nothing about a driver's personal characteristics or identifying information. This technology does not use facial recognition software.

Currently, the Yolo County Sheriff's Office and the cities of West Sacramento and Woodland employ fixed ALPR cameras. The Davis Police Department currently has limited investigative capabilities using this technology, often relying on information from other jurisdictions that possess a more robust ALPR technology infrastructure. As a result, Department personnel face challenges in developing investigative leads related to crimes that occur within the City, which neighboring agencies do not encounter.

The Police Department currently operates ALPR systems installed on parking enforcement vehicles for electronic chalking and e-permit verification citywide. ALPR is currently the best way to conduct timed zone enforcement without using parking meters. The current ALPR use policy allows for ALPR data collected by parking enforcement vehicles to also be utilized for criminal investigations or locating stolen/wanted vehicles.

The City Council previously authorized the use of the ALPR system after creating the Surveillance Technology approval and review process in 2018. Council has reapproved the use of ALPR for each subsequent year, including the City Council meeting on June 4, 2024.[1] The Department is seeking approval from Council to increase the number and type of ALPRs already approved.

[1] Surveillance Technology Staff Report, Renewals, June 4, 2024.

All data collected by the ALPR system is temporarily held in a secured database. The Department protects this data and does not share it unless authorized by policy.

Motorola Solutions ALPR/Public Safety Cameras

Motorola Solutions (Motorola) provides law enforcement agencies with various technology solutions, including an ALPR system with integrated remote public safety cameras. This technology combines the investigative benefits of both ALPR and remote public safety cameras into one system, reducing overall program costs. Motorola ALPR is a vehicle location intelligence solution that combines ALPR basics with unique, powerful analytics. Users can run a license plate number through law enforcement databases to discover the owner's identity and if any warrants exist. With partial plate numbers or vehicle descriptions, officers can conduct searches that return possible matches for review. They can also apply date and time filters to help narrow investigative leads. When a subject of interest in a criminal investigation is identified, associate analysis can distinguish vehicles frequently seen with them, and convoy analysis can identify vehicles that travel together – automating and streamlining what used to require hours of stakeouts and time-consuming manual comparison. Motorola's ALPR technology is designed to help transition license plate recognition data into actionable intelligence when investigating criminal cases or attempting to locate critical missing persons.

Motorola fixed license plate readers are much less expensive and easier to install than mobile ALPRs on vehicles. They also provide the advantage of always being in service, while vehicle-mounted cameras only serve when and where officers drive ALPR vehicles. Fixed ALPRS provides coverage that results in more consistent and unbiased data collection.

Motorola also guarantees exclusive customer ownership of collected data and offers granular control over ALPR data. The Department determines which members can access data and how long it is retained. These systems allow the Department to configure alerts for vehicles related to criminal investigations and vehicles wanted for criminal offenses from allied agencies. Access can be granted to a crime analyst, public safety dispatchers, specific groups of investigators, and officers.

Fixed Public Safety Cameras

Remote public safety cameras are portable or fixed cameras which are remotely accessed by Police Department employees. The cameras are web-based and use cell phone service or fiber-optic connections to access the devices. Once securely accessed, users can monitor the device, toggle it remotely and record video, but not audio. Each camera has its own digital video recorder (DVR) that records data, which can then be accessed by an external hard drive or other device. Cameras can be attached to fixed objects such as buildings, traffic standards, or light poles. The devices can either be attached to a power source or run by a solar-charged battery. Remote cameras are used to monitor areas where crime has been reported or may occur, surveil individuals suspected of committing a crime, and monitor crowd size and dynamics at City events to deploy resources better. Motorola has introduced a camera platform that integrates public safety camera capabilities alongside ALPR, providing both capabilities in a less expensive platform.

The Police Department currently uses fixed remote public safety cameras, which were authorized at the October 30, 2018[2] City Council meeting. City Council expanded the use of

[2] Surveillance Technology Staff Report, Public Safety Cameras, October 30, 2018.

fixed public safety cameras at the March 10, 2020[3], City Council meeting. The fixed cameras are installed at Richards/Olive and Mace/I-80 intersections. Since their initial authorization, the City Council has approved the continued use of public safety cameras annually.

The Department has experienced significant success with the currently approved public safety cameras. In 2024, investigators used these cameras 65 times for specific investigations aimed at identifying a suspect or suspect vehicle, yielding 53 positive results. Out of the cases where current cameras may have recorded video evidence of these crimes, only 12 yielded no investigative leads. Approximately 81% of the investigations where existing public safety cameras were used resulted in a positive result, closing several cases that would have likely gone unsolved otherwise.

Furthermore, since public safety cameras are already approved for use, the Council may choose to adjust the number of cameras for use by approving additional cameras as the Council sees fit.

Traffic Engineering

The ALPR technology has other uses that are not law enforcement related. The City of Davis' Public Works Engineering and Transportation Department can also use ALPR technology to assist in determining traffic patterns and volume by looking at the origins and destinations of various trips to understand better how to prioritize future projects. This anonymized data (non-identifiable) could be shared with Public Works Engineering and Transportation to conduct comprehensive traffic flow analyses, identify congestion hotspots, and understand travel behavior. By leveraging this information, traffic engineers can make data-driven decisions to optimize traffic signals, adjust lane usage, and plan future infrastructure improvements. ALPR technology can also help traffic engineers manage congestion more effectively. By analyzing the data collected from ALPRs, engineers can implement adaptive traffic control systems that adjust signal timings based on real-time traffic conditions, reducing delays and potentially improving overall traffic flow.

Surveillance Impact Report

Information describing the surveillance technology and how it works, including product descriptions from manufacturers;

(a) Information on the proposed purpose(s) for the surveillance technology:

The Davis Police Department is committed to finding established technology that can increase police personnel effectiveness while improving community safety. Many unsolved cases involve vehicles that are subject to further investigation by the Department. Effective use of surveillance technologies has become a critical component for both crime prevention and criminal case investigations. For example, upon deployment of ALPR, the Morgan Hill Police Department recovered 51 stolen vehicles in just under three months. Purchasing these ALPR cameras will assist in identifying license plates related to a criminal investigation for a specific location or intersection 24 hours a day. It will enhance previously approved cameras the Department uses while increasing coverage of additional ingress and egress routes within the City's jurisdiction.

[3] Surveillance Technology Staff Report, Public Safety Cameras, March 10, 2020.

(b) If applicable, the location(s) it may be deployed and crime statistics for any location(s);

Additional ALPR cameras would be placed in strategic locations determined by thoroughfares, which are primary egress and ingress routes to Davis. Nine (9) intersections have been identified as being the most beneficial.

- Lake/Russell
- Lake/Covell
- 113/Covell
- 113/Russell
- Southbound CR 100A (which later turns into Sycamore Ln.) south of CR 29
- Southbound CR 99D (which later turns into John Jones Rd.) south of CR 29
- F St. south of CR 29
- Pole Line south of CR 29
- Mace/Montgomery

(c) An assessment identifying any potential impact on civil liberties and civil rights and discussing any plans to safeguard the rights of the public;

ALPR and public safety cameras do raise privacy issues. Fixed ALPR cameras are placed in locations that are open to the public and collect substantial amounts of data related to vehicles that pass through specific areas. Even when used for specific reasons, the camera will likely capture video unrelated to criminal activity. There are obvious concerns with having video data of the public, especially when there is no criminal activity depicted.

Additionally, there are concerns regarding data misuse and infringing upon individual rights by recording movements or location patterns of individuals seeking medical attention or health services for reproductive rights. Senate Bill 34 (Civil Code, § 1798.90.55, subd. (b)) prevents California law enforcement agencies from sharing ALPR data with private entities or out-of-state law enforcement agencies, including federal agencies. There are also issues regarding data being shared with immigration enforcement agencies. The California Values Act (Government Code 7284.6) and Senate Bill 34 (Civil Code, § 1798.90.55) restrict local law enforcement from sharing automated license plate reader data or personal information with any federal agency for immigration enforcement. Through policy, the Department will restrict the information collected from the ALPR cameras to only authorized Department members and prohibit sharing any data with federal immigration agencies, including Immigration and Customs Enforcement (ICE) and Customs and Border Patrol (CBP).

The American Civil Liberties Union (ACLU) has criticized law enforcement agencies' collection of ALPR images because of the risks it poses to privacy. The ACLU stated that increasing numbers of cameras, long data retention periods, and sharing of ALPR images among law enforcement agencies allow agencies to track individuals' movements in detail, and it has voiced concerns that such constant monitoring can inhibit the exercise of free speech and association.[4]

To provide safeguards, Davis Police Department policy must address privacy concerns. To ensure that data collected by ALPR cameras are used appropriately, the Department has developed a policy to address the following areas of concern:

[4] Auditor of the State of California. (2020). Automated License Plate Readers.

- ALPR shall only be used for official law enforcement purposes. Aggregate data may be used for traffic engineering projects upon approval of the Police Chief.
- All Department members must complete approved training prior to use.
- Employees shall not use to harass and/or intimidate an individual or group.
- Employees shall not share, disclose, or provide access to any ALPR data with federal immigration enforcement agencies, including Immigration and Customs Enforcement (ICE) or Border Patrol agents, consistent with existing State law.
- Employees shall not use ALPR data to target individuals based on their health or medical facility choices or to surveil individuals seeking reproductive healthcare services.
- Employees shall not use ALPR data to identify, track, or monitor individuals associated with reproductive health facilities, clinics, or services.
- Employees shall not take any police action that restricts an individual's freedom based solely on an ALPR alert/data.
- Officers shall visually verify that the license plate of interest matches identically with the image of the license plate number captured (read) by the LPR.

Additionally, the Department has selected Motorola as a preferred fixed public safety camera and ALPR provider for the following reasons:

- The Department currently has a contract with Motorola for all in-car police cameras, body-worn cameras and cloud-based storage of video data;
- The City has a contract with Motorola (Avigilon) for public safety cameras currently in use, and additional cameras can be easily added to the existing software and hardware;
- The provider has encrypted the transfer of data;
- The provider requires users to provide a law enforcement reason to search the system;
- The provider ensures the Department owns the rights to all images collected through their equipment and will ensure strict compliance with the Department's policy while stored on Motorola servers.

(d) The fiscal costs for the surveillance technology, including initial purchase, personnel and other ongoing costs, and any current or potential sources of funding;

Purchase Cost
The projected initial purchase cost for cameras (29), installation, hardware and associated software is ~$415,180.00.

Personnel Costs
Minimal to operate the systems.

Ongoing Costs
Annual recurring costs are ~$17,800.00.

Potential Sources of Funding
The Department intends to apply for a Department of Justice, Community Oriented Policing Services (COPS) grant to fund initial project costs. The Department of Justice (DOJ) Community Oriented Policing Services (COPS) Office grant program is designed to support law enforcement agencies in implementing community-oriented policing strategies. The

COPS Office grants provide funding, resources, and technical assistance to develop and improve these community policing efforts across the United States. The COPS Technology Program focuses on integrating technology into community policing efforts, providing funding for tools that enhance communication, data sharing, and overall effectiveness in policing. The Department intends to submit a funding request for all implementation costs associated with the project.

Ongoing costs are anticipated to be funded through the California Supplemental Law Enforcement Services Fund (SLESF). SLESF is a grant fund, and the enabling legislation mandates that each municipality receive funds yearly to be spent on "frontline law enforcement services."

(e) Whether use or maintenance of the technology will require data gathered by the technology to be handled or stored by a third-party vendor on an ongoing basis;
Data collected by Motorola is temporarily stored on the device (camera) until it is uploaded to their cloud provider (Azure GovCloud). The data is then removed from the local device. Once on the cloud, all footage and metadata is encrypted throughout its entire lifecycle, from on-device to storage in the cloud, and follows CJIS Security Policy guidance for encryption at rest and in transit using at least 128-bit ciphers. Motorola utilizes the Azure GovCloud for its cloud offerings for infrastructure hardware. Microsoft employs strict policies to protect all media within the Azure GovCloud and is listed as CJIS compliant with 37 states, including California. The Federal Risk and Authorization Management Program (FedRAMP) authorization by the Department of Homeland Security ensures media protection and disposal policies consistent with the CJIS Security Policy and the National Institute of Standards and Technology's (NIST) 800-53 controls, a comprehensive set of security and privacy controls for protecting information systems. Microsoft Azure Data Center and storage facilities exhibit extensive physical security controls that are in place and equivalent to or greater than CJIS Physically Secure Location criteria. Microsoft manages physical security at the colocation data center. They are responsible for physical security at that location and have been evaluated by Motorola Solutions staff and a third-party auditor.

Motorola does not share, sell, or use law enforcement-generated Criminal Justice Data in any way. Furthermore, any data retention policy or the sharing of an agency's data is entirely in the control of the agency. The Police Department would require a written contract with Motorola containing provisions that any ALPR system operator or third party that hosts ALPR information comply with all applicable laws regarding the collection, storage, use, access, sharing and retention of any ALPR information.

(f) A summary of the experience, if any, other governmental entities have had with the proposed technology, including information about the effectiveness, any known adverse information about the technology such as unanticipated costs, failures, civil rights or civil liberties abuses.
ALPR cameras are widely used by law enforcement agencies in the United States. Thousands of cities in the US use ALPR cameras, and the technology has become ubiquitous throughout the greater Sacramento region. In Yolo County, the Yolo County Sheriff's Office, West Sacramento Police Department, and Woodland Police Department currently utilize fixed ALPR cameras. Several agencies employ ALPR in Northern California and the Bay area, including Sacramento, Berkeley, Oakland, San Francisco, San Jose, Stockton, San Mateo, Vacaville and Richmond.

Many of the agencies using ALPR have provided example cases where the technology was critical in identifying a vehicle related to a criminal investigation, locating missing persons, or increasing the recovery rate of stolen vehicles. Vacaville PD participated in a long-term study to determine the effectiveness of their ALPR system. The results revealed an approximate 33% decrease in the number of reported stolen vehicles and a 35% increase in vehicle theft arrests. ALPR systems are known for their accuracy, which can approach 99% in controlled environments and 90–98% in real-world settings. ALPR systems can also help law enforcement agencies make more confident decisions, accurately identify suspects, and reduce the likelihood of wrongful accusations.

Primary concerns regarding the use of ALPR include data misuse, inadequate policies, failure to conduct audits, and sharing information with federal agencies involved in immigration enforcement.

Surveillance Use Policy

Proposed policies for City Council consideration and adoption are attached. (Attachment 1)

Attachments

1. Use Policy - Automatic License Plate Readers

Attachment 1

DAVIS POLICE DEPARTMENT

AUTOMATED LICENSE PLATE READERS (ALPR)
Policy 1000

DEPARTMENT MANUAL

1000.1 COUNCIL APPROVAL
On XXXX, the Davis City Council, in accordance with the Surveillance Technology Ordinance, adopted the following ALPR Use Policy (26.07.030 Davis Municipal Code).

1000.2 PURPOSE
The purpose of this policy is to provide guidance for the capture, storage, and use of digital data obtained through the use of Automated License Plate Reader (ALPR) technology. Department Members shall adhere to the requirements in this policy.

1000.3 POLICY
The policy of the Davis Police Department is to utilize ALPR technology to capture and store digital license plate data and images while recognizing the established privacy rights of the public.

All data and images gathered by the ALPR are for the official use of this Department. Because such data may contain confidential (CLETS) information, it is not open to public review.

The Davis Police Department does not permit the sharing of ALPR data gathered by the City for federal immigration enforcement, pursuant to the California Values Act (Government Code § 7282.5; Government Code § 7284.2 et seq) – these federal immigration agencies include Immigrations and Customs Enforcement (ICE) and Customs and Border Patrol (CBP).

1000.4 DEFINITIONS

(a) **Automated License Plate Reader (ALPR):** A fixed or mobile device that uses cameras and computer technology to compare digital images to lists of known information of interest during criminal investigations and as part of a comprehensive parking management system, including electronic vehicle chalking to enforce time limit parking restrictions and electronic parking permit management.

(b) **ALPR Operator:** Trained Department members who may utilize the ALPR system/ equipment. ALPR operators may be assigned to any position within the Department, and the ALPR Administrator may order the deployment of the ALPR systems for use in various efforts.

(c) **ALPR Administrator:** The Police Chief or thier designee serves as the Department's ALPR Administrator.

(d) **Hot List:** A list of license plates associated with vehicles of interest compiled from one or more databases including, but not limited to, NCIC, CA DMV, Local BOLOs, etc.

(e) **Vehicles of Interest:** Including, but not limited to vehicles that are reported as stolen, display stolen license plates or tags; vehicles linked to missing and/or wanted persons; vehicles flagged by the Department of Motor Vehicle Administration or law enforcement agencies and parking management, including electronic vehicle chalking to enforce time limit parking restrictions and electronic parking permit management.

(f) **Detection:** Data obtained by an ALPR of an image (such as a license plate) within public view that was read by the device, including potential images (such as the plate and description of the vehicle on which it was displayed), and information regarding the location of the ALPR system at the time of the ALPR's read.

(g) **Hit Alert:** Notification from the ALPR system that a scanned license plate number may be in the National Crime Information Center (NCIC) or other law enforcement database for a specific reason including, but not limited to, being related to a stolen car, wanted person, missing person, domestic violation protective order or terrorist-related activity.

1000.5 ADMINISTRATION

The ALPR technology, also known as License Plate Recognition (LPR), allows for the automated detection of license plates. It is used by the Davis Police Department to convert data associated with vehicle license plates for official law enforcement purposes, including identifying stolen or wanted vehicles, stolen license plates and missing persons. It may also be used to gather information related to active warrants, suspect apprehension and stolen property recovery. ALPR technology is also used as part of a comprehensive parking management system, including electronic vehicle chalking to enforce time limit parking restrictions and electronic parking permit management.

ALPR ADMINISTRATOR

The Police Chief, or their designee, shall be responsible for compliance with the requirements of Civil Code § 1798.90.5 et seq. This includes but is not limited to (Civil Code § 1798.90.51; Civil Code § 1798.90.53; Civil Code § 1798.90.55):

(a) Only properly trained sworn officers, crime analysts, police services specialists and public safety dispatchers are allowed access to the ALPR system or to collect ALPR information. The Police Chief may authorize other City employees to access the ALPR system for necessary purposes such as Information Technology or Systems maintenance, installation assistance or updates. This access may extend to CJIS approved vendors.

(b) Ensuring that training requirements are identified and completed for authorized users.

(c) Ensuring that when an authorized user leaves the employment of the Davis Police Department, that user’s account shall be disabled.

(d) ALPR system monitoring to ensure the security of the information and compliance with applicable privacy laws.

(e) Ensuring procedures are followed for system operators to maintain records of access in compliance with Civil Code § 1798.90.52.

(f) Working with the Custodian of Records and vendor on the retention and destruction of ALPR data.

(g) Ensure this policy and related procedures are conspicuously posted on the City's website.

(h) Ensuring a written contract with any ALPR system operator or third-party vendor hosting any ALPR information that the Department collects and provides to third-party vendors to host. Any such contract must contain provisions that any ALPR system operator or third party that hosts ALPR information comply with all applicable laws regarding the collection, storage, use, access, sharing and retention of any ALPR information.

1000.6 PROCEDURE

An ALPR shall only be used for official law enforcement business. Use of an ALPR is restricted to the purposes outlined below. Department members shall not use or allow others to use the equipment or database records for any unauthorized purpose (Civil Code § 1798.90.51; Civil Code § 1798.90.53; Civil Code § 1798.90.55).

(a) An ALPR shall only be used for official law enforcement business.

(b) An ALPR may be used in conjunction with any routine patrol operation or to support criminal investigations. Reasonable suspicion or probable cause is not required before using an ALPR database.

(c) Partial license plates and unique vehicle descriptions reported during crimes may be entered into the ALPR system in an attempt to identify suspect vehicles.

(d) No member of this Department shall operate ALPR equipment or access ALPR data without first completing Department-approved training.

(e) If feasible, the officer shall verify an ALPR response through the California Law Enforcement Telecommunications System (CLETS) before taking enforcement action that is based solely on an ALPR alert. Once an alert is received, the operator shall confirm that the observed license plate from the system matches the license plate of the observed vehicle. Before any law enforcement action is taken in response to an ALPR alert, the alert will be verified through a CLETS inquiry via in-car computer or through Dispatch.

(f) Members will not take any police action that restricts the freedom of any individual based solely on an ALPR alert unless it has been validated. Because the ALPR alert may relate to a vehicle and may not relate to the person operating the vehicle, officers are reminded that they need to have reasonable suspicion and/or probable cause to make an enforcement stop of any vehicle. (For example, if a vehicle is entered into the system because of its association with a wanted individual, Officers should attempt to visually

match the driver to the description of the wanted subject prior to making the stop or should have another legal basis for making the stop.)

(g) The Police Chief may authorize other City employees to access the non-confidential data from the ALPR system to study parking patterns as part of a comprehensive parking management plan or to assist with traffic engineering.

(h) Hot Lists. Designation of hot lists to be utilized by the ALPR system shall be made by the ALPR Administrator or their designee. Hot Lists shall be obtained or compiled from sources as may be consistent with the purposes of the ALPR system set forth in this Policy. Hotlists utilized by the Department's ALPR system may be updated by agency sources more frequently than the Department may be uploading them, and thus, the Department's ALPR system will not have access to real-time data. Occasionally, errors in the ALPR system's reading of a license plate may occur. Therefore, an alert alone shall not be a basis for police action (other than following the vehicle of interest). Prior to initiation of a stop of a vehicle or other intervention based on an alert, Department members shall undertake the following:

1. Verification of status on a Hot List: An officer must receive confirmation from a Davis Police Department Public Safety Dispatcher or other Department computer device that the license plate or vehicle is still stolen, wanted, or otherwise of interest before proceeding (absent exigent circumstances).

2. Visual verification of license plate number: Officers shall visually verify that the license plate of interest matches identically with the image of the license plate number captured (read) by the ALPR, including both the alphanumeric characters of the license plate, state of issue, and vehicle descriptors before proceeding. Department members alerted to the fact that an observed motor vehicle's license plate is entered as a hot plate (hit) in a specific BOLO (be on the lookout) list are required to make a reasonable effort to confirm that a wanted person is actually in the vehicle and/or that a reasonable basis exists before a Department member would have a lawful basis to stop the vehicle.

3. Department members will clear all stops from hot list alerts by indicating the positive ALPR hit, i.e., with an arrest or other enforcement action. If it is not obvious in the text of the call as to the correlation between the ALPR hit and the arrest, then the Department member shall update the Public Safety Dispatcher and original member and/or a crime analyst inputting the vehicle in the hot list (hit).

4. General Hot Lists (SVS, SFR, and SLR) will be automatically downloaded into the ALPR system a minimum of once a day, with the most current data overwriting the old data.

5. All entries and updates of specific Hot Lists within the ALPR system will be documented by the requesting Department member within the appropriate general offense report. As such, specific Hot Lists shall be approved by the ALPR Administrator.

6. All entries and updates of specific Hot Lists within the ALPR system will be documented by the requesting Department member within the appropriate general offense report. As such, specific Hot Lists shall be approved by the ALPR

Administrator (or their designee) before initial entry within the ALPR system. The updating of such a list within the ALPR system shall thereafter be accomplished pursuant to the approval of the Department member's immediate supervisor. The hits from these data sources should be viewed as informational, created solely to bring the officer's attention to specific vehicles that have been associated with criminal activity.

All Hot Plates and suspect information entered into the ALPR system will contain the following information at a minimum:

- Entering Department member's name
- Related case number
- Short synopsis describing the nature of the originating incident

Login/Log-Out Procedure: To ensure proper operation and facilitate oversight of the ALPR system, all users will be required to have individual credentials for access and use of the systems and/or data, which has the ability to be fully audited.

Permitted/Impermissible Uses: The ALPR system and all data collected are the property of the Davis Police Department. Department members may only access and use the ALPR system for official and legitimate California law enforcement purposes consistent with this Policy. The following uses of the ALPR system are expressly prohibited:

1. **Invasion of Privacy:** Except when done pursuant to a court order such as a search warrant, it is a violation of this Policy to utilize the ALPR to record license plates except those of vehicles that are exposed to public view (e.g., vehicles on a public road or street, or that are on private property but whose license plate(s) are visible from a public road, street, or a place to which members of the public have access, such as the parking lot of a shop or other business establishment).

2. **Harassment or Intimidation:** It is a violation of this Policy to use the ALPR system to harass and/or intimidate any individual or group.

3. **Use Based on a Protected Characteristic**: It is a violation of this Policy to use the LPR system or associated scan files or hot lists solely because of a person's or group's race, gender, religion, political affiliation, nationality, ethnicity, sexual orientation, disability, or other classification protected by law.

4. **Personal Use:** It is a violation of this Policy to use the ALPR system or associated scan files or hot lists for any personal purpose.

5. **Reproductive Rights:** ALPR data shall not be used to target individuals based on their reproductive health choices or to surveil individuals seeking reproductive healthcare services. Members shall not use ALPR data to identify, track, or monitor individuals associated with reproductive health facilities, clinics, or services.ALPR data shall not be shared with out-of-state law enforcement agencies (Civil Code § 1798.90.55).

6. **Federal Immigration Enforcement:** Members shall not share, disclose, or provide access to any ALPR data with federal immigration enforcement agencies, including Immigration and Customs Enforcement (ICE) or Border Patrol agents. Requests for

ALPR data from these agencies will be denied, and members must refer such inquiries to a designated supervisor (Government Code 7284.6; Civil Code § 1798.90.55).

7. **First Amendment Rights:** This Policy prohibits the use of the ALPR system, associated scan files, or hot lists to infringe upon First Amendment rights.

No ALPR operator may access California Law Enforcement Telecommunications System (CLETS) data unless otherwise authorized to do so. If practicable, the officer should verify an ALPR response through the California Law Enforcement Telecommunications System (CLETS) before taking enforcement action based solely on an ALPR alert.

1000.7 DATA COLLECTION AND RETENTION

The Deputy Director of Police Services is responsible for ensuring systems and processes are in place for the proper collection and retention of ALPR data. Data will be transferred from devices to the designated storage in accordance with Department procedures. Evidentiary hit data or other related ALPR data shall be treated in the same manner as other evidence. Data shall be accessed, maintained, stored, and retrieved in a manner that ensures its integrity as evidence, including strict adherence to chain of custody requirements.

All ALPR data downloaded to the ALPR server should be stored for no longer than one year and in accordance with the established records retention schedule. Thereafter, ALPR data should be purged unless it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action or is subject to a discovery request or other lawful action to produce records.

The ALPR vendor will store the data (data hosting) and ensure proper maintenance and security of data stored in their data center. The ALPR vendor will purge data at the end of the one year of storage. However, this will not preclude the Department from maintaining any relevant vehicle data obtained from the system after that period pursuant to the established City of Davis retention schedule mentioned above or outlined elsewhere. Relevant vehicle data are scans corresponding to the vehicle of interest on a hot list. The ALPR vendor and Department shall ensure that the necessary data is captured and stored to accurately report the relevant data required in the Annual Surveillance Technology report. Once the City Council approves the Annual Surveillance Technology report, all said data may be purged as long as it doesn't violate the City Retention guidelines.

Restrictions on Use of Vendor Data: Information gathered or collected and records retained by the Davis Police Department ALPR system will not be sold, accessed, or used for any purpose other than legitimate California law enforcement or public safety purposes.

1000.8 ACCOUNTABILITY

All saved data will be safeguarded and protected by procedural and technological means. The Davis Police Department will observe the following safeguards regarding access to and use of stored data (Civil Code § 1798.90.51; Civil Code § 1798.90.53):

(a) Non-law enforcement requests for access to stored ALPR data shall be processed according to the Release of Records/Public Records Act Policy in accordance with applicable law.

(b) All ALPR data downloaded to any workstation or server shall be accessible only through a login/password-protected system.

(c) Davis Police Department members approved to access ALPR data under these guidelines are permitted to access the data for legitimate California law enforcement purposes only, such as when the data relates to a specific criminal investigation or Department-related civil or administrative action.

(d) Aggregated ALPR data not related to specific criminal investigations shall not be released to any local or State entity without the consent of the Police Chief (i.e., Permissible use could include the Public Works Engineering & Transportation Department's request for non-confidential (anonymized) data for the volume of vehicular traffic associated with specific events, roads or intersections).

(e) The Professional Standards Lieutenant will conduct ALPR system audits regularly, at least annually.

(f) ALPR data may be released to other authorized and verified California law enforcement officials and agencies for legitimate law enforcement purposes (Civil Code § 1798.90.53).

(g) Every ALPR Detection Browsing Inquiry must be documented by either the associated Davis Police Department case number or incident number, and/or a reason for the inquiry.

(h) Any member who negligently engages in an impermissible use of the ALPR system or associated scan files or hot lists may be subject to criminal prosecution and/or administrative sanctions, up to and including termination.

1000.9 ALPR DATA DETECTION BROWSING AUDITS

The Professional Standards Lieutenant or the Chief's designee is responsible for ensuring that an audit of ALPR detection browsing inquiries is conducted at least annually. The Department will audit a sampling of the ALPR system utilization from the prior 12-month period to verify proper use in accordance with the above-authorized uses. The audit shall randomly select at least five detection browsing inquiries conducted by Department employees during the preceding 12-month period and determine if each inquiry meets the requirements established in policy.

The audit shall be documented in an internal Department memorandum to the Police Chief. After the Police Chief reviews the memorandum and any associated documentation, the Professional Standards Lieutenant shall file and retain it. This audit should be shared in the Surveillance Technology report.

1000.10 RELEASING ALPR DATA

The ALPR data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law.

(a) The release of ALPR data to any third party will be processed in a manner consistent with applicable Departmental policy, law and current discovery requests. When criminal

charges are being sought, all related data will be provided to the District Attorney's Office.

(b) The digitally recorded ALPR data is the property of the Davis Police Department. Dissemination outside the agency is strictly prohibited without specific authorization of the Police Chief or their designee.

(c) ALPR data is subject to the provisions of the Davis Police Department's Immigration Policy (423) and may not be shared with federal immigration enforcement officials.

1000.11 TRAINING

The Training Coordinator shall ensure that members receive Department-approved training to be authorized to use or access the ALPR system. Training shall include the following topics at minimum.

(a) Overview of ALPR technology.

(b) Legal framework and compliance requirements.

(c) Ethical considerations.

(d) Data analysis and interpretation.

(e) Reporting and accountability.

Todd Henry
Police Chief