



Office of the City Manager

ACTION CALENDAR
November 10, 2025

To: Honorable Mayor and Members of the City Council

From: Paul Buddenhagen, City Manager

Submitted by: Jennifer Louis, Chief of Police

Subject: Annual Surveillance Technology Report for Body Worn Cameras, GPS Trackers, Fixed Surveillance Video Cameras, Parking Enforcement Officer Automated License Plate Readers, the Street Level Imagery Project, Unmanned Aerial Systems, and Fixed Automated License Plate Readers

RECOMMENDATION

Pursuant to Chapter 2.99 of the Berkeley Municipal Code, adopt a resolution accepting the Surveillance Technology Report for Body Worn Cameras, GPS Trackers, Fixed Surveillance Video Cameras, Automated License Plate Readers, the Street Level Imagery Project, Unmanned Aerial Systems, and Fixed Automated License Plate Readers.

FISCAL IMPACTS OF RECOMMENDATION

These technologies have existing budget approval and there are no new fiscal impacts associated with adopting the attached resolution.

CURRENT SITUATION AND ITS EFFECTS

On March 27, 2018, the City Council adopted Ordinance 7,592-N.S., adding Chapter 2.99 to the Berkeley Municipal Code, which is also known as the Surveillance Technology Use and Community Safety Ordinance (referred to here as the Ordinance). Section 2.99.070 of the Ordinance requires that the City Manager must submit to the City Council a Surveillance Technology Report as defined by Section 2.99.020(2) of the Ordinance annually, at the first regular City Council meeting in November.

The purpose of the Ordinance is to provide transparency surrounding the use of surveillance technology, as defined by Section 2.99.020 of the City's Municipal Code, and to ensure that decisions surrounding the acquisition and use of surveillance technology consider the impacts that such technology may have on civil rights and civil liberties. Further, the Ordinance requires that the City evaluate all costs associated with

the acquisition of surveillance technology and regularly report on their use. The purpose of this staff report and attached resolution is to satisfy the annual reporting requirement as outlined in Section 2.99.070. For each of the seven approved technologies, Annual Surveillance Technology Report and accompanying audits (where required by BPD policy) are attached to this report. These reports fulfill all section-by-section reporting requirements of the Ordinance.

One of the mandated reporting categories of the Ordinance is whether complaints have been received by the community about Police Department's use of surveillance technologies. To date, Berkeley Police Department Internal Affairs Bureau (IAB) has not received any external personnel complaints surrounding these technologies. External complaints from community members can be made in writing, via email, in person or via telephone. Complaints can be received with direct communication to the Internal Affairs Bureau from the complainant and/or be received by any member of the Department and then forwarded through the chain of command. If a community member initiates a complaint against a subject employee and during the investigation it is determined the subject employee violated policy regarding the misuse of technology, an additional complaint is initiated by the Chief of Police.

Community members also have the right to initiate complaints against employees of BPD by reporting directly to the Office of the Director of Police Accountability (ODPA). The Director of Police Accountability notifies the Chief of Police when an investigation into a complaint is initiated by the PAB, which would prompt a parallel IAB investigation.

An additional reporting category covers audits. All audits required by policy were completed during this reporting period. The only audit finding resulted from the fixed automated license plate reader (ALPR) audit, the first audit conducted since this technology was fully implemented earlier this year. The complete audit is included in Attachment 8. The audit confirmed that all Berkeley Police Department users complied with Policy 1305 requirements. External agencies demonstrated 100% authorized access and 99.81% compliance with permitted search reasons. In response to the small number of statewide searches that included federal acronyms, the Department tightened sharing controls to exclude out-of-region agencies, disabled the statewide lookup feature, and instituted new protocols to revoke access when a partner agency's search appears inconsistent with policy. Additional roll call training and vendor-side safeguards are being developed to ensure that the system continues to align with both state law and Berkeley's Sanctuary City Ordinance.

During this reporting period, the City advanced a major surveillance technology initiative with the ALPR system. The ALPR network, consisting of 52 cameras approved by Council, became fully operational following the conclusion of its introductory phase in January 2025, and has since resulted in more than 50 arrests and 40 recovered stolen vehicles that likely would not have occurred without the technology.

Work is also underway on the Council referrals related to additional fixed surveillance cameras. This technology, like the existing ALPR system, works to support public safety and criminal investigations.

ENVIRONMENTAL SUSTAINABILITY AND CLIMATE IMPACTS

There are no identifiable environmental effects or opportunities associated with the content of this report.

RATIONALE FOR RECOMMENDATION

City Council is being requested to adopt the attached resolution for the City to be in compliance with the Ordinance.

CONTACT PERSON

Jennifer Louis, Chief of Police, (510) 981-5700

Arlo Malmberg, Strategic Planning and Accountability Manager, (510) 981-5747

ATTACHMENTS

1. Resolution
2. Surveillance Technology Report: Body Worn Cameras
3. Surveillance Technology Report: Global Positioning System (GPS) Tracking Devices
4. Surveillance Technology Report: Fixed Surveillance Video Cameras
5. Surveillance Technology Report: Parking Enforcement Automated License Plate Readers
6. Surveillance Technology Report: Street Level Imagery Project
7. Surveillance Technology Report: Unmanned Aerial Systems (UAS)
8. Surveillance Technology Report: Fixed Automated License Plate

RESOLUTION NO. XX,XXX-N.S.

A RESOLUTION ACCEPTING THE SURVEILLANCE TECHNOLOGY REPORT FOR BODY WORN CAMERAS, GPS TRACKERS, FIXED SURVEILLANCE VIDEO CAMERAS, PARKING ENFORCEMENT OFFICER AUTOMATED LICENSE PLATE READERS, THE STREET LEVEL IMAGERY PROJECT, UNMANNED AERIAL SYSTEMS, AND FIXED AUTOMATED LICENSE PLATE READERS

WHEREAS, on March 27, 2018, the City Council adopted Ordinance 7,592-N.S., which is known as the Surveillance Technology Use and Community Safety Ordinance ("Ordinance"); and

WHEREAS, Section 2.99.070 of the Ordinance requires that the City Manager must submit to the City Council a Surveillance Technology Report as defined by Section 2.99.020(2) of the Ordinance at the first regular City Council meeting in November; and

WHEREAS, the Surveillance Technology Reports satisfy the requirements of the Ordinance.

NOW THEREFORE, BE IT RESOLVED by the Council of the City of Berkeley that the Council hereby accepts the Surveillance Technology Reports for Body Worn Cameras, GPS Trackers, Fixed Surveillance Video Cameras, Parking Enforcement Officer Automated License Plate Readers, the Street Level Imagery Project, Unmanned Aerial Systems, and Fixed Automated License Plate Readers.

Surveillance Technology Report: Body Worn Cameras**October 1, 2024 – Sept. 30, 2025**

Description	A description of all non-privileged and non-confidential information about use of the Surveillance Technology, including but not limited to the quantity of data gathered and sharing of data, if any, with outside entities. If sharing has occurred, the report shall include general, non-privileged and non-confidential information about recipient entities, including the names of the entities and purposes for such sharing. Body Worn Cameras are used to capture video recordings of contacts between department personnel and the public, to provide an objective record of these events. These recording are used in support of criminal prosecutions, to limit civil liability, increase transparency and enhance professionalism and accountability in the delivery of police services to the community. Body Worn Camera (BWC) files are shared with the Alameda County District Attorney's office in support of prosecution for crime and may be shared with other law enforcement agencies to support criminal investigations. Policy regarding activation of the Body Worn Camera BPD Policy 425.7 Members shall activate the BWC as required by this policy in (a)-(f) below and may activate the BWC at any time the member believes it would be appropriate or valuable to record an incident within the limits of privacy described herein. The BWC shall be activated in any of the following situations: (a) All in-person enforcement and investigative contacts including pedestrian stops and field interview (FI) situations. (b) Traffic stops including, but not limited to, traffic violations, stranded motorist assistance and all crime interdiction stops. (c) Self-initiated field contacts in which a member would normally notify the Communications Center. (d) Any search activity, including the service of search or arrest warrants; probation, parole, or consent searches where the member is seeking evidence of an offense, or conducting a safety sweep or community caretaking sweep of the premises. Once a location has been secured and the member is not interacting with detainees or arrestees, the member may mute their BWC when conducting a search for evidence.
-------------	--

(e) Any other contact that the member determines has become adversarial after the initial contact in a situation where the member would not otherwise activate BWC recording.

(f) Transporting any detained or arrested person and where a member facilitates entry into or out of a vehicle, or any time the member expects to have physical contact with that person.

What data is captured by this technology:

BWC use is limited to enforcement and investigative activities involving members of the public. The BWC recordings will capture video and audio evidence for use in criminal investigations, administrative reviews, training, civil litigation, and other proceedings protected by confidentiality laws and department policy. Improper use or release of BWC recordings may compromise ongoing criminal and administrative investigations or violate the privacy rights of those recorded and is prohibited.

How the data is stored:

BWC videos are stored on a secure server. All BWC data will be uploaded and stored on Axon Cloud Services, Evidence.com. Axon complies with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union and Switzerland to the United States (collectively, "Privacy Shield"). Axon has certified to the U.S. Department of Commerce that it adheres to the Privacy Shield Principles.

Retention duration of digital data:

All BWC videos and digital evidence are assigned a category. The categories are used to organize data. Each category also defines the retention duration. The category definitions and retention durations are as follows:

Category	Retention Duration
Uncategorized	Until manually deleted
187 / Felony Sex Assault	Until manually deleted
Civil / City / Non-Evidence	1 year
Collision	2 years
Consent / Aid	108 weeks
Detention / Warrant Only	108 weeks
Felony Evidence	5 years

	Litigation	Until manually deleted														
	Misdemeanor Evidence	2 years														
	Officer Injury	Until manually deleted														
	OIS / Critical Incident	Until manually deleted														
	Pending Review	Until manually deleted														
	Personnel / VSA	3 years														
	Personnel Complaint	Until manually deleted														
	Traffic Stop	108 weeks														
	Training	60 days														
	Use of Force	108 weeks														
Summary of Body Worn Camera Videos Uploaded Oct. 1, 2024 to Sept. 30, 2025:																
<table><tr><th>Metric</th><th>Value</th></tr><tr><td>Number of BWC Videos</td><td>67,803</td></tr><tr><td>Hours of Videos</td><td>15,853</td></tr><tr><td>GB of Videos</td><td>27,561</td></tr></table>			Metric	Value	Number of BWC Videos	67,803	Hours of Videos	15,853	GB of Videos	27,561						
Metric	Value															
Number of BWC Videos	67,803															
Hours of Videos	15,853															
GB of Videos	27,561															
Summary of all other active digital evidence uploaded, Oct. 1, 2024 to Sept. 30, 2025:																
<table><tr><th>Type</th><th>File Count</th></tr><tr><td>Audio</td><td>1,509</td></tr><tr><td>Document</td><td>2,745</td></tr><tr><td>Image</td><td>70,854</td></tr><tr><td>Other</td><td>1,188</td></tr><tr><td>Other Video*</td><td>9,870</td></tr><tr><td>Total</td><td>86,166</td></tr></table>			Type	File Count	Audio	1,509	Document	2,745	Image	70,854	Other	1,188	Other Video*	9,870	Total	86,166
Type	File Count															
Audio	1,509															
Document	2,745															
Image	70,854															
Other	1,188															
Other Video*	9,870															
Total	86,166															
* Includes all uploaded non-BWC videos and other videos booked into the evidence management system. Other videos include iPhone videos, security camera video, and copies of BWC videos (for redaction, etc.).																
Geographic Deployment	Where applicable, non-privileged and non-confidential information about where the surveillance technology was deployed geographically. Body Worn Cameras are worn by all BPD uniformed officers city-wide at all times; BWC’s are not deployed based on geographic considerations.															
Complaints	A summary of each complaint, if any, received by the City about the Surveillance Technology.															

	There have been no complaints about the deployment and use of Body Worn Cameras.
Audits and Violations	The results of any non-privileged internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response. File meta-data are routinely reviewed by our BWC manager, to ensure required metadata fields are completed. There have been no complaints with regards to violations of the Surveillance Use Policy.
Data Breaches	Non-privileged and non-confidential information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response. There have been no known data breaches or other unauthorized access to BWC data.
Effectiveness	Information that helps the community assess whether the Surveillance Technology has been effective in achieving its identified outcomes. Body Worn Cameras have proven effective in supporting criminal prosecutions, as video footage is available for all criminal prosecutions. Body Worn Cameras have been effective for training purposes, as footage can be reviewed in incident de-briefs. Body Worn Cameras have been extremely effective in support of Internal Affairs investigations and Use of Force Review.
Costs	Total annual costs for the Surveillance Technology, including personnel and other ongoing costs. The annual cost for the Body Worn Cameras, including cameras, replacement cameras, software, and Axon's secure digital evidence management system is \$222,442 per year over a five-year, \$1,112,213 contract. The contract started in 2022 and will expire in August, 2026. There is one full-time employee assigned to the BWC program, an Applications Programmer Analyst II, at a cost of \$168,940 per year, including benefits.

Surveillance Technology Report: Global Positioning System Tracking Devices**October 1, 2024 – Sept. 30, 2025**

Description	A description of all non-privileged and non-confidential information about use of the Surveillance Technology, including but not limited to the quantity of data gathered and sharing of data, if any, with outside entities. If sharing has occurred, the report shall include general, non-privileged and non-confidential information about recipient entities, including the names of the entities and purposes for such sharing. Global Positioning System Trackers are used to track the movements of vehicles, bicycles, other items, and/or individuals. What data is captured by this technology: A GPS Tracker data record consists of date, time, latitude, longitude, map address, and tracker identification label. The data does not contain any images, names of subjects, vehicle information or other identifying information on individuals. How the data is stored: The data from the GPS tracker is encrypted by the vendor. The data is only accessible through a secure website to BPD personnel who have been granted security access. Retention period of data: Tracker data received from the vendor shall be kept in accordance with applicable laws, BPD policies that do not conflict with applicable law or court order, and/or as specified in a search warrant. The Global Positioning System “Electronic Stake Out” (ESO) devices were not deployed during this reporting period. COVERTTRACK Stealth V GPS devices were used in four separate investigations during this reporting period: • An investigation of a shooting. The suspect was arrested for PC 245 numerous other violations. • An investigation of a carjacking. The suspect was arrested for PC 215 (via gun) and firearm violations.
-------------	--

	• An investigation of a robbery. The suspect was arrested for PC 211 and multiple counts of PC 459/PC 487 (Organized Retail Theft). • An investigation of a robbery. The investigation is ongoing. Data may be shared with the District Attorney's Office for use as evidence to aid in prosecution, in accordance with laws governing evidence; other law enforcement personnel as a part of an active criminal investigation; and other third parties, pursuant to a court order.
Geographic Deployment	Where applicable, non-privileged and non-confidential information about where the surveillance technology was deployed geographically. COVERTTRACK Stealth V GPS devices are deployed with judicial pre-approval, based on suspect location, rather than geographical consideration.
Complaints	A summary of each complaint, if any, received by the City about the Surveillance Technology. There were no complaints made regarding GPS Trackers.
Audits and Violations	The results of any non-privileged internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response. There were no known violations relating to GPS Trackers.
Data Breaches	Non-privileged and non-confidential information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response. There were no known data breaches relating to GPS Trackers.
Effectiveness	Information that helps the community assess whether the Surveillance Technology has been effective in achieving its identified outcomes. The GPS ESO trackers were not used during this time period. The program was suspended in mid-March 2020 due to the COVID-19 pandemic and has not been reimplemented. Our subscription was renewed and we upgraded our equipment, however, we have not used the trackers during this reporting period. COVERTTRACK Stealth V GPS trackers are effective in that they provide invaluable information on suspect vehicle locations. During complex investigations, many suspects are moving throughout the Bay area and beyond. These devices assist investigators with developing information regarding suspect locations that may never have been discovered without GPS assistance.

	GPS trackers greatly reduce costs associated with surveillance operations. Surveillance operations generally involve three or more officers for the entire duration of an operation. A moving surveillance is extremely resource-intensive, requiring multiple officers in multiple vehicles for extended periods of time. Evidence can be fleeting, and GPS trackers allow officers to investigate in a timely manner. GPS trackers have assisted officers with recovering evidence that may have been removed or discarded if officers were unable to quickly develop a location for a suspect.
Costs	Total annual costs for the Surveillance Technology, including personnel and other ongoing costs. The annual cost for the COVERTTRACK Stealth V GPS data service is \$1,834.53. There was no cost for the GPS “Electronic Stake Out” (ESO) this year. In April of 2022, the police department paid \$2,364.88 to upgrade the devices and for three years of tracking service. There are staff time costs associated with preparing and placing COVERTTRACK GPS trackers. The investigator must prepare a search warrant and obtain a judge’s approval, and a small number of officers must place the tracker on the suspect’s car. The total number of hours is a fraction of the time it would take to do a full surveillance operation involving numerous officers. There are staff time costs associated with preparing ESO trackers and placing ESO tracker-equipped bikes for bait bike operations. The time associated to prepare an ESO GPS equipped surveillance is approximately two-four hours. The total number of hours is extremely small, given the large number of operations, and resulting arrests from prior cases.

Surveillance Technology Report: External Fixed Surveillance Video Cameras**October 1, 2024 – Sept. 30, 2025**

Description	A description of all non-privileged and non-confidential information about use of the Surveillance Technology, including but not limited to the quantity of data gathered and sharing of data, if any, with outside entities. If sharing has occurred, the report shall include general, non-privileged and non-confidential information about recipient entities, including the names of the entities and purposes for such sharing. External fixed surveillance cameras record video (without audio) to support investigations. Officers can view live feeds and access recordings stored for up to 180 days. These cameras provide situational awareness during active incidents and supply evidence that strengthens investigations and helps the District Attorney make charging decisions. What data is captured by this technology: The external fixed surveillance cameras record and capture non-audio activity (data) for the following purposes: i. To address identified areas of criminal activity. ii. To respond to critical incidents. iii. To assist in identifying, apprehending and prosecuting offenders. iv. To document officer and offender conduct during interactions to safeguard the rights of the public and officers. v. To monitor pedestrian and vehicle traffic activity in order to assist with traffic related investigations. vi. To document employee, employer, and/or customer conduct during interactions to safeguard the employee, employer, and customer from misconduct. How the data is stored: The data on the external fixed video surveillance cameras is stored in secure servers that are managed by the City of Berkeley Radio Shop. Each camera system (San Pablo Park, Berkeley Marina, University Avenue and Sixth Street) has its own respective server for data storage.
-------------	--

	Retention period of data: Video surveillance recordings are not government records pursuant to California Government Code 34090 in and of themselves. Except as otherwise permitted in this section, video surveillance recordings shall be purged within one hundred and eighty (180) days of recording. The external fixed video surveillance cameras at University Avenue and Sixth Street were accessed 17 times during this reporting period for investigations of robbery and assault with a deadly weapon cases. The external fixed video surveillance cameras at San Pablo Park were accessed 15 times during this reporting period for investigations of homicide, robbery, property crime and traffic cases. The external fixed video surveillance cameras at the Berkeley Marina were accessed 24 times during this reporting period for investigations of property crimes and robbery cases. The Avigilon platform was accessed 5 times for administrative reasons during this reporting period. Data may be shared with the District Attorney's Office for use as evidence to aid in prosecution, in accordance with laws governing evidence; other law enforcement personnel as a part of an active criminal investigation; and other third parties, pursuant to a court order.
Geographic Deployment	Where applicable, non-privileged and non-confidential information about where the surveillance technology was deployed geographically. The external fixed video surveillance cameras are geographically deployed at San Pablo Park, the Berkeley Marina, and at the intersection of University Avenue and Sixth Street.
Complaints	A summary of each complaint, if any, received by the City about the Surveillance Technology. There were no known complaints associated with the external fixed video surveillance cameras.
Audits and Violations	The results of any non-privileged internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response. The required audits were completed and are attached below.

Data Breaches	Non-privileged and non-confidential information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response. There were no known data breaches related to the external fixed video surveillance cameras.
Effectiveness	Information that helps the community assess whether the Surveillance Technology has been effective in achieving its identified outcomes. External fixed video surveillance cameras monitor pedestrian and vehicle activity and can assist investigators with criminal and traffic related investigations. The cameras are also meant to prevent and deter criminal activity and augment police resources in a cost-effective manner.
Costs	Total annual costs for the Surveillance Technology, including personnel and other ongoing costs. The initial cost of the San Pablo Park Cameras was \$64,829.46 The initial cost of the Marina cameras was \$106,620.14 The annual cost for maintenance and other ongoing costs, including compliance and other reporting and oversight requirements is \$13,443.20. The amount originally made available for the Edgeworth contract was \$600,000.



Berkeley Police Department Memorandum



To: Chief Louis

From: Arlo Malmberg, Strategic Planning and Accountability Manager

RE: Avigilon Surveillance Camera Audit – July 2024 to December 2024

OVERVIEW

The Berkeley Police Department's Strategic Planning and Accountability Manager conducted an audit of the Avigilon camera system to assess compliance with Policy 1304, Surveillance Use Policy – External Fixed Video Surveillance Cameras. The audit scope included access records for the Avigilon camera system between July 1, 2024 and December 31, 2024 at the following locations: Marina, San Pablo Park, and the intersection of 6th Street and University Avenue. The audit methodology involved analyzing these access records for unauthorized access, data breaches, and prohibited uses.

The audit found full compliance with Policy 1304, with no instances of unauthorized access, data breaches, data errors, or prohibited uses detected. All system access was made by authorized personnel as stipulated in the policy.

BACKGROUND

Policy 1304 requires that surveillance camera data may only be accessed by trained and authorized BPD members for legitimate law enforcement purposes. Prohibited uses include discriminatory targeting, unauthorized dissemination of video footage, or surveillance inconsistent with civil liberties protections

SCOPE AND METHODOLOGY

The scope of this audit included all access records for the Avigilon camera system between July 1, 2024 and December 31, 2024.

The audit methodology involved:

1. Retrieving Avigilon camera system access records for the specified timeframe from the Avigilon platform.

2. Analyzing the records for any instances of unauthorized access, data breaches, or prohibited uses.
3. Verifying that all system access was made by authorized personnel as stipulated in Policy 1304.

SUMMARY OF FINDINGS

Objective #	Audit Objectives	% Meeting Standards
1	Authorized access to camera system	100%
2	No data breaches	100%
3	No prohibited uses	100%

DETAILED FINDINGS**Objective 1: Authorized access****Criteria:**

1304.4 DATA ACCESS: "Access to video surveillance cameras data shall be limited to BPD personnel utilizing the camera database for uses described above and pursuant to Use Policy 351"

Inspection Procedure:

- Review all access records for the Avigilon camera system during the audit period.
- Verify that all access was made by authorized personnel.

Findings:

- All access by BPD staff to the Avigilon camera system was made by authorized personnel.
- System maintenance access by other City of Berkeley staff was also noted.

Recommendations:

- None. The 100% compliance rate meets department standards.

Objective 2: No prohibited uses

Criteria:

1304.11 AUDITING AND OVERSIGHT: " BPD will enforce against prohibited uses of this policy pursuant to Policy 1010, Personnel Complaints or other applicable law or policy. The City Manager shall enforce against any prohibited use of the cameras and/or access to data by other City of Berkeley personnel."

Inspection Procedure:

- Review access records for any indication of prohibited uses of the camera system or data.

Findings:

- No prohibited uses of the camera system or associated data were detected during the audit period.
- Marina: 3 accesses, all for property crime investigations.
- San Pablo Park: 23 accesses, including 9 for homicide investigations, 3 for robbery investigations, 3 for traffic investigations, 2 for property crimes investigations, and 6 accesses for administrative purposes.
- 6th Street & University: 6 accesses, including 2 for robbery investigations, 2 for traffic investigations, 1 for a property crime investigation and 1 for a homicide investigation.

Recommendations:

- None. The 100% compliance rate meets department standards.



Berkeley Police Department Memorandum



To: Chief Louis

From: Arlo Malmberg, Strategic Planning and Accountability Manager

RE: Avigilon Surveillance Camera Audit – January 2025 to June 2025

OVERVIEW

The Berkeley Police Department's Strategic Planning and Accountability Manager conducted an audit of the Avigilon camera system to assess compliance with Policy 1304, Surveillance Use Policy – External Fixed Video Surveillance Cameras. The audit scope included access records for the Avigilon camera system between January 1, 2025 and June 30, 2025 at the following locations: Marina, San Pablo Park, and the intersection of 6th Street and University Avenue. The audit methodology involved analyzing these access records for unauthorized access, data breaches, and prohibited uses.

The audit found full compliance with Policy 1304, with no instances of unauthorized access, data breaches, data errors, or prohibited uses detected. All system access was made by authorized personnel as stipulated in the policy.

BACKGROUND

Policy 1304 requires that surveillance camera data may only be accessed by trained and authorized BPD members for legitimate law enforcement purposes. Prohibited uses include discriminatory targeting, unauthorized dissemination of video footage, or surveillance inconsistent with civil liberties protections

SCOPE AND METHODOLOGY

The scope of this audit included all access records for the Avigilon camera system between January 1, 2025 and June 30, 2025.

The audit methodology involved:

1. Retrieving Avigilon camera system access records for the specified timeframe from the Avigilon platform.

2. Analyzing the records for any instances of unauthorized access, data breaches, or prohibited uses.
3. Verifying that all system access was made by authorized personnel as stipulated in Policy 1304.

SUMMARY OF FINDINGS

Objective #	Audit Objectives	% Meeting Standards
1	Authorized access to camera system	100%
2	No data breaches	100%
3	No prohibited uses	100%

DETAILED FINDINGS

Objective 1: Authorized access

Criteria:

1304.4 DATA ACCESS: "Access to video surveillance cameras data shall be limited to BPD personnel utilizing the camera database for uses described above and pursuant to Use Policy 351"

Inspection Procedure:

- Review all access records for the Avigilon camera system during the audit period.
- Verify that all access was made by authorized personnel.

Findings:

- All access by BPD staff to the Avigilon camera system was made by authorized personnel.
- System maintenance access by other City of Berkeley staff was also noted.

Recommendations:

- None. The 100% compliance rate meets department standards.

Objective 2: No prohibited uses

Criteria:

1304.11 AUDITING AND OVERSIGHT: " BPD will enforce against prohibited uses of this policy pursuant to Policy 1010, Personnel Complaints or other applicable law or policy. The City Manager shall enforce against any prohibited use of the cameras and/or access to data by other City of Berkeley personnel."

Inspection Procedure:

- Review access records for any indication of prohibited uses of the camera system or data.

Findings:

- No prohibited uses of the camera system or associated data were detected during the audit period.
- Marina: 14 accesses, including 12 for property crimes investigations and 2 for robbery investigations.
- San Pablo Park: 9 accesses, including 4 for robbery investigations, 3 for property crime investigations, and 1 for a traffic investigation, and 1 for a disturbance investigation.
- 6th Street & University: 5 accesses, including 3 for robbery investigations and 2 for assault with a deadly weapon investigations.

Recommendations:

- None. The 100% compliance rate meets department standards.

Surveillance Technology Report: PEO Automated License Plate Readers**October 1, 2024 – Sept. 30, 2025**

Description	A description of all non-privileged and non-confidential information about use of the Surveillance Technology, including but not limited to the quantity of data gathered and sharing of data, if any, with outside entities. If sharing has occurred, the report shall include general, non-privileged and non-confidential information about recipient entities, including the names of the entities and purposes for such sharing. Automated License Plate Readers (ALPRs) are used by Parking Enforcement Officers (PEOs) for time zone parking. The City's Transportation Division uses anonymized information for purposes of supporting the City's Go Berkeley parking management program. PEO ALPR use replaced the practice of physically "chalking" tires, which a more effective means of identifying violators. What data is captured by this technology: ALPR technology functions by automatically capturing an image of a vehicle's license plate, transforming that image into alphanumeric characters using optical character recognition software, and storing that information, along with relevant metadata (e.g. geo-location and temporal information, as well as data about the PEO ALPR). How the data is stored: The data is stored on a secure server by the vendor. Retention period of data: During this reporting period collected images and metadata of hits were stored no more than 365 days. Reads and metadata of reads were not stored more than 14 days in accordance with policy 1302. Current use policy adopted September 13, 2022 sets new retention periods that are now in effect. Summary of PEO ALPR Time Zone Enforcement Data Genetec is the vendor for the PEO ALPR Time Zone enforcement system. A "read" indicates the PEO ALPR system successfully read a license plate. The information that is generated when a plate is viewed by the PEO ALPR camera is the license plate number, state and geographical (GPS) location it was viewed. A "hit" indicates the PEO ALPR system detected a possible violation, which prompts the Parking Enforcement Officer to further assess the vehicle. At hit is
-------------	--

when the read information is recognized as a license plate that matches, or does not match an entry in a list such as permit list or the stolen vehicle “hot list”. In many cases, hits are “rejected” or “not enforced”, meaning no enforcement action is taken, because the Parking Enforcement Officer determines the vehicle has an appropriate placard or permit, or there is other information or assignment which precludes citation.

The following are key statistics for this reporting period:

- 2,901,622 reads
- 117,937 hits
- 41,734 enforced hits resulted in citation issuance.
- 1,519 not-enforced hits due to either, 1) PEO ALPR experiencing technical issues and PEO unable to validate the hit in the system, which only gives option to not enforce, or 2) PEO error in accepting the hit initially.
- 74,684 hits were not acted upon for a variety of reasons including but not limited to:
 - Customer comes out to move a vehicle. PEO’s are directed not to issue that citation.
 - PEO gets to the dashboard and sees a permit not visible from a previous location.
 - PEO does a vehicle evaluation and confirms that the vehicle moved from the hit location (e.g. across the street within GPS range).
 - Stolen car.
 - Similar plates.
 - GIG cars or Revel scooters.
 - PEOs mistakenly leave their PEO ALPR on collecting data, but leave the area being enforced to drive to another location on another assignment, such as a traffic post at a collision scene.

	All BPD PEO ALPR data may only be shared with other law enforcement or prosecutorial agencies for official law enforcement purposes, or as otherwise permitted by department policy and law. All PEO ALPR data is subject to the provisions of BPD Policy 415 - Immigration Law, and therefore may not be shared with federal immigration enforcement officials. During this reporting period there were no law enforcement investigative vehicle inquiries.
Geographic Deployment	Where applicable, non-privileged and non-confidential information about where the surveillance technology was deployed geographically. Only Parking Enforcement Vehicles are equipped with PEO ALPRs. PEO ALPRs are deployed based on areas where there are parking time restrictions. PEO ALPRs are not deployed based on geographic considerations not related to parking enforcement.
Complaints	A summary of each complaint, if any, received by the City about the Surveillance Technology. There have been no complaints about the deployment and use of Automated License Plate Readers.
Audits and Violations	The results of any non-privileged internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response. The required audits were completed and are attached below.
Data Breaches	Non-privileged and non-confidential information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response. There have been no known data breaches or other unauthorized access to Automated License Plate Reader data.
Effectiveness	Information that helps the community assess whether the Surveillance Technology has been effective in achieving its identified outcomes. PEO ALPRs have proven effective in parking enforcement for time zone enforcement. The PEO ALPRs' ability to read and check license plates while being driven greatly increases efficiency, allowing an operator to cover larger areas more quickly without having to stop except to confirm a hit.

	An additional benefit of the Parking Enforcement PEO ALPR system is that sometimes hits indicate a possible stolen vehicle. These hits allow for the timelier recovery of stolen vehicles in the City of Berkeley.
Costs	Total annual costs for the Surveillance Technology, including personnel and other ongoing costs. The annual system maintenance cost for Genetec is \$51,720. This cost is borne by the Transportation Division, which covers warranties, support, and cellular connection costs. Genetec PEO ALPR units are installed on 22 Parking Enforcement vehicles. Parking Enforcement personnel perform a variety of parking enforcement activities and are not limited solely to time zone enforcement. Therefore, personnel costs specifically attributable to time zone enforcement are not tracked.



Berkeley Police Department Memorandum



To: Chief Louis

From: Arlo Malmberg, Strategic Planning and Accountability Manager

RE: Genetec Automated License Plate Reader Audit – July 2024 to December 2024

OVERVIEW

The Berkeley Police Department's Strategic Planning and Accountability Manager conducted an audit of the Genetec ALPR system to assess compliance with Policy 1302, Surveillance Use Policy – Automated License Plate Reader (ALPR). The audit scope included access records for the Genetec ALPR system between July 1, 2024 and December 31, 2024. The audit methodology involved analyzing these access records for unauthorized access, data breaches, and prohibited uses.

The audit found full compliance with Policy 1302, with no instances of unauthorized access, data breaches, data errors, or prohibited uses detected. All system access was made by authorized personnel as stipulated in the policy.

BACKGROUND

Policy 1302 outlines the requirements for use and access to the Genetec ALPR systems by Parking Enforcement Officers. The policy mandates biannual audits of the ALPR system to ensure compliance and detect any unauthorized access or data breaches.

SCOPE AND METHODOLOGY

The scope of this audit included all access records for the Genetec ALPR system between July 1, 2024 and December 31, 2024.

The audit methodology involved:

1. Retrieving Genetec ALPR system access records for the specified timeframe from the Parking Enforcement Manager.
2. Analyzing the records for any instances of unauthorized access, data breaches, or prohibited uses.

3. Verifying that all system access was made by authorized personnel as stipulated in Policy 1302.

SUMMARY OF FINDINGS

Objective #	Audit Objectives	% Meeting Standards
1	Authorized access to ALPR system	100%
2	No data breaches	100%
3	No prohibited uses	100%

DETAILED FINDINGS**Objective 1: Authorized access to ALPR system****Criteria:**

1302.5 DATA ACCESS (a): "Only properly trained Parking Enforcement Officers, Sworn Officers as selected by the Investigation's Division Captain, and Information Technology personnel are allowed access to the Genetec ALPR system or to collect ALPR information."

Inspection Procedure:

- Review all access records for the Genetec ALPR system during the audit period.
- Verify that all access was made by authorized personnel.

Findings:

- All access to the Genetec ALPR system was made by authorized personnel
- System maintenance access by Genetec personnel and City of Berkeley IT was also noted and deemed appropriate.

Recommendations:

- None. The 100% compliance rate meets department standards.

Objective 2: No data breaches

Criteria:

1302.11 AUDITING AND OVERSIGHT (1): “Any unauthorized access or data breach shall be reported immediately to the City Manager...”

Inspection Procedure:

- Analyze access records for any signs of data breaches.
- Confirm with the Parking Enforcement Manager that no data breaches were reported during the audit period.

Findings:

- No data breaches were detected or reported during the audit period.

Recommendations:

- None. The 100% compliance rate meets department standards.

Objective 3: No prohibited uses

Criteria:

1302.11 AUDITING AND OVERSIGHT (1): “...BPD will enforce against prohibited uses of the Genetec ALPR system, associated ALPR Read and Hit metadata, and lists and databases pursuant to Policy P-26, or other applicable law or policy.”

Inspection Procedure:

- Review access records for any indication of prohibited uses of the ALPR system.

Findings:

- No prohibited uses of the ALPR system or associated data were detected during the audit period.
- Most system accesses were by Genetec personnel for IT support and user management. The remaining accesses were primarily by the Parking Enforcement Manager and Supervisors for reviewing system configurations.

Recommendations:

- None. The 100% compliance rate meets department standards.



Berkeley Police Department Memorandum



To: Chief Louis

From: Arlo Malmberg, Strategic Planning and Accountability Manager

RE: Genetec Automated License Plate Reader Audit – January 2025 to June 2025

OVERVIEW

The Berkeley Police Department's Strategic Planning and Accountability Manager conducted an audit of the Genetec ALPR system to assess compliance with Policy 1302, Surveillance Use Policy – Automated License Plate Reader (ALPR). The audit scope included access records for the Genetec ALPR system between January 1, 2025 and June 30, 2025. The audit methodology involved analyzing these access records for unauthorized access, data breaches, and prohibited uses.

The audit found full compliance with Policy 1302, with no instances of unauthorized access, data breaches, data errors, or prohibited uses detected. All system access was made by authorized personnel as stipulated in the policy.

BACKGROUND

Policy 1302 outlines the requirements for use and access to the Genetec ALPR systems by Parking Enforcement Officers. The policy mandates biannual audits of the ALPR system to ensure compliance and detect any unauthorized access or data breaches.

SCOPE AND METHODOLOGY

The scope of this audit included all access records for the Genetec ALPR system between January 1, 2025 and June 30, 2025.

The audit methodology involved:

1. Retrieving Genetec ALPR system access records for the specified timeframe from the Parking Enforcement Manager.
2. Analyzing the records for any instances of unauthorized access, data breaches, or prohibited uses.

3. Verifying that all system access was made by authorized personnel as stipulated in Policy 1302.

SUMMARY OF FINDINGS

Objective #	Audit Objectives	% Meeting Standards
1	Authorized access to ALPR system	100%
2	No data breaches	100%
3	No prohibited uses	100%

DETAILED FINDINGS**Objective 1: Authorized access to ALPR system****Criteria:**

1302.5 DATA ACCESS (a): "Only properly trained Parking Enforcement Officers, Sworn Officers as selected by the Investigation's Division Captain, and Information Technology personnel are allowed access to the Genetec ALPR system or to collect ALPR information."

Inspection Procedure:

- Review all access records for the Genetec ALPR system during the audit period.
- Verify that all access was made by authorized personnel.

Findings:

- All access to the Genetec ALPR system was made by authorized personnel
- System maintenance access by Genetec personnel and City of Berkeley IT was also noted and deemed appropriate.

Recommendations:

- None. The 100% compliance rate meets department standards.

Objective 2: No data breaches

Criteria:

1302.11 AUDITING AND OVERSIGHT (1): “Any unauthorized access or data breach shall be reported immediately to the City Manager...”

Inspection Procedure:

- Analyze access records for any signs of data breaches.
- Confirm with the Parking Enforcement Manager that no data breaches were reported during the audit period.

Findings:

- No data breaches were detected or reported during the audit period.

Recommendations:

- None. The 100% compliance rate meets department standards.

Objective 3: No prohibited uses

Criteria:

1302.11 AUDITING AND OVERSIGHT (1): “...BPD will enforce against prohibited uses of the Genetec ALPR system, associated ALPR Read and Hit metadata, and lists and databases pursuant to Policy P-26, or other applicable law or policy.”

Inspection Procedure:

- Review access records for any indication of prohibited uses of the ALPR system.

Findings:

- No prohibited uses of the ALPR system or associated data were detected during the audit period.
- Most system accesses were by Genetec personnel for IT support and user management. The remaining accesses were primarily by the Parking Enforcement Manager and Supervisors for reviewing system configurations.

Recommendations:

- None. The 100% compliance rate meets department standards.

Surveillance Technology Report: Street Level Imagery Project**October 1, 2024 – Sept. 30, 2025**

Description	A description of all non-privileged and non-confidential information about the use of the Surveillance Technology, including but not limited to the quantity of data gathered and sharing of data, if any, with outside entities. If sharing has occurred, the report will include general, non-privileged and non-confidential information about recipient entities, including the names of the entities and purposes for such sharing. Street level imagery is utilized exclusively by authorized City staff for infrastructure asset management and planning activities. The street level imagery of City infrastructure assets in the Public Right of Way that is provided to the City will not consist of information that is capable of being associated with any individual or group.
Geographic Deployment	Where applicable, non-privileged and non-confidential information about where the surveillance technology was deployed geographically. Street level imagery was collected by driving through the entire community over a three week period in December of 2020. It is accessible to the City through a proprietary third-party application, Street Smart TM.
Complaints	A summary of each complaint, if any, received by the City about the Surveillance Technology. There have been no complaints about the use of Street Smart TM.
Audits and Violations	The results of any non-privileged internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response. There have been no complaints with regards to the Street Level Imagery Project.
Data Breaches	Non-privileged and non-confidential information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response. There have been no known data breaches or other unauthorized access to Cyclomedia Street Level Imagery data.
Effectiveness	Information that helps the community assess whether the Surveillance Technology has been effective in achieving its identified outcomes. Staff considered hiring contractors to use GPS in the field to create and update the infrastructure asset GIS data. This method is costly and time consuming. Cyclomedia's unique and patented processing techniques allow positionally-

	accurate GIS data to be collected in a cost-effective way and over a shorter period of time than a “boots on the ground” GPS field survey. The Imagery extracted the following Citywide Infrastructure assets to create accurate and current Geographic Information Systems (GIS) data inventories: • Bus pads / stops • Maintenance Access Holes • Pavement Striping • Curb paint color • Parking meters • Pedestrian Signal • Pavement marking • Storm drains • Signs • Street trees • Traffic lights The street level imagery captured was used to: Create a street sign GIS layer with condition assessment to support compliance with the Manual on Uniform Traffic Control Devices Code and provide an accurate inventory of City signs. The prior sign inventory is contained in a spreadsheet that does not have accurate location data. Created a curb color layer with condition assessment to indicate where there are red, yellow, blue, white and green colors. This is critical to support Public Safety. Created pavement striping and paint symbol layers to support Transportation Planning and Vision Zero. Benefits: The data from the street level imagery was integrated into the City’s work order and asset management system for planning activities and to document repair and maintenance. Planners can use the street level imagery provided to the City to take measurements remotely, such as sidewalk width and public right of way impacts at proposed development locations. The data provides a comprehensive snapshot of the City that would be helpful for cost recovery in the event of a major disaster.
--	--

	City staff can use the street level imagery to plan the location of road markings for pedestrian crossings, bike lanes or other striping. City staff can remotely take accurate measurements of infrastructure assets to adequately plan for repair and replacement. City staff can use street level imagery to enhance community engagement. The street level imagery can be used to identify and depict the impact of development such as an intersection restriping plan in order to article before and after conditions.																														
Costs	Total annual costs for the Surveillance Technology, including personnel and other ongoing costs. The total cost of the system is \$232,611 and is itemized below. <table border="1"> <thead> <tr> <th>Year No.</th><th>Description</th><th>Cost</th><th>Notes</th></tr> </thead> <tbody> <tr> <td>1</td><td>Licenses</td><td>\$48,000</td><td>Resolution No: 69,482-N.S. 30JUN20</td></tr> <tr> <td>1</td><td>Professional Services for asset extraction</td><td>\$139,401</td><td>Resolution No: 69,482-N.S. 30JUN20</td></tr> <tr> <td>2</td><td>Licenses and Support – One-Time</td><td>\$41,100</td><td>Resolution No: 70,487-N.S. 26JUL22</td></tr> <tr> <td>3</td><td>License and Support – Ongoing Annual Costs</td><td>\$4,110</td><td>Resolution No: 70,487-N.S. 26JUL22</td></tr> <tr> <td>4</td><td>License and Support – Ongoing Annual Costs</td><td>\$4,110</td><td>Resolution No: 70,487-N.S. 26JUL22</td></tr> <tr> <td>5</td><td>License and Support – Ongoing Annual Costs</td><td>\$4,110</td><td>Resolution No: 70,487-N.S. 26JUL22</td></tr> </tbody> </table>			Year No.	Description	Cost	Notes	1	Licenses	\$48,000	Resolution No: 69,482-N.S. 30JUN20	1	Professional Services for asset extraction	\$139,401	Resolution No: 69,482-N.S. 30JUN20	2	Licenses and Support – One-Time	\$41,100	Resolution No: 70,487-N.S. 26JUL22	3	License and Support – Ongoing Annual Costs	\$4,110	Resolution No: 70,487-N.S. 26JUL22	4	License and Support – Ongoing Annual Costs	\$4,110	Resolution No: 70,487-N.S. 26JUL22	5	License and Support – Ongoing Annual Costs	\$4,110	Resolution No: 70,487-N.S. 26JUL22
Year No.	Description	Cost	Notes																												
1	Licenses	\$48,000	Resolution No: 69,482-N.S. 30JUN20																												
1	Professional Services for asset extraction	\$139,401	Resolution No: 69,482-N.S. 30JUN20																												
2	Licenses and Support – One-Time	\$41,100	Resolution No: 70,487-N.S. 26JUL22																												
3	License and Support – Ongoing Annual Costs	\$4,110	Resolution No: 70,487-N.S. 26JUL22																												
4	License and Support – Ongoing Annual Costs	\$4,110	Resolution No: 70,487-N.S. 26JUL22																												
5	License and Support – Ongoing Annual Costs	\$4,110	Resolution No: 70,487-N.S. 26JUL22																												

Surveillance Technology Report: Unmanned Aerial Systems**October 1, 2024 – Sept. 30, 2025**

Description	A description of all non-privileged and non-confidential information about use of the Surveillance Technology, including but not limited to the quantity of data gathered and sharing of data, if any, with outside entities. If sharing has occurred, the report shall include general, non-privileged and non-confidential information about recipient entities, including the names of the entities and purposes for such sharing. Unmanned Aerial Systems (UAS) also commonly referred to as a drone are requested pursuant to our Mutual Assistance protocols. If a situation arises wherein the safety to the community, officers, or the offender can be increased through the means of de-escalation (adding time and distance to the situation) a supervisor can make the request. During this reporting period, the Police Department sought mutual assistance for drones on 5 occasions. What data is captured by this technology: Unmanned Aerial Systems are owned and operated by the respective agency. While each piece of equipment is unique, generally UAS can both record video and audio, while transmitting the data to the operator, thereby qualifying as a piece of Surveillance Technology pursuant to BMC 2.99.020. How the data is stored: During this reporting period Concord Police Department (CPD), Oakland Police Department (OPD), and Danville Police Department (DPD) assisted the Berkeley Police Department by providing drones. Per their policy, those agencies retain images captured during a UAS mission if there is reasonable suspicion of criminal activity. BPD personnel would request that evidence from those agencies if it was needed in support of criminal activity. During this reporting period no data was stored by BPD. Retention period of data: Policy 1303.7: If available, any data collected by the use of a UAS should be purged by BPD within 60 days if it doesn't contain any data of evidentiary value. If the data has evidentiary value, it should be uploaded into BPD's evidence database and kept pursuant to the established retention guidelines set forth in policy 804-Records Maintenance and Release. Summary of Uses of UAS
-------------	--

	- Case 24-00014436 (10/17/24, Antioch): Antioch PD drone deployed during a high-risk homicide warrant service. Use aligned with policy provisions for high-risk warrant service. - Case 24-00049593 (10/23/24, Berkeley): San Francisco PD drone deployed during high-risk warrant service requested by SFPD for a burglary suspect with prior firearms history. Use aligned with policy provisions for high-risk warrant service. - Case 25-00010214 (3/5/25, Antioch): Antioch PD drone deployed during a high-risk homicide warrant service. Use aligned with policy provisions for high-risk warrant service. - Case 25-00012777 (3/20/25, Oakland): Oakland PD drone deployed during a high-risk warrant service for armed robbery suspects. Use aligned with policy provisions for high-risk warrant service. - Case 25-00027771 (9/3/25, San Francisco): San Francisco PD drone deployed during BPD SRT operation to serve a high-risk arrest and search warrant. Use aligned with policy provisions for high-risk warrant service.
Geographic Deployment	Where applicable, non-privileged and non-confidential information about where the surveillance technology was deployed geographically. A UAS was used 5 times during this reporting period; twice in Antioch, and once in Berkeley, Oakland and San Francisco.
Complaints	A summary of each complaint, if any, received by the City about the Surveillance Technology. During this reporting period the City received no complaints about the deployment of UAS.
Audits and Violations	The results of any non-privileged internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response. There were no known violations relating to the UAS Surveillance Use Policy.
Data Breaches	Non-privileged and non-confidential information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response. There have been no known data breaches or other unauthorized access to any of the data from UAS.

Effectiveness	Information that helps the community assess whether the Surveillance Technology has been effective in achieving its identified outcomes. UAS are often used to search properties before officers. This allows officers to see video from the UAS and confirm a suspect is not waiting inside with a weapon. By sending the UAS in before officers, the risk of a confrontation that could result in death or serious injury to the suspect, others inside the house and officers, is significantly reduced.
Costs	Total annual costs for the Surveillance Technology, including personnel and other ongoing costs. The annual cost for UAS is zero as the uses were covered by the responding agencies under the Mutual Assistance agreement. The only costs associated is staff time at each respective incident, however no costs for the use of the technology were incurred. It should be noted that some agencies have indicated an intent to charge for personnel costs associated with providing a drone.

Surveillance Technology Report: Fixed Automated License Plate Readers**October 1, 2024 – September 30, 2025**

Description	A description of all non-privileged and non-confidential information about use of the Surveillance Technology, including but not limited to the quantity of data gathered and sharing of data, if any, with outside entities. If sharing has occurred, the report shall include general, non-privileged and non-confidential information about recipient entities, including the names of the entities and purposes for such sharing. Fixed Automated License Plate Readers (ALPRs) capture images of license plates and convert them to alphanumeric characters. Each detection includes time, GPS location, plate state, and camera ID. The system flags plates against hotlists or BOLOs set by BPD for law-enforcement purposes. No facial recognition is used. What data is captured by this technology: • Plate image and cropped plate image • Parsed plate number and state • Date/time and GPS location • Camera identifier and system metadata How the data is stored: Flock hosts the data in its secure cloud environment. Retention period of data: Retention follows BPD’s ALPR policy for fixed systems. Plate detections (“reads”) are retained 30 days. Images and metadata associated with investigative “hits” are retained 30 days unless preserved by case hold. Summary of Fixed ALPR Data The alert figures below represent the number of times the system flagged license plates during the reporting period. The first three categories—felony vehicle, stolen vehicle, and stolen license plate alerts—were generated through the California SVS (Stolen Vehicle System). The “hotlist alerts” reflect license plates tied to ongoing BPD investigations into specific crimes.
-------------	--

	○ 73 felony vehicle alerts ○ 643 stolen vehicle alerts ○ 48,398 stolen license plate alerts ○ 253 hotlist alerts BPD shares ALPR data only with California law-enforcement agencies for official law-enforcement purposes, not for federal immigration enforcement. During this period, access was limited to California agencies that signed a letter agreeing to follow state law with respect to ALPR usage.
Geographic Deployment	Where applicable, non-privileged and non-confidential information about where the surveillance technology was deployed geographically. The 52 cameras are fixed at locations across Berkeley. Positioning focuses on city ingress/egress points and high-traffic corridors that support crime-prevention and investigative leads.
Complaints	A summary of each complaint, if any, received by the City about the Surveillance Technology. There have been no submitted complaints about the deployment and use of Automated License Plate Readers.
Audits and Violations	The results of any non-privileged internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response. The required audit was completed and is attached below.
Data Breaches	Non-privileged and non-confidential information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response. There have been no known data breaches or other unauthorized access to Fixed Automated License Plate Reader data.
Effectiveness	Information that helps the community assess whether the Surveillance Technology has been effective in achieving its identified outcomes. Fixed ALPRs generated investigative leads for stolen vehicles and other priority cases. The network provides time-stamped detections across major corridors, which shortens suspect-vehicle identification and recovery timelines during active investigations.

Costs	Total annual costs for the Surveillance Technology, including personnel and other ongoing costs. \$179,500 for year one, and \$165,000 in year two and any subsequent years.
-------	---



Berkeley Police Department Memorandum



To: Chief Louis

From: Arlo Malmberg, Strategic Planning and Accountability Manager

RE: Flock Automated License Plate Reader Audit – January 2025 to June 2025

OVERVIEW

The Berkeley Police Department's Strategic Planning and Accountability Manager conducted an audit of the Flock ALPR system to assess compliance with Policy 1305, Surveillance Use Policy – Fixed Automated License Plate Reader (ALPR). The audit scope included access records for the Flock ALPR system between January 1, 2025 and June 30, 2025. The audit methodology involved analyzing these access records for unauthorized access, data breaches, and prohibited uses.

The audit found 100% compliance by Berkeley PD personnel with ALPR policy and 100% compliance with authorized access by external agencies. The audit also found 99.81% compliance with permitted search reasons by external agencies.

BACKGROUND

Policy 1305 outlines the requirements for use and access to the Flock ALPR systems by BPD staff. The policy mandates biannual audits of the ALPR system to ensure compliance and detect any unauthorized access or data breaches.

SCOPE AND METHODOLOGY

The scope of this audit included all access records for the Flock ALPR system between January 1, 2025 and June 30, 2025.

The audit methodology involved:

1. Reviewing system access records for the specified timeframe from the Flock platform.
2. Analyzing the records for any instances of unauthorized access, data breaches, or prohibited uses as stipulated in Policy 1305.

SUMMARY OF FINDINGS

Objective #	Audit Objectives	% Meeting Standards
1	BPD – Authorized access	100%
2	BPD – Permitted uses	100%
3	External – Authorized access	100%
4	External – Permitted uses	99.81%

DETAILED FINDINGS**Objective 1: BPD – Authorized Access****Criteria:**

1305.3 AUTHORIZED AND PROHIBITED USES (j): " 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."

Inspection Procedure:

- Review all access records for the Flock ALPR system during the audit period.
- Verify user roles.

Findings:

- All access to the Flock ALPR system was made by authorized personnel.

Objective 2: BPD – Permitted Uses**Criteria:**

1305.3 AUTHORIZED AND PROHIBITED USES (k): "Permitted/Impermissible Uses. The ALPR system, and all data collected, is the property of the Berkeley Police Department. Department personnel 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 specifically prohibited:

1. Invasion of Privacy: Except when done pursuant to a court order such as a search warrant, 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. First Amendment Rights. It is a violation of this policy to use the LPR system or associated scan files or hot lists for the purpose or known effect of infringing upon First Amendment rights."

Inspection Procedure:

- Query access records for terms associated with impermissible use.
- Confirm that each search recorded a case/incident number and/or reason.

Findings:

- No impermissible uses detected across officer activity. Reasons documented in line with Policy 1305's requirement to capture case/incident number and/or reason.

Objective 3: External – Authorized Access

Criteria:

1305.10 THIRD PARTY DATA-SHARING: "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....The Berkeley Police Department does not permit the sharing of ALPR data gathered by the City or its contractors/subcontractors for purpose of federal immigration enforcement, these federal immigration agencies include Immigrations and Customs Enforcement (ICE) and Customs and Border Patrol (CBP)."

Inspection Procedure:

- Query access records for Federal and out-of-state agencies.

Findings:

- No Federal or out-of-state agencies searched across BPD's ALPR network.

Objective 4: External – Permitted Uses

Criteria:

1305.10 THIRD PARTY DATA-SHARING: "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....The Berkeley Police Department does not permit the sharing of ALPR data gathered by the City or its contractors/subcontractors for purpose of federal immigration enforcement, these federal immigration agencies include Immigrations and Customs Enforcement (ICE) and Customs and Border Patrol (CBP)."

Inspection Procedure:

- Query access records for terms associated with impermissible use.

Findings:

- 0.19% of searches made reference to a federal agency acronym.
- All of those searches were broad searches of all available California networks; none targeted Berkeley specifically.
- 1 search included the term "ICE", and 2 unique searches included the term "CBP". These searches correspond to "statewide lookup" searches that affected all California agencies that had the "statewide lookup" feature enabled at the time. We have since disabled this feature (see Departmental Actions below).
- As verified in Objective 3, no federal agencies, and no agencies outside of California accessed Berkeley's ALPR network.
- The presence of those terms does not by itself establish a violation of California law or Policy 1305. We cannot conclude a state-law violation from reason-field text alone. For example, 5 searches included the term "DHS." Upon closer examination, they were in reference to DHS PD, or Desert Hot Springs Police Department.

DEPARTMENTAL ACTIONS

Recognizing potential risks revealed both via this audit and as discovered by incidents in other jurisdictions, BPD implemented several preventative measures to further protect Berkeley data while still maintaining the technology's public safety value.

- **Access narrowing during audit.** After the finding above, by order of the Chief, BPD tightened access in response to community concerns and to align strictly with Policy 1305's sharing provisions:
 - Revoked network access for all agencies outside the nine Bay Area counties plus Sacramento County.
 - Turned off the statewide lookup tool.
 - Nationwide lookup had already been disabled before rollout.
 - Since undertaking these actions, 0 searches have referenced "ICE", "CBP", or any other federal immigration enforcement agency.
- **Ongoing controls.** BPD now by protocol will revoke sharing for any agency if a search reason appears to fall outside of that which is permitted by BPD policy, ordinance or law until that agency provides a written explanation and assurances that its use of our data is consistent with Policy 1305 and California law.
 - To promote regional compliance, we will notify requesting agencies whenever a search reason includes language that may fall outside the allowable parameters.
 - To ensure continued full compliance internally, BPD will conduct roll call training regarding use policies for ALPRs, access controls and the intersection with state law and the recently passed Sanctuary City Ordinance.

VENDOR ACTIONS

Flock acknowledged that permissive default sharing was a flaw and has taken corrective steps to support California law and Berkeley's Sanctuary City policy.

- Flock shifted to **restrictive-by-default sharing**, paused all federal pilots, created a distinct "Federal" organization label, removed federal users from Statewide and National Lookup, and began publishing ongoing compliance updates.
- Flock now enforces state-border sharing limits, **prevents federal or out-of-state access to California data**, blocks searches tied to immigration or reproductive-health enforcement through keyword filters, and presents clearer prompts on share requests.

- Flock is developing **proactive audit alerts** for 2026 to make it easy to screen for unpermitted uses in real time.

