

Page numbers for this agenda packet are marked in **blue** to distinguish them from the numbering within individual documents.



**POLICE ACCOUNTABILITY BOARD
REGULAR MEETING AGENDA PACKET
SUPPLEMENTAL #1
November 5, 2025
6:30 PM**

Board Members

Joshua Cayetano (Chair)	Leah Wilson (Vice-Chair)
Kitty Calavita	Juliet Leftwich
Randy Wells	Joshua Buswell-Charkow

MEETING LOCATION

Office of the Director of Police Accountability
1900 Addison Street, Floor 3
Berkeley, CA 94704

Item	Description	Page
9.b.	Letter from Chair Cayetano to the PAB Titled "Item 9.b. – Berkeley Police Department's Annual Surveillance Technology Report"	1
9.c.	ODPA Memorandum Titled "Update on BPD Radio Encryption and Potential Next Steps"	87

Item 9.b.

Letter from Chair Cayetano to the PAB Titled “Item 9.b. – Berkeley Police Department’s Annual Surveillance Technology Report”



Josh Cayetano | Chair
Police Accountability Board
JCayetano@berkeleyca.gov

November 4, 2025

VIA ELECTRONIC MAIL

Police Accountability Board
DPA@berkeleyca.gov
1900 Addison Street, 3rd Floor
Berkeley, CA 94704

Re: Item 9b - Berkeley Police Department's Annual Surveillance Technology Report

Dear Board Members:

The Berkeley Police Department's (BPD) Annual Surveillance Technology Report¹ (or "Report") is currently on the Berkeley City Council's action calendar for its November 10, 2025, meeting (Attachment 1). This memorandum identifies two concerns with the Report for the Board's awareness and consideration.

First, the Report omits mention of complaints received by the Office of the Director of Police Accountability (ODPA) and the Police Accountability Board (PAB) involving the use of surveillance technology. Berkeley Municipal Code 2.99.020(2)(c)² (Attachment 2) plainly states that the Report shall include "[a] summary of each complaint, if any, received by *the City* about the Surveillance Technology." During the reporting period, the PAB received civilian complaints about surveillance technology, specifically body-worn cameras. The complaints identified instances in which officers failed to activate their body-worn cameras in a timely manner, did not activate them at all, deactivated them earlier than required, or muted audio without a clear justification, which may have resulted in the absence of certain video or audio evidence.³ Instead

¹ See Attachment 1: Berkeley Police Department Annual Surveillance Technology Report

² See Attachment 2: Berkeley Municipal Code § 2.99.020: [https://berkeley.municipal.codes/BMC/2.99.020\(2\)\(c\)](https://berkeley.municipal.codes/BMC/2.99.020(2)(c))

³ Complainants generally do not have access to body-worn camera (BWC) footage under current state law, except in limited disclosure circumstances prescribed by statute (e.g., critical incidents or sustained misconduct findings). As a result, it is unlikely that a complaint form would include allegations of BWC policy violations—such as delayed activation, premature deactivation, or omission of footage—without the complainant first being able to view the relevant video evidence.

of including these instances, the Report only references complaints received by the Berkeley Police Department's Internal Affairs Unit. If BPD does not submit a supplemental item or notice to Council correcting the omission, then I recommend the Board provide Council with a summary of the complaints involving Surveillance Technology that ODPa and the PAB have received and ask Council to instruct BPD to collaborate with ODPa to include that information in future reports.

Second, pages 40 to 45 of the Report describe the results of a Flock ALPR audit, which found that an external agency had searched ALPR data for the purposes of federal immigration enforcement, a practice that violates BPD policy. The audit report itself is written in vague terms. It does not explain which California agency improperly accessed ALPR data, nor does it explain when BPD identified the non-compliant use of the statewide ALPR data lookup function. The audit report also does not conclude that there was a violation of California law or Policy⁴ 1305 (Attachment 3), notwithstanding its reference to ICE and CBP, reasoning that "the presence of [terms associated with impermissible use] does not by itself establish a violation." Despite the vague description and the equivocal conclusion, BPD explains in detail the remedial actions that it took to narrow access to ALPR data and reassure the community that a future violation is unlikely. Besides disabling the statewide lookup tool feature, BPD states that it will now revoke sharing for any agency that uses a term associated with impermissible use until they have provided a written explanation and assurances that the use of Berkeley's data is consistent with California law and Policy 1305.

While I appreciate BPD's commitment to remediating the non-compliance and the steps that it has taken to ensure future compliance with California law and Policy 1305, the Board should take notice of the timing of the ALPR audit report and its presentation. My understanding is that BPD identified the noncompliant use of Flock ALPR data in July 2025, before its presentation to Council, requesting that the City contract with Flock for its external fixed surveillance cameras. In its materials (Attachment 4) that were submitted pursuant to the Surveillance Technology Ordinance, BPD did not mention that it had identified a potential policy violation of Policy 1305 or Berkeley's sanctuary city resolution.⁵ In fact, the Board submitted materials, urging Council to adopt revisions to the Fixed Surveillance Camera Use Policy, citing data security issues that were reported in *other* jurisdictions⁶ and still, BPD did not mention, either in its papers or at the hearing,

⁴ See Attachment 3: BPD Policy 1305 – Fixed ALPR

⁵ See Attachment 4: STO Submission for External Fixed Surveillance Cameras: BPD stated that "[s]afeguarding privacy from potential misuse, particularly concerning federal immigration enforcement, is critical. Protections include state law (e.g., SB 54 prohibits sharing certain information for federal immigration enforcement), alignment of BPD policy with state law, Flock's terms forbidding such sharing, and prompt notification procedures if federal access is requested.....Use will comply with California SB 54, prohibiting data sharing for federal immigration enforcement. Flock's Terms of Agreement also forbid sharing data with federal immigration agencies. The City will be notified if federal authorities request access, allowing for intervention and oversight."

⁶ PAB Response to BPD's Surveillance Acquisition Report and External Fixed Surveillance Cameras Use Policy: [https://berkeleyca.gov/sites/default/files/documents/2025-07-17 Letter to Council re Surveillance Camera Policy - Final %283%29.pdf](https://berkeleyca.gov/sites/default/files/documents/2025-07-17%20Letter%20to%20Council%20re%20Surveillance%20Camera%20Policy%20-%20Final%203%29.pdf)

the breach that it identified. BPD, in other words, was less than forthcoming about the data security issues with Flock Safety.

The Board recommended to Council, and Council agreed, to subject external fixed surveillance camera data to the same audit procedures as ALPR data based on the Board's historic understanding of the audit procedure. After reviewing the audit report and considering the delayed notification to the Board and the Council, I recommend that the Board urge Council to (1) shorten the timeframe of notification of a potential data breach; (2) require BPD to identify the agencies that accessed Berkeley's data for an improper purpose and the agencies that have had their access revoked as a result of the improper use; and (3) memorialize the remedial controls that BPD implemented in Policies 1304 and 1305. I also ask that the Board consider what other changes to BPD Policy 1304⁷ (Attachment 5) or 1305, if any, are appropriate in light of the Report.

Respectfully submitted,

Joshua Cayetano
Joshua Cayetano | Chair
Police Accountability Board
City of Berkeley, CA

Cc: Hansel A. Aguilar, Director of Police Accountability

Attachments:

1. BPD Annual Surveillance Technology Report
2. Berkeley Municipal Code Chapter (BMC) 2.99.020
3. BPD Policy 1305 – Fixed Automated License Plate Readers
4. Surveillance Technology Ordinance Submission – External Fixed Surveillance Cameras (Item 17, July 22, 2025)
5. BPD Policy 1304 – External Fixed Surveillance Video Cameras

⁷ See Attachment 5: BPD Policy 1304 - Surveillance Use Policy External Fixed Video Surveillance Cameras

Attachment 1:
BPD Annual Surveillance Technology Report



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

Page 2 of 45

Annual Surveillance Technology Report

ACTION CALENDAR
November 10, 2025

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.

Page 3 of 45

Annual Surveillance Technology Report

ACTION CALENDAR
November 10, 2025

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

Page 4 of 45

ATTACHMENT 1
Page 1

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><td>Metric</td><td>Value</td></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><td>Type</td><td>File Count</td></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.															

Page 8 of 45

ATTACHMENT 2

Page 4

	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.
-------------	--

Page 10 of 45

ATTACHMENT 3
Page 2

	- 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.

Page 11 of 45

ATTACHMENT 3
Page 3

	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.

Page 14 of 45

ATTACHMENT 4
Page 3

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.

Page 17 of 45ATTACHMENT 4
Page 6**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.

Page 23 of 45

ATTACHMENT 5
Page 3

	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.

Page 24 of 45

ATTACHMENT 5
Page 4

	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.

Page 36 of 45ATTACHMENT 7
Page 3

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.

Page 39 of 45

ATTACHMENT 8
Page 3

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.

Page 45 of 45

ATTACHMENT 8
Page 9

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

Attachment 2:
Berkeley Municipal Code Chapter 2.99.020

MUNICIPAL CODE

Chapter 2.99

ACQUISITION AND USE OF SURVEILLANCE TECHNOLOGY

Sections:

- 2.99.010

Purposes.
- 2.99.020

Definitions.
- 2.99.030

City Council Approval Requirement.
- 2.99.040

Temporary Acquisition and Use of Surveillance Equipment.
- 2.99.050

Compliance for Existing Surveillance Technology.
- 2.99.060

Determination by City Council that Benefits Outweigh Costs and Concerns.
- 2.99.070

Oversight Following City Council Approval.
- 2.99.080

Public Access to Surveillance Technology Contracts.
- 2.99.090

Enforcement.
- 2.99.100

Whistleblower Protections.
- 2.99.110

Severability.

- A. Through the enactment of this Chapter, the City seeks to establish a thoughtful process regarding the procurement and use of Surveillance Technology that carefully balances the City’s interest in protecting public safety with its interest in protecting the privacy and civil rights of its community members.
- B. Transparency is essential when the City is considering procurement and use of Surveillance Technology.
- C. Although such technology may be beneficial to public order and safety, it has the potential to put both privacy and civil liberties at risk.
- D. Decisions relating to Surveillance Technology should occur with strong consideration of the impact such technologies may have on civil rights and civil liberties, as with all rights guaranteed by the California and United States Constitutions.
- E. Surveillance Technology may involve immediate, as well as ongoing, financial costs. Before the City acquires any Surveillance Technology, it must evaluate all costs associated with the procurement, installation, use and maintenance of the technology.
- F. Decisions regarding whether and how Surveillance Technologies should be funded, acquired, or used should be
- 2.99.010

Purposes.


- oversight, and accountability measures, are important in the protection of civil rights and civil liberties.
- H. Data reporting measures will enable the City Council and public to confirm that mandated civil rights and civil liberties safeguards have been strictly observed. (Ord. 7592-NS § 2 (part), 2018)

The following definitions apply to this Chapter:

1. "Surveillance Technology" means an electronic device, system utilizing an electronic device, or similar technological tool used, designed, or primarily intended to collect audio, electronic, visual, location, thermal, olfactory, biometric, or similar information specifically associated with, or capable of being associated with, any individual or group. Examples of covered Surveillance Technology include, but are not limited to: cell site simulators (Stingrays); automatic license plate

readers; body worn cameras; gunshot detectors (ShotSpotter); facial recognition software; thermal imaging systems, except as allowed under Section 1(d); social media analytics software; gait analysis software; and video cameras that record audio or video and can remotely transmit or can be remotely accessed.

"Surveillance Technology" does not include the following devices or hardware, unless they have been equipped with, or are modified to become or include, a Surveillance Technology as defined in Section 1 (above):

- a. Routine office hardware, such as televisions, computers and printers, that is in widespread public use and will not be used for any surveillance functions;
- b. Handheld Parking Citation Devices, that do not automatically read license plates;
- c. Manually-operated, portable digital cameras, audio recorders, and video recorders that are not to be used remotely and whose functionality is limited to manually capturing, viewing, editing and downloading video and/or audio recordings, but not including body worn cameras;
- d. Devices that cannot record or transmit audio or video or be remotely accessed, such as image stabilizing binoculars or night vision goggles or thermal imaging cameras used for fire operations, search and rescue

2.99.020



Definitions.

surveillance data, such as two-way radios, email systems and city-issued cell phones;

- f. Municipal agency databases;
- g. Medical equipment used to diagnose, treat, or prevent disease or injury, including electrocardiogram machines;
- h. Cybersecurity capabilities, technologies and systems used by the City of Berkeley Department of Information Technology to predict, monitor for, prevent, and protect technology infrastructure and systems owned and operated by the City of Berkeley from potential cybersecurity events and cyber-forensic based investigations and prosecutions of illegal computer based activity;
- i. Stationary security cameras affixed to City property or facilities.
- j. Personal communication device, which means a cellular telephone, a personal digital assistant, a wireless capable tablet or similar wireless two-way communications and/or portable Internet accessing device, that has not been modified beyond stock manufacturer capabilities, whether procured or subsidized by a City entity or personally owned, that is used in the regular course of conducting City business.

2. "Surveillance Technology Report" means an annual written report by the City Manager covering all of the City of Berkeley's Surveillance Technologies that includes all of the following information with regard to each type of Surveillance Technology:

- a. 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;
- b. Geographic Deployment: Where applicable, non-privileged and non-confidential information about where the surveillance technology was deployed geographically;
- c. Complaints: A summary of each complaint, if any, received by the City about the Surveillance Technology;
- d. 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;
- e. 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;
- f. Effectiveness: Information that helps the community assess whether the Surveillance Technology has been effective in achieving its identified outcomes;
- g. Costs: Total annual costs for the Surveillance Technology, including personnel and other ongoing costs.

3. "Surveillance Acquisition Report" means a publicly-released written report produced prior to acquisition or to proposed permanent use after use in Exigent Circumstances pursuant to Section [2.99.040](#) (2), of a type of Surveillance Technology that includes the following:

- a. Description: Information describing the Surveillance Technology and how it works, including product descriptions from manufacturers;
- b. Purpose: Information on the proposed purpose(s) for the Surveillance Technology;

Attachment 3:
BPD Policy 1305 – Fixed Automated License
Plate Readers

Surveillance Use Policy-Fixed Automated License Plate Readers (ALPRs)

1305.1 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 Personnel shall adhere to the requirements of the Surveillance Use-Fixed ALPRs in this policy as well as the corresponding Use Policy -422.

The policy of the Berkeley 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 information, it is not open to public review.

The Berkeley Police Department does not permit the sharing of ALPR data gathered by the City or its contractors/subcontractors 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).

1305.2 DEFINITIONS

- (a) Automated License Plate Reader (ALPR): A device that uses cameras and computer technology to compare digital images to lists of known information of interest.
- (b) ALPR Operator: Trained Department members who may utilize 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 Investigations Bureau Captain or the Chief's designee, serves as the ALPR Administrator for the Department.
- (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 BOLO's, etc.
- (e) Vehicles of Interest: Including, but not limited to vehicles which are reported as stolen, display stolen license plates or tags; vehicles linked to missing and/or wanted persons and vehicles flagged by the Department of Motor Vehicle Administration or law enforcement agencies.
- (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 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 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

Berkeley Police Department

Law Enforcement Manual

Surveillance Use Policy-Fixed Automated License Plate Readers (ALPRs)

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.

1305.3 AUTHORIZED AND PROHIBITED USES

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).

- (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 should 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 should confirm that the observed license plate from the system matches the license plate of the observed vehicle. Before any law enforcement action is taken because of an ALPR alert, the alert will be verified through a CLETS inquiry via MDT 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) Hot Lists. Designation of hot lists to be utilized by the ALPR system shall be made by the ALPR Administrator or his/her 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. Hot lists utilized by the Department's LPR system may be updated by agency sources more frequently than the Department may be uploading them and thus the Department's LPR system will not have access to real time data. Occasionally, there may be errors in the LPR system's read of a license plate. Therefore, an alert alone shall not be a basis for police action (other than following the vehicle of interest).
- (h) 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 Berkeley Police Department Communications Dispatcher or other department computer device, that the license plate is still stolen, wanted, or otherwise of interest before proceeding (absent exigent circumstances).

Berkeley Police Department

Law Enforcement Manual

Surveillance Use Policy-Fixed Automated License Plate Readers (ALPRs)

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 LPR, 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 of the ALPR Hit and the arrest, then the Department member shall update with the Communications Dispatcher and original person 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 (or his/her 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 officers attention to specific vehicles that have been associated with criminal activity.
- (i) All Hot Plates and suspect information entered into the ALPR system will contain the following information as a minimum:
 1. Entering Department member's name
 2. Related case number
 3. Short synopsis describing the nature of the originating call
 - (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.
 - (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

Berkeley Police Department

Law Enforcement Manual

Surveillance Use Policy-Fixed Automated License Plate Readers (ALPRs)

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.
- (l) Anyone who intentionally, or negligently, engages in an impermissible use of the ALPR system or associated scan files or hot lists shall be subject to administrative sanctions, up to and including termination, pursuant to and consistent with the relevant collective bargaining agreements and departmental policies.
- (m) 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 that is based solely on an ALPR alert.

1305.4 DATA COLLECTION

The Investigations Division Captain is responsible for ensuring systems and processes are in place for the proper collection and retention of ALPR data. Data will be transferred from vehicles to the designated storage in accordance with department procedures. Evidentiary hit data shall be transferred into the Department's digital evidence repository through secure integration.

All ALPR data downloaded to the ALPR server should be stored for no longer than 30 days, 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. In those circumstances the applicable data should be downloaded from the server and uploaded into BPD's digital evidence repository.

ALPR vendor, will store the data (data hosting) and ensure proper maintenance and security of data stored in their data towers. The ALPR vendor will purge their data at the end of the 30 days of storage. However, this will not preclude Berkeley Police Department from maintaining any relevant vehicle data obtained from the system after that period pursuant to the established City of Berkeley 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

Berkeley Police Department

Law Enforcement Manual

Surveillance Use Policy-Fixed Automated License Plate Readers (ALPRs)

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 so long as it doesn't violate the Retention guidelines.

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

1305.5 DATA ACCESS

- (a) No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.
- (b) No ALPR operator may access California Law Enforcement Telecommunications System (CLETS) data unless otherwise authorized to do so.
- (c) If practical, an operator should verify an ALPR response through the California Law Enforcement Telecommunications System (CLETS) before taking enforcement action that is based solely on an ALPR alert.

1305.6 DATA PROTECTION

All saved data will be safeguarded and protected by both procedural and technological means. The Berkeley 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 Records Maintenance and Release 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 capable of documenting all access of information by name, date and time (Civil Code § 1798.90.52).
- (c) Berkeley 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 relate 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, state or federal agency or entity without the consent of the Chief of Police or City Manager (i.e. If transportation department requested volume of vehicular traffic associated with specific events, it could conceivably be provided with the count of vehicles, but not the specific license plates with appropriate permissions).
- (e) Measures will be taken to ensure the accuracy of ALPR information. Errors discovered in ALPR data collected by ALPR units shall be marked, corrected or deleted in accordance with the type and severity of the error in question.

Berkeley Police Department

Law Enforcement Manual

Surveillance Use Policy-Fixed Automated License Plate Readers (ALPRs)

- (f) ALPR system audits will be conducted by the Office of Strategic Planning and Accountability on a regular basis, at least biennial.
- (g) Such ALPR data may be released to other authorized and verified law enforcement officials and agencies for legitimate California law enforcement purposes.
- (h) Every ALPR Detection Browsing Inquiry must be documented by either the associated Berkeley Police case number or incident number, and/or a reason for the inquiry

For security or data breaches, see the Records Release and Maintenance Policy.

1305.7 CIVIL LIBERTIES AND RIGHTS PROTECTION

The Berkeley Police Department is dedicated to the most efficient utilization of its resources and services in its public safety endeavors. The Berkeley Police Department recognizes the need to protect its ownership and control over shared information and to protect the privacy and civil liberties of the public, in accordance with federal and state law. The procedures described within this policy (Data Access, Data Protection, Data Retention, Public Access and Third-Party Data Sharing) protect against the unauthorized use of ALPR data. These policies ensure the data is not used in a way that would violate or infringe upon anyone's civil rights and/or liberties, including but not limited to potentially disparate or adverse impacts on any communities or groups.

1305.8 DATA RETENTION

All ALPR data belongs to the Department. All ALPR data downloaded to the ALPR server should be stored for no longer than 30 days, 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. In those circumstances the applicable data should be downloaded from the server and uploaded into BPD's digital evidence repository.

ALPR vendor, will store the data (data hosting) and ensure proper maintenance and security of data stored in their data towers. The ALPR vendor will purge their data at the end of the 30 days of storage. However, this will not preclude Berkeley Police Department from maintaining any relevant vehicle data obtained from the system after that period pursuant to the established City of Berkeley 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 so long as it doesn't violate the Retention guidelines.

1305.9 PUBLIC ACCESS

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

Berkeley Police Department

Law Enforcement Manual

Surveillance Use Policy-Fixed Automated License Plate Readers (ALPRs)

The Department shall to the extent feasible aim to offer a transparency portal wherein the number of scans, hits, and queries is available to the public in real-time, or as near as real-time as feasible. All data shall be reported in the Annual Surveillance Technology Report.

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.

- (a) A supervisor at the requesting agency will sign an acknowledgment letter stating that the shared data will only be used for the purposes that are aligned with the Berkeley Police Department's policy. 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).
- (b) The signed letter is retained on file. Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed as provided in the Records Maintenance and Release Policy (Civil Code § 1798.90.55).
- (c) All signed letters shall be routed to the Office of Strategic Planning and Accountability for compliance and reporting.

ALPR data is subject to the provisions of the Berkeley Police Department's Immigration Law Policy, and hence may not be shared with federal immigration enforcement officials.

1305.11 TRAINING

Training for the operation of ALPR Technology shall be provided by BPD personnel. All BPD employees who utilize ALPR Technology shall be provided a copy of this Surveillance Use Policy.

1305.12 AUDITING AND OVERSIGHT

ALPR system audits will be conducted by the Office of Strategic Planning and Accountability on a regular basis, at least biannually. The data from the fixed ALPRs shall be reported annually in the Surveillance Technology Report.

Any ALPR data or images that are utilized for an investigation that becomes evidence in a case will be made available to the Office of the Director of Police Accountability (ODPA) as it relates to a specific complaint of misconduct. Additionally, the results of any audits will be shared with the ODPA upon their completion.

1305.13 MAINTENANCE

Any installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the Investigations Division Captain or his or her designee. The Investigations Division Captain will assign members under his/her command to administer the day-to-day operation of the ALPR equipment and data. Equipment maintenance shall be provided by the vendor.

Berkeley Police Department
Law Enforcement Manual

Surveillance Use Policy-Fixed Automated License Plate Readers (ALPRs)

1305.14 ATTACHMENTS

See attachment: [ALPR Acknowledgment Letter.pdf](#)

Attachment 4:
Surveillance Technology Ordinance Submission –
External Fixed Surveillance Cameras (Item 17,
July 22, 2025)



ACTION CALENDAR
July 22, 2025

To: Honorable Mayor and Members of the City Council
 From: Paul Buddenhagen, City Manager
 Submitted by: Jennifer Louis, Chief of Police
 Subject: Surveillance Technology Ordinance Submission for External Fixed Surveillance Cameras (Flock Safety Condor Video Cameras)

RECOMMENDATION

Adopt a Resolution:

1. Accepting the attached Surveillance Acquisition Report for the Flock Safety Condor video cameras, pursuant to Berkeley Municipal Code (B.M.C.) Chapter 2.99.
2. Re-affirming the associated Berkeley Police Department (BPD) Use Policies (BPD Policy 351: External Fixed Video Surveillance Cameras and BPD Policy 1304: Surveillance Use Policy—External Fixed Video Surveillance Cameras), which were previously approved by Council on June 13, 2023.

CURRENT SITUATION AND ITS EFFECTS

This report is submitted in accordance with the Surveillance Technology Ordinance (STO) process, as codified in B.M.C. Chapter 2.99. The City is transitioning its External Fixed Video Surveillance Camera program to a new vendor, Flock Safety, and deploying Flock Safety Condor video cameras. This transition and the introduction of a new model of technology requires the submission of a Surveillance Acquisition Report for review and acceptance by the City Council.

This action will allow the Police Department to proceed with the camera installation plan as previously directed by Council, utilizing modern, solar-powered technology that resolves prior installation challenges and integrates with the City's existing Automated License Plate Reader (ALPR) network.

BACKGROUND

On October 12, 2021, and again on January 30, 2024, the City Council authorized the installation of an external fixed video surveillance camera program to enhance public safety. Subsequent analysis identified Flock Safety's solar-powered Condor cameras as

the most effective technology to meet the City's needs and overcome significant power supply and right-of-way challenges associated with the previous vendor. On March 18, 2025, Council approved updated locations for the cameras and directed BPD to initiate the STO review process.

The adoption of a new vendor and specific technology initiated the requirement under the STO to submit a new Surveillance Acquisition Report for approval by Council. The BPD policies governing the use of this technology—Policy 351 and Policy 1304—are not being changed. These Use Policies underwent the full STO review process, including pursuant to the ordinance, Police Accountability Board (PAB) review, and were formally approved by the City Council on June 13, 2023. They are included with this submission solely to fulfill the procedural requirements of the ordinance, which mandates that a complete package of STO documents be presented. Also pursuant to policy, this acquisition report and the previously approved policies were submitted to the PAB on June 19, 2025.

RATIONALE FOR RECOMMENDATION

Accepting the Surveillance Acquisition Report is the final procedural step required under the STO to implement the Council-approved External Fixed Video Surveillance Camera program with the selected vendor, Flock Safety. This action ensures the City remains in full compliance with its surveillance oversight laws while allowing the Police Department to deploy a critical tool to deter crime and support criminal investigations. The Flock Condor cameras offer superior technical capabilities and flexible installation options that will allow the project to be completed promptly and effectively.

Furthermore, the Flock Safety Condor cameras align with the City's high standards for data privacy and civil liberties protection. As detailed in the Surveillance Acquisition Report, the system employs robust, multi-layered security measures, including end-to-end encryption, secure cloud storage on AWS GovCloud, and strict access controls. The technology integrates seamlessly into the Police Department's existing workflows, operating on the same platform as the City's ALPR network, which maximizes its public safety value without creating new operational burdens. This combination of advanced security, adherence to strict use policies, and operational efficiency ensures that the deployment of these cameras fully meets the Council's original intent to enhance safety while upholding community values.

ENVIRONMENTAL SUSTAINABILITY AND CLIMATE IMPACTS

Transitioning to solar-powered cameras will reduce the carbon footprint of this project.

FISCAL IMPACTS OF RECOMMENDATION

As detailed in the attached Surveillance Acquisition Report, Flock Safety Condor cameras are priced as a subscription service at \$5,000 per camera per year. For the 16 proposed cameras, the total annual cost is approximately \$80,000. This recurring

Surveillance Technology Ordinance Submission for
External Fixed Surveillance Cameras (Flock Safety Condor Video Cameras)

ACTION CALENDAR
July 22, 2025

cost includes hardware, installation, ongoing maintenance, cellular service, data hosting, and software updates. Funding for this program is allocated from the FY 2024 baseline Public Works budget, with sufficient funds available to cover operating costs for four years. Further use of the technology beyond the initial four years will require additional funding allocations.

CONTACT PERSON

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

ATTACHMENTS

1. Resolution
2. Surveillance Acquisition Report: Flock Safety Condor Video Cameras
3. BPD Policy 351: External Fixed Video Surveillance Cameras (Approved 6/13/2023)
4. BPD Policy 1304: Surveillance Use Policy—External Fixed Video Surveillance Cameras (Approved 6/13/2023)

Surveillance Technology Ordinance Submission for
External Fixed Surveillance Cameras (Flock Safety Condor Video Cameras)

ACTION CALENDAR
July 22, 2025

RESOLUTION NO. ##,###-N.S.

ACCEPTING THE SURVEILLANCE ACQUISITION REPORT FOR FLOCK SAFETY
CONDOR VIDEO CAMERAS

WHEREAS, the City of Berkeley is committed to leveraging technology to enhance public safety while ensuring transparency, oversight, and the protection of civil liberties and civil rights, as codified in the Surveillance Technology Ordinance (B.M.C. Chapter 2.99); and

WHEREAS, the City Council previously authorized the implementation of an External Fixed Video Surveillance Camera program to aid in deterring crime and supporting criminal investigations; and

WHEREAS, the Police Department has, in accordance with B.M.C. 2.99.030, prepared and submitted a Surveillance Acquisition Report detailing the technology's description, purpose, location, impact, and safeguards; and

WHEREAS, the governing Use Policies for this technology, BPD Policy 351 and BPD Policy 1304, were previously reviewed and approved by the City Council on June 13, 2023, and are submitted herewith without change, pursuant to the requirements of the Surveillance Technology Ordinance.

NOW, THEREFORE, BE IT RESOLVED by the Council of the City of Berkeley that the City Council hereby accepts the Surveillance Acquisition Report for the Flock Safety Condor Video Cameras, allowing the City Manager and Police Department to proceed with the acquisition and deployment of this technology in accordance with the report and the previously approved Use Policies.

Surveillance Acquisition Report: External Fixed Surveillance Cameras - Flock Safety Condor Video Cameras

This report is submitted in accordance with Berkeley Municipal Code (BMC) Chapter 2.99 concerning the Acquisition and Use of Surveillance Technology. The City of Berkeley is transitioning its External Fixed Video Surveillance Camera program vendor from Edgeworth Integration, LLC to Flock Safety and plans to deploy Flock Safety Condor video cameras.

1. Description (BMC 2.99.020(3)(a))

- Condor cameras capture high-definition video footage. PTZ models allow for remote control to pan, tilt, and zoom.
- They operate on the FlockOS platform, which is the same platform through which Berkeley PD currently accesses Automatic License Plate Readers (ALPR).
- The cameras do not record audio, and audio recording is explicitly prohibited by Berkeley policy for these types of cameras.
- The system utilizes AI for features like "People Detection Alerts" (identifying human presence without facial recognition) and "Visual Alerts" (tracking vehicles across feeds).
- Some models feature dual lenses to maintain wide-angle context while zoomed in.
- They offer features like 25x optical zoom and high-quality nighttime imagery.
- Crucially for Berkeley's deployment challenges, Flock offers solar-powered, LTE-enabled cameras, eliminating the need for direct electrical wiring or complex network infrastructure setup on city poles.
- Data is transmitted wirelessly via cellular connection to cloud storage. Flock provides installation, ongoing maintenance, cellular service, and software updates as part of its subscription model.

2. Purpose (BMC 2.99.020(3)(b))

The proposed purpose for the Flock Safety Condor cameras is to provide real-time awareness and investigative capacity in following use cases:

- To support specific and active criminal investigations.
- To support serious traffic-related investigations.
- To support police misconduct investigations, and
- To respond to and review critical incidents or natural disasters.

3. Location (BMC 2.99.020(3)(c))

The cameras are proposed for deployment adjacent to the following intersections, chosen for high pedestrian traffic and analysis of crime trends:

- | | |
|-------------------|----------------------------|
| • Center / MLK | • College / Ashby |
| • Milvia / Alston | • 9 th / Gilman |

Page 6 of 18

- Center / Shattuck
- University / Shattuck
- Cedar / Shattuck
- Durant / Telegraph
- 4th / Virginia
- University / MLK
- Solano / Colusa
- 4th / Hearst
- Adeline / Fairview
- Shattuck / Ashby
- 62rd / King
- College / Alcatraz

Additional potential locations if funding allows include Ashby Ave / Domingo Ave, Ashby Ave / San Pablo Ave, Dwight Ave / San Pablo Ave, and University Ave / San Pablo Ave. This plan reallocates previously approved locations now covered by ALPRs or facing installation barriers.

4. Impact (BMC 2.99.020(3)(d))

- The deployment aims to enhance public safety and aid investigations.
- As with any surveillance, there is a potential impact on privacy and civil liberties, specifically the expectation of anonymity in public spaces. The cameras will capture video of public areas with high foot traffic.
- Concerns regarding potential disparate impacts on specific communities are acknowledged. Mitigation measures (Section 5) and adherence to a strict Use Policy are intended to prevent discriminatory use.
- Safeguarding privacy from potential misuse, particularly concerning federal immigration enforcement, is critical. Protections include state law (e.g., SB 54 prohibits sharing certain information for federal immigration enforcement), alignment of BPD policy with state law, Flock's terms forbidding such sharing, and prompt notification procedures if federal access is requested.
- The technology provider, Flock Safety, states its video cameras do not use facial recognition technology. Berkeley city policy explicitly prohibits the use of facial recognition technology.

5. Mitigation (BMC 2.99.020(3)(e))

- A comprehensive Surveillance Use Policy specific to this technology is in place and enforced (Policy 1304), outlining authorized uses, data handling, retention, and oversight, consistent with BMC 2.99.020(4).
- Use will comply with California SB 54, prohibiting data sharing for federal immigration enforcement. Flock's Terms of Agreement also forbid sharing data with federal immigration agencies. The City will be notified if federal authorities request access, allowing for intervention and oversight.
- Data access will be restricted to authorized personnel via secure login credentials managed by the City. Audit trails will log all access. Role-based access controls are available to manage least privilege.
- Data will be encrypted during transmission (TLS 1.2+) and storage (AES-256) to mitigate cybersecurity risks and prevent unauthorized third-party access. Data is stored on AWS GovCloud meeting strict governmental security standards.
- Data will be retained for a limited period pursuant to the Department Use Policy, and automatically deleted thereafter using secure methods compliant with NIST 800-88 to reduce risks associated with unauthorized use.

Page 7 of 18

- The technology will not be used for facial recognition or to unlawfully discriminate based on protected characteristics. The cameras will not be used for automated traffic enforcement.
- Signage will be posted in areas where cameras are deployed. This report and the subsequent Use Policy will be public documents.
- Using solar-powered cameras minimizes infrastructure impact and reliance on grid power at specific pole locations.

6. Data Types and Sources (BMC 2.99.020(3)(f))

- High-definition video recordings of public spaces. Associated metadata including date, time, and camera location. AI-derived alerts for human presence (without identification) or vehicle characteristics (if integrated with ALPR features).
- Video feeds directly from the Flock Safety Condor cameras affixed to City-owned poles or other suitable infrastructure in public rights-of-way. The system may integrate data/alerts from the City's existing Flock ALPR system.

7. Data Security (BMC 2.99.020(3)(g))

Flock Safety describes a multi-layered security architecture prioritizing encryption, data protection, and compliance. Key aspects include:

- Flock states its practices align with principles in the FTC Safeguards Rule and comply with frameworks like NIST CSF, NIST 800-53 Rev 5, and holds ISO 27001 certification.
- Flock employs dedicated security teams (Product Security, Corporate Security, Risk/Compliance) including a CISO and professionals with CISSP and CIPP certifications.
- Regular risk assessments (annual, utilizing NIST frameworks) are conducted, prioritized threats are tracked, and cyber threat intelligence is monitored. Quarterly security reviews and board transparency ensure oversight.
- Data is encrypted in transit (TLS 1.2+ or higher) and at rest (AES-256).
- Data is stored in Flock Safety's secure cloud environment (AWS, including AWS GovCloud for CJIS data accessible only by Law Enforcement), leveraging geographic redundancy and robust backup policies.
- Role-based access controls (RBAC) enforce least privilege for both customer administrators and Flock personnel. Access is centrally managed via an identity provider, reviewed quarterly.
- Multi-Factor Authentication (MFA) is required for privileged access and recommended for all users (supported methods include authenticator apps, SMS, customer SSO). SSO technologies (Azure AD, Okta, SAML) are supported.
- Regular security assessments (including OWASP checks, vulnerability scanning) are performed on in-house and third-party applications. Advanced tooling monitors platform, container, endpoint, and network security.
- Hardware/software inventories are actively managed. A formal SDLC process (Agile, GitHub for source code, Jira for tracking) governs changes, with mandatory reviews, testing, separation of environments, and infrastructure management via Terraform.
- Data is automatically deleted after the retention period pursuant to policy using secure methods (e.g., cryptographic wiping) aligned with NIST 800-88 guidelines.

Page 8 of 18

- Continuous monitoring (including SIEM) detects unauthorized access attempts, security events, and logs privileged user access.
- Comprehensive security awareness training is mandatory for all personnel upon hire, annually, and for significant changes, covering policies, incident response, and role-specific duties.
- Flock undergoes regular third-party assessments including SOC 2 Type II (annually), ISO 27001 certification, and CJIS ACE compliance assessment. A formal third-party risk management program vets vendors integrated with Flock products.
- Flock maintains a documented incident response plan that is tested quarterly and reviewed annually, defining roles, responsibilities, and procedures for handling breaches.

8. Fiscal Impact (BMC 2.99.020(3)(h))

- Flock Safety cameras are priced as a subscription service at \$5,000 per camera per year. For the 16 proposed cameras, the annual cost is \$80,000. This includes installation, maintenance, data hosting, cellular connectivity, and software updates.
- The FY 2024 baseline Public Works budget allocated \$600,000 for external cameras. \$290,000 was disbursed to the previous vendor, Edgeworth; the City aims to reassign these funds to other projects. The remaining \$310,000 is sufficient to cover over four years of operating costs for the 16 Flock cameras. Recovering the \$290,000 could fund an additional four years.
- Ongoing costs include City staff time for system administration, oversight, auditing, and reporting, similar to the previous system. Specific costs are TBD but covered within existing departmental budgets.
- The City intends to seek grant funding to potentially offset purchase/subscription costs.

9. Third Party Dependence and Access (BMC 2.99.020(3)(i))

- The City will depend on Flock Safety for the camera hardware, the FlockOS software platform, cellular data transmission, cloud storage, system maintenance, and software updates. This is inherent in the subscription model.
- Flock Safety handles and stores the data on its cloud platform.
- The City owns the data. Flock Safety states it will not share or sell customer data. Access to the data by third parties (including Flock Safety personnel) is controlled by the City through permissions managed within the FlockOS platform. Any data sharing with other entities (e.g., other law enforcement agencies) would be governed by Berkeley PD's Surveillance Use Policy and applicable laws.
- The City's contract with Flock Safety will require the company to provide prompt notification of any data request from a federal agency. Flock will not release data unless legally compelled to do so by federal law, and in such cases, will provide the City with advance notice to the greatest extent possible before complying.

10. Alternatives (BMC 2.99.020(3)(j))

- Continuing with the originally approved vendor, Edgeworth Integration, was considered but deemed infeasible due to insurmountable technical challenges related to power requirements at proposed locations and installation delays.

Page 9 of 18

- Relying solely on traditional policing techniques (e.g., increased officer patrols) is an alternative but does not provide the persistent monitoring or video evidence capabilities offered by cameras.
- Deciding against deploying fixed video surveillance cameras altogether.

11. Experience of Other Entities (BMC 2.99.020(3)(k))

- Many cities, including neighboring jurisdictions like San Francisco, Oakland, and San Jose, utilize fixed surveillance cameras as a tool for public safety and crime deterrence, often with their own specific use policies.
- Flock Safety systems (including LPR and video) are used by numerous law enforcement agencies nationally. These agencies often cite benefits in investigations and situational awareness.

External Fixed Video Surveillance Cameras

351.1 PURPOSE AND SCOPE

This policy provides guidance for the placement and monitoring of City of Berkeley external fixed video surveillance cameras by the Berkeley Police Department (BPD).

This policy only applies to fixed, overt, marked external video surveillance systems utilized by the BPD. It does not apply to mobile audio/video systems, covert audio/video systems or any other image-capturing devices used by the Department, as authorized by the City Council for use by other City Departments. BPD Personnel shall adhere to the requirements for External Fixed Video Surveillance Cameras covered in this policy as well as the corresponding Surveillance Use Policy -1304.

351.2 POLICY

The Berkeley Police Department utilizes a video surveillance system to enhance its anti-crime strategy, to effectively allocate and deploy personnel, and to enhance safety and security in public areas. As specified by this policy, cameras may be placed in strategic locations throughout the City to record, deter, and solve crimes, to help the City safeguard against potential threats to the public, and to help manage emergency response situations during natural and human-made disasters, among other uses specified in Section 351.3.1.

Video surveillance in public areas will be conducted in a legal and ethical manner while recognizing and protecting constitutional standards of privacy.

351.3 OPERATIONAL GUIDELINES

Only City Council-approved video surveillance equipment shall be utilized. BPD members authorized to review video surveillance may only record and review public areas and public activities where no reasonable expectation of privacy exists and pursuant to Section 351.3.1. The City Manager shall obtain Council approval of any proposed additional locations for the placement and use of video surveillance technology.

351.3.1 PLACEMENT REVIEW AND MONITORING

Camera placement will only occur in locations approved by the City Council and will be guided by this policy and the underlying purpose or strategy associated with the overall video surveillance plan. As appropriate, the Chief of Police should confer with other affected City departments when evaluating camera placement. Environmental factors, including lighting, location of buildings, presence of vegetation or other obstructions, should also be evaluated when determining placement.

Camera placement includes existing cameras such as those located at San Pablo Park, the Berkeley Marina, and cameras placed in Council identified and approved intersections throughout the City, and potential future camera locations as approved by City Council.

Current City Council approved locations:

Page 11 of 18
Berkeley Police Department
 Law Enforcement Services Manual

External Fixed Video Surveillance Cameras

- 6th Street at University Avenue
- San Pablo Avenue at University Avenue
- 7th Street at Dwight Way
- San Pablo Avenue at Dwight Way
- 7th Street at Ashby Avenue
- San Pablo Avenue at Ashby Avenue
- Sacramento Street at Ashby Avenue
- College Avenue at Ashby Avenue
- Claremont Avenue at Ashby Avenue
- 62nd Street at King Street

The cameras shall only record video images and not sound. Recorded images pursuant to Section 351.5 may be accessed, reviewed, and used for specific criminal or BPD administrative investigations and video surveillance may be accessed and reviewed by authorized BPD personnel for the following purposes:

- (a) To support specific and active criminal investigations.
- (b) To support serious traffic-related investigations.
- (c) To support police misconduct investigations, and
- (d) To respond to and review critical incidents or natural disasters.

Unauthorized recording, viewing, reproduction, dissemination, or retention of video footage is prohibited.

351.3.2 FIXED CAMERA MARKINGS

All public areas monitored by video surveillance equipment shall be marked in a conspicuous manner with unobstructed signs to inform the public that the area is under police surveillance.

351.3.3 INTEGRATION WITH OTHER TECHNOLOGY

The Department is prohibited from integrating or accessing system capabilities of the video surveillance system with other systems, such as gunshot detection, automated license plate recognition, facial recognition and other video-based analytical systems.

351.4 VIDEO SUPERVISION

Access to video surveillance camera data shall be limited to Berkeley Police Department (BPD) personnel utilizing the camera database for uses authorized above, with technical assistance from Public Works Department and Department of Information Technology personnel. Information may be shared in accordance with Sections 351.6 or 1304.9 below. BPD members seeking access to the camera system shall obtain the approval of the Investigations Division Captain, or their designee.

Page 12 of 18
Berkeley Police Department
Law Enforcement Services Manual

External Fixed Video Surveillance Cameras

Supervisors should monitor video surveillance access and usage to ensure BPD members are complying with this policy, other applicable department policy, and applicable laws. Supervisors should ensure such use and access is appropriately documented.

351.4.1 VIDEO LOG

No one without authorization will be allowed to login and view the recordings. Those who are authorized and login should automatically trigger the audit trail function to ensure compliance with the guidelines and policy.

351.4.2 PROHIBITED ACTIVITY

Video surveillance systems will not intentionally be used to invade the privacy of individuals or observe areas where a reasonable expectation of privacy exists.

Video surveillance systems shall not be used in an unequal or discriminatory manner and shall not target protected individual characteristics including, but not limited to race, ethnicity, national origin, religion, disability, gender or sexual orientation.

Video surveillance equipment shall not be used to harass, intimidate or discriminate against any individual or group.

Video surveillance systems and recordings are subject to the Berkeley Police Department's Immigration Law Policy, and hence may not be shared with federal immigration enforcement officials.

351.5 STORAGE AND RETENTION OF MEDIA

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. Recordings of incidents involving use of force by a police officer or involving, detentions, arrests, or recordings relevant to a formal or informal complaint against a sworn police officer shall be retained for a minimum of two years and one month. Recordings relating to court cases and complaints against BPD sworn officers that are being adjudicated will be manually deleted at the same time other evidence associated with the case is purged in line with the Department's evidence retention policy. Any recordings related to a police misconduct investigation shall be maintained until such matter is fully adjudicated, at which time it shall be deleted in line with the Department's evidence retention policy, and any applicable orders from the court.

Any recordings needed as evidence in a criminal or police misconduct proceeding shall be copied to a suitable medium and booked into evidence in accordance with current evidence procedures.

351.5.1 EVIDENTIARY INTEGRITY

All media downloaded and retained pursuant to this Policy shall be treated in the same manner as other evidence. Media shall be accessed, maintained, stored and retrieved in a manner that ensures its integrity as evidence, including strict adherence to chain of custody requirements. Electronic trails, including encryption, digital masking of innocent or uninvolved individuals to

Page 13 of 18
Berkeley Police Department
Law Enforcement Services Manual

External Fixed Video Surveillance Cameras

preserve anonymity, authenticity certificates and date and time stamping, shall be used as appropriate to preserve individual rights and to ensure the authenticity and maintenance of a secure evidentiary chain of custody.

351.6 RELEASE OF VIDEO IMAGES

Data collected and used in a police report shall be made available to the public in accordance with department policy and applicable state or federal law, also referenced in Policy 1304.8.

Requests for recorded video images from the public or the media shall be processed in the same manner as requests for department public records pursuant to Policy 804, Records Maintenance and Release.

Requests for recorded video from other law enforcement agencies shall be referred to the Investigations Division Captain, or their designee for release in accordance with this policy and must be related to a specific active criminal investigation.

Requests for recorded video from the Office of Director of Police Accountability and Police Accountability Board shall be referred to the Investigations Division Captain, or their designee, for release in accordance with Charter Article XVIII, Section 25, Subdivision (20)(a).

Recorded video images that are the subject of a court order or subpoena shall be processed in accordance with the established department subpoena process.

351.7 VIDEO SURVEILLANCE AUDIT

The video surveillance software generates a site log each time the system is accessed. The site log is broken down by server, device, user or general access. The site log is kept on the server for two years and is exportable for reporting. System audits will be conducted by the Office of Strategic Planning and Accountability on a regular basis, at least biennial.

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

The audit shall be documented in the form an internal department memorandum to the Chief of Police. The memorandum shall include any data errors found so that such errors can be corrected. After review by the Chief of Police, the memorandum and any associated documentation shall be published on the City of Berkeley website in an appropriate location, and retained within the Office of Strategic Planning and Accountability.

351.8 TRAINING

All department members authorized to operate or access video surveillance systems shall receive appropriate training. Training should include guidance on the use of cameras, associated software, and review of relevant policies and procedures, including this policy, as well as review of relevant City of Berkeley laws and regulations. Training should also address state and federal law related to the use of video surveillance equipment and privacy. All relevant recordings that are utilized

Page 14 of 18
Berkeley Police Department
Law Enforcement Services Manual

External Fixed Video Surveillance Cameras

will be collected pursuant to Policy 802, Property and Evidence, and retained pursuant to Policy 804, Records and Maintenance.

351.9 MAINTENANCE

It shall be the responsibility of the Public Works Director to facilitate and coordinate any updates and required maintenance, with access limited to that detailed in the City Manager's promulgated policies.

Surveillance Use Policy-External Fixed Video Surveillance Cameras

1304.1 PURPOSE

This policy provides guidance for the use of City of Berkeley external fixed video surveillance cameras by the Berkeley Police Department (BPD).

This policy only applies to fixed, overt, marked external video surveillance systems utilized by BPD. It does not apply to mobile audio/video systems, covert audio/video systems or any other image-capturing devices used by the Department. Department personnel shall adhere to the requirements for External Fixed Video Surveillance Cameras covered in this policy as well as the corresponding Use Policy-351.

This Surveillance Use Policy is legally-enforceable pursuant to BMC 2.99.

1304.2 AUTHORIZED USE

Only BPD members who receive training on this policy, who are then granted access by an administrator may access the data from the video surveillance cameras. This data may only be accessed to further a legitimate law enforcement purpose, as listed in this Policy. Members must follow the necessary logging mechanisms, such as case number and case type when querying the database.

The cameras shall only record video images and not sound. Recorded images pursuant to Section 351.5 may be accessed, reviewed, and used for specific criminal or BPD administrative investigations and video surveillance may be accessed and reviewed by authorized BPD personnel for the following purposes:

- (a) To support specific and active criminal investigations.
- (b) To support serious traffic-related investigations.
- (c) To support police misconduct investigations, and
- (d) To respond to and review critical incidents or natural disasters.

Unauthorized recording, viewing, reproduction, dissemination, or retention of video footage is prohibited.

The following are prohibited uses of the video surveillance system:

- (a) Unauthorized recording, viewing, reproduction, dissemination, or retention of video footage is prohibited.
- (b) Video surveillance systems will not intentionally be used to invade the privacy of individuals or observe areas where a reasonable expectation of privacy exists.
- (c) Video surveillance systems shall not be used in an unequal or discriminatory manner and shall not target protected individual characteristics including, but not limited to race, ethnicity, national origin, religion, disability, gender or sexual orientation.

Page 16 of 18
Berkeley Police Department
 Law Enforcement Services Manual

Surveillance Use Policy-External Fixed Video Surveillance Cameras

- (d) Video surveillance equipment shall not be used to harass, intimidate or discriminate against any individual or group.
- (e) Video surveillance systems and recordings are subject to the Berkeley Police Department's Immigration Law Policy, and hence may not be shared with federal immigration enforcement officials.

1304.3 DATA COLLECTION

The cameras will film and store video on City of Berkeley encrypted servers. License plate and facial recognition data hardware is not installed on the cameras and may not be installed or used unless approved by the City council. Audio is a standard feature of the camera, but is deactivated by the system administrator and may not be activated or used unless approved by the City Council. The cameras and storage devices shall be wholly owned and operated/maintained by the City of Berkeley.

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, with technical assistance from Public Works Department and Department of Information Technology personnel. Information may be shared in accordance with 1304.9 below. BPD members seeking access to the video surveillance system shall obtain the approval of the Investigations Division Captain, or their designee.

Supervisors should monitor camera access and usage to ensure BPD members are complying with this policy, other applicable department policy, and applicable laws. Supervisors should ensure such use and access is appropriately documented.

1304.5 DATA PROTECTION

All data transferred from the cameras and the servers shall be encrypted. Access to the data must be obtained through the Public Works Department according to this policy and published regulations that limit access and use of data by Public Works and other City Departments and personnel. All system access including system log-in, access duration, and data access points is accessible and reportable and shall be documented by the Public Works Department's authorized administrator. All relevant recordings that are utilized will be collected pursuant to Policy 802, Property and Evidence, and retained pursuant to Policy 804 Records and Maintenance.

1304.6 CIVIL LIBERTIES AND RIGHTS PROTECTION

The Berkeley Police Department is dedicated to the most efficient utilization of its resources and services in its public safety endeavors. The Berkeley Police Department recognizes the need to protect its ownership and control over shared information and to protect the privacy and civil liberties of the public, in accordance with federal and state law. Provisions of this policy, including 1304.4 Data Access, 1304.5 Data Protection, 1304.7 Data Retention, 1304.8 Public Access and 1304.9 Third Party Data Sharing serve to protect against any unauthorized use of video

Page 17 of 18
Berkeley Police Department
Law Enforcement Services Manual

Surveillance Use Policy-External Fixed Video Surveillance Cameras

surveillance camera data. License plate and facial recognition data hardware is not installed on the cameras. Audio is a standard feature of the camera, but is deactivated by the system administrator. These procedures ensure the data is not used in a way that would violate or infringe upon anyone's civil rights and/or liberties, including but not limited to potentially disparate or adverse impacts on any communities or groups.

1304.7 DATA RETENTION

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. Recordings of incidents involving use of force by a police officer or involving detentions, arrests, or recordings relevant to a formal or informal complaint against a police officer shall be retained for a minimum of two years and one month. Recordings relating to court cases and complaints against BPD sworn officers that are being adjudicated will be manually deleted at the same time other evidence associated with the case is purged in line with the Department's evidence retention policy. Any recordings related to BPD administrative proceedings pursuant to this section shall be maintained until such matter is fully adjudicated, at which time it shall be deleted in line with the Department's evidence retention policy, and any applicable orders from the court. All data will automatically delete after the aforementioned retention period by the System Administrator from Public Works.

Any recordings needed as evidence in a criminal or police misconduct proceeding shall be copied to a suitable medium and booked into evidence in accordance with current evidence procedures.

1304.8 PUBLIC ACCESS

Data collected and used in a police report shall be made available to the public in accordance with department policy and applicable state or federal law.

Requests for recorded video images from the public or the media shall be processed in the same manner as requests for department public records pursuant to Policy 804.

Recorded video images that are the subject of a court order or subpoena shall be processed in accordance with the established department subpoena process.

1304.9 THIRD-PARTY DATA-SHARING

Requests for recorded video from other law enforcement agencies shall be referred to the Investigations Division Captain, or their designee for release in accordance with this policy, and must be related to a specific active criminal investigation.

Data collected from the video surveillance system may be shared with the following:

- (a) The District Attorney's Office for use as evidence to aid in prosecution, in accordance with laws governing evidence;
- (b) Other law enforcement personnel as part of an active criminal investigation;

Page 18 of 18
Berkeley Police Department
 Law Enforcement Services Manual

Surveillance Use Policy-External Fixed Video Surveillance Cameras

- (c) Recorded video images that are the subject of a court order or subpoena shall be processed in accordance with the established department subpoena process

Requests for recorded video from the Office of Director of Police Accountability and Police Accountability Board shall be referred to the Investigations Division Captain, or their designee, for release in accordance with Charter Article XVIII, Section 125, Subdivision (20)(a).

1304.10 TRAINING

All BPD members authorized to operate or access video surveillance systems shall receive appropriate training. Training should include guidance on the use of cameras, associated software, and review of relevant policies and procedures, including this policy as well as review of relevant City of Berkeley laws and regulations.

Training should also address state and federal law related to the use of video surveillance equipment and privacy. All relevant recordings that are utilized will be collected pursuant to Policy 802 Property and Evidence, and retained pursuant to Policy 804 Records Maintenance.

1304.11 AUDITING AND OVERSIGHT

The video surveillance software generates a site log each time the system is accessed. The site log is broken down by server, device, user or general access. The site log is kept on the server for two years and is exportable for reporting. Video surveillance system audits will be conducted by the Professional Standards Bureau's Audit and Inspections Sergeant on a regular basis, at least biennial.

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.

The audit shall be documented in the form of an internal department memorandum to the Chief of Police. The memorandum shall include any data errors found so that such errors can be corrected. After review by the Chief of Police, the memorandum and any associated documentation shall be placed into the annual report filed with the City Council pursuant to BMC Section 2.99.020 2. d., published on the City of Berkeley website in an appropriate location, and retained within the Professional Standards Bureau.

1304.12 MAINTENANCE

It shall be the responsibility of the Public Works Department to facilitate and coordinate any updates and required maintenance with access limited to that detailed in the City Manager's promulgated policies.

Attachment 5:
BPD Policy 1304 – External Fixed Surveillance
Video Cameras

Surveillance Use Policy-External Fixed Video Surveillance Cameras

1304.1 PURPOSE

This policy provides guidance for the use of City of Berkeley external fixed video surveillance cameras by the Berkeley Police Department (BPD).

This policy only applies to fixed, overt, marked external video surveillance systems utilized by BPD. It does not apply to mobile audio/video systems, covert audio/video systems or any other image-capturing devices used by the Department. Department personnel shall adhere to the requirements for External Fixed Video Surveillance Cameras covered in this policy as well as the corresponding Use Policy-351.

This Surveillance Use Policy is legally-enforceable pursuant to BMC 2.99.

1304.2 AUTHORIZED USE

Only BPD members who receive training on this policy, who are then granted access by an administrator may access the data from the video surveillance cameras. This data may only be accessed to further a legitimate law enforcement purpose, as listed in this Policy. Members must follow the necessary logging mechanisms, such as case number and case type when querying the database.

The cameras shall only record video images and not sound. Recorded images pursuant to Section 351.5 may be accessed, reviewed, and used for specific criminal or BPD administrative investigations and video surveillance may be accessed and reviewed by authorized BPD personnel for the following purposes:

- (a) To support specific and active criminal investigations.
- (b) To support serious traffic-related investigations.
- (c) To support police misconduct investigations, and
- (d) To respond to and review critical incidents or natural disasters.

Unauthorized recording, viewing, reproduction, dissemination, or retention of video footage is prohibited.

The following are prohibited uses of the video surveillance system:

- (a) Unauthorized recording, viewing, reproduction, dissemination, or retention of video footage is prohibited.
- (b) Video surveillance systems will not intentionally be used to invade the privacy of individuals or observe areas where a reasonable expectation of privacy exists.
- (c) Video surveillance systems shall not be used in an unequal or discriminatory manner and shall not target protected individual characteristics including, but not limited to race, ethnicity, national origin, religion, disability, gender or sexual orientation.

Berkeley Police Department

Law Enforcement Manual

Surveillance Use Policy-External Fixed Video Surveillance Cameras

- (d) Video surveillance equipment shall not be used to harass, intimidate or discriminate against any individual or group.
- (e) Video surveillance systems and recordings are subject to the Berkeley Police Department's Immigration Law Policy, and hence may not be shared with federal immigration enforcement officials.

1304.3 DATA COLLECTION

The cameras will film and store video on City of Berkeley encrypted servers. License plate and facial recognition data hardware is not installed on the cameras and may not be installed or used unless approved by the City council. Audio is a standard feature of the camera, but is deactivated by the system administrator and may not be activated or used unless approved by the City Council. The cameras and storage devices shall be wholly owned and operated/maintained by the City of Berkeley.

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, with technical assistance from Public Works Department and Department of Information Technology personnel. Information may be shared in accordance with 1304.9 below. BPD members seeking access to the video surveillance system shall obtain the approval of the Investigations Division Captain, or their designee.

Supervisors should monitor camera access and usage to ensure BPD members are complying with this policy, other applicable department policy, and applicable laws. Supervisors should ensure such use and access is appropriately documented.

1304.5 DATA PROTECTION

All data transferred from the cameras and the servers shall be encrypted. Access to the data must be obtained through the Public Works Department according to this policy and published regulations that limit access and use of data by Public Works and other City Departments and personnel. All system access including system log-in, access duration, and data access points is accessible and reportable and shall be documented by the Public Works Department's authorized administrator. All relevant recordings that are utilized will be collected pursuant to Policy 802, Property and Evidence, and retained pursuant to Policy 804 Records and Maintenance.

1304.6 CIVIL LIBERTIES AND RIGHTS PROTECTION

The Berkeley Police Department is dedicated to the most efficient utilization of its resources and services in its public safety endeavors. The Berkeley Police Department recognizes the need to protect its ownership and control over shared information and to protect the privacy and civil liberties of the public, in accordance with federal and state law. Provisions of this policy, including 1304.4 Data Access, 1304.5 Data Protection, 1304.7 Data Retention, 1304.8 Public Access and 1304.9 Third Party Data Sharing serve to protect against any unauthorized use of video surveillance camera data. License plate and facial recognition data hardware is not installed on the cameras. Audio is a standard feature of the camera, but is deactivated by the system administrator.

Berkeley Police Department

Law Enforcement Manual

Surveillance Use Policy-External Fixed Video Surveillance Cameras

These procedures ensure the data is not used in a way that would violate or infringe upon anyone's civil rights and/or liberties, including but not limited to potentially disparate or adverse impacts on any communities or groups.

1304.7 DATA RETENTION

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. Recordings of incidents involving use of force by a police officer or involving detentions, arrests, or recordings relevant to a formal or informal complaint against a police officer shall be retained for a minimum of two years and one month. Recordings relating to court cases and complaints against BPD sworn officers that are being adjudicated will be manually deleted at the same time other evidence associated with the case is purged in line with the Department's evidence retention policy. Any recordings related to BPD administrative proceedings pursuant to this section shall be maintained until such matter is fully adjudicated, at which time it shall be deleted in line with the Department's evidence retention policy, and any applicable orders from the court. All data will automatically delete after the aforementioned retention period by the System Administrator from Public Works.

Any recordings needed as evidence in a criminal or police misconduct proceeding shall be copied to a suitable medium and booked into evidence in accordance with current evidence procedures.

1304.8 PUBLIC ACCESS

Data collected and used in a police report shall be made available to the public in accordance with department policy and applicable state or federal law.

Requests for recorded video images from the public or the media shall be processed in the same manner as requests for department public records pursuant to Policy 804.

Recorded video images that are the subject of a court order or subpoena shall be processed in accordance with the established department subpoena process.

1304.9 THIRD-PARTY DATA-SHARING

Requests for recorded video from other law enforcement agencies shall be referred to the Investigations Division Captain, or their designee for release in accordance with this policy, and must be related to a specific active criminal investigation.

Data collected from the video surveillance system may be shared with the following:

- (a) The District Attorney's Office for use as evidence to aid in prosecution, in accordance with laws governing evidence;
- (b) Other law enforcement personnel as part of an active criminal investigation;
- (c) Recorded video images that are the subject of a court order or subpoena shall be processed in accordance with the established department subpoena process

Berkeley Police Department

Law Enforcement Manual

Surveillance Use Policy-External Fixed Video Surveillance Cameras

Requests for recorded video from the Office of Director of Police Accountability and Police Accountability Board shall be referred to the Investigations Division Captain, or their designee, for release in accordance with Charter Article XVIII, Section 125, Subdivision (20)(a).

1304.10 TRAINING

All BPD members authorized to operate or access video surveillance systems shall receive appropriate training. Training should include guidance on the use of cameras, associated software, and review of relevant policies and procedures, including this policy as well as review of relevant City of Berkeley laws and regulations.

Training should also address state and federal law related to the use of video surveillance equipment and privacy. All relevant recordings that are utilized will be collected pursuant to Policy 802 Property and Evidence, and retained pursuant to Policy 804 Records Maintenance.

1304.11 AUDITING AND OVERSIGHT

The video surveillance software generates a site log each time the system is accessed. The site log is broken down by server, device, user or general access. The site log is kept on the server for two years and is exportable for reporting. Video surveillance system audits will be conducted by the Professional Standards Bureau's Audit and Inspections Sergeant on a regular basis, at least biennial.

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.

The audit shall be documented in the form of an internal department memorandum to the Chief of Police. The memorandum shall include any data errors found so that such errors can be corrected. After review by the Chief of Police, the memorandum and any associated documentation shall be placed into the annual report filed with the City Council pursuant to BMC Section 2.99.020 2. d., published on the City of Berkeley website in an appropriate location, and retained within the Professional Standards Bureau.

1304.12 MAINTENANCE

It shall be the responsibility of the Public Works Department to facilitate and coordinate any updates and required maintenance with access limited to that detailed in the City Manager's promulgated policies.

Item 9.c.

ODPA Memorandum Titled "Update on BPD Radio Encryption and
Potential Next Steps



MEMORANDUM

Date: September 10, 2025
 To: Honorable Members of the Police Accountability Board (PAB)
 From: Hansel Aguilar, Director of Police Accountability (DPA) *HA*
 Jose Murillo, ODPA Policy Analyst *JM*
 Subject: Update on BPD Radio Encryption and Potential Next Steps

This memorandum updates the Police Accountability Board (PAB) on the status of the Berkeley Police Department's (BPD) transition to encrypted radio channels following the City Council's consideration of the proposal on October 28, 2025.¹

Background

On September 10, 2025, the Office of the Director of Police Accountability (ODPA) issued a memorandum informing the Police Accountability Board (PAB) of the transition of Alameda County police departments to full radio encryption², as part of a coordinated effort led by the East Bay Regional Communication System Authority (EBRCSA) to be in compliance with the California Department of Justice (DOJ) Bulletin 20-09-CJIS³. At the time of the memorandum and during the PAB's September 17, 2025, regular meeting, the Board was informed that the Berkeley Police Department (BPD) would maintain its existing radio communication practices for the time being, while not ruling out the possibility of full encryption in the future. The memorandum's preliminary analysis of the advantages and trade-offs of full radio encryption was intended to serve as a foundation

¹ Berkeley City Council Regular Meeting Agenda for October 28, 2025: <https://berkeleyca.gov/city-council-regular-meeting-agenda-october-28-2025>

² September 10, 2025 ODPA Memorandum to the PAB titled "Overview and Considerations for Potential Police Radio Encryption at Berkeley Police Department": <https://berkeleyca.gov/sites/default/files/legislative-body-meeting-attachments/2025-09-17%20PAB%20Regular%20Meeting%20Packet.pdf#Page=74>

³ California Department of Justice Bulletin 20-09-CJIS "Confidentiality of Information from the California Enforcement Telecommunications Systems (CLETS)": https://www.oag.ca.gov/sites/all/files/agweb/pdfs/info_bulletins/20-09-cjis.pdf

for potential future PAB policy review, should the BPD later decide—or be required—to encrypt its radio communications. The PAB did not take a formal position at that time.⁴

At its October 14, 2025 meeting, the Agenda and Rules Committee (ARC) approved the City Manager's request to place the topic of police radio encryption on the October 28, 2025 City Council agenda under the consent calendar.⁵ Following the item's inclusion on the agenda—and in response to community feedback and concerns raised by members of the press—Director Aguilar and Chair Cayetano submitted a letter⁶ to the Council recommending that action on the item be postponed to allow for additional research and community engagement. The letter did not take a position for or against radio encryption but instead called for a more comprehensive public discussion and further study of the issue.

At the October 28 regular meeting, the topic drew significant public interest, with 31 members of the public offering comment and sharing their perspectives. Council moved the item from the consent calendar to the action calendar to allow for discussion of the item and ultimately approved the resolution authorizing the transition,⁷ as revised in the supplemental materials.⁸ The revisions included a requirement for a public call log listing the general type of call, the nearest intersection or block-level address, and the time the call was received—with a brief delay to protect privacy and operational safety. The implementation date was unavailable as of the time of this memo but the Resolution

⁴ PAB Regular Meeting Minutes for September 17, 2025: <https://berkeleyca.gov/sites/default/files/legislative-body-meeting-minutes/DRAFT%202025-09-17%20Regular%20Meeting%20Minutes.pdf>

⁵ Berkeley City Council Agenda and Rules Committee Special Meeting Minutes for October 14, 2025: <https://berkeleyca.gov/sites/default/files/legislative-body-meeting-minutes/10-14%20Minutes%20-%20Agenda%20Committee.pdf>

⁶ October 28, 2025 ODP Letter to Council Titled "Importance of Proper Vetting for Public Safety Policy Changes – Concerns About Item 18 "Authorization to Encrypt Berkeley Police Department Primary Radio Channels:" https://berkeleyca.gov/sites/default/files/documents/2025-10-28%20DPA%20Ltr%20to%20CoB%20Council-%20Radio%20Encryption%20Concerns_Final.pdf

⁷ Annotated Agenda for the Berkeley City Council Meeting of October 28, 2025: <https://berkeleyca.gov/sites/default/files/city-council-meetings/2025-10-28%20Annotated%20Agenda%20-%20Council.pdf>

⁸ Supplemental Material for Item 18 of the Berkeley City Council's October 28, 2025 Meeting: <https://berkeleyca.gov/sites/default/files/documents/Supp%20%20Packet%20-Encryption.pdf>

called for the implementation “as soon as practicable following Council authorization and administrative preparation.”⁹

PAB Authority

Section 125(3)(a)(1) of the Berkeley City Charter¹⁰ authorizes the PAB to advise and make recommendations to the public, City Council, and City Manager on matters related to the operation of the Berkeley Police Department (BPD), including all written policies, practices, and procedures. Additionally, Charter Section 125(17)(a)¹¹ requires the Chief of Police to submit all newly adopted departmental policies and revisions to the Board within thirty (30) days of implementation. The Board may review BPD policies, practices, and procedures at its discretion, or in response to a public request, a policy complaint, or a complaint filed against an officer. In light of the considerable public interest in this topic, the PAB may wish to undertake a policy review of police radio encryption to inform its assessment of the forthcoming policy and to provide the community with further information on best practices related to the issue.

Courses of Action:

In considering a new policy review, the Board may consider a range of potential action¹², including:

1. Assigning a Board member to conduct the review.
2. Directing ODPa staff to carry out the research
3. Establishing a subcommittee to carry out the research.
4. Choose not to take on the review.

Recommendation:

The PAB should undertake a review of police radio encryption, examining relevant laws, community concerns, and other jurisdictions’ practices, and use these findings to provide a clear, informed recommendation to the BPD.

⁹ Id.

¹⁰ Berkeley City Charter Section 125(3)(a)(1): [https://berkeley.municipal.codes/Charter/125\(3\)\(a\)](https://berkeley.municipal.codes/Charter/125(3)(a))

¹¹ Berkeley City Charter Section 125(17)(a): [https://berkeley.municipal.codes/Charter/125\(17\)\(a\)/share](https://berkeley.municipal.codes/Charter/125(17)(a)/share)

¹² Section G(3)(a) "Policy Complaints and Reviews" of the PAB's Standing Rules: https://berkeleyca.gov/sites/default/files/2022-02/PoliceAccountabilityBoard_StandingRules.pdf