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

November 10, 2025

VIA ELECTRONIC MAIL

Honorable Mayor Ishii and Members of the Berkeley City Council
Council@berkeleyca.gov
2180 Milvia Street
Berkeley, CA 94704

Re: Item 11 - 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

Dear Honorable Mayor Ishii and Members of the Berkeley City Council:

On behalf of the Police Accountability Board (PAB), I write to highlight three concerns regarding Berkeley Police Department's (BPD) Annual Surveillance Technology Report (or "Report"), currently Item 11 on the Berkeley City Council's action calendar for its November 10, 2025, meeting.[1]

First, the Report was published to the Council's action calendar without input from or even advance notice to the PAB. BPD Policy 1305.12 specifically requires that the results of any audits of ALPR data—like the audit described in the Report—be shared with Office of the Director of Police Accountability (ODPA) upon their completion.[2] More fundamentally, as we explained in a recent letter regarding BPD's unilateral proposal to encrypt radios,[3] both the Council and the

[1] At its November 6, 2025 meeting, the PAB voted 5-0 to approve a Motion to authorize Chair Cayetano to send a letter to the City Council, either prior to the November 10th Regular Council meeting or at a later appropriate time, to address procedural and substantive concerns regarding the Annual Surveillance Technology Report and to reiterate the PAB's opposition to the use of Flock. Video recording can be accessed at the following link with relevant remarks at [01:17:56]: https://youtu.be/lPytFxB6jyw?si=eu9uiwxrvfYYZiiQ
[2] See Attachment 1: BPD Policy 1305 – Fixed ALPR
[3] October 28, 2025 ODPA Letter to Council Re: Importance of Proper Vetting for Public Safety Policy Changes — Concerns About

public benefit from the PAB's review of public safety items submitted on behalf of BPD prior to their publication. In this instance, if the PAB was provided with the draft prior to publication, the PAB could have informed BPD and the City Manager that Berkeley Municipal Code 2.99.020(2)(c) requires that the Report include a summary of complaints received by the City, including the PAB, and provided BPD and the City Manager with that relevant information.[4] The day that the ODPA and the PAB noticed that the Report did not include the required information, we notified the City Manager and Chief Louis.

Specifically, the PAB and ODPA notified the City Manager of two complaints involving the use of body-worn camera, a surveillance technology enumerated in BMC 2.99.020.[5] In response, the Chief argued that the complaints should not be included in the Report because the allegations were not raised by a member of the public in their initial complaint. The PAB respectfully disagrees. If that were true, complaints alleging failure to follow BPD's body-worn camera policy would rarely, if ever, be included in the Report because complainants are routinely prevented from accessing body worn camera footage under current BPD practices. Omitting the types of complaints that the PAB identified would circumvent the purpose of the Surveillance Technology Ordinance by decreasing transparency and depriving the Council of the data that ensures the safeguards of the people's civil liberties have been "strictly observed."[6] We ask Council to require BPD to supplement this year's annual report with all complaints about Surveillance Technology, including the ones submitted to the PAB, and "any information about violations or potential violations of the Surveillance Use Policy" as required by law.[7]

Second, pages 40 to 45 of the Report describe the results of a Flock ALPR audit conducted by BPD, which inexplicably refuses to conclude that one or more external agencies searched Berkeley

---

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

[4] Berkeley Municipal Code 2.99.020(2)(c) plainly states that the Report shall include "[a] summary of each complaint, if any, received by ***the City*** about the Surveillance Technology."

[5] 2024-CI-0031, Allegation 6: Improper Police Procedures (Improper body-worn camera use) – Whether the subject officers activated their BWC as required by policy; 2025-CI-0018, Allegation 6: Improper Police Procedures (Improper body-worn camera use) – Whether the subject officers activated their BWC as required by policy.

[6] BMC 2.99.010 states that "In addition to applicable local, state, and federal law, legally enforceable safeguards, including robust transparency, oversight, and accountability measures, are important in the protection of civil rights and civil liberties" and "Data reporting measures will enable the City Council and public to confirm that mandated civil rights and civil liberties safeguards have been strictly observed."

[7] The Ordinance explicitly mandates that BPD include "any information about violations or potential violations of the Surveillance Use Policy." BMC 2.99.020(2)(d).

and other California cities' ALPR data for the purposes of federal immigration enforcement, a practice that violates BPD policy. BPD explains that an unidentified number of external law enforcement agencies entered "ICE" once and "CBP" twice in the reason field when it searched the statewide ALPR data, including Berkeley's. BPD does not explain which California agencies improperly accessed ALPR data, nor does it explain when BPD identified the non-compliant use of the statewide ALPR data lookup function. Notwithstanding the reference to ICE and CPB, BPD does not conclude that there was a violation of California law or Policy 1305, 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.[8] These measures have not been formally memorialized in BPD Policy at the time of this writing.

Third, while the PAB appreciates 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 Council should take notice of the timing of the ALPR audit report and its presentation. 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 that were submitted pursuant to the Surveillance Technology Ordinance, BPD did not mention that it identified a potential policy violation of Policy 1305 or Berkeley's sanctuary city resolution.[9] In fact, the PAB submitted materials, urging Council to adopt revisions to the Fixed Surveillance Camera Use Policy, citing data security issues that were reported in *other* jurisdictions, and still,

[8] At the PAB meeting on November 5, 2025, BPD refused to identify the agencies responsible for the potential breach because "*those fall under investigatory records that aren't released publicly*."
Relevant remarks [40:42] https://youtu.be/lPytFxB6jyw?si=gCtR8SUAWQy7gqOC&t=2442

[9] See Attachment 2: 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*."

BPD did not mention, either in its papers or at the hearing, the breach that it identified. BPD, in other words, was less than forthcoming about the data security issues with Flock Safety.

The PAB recommended to Council, and Council agreed, to subject external fixed surveillance camera data to the same audit procedures as ALPR data based on the PAB's historic understanding of the audit procedure. After reviewing the audit report and considering the delayed notification to the PAB and the Council, the PAB recommends that the Council (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; (3) memorialize the remedial controls that BPD implemented in Policies 1304 and 1305; and (4) require BPD or the City Manager to include an addendum or follow-up report on the identified instances of ODPA/PAB identified misuse in the surveillance report.

Respectfully submitted,

Joshua Cayetano

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

Cc: Paul Buddenhagen, City Manager
David White, Deputy City Manager
Jennifer Louis, Chief of Police
Jen Tate, Deputy Chief of Police
Hansel A. Aguilar, Director of Police Accountability
Farimah Brown, City Attorney
Mark Numainville, City Clerk

ATTACHMENTS: BPD Policy 1305 – Fixed ALPR
STO Submission for External Fixed Surveillance Cameras

ATTACHMENT 1

BPD Policy 1305 – Fixed ALPR

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

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).

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 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 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.

(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.

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.

1305.14 ATTACHMENTS

See attachment: ALPR Acknowledgment Letter.pdf

Attachments

ALPR Acknowledgment Letter.pdf

AUTOMATED LICENSE PLATE READERS

DATA SHARING ACKNOWLEDGMENT LETTER

This letter is to certify that the (AGENCY NAME) has requested to receive data from the Berkeley Police Department's Automated License Plate Readers Program.

Data shared by the Berkeley Police Department will only be used for legitimate California law enforcement purposes ONLY, and not for other purposes such as immigration, personal use, harassment, and any other usages that are against the Berkeley Police Department's Policy.

By signing this letter, the representatives of (AGENCY NAME) agree to abide by this policy.

_____
(Signature/Print name)

_____
(Title/Rank)

_____
(Date)

ATTACHMENT 2

STO Submission for External Fixed Surveillance Cameras

17

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

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)

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
- Milvia / Alston
- College / Ashby
- 9th / Gilman

- 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.

- 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.

- 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.

- 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:

- 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.

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

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

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.

(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. 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

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.