

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

PUBLIC MEETING MATERIAL



**POLICE ACCOUNTABILITY BOARD
REGULAR MEETING AGENDA PACKET
October 21, 2026
6:30 PM**

Board Members

Joshua Cayetano (Chair)	Leah Wilson (Vice-Chair)
Joshua Buswell-Charkow	Stephanie Allan
Patrick DeTemple	Jasmina Viteskic
Anay Sharma	Dwayne Phillips (Alternate)

MEETING LOCATION

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

Agenda Item Materials

Item	Description	Page
2	October 21, 2026 PAB Regular Meeting Agenda	1
4	Minutes for the Regular Meeting of October 7, 2026	7
8	Subcommittee List	15
9.a.i	Preliminary Review and Recommendation of Policy Complaint 2026-PR-0002	18
9.a.ii	Preliminary Review and Recommendation of Policy Complaint 2026-PR-0003	24
9.a.iii	Preliminary Review and Recommendation of Policy Complaint 2026-PR-0004	30
9.b.	October 16, 2026 Memorandum from the ODPA to the PAB Titled "Review of BPD Surveillance Technology Proposals and Policy Revisions"	38

Off Agenda Reports

Item	Description	Page
1	Policy Review Status Updates	179
2	Legislative Updates Relevant to the PAB's Work	182
3	List of Remaining 2026 PAB Meetings	187

Item 2

October 21, 2026 PAB Regular Meeting Agenda



POLICE ACCOUNTABILITY BOARD
REGULAR MEETING AGENDA
WEDNESDAY, OCTOBER 21, 2026
6:30 P.M.

Board Members

Joshua Cayetano (Chair)	Leah Wilson (Vice-Chair)
Joshua Buswell-Charkow	Stephanie Allan
Patrick DeTemple	Jasmina Viteskic
Anay Sharma	Dwayne Phillips (Alternate)

MEETING LOCATION

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

PUBLIC NOTICE

To access the meeting remotely: join from a PC, Mac, iPad, iPhone, or Android device using this URL: <https://us02web.zoom.us/j/89007838093>. If you do not wish for your name to appear on the screen, use the drop-down menu and click on “rename” to rename yourself to be anonymous. To request to speak, use the “raise hand” icon on the screen. To join by phone: Dial **1 669 900 6833** and enter Meeting ID **890 0783 8093**. If you wish to comment during the public comment portion of the agenda, press *9 and wait to be recognized.

LAND ACKNOWLEDGMENT

The City of Berkeley recognizes that the community we live in was built on the territory of xučyun (Huchiun (Hooch-yoon)), the ancestral and unceded land of the Chochenyo (Chochen-yo)-speaking Ohlone (Oh-low-nee) people, the ancestors and descendants of the sovereign Verona Band of Alameda County. This land was and continues to be of great importance to all of the Ohlone Tribes and descendants of the Verona Band. As we begin our meeting tonight, we acknowledge and honor the original inhabitants of Berkeley, the documented 5,000-year history of a vibrant community at the West Berkeley Shellmound, and the Ohlone people who continue to reside in the East Bay. We recognize that Berkeley's residents have and continue to benefit from the use and occupation of this uncaded stolen land since the City of Berkeley's incorporation in 1878. As stewards of the laws regulating the City of Berkeley, it is not only vital that we recognize the history of this land, but also recognize that the Ohlone people are present members of Berkeley and other East Bay communities today.

AGENDA

1. CALL TO ORDER AND ROLL CALL (2 MINUTES)

2. APPROVAL OF AGENDA (2 MINUTES)

3. PUBLIC COMMENT (TBD)

Speakers are generally allotted up to three minutes but may be allotted less time if there are many speakers; they may comment on any matter within the Board's jurisdiction at this time, except confidential personnel matters.

4. APPROVAL OF MINUTES (5 MINUTES)

- a. Minutes for the Regular Meeting of October 7, 2026.

5. ODPa STAFF REPORT (10 MINUTES)

Announcements, updates, and other items.

6. CHAIR AND BOARD MEMBERS' REPORTS (10 MINUTES)

The Chair and Board Members report on their activities.

7. CHIEF OF POLICE'S REPORT (10 MINUTES)

Crime/cases of interest, community engagement/department events, staffing, training, and other items of interest.

8. SUBCOMMITTEE REPORTS (10 MINUTES)

Report of activities and meeting schedule for all subcommittees, possible appointment or reassignment of members to subcommittees, and additional discussion and action as warranted for the subcommittees listed on the PAB's Subcommittee List included in the agenda packet.

9. DISCUSSION AND ACTION ITEMS (ESTIMATED TIME: 50 MINUTES)

The PAB will discuss and may act on the following items, including providing feedback, recommendations, or other directions, as appropriate.

- a. Discussion and action on the acceptance or rejection of the following policy complaints (ODPA) – (30 Minutes):
 - i. 2026-PR-0002
 - ii. 2026-PR-0003
 - iii. 2026-PR-0004
- b. Update and discussion on the Berkeley Police Department's vendor RFP for surveillance technology, revised Surveillance Technology Use Policies, and Acquisition Reports. (ODPA) – (20 Minutes)

10. PUBLIC COMMENT (TBD)

Speakers are generally allotted up to three minutes but may be allotted less time if there are many speakers; they may comment on any matter within the Board's jurisdiction at this time, except confidential personnel matters.

11. CLOSED SESSION

CLOSED SESSION ITEMS

Pursuant to the Court's order in *Berkeley Police Association v. City of Berkeley, et al.*, Alameda County Superior Court Case No. 2002-057569, the Board will recess into closed session to discuss and act on the following matter(s):

- a. Conference With Labor Negotiators; Government Code § 54957.6
Designated representatives: Leah Wilson, Designated PAB Representative;
Mary Opler, Director of Police Accountability
Employee organization: Berkeley Police Association
- b. Case Updates and Recommendations Regarding Complaints Received by the ODPA:
 - i. 2023-CI-0016
 - ii. 2025-CI-0018
 - iii. 2025-CI-0030
 - iv. 2025-CI-0037
 - v. 2026-CI-0002
 - vi. 2026-CI-0005
 - vii. 2026-CI-0007
 - viii. 2026-CI-0008
 - ix. 2026-CI-0010
 - x. 2026-CI-0011
 - xi. 2026-CI-0012
 - xii. 2026-CI-0015
 - xiii. 2026-CI-0016
 - xv. 2026-CI-0019
 - xvi. 2026-CI-0020
 - xvii. 2026-CI-0021
 - xviii. 2026-CI-0022
 - xix. 2026-CI-0023
 - xx. 2026-CI-0024
 - xxi. 2026-CI-0025
 - xxii. 2026-CI-0026
 - xxiii. 2026-CI-0027
 - xxiv. 2026-CI-0028
 - xxv. 2026-CI-0029
 - xxvi. 2026-CI-0030
 - xxvii. 2026-CI-0031

xiv. 2026-CI-0018

xxviii. 2026-CI-0032

xxix. 2026-CI-0033

xxx. 2026-CI-0034

END OF CLOSED SESSION

12.ANNOUNCEMENT OF CLOSED SESSION ACTIONS (1 MINUTE)

13.ADJOURNMENT (1 MINUTE)

Off Agenda Reports

1. Policy, Practice, and Procedure Review Status Report
2. Legislative Updates Relevant to the PAB's Work
3. 2026 PAB Meeting Calendar

Communications Disclaimer

Communications to the Police Accountability Board, like all communications to Berkeley boards, commissions, or committees, are public records and will become part of the City's electronic records, which are accessible through the City's website. Please note: e-mail addresses, names, addresses, and other contact information are not required, but if included in any communication to a City board, commission, or committee, will become part of the public record. If you do not want your e-mail address or any other contact information to be made public, you may deliver communications via U.S. Postal Service or in person to the Board Secretary. If you do not want your contact information included in the public record, do not include that information in your communication. Please contact the Board Secretary for further information.



Communication Access Information (A.R. 1.12)

To request a disability-related accommodation(s) to participate in the meeting, including auxiliary aids or services, please contact the Disability Services specialist at 981-6418 (V) or 981-6347 (TDD) at least three business days before the meeting date.

SB 343 Disclaimer

Any writings or documents provided to a majority of the Board regarding any item on this agenda will be made available for public inspection at the Office of the Director of Police Accountability, located at 1900 Addison Street, Floor 3, Berkeley, CA 94704

Contact the Director of Police Accountability (Board Secretary) at:

1900 Addison Street, Floor 3, Berkeley, CA 94704

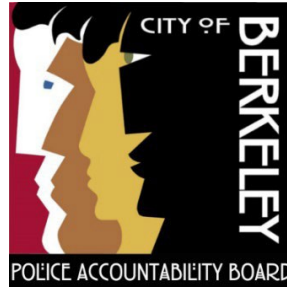
TEL: 510-981-4950 TDD: 510-981-6903 FAX: 510-981-4955

Website: <https://berkeleyca.gov/dpa>

Email: dpa@berkeleyca.gov

Item 4

Minutes for the Regular Meeting of October 7, 2026



**POLICE ACCOUNTABILITY BOARD
REGULAR MEETING MINUTES
WEDNESDAY, OCTOBER 7, 2026
6:30 P.M.**

Board Members

Joshua Cayetano (Chair)	Leah Wilson (Vice-Chair)
Joshua Buswell-Charkow	Stephanie Allan
Patrick DeTemple	Jasmina Viteskic
Anay Sharma	Dwayne Phillips (Alternate)

MEETING LOCATION

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

MEETING MINUTES

1. CALL TO ORDER AND ROLL CALL AT 6:34 PM

Present:	Board Member Joshua Cayetano (Chair)
	Board Member Stephanie Allan
	Board Member Patrick DeTemple
	Board Member Joshua Buswell-Charkow
	Board Member Anay Sharma
	Board Member Jasmina Viteskic
Absent:	Board Member Leah Wilson (Vice Chair) ¹
ODPA Staff:	Mary Opler, Director of Police Accountability
	Kathy Lee, Transition Support
	Jose Murillo, Policy Analyst
	Syed Mehdi, Data Analyst
	Daniel Weinberg, Investigator
BPD Staff:	Chief Jennifer Louis
	Lt. Jesse Grant

¹ Board Member Wilson (Vice Chair) was granted a leave of absence for the October 7, 2026 PAB Meeting.

2. APPROVAL OF AGENDA

Motion to approve the agenda.

Moved/Second (Buswell-Charkow/Viteskic) Motion carried.

Ayes: Cayetano, Wilson, Allan, Buswell-Charkow, DeTemple and Sharma.

Noes: None. Abstain: None. Absent: Wilson.

3. PUBLIC COMMENT

1 Physically Present Speaker

5 Virtually Present Speakers

4. APPROVAL OF MINUTES

- a. Minutes for the Regular Meeting of September 23, 2026.

Motion to approve the minutes for the Regular Meeting of September 23, 2026.

Moved/Second (Buswell-Charkow/DeTemple) Motion carried.

Ayes: Viteskic, Allan, Buswell-Charkow, DeTemple and Sharma.

Noes: None. Abstain: Cayetano. Absent: Wilson.

5. ODPA STAFF REPORT

Transition Support, Kathy Lee introduced Mary Opler, the new Director of Police Accountability. Director Opler described her background in civilian oversight, criminal trial work and emergency management, thanked the Board and staff, and said she would contact Board members individually. Kathy Lee reported on her participation in scoring public safety technology RFP proposals, with further discussion under Item 9.d. She also reported that City Council had voted on September 29 not to lift the tear gas ban.

6. CHAIR AND BOARD MEMBERS' REPORTS

The Chair and Board Members reported on their activities since the last PAB meeting on September 23, 2026.

7. CHIEF OF POLICE'S REPORT

Chief Jennifer Louis reported on traffic safety operations, BPD's assistance to Oakland Police Department in a possible double homicide investigation on Panoramic Way, and community outreach. She announced Coffee with a Cop for October 21, from 11 a.m. to 1 p.m. She also provided updates on air support and vehicle pursuit policies, surveillance technology reporting, and revised acquisition and use documents. The Board discussed audit improvements, independent verification, and the staff time, costs, and access requirements associated with external audits.

8. SUBCOMMITTEE REPORTS

Subcommittees provided updates on their activities since the PAB's last meeting on September 23, 2026. Board Member Allan was reassigned from Outreach and

Engagement to Metrics and Operations, and Chair Cayetano joined the Outreach and Engagement subcommittee.

9. DISCUSSION AND ACTION ITEMS

- a. Action on Commendation of Interim Director Kathy Lee for Public Service to Berkeley (Cayetano)

Motion to approve the resolution commending Interim Director Kathy Lee for her public service to Berkeley, as amended to include Vice Chair Wilson's proposed whereas clause.

Moved/Second (Cayetano/Buswell-Charkow) Motion carried.

Ayes: Viteskic, Wilson, Buswell-Charkow, DeTemple, Allan and Sharma.

Noes: None. Abstain: None. Absent: Wilson.

- b. Berkeley Police Department's Flock Automated License Plate Reader Audits for January 2026 – June 2026 (Continued from September 23, 2026)

- i. Discussion and Action on Independent Auditor of Surveillance Technology Proposal (Allan)

Motion to recommend an independent audit of surveillance technology by the City Auditor's Office or an external vendor, covering the year following completion of the RFP vendor selection process, and to ask City Council to explore fiscally responsible funding through vendor contracts or another mechanism.

Moved/Second (Allan/Cayetano) Motion failed.

Ayes: Cayetano and Allan.

Noes: Buswell-Charkow, DeTemple, Viteskic and Sharma. Abstain: None. Absent: Wilson.

- ii. Discussion and Action on BPD ALPR Audit Report for January 2026 (Cayetano)

Motion to (1) request BPD's written response to the Secure Justice letter, provided to PAB by November 2, 2026; (2) establish a subcommittee of PAB members, with participation from BPD and the City Auditor's, City Manager's and City Attorney's offices, to develop audit parameters and discuss changes to the audit process; and (3) request the City Attorney's assessment of whether current surveillance technology practices comply with Fourth Amendment case law in light of recent developments.

Moved/Second (Cayetano/Allan) Motion carried.

Ayes: Viteskic, Wilson, Buswell-Charkow, DeTemple, Allan and Sharma.

Noes: None. Abstain: None. Absent: Wilson.

- c. Update on the Status of BPD Policy 300 "Use of Force" (Continued from September 23, 2026) (Cayetano)

Chair Cayetano reported that the Board's request for records related to BPD Policy 300 "Use of Force" remained outstanding. The Board took no action on this item.

- d. Update on Evaluation of Responses to Request for Proposals for Public Safety

Technology (Wilson)

Katherine Lee summarized the public safety technology RFP evaluation, with the presentation of a vendor contract expected before City Council in November. Chair Cayetano proposed a group to review community video streams and additional UAS policy revisions within the next two meetings. Interested members were asked to contact the Chair and Director Opler.

- e. Recommendations for Issuing PAB Commendations to Berkeley Police Department Officers Based on Commendations Received Between April and July 2026 (Buswell-Charkow)

Motion to approve the recommended PAB commendations, with Arlo Malmberg's recognition outside the Charter Section L commendation process for sworn officers.

Moved/Second (Sharma/Viteskic) Motion carried.

Ayes: Buswell-Charkow, DeTemple, Sharma, Viteskic, Cayetano and Allan.

Noes: None. Abstain: None. Absent: Wilson.

10. PUBLIC COMMENT

0 Physically Present Speakers

1 Virtually Present Speaker

11. CLOSED SESSION

CLOSED SESSION ITEMS

Pursuant to the Court's order in *Berkeley Police Association v. City of Berkeley, et al.*, Alameda County Superior Court Case No. 2002-057569, the Board will recess into closed session to discuss and act on the following matter(s):

- a. Conference With Labor Negotiators; Government Code § 54957.6 Designated representatives: Leah Wilson, Designated PAB Representative; Katherine Lee, Interim Director of Police Accountability Employee organization: Berkeley Police Association

No action taken.

- b. Case Updates and Recommendations Regarding Complaints Received by the ODPa:

2026-CI-0005

Motion to accept staff's recommendations for Allegations 1-8 in ODPa Complaint 2026-CI-0005

Moved/Second (Allan/Sharma) Motion carried.

Ayes: Viteskic, Cayetano, Allan, DeTemple, Buswell-Charkow and Sharma.

Noes: None. Abstain: None. Absent: Wilson.

Motion to modify staff's recommendations for Officer 1 and accept staff's recommendations for Officer 2 for Allegation 9 in ODPa Complaint 2026-CI-0005

Moved/Second (Cayetano/Buswell-Charkow) Motion carried.

Ayes: Viteskic, Cayetano, Buswell-Charkow and Sharma.

Noes: Allan and DeTemple. Abstain: None. Absent: Wilson.

Motion to accept staff's recommendations for Officer 1 and modify staff's recommendations for Officer 2 for Allegation 10 in ODPa Complaint 2026-CI-0005

Moved/Second (Viteskic/Cayetano) Motion carried.

Ayes: Viteskic, Cayetano, Buswell-Charkow, Allan, DeTemple and Sharma.

Noes: None. Abstain: None. Absent: Wilson.

Motion to accept staff's recommendations for Officers 1 and 2 for Allegation 11 in ODPa Complaint 2026-CI-0005.

Moved/Second (Viteskic/Sharma) Motion carried.

Ayes: Viteskic, Cayetano, Allan, DeTemple and Sharma.

Noes: Buswell-Charkow. Abstain: None. Absent: Wilson.

Motion to modify staff's recommendations for Officer 3 for Allegation 11 in ODPa Complaint 2026-CI-0005.

Moved/Second (Sharma/Viteskic) Motion carried.
Ayes: Viteskic, Cayetano, Allan, DeTemple, Buswell-Charkow and Sharma.
Noes: Cayetano. Abstain: None. Absent: Wilson.

Motion to accept staff's recommendations for Allegation 12 in ODPa Complaint 2026-CI-0005.

Moved/Second (Cayetano/Sharma) Motion carried.
Ayes: Buswell-Charkow, Viteskic, Cayetano, Allan, DeTemple and Sharma.
Noes: None. Abstain: None. Absent: Wilson.

Motion to modify staff's recommendations for Officer 2 for Allegation 11 in ODPa Complaint 2026-CI-0005, overruling the previous motion on this allegation.

Moved/Second (Allan/DeTemple) Motion carried.
Ayes: Viteskic, Cayetano, Allan and DeTemple.
Noes: None. Abstain: Buswell-Charkow and Sharma. Absent: Wilson

Motion to modify staff's recommendations for Allegation 13 in ODPa Complaint 2026-CI-0005.

Moved/Second (Sharma/Cayetano) Motion carried.
Ayes: Viteskic, Cayetano, Buswell-Charkow, Sharma and DeTemple.
Noes: None. Abstain: Allan. Absent: Wilson

Motion to modify recommended disciplinary actions for ODPa Complaint 2026-CI-0005.

Moved/Second (Viteskic/Sharma) Motion carried.
Ayes: Viteskic, Cayetano, Buswell-Charkow, Sharma, Allan and DeTemple.
Noes: None. Abstain: None. Absent: Wilson

2026-CI-0007

Motion to accept staff's recommendations for ODPa Complaint 2026-CI-0007.

Moved/Second (Allan/Sharma) Motion carried.
Ayes: Cayetano, Buswell-Charkow, Sharma, Viteskic, Allan and DeTemple.
Noes: None. Abstain: None. Absent: Wilson.

2026-CI-0011

Motion to accept the staff's recommendations in ODPa Complaint 2026-CI-0011 with two modifications.

Moved/Second (DeTemple/Sharma) Motion carried.
Ayes: Viteskic, DeTemple, Buswell-Charkow and Sharma.
Noes: None. Abstain: Cayetano and Allan. Absent: Wilson.

2024-CI-0004

Motion to administratively close ODPa Complaint 2024-CI-0004.

Moved/Second (Cayetano/Viteskic) Motion carried.
Ayes: Viteskic, Wilson, Allan, DeTemple, Cayetano, Buswell-Charkow and Sharma.
Noes: None. Abstain: None. Absent: Wilson.

END OF CLOSED SESSION

12.ANNOUNCEMENT OF CLOSED SESSION ACTIONS

Chair Cayetano announced the closed session actions.

13.ADJOURNMENT AT 10:34 PM

Motion to adjourn. Moved/Second (Sharma/Viteskic). The meeting was adjourned at 10:34 PM by unanimous consent.

Item 8
Subcommittee List

Updated on 10/16/2026



SUBCOMMITTEE LIST

Important Note: As of October 14, 2026, the PAB has 7 of its 9 seats filled, resulting in a quorum of 4 members. Subcommittees must be composed of fewer than a quorum and may not consist of a single member. Accordingly, vacancies must be filled or the subcommittee must be disbanded. If disbanded, its work can be reassigned to individual board members or formally paused or discontinued. For additional information on subcommittee requirements, please visit Chapter II Section 5 of the City of Berkeley's Commissioner's Manual:

<https://berkeleyca.gov/sites/default/files/documents/Commissioners%27%20%26%20Board%20Members%27%20Manual%202025%20Edition.pdf#Page=30>

Subcommittee	Board Members	Chair	BPD Reps
Policy Reviews Formed 11-08-2023 Scope Expanded 12-11-2024 to include BWC Policy Review Scope Expanded 09-09-2026 to include EIS Update Process	Cayetano DeTemple	N/A	Deputy Chief Tate
Metrics & Operations Formed 02-05-2025 after the Budget & Metrics and Operations & Processes Subcommittees were consolidated into one	Wilson Allan	N/A	N/A
Outreach & Engagement Formed 11-08-2023 Scope Expanded 03-02-2024 Formerly "Commendations"	Cayetano Buswell-Charkow	N/A	N/A

Updated on 10/16/2026

Policies and Practices on Encampment Clearances Formed 6-25-2025	Wilson Sharma	TBD	TBD
--	------------------	-----	-----

LIAISON LIST

Liaison Name	Assignment
Cayetano	Represent the PAB in the BPD UOF Policy Update Process
Wilson	Represent the PAB in the Regulations Negotiation Process
Wilson	Tier 1 Evaluator for Public Safety Technology Proposals
DeTemple	Tier 1 Evaluator for Public Safety Technology Proposals
Sharma	Tier 2 Evaluator for Public Safety Technology Proposals

POLICY COMPLAINTS ASSIGNED TO BOARD MEMBERS

Policy Review #	Assigned Board Member(s)	Description
2025-PR-0001	Cayetano Sharma	BPD Policy 1004 "Anti-Retaliation" & BPD Policy 1010 "Personnel Complaints"

Item 9.a.i

**Preliminary Review and Recommendation of Policy
Complaint 2026-PR-0002**



MEMORANDUM

Date: October 13, 2026
To: Honorable Members of the Police Accountability Board (PAB)
From: Mary Opler, Director of Police Accountability
Jose Murillo, ODPa Policy Analyst
Subject: Preliminary Review and Recommendation of Policy Complaint 2026-PR-0002

This memorandum provides a preliminary review of Policy Complaint Number 2026-PR-0002 and a recommendation for the PAB's consideration.

Policy Complaint Review Process:

Under Appendix C of the PAB Policy Manual (pp. 23–24),¹ the PAB may initiate a review of a Berkeley Police Department policy, practice, or procedure in response to a submitted policy complaint. Initiating a review requires a majority vote of the Board. If the Board votes to proceed, the Policy Committee recommends how the review should be assigned, considering its scope, available capacity, timeline, and potential impact. Assignment options include a Board member, the Policy Committee, an ad hoc subcommittee, or Office of the Director of Police Accountability (ODPA); the Committee may also recommend against review. The PAB then takes formal action on the Committee's recommendation.

Policy Complaint Background:

On September 22, 2026, the ODPa received Policy Complaint 2026-PR-0002 via its online filing portal. The complaint was submitted anonymously, without a name or contact information for staff to follow up. The provided statement, included in Attachment 1, criticizes BPD's reported release of a man who allegedly followed a woman and climbed a gate while carrying what the complainant described as a weapon. The complainant questions the adequacy and consistency of the police response and suggests officers would have responded differently had their own family member been involved.

¹ Police Accountability Board Policy Manual, Appendix C: <https://berkeleyca.gov/sites/default/files/2026-07/PABPolicyManual-FINAL%20%281%29.pdf>

ODPA staff presumes that the complainant was referring to the incident reported by ABC7 in which a man allegedly chased a UC Berkeley student into her apartment complex on September 15, 2026, climbed a locked gate, and pulled out an object police identified as a barbecue lighter.² According to the report, BPD detained and released the man the following day. In a statement provided by BPD and cited in the article, the department explained that officers could not make a warrantless arrest based solely on a misdemeanor trespass committed outside their presence.³ The article also reports that the man was subsequently arrested on September 19 on an unrelated felony warrant, while prosecutors continued reviewing the student's case.

The complaint did not provide any additional information beyond their short statement.

Recommendation:

ODPA does not recommend referring this complaint to the Policy Review Subcommittee for further consideration. At this stage, ODPA anticipates that a policy review of this incident would have limited community impact and does not warrant prioritization given the PAB's current priorities and available resources. The concern also involves state-law limitations on warrantless arrests for misdemeanor trespass committed outside an officer's presence, which BPD cited as the reason officers could not make an arrest under the circumstances.

Attachment:

Policy Complaint Number 2026-PR-0002

² Quigley, Dryden. "VIDEO: Man Scales Locked Gate After Chasing UC Berkeley Student Home." ABC7, September 23, 2026. <https://abc7.com/post/video-man-scales-locked-gate-chasing-uc-berkeley-student-home/19856045/>

³ Berkeley Police Department's September 22, 2026 Statement (See video description): <https://youtu.be/VFjU5Hu3p-E?si=82bUyBoFtfhsHvF4>

Policy/Practice/Procedure Form



Tracking Number **ODPA-260922-497446**

Created by - | 09/22/2026 | Version 1

Case Details (Version 1)

Personal Information

Basic Information

Email

First Name

Last Name

Phone

File Anonymously ☒ Yes

Work Telephone

Mailing Address

Street name

Apt/Unit

State

City

Zip Code

Occupation

Demographics

Please provide as many details about the incident as possible. Your recollection about the incident is invaluable.

Date of Birth

Ethnicity

Race

Gender

Incident Details

Statement

I just saw in TikTok ABC News' report regarding your police department letting a male individual who climbed a gate with a weapon while following a woman go free. You guys are irresponsible. I'm almost certain you guys have arrested people for less. That could've been my sister as I think about her college years there. It's sad. I'm sure if that happened to someone related to you all that you would have had a different interaction. Do better.

Location of Incident (if applicable)

Date of Incident (if applicable)

Time of Incident (if applicable)

What changes to BPD policy, practice, or procedure do you propose?

Additional Information

Use this space for any additional information you wish to provide about your complaint. (Or, attach relevant documentation you believe will be useful to the Police Accountability Board in evaluating your complaint.)

Upload Document

Incident External Links

How Did You Hear About Us

Policy/Practice/Procedure Form



Tracking Number **ODPA-260922-497446**

Created by - | 09/22/2026 | Version 1

Attachments

No attachments available for this case.

Item 9.a.ii

Preliminary Review and Recommendation of Policy
Complaint 2026-PR-0003



MEMORANDUM

Date: October 13, 2026
To: Honorable Members of the Police Accountability Board
From: Mary Opler, Director of Police Accountability
Jose Murillo, ODPa Policy Analyst
Subject: Preliminary Review and Recommendation of Policy Complaint 2026-PR-0003

This memorandum provides a preliminary review of Policy Complaint Number 2026-PR-0003 and a recommendation for the PAB's consideration.

Policy Complaint Review Process:

Under Appendix C of the PAB Policy Manual (pp. 23–24),¹ the PAB may initiate a review of a Berkeley Police Department policy, practice, or procedure in response to a submitted policy complaint. Initiating a review requires a majority vote of the Board. If the Board votes to proceed, the Policy Committee recommends how the review should be assigned, considering its scope, available capacity, timeline, and potential impact. Assignment options include a Board member, the Policy Committee, an ad hoc subcommittee, or ODPa; the Committee may also recommend against review. The PAB then takes formal action on the Committee's recommendation.

Policy Complaint Background:

On September 29, 2026, the ODPa received Policy Complaint 2026-PR-0003 via its online filing portal. The complaint was submitted anonymously, without a name or contact information for staff to follow up. The provided statement, included in Attachment 1, describes an incident on August 12, 2026, in which a parking enforcement officer allegedly sprayed a cleaning substance onto a parking meter near 1048 University Avenue, causing mist to contact the complainant's face and be inhaled as they walked past. The complainant proposes applying cleaning substances directly to a towel when

¹ Police Accountability Board Policy Manual, Appendix C: <https://berkeleyca.gov/sites/default/files/2026-07/PABPolicyManual-FINAL%20%281%29.pdf>

members of the public are nearby and requests clarification on whether existing policy already requires this practice.

Recommendation:

ODPA does not recommend referring this complaint to the Policy Review Subcommittee for further consideration. At this stage, ODPA anticipates that a policy review of this incident would have limited community impact and does not warrant prioritization given the PAB's current priorities and available resources. The available information describes a single incident involving parking meter cleaning and does not indicate a recurring practice or broader policy concern requiring Board review.

Attachment:

Policy Complaint Number 2026-PR-0003

Policy/Practice/Procedure Form



Tracking Number **ODPA-260929-626156**

Created by - | 09/29/2026 | Version 1

Case Details (Version 1)

Personal Information

Basic Information

Email

First Name

Last Name

Phone

File Anonymously ☒ Yes

Work Telephone

Mailing Address

Street name

Apt/Unit

State

City

Zip Code

Occupation

Demographics

Please provide as many details about the incident as possible. Your recollection about the incident is invaluable.

Date of Birth

Ethnicity

Race

Gender

Incident Details

Statement

On 8/12/26 approx. 11:10-11:15am next to the PETS referral parking lot, a PEO was cleaning the parking meter by spraying it with a spray bottle. The mist from the bottle dissipated through the air surrounding the sidewalk causing it to hit my face as i walked by. First of all, I breathed and walked into unknown chemical substances sprayed inconsiderately by a public servant that landed on my facial skin.

Location of Incident (if applicable) next to the PETS referral parking lot near 1048 university ave

Date of Incident (if applicable) August 12, 2026

Time of Incident (if applicable) 11:10 AM

What changes to BPD policy, practice, or procedure do you propose? I propose not openly spraying chemicals when members of the public are nearby. if anyone is nearby, i suggest spraying into the towel then wiping the parking meter. Instead of covering the parking meter in a chemical mist that can catch the wind and get on people's skin and in their lungs. If this is already policy, please let me know so i can submit a complaint instead.

Additional Information

Use this space for any additional information you wish to provide about your complaint. (Or, attach relevant documentation you believe will be useful to the Police Accountability Board in evaluating your complaint.)

Upload Document

Incident External Links

How Did You Hear About Us

Policy/Practice/Procedure Form



Tracking Number **ODPA-260929-626156**

Created by - | 09/29/2026 | Version 1

Attachments

No attachments available for this case.

Item 9.a.iii

Preliminary Review and Recommendation of Policy
Complaint 2026-PR-0004



MEMORANDUM

Date: October 14, 2026
To: Honorable Members of the Police Accountability Board
From: Mary Opler, Director of Police Accountability
Jose Murillo, ODPa Policy Analyst
Subject: Preliminary Review and Recommendation of Policy Complaint 2026-PR-0004

This memorandum provides a preliminary review of Policy Complaint Number 2026-PR-0004 and a recommendation for the PAB's consideration.

Policy Complaint Review Process:

Under Appendix C of the PAB Policy Manual (pp. 23–24),¹ the PAB may initiate a review of a Berkeley Police Department policy, practice, or procedure in response to a submitted policy complaint. Initiating a review requires a majority vote of the Board. If the Board votes to proceed, the Policy Committee recommends how the review should be assigned, considering its scope, available capacity, timeline, and potential impact. Assignment options include a Board member, the Policy Committee, an ad hoc subcommittee, or ODPa; the Committee may also recommend against review. The PAB then takes formal action on the Committee's recommendation.

Policy Complaint Background:

On September 30, 2026, the ODPa received Policy Complaint 2026-PR-0004 via its online filing portal. The completed form is included as Attachment 1. The complaint concerns BPD's emergency response and traffic control practices following a collision at Ashby Avenue and Fulton Street on September 21, 2026.

The complainant reported arriving at the Fulton Street entrance to Sylvia Mendez Elementary School at approximately 8:00 a.m. and observing two police vehicles traveling south on Fulton Street with emergency lights and sirens activated. According to the complainant, both vehicles maneuvered around cars queued for the school's rolling drop-

¹ Police Accountability Board Policy Manual, Appendix C: <https://berkeleyca.gov/sites/default/files/2026-07/PABPolicyManual-FINAL%20%281%29.pdf>

off program and entered an intersection staffed by a crossing guard, with families in the crosswalks. The vehicles also passed families bicycling along the Russell and Fulton bicycle boulevards and arriving at the school's Fulton Street entrance. The complainant described the experience as frightening and expressed concern about the risk to children and families, although no injuries involving the emergency vehicles were reported. The complainant also raised concerns about the potential disruption to learning and emotional impact on students when emergency vehicles use streets adjacent to schools. The complainant noted that a responding fire truck accessed the collision via Ashby Avenue, using either Shattuck Avenue or Adeline Street, which the complainant described as what she believed to be the appropriate approach.

At approximately 8:30 a.m., the complainant went to Ashby Avenue and Fulton Street to observe the collision response. The complainant reported that eastbound traffic on Ashby Avenue was blocked at Fulton Street and that diverted drivers were turning south onto Fulton Street through both red and green lights without regard for pedestrians and bicyclists, including pedestrians in the crosswalk. Although two police vehicles remained at the scene, the complainant observed no officers directing traffic and expressed concern about the safety of vehicles diverted onto nearby residential streets.

The complainant proposed that BPD avoid using streets adjacent to schools as emergency response routes when possible, particularly during drop-off and pickup times and preferably throughout the school day, and instead use major streets such as Shattuck Avenue or Adeline Street. The complainant also requested active traffic control at intersections affected by collisions or closures, including directing diverted vehicles, enforcing traffic signals, and ensuring that drivers yield to pedestrians and bicyclists.

Relevant Policies:

BPD Policies 309, "Officer Response to Calls,"² and 501, "Motor Vehicle Collision Investigations,"³ establish safety responsibilities relevant to the complaint. Sections 309.2 and 309.3 require officers responding to emergencies to drive with due regard for public safety and reduce speed at intersections, while Section 309.5 requires supervisory monitoring that considers traffic and roadway conditions. These requirements apply to conditions such as the crowded school drop-off area described by the complainant. Sections 501.7 and 501.5(a)(4) address assessing traffic-control needs at collision scenes and responding to non-injury collisions when vehicles or debris create traffic

²Berkeley Police Department Policy 309 "Officer Response to Calls":
https://berkeleyca.gov/sites/default/files/RELEASE_20260721_T173558_Berkeley%20PD%20Policy%20Manual.pdf#page=123

³Berkeley Police Department Policy 501 "Motor Vehicle Collision":
https://berkeleyca.gov/sites/default/files/RELEASE_20260721_T173558_Berkeley%20PD%20Policy%20Manual.pdf#page=512

hazards. However, the reviewed provisions do not specifically require officers to *avoid* school streets during drop-off or pickup or provide officer-directed traffic control at every intersection affected by a closure.

Recommendation:

If the PAB wishes to pursue the issues raised in Policy Complaint 2026-PR-0004, ODPa recommends referring the complaint to the Policy Review Subcommittee for further research and a determination of whether to accept it for policy review. The review could center on whether BPD should adopt specific guidance for selecting emergency-response routes near schools, including avoiding school streets during drop-off and pickup when reasonably feasible while preserving timely responses to emergencies. The Subcommittee could also consider whether existing traffic-control procedures sufficiently address pedestrian and bicyclist safety when collisions or road closures divert traffic near schools.

Attachment:

1. Policy Complaint No. 2026-PR-0004



Policy/Practice/Procedure Form

Tracking Number **ODPA-260930-309224**

Created by - | 09/30/2026 | Version 1

Case Details (Version 1)

Personal Information

Basic Information

Email	[REDACTED]
First Name	[REDACTED]
Last Name	[REDACTED]
Phone	
File Anonymously	
Work Telephone	

Mailing Address

Street name	
Apt/Unit	
State	California
City	Berkeley
Zip Code	94704

Occupation

Demographics

Please provide as many details about the incident as possible. Your recollection about the incident is invaluable.

Date of Birth

Ethnicity

Race

Gender

Incident Details

Statement

On Monday, September 21, 2026 there was a car crash on Ashby and Fulton around 8am. I arrived to the Sylvia Mendez Elementary entrance gate on Fulton just in time to see a police car heading south on Fulton with lights and siren blaring. It was quickly followed by a second, both of which needed to go around the many cars queued up on Fulton for our Rolling Drop Off and enter an intersection staffed by our crossing guard and with families in the crosswalks. Then they had to pass the many families that bike on the Russell and Fulton Bike Boulevards and drop off at the Fulton entrance gate. It was a terrifying start to the school day and we are so fortunate that no one was injured by emergency vehicles speeding by our school during Drop Off time.

My first issue is local streets by schools should NOT be used as cut through for emergency responses - ESPECIALLY during drop off/pickup times but frankly anytime during the school day as it's disruptive to learning and can be emotionally disturbing to students. The fire truck that responded to this car crash correctly accessed the scene by using either Shattuck or Adeline to access the crash via Ashby.

Around 8:30am I headed down to Fulton and Ashby to observe the incident. Eastbound car traffic was blocked at Fulton so the drivers were rolling through the light (red and green) without regard to pedestrians and people on bikes to turn south onto Fulton. There was no one directing traffic and likely no one ensuring that all these cars heading off Ashby and onto local streets were driving safe. Two police vehicles were still at the scene.

So my second issue is that cars were then rolling through red lights with pedestrians in the crosswalk due to the lack of police enforcement and instructions at a closed intersection.

Location of Incident (if applicable) Ashby and Fulton

Date of Incident (if applicable) September 21, 2026

Time of Incident (if applicable) 08:30 AM

What changes to BPD policy, practice, or procedure do you propose? The community member wants two main changes:

- Emergency response routes that avoid school streets, especially during drop-off and pickup, and preferably throughout the school day. They suggest using major streets such as Shattuck or Adeline to reach incidents when possible.
- Active traffic control at intersections affected by collisions or closures, including officers directing diverted vehicles, enforcing traffic signals, and ensuring drivers yield to pedestrians and bicyclists.

Their broader concern is protecting children and families from both emergency vehicle traffic and unsafe driving caused by traffic diversions.

Additional Information

Use this space for any additional information you wish to provide

about your complaint. (Or, attach relevant documentation you believe will be useful to the Police Accountability Board in evaluating your complaint.)

Upload Document

Incident External Links

How Did You Hear About Us

Website

Policy/Practice/Procedure Form



Tracking Number **ODPA-260930-309224**

Created by - | 09/30/2026 | Version 1

Attachments

No attachments available for this case.

Item 9.b.

**October 16, 2026 Memorandum from the ODPA to the
PAB Titled “Review of BPD Surveillance Technology
Proposals and Policy Revisions”**



MEMORANDUM

Date: October 16, 2026

To: Honorable Members of the Police Accountability Board (PAB)

From: Mary Opler, Director of Police Accountability
Jose Murillo, ODPa Policy Analyst

Subject: Review of BPD Surveillance Technology Proposals and Policy Revisions

The purpose of this memorandum is to provide the PAB an overview of the proposed revisions to BPD’s external fixed video surveillance cameras, Automated License Plate Readers, Unmanned Aerial Systems (UAS—commonly referred to as drones), community video stream, and investigative software policies and associated acquisition reports. It highlights changes and identifies issues that may warrant clarification, further review, or recommendations from the Board.

Background:

On March 24, 2026, the City Council considered Item 26, “Public Safety Technology: Surveillance Technology Ordinance and Police Equipment Ordinance Approvals, Policy Updates, and Contract Authority.” The item proposed approvals for BPD’s surveillance technology package and amendments to its Flock Safety contract covering drones, fixed cameras, investigative software, and ALPR renewal. Following public comment, Council continued the item without approving the package. Although initially continued to June 2, the matter returned at a special meeting on May 7.¹

During that interval, the PAB continued reviewing the proposal’s procurement process and alternatives. In its May 4 memorandum to Council, the Board raised concerns about vendor

¹ March 24, 2026, Berkeley City Council Annotated Agenda, Item 26, pp. 14–15:
<https://berkeleyca.gov/sites/default/files/city-council-meetings/2026-03-24%20Annotated%20Agenda%20-%20Council.pdf#page=14>;

dependence and the proposed contracting approach and recommended a competitive Request for Proposals (RFP) incorporating the City’s technical requirements and policy safeguards.²

On May 7, Council adopted Resolution No. 72,254-N.S., declining to proceed with the full proposed Flock Master Services Agreement and directing the City Manager to initiate an RFP process in consultation with the PAB and BPD. Council authorized a limited, 12-month ALPR contract extension of up to \$200,000 while approving amended UAS surveillance and equipment use policies and the fixed-camera surveillance use policy. Council referred the Community Video Streams materials to the Public Safety Policy Committee and directed additional analysis of UAS needs and alternative vendors.³

The May 7 action incorporated safeguards addressing retention, deployment, and oversight. These included a five-day retention period for non-evidentiary UAS footage, supervisory approval for deployments other than Drone as First Responder, operator decertification procedures, and monthly audits with semiannual reporting for UAS and fixed cameras.⁴ Council also narrowed UAS deployment at mass gatherings to specified circumstances involving violent criminal activity, probable cause of a felony, and an active threat of serious bodily injury.

On June 2, the Public Safety Policy Committee reviewed the Community Video Streams and Investigative Software proposals and requested revisions concerning privacy, live access, data sources, retention, human oversight, and auditing.⁵ On June 30, Council adopted Resolution No. 72,369-N.S., accepting the acquisition reports and approving Surveillance Use Policies 1306 and

² May 4, 2026, PAB Memorandum to Council, “Surveillance Technology Procurement — Process Deficiencies, Vendor Dependence, and Availability of Competitive Alternatives”:

https://berkeleyca.gov/sites/default/files/2026-05/2026-05-04%20PAB%20Memo_Surveillance%20Tech%20Process%20Deficiencies_Final%20%28Signed%29.pdf.

³ May 7, 2026, Berkeley City Council Special Meeting Annotated Agenda, Item 1a, pp. 3–4:

<https://berkeleyca.gov/sites/default/files/city-council-meetings/2026-05-07%20Annotated%20Agenda%20-%20Council.pdf#page=3>.

⁴ May 7, 2026, Revised Agenda Material Submitted by Mayor Adena Ishii, Item 1a, pp. 2–5:

https://berkeleyca.gov/sites/default/files/2026-05/2026-05-07%20BAC_Flock_Supplemental_Item26_5_07_2026Meeting.pdf#page=2.

⁵ June 2, 2026, Public Safety Policy Committee Special Meeting Minutes, Item 2, p. 3:

<https://berkeleyca.gov/sites/default/files/legislative-body-meeting-minutes/2026-06-02%20Annotated%20Agenda%20Public%20Safety.pdf#page=3>.

1307. These approvals did not select vendors or authorize contracts; Council retained the ability to require further revisions before granting contract authority. At the same meeting, Council approved issuance of the public safety technology RFP under Item 19.⁶

The city released RFP No. 26-11794-C, “Public Safety Technology,” on July 7, with proposals due August 20. The solicitation covered ALPRs, fixed video surveillance cameras, Drone as First Responder, field-deployed drones, community video stream integration, and investigative software. Vendors could submit proposals for individual components or combinations of technologies, allowing the city to consider multiple vendors. A team consisting of BPD personnel, two PAB members, and the former Interim DPA, evaluated the proposals in September, and Council consideration of contracts is anticipated in November.⁷

The revised policies presented in this memorandum incorporate vendor-neutral language and are intended to address Council’s actions and the requirements of BMC Chapter 2.99,⁸ subject to the PAB’s review.

BPD’s Proposed Changes & ODPa Observations

The table below groups the documents by technology and shows how the policies and supporting materials fit together. Operational policies guide Department personnel, while surveillance use policies address authorized uses, data access, retention, sharing, and oversight. Each technology has an accompanying acquisition report. Because state law classifies UAS as military equipment, the UAS materials also include an impact statement and proposed update to Policy 709.

Technology	Operational Policy	Surveillance Use Policy	Supporting Materials
External Fixed Video Surveillance Cameras	Policy 351, “External Fixed Video Surveillance Cameras”	Policy 1304, “Surveillance Use Policy – External Fixed Video Surveillance Cameras”	Acquisition Report – External Fixed Video Surveillance Cameras
Automated License Plate Readers	Policy 422, “Fixed Automated License Plate Readers (ALPRs)”	Policy 1305, “Surveillance Use Policy – Fixed Automated License Plate Readers (ALPRs)”	Acquisition Report – Automated License Plate Readers (ALPRs)

⁶ June 30, 2026, Berkeley City Council Annotated Agenda, Items 19 and 46, pp. 8 and 19: <https://berkeleyca.gov/sites/default/files/city-council-meetings/2026-06-30%20Annotated%20Agenda%20-%20Council.pdf>.

⁷ City of Berkeley, RFP No. 26-11794-C, “Public Safety Technology,” July 7, 2026, pp. 1–2 and 16: https://berkeleyca.gov/sites/default/files/2026-07/RFP%20-%20Public%20Safety%20Technology_2.pdf.

⁸ Berkeley Municipal Code 2.99: <https://berkeley.municipal.codes/BMC/2.99>

Technology	Operational Policy	Surveillance Use Policy	Supporting Materials
Community Video Stream	Policy 355, "Community Video Streams"	Policy 1306, "Surveillance Use Policy – Community Video Streams"	Acquisition Report – Community Video Streams (CVS)
Unmanned Aerial Systems	Policy 611, "Unmanned Aerial System (UAS) Operations"	Policy 1303, "Surveillance Use Policy – Unmanned Aerial Systems (UAS)"	Acquisition Report – Unmanned Aerial Systems (UAS); Impact Statement and Policy 709 Update –Unmanned Aerial Systems
Investigative Software	No separate operational policy included	Policy 1307, "Surveillance Use Policy – Investigative Software"	Acquisition Report – Investigative Software

The following table summarizes the deadlines for PAB action on each technology under the Surveillance Technology Ordinance (BMC § 2.99.030.2)⁹ and the Police Equipment Ordinance (BMC § 2.100.050(D)(3)).¹⁰

Technology	Date Received	STO Deadline	PEO Deadline
UAS	10/2/2026	11/1/2026	11/16/2026
Community Video Streams and Investigative Software	10/6/2026	11/5/2026	Not Applicable
Fixed ALPRs and External Fixed Video Surveillance Cameras	10/9/2026	11/8/2026	Not Applicable

⁹ BMC § 2.99.030.2: [https://berkeley.municipal.codes/BMC/2.99.030\(2\)](https://berkeley.municipal.codes/BMC/2.99.030(2))

¹⁰ BMC § 2.100.050(D)(3): <https://berkeley.municipal.codes/BMC/2.100.050>

Fixed Video Surveillance Cameras

The proposed revisions to Policies 351 and 1304 introduce substantive changes to retention requirements, access documentation, and oversight. The policy redlines incorporate feedback from the City Attorney's Office and discussions with the City Council.

The acquisition reports retain verbatim language from previously approved versions wherever possible. They have been reformatted to align with recent acquisition reports and updated to reflect developments since the earlier versions were prepared. These updates include removing vendor-specific references and replacing outdated case examples with current research and experiences from other jurisdictions.

Notably, the redlines replace specific preservation requirements for recordings involving uses of force, detentions, arrests, and misconduct complaints with broader evidentiary retention language. They also establish monthly audits and semiannual reporting to the PAB, while revising requirements for access logs and procedures for routing ODPA and PAB requests. The table below summarizes these changes and the relevant provisions of the acquisition reports, followed by any issues for PAB consideration.

Policy 351 External Fixed Video Surveillance Cameras

Policy Section / Page	Proposed Redline	ODPA Comments
351.5 — Retention / pp. 3–4	Removes specific retention requirements for use-of-force, detention, arrest, and officer-complaint recordings, including the two-year-and-one-month minimum. Substitutes retention under applicable state law and Department evidence policies.	ODPA has no comments.
351.5 — Evidence Storage / pp. 3–4	Replaces the requirement to copy and book recordings into evidence with storage in the Department's digital evidence system.	ODPA has no comments.
351.5 — Extensions and Destruction / p. 4	Adds documented retention extensions authorized by the Investigations Division Captain or designee, and documented destruction after retention requirements and legal holds expire. References Evidence.com.	ODPA has no comments.
351.5 — Deployment Authority / p. 4	Adds authority for the City Manager, or delegated Police Chief, to pause or end	ODPA has no comments.

Policy Section / Page	Proposed Redline	ODPA Comments
	deployment, with Council notification within 48 hours.	
351.6 — Accountability Access / pp. 4–5	Changes the referral contact for ODPA and PAB requests to the Support Services Division Captain or the Chief’s designee.	ODPA has no comments.
351.6 — Immigration Enforcement / p. 5	Adds Sanctuary City Ordinance and Immigration Law Policy language prohibiting sharing with federal immigration enforcement officials.	ODPA has no comments.
351.7 — Access Logs / p. 5	Changes specified log categories to information logs “may include,” uses “should” for two-year retention and exportability, and removes the server-storage requirement.	ODPA has no comments.
351.7 — Audits / p. 5	Changes audits from biennial to monthly and adds semiannual publication and delivery of reports to the PAB.	The PAB may wish to consider requesting language clarifying that the Board may request monthly audit results and that those results must be provided upon request.

Policy 1304 External Fixed Video Surveillance Cameras

Policy Section / Page	Proposed Redline	ODPA Comments
1304.3 — Data Collection / p. 2	Removes the requirement that encrypted servers be City servers. Replaces statements about installed recognition hardware with restrictions on its use and removes the description of audio as a standard, deactivated feature.	ODPA has no comments.
1304.5 — Data Protection / p. 2	Removes Public Works’ specified role in controlling data access and documenting system access.	ODPA has no comments.

Policy Section / Page	Proposed Redline	ODPA Comments
1304.6 — Civil Liberties / pp. 2–3	Revises recognition language from hardware installation to use and states that audio may not be activated or used without Council approval.	ODPA has no comments.
1304.7 — Retention / p. 3	Removes specific retention periods and procedures for officer-related incidents and complaints. Adds digital evidence storage, retention under applicable law and Department policies, documented extensions, and destruction procedures referencing Evidence.com.	ODPA has no comments.
1304.9 — Accountability Access / p. 4	Changes the referral contact for ODPA and PAB requests to the Support Services Division Captain or the Chief’s designee.	ODPA has no comments.
1304.9 — Immigration Enforcement and Vendor References / p. 4	Adds Sanctuary City Ordinance and Immigration Law Policy language. Replaces “Flock” with “the vendor” in the federal-agency data-disclosure notification provision.	ODPA has no comments.
1304.11 — Access Logs / p. 5	Changes specified log categories to information logs “may include,” uses “should” for retention and exportability, and removes the server-storage requirement.	ODPA has no comments.
1304.11 — Audits / p. 5	Changes audits from biennial to monthly and adds semiannual publication and delivery of reports to the PAB.	The PAB may wish to consider requesting language clarifying that the Board may request monthly audit results and that those results must be provided upon request.

Automated License Plate Readers

The proposed redlines to Policies 422 and 1305 are concentrated primarily on accountability and oversight, including the reassignment of responsibilities to OSPA, monthly auditing, semiannual reporting to the PAB, and references to the City’s Sanctuary City Ordinance. As is the case with the external fixed cameras, the redlines in the policies respond to comments from the City Attorney’s Office and Council discussions. The table below summarizes the revisions and relevant acquisition report provisions, followed by questions requiring clarification.

Policy 422 ALPRs

Policy Section / Page	Proposed Redline	ODPA Comments
422.7 — Accountability / p. 6	Transfers audit responsibility from the Professional Standards Bureau’s Audit and Inspections Sergeant to the Office of Strategic Planning and Accountability (OSPA).	ODPA has no comments.
422.8 — Browsing Audits / p. 6	Assigns browsing audits to OSPA or the Chief’s designee. Adds monthly audits and semiannual publication and delivery of reports to the PAB; existing biennial language remains.	ODPA has no comments.
422.8 — Audit Records / p. 7	Assigns retention of audit documentation to OSPA and revises the reporting reference to the Annual Surveillance Ordinance Report.	ODPA has no comments.
422.9 — Releasing Data / p. 7	Routes signed data-sharing acknowledgment letters to OSPA for compliance and reporting.	ODPA has no comments.
Immigration Enforcement Provision / p. 7	Adds the City’s Sanctuary City Ordinance to the existing immigration-enforcement sharing restriction.	ODPA has no comments.

Policy 1305 ALPRs

Policy Section / Page	Proposed Redline	ODPA Comments
1305.6 — Data Protection / p. 6	Assigns audits to OSPA and changes “biennial” to “twice a year.”	ODPA has no comments.
1305.10 — Third-Party Data Sharing / p. 7	Routes signed acknowledgment letters to OSPA and added the Sanctuary City Ordinance to the immigration-enforcement sharing restriction.	ODPA has no comments.
1305.12 — Audit Responsibility / p. 7	Transfers audit responsibility to OSPA and deletes the requirement to share audit results with ODPA upon completion and replaces it with a requirement for semiannual public reports that will also be provided to the PAB. ALPR data or images that are utilized for an investigation that becomes evidence in a case will be made available to the ODPA as it relates to a specific complaint of misconduct	ODPA has no comments.
1305.12 — Audit Frequency and Reporting / p. 8	Adds monthly audits and semiannual publication and delivery of reports to the PAB. Earlier twice-yearly/biannual audit language remains elsewhere in the policy.	The PAB may wish to consider requesting language clarifying that the Board may request monthly audit results and that those results must be provided upon request.

Community Video Streams

The Community Video Streams materials address conditions for integrating privately owned cameras into BPD’s system, accessing live footage, and protecting privacy. Although the proposal returns to the PAB following Council action, the supplied versions of Policies 355 and 1306 do not display tracked changes following City Council’s June 30, 2026, approval.

Unmanned Aerial Systems

On May 7, 2026, Council approved Policies 1303 and 611 and referred the Acquisition Report and Impact Statement back to the City Manager. The redlines identify all changes made since the versions considered on May 7. These revisions implement Council’s direction and ensure the documents are vendor-neutral. The language is designed to accommodate the capabilities of the vendors selected by the RFP selection committee, whose identities have not yet been made public.

The proposed revisions to the UAS materials are targeted but substantive, addressing deployment authority, authorized uses, retention, and accountability. They establish supervisory approval requirements, with an exception for Drone as First Responder deployments; narrow certain authorized uses; shorten the specified retention period; and introduce operator decertification provisions and monthly audits. The revised Impact Statement also includes a Berkeley-specific assessment of need and supporting baseline information.

The table below summarizes the revisions across the UAS materials, followed by issues related to deployment safeguards and program evaluation.

Policy 611 Unmanned Aerial System (UAS) Operations

Policy Section / Page	Proposed Redline	ODPA Comments
611.5 — Permitted Use / p. 3	Changes “may” to “shall only” and requires supervisory approval for all deployments except Drone as First Responder (DFR).	ODPA has no comments.
611.5 — Mass Gatherings / p. 3	Limits deployment at mass gatherings or special events to violent criminal activity involving probable cause of a felony and an active threat of serious bodily injury.	ODPA has no comments.
611.7 – Decertification New Provision / p. 4	Allows suspension of pilot or visual-observer certification pending review of violations. Assigns reinstatement, retraining, or permanent decertification decisions to the Chief or designee.	ODPA has no comments.
611.7 - Audits New Provision / p. 4	Adds monthly OSPA audits, twice-yearly publication of reports, and	The “should be” language was carried over verbatim

Policy Section / Page	Proposed Redline	ODPA Comments
	language stating reports should be sent to the PAB.	from the mayor's supplemental, so it was not intended to convey a different standard. ODPA staff recommends that the PAB recommend removing "should be" to standardize the language with the other policies. The PAB may wish to consider requesting language clarifying that the Board may request monthly audit results and that those results must be provided upon request.
611.8 — Retention / p. 4	Reduces the period for purging non-evidentiary footage from 60 days to five days.	ODPA has no comments.

Policy 1303 Surveillance Use Policy – Unmanned Aerial System (UAS)

Policy Section / Page	Proposed Redline	ODPA Comments
1303.2 — Authorized Use / p. 1	Changes "may" to "shall only" and requires supervisory approval for deployments other than DFR.	ODPA has no comments.
1303.2 — Mass Gatherings / p. 2	Limits deployment to violent criminal activity involving probable cause of a felony and an active threat of serious bodily injury.	ODPA has no comments.
1303.8 — Retention / p. 4	Reduces the period for purging non-evidentiary footage from 60 days to five days.	ODPA has no comments.
1303.12 — Audits / p. 5	Changes audits from biennial to monthly, requires twice-yearly	The "should be" language was carried over verbatim from the mayor's supplemental, so it was not

Policy Section / Page	Proposed Redline	ODPA Comments
	publication, and states reports should be sent to the PAB.	intended to convey a different standard. ODPa staff recommends that the PAB recommend removing “should be” to standardize the language with the other policies. The PAB may wish to consider requesting language clarifying that the Board may request monthly audit results and that those results must be provided upon request.
1303.12 — Decertification / p. 5	Adds that policy violations may result in decertification under Policy 611.	ODPA flags the use of “intentional” in the provision addressing disciplinary action. Because intent may need to be established through circumstantial evidence and can be difficult to determine in misconduct investigations, the PAB may wish to consider whether limiting this provision to intentional violations could complicate accountability when misuse is characterized as unintentional, and whether the language should be revised to address violations more broadly.

BMC 2.99 Acquisition Report – Unmanned Aerial System

Policy Section / Page	Proposed Redline	ODPA Comments
1 — Description / pp. 1–2	Reorganizes the equipment description into three deployment categories: interior field-deployed, outdoor field-deployed, and DFR. Adds Brinc and Skydio examples and removes the planned replacement with Flock Alpha within two years.	ODPA has no comments.
1 — Manufacturers’ Descriptions / pp. 2–3	Adds descriptions of Brinc Lemur 2, Skydio R10, Brinc Responder, and Skydio X10.	ODPA has no comments.
5 — Mitigations / p. 5	Specifies that the secure evidence-storage statement applies to video with evidentiary value.	ODPA has no comments.
8 — Cost Assumptions and Funding / p. 6	Adds cost variability based on quantities, purchase or lease terms, contract length, and bundling. Identifies the operating budget as the anticipated funding source and discusses potential overtime savings and discounts.	ODPA has no comments.
8 — Initial Costs / p. 7	Specifies four interior and four outdoor units and adds a \$150,000 figure without clearly deleting or separating the existing \$44,500 figure. Adds ranges of \$100,000–\$200,000 for the first-year DFR lease, \$0–\$150,000 for first-year radar, and \$0–\$15,000 for dock installation.	ODPA has no comments.
8 — Compliance and Personnel Costs / pp. 7–8	Adds discussion of compliance costs and states that compliance and operational personnel costs would be	ODPA has no comments.

Policy Section / Page	Proposed Redline	ODPA Comments
	absorbed within existing staffing costs.	
8 — Ongoing Costs and Upgrades / p. 8	Changes the annual DFR lease estimate to \$100,000–\$200,000. Removes the promised Flock Alpha upgrade and describes hardware upgrades as often included in lease or purchase agreements.	ODPA has no comments.
9 — Third-Party Dependence / pp. 8–9	Limits the statement about uploading all UAS data to Evidence.com to data with evidentiary value.	ODPA has no comments.

BMC 2.100 Impact Statement and Policy 709 Update

Policy Section / Page	Proposed Redline	ODPA Comments
1 — Description / pp. 1–2	Reframes equipment around three deployment categories and adds Brinc and Skydio examples. Removes the planned replacement with Flock Alpha within two years.	ODPA has no comments.
1 — Integration / p. 2	Removes the reference to integration with Flock, retaining integration with the current CAD system.	ODPA has no comments.
1 — Quantity / p. 2	Replaces model-specific quantities with four interior field-deployed units, four outdoor field-deployed units, and two DFR units. Deletes the future Flock Alpha replacement unit.	ODPA has no comments.
1 — Capabilities / p. 3	Replaces model-specific descriptions with descriptions of interior, outdoor, and DFR capabilities.	ODPA has no comments.

Policy Section / Page	Proposed Redline	ODPA Comments
1 — Manufacturers’ Descriptions / p. 4	Adds descriptions of Brinc Lemur 2, Skydio R10, Brinc Responder, and Skydio X10.	ODPA has no comments.
3 — Initial Costs / p. 6	Specifies four interior and four outdoor units and adds \$150,000 without clearly deleting or separating the existing \$44,500 figure. Adds cost ranges for the DFR lease, radar, and dock installation.	ODPA has no comments.
3 — Compliance Costs / p. 6	Adds the Department’s characterization of ordinance-compliance financial risk as minimal, citing a 90-day opportunity to cure issues.	ODPA has no comments.
3 — Ongoing Costs and Upgrades / pp. 6–7	Revises the annual DFR lease estimate to \$100,000–\$200,000 and replaces the Flock Alpha upgrade commitment with broader language about hardware upgrades under lease or purchase agreements.	ODPA has no comments.
6 — Berkeley-Specific Need Assessment / p. 9	Adds a response to Council’s May 7 referral discussing limits of existing aerial-need data, Special Response Team activity, deployment logging, and delays obtaining outside aerial support.	ODPA has no comments.
6 — Baseline Measures / pp. 9–10	Adds 2025 use-of-force totals, response times, and crime-clearance rates, together with the Department’s anticipated DFR benefits.	ODPA has no comments.
6 — Alternatives / p. 10	Adds the Department’s rationale for concluding that existing response	ODPA has no comments.

Policy Section / Page	Proposed Redline	ODPA Comments
	methods and outside aerial support do not meet the identified need.	

Investigative Software

Policy 1307 and its accompanying acquisition report constitute a new proposal requiring review of the full framework for use and oversight. City Council approved Policy 1307 and the Surveillance Acquisition Report on June 30, 2026. The only change from the Council-approved versions is a redline in Policy 1307.4 in response to the mayor’s comments on June 30 regarding item 7 of the Public Safety Policy Committee’s qualified positive recommendation to Council, which asked the Department to further clarify which personnel will be authorized to access the Investigative Software.

Policy 1307 Surveillance Use Policy – Investigative Software

Policy Section / Page	Proposed Redline	ODPA Comments
1307.4 — Data Access / p. 3	Replaces “BPD personnel” with sworn personnel and professional staff whose assignments require investigative or analytical support, expressly including patrol officers conducting initial investigations. Adds approval by the Chief or designee while retaining training and documented investigative-need requirements.	ODPA has no comments.

Conclusion and Recommendation:

The PAB may wish to focus its review on the ALPR, UAS, and fixed-camera policies, which contain the most substantial revisions. Based on ODPA’s review, the policies align with City Council’s actions and have been redlined to reflect feedback from the City Attorney’s Office and Council discussions. After considering the comments outlined in this memo and determining whether it agrees with staff’s recommendations, the PAB could approve the policies as presented or with recommended changes.

Attachment List:

- 1) Policy 351 — External Fixed Video Surveillance Cameras
- 2) Policy 1304 — Surveillance Use Policy—External Fixed Video Surveillance Cameras
- 3) Acquisition Report — External Fixed Video Surveillance Cameras
- 4) Policy 422 — Fixed Automated License Plate Readers (ALPRs)
- 5) Policy 1305 — Surveillance Use Policy—Fixed Automated License Plate Readers (ALPRs)
- 6) Acquisition Report — Automated License Plate Readers (ALPRs)
- 7) Policy 355 — Community Video Streams
- 8) Policy 1306 — Surveillance Use Policy—Community Video Streams
- 9) Acquisition Report — Community Video Streams
- 10) Policy 611 — Unmanned Aerial System (UAS) Operations
- 11) Policy 1303 — Surveillance Use Policy—Unmanned Aerial System (UAS)
- 12) Acquisition Report — Unmanned Aerial System
- 13) Impact Statement and Policy 709 Update — Unmanned Aerial System
- 14) Acquisition Report — Investigative Software
- 15) Policy 1307 — Surveillance Use Policy—Investigative Software

Attachment 1

Policy 351 — External Fixed Video Surveillance Cameras

Attachments to ODPa Memorandum Dated October 16, 2026: “Review of BPD
Surveillance Technology Proposals and Policy Revisions”

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:

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,
- (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 may integrate technologies not otherwise prohibited with the video surveillance system, provided that such use does not conflict with this policy or expand internal or external access beyond what is allowed by policy. For example, integration may occur on a shared access platform where video data and automated license plate reader data are viewable in the same system.

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.

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, unless required by federal law.

Video recordings shall not be disclosed to law enforcement agencies from other states if the purpose of the request is to support the enforcement of laws that restrict or criminalize reproductive rights or rights regarding the provision or receipt of gender-affirming care.

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.

Evidentiary data downloaded for investigations is stored in the Department's digital evidence system.

Length of retention: Evidentiary footage within the Department's possession, custody or control shall be retained for the period prescribed by applicable state law governing criminal evidence and Department evidence policies (currently consistent with the applicable statute of limitations for the underlying offense, plus administrative hold requirements).

Basis: Retention period is based on the evidentiary and legal requirements of the associated criminal investigation or proceeding.

Authorization for extensions: Extensions beyond the standard period may be authorized by the Investigations Division Captain or their designee, and shall be documented in the case record.

Berkeley Police Department
Law Enforcement Services Manual

External Fixed Video Surveillance Cameras

Destruction procedures: Upon expiration of the applicable retention period and confirmation that no active legal hold exists, footage shall be purged from Evidence.com in accordance with standard evidence disposition procedures, with destruction documented in the case management system.

This policy reaffirms the City Manager's authority, which may be delegated to the Berkeley Police Chief, to pause or end the deployment of the subject equipment at any time and for any cause. The City Council shall be, within 48 hours, notified of any such decision to pause or end its deployment.

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 Support Services Division Captain or the Chief's 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.

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

The Chief of Police will report any request from federal immigration authorities, vendor, or any non-local agency to access data for federal immigration enforcement purposes within 10 days of receiving the request.

In the event a Federal Agency is given BPD-owned data stored with the vendor, the Berkeley Police Chief or designee will notify the City Manager, City Attorney, and City Council within 72 hours of the discovery of the incident.

Berkeley Police Department
Law Enforcement Services Manual

External Fixed Video Surveillance Cameras

351.7 VIDEO SURVEILLANCE AUDIT

The video surveillance software will generate a site log each time the system is accessed. The site log may include server, device, user or general access. The site log should be kept for two years and be exportable for reporting.

System audits will be conducted by the Office of Strategic Planning and Accountability (OSPA) on a regular basis, at least monthly. A report of these audits shall be published semiannually and sent to the Police Accountability Board. As part of the audit, OSPA will confirm that BPD doesn't enter any direct data sharing agreements or give direct access to outside agencies. A log of any instance of when surveillance footage has been shared, including date, time, reasons for search, and any recipient agencies.

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 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 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.

Attachment 2

Policy 1304 — Surveillance Use Policy—External Fixed Video Surveillance Cameras

**Attachments to ODPa Memorandum Dated October 16, 2026: “Review of BPD
Surveillance Technology Proposals and Policy Revisions”**

Policy
1304

Berkeley Police Department
Law Enforcement Services Manual

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 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, unless required by federal law.
- (f) Video recordings shall not be disclosed to law enforcement agencies from other states if the purpose of the request is to support the enforcement of laws that restrict or criminalize reproductive rights or rights regarding the provision or receipt of gender-affirming care.

1304.3 DATA COLLECTION

The cameras will film and store video on encrypted servers. License plate and facial recognition is not used on the cameras and may not be used unless approved by the City council. Audio may not be activated or used unless approved by the City Council. Surveillance camera data shall be wholly owned 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. 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 is not used on the cameras. Audio may not be activated or used unless approved by the City Council.. 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.

Berkeley Police Department
Law Enforcement Services Manual

Surveillance Use Policy-External Fixed Video Surveillance Cameras

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.

Evidentiary data downloaded for investigations is stored in the Department's digital evidence system.

Length of retention: Evidentiary footage within the Department's possession, custody or control shall be retained for the period prescribed by applicable state law governing criminal evidence and Department evidence policies (currently consistent with the applicable statute of limitations for the underlying offense, plus administrative hold requirements).

Basis: Retention period is based on the evidentiary and legal requirements of the associated criminal investigation or proceeding.

Authorization for extensions: Extensions beyond the standard period may be authorized by the Investigations Division Captain or their designee, and shall be documented in the case record.

Destruction procedures: Upon expiration of the applicable retention period and confirmation that no active legal hold exists, footage shall be purged from Evidence.com in accordance with standard evidence disposition procedures, with destruction documented in the case management system.

This policy reaffirms the City Manager's authority, which may be delegated to the Berkeley Police Chief, to pause or end the deployment of the subject equipment at any time and for any cause. The City Council shall be, within 48 hours, notified of any such decision to pause or end its deployment.

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

Berkeley Police Department
Law Enforcement Services Manual

Surveillance Use Policy-External Fixed Video Surveillance Cameras

- 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 Support Services Division Captain or the Chief's designee, for release in accordance with Charter Article XVIII, Section 125, Subdivision (20)(a).

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

The Chief of Police will report any request from federal immigration authorities, vendor, or any non-local agency to access data for federal immigration enforcement purposes within 10 days of receiving the request.

In the event a Federal Agency is given BPD-owned data stored with the vendor, the Berkeley Police Chief or designee will notify the City Manager, City Attorney, and City Council within 72 hours of the discovery of the incident.

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 will generate a site log each time the system is accessed. The site log may include server, device, user or general access. The site log should be kept for two years and be exportable for reporting.

External fixed video surveillance camera system audits will be conducted by the Office of Strategic Planning and Accountability (OSPA) on a regular basis, at least monthly. A report of these audits will be published semiannually and sent to the Police Accountability Board. As part of the audit, OSPA will confirm that BPD doesn't enter any direct data sharing agreements or give direct access to outside agencies. A log of any instance of when surveillance video and/or audio data has been shared, including date, time, reasons for search, and any recipient agencies.

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.

Berkeley Police Department
Law Enforcement Services Manual

Surveillance Use Policy-External Fixed Video Surveillance Cameras

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 ACCOUNTABILITY

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:

- (a) Non-law enforcement requests for access to stored external fixed video surveillance camera data shall be processed according to the Records Maintenance and Release Policy in accordance with applicable law.
- (b) All external fixed video surveillance camera 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.
- (c) Berkeley Police Department members approved to access external fixed video surveillance camera 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 external fixed video surveillance camera 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.
- (e) Measures will be taken to ensure the accuracy of external fixed video surveillance camera information. Errors discovered in external fixed video surveillance camera data collected by external fixed video surveillance camera units shall be marked, corrected or deleted in accordance with the type and severity of the error in question.
- (f) Such external fixed video surveillance camera data may be released to other authorized and verified law enforcement officials and agencies for legitimate California law enforcement purposes.
- (g) Every external fixed video surveillance camera 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.

1304.13 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.

Berkeley Police Department
Law Enforcement Services Manual

Surveillance Use Policy-External Fixed Video Surveillance Cameras

Attachment 3

**Acquisition Report — External Fixed Video Surveillance
Cameras**

**Attachments to ODPa Memorandum Dated October 16, 2026: “Review of BPD
Surveillance Technology Proposals and Policy Revisions”**

Background

Pursuant to BMC 2.99 Surveillance Technology Ordinance, this report and the associated surveillance use policy must be approved by City Council before “[a]cquiring new Surveillance Technology” (BMC 2.99.030(1)(b)). The Berkeley Police Department (BPD) seeks to deploy external fixed video surveillance cameras to enhance its anti-crime strategy, to effectively allocate and deploy personnel, and to enhance safety and security in public areas. 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.

This acquisition report covers camera hardware, the associated software platform, cellular data transmission, and cloud storage. The City will procure solar-powered, LTE-enabled cameras, eliminating the need for direct electrical wiring or complex network infrastructure setup on city poles.

This document satisfies the requirements of BMC 2.99 for “publicly-released written report produced prior to acquisition... that includes...” sections covering description, purpose, location, impact, mitigation, data types and sources, data security, fiscal cost, third party dependence and access, alternatives, and experience of other entities of the equipment.

1. Description

Information describing the Surveillance Technology and how it works, including product descriptions from manufacturers

Description:

- External fixed surveillance cameras capture high-definition video footage.
- The cameras do not record audio, and audio recording is explicitly prohibited by Berkeley policy for these types of cameras.
- The system may utilize AI for features such as 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.
- Some models offer features like 25x optical zoom and high-quality nighttime imagery.
- The City will procure cameras that eliminate the need for direct electrical wiring or complex network infrastructure setup on city poles.

How it Works:

BERKELEY POLICE DEPARTMENT BMC 2.99 ACQUISITION REPORT – EXTERNAL FIXED VIDEO SURVEILLANCE CAMERAS

Data is transmitted wirelessly via encrypted cellular connection to cloud storage compliant with Criminal Justice Information Services (CJIS) standards. The vendor provides installation, ongoing maintenance, cellular service, and software updates as part of its subscription model. Authorized BPD personnel access the system via secure login, with multi-factor authentication and each login automatically triggers the audit trail function to ensure compliance with policy.

Manufacturers’ Descriptions:

The following are manufacturers’ descriptions of external fixed video surveillance cameras that are representative of a broader range of cameras that are used for the same purposes and are not intended to express a preference for any particular vendor.

“Protect remote, hard-to-wire areas. Install Verkada products in locations that are hard to wire or lack connectivity, such as parking lots, construction sites, parks, and trails.”

“The Flock Safety Dual-Lens PTZ camera delivers uninterrupted wide-angle coverage and zoomed-in detail at the same time, giving law enforcement and security teams complete situational awareness, and dependable, high-definition evidence without the compromises of traditional PTZ systems.”

“Axon Outpost can be mounted on new or existing poles, buildings, vehicles, trailers, or trees to expand coverage all around an agency’s jurisdiction.”

2. Purpose

Information on the proposed purpose(s) for the Surveillance Technology

The proposed purpose for the external fixed surveillance cameras is to provide real-time awareness and investigative capacity in the 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

The general location(s) it may be deployed and reasons for deployment

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	9th / Gilman
Center / Shattuck	Solano / Colusa

BERKELEY POLICE DEPARTMENT BMC 2.99 ACQUISITION REPORT – EXTERNAL FIXED VIDEO SURVEILLANCE CAMERAS

University / Shattuck	4th / Hearst
Cedar / Shattuck	Adeline / Fairview
Durant / Telegraph	Shattuck / Ashby
4th / Virginia	62nd / King
University / MLK	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

An assessment identifying potential impacts on civil liberties and civil rights including but not limited to potential disparate or adverse impacts on any communities or groups

- 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 (SB 54 prohibiting sharing for federal immigration enforcement), alignment of BPD policy with state law, and prompt notification procedures if federal access is requested.
- Berkeley city policy explicitly prohibits the use of facial recognition technology.

5. Mitigations

Information regarding technical and procedural measures that can be implemented to appropriately safeguard the public from any impacts identified

- 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. The City requires that any 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.
- Video recordings shall not be disclosed to law enforcement agencies from other states if the purpose of the request is to support the enforcement of laws that

BERKELEY POLICE DEPARTMENT BMC 2.99 ACQUISITION REPORT – EXTERNAL FIXED VIDEO SURVEILLANCE CAMERAS

restrict or criminalize reproductive rights or rights regarding the provision or receipt of gender-affirming care.

- 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 and storage to mitigate cybersecurity risks and prevent unauthorized third-party access. Data is stored on the device or on a secure cloud environment meeting strict governmental security standards.
- Data will be retained for a limited period pursuant to the Department Use Policy (180 days, except as otherwise permitted by policy), and automatically deleted thereafter using secure methods 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.
- System audits will be conducted by the Office of Strategic Planning and Accountability (OSPA). As part of the audit, OSPA will confirm that BPD doesn't enter any direct data sharing agreements or give direct access to outside agencies.
- In the event a Federal Agency is given BPD-owned data stored with the vendor, the Berkeley Police Chief or designee will notify the City Manager, City Attorney, and City Council within 72 hours of the discovery of the incident.
- Using solar-powered cameras minimizes infrastructure impact and reliance on grid power at specific pole locations.

6. Data Types and Sources

A list of the sources of data proposed to be collected, analyzed, or processed by the Surveillance Technology, including "open source" data

- 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 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 ALPR system.

7. Data Security

Information about the steps that can be taken to ensure adequate security measures to safeguard the data collected or generated from unauthorized access or disclosure

BERKELEY POLICE DEPARTMENT BMC 2.99 ACQUISITION REPORT – EXTERNAL FIXED VIDEO SURVEILLANCE CAMERAS

- All data transferred from the cameras and the servers shall be encrypted.
- Only BPD members who receive training on the Use Policy, and who are then granted access by an administrator, may access the data. BPD members seeking access shall obtain the approval of the Investigations Division Captain, or their designee.
- All camera 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.
- Every browsing inquiry must be documented by either the associated Berkeley Police case number or incident number, and/or a reason for the inquiry.
- The video surveillance software generates a site log each time the system is accessed. The site log is kept on the server for two years and is exportable for reporting.
- All relevant recordings that are utilized will be collected pursuant to Policy 802, Property and Evidence, and retained pursuant to Policy 804, Records Maintenance, with strict adherence to chain of custody requirements.

8. Fiscal Cost

The fiscal costs for the Surveillance Technology, including initial purchase, personnel and other ongoing costs, including to the extent practicable costs associated with compliance with this and other reporting and oversight requirements, as well as any current or potential sources of funding.

The costs below represent estimates, and will vary based on the number of cameras deployed, camera models, and software features selected. The anticipated source of funding is the Department's existing operating budget as well as \$310,000 that was previously allocated for surveillance cameras.

Initial Cost:

- Hardware: Camera hardware is anticipated to be provided as part of the subscription model.
- Installation: Installation is anticipated to be provided as part of the subscription model. Solar-powered, LTE-enabled cameras eliminate the cost of direct electrical wiring or network infrastructure on City poles.

Cost of Use:

- City staff time for system administration, oversight, auditing, and reporting. These costs will be absorbed within existing departmental budgets.

Costs of Potential Adverse Impacts:

- Potential costs could arise from data breach litigation or claims of privacy violation. However, encryption, limited retention, restrictions on data sharing, and strict audit

BERKELEY POLICE DEPARTMENT BMC 2.99 ACQUISITION REPORT – EXTERNAL FIXED VIDEO SURVEILLANCE CAMERAS

logs minimize this risk. Strict adherence to the Use Policy will further mitigate liability.

- Costs of compliance with reporting and oversight requirements: The cost of compliance with BMC 2.99 will be absorbed into the existing salary costs of PD staff.

Annual and Ongoing Costs:

- The annual subscription cost is estimated to range from \$125,000 to \$325,000 per year. This covers camera hardware, cellular service, cloud storage, software, and maintenance.

Training Costs:

- Personnel: The operational cost is absorbed within the existing salary of the investigating officers and City staff, and this increased efficiency will likely result in time savings by reducing the need to canvass for and collect video evidence manually. Training is anticipated to be included in the software subscription and absorbed into regular in-service training hours.

Maintenance and Storage Costs:

- Ongoing maintenance, cellular service, and cloud storage are anticipated to be included in the subscription.

Upgrade Costs:

- Software updates are anticipated to be included in the annual subscription.

9. Third Party Dependence and Access

Whether use or maintenance of the technology will require data gathered by the technology to be handled or stored by a third-party vendor on an ongoing basis, and whether a third party may have access to such data or may have the right to sell or otherwise share the data in aggregated, disaggregated, raw or any other formats

The City will depend on the vendor for the camera hardware, the software platform, cellular data transmission, cloud storage, system maintenance, and software updates. This is inherent in the subscription model.

The vendor handles and stores the data on its cloud platform or on the device.

The City owns the data. The City's contract will require that the vendor not share or sell customer data. Access to the data by third parties (including vendor personnel) is controlled by the City through permissions managed within the 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.

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

The City’s contract with the vendor will require the company to provide prompt notification of any data request from a federal agency. The vendor 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

A summary and general assessment of potentially viable alternative methods (whether involving the use of a new technology or not), if any, considered before deciding to propose acquiring the Surveillance Technology

Hardwired cameras requiring direct electrical and network connections were considered but deemed unfeasible 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 is not feasible due to staffing constraints and recruitment challenges.

Deciding against deploying fixed video surveillance cameras altogether. Without this technology, the Department would forgo the investigative and situational awareness benefits of video evidence at the proposed locations. Video evidence is critical in generating leads and solving crimes where there are limited or no witnesses, or discrepancies in reported observations.

11. Experience of Other Entities

To the extent such information is available, a summary of the experience of comparable government entities with the proposed technology, including any unanticipated financial or community costs and benefits, experienced by such other entities

Many neighboring jurisdictions, including San Francisco, Oakland, and San Jose, use fixed surveillance cameras for public safety. According to the Mayor’s office, San Francisco’s Real-Time Investigation Center, which combines public safety cameras with other technology, has assisted in more than 1,500 arrests over two years.

A 2019 meta-analysis of 40 years of research found that cameras are associated with a significant but modest decrease in crime. Vehicle crime and property crime fell significantly, but there was no significant effect on violent crime or disorder. The authors recommend targeting cameras at vehicle and property crime and not using them as a stand-alone measure. Consistent with this, the Department proposes cameras as one investigative tool among many, not as a substitute for patrol or investigations.

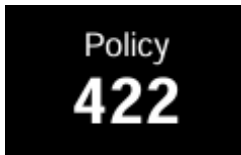
BERKELEY POLICE DEPARTMENT BMC 2.99 ACQUISITION REPORT – EXTERNAL FIXED VIDEO SURVEILLANCE CAMERAS

Criticism of the technology centers on large programs such as Detroit’s Project Green Light and Chicago’s Operation Virtual Shield. These have been faulted for continuous citywide monitoring, facial recognition, and limited transparency. The program proposed here has none of these features.

Attachment 4

**Policy 422 — Fixed Automated License Plate Readers
(ALPRs)**

Attachments to ODPa Memorandum Dated October 16, 2026: “Review of BPD
Surveillance Technology Proposals and Policy Revisions”



Berkeley Police Department

Law Enforcement Services Manual

Fixed Automated License Plate Readers (ALPRs)

422.1 PURPOSE AND SCOPE

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 Fixed ALPRs in this policy as well as the corresponding Surveillance Use-Fixed ALPRs policy-1305.

422.2 POLICY

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).

422.3 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.

422.4 ADMINISTRATION

The ALPR technology, also known as License Plate Recognition (LPR), allows for the automated detection of license plates. It is used by the Berkeley Police Department to convert data associated with vehicle license plates for official law enforcement purposes, including identifying stolen or wanted vehicles, stolen license plates and missing persons. It may also be used to gather information related to active warrants, suspect apprehension and stolen property recovery.

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

422.4.1 ALPR ADMINISTRATOR

The Investigations Division Captain, or his/her designee, shall be responsible for compliance with the requirements of Civil Code § 1798.90.5 et seq. This includes, but is not limited to (Civil Code § 1798.90.51; Civil Code § 1798.90.53):

- (a) Only properly trained sworn officers, crime analysts, communication operators, records clerks, parking enforcement officers, and police assistants are allowed access to the ALPR system or to collect ALPR information.
- (b) Ensuring that training requirements are completed for authorized users.
- (c) ALPR system monitoring to ensure the security of the information and compliance with applicable privacy laws.
- (d) Ensuring procedures are followed for system operators to maintain records of access in compliance with Civil Code § 1798.90.52.
- (e) The title and name of the current designee in overseeing the ALPR operation.
- (f) Working with the Custodian of Records, or vendor on the retention and destruction of ALPR data, ensuring this policy and related procedures are conspicuously posted on the City's website.

422.5 OPERATIONS

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

Use of an ALPR is restricted to the purposes outlined below. Department members shall not use, or allow others to use the equipment or database records for any unauthorized purpose

(Civil Code § 1798.90.51; Civil Code § 1798.90.53). (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:

- Entering Department member's name
- Related case number.
- 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 engages in an impermissible use of the ALPR system or associated scan files or hot lists may shall be subject to administrative sanctions, up to and including termination, pursuant to and consistent with the relevant collective bargaining agreements and departmental policies. Partial license plates reported during crimes may be entered into the ALPR system in an attempt to identify suspect vehicles.

(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.

422.6 DATA COLLECTION AND RETENTION

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. The Department should if feasible find a solution to transfer evidentiary hit data into it's digital evidence repository through secure integration. 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.

422.7 ACCOUNTABILITY

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.

422.8 ALPR DATA DETECTION BROWSING AUDITS

It is the responsibility of the Office of Strategic Planning and Accountability (OSPA) or the Chief's designee to ensure that an audit is conducted of ALPR detection browsing inquiries at least biennial. The Department will audit a sampling of the ALPR system utilization from the prior 24-month period to verify proper use in accordance with the above- authorized uses. The audit shall randomly select at least 10 detection browsing inquiries conducted by department employees during the preceding 24-month period and determine if each inquiry meets the requirements established in policy section 462.6(e).

Audits will be conducted by the OSPA on a regular basis, at least monthly. A report of these audits will be published semiannually and sent to the Police Accountability Board.

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 filed and retained by the OSPA. This audit should be shared in the Annual Surveillance Ordinance Report.

422.9 RELEASING ALPR DATA

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

(a) A supervisor at the requesting agency will sign an acknowledgement 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). See attached letter.

(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.

422.10 &

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

422.10 OFFICE OF THE DIRECTOR OF POLICE ACCOUNTABILITY

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.

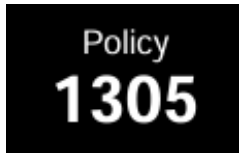
422.10422.11 TRAINING

The Personnel and Training Sergeant shall ensure that members receive department-approved training in order to be authorized to use or access the ALPR system (Civil Code § 1798.90.51; Civil Code § 1798.90.53)

Attachment 5

**Policy 1305 — Surveillance Use Policy—Fixed
Automated License Plate Readers (ALPRs)**

**Attachments to ODPa Memorandum Dated October 16, 2026: “Review of BPD
Surveillance Technology Proposals and Policy Revisions”**



Berkeley Police Department

Law Enforcement Services Manual

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

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

Use of an ALPR is restricted to the purposes outlined below. Department members shall not use, or allow others to use the equipment or database records for any unauthorized purpose (Civil Code § 1798.90.51; Civil Code § 1798.90.53).

(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:

- Entering Department member's name
- Related case number.
- 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 engages in an impermissible use of the ALPR system or associated scan files or hot lists may shall be subject to administrative sanctions, up to and including termination, pursuant to and consistent with the relevant collective bargaining agreements and departmental policies. Partial license plates reported during crimes may be entered into the ALPR system in an attempt to identify suspect vehicles.

(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. The Department should if feasible find a solution to transfer evidentiary hit data into it's digital evidence repository through secure integration. 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 twice a year.

(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 acknowledgement 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). See attached letter.

(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 City of Berkeley's Sanctuary City Ordinance and 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.

Audits will be conducted by the Office of Strategic Planning and Accountability (OSPA) on a regular basis, at least monthly. A report of these audits will be published semiannually and sent to the Police Accountability Board.

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

Attachment 6

**Acquisition Report — Automated License Plate Readers
(ALPRs)**

Attachments to ODPa Memorandum Dated October 16, 2026: “Review of BPD
Surveillance Technology Proposals and Policy Revisions”

Background

Pursuant to BMC 2.99 Surveillance Technology Ordinance, this report and the associated surveillance use policy must be approved by City Council before “[a]cquiring new Surveillance Technology” (BMC 2.99.030(1)(b)). The Berkeley Police Department (BPD) seeks to utilize a network of fixed automated license plate readers (ALPRs). The ALPRs will be affixed to street poles, street lights, or other similar objects that are either owned by the City of Berkeley or wherein a right-of-way agreement has been established.

This acquisition report covers fixed ALPR camera systems, the associated license plate recognition software, and vendor data hosting. It is not intended to express a preference for any particular vendor.

This document satisfies the requirements of BMC 2.99 for “publicly-released written report produced prior to acquisition... that includes...” sections covering description, purpose, location, impact, mitigation, data types and sources, data security, fiscal cost, third party dependence and access, alternatives, and experience of other entities of the equipment.

1. Description

Information describing the Surveillance Technology and how it works, including product descriptions from manufacturers

Description:

Fixed Automated License Plate Readers (ALPRs) are camera systems with software designed for license plate recognition. The camera systems are typically mounted on street poles, street lights, and highway overpasses.

This technology does not have facial recognition, and is not tied to any personal identifying information or used for traffic enforcement.

How it Works:

ALPRs are designed to capture license plate numbers which come into view, along with the location, date and time. The data, which includes an image of the front or the back of the car displaying the license plate, is then uploaded to a central server operated by the vendor. The license plate data is cross referenced with systems such as Stolen Vehicle Systems (SVS), and other lists like Amber alerts to notify police of vehicles with hits.

General Hot Lists like SVS will be automatically downloaded into the ALPR system a minimum of once a day with the most current data overwriting the old data. 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.

Manufacturers’ Descriptions:

The following are manufacturers’ descriptions of fixed ALPR systems that are representative of a broader range of systems that are used for the same purposes and are not intended to express a preference for any particular vendor.

“[Motorola] ReaperHD Fixed LPR Camera System. A workhorse for high-accuracy, high-volume license plate scanning. Monitor even your most traffic-heavy locations. This complete, fixed solution enables you to receive real-time alerts, conduct comprehensive searches and leverage advanced analytics to uncover new insights and operate more efficiently.”

“Flock combines industry-leading LPR cameras, vehicle intelligence, and the nation's largest LPR network to help teams find evidence faster, without compromising privacy or accountability.”

“Axon Outpost combines livestreaming, ALPR, and vehicle recognition in one device—so officers don’t just get a hit, they get the full picture in real time. It’s everything agencies need to act faster and respond smarter.”

2. Purpose

Information on the proposed purpose(s) for the Surveillance Technology

The proposed purpose of fixed ALPRs is to convert data associated with vehicle license plates for official law enforcement purposes in the following use cases:

- To identify stolen or wanted vehicles and stolen license plates.
- To locate missing persons.
- To gather information related to active warrants, suspect apprehension and stolen property recovery.
- To identify suspect vehicles using partial license plates and unique vehicle descriptions reported during crimes.

The use of ALPRs to alert police of a wanted vehicle or vehicle of interest entering into their respective jurisdiction has become increasingly more commonplace. This technology is being utilized on our local freeways, bridges, and in some instances in private parking lots. An effective deployment of ALPRs can aid the Berkeley Police Department in its efforts to focus on a wanted vehicle prior to a crime occurring in the City of Berkeley, and potentially avoid an instance of victimization.

3. Location

The general location(s) it may be deployed and reasons for deployment

BPD currently has 52 fixed ALPRs in the City of Berkeley. While the cameras are permanent installations, if found ineffective in the installed location, the Department can elect to

BERKELEY POLICE DEPARTMENT BMC 2.99 ACQUISITION REPORT – FIXED AUTOMATED LICENSE PLATE READERS

move the camera to another location at nominal cost. ALPR locations will be reported to City Council. It's preferred to leave cameras installed in locations for periods of minimally a year. Locations are determined using crime data, known locations of ingress or egress into the City of Berkeley, and commonly known direction of travel after criminal acts based on information provided from investigators. The Department will balance the need to deploy the camera systems equitably across the City of Berkeley with the need to deploy the cameras in an effective manner. BPD will solicit input from the selected vendor for an effective deployment.

4. Impact

An assessment identifying potential impacts on civil liberties and civil rights including but not limited to potential disparate or adverse impacts on any communities or groups

The Department acknowledges that fixed ALPRs involve privacy considerations, as the cameras read the license plates of vehicles that pass within view, not only vehicles of interest. 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 utilized with ALPR Units will help to prevent unauthorized use of its data. The procedures will 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.

The City of Berkeley is a Sanctuary City, and 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 Immigration and Customs Enforcement (ICE) and Customs and Border Protection (CBP).

To address potential disparate impacts, the Department will balance the need to deploy the camera systems equitably across the City of Berkeley with the need to deploy the cameras in an effective manner. The data from the fixed ALPRs shall be reported annually in the Surveillance Technology Report.

5. Mitigations

Information regarding technical and procedural measures that can be implemented to appropriately safeguard the public from any impacts identified

To safeguard the public's welfare and civil liberties, the Department will implement the following affirmative technical and procedural measures:

BERKELEY POLICE DEPARTMENT BMC 2.99 ACQUISITION REPORT – FIXED AUTOMATED LICENSE PLATE
READERS

- All ALPR data downloaded to the ALPR server should be stored for no longer than 30 days. Thereafter, ALPR data should be purged unless it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action or is subject to a discovery request or other lawful action to produce records. The ALPR vendor will purge their data at the end of the 30 days of storage.
- No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.
- 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.
- 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.
- 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. Prior to initiation of a stop, officers must receive confirmation that the license plate is still stolen, wanted, or otherwise of interest, and must visually verify that the license plate matches the image captured by the ALPR.
- The use policy specifically prohibits use of the ALPR system for invasion of privacy, harassment or intimidation, use based on a protected characteristic, personal use, or for the purpose or known effect of infringing upon First Amendment rights. Anyone who intentionally engages in an impermissible use shall be subject to administrative sanctions, up to and including termination.
- ALPR data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law, and only after a supervisor at the requesting agency signs an acknowledgement letter. ALPR data may not be shared for federal immigration enforcement.
- ALPR system audits will be conducted by the Professional Standards Bureau's Audit and Inspections Sergeant on a regular basis, at least biennial. The results of any audits will be shared with the Office of the Director of Police Accountability (ODPA) upon their completion.
- 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.

6. Data Types and Sources

A list of the sources of data proposed to be collected, analyzed, or processed by the Surveillance Technology, including "open source" data

Images of license plates and location metadata may be obtained through the use of ALPR cameras. The vendor's system may have searching capabilities due to technology from

machine learning that allow officers to search by vehicle type, make, color, license plate state, bumper sticker (the presence of a bumper sticker, not the image or content), decals (again the presence of a decal, not the image or content) and roof racks. All data stored in the vendor's servers shall be securely protected with end-to-end encryption.

7. Data Security

Information about the steps that can be taken to ensure adequate security measures to safeguard the data collected or generated from unauthorized access or disclosure

BPD takes data security seriously. 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 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.
- (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 twice a year.
- (g) Such ALPR data may be released to other authorized and verified law enforcement officials and agencies for legitimate 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.

8. Fiscal Cost

The fiscal costs for the Surveillance Technology, including initial purchase, personnel and other ongoing costs, including to the extent practicable costs associated with compliance with this and other reporting and oversight requirements, as well as any current or potential sources of funding.

The costs below represent estimates. The anticipated source of funding is the Department's existing operating budget which already accommodates an ALPR contract.

Initial Cost:

- Hardware: Individual camera costs are expected to range from \$2,500 to \$5,000 each, with the cost of installation to vary.
- Purchase and Installation: BPD believes that for the proposed 52 camera deployment, the cost to purchase and install will not exceed an initial cost of \$175,000.

Cost of Use:

- The operational cost is absorbed within the existing salary of Department personnel.

Costs of Potential Adverse Impacts:

- Potential costs could arise from data breach litigation or claims of privacy violation. However, the 30-day retention period, restrictions on data sharing, and strict audit logs minimize this risk. Strict adherence to the Use Policy will further mitigate liability.
- Costs of compliance with reporting and oversight requirements: The cost of compliance with BMC 2.99 will be absorbed into the existing salary costs of PD staff.

Annual and Ongoing Costs:

- The yearly subscription cost is expected to range from \$150,000 to \$175,000 a year.

Training Costs:

- Personnel: The operational cost is absorbed within the existing salary of Department personnel, and the increased efficiency of receiving automated alerts on vehicles of interest will likely result in time savings for patrol officers and investigators. Training for the operation of ALPR Technology shall be provided by BPD personnel and absorbed into regular in-service training hours. Any vendor-provided training is anticipated to be included in the subscription.

Maintenance and Storage Costs:

- Equipment maintenance and data hosting shall be provided by the vendor and are anticipated to be included in the annual subscription.

Upgrade Costs:

- Software upgrades are anticipated to be included in the annual subscription. If a camera is found ineffective in its installed location, it can be moved to another location at nominal cost.

9. Third Party Dependence and Access

Whether use or maintenance of the technology will require data gathered by the technology to be handled or stored by a third-party vendor on an ongoing basis, and whether a third party may have access to such data or may have the right to sell or otherwise share the data in aggregated, disaggregated, raw or any other formats

The ALPR vendor would store the data (data hosting) and ensure proper maintenance and security of data stored in their data towers. The vendor will purge their data at the end of 30 days of storage. However, this will not preclude the 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 (i.e. if detectives establish a hit results in evidentiary value it should be incorporated into the digital evidence of that specific case, and thereby would be kept longer than the aforementioned 30 days).

Restrictions on use of fixed ALPR Data: Information gathered or collected, and records retained by the vendor will not be sold, accessed, or used for any purpose other than legitimate law enforcement or public safety purpose unless allowed by policy (i.e. metadata will be permissible use for annual surveillance reporting).

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 supervisor at the requesting agency will sign an acknowledgement letter stating that the shared data will only be used for the purposes that are aligned with the Berkeley Police Department's policy. 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). ALPR data is subject to the provisions of the City of Berkeley's Sanctuary City Ordinance and Berkeley Police Department's Immigration Law Policy, and hence may not be shared with federal immigration enforcement officials.

10. Alternatives

A summary and general assessment of potentially viable alternative methods (whether involving the use of a new technology or not), if any, considered before deciding to propose acquiring the Surveillance Technology

An alternative is the deployment of additional police resources. The inherent problem with this alternative is that it is difficult to hire and train additional police officers and the cost would be significantly higher than adding technology. Furthermore, this technology furthers the Department's goal in protecting and safeguarding our community through precision based policing strategies.

A final alternative would be not acquiring fixed ALPRs. Without this technology, the Department would lose an effective tool for deterring and solving crime, would not receive alerts when a wanted vehicle or vehicle of interest enters the City, and would continue to rely on officers observing wanted vehicles by chance or on ALPR hits generated by neighboring jurisdictions.

11. Experience of Other Entities

To the extent such information is available, a summary of the experience of comparable government entities with the proposed technology, including any unanticipated financial or community costs and benefits, experienced by such other entities

ALPRs are in widespread use across the Bay Area. Nearly every law enforcement agency in Alameda County operates an ALPR program. San Francisco runs nearly 500 cameras, and Oakland's City Council approved a contract to maintain 291.

The strongest evidence on effectiveness comes from a 2026 study by University of South Carolina criminologists Scott Mourtgos and Ian Adams. It is the first large-scale causal evaluation of fixed ALPR networks. The study tracked 216 agencies as they deployed fixed ALPRs at different times, using official FBI crime data. It found:

- Motor vehicle theft fell 11 percent after deployment.
- Arrest clearance rates for motor vehicle theft rose by 16 percent.

Motor vehicle theft is historically one of the hardest crimes to clear by arrest, and Mourtgos said the results suggest a real public safety benefit for jurisdictions that adopt the technology. Local experience is consistent with this. When Richmond turned its cameras off, its police chief reported that auto thefts rose 33 percent and there was a slowdown in arrests and vehicle recoveries.

Many Bay Area agencies using Flock Safety have also had serious problems. Most involved outside agencies searching local data through vendor network settings that the local agency did not control or know about.

- **Mountain View.** An audit found that national and statewide lookup functions had been enabled from the start, allowing agencies to search the city's data without

authorization. The City Council unanimously voted to cancel the contract in February 2026.

- **Richmond.** Richmond suspended its cameras in late 2025 after learning that police agencies across the country could search its data. The Council voted 4-3 in March 2026 to temporarily restore the system through the end of the year. On October 6, 2026, the Council approved a new contract with a different vendor for police drones and surveillance cameras but sent license plate readers back for a future vote.
- **San Francisco.** A class-action lawsuit alleges that federal and out-of-state agencies accessed SFPD's camera data more than 1.6 million times over seven months. The city's Human Rights Commission found that the vendor had enabled nationwide searching without police knowledge.
- **Other jurisdictions.** Santa Cruz and Los Altos Hills terminated their contracts in January 2026, and Santa Clara County ended the Sheriff's use of the system.

Misuse by individual officers has also been documented. An off-duty San Jose police officer used the system to track a domestic violence victim and shared her location with the man accused of abusing her. The officer was fired following a criminal investigation, and the case was referred to California POST for possible decertification, which could bar him from working as a police officer in California.

These experiences show that the most serious problems came from vendor-controlled sharing features and inadequate oversight or illegal actions of individual users, not from the core function of checking plates against hot lists. The Department's use policy addresses these risks with:

- A 30-day retention limit
- A prohibition on sharing for immigration enforcement
- Signed acknowledgement letters before any data is shared
- Individual auditable credentials
- Documentation of every inquiry
- Regular audits shared with the PAB

Under Department policy, members are obligated to follow the use policy. Anyone who intentionally engages in an impermissible use of the ALPR system, scan files, or hot lists shall be subject to administrative sanctions, up to and including termination. Negligent misuse may also result in sanctions up to and including termination.

In addition, the Department will only procure a system in which the Department controls all sharing settings and no outside agency can search Berkeley data by default.

Attachment 7

Policy 355 — Community Video Streams

Attachments to ODPa Memorandum Dated October 16, 2026: “Review of BPD
Surveillance Technology Proposals and Policy Revisions”

Policy

355

Berkeley Police Department

Law Enforcement Services Manual

Community Video Streams

355.1 PURPOSE AND SCOPE

This policy provides guidance for the use of the community video stream integration by the Berkeley Police Department (BPD). The purpose of accessing community video streams is to provide real-time awareness and investigative capacity in the following use cases:

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

This initiative leverages software integration to access camera footage from cameras voluntarily registered and shared with BPD. This approach acts as a resource multiplier, allowing authorized staff to virtually canvass areas for evidence and gain real-time situational awareness during critical incidents without the cost or intrusiveness of installing new City poles and cameras.

355.2 POLICY

The Berkeley Police Department utilizes a community video streams system to enhance its anti-crime strategy, to effectively allocate and deploy personnel, support investigations, and to enhance safety and security in public areas. As specified by this policy, cameras owned by community partners in strategic locations throughout the City may be shared with the Police Department in order 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 355.3.1.

Community video streams in public areas will be used in a legal and ethical manner while recognizing and protecting constitutional standards of privacy.

355.3 OPERATIONAL GUIDELINES

BPD members authorized to review community video streams may only access and review video from public areas and public activities where no reasonable expectation of privacy exists, and only for the purposes authorized by this policy.

355.3.1 PLACEMENT REVIEW AND MONITORING

Deployment of the Community Video Stream integration is a voluntary software integration with the Police Department. However, the Department will focus its integration efforts on cameras located in the following high-priority areas:

- Integration will be prioritized for cameras owned by businesses and non-residential commercial property owners in major thoroughfares and districts, such as the Elmwood, Solano, Telegraph, Fourth Street, and Downtown business improvement districts.
- To facilitate rapid response to active shooter events, mass casualty incidents, or other critical public safety threats, the Department may enter into agreements with facilities or

Berkeley Police Department
Law Enforcement Services Manual

campuses where immediate video access could be vital for saving lives.

Actual locations are determined entirely by the entities that voluntarily agree to register or integrate their cameras and meet the requirements for integration. All locations will be within the City of Berkeley.

355.3.2 COMMUNITY VIDEO STREAM CAMERA MARKINGS

All public areas monitored by integrated community video streams shall be marked in a conspicuous manner with unobstructed signs to inform the public that the area is under police surveillance, as required by the Pre-Integration Review process below. Signage shall be maintained for the duration of the integration.

355.3.3 INTEGRATION WITH OTHER TECHNOLOGY

The Department may integrate technologies not otherwise prohibited with the community video streams system, provided that such use does not conflict with this policy or expand internal or external access beyond what is allowed by City law or Department policy. For example, integration may occur on a shared access platform where video data and automated license plate reader data are viewable in the same system.

355.3.4 PRE-INTEGRATION REVIEW

Before any community video stream is integrated into the Department's system, the following review process shall be completed:

- A designated Department member shall conduct an in-person visit to each camera location to:
 - Confirm the camera's physical location and field of view.
 - Verify the camera is not positioned to capture areas where a reasonable expectation of privacy exists, including but not limited to the interior of residences, private yards, restrooms, changing areas, or medical facilities.
- Prior to integration, signage shall be posted in a conspicuous location near each integrated camera informing the public that the area is monitored by a camera integrated with the Berkeley Police Department. Signage shall be maintained for the duration of the integration.
- The Department shall publish and maintain on the City of Berkeley website a current list and map of all community cameras that have been integrated with the Department's system.
- The Investigations Division Captain, or their designee, shall review and approve the site assessment before integration is finalized. Integration shall not proceed if the site assessment identifies unresolved privacy concerns.
- Upon discovery that an integrated camera has been repositioned to capture an area where a reasonable expectation of privacy exists, the Department shall immediately pause that

Berkeley Police Department
Law Enforcement Services Manual

camera's integration until the camera is positioned in compliance with this policy.

355.4 VIDEO SUPERVISION

Access to community video streams 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 355.6 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 community video streams 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.

355.4.1 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.

355.4.2 PROHIBITED ACTIVITY

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

Community video streams 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.

Community video streams equipment shall not be used to harass, intimidate or discriminate against any individual or group.

Community video streams 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, unless required by federal law.

Video recordings shall not be disclosed to law enforcement agencies from other states if the purpose of the request is to support the enforcement of laws that restrict or criminalize reproductive rights or rights regarding the provision or receipt of gender-affirming care.

Community video streams shall not be accessed for the purpose of monitoring, documenting, or recording individuals engaged in activity protected by the First Amendment to the United States Constitution or Article I of the California Constitution, including but not limited to lawful protests, demonstrations, political gatherings, or religious assemblies. Access during or in the vicinity of such activity is permissible only where there exists a clear, articulable, and imminent public safety threat that is actively occurring, and such access shall be limited in scope to the specific threat. Any such access shall be documented in the system log, including the specific articulable threat justifying access.

Community video streams shall not capture or transmit audio; any camera integrated into the

Berkeley Police Department
Law Enforcement Services Manual

Department's system must be configured for video only.

Real-time access to live video streams is permitted only when there is an active CAD incident or call for service; the associated incident number must be entered in the system log prior to initiating live viewing, and access shall terminate upon closure of that incident.

355.5 STORAGE AND RETENTION OF MEDIA

The Department acknowledges that the Community Video Stream integration relies on cameras and storage systems owned and operated by non-City entities. Consequently, video footage and associated metadata that is not downloaded or captured by the Department remains under the sole control and retention schedule of the camera owner.

Evidentiary data downloaded for investigations is stored in the Department's digital evidence system.

Length of retention: Evidentiary footage shall be retained for the period prescribed by applicable state law governing criminal evidence and Department evidence policies (currently consistent with the applicable statute of limitations for the underlying offense, plus administrative hold requirements).

Basis: Retention period is based on the evidentiary and legal requirements of the associated criminal investigation or proceeding.

Authorization for extensions: Extensions beyond the standard period may be authorized by the Investigations Division Captain or their designee, and shall be documented in the case record.

Destruction procedures: Upon expiration of the applicable retention period and confirmation that no active legal hold exists, footage shall be purged from Evidence.com in accordance with standard evidence disposition procedures, with destruction documented in the case management system.

355.5.1 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.

355.6 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.

Berkeley Police Department
Law Enforcement Services Manual

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.

The Chief of Police will report any request from federal immigration authorities, vendor, or any non-local agency to access data for federal immigration enforcement purposes within 10 days of receiving the request.

In the event a Federal Agency is given BPD-owned data from Community Video Streams, the Berkeley Police Chief or designee will notify the City Manager, City Attorney, and City Council within 72 hours of the discovery of the incident.

The Department does not own, control, or have the right to share the live video streams or raw data stored on the third-party camera systems involved in this integration. Release and data-sharing provisions in this policy and in Surveillance Use Policy 1306 apply only to evidentiary data the Department has actually downloaded and retained.

355.7 COMMUNITY VIDEO STREAMS AUDIT

The community video streams 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 (OSPA) on a regular basis, at least twice a year. As part of the audit, OSPA will confirm that BPD does not enter any direct data sharing agreements or give direct access to outside agencies. A log of any instance of when surveillance footage has been shared, including date, time, reasons for search, and any recipient agencies. As part of each audit, OSPA shall review a sample of system access logs to verify that queries were associated with a valid case or incident number, conducted by an authorized user, and consistent with the authorized uses enumerated in this policy.

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 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 published on the City of Berkeley website in an appropriate location, and retained within the Office of Strategic Planning and Accountability.

355.8 TRAINING

All BPD members authorized to access community video streams systems shall receive appropriate training. Training should include guidance on the use of cameras, associated

Berkeley Police Department
Law Enforcement Services Manual

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.

355.9 MAINTENANCE

It shall be the responsibility of the private owners of the cameras to facilitate and coordinate any updates and required maintenance.

Attachment 8

**Policy 1306 — Surveillance Use Policy—Community
Video Streams**

**Attachments to ODPa Memorandum Dated October 16, 2026: “Review of BPD
Surveillance Technology Proposals and Policy Revisions”**

Policy
1306

Berkeley Police Department
Law Enforcement Services Manual

Surveillance Use Policy - Community Video Streams

1306.1 PURPOSE

This policy provides guidance for the use of the Community Video Stream integration by the Berkeley Police Department (BPD). The purpose of accessing community video streams is to provide real-time awareness and investigative capacity.

This initiative leverages software integration to access video footage from cameras voluntarily registered and shared with the Police Department. This approach acts as a resource multiplier, allowing authorized staff to virtually canvass areas for evidence and gain real-time situational awareness during critical incidents without the cost or intrusiveness of installing new City poles and cameras.

1306.2 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 community video streams. 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.

Community video streams 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) Community video streams shall not intentionally be used to invade the privacy of individuals or observe areas where a reasonable expectation of privacy exists.
- (c) Community video streams 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 Services Manual

- (d) Video surveillance equipment shall not be used to harass, intimidate or discriminate against any individual or group.
- (e) Community video streams and recordings that are retained by Berkeley Police Department as evidence are subject to the Berkeley Police Department's Immigration Law Policy, and hence may not be shared with federal immigration enforcement officials, unless required by law.
- (f) Community video streams and recordings that are retained by Berkeley Police Department as evidence shall not be disclosed to law enforcement agencies from other states if the purpose of the request is to support the enforcement of laws that restrict or criminalize reproductive rights or rights regarding the provision or receipt of gender-affirming care.
- (g) Community video streams shall not be accessed for the purpose of monitoring, documenting, or recording individuals engaged in activity protected by the First Amendment to the United States Constitution or Article I of the California Constitution, including but not limited to lawful protests, demonstrations, political gatherings, or religious assemblies. Access during or in the vicinity of such activity is permissible only where there exists a clear, articulable, and imminent public safety threat that is actively occurring, and such access shall be limited in scope to the specific threat. Any such access shall be documented in the system log, including the specific articulable threat justifying access.
- (h) Community video streams shall not capture or transmit audio; any camera integrated into the Department's system must be configured for video only.
- (i) Real-time access to live video streams is permitted only when there is an active CAD incident or call for service; the associated incident number must be entered in the system log prior to initiating live viewing, and access shall terminate upon closure of that incident.

1306.3 DATA COLLECTION

Data collection is limited to camera footage and associated metadata voluntarily provided by community members; data collection for other purposes is prohibited. Community members create an account and register their cameras. This places a pin on the BPD map indicating a camera exists at that location. For compatible systems that opt-in, the video feed is routed via secure API to the BPD dashboard. The system integrates data from third-party hardware owned by non-City entities. BPD does not own the cameras. Camera owners retain ownership and either party can revoke access at any time.

1306.4 DATA ACCESS

Access to community video streams data shall be limited to BPD personnel utilizing the camera database for uses described above and pursuant to the Community Video

Berkeley Police Department
Law Enforcement Services Manual

Streams Policy. BPD members seeking access to the video surveillance system shall obtain the approval of the Investigations Division Captain, or their designee. Members accessing the database must follow the necessary logging mechanisms, such as case number and case type when querying the database.

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.

The vendor will retain no right access, use, sell or otherwise share community video streams data for any purpose without BPD's written consent.

1306.5 DATA PROTECTION

This program shall utilize a multi-layered security architecture to preserve the integrity and confidentiality of the data:

- Access shall require secure login credentials with Multi-Factor Authentication (MFA).
- Access shall be restricted to authorized personnel and audited for compliance.
- The storage environment shall comply with CJIS standards.
- Evidentiary data downloaded for investigations shall be stored in the Department's digital evidence system and retained according to state law. Non-evidentiary data remains under the control of the camera owner.

1306.6 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 1306.2 Authorized Use, 1306.4 Data Access, 1306.5 Data Protection, 1306.7 Data Retention, 1306.8 Public Access, 1306.9 Third Party Data Sharing, and 1306.13 Pre-Integration Review serve to protect against any unauthorized use of community video streams. The use of facial recognition technology on any community video stream is prohibited. 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. The Department will assess after implementation whether the distribution of integrated cameras reflects a pattern that could suggest a disparate impact, and will address any such pattern identified through the ordinance's Annual Report.

1306.7 DATA RETENTION

The Department acknowledges that the Community Video Stream integration relies on cameras and storage systems owned and operated by non-City entities. Consequently, video footage and associated metadata that is not downloaded or captured by the Department remains under the sole control and retention schedule of the camera owner.

Berkeley Police Department

Law Enforcement Services Manual

Evidentiary data downloaded for investigations is stored in the Department's digital evidence system.

Length of retention: Evidentiary footage within the Department's possession, custody or control shall be retained for the period prescribed by applicable state law governing criminal evidence and Department evidence policies (currently consistent with the applicable statute of limitations for the underlying offense, plus administrative hold requirements).

Basis: Retention period is based on the evidentiary and legal requirements of the associated criminal investigation or proceeding.

Authorization for extensions: Extensions beyond the standard period may be authorized by the Investigations Division Captain or their designee, and shall be documented in the case record.

Destruction procedures: Upon expiration of the applicable retention period and confirmation that no active legal hold exists, footage shall be purged from Evidence.com in accordance with standard evidence disposition procedures, with destruction documented in the case management system.

This policy reaffirms the City Manager's authority, which may be delegated to the Berkeley Police Chief, to pause or end the deployment of the subject equipment at any time and for any cause. The City Council shall be, within 48 hours, notified of any such decision to pause or end its deployment.

1306.8 PUBLIC ACCESS

Data collected by the Department 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.

1306.9 THIRD-PARTY DATA-SHARING

The Department does not own, control, or have the right to share the live video streams or raw data stored on the third-party camera systems involved in this integration. Consequently, the Department cannot and shall not grant third-party access to the camera registry or the live video feeds themselves.

Requests for evidentiary footage retained by BPD 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.

The Chief of Police will report any request from federal immigration authorities, vendor, or any non-local agency to access data for federal immigration enforcement purposes within 10 days of receiving the request.

Berkeley Police Department

Law Enforcement Services Manual

In the event a Federal Agency is given BPD-owned data from Community Video Streams, the Berkeley Police Chief or designee will notify the City Manager, City Attorney, and City Council within 72 hours of the discovery of the incident.

The CVS integration is provided through a third-party platform vendor, but the Department maintains no standing pool of community video stream data with the vendor: non-evidentiary video remains on the camera owner's system, and the Department retains footage only when it is downloaded as evidence, after which it is held in the Department's own digital evidence system and governed by the Department's evidence-retention and immigration policies. The vendor may access the data only to operate the platform. No non-City entity, including any federal agency, is granted direct access to the camera registry or video feeds; a non-City law enforcement agency may obtain only retained evidentiary footage through standard evidence sharing protocols with pre-authorization from the Investigations Captain, and only for a specific active criminal investigation supported by valid legal process, with any recipient bound by this policy, the Department's Immigration Law Policy, and the bar on using the footage to enforce other states' laws restricting reproductive or gender-affirming care.

1306.10 TRAINING

All BPD members authorized to access community video streams 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.

1306.11 AUDITING AND OVERSIGHT

The community video streams software generates a site log each time the system is accessed. 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. Community video stream audits will be conducted on a regular basis, at least twice a year. As part of the audit, OSPA will confirm that BPD does not enter any direct data sharing agreements or give direct access to outside agencies. A log of any instance of when surveillance footage has been shared, including date, time, reasons for search, and any recipient agencies. As part of each audit, OSPA shall review a sample of system access logs to verify that queries were associated with a valid case or incident number, conducted by an authorized user, and consistent with the authorized uses enumerated in this policy.

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.

Berkeley Police Department

Law Enforcement Services Manual

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 ACCOUNTABILITY

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:

- (a) Non-law enforcement requests for access to stored community video streams data shall be processed according to the Records Maintenance and Release Policy in accordance with applicable law.
- (b) All community video streams 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.
- (c) Berkeley Police Department members approved to access community video streams 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 community video streams 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.
- (e) Measures will be taken to ensure the accuracy of community video streams information. Errors discovered in community video streams data collected by community video streams units shall be marked, corrected or deleted in accordance with the type and severity of the error in question.
- (f) Such community video streams data may be released to other authorized and verified law enforcement officials and agencies for legitimate California law enforcement purposes.
- (g) Every community video streams 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.

1306.12 MAINTENANCE

It shall be the responsibility of the private owners of the cameras to facilitate and coordinate any updates and required maintenance.

1306.13 PRE-INTEGRATION REVIEW

Before any community video stream is integrated into the Department's system, the

Berkeley Police Department

Law Enforcement Services Manual

following review process shall be completed:

1. A designated Department member shall conduct an in-person visit to each camera location to:
 - a. Confirm the camera's physical location and field of view.
 - b. Verify the camera is not positioned to capture areas where a reasonable expectation of privacy exists, including but not limited to the interior of residences, private yards, restrooms, changing areas, or medical facilities.
2. All public areas monitored by integrated community video streams shall be marked in a conspicuous manner with unobstructed signs to inform the public that the area is under police surveillance. Signage shall be maintained for the duration of the integration.
3. The Department shall publish and maintain on the City of Berkeley website a current list and map of all community cameras that have been integrated with the Department's system.
4. The Investigations Division Captain, or their designee, shall review and approve the site assessment before integration is finalized. Integration shall not proceed if the site assessment identifies unresolved privacy concerns.
5. Upon discovery that an integrated camera has been repositioned to capture an area where a reasonable expectation of privacy exists, the Department shall immediately pause that camera's integration until the camera is positioned in compliance with this policy.

Attachment 9

Acquisition Report — Community Video Streams

Attachments to ODPa Memorandum Dated October 16, 2026: “Review of BPD
Surveillance Technology Proposals and Policy Revisions”

Background

Pursuant to BMC 2.99 Surveillance Technology Ordinance, this report and the associated surveillance use policy must be approved by City Council before “[e]ntering into an agreement with a non-City entity to acquire, share or otherwise use Surveillance Technology or the information it provides” (BMC2.99.030(1)(d)). The Berkeley Police Department (BPD) seeks to implement a community safety video integration capability to enhance real-time public safety operations and improve investigative efficiency. This initiative leverages software integration to access video footage from cameras voluntarily registered and shared by non-City entities.

This acquisition report is not for physical hardware but for the software capability to view community video streams. This approach acts as a resource multiplier, allowing authorized staff to virtually canvass areas for evidence and gain real-time situational awareness during critical incidents without the cost of installing new City poles and cameras.

This document satisfies the requirements of BMC 2.99 for “publicly-released written report produced prior to acquisition... that includes...” sections covering description, purpose, location, impact, mitigation, data types and sources, data security, fiscal cost, third party dependence and access, alternatives, and experience of other entities of the equipment.

1. Description

Information describing the Surveillance Technology and how it works, including product descriptions from manufacturers

Description:

The technology does not involve the City purchasing new cameras. Instead, it leverages software integrations to allow authorized BPD personnel to view live or recorded video streams from private cameras, only where the owner has explicitly granted permission to share data.

This system aggregates disparate video feeds into a centralized dashboard accessible to authorized BPD personnel, acting as a resource multiplier for investigations without requiring the City to install infrastructure.

How it Works:

The system functions through a cloud-based platform. Community members create an account and register their cameras. This places a pin on the BPD map indicating a camera exists at that location. For compatible systems that opt-in, the video feed is routed via secure API to the BPD dashboard. Access is permission-based. Camera owners retain ownership and can revoke access at any time. BPD personnel access the system via

secure login. Live viewing is restricted to active incidents, while historical access is used for gathering evidence.

Manufacturers' Descriptions:

The following are manufacturers' descriptions of investigative software platforms that are representative of a broader range of platforms that are used for the same purposes and are not intended to express a preference for any particular vendor.

"Flock Safety Wing® allows customers to easily integrate video cameras into FlockOS® for a seamless workflow. [It] integrates live stream traffic cameras, publicly or privately owned livestream security cameras into one cloud-based situational awareness dashboard to increase response time in mission-critical incidents."

"Residents and businesses are creating safer communities with Axon Community Connect, a voluntary, permission-based security initiative. The platform enables secure camera sharing with local law enforcement to support faster response in the event of an emergency."

2. Purpose

Information on the proposed purpose(s) for the Surveillance Technology

The proposed purpose of accessing community video streams 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

The general location(s) it may be deployed and reasons for deployment

Deployment of the Community Video Stream integration is a voluntary software integration with the Police Department. The Department will focus integration efforts on cameras located in the following high-priority areas:

- Integration will be prioritized for cameras owned by businesses and non-residential commercial property owners in major thoroughfares and districts, such as the Elmwood, Solano, Telegraph, Fourth Street, and Downtown business districts.

- To facilitate rapid response to active shooter events, mass casualty incidents, or other critical public safety threats, the Department may enter into agreements with facilities or campuses where immediate video access could be vital for saving lives.

Actual locations are determined entirely by the entities that voluntarily agree to register or integrate their cameras and meet the requirements for integration. All locations will be within the City of Berkeley.

4. Impact

An assessment identifying potential impacts on civil liberties and civil rights including but not limited to potential disparate or adverse impacts on any communities or groups

The Department acknowledges that community video streams involve privacy considerations. The use policy strictly prohibits accessing cameras in areas where a reasonable expectation of privacy exists without a warrant. Access would be driven by specific criminal incidents or calls for service, not constant monitoring. The policy, local ordinances, and state law all would prohibit sharing this information for immigration enforcement purposes.

To further mitigate impacts, every camera must pass a Pre-Integration Review- including an in-person site assessment to confirm the camera is not positioned to capture areas where a reasonable expectation of privacy exists- before it is connected to the Department's system.

Because integration efforts will be prioritized in commercial and business districts rather than residential areas, the Department does not anticipate a disparate impact on any particular demographic or residential community at this time. However, because participation is voluntary and driven by which owners choose to share their cameras, the Department cannot fully assess potential disparate impacts in advance. The Department will assess after implementation whether the distribution of integrated cameras reflects a pattern that could suggest a disparate impact, and will address any such pattern identified through the ordinance's Annual Report.

5. Mitigations

Information regarding technical and procedural measures that can be implemented to appropriately safeguard the public from any impacts identified

To safeguard the public's welfare and civil liberties, the Department will implement the following affirmative technical and procedural measures:

- Access is strictly permission-based. Camera owners must actively "opt-in" and can revoke access at any time.

- The use of facial recognition technology on any stream is strictly prohibited.
- All system access is logged. The audit trail records the user, date, time, and specific camera accessed as well as the case number and/or reason.
- Data is stored on CJIS-compliant servers.

Pre-Integration Review: In addition to the above, before any community video stream is integrated into the Department's system, the following review process shall be completed:

- A designated Department member shall conduct an in-person visit to each camera location to: (i) confirm the camera's physical location and field of view; and (ii) verify the camera is not positioned to capture areas where a reasonable expectation of privacy exists, including but not limited to the interior of residences, private yards, restrooms, changing areas, or medical facilities.
- Prior to integration, signage shall be posted near each location with integrated cameras informing the public that the area is monitored by a camera integrated with the Berkeley Police Department. Signage shall be maintained for the duration of the integration.
- The Department shall publish and maintain on the City of Berkeley website a current list and map of all community cameras that have been integrated with the Department's system.
- The Investigations Division Captain, or their designee, shall review and approve the site assessment before integration is finalized. Integration shall not proceed if the site assessment identifies unresolved privacy concerns.
- Upon discovery that an integrated camera has been repositioned to capture an area where a reasonable expectation of privacy exists, the Department shall immediately pause that camera's integration until the camera is positioned in compliance with this policy.

6. Data Types and Sources

A list of the sources of data proposed to be collected, analyzed, or processed by the Surveillance Technology, including "open source" data

Data collection is limited to camera footage and associated metadata voluntarily provided by community members. The system would integrate data from third-party hardware owned by non-City entities. BPD would not own the cameras nor any non-evidentiary data. Footage found to contain evidentiary value would be downloaded and stored according to existing evidence retention policies and protocols.

7. Data Security

Information about the steps that can be taken to ensure adequate security measures to safeguard the data collected or generated from unauthorized access or disclosure

This program would utilize a multi-layered security architecture to preserve the integrity and confidentiality of the data:

- Access requires secure login credentials with Multi-Factor Authentication (MFA).
- Access is restricted to authorized personnel and audited for compliance.
- The storage environment complies with CJIS standards.
- Evidentiary data downloaded for investigations is stored in the Department's digital evidence system (Evidence.com) and retained according to state law. Non-evidentiary data remains under the control of the camera owner.

8. Fiscal Cost

The fiscal costs for the Surveillance Technology, including initial purchase, personnel and other ongoing costs, including to the extent practicable costs associated with compliance with this and other reporting and oversight requirements, as well as any current or potential sources of funding.

The costs below represent estimates. Hardware costs and integration costs are paid by the private camera owners. The anticipated source of funding is the Department's existing operating budget. We expect that the use of this technology, in combination with other investigative and situational-awareness tools, will reduce the need for overtime by improving the efficiency of investigations and real-time response, generating savings that can offset ongoing subscription costs. In addition, we anticipate that vendors may offer this integration capability at reduced or no additional cost if it is bundled with other technology or services already procured by the Department, further limiting the net fiscal impact.

Initial Cost:

- Hardware: \$0 (Cameras are owned by private entities).
- Software Integration: Estimated \$30 per stream per year paid by camera owners.

Cost of Use:

- The operational cost is absorbed within the existing salary of the investigating officers and this increased efficiency will likely result in time savings.

Costs of Potential Adverse Impacts:

- Potential costs could arise from data breach litigation or claims of privacy violation. However, the reliance on voluntary consent to access cameras that already are in

place as well as strict audit logs minimizes this risk. Strict adherence to the Use Policy will further mitigate liability.

- Costs of compliance with reporting and oversight requirements: potential costs could arise from data breach litigation or claims of privacy violation. However, the reliance on voluntary consent to access cameras that already are in place as well as strict audit logs minimizes this risk. Strict adherence to the Use Policy will further mitigate liability. The cost of compliance with BMC 2.99 will be absorbed into the existing salary costs of PD staff.

Annual and Ongoing Costs:

- Annual subscription cost for the platform to integrate the streams is estimated to be \$65,000.

Training Costs:

- Personnel: The operational cost is absorbed within the existing salary of the investigating officers and this increased efficiency will likely result in time savings. Training is included in the software subscription and absorbed into regular in-service training hours.

Maintenance and Storage Costs:

- Maintenance of the software platform is included in the subscription. Maintenance of physical cameras is the responsibility of the private owners.

Upgrade Costs:

- Software upgrades are included in the annual subscription model.

9. Third Party Dependence and Access

Whether use or maintenance of the technology will require data gathered by the technology to be handled or stored by a third-party vendor on an ongoing basis, and whether a third party may have access to such data or may have the right to sell or otherwise share the data in aggregated, disaggregated, raw or any other formats

All evidentiary video will be uploaded and stored on the Department's digital evidence platform (Evidence.com) in line with existing departmental protocol for evidence collection. The evidence platform vendor complies with applicable data protection frameworks regarding the collection, use, and retention of personal information.

Live and recorded video streams that have not been downloaded as evidence remain on the third-party camera systems and under the control of the camera owners. The Department does not own, store, or have ongoing custody of this data.

The CVS integration is provided through a third-party platform vendor, but the Department maintains no standing pool of community video stream data with the vendor: non-evidentiary video remains on the camera owner's system, and the Department retains footage only when it is downloaded as evidence, after which it is held in the Department's own digital evidence system and governed by the Department's evidence-retention and immigration policies. The vendor may access the data only to operate the platform. No non-City entity, including any federal agency, is granted direct access to the camera registry or video feeds; a non-City law enforcement agency may obtain only retained evidentiary footage through standard evidence sharing protocols with pre-authorization from the Investigations Captain, and only for a specific active criminal investigation supported by valid legal process, with any recipient bound by this policy, the Department's Immigration Law Policy, and the bar on using the footage to enforce other states' laws restricting reproductive or gender-affirming care.

10. Alternatives

A summary and general assessment of potentially viable alternative methods (whether involving the use of a new technology or not), if any, considered before deciding to propose acquiring the Surveillance Technology

In the absence of a community video streams program, the primary alternative is the traditional method of physical canvassing. This process requires officers to physically walk neighborhoods after a crime, locate cameras, identify owners, and request footage manually. This method is time and resource-consuming and often relies on the owner being present, having the appropriate login and being technically capable of exporting the footage. It delays investigations and pulls officers away from other duties. In contrast, remote access makes the process more efficient for both the department and the community member.

The Department considered significantly expanding the network of City-owned and operated fixed cameras to match the coverage provided by community streams. This alternative was deemed fiscally unfeasible. The cost to purchase additional City-owned cameras would be prohibitively expensive.

Another alternative is to rely on physical surveillance by officers to deter crime and capture evidence. While physical surveillance is a valid tactic, it is limited by the cost and availability of resources. It does not provide the persistent, resource-multiplying capability of a camera network, nor does it allow for the retrospective review of evidence crucial for prosecution.

A final alternative would be not acquiring access to community video streams. Without this technology, the Department would forgo enhancements in investigative efficiency and

would continue to rely on slower, manual methods that may result in the loss of critical evidence or loss of available personnel power.

11. Experience of Other Entities

To the extent such information is available, a summary of the experience of comparable government entities with the proposed technology, including any unanticipated financial or community costs and benefits, experienced by such other entities

Community video integration is in active use regionally and nationally; most comparably, the Oakland City Council approved a similar program in December 2025, with comparable tools operating in San Francisco, Alameda County, and other jurisdictions. Criticism of the technology is found with the largest programs: Detroit's Project Green Light and Chicago's Operation Virtual Shield have been faulted for expanding into continuous, citywide monitoring, for pairing camera feeds with facial recognition, and in Chicago's case, for operating with limited regulation or public transparency. These criticisms do not transfer to the program proposed here. The Department seeks to integrate only voluntarily shared feeds that owners may revoke at any time; live access is limited to active incidents rather than continuous monitoring; facial recognition is prohibited on any stream; and the program operates under the public BMC 2.99 review process, with a published list and map of all integrated cameras, on-site signage, audit logging, express prohibition on use for monitoring first amendment assemblies, and biennial OSPA review. The features that generated controversy elsewhere- always-on monitoring, facial recognition, and the absence of oversight- are excluded here by design.

Attachment 10

**Policy 611 — Unmanned Aerial System (UAS)
Operations**

Attachments to ODPa Memorandum Dated October 16, 2026: “Review of BPD
Surveillance Technology Proposals and Policy Revisions”

Policy
611

Berkeley Police Department
Law Enforcement Services Manual

Unmanned Aerial System (UAS) Operations

611 PURPOSE AND SCOPE

The purpose of this policy is to establish guidelines for the use of an unmanned aerial system (UAS) and for the storage, retrieval and dissemination of images and data captured by the UAS. Department personnel shall adhere to requirements for Unmanned Aerial Systems covered in this policy as well as the corresponding Surveillance Use Policy 1303.

611.1 DEFINITIONS

Drone as First Responder (DFR) - A mode of operation where a UAS is deployed immediately in response to a call for service or other emergency. This mode of operation provides real-time aerial situational awareness to dispatchers, analysts and responding officers, assisting in the assessment of incidents, the coordination of resources, and the potential de-escalation or clearance of calls without the need for immediate physical police presence.

Federal Aviation Administration (FAA) – An entity of the federal government that regulates all aspects of civil aviation.

Pilot in Command (PIC) – Trained officer who is the sole person responsible for the operation of the UAS.

Unmanned Aerial System (UAS) - An unmanned aircraft of any type that is capable of sustaining directed flight, whether preprogrammed or remotely controlled (commonly referred to as an unmanned aerial vehicle (UAV)), and all of the supporting or attached systems designed for gathering information through imaging, recording or any other means.

Visual Observer – Trained officer who may act as a spotter for PIC to assist in navigating the UAS and avoidance of hazards.

611.2 POLICY

Unmanned aerial systems may be utilized for the purpose of enhancing the department's mission to safeguard our diverse community by enabling remote visual

assessment and real-time situational awareness in the situations specified in this policy. Any use of a UAS will also be in strict accordance with BMC 13.114 Sanctuary City Ordinance, constitutional and privacy rights, and FAA regulations.

All uses of the UAS shall be reported in compliance with the Berkeley Municipal Code (BMC) 2.99 Surveillance Technology Ordinance, and BMC 2.100 Police Equipment Ordinance.

Additionally, the Department shall publish data regarding specific requests, flight paths, and deployments on the Department's transparency portal. Flight logs and incident types for DFR operations should be published as soon as practicable, typically within one hour of docking.

611.3 PRIVACY

The Department acknowledges that UAS operations involve inherent privacy considerations, specifically the risk of inadvertently capturing footage of private areas (e.g., backyards or through windows) or uninvolved community members. To address this, the Department prioritizes civil liberties by restricting recording to authorized missions and strictly adhering to the restrictions on random surveillance outlined in Section 611.6 (Prohibited Use).

To safeguard these rights, UAS operations shall adhere to the following restrictions:

- 1) Absent a warrant or exigent circumstances, operators and observers shall adhere to FAA regulations and shall not intentionally record or transmit images of any location where a person would have a reasonable expectation of privacy (e.g., residence, yard, enclosure).
- 2) Operators and observers shall take reasonable precautions to avoid inadvertently recording or transmitting images of uninvolved community members or areas where there is a reasonable expectation of privacy. Cameras shall be diverted away from private spaces when not actively engaged in a permitted use.
- 3) For DFR operations, cameras shall be programmed to orient toward the horizon (preventing ground recording) while in transit to a call for service and shall only be directed toward the scene upon arrival at the authorized location.

611.4 PROGRAM COORDINATOR

The Police Chief will appoint a program coordinator who will be responsible for the management of the UAS program. The program coordinator will ensure that policies and procedures conform to current laws, regulations, and best practices.

611.5 PERMITTED USE

Authorized operators shall only deploy the UAS in the following circumstances, subsequent to supervisory approval for all deployments with the sole exception of Drone as First Responder (DFR) deployments:

- 1) To provide real-time situational awareness during high-risk or critical incidents, such as barricaded suspects, hostage situations, active shooters, the apprehension of armed and dangerous suspects, the pre-planning and service of a warrant allowing officers to create time and distance to formulate de-escalation strategies, facilitate safe tactical planning, and reduce the need for immediate physical engagement.
- 2) To assist in locating lost, missing, or injured persons during search and rescue operations.
- 3) To rapidly respond to calls for service to verify the nature of the incident, potentially determining that a law enforcement response is unnecessary for unfounded reports or low-priority incidents, thereby acting as a resource multiplier and keeping patrol officers available for other calls.
- 4) To locate fleeing suspects to effectively contain perimeters and reduce the need for dangerous ground-based foot pursuits.
- 5) To track fleeing vehicles from a safe distance, allowing patrol units to de-escalate or terminate dangerous ground pursuits while maintaining visual contact.
- 6) To clear interior buildings or confined spaces remotely to prevent potentially violent encounters between officers and hidden suspects.
- 7) To assist the Fire Department with fire mitigation and suppression, hazardous materials releases, or disaster response and recovery.
- 8) To remotely inspect potential explosive devices or hazardous objects.
- 9) To document complex crime scenes, accident scenes, or areas where an aerial perspective is critical for the investigation.
- 10) To respond to violent criminal activity at mass gatherings or special events only when there is probable cause of a felony and an active threat of serious bodily injury.
- 11) To mitigate hazards caused by other UAS interfering with emergency operations.
- 12) For pilot certification training and maintenance of proficiency.
- 13) To address other unforeseen exigent circumstances where there is an imminent threat to public safety, provided the deployment is consistent with the general privacy and safety principles of this policy.

611.6 PROHIBITED USE

- 1) The UAS shall not be used:
 - a) To conduct random or arbitrary surveillance activities. This prohibition includes, but is not limited to, first amendment assemblies in accordance with Policy 428 First Amendment Assemblies.
 - b) To target a person based solely on actual or perceived characteristics, such as race, ethnicity, national origin, religion, sex, sexual orientation, gender identity or expression, economic status, age, cultural group, or disability.
 - c) To harass, intimidate, or discriminate against any individual or group.
- 2) Furthermore, the UAS shall not be equipped with:
 - a) Facial recognition software
 - b) Biometric analysis capabilities
 - c) Weapons of any kind, including lethal or non-lethal munitions.

611.7 TRAINING

The Program Coordinator will coordinate training of PICs and Visual Observers. The training course and materials will be approved through the training staff. An approved department instructor will oversee all training. Each training session will be documented and forwarded to the Policy and Training Bureau Sergeant.

DECERTIFICATION

The Program Coordinator may suspend a PIC's or Visual Observer's certification pending review for any violation of this policy, Policy 1303, or FAA regulations, including for an unauthorized deployment. The Chief of Police or their designee shall decide whether to reinstate, require retraining, or permanently decertify.

The Office of Strategic Planning and Accountability shall conduct monthly audits of UAS use as required in Policy 1303. A report of these audits shall be published twice a year and should be sent to the Police Accountability Board.

611.8 RETENTION REQUIREMENTS

UAS footage should be purged by BPD within 5 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.

611.9 RELEASE OF RECORDINGS

- 1) Unauthorized use, duplication, and/or distribution of UAS camera footage is prohibited. Personnel shall not make copies of any UAS camera footage for their personal use and are prohibited from using a recording device such as a personal camera or any secondary video camera to capture UAS camera footage.
- 2) All UAS camera footage is property of the Berkeley Police Department and shall not be copied, released or disseminated in any form or manner outside the parameters of established policy, procedure, or laws.
- 3) The Custodian of Records, or their designee, will be responsible for handling requests for UAS camera footage.

Attachment 11

**Policy 1303 — Surveillance Use Policy—Unmanned
Aerial System (UAS)**

Attachments to ODPa Memorandum Dated October 16, 2026: “Review of BPD
Surveillance Technology Proposals and Policy Revisions”

Policy
1303

Law Enforcement Services Manual

Surveillance Use Policy-Unmanned Aerial System (UAS)

1303.1 PURPOSE

The purpose of this policy is to establish guidelines for the use of an unmanned aerial system (UAS) and for the storage, retrieval and dissemination of images and data captured by the UAS. Department personnel shall adhere to requirements for Unmanned Aerial Systems covered in this policy as well as the corresponding Use Policy - 611.

1303.2 AUTHORIZED USE

Authorized operators shall only deploy the UAS in the following circumstances, subsequent to supervisory approval for all deployments with the sole exception of Drone as First Responder (DFR) deployments:

1. To provide real-time situational awareness during high-risk or critical incidents, such as barricaded suspects, hostage situations, active shooters, the apprehension of armed and dangerous suspects, the pre-planning and service of a warrant allowing officers to create time and distance to formulate de-escalation strategies, facilitate safe tactical planning, and reduce the need for immediate physical engagement.
2. To assist in locating lost, missing, or injured persons during search and rescue operations.
3. To rapidly respond to calls for service to verify the nature of the incident, potentially determining that a law enforcement response is unnecessary for unfounded reports or low-priority incidents, thereby acting as a resource multiplier and keeping patrol officers available for other calls.
4. To locate fleeing suspects to effectively contain perimeters and reduce the need for dangerous ground-based foot pursuits.
5. To track fleeing vehicles from a safe distance, allowing patrol units to de-escalate or terminate dangerous ground pursuits while maintaining visual contact.
6. To clear interior buildings or confined spaces remotely to prevent potentially

violent encounters between officers and hidden suspects.

7. To assist the Fire Department with fire mitigation and suppression, hazardous materials releases, or disaster response and recovery.
8. To remotely inspect potential explosive devices or hazardous objects.
9. To document complex crime scenes, accident scenes, or areas where an aerial perspective is critical for the investigation.
10. To respond to violent criminal activity at mass gatherings or special events only when there is probable cause of a felony and an active threat of serious bodily injury.
11. To mitigate hazards caused by other UAS interfering with emergency operations.
12. For pilot certification training and maintenance of proficiency.
13. To address other unforeseen exigent circumstances where there is an imminent threat to public safety, provided the deployment is consistent with the general privacy and safety principles of this policy.

1303.3 PROHIBITED USE

The UAS shall not be used:

1. To conduct random or arbitrary surveillance activities. This prohibition includes, but is not limited to, first amendment assemblies in accordance with Policy 428 First Amendment Assemblies.
2. To target a person based solely on actual or perceived characteristics, such as race, ethnicity, national origin, religion, sex, sexual orientation, gender identity or expression, economic status, age, cultural group, or disability.
3. To harass, intimidate, or discriminate against any individual or group.

Furthermore, the UAS shall not be equipped with:

1. Facial recognition software
2. Biometric analysis capabilities
3. Weapons of any kind, including lethal or non-lethal munitions.

1303.4 DATA COLLECTION

Data collection shall be limited to video (visible and infrared) and associated telemetry (e.g., flight path, altitude) necessary for safe flight operations and situational awareness. The UAS will capture real-time video to assist pilots in navigating safely and assessing authorized scenes. These recordings shall be utilized solely for legitimate law enforcement purposes, including criminal investigations, administrative reviews, and training, in strict accordance with state laws and Department policy.

1303.5 DATA ACCESS

Access to videos shall be limited to authorized personnel with a legitimate law enforcement or administrative need. Any release or access to videos by third parties requires prior authorization and shall be limited to legally authorized agencies or pursuant to a valid court order.

1303.6 DATA PROTECTION

The Department shall implement and maintain comprehensive data security protocols to preserve the integrity, confidentiality, and lawful use of UAS videos. Video recording shall occur only during authorized operations and shall not include continuous or passive surveillance.

1303.7 CIVIL LIBERTIES AND RIGHTS PROTECTIONS

The Department acknowledges that UAS operations involve inherent privacy considerations, specifically the risk of inadvertently capturing footage of private areas (e.g., backyards or through windows) or uninvolved community members. To address this, the Department prioritizes civil liberties by restricting recording to authorized missions and strictly adhering to the restrictions on random surveillance outlined in Section 611.6 (Prohibited Use).

To safeguard these rights, UAS operations shall adhere to the following restrictions:

1. Absent a warrant or exigent circumstances, operators and observers shall adhere to FAA regulations and shall not intentionally record or transmit images of any location where a person would have a reasonable expectation of privacy (e.g., residence, yard, enclosure).
2. Operators and observers shall take reasonable precautions to avoid inadvertently recording or transmitting images of uninvolved community members or areas where there is a reasonable expectation of privacy. Cameras shall be diverted away from private spaces when not actively engaged in a permitted use.

3. For DFR operations, cameras shall be programmed to orient toward the horizon (preventing ground recording) while in transit to a call for service and shall only be directed toward the scene upon arrival at the authorized location.

1303.8 DATA RETENTION

UAS footage should be purged by BPD within 5 days if it does not 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.

1303.9 PUBLIC ACCESS

Unauthorized use, duplication, and/or distribution of UAS camera footage is prohibited. Personnel shall not make copies of any UAS camera footage for their personal use and are prohibited from using a recording device such as a personal camera or any secondary video camera to capture UAS camera footage.

All UAS camera footage is property of the Berkeley Police Department and shall not be copied, released or disseminated in any form or manner outside the parameters of established policy, procedure, or laws.

The Custodian of Records, or their designee, will be responsible for handling requests for UAS camera footage.

1303.10 THIRD PARTY DATA SHARING

Pursuant to the Records Maintenance and Release policy, data collected from the UAS may only be shared with other law enforcement agencies on a case-by-case basis in connection with an active investigation, or in response to a lawful judicial warrant or court order in compliance with state and local law.

1303.11 TRAINING

The Program Coordinator will coordinate training of PICs and Visual Observers. The training course and materials will be approved through the training staff. An approved department instructor will oversee all training. Each training session will be documented and forwarded to the Policy and Training Bureau Sergeant.

1303.12 AUDITING AND OVERSIGHT

Division Captains or their designee shall ensure compliance with this Surveillance Use Policy.

The Office of Strategic Planning and Accountability shall conduct monthly audits of UAS use. A report of these audits shall be published twice a year and should be sent to the Police Accountability Board.

Intentional violation of this policy may serve as grounds for disciplinary action pursuant to the Policy 1010, Personnel Complaints policy. Violations of this policy may also result in decertification under Policy 611.

1303.13 MAINTENANCE

All UAS maintenance shall be conducted by the owner/operator of the device consistent with the manufacturer's specifications and as needed based on UAS usage.

Attachment 12

Acquisition Report — Unmanned Aerial System

**Attachments to ODPa Memorandum Dated October 16, 2026: “Review of BPD
Surveillance Technology Proposals and Policy Revisions”**

Background

The Berkeley Police Department (BPD) seeks to acquire a comprehensive Unmanned Aerial System (UAS) program to enhance public safety operations and improve incident response times. This acquisition includes three distinct capabilities: interior-capable drones for searching confined spaces, field-deployed drones carried in patrol vehicles for immediate on-scene situational awareness, and a "Drone as a First Responder" (DFR) system capable of launching from a rooftop docking station. While UAS technology offers broad applications across various City departments such as for wildfire monitoring and disaster response, this Acquisition Report specifically addresses the use of this equipment by the Police Department for law enforcement purposes.

This document satisfies the requirements of BMC 2.99 for “publicly-released written report produced prior to acquisition... that includes...” sections covering description, purpose, location, impact, mitigation, data types and sources, data security, fiscal cost, third party dependence and access, alternatives, and experience of other entities of the equipment.

1. Description

Information describing the Surveillance Technology and how it works, including product descriptions from manufacturers

The following are descriptions of drone models that are representative of a broader range of drones used for the same purposes.

Description:

The Unmanned Aerial System (UAS) described in this appendix consists of three categories of deployment models- interior field-deployed, outdoor field-deployed, and Drone as First Responder (DFR)- and aircraft, including attached cameras, and internal components to support the safe and effective operation of the systems. Examples of UAS models in each category are:

- Interior field-deployed: Avata 2 / Brinc Lemur / Skydio R10: This UAS would be used for tactical operations and searches within interior confined spaces such as a warehouse, commercial building or residence.
- Outdoor field-deployed: DJI Matrice 4T / Brinc Responder / Skydio X10: This UAS would be used for patrol operations to rapidly respond to the scene of an incident and provide real-time video and situational awareness to officers responding to the

scene. These systems would include the UAS, batteries, and software integration with our current CAD and Flock systems.

- DFR: DJI Matrice 4TD / Flock Alpha / Brinc Responder / Skydio X10: This UAS would be dedicated to DFR response to rapidly respond to the scene of an incident and provide real-time video and situational awareness to officers responding to the scene. It would also include the installation of two charging and telecommunications docks on the roof of the Public Safety Building.

How it Works:

Remote controllers would be used to operate each type of UAS. They provide a live video feed and ensure the safe and effective operations of the UAS. Digital media cards would be installed in the UAS and would store the video footage from the flights. The DFR system includes the installation of two charging and telecommunications docks.

Manufacturers' Descriptions:

"DJI Avata 2 is a compact and portable FPV camera drone equipped with built-in propeller guards. The aircraft uses both GNSS and a Vision System, allowing for stable hovering and smooth aerobatic maneuvers while flying both indoors and out."

"Fly with confidence inside thanks to LEMUR 2's hardware and flight software capabilities. Quickly deployable; Shatter glass to breach windows; Stable flight with 360° position hold; Pushes open ajar doors"

"Skydio R10: The ease, durability and low operational cost of small consumer drones popular for indoor use, with the onboard lighting, communications and cloud integrations your mission demands. Launch, command, stream, and upload—everything needed to get the job done, built in."

"The DJI Matrice 4 Thermal drone introduces a compact, intelligent drone for professional use. Equipped with a thermal camera, enhanced sensing, and a laser range finder, this drone offers safer and more reliable operations. The Matrice 4T is ideal for industries including electricity, emergency response, public safety, and forestry conservation."

"Responder: A powerful aerial tool for public safety agencies – built right here in the USA. 42min Flight Time; 40X Total Zoom; 640PX Thermal Camera; 4G Teleoperations"

"Skydio X10: The best sensors for a drone this small, piloted by the most advanced AI in the sky. To get the data you need, wherever and whenever you need it. 45mph Max flight speed. 40min Max flight time. <40sec Deployment time. IP55 Certified against dust and water."

"The DJI Matrice 4TD is a professional-grade thermal drone designed for rapid, accurate intelligence across utility inspections, solar and wind maintenance, industrial monitoring, public safety, and search-and-rescue missions. Combining high-resolution thermal imaging with a visual camera, this dual-spectrum platform reveals details invisible to conventional sensors, allowing teams to detect overheating equipment, identify hotspots in solar arrays, monitor turbine performance, and locate heat signatures during emergency operations. Rugged, IP-rated construction and extended flight endurance ensure reliable performance in challenging environments, making the M4TD a mission-ready solution for demanding field conditions."

"Flock Alpha sets a new standard for rapid response in public safety. American-made and NDAA-compliant, Flock Alpha is purpose-built for DFR, enhancing speed, coverage area, and camera power in a fully integrated solution."

2. Purpose

Information on the proposed purpose(s) for the Surveillance Technology

The primary objective of the UAS program is to leverage technology to preserve life and enhance safety.

- By providing an aerial vantage point, the UAS allows officers to create time and distance from a threat. This provides opportunities for negotiation and de-escalation that are not possible when officers are forced to make split-second decisions face-to-face with a suspect.
- The UAS allows for the remote assessment of hazardous scenes (e.g., suspicious devices, armed individuals), reducing the physical risk to officers and bystanders.
- UAS can rapidly clear calls for service (such as unfounded reports), allowing patrol officers to remain available for genuine emergencies and reducing police presence where it is not needed.

3. Location

The general location(s) it may be deployed and reasons for deployment

Officers may use UAS anywhere officers have jurisdiction to operate as sworn peace officers. All deployments are strictly governed by the authorized use cases and privacy protections established in Policy 611 (UAS Operations) and Surveillance Use Policy 1303.

4. Impact

An assessment identifying potential impacts on civil liberties and civil rights including but not limited to potential disparate or adverse impacts on any communities or groups

The Department acknowledges that UAS operations involve inherent privacy considerations, including the risk of inadvertently capturing footage of private areas (e.g., backyards or through windows) or uninvolved community members. To address this, the Department has established strict prohibitions against random surveillance or targeting individuals based on protected characteristics. While the aerial vantage point provides critical safety data, the Department's policies prioritize civil liberties by restricting recording to authorized missions and mandating that cameras be diverted away from private spaces when not actively engaged in a call for service, as detailed in the "Mitigations" section below.

5. Mitigations

Information regarding technical and procedural measures that can be implemented to appropriately safeguard the public from any impacts identified

To safeguard the public's welfare and civil liberties, the Department will implement the following affirmative technical and procedural measures:

- All DFR cameras will be programmed to orient toward the horizon (preventing ground recording) while in transit to a call for service. The camera will only point down upon arrival at the authorized scene.
- All UAS flights are logged, and flight data is auditable. Video data with evidentiary value is stored on secure, encrypted servers (Evidence.com) with strict chain-of-custody controls.
- The UAS will not be equipped with facial recognition software or weapons of any kind.
- As required by BMC 2.99 and BMC 2.100, the Department will publish data regarding deployments on an annual basis.
- Information including flight logs and incident type will be published on a publicly accessible transparency portal shortly after the conclusion of a flight, typically within 1 hour after docking.
- The program is subject to review by the Police Accountability Board and approval by the City Council via the Annual Military Equipment Report and the Annual Surveillance Technology Report.

6. Data Types and Sources

A list of the sources of data proposed to be collected, analyzed, or processed by the Surveillance Technology, including "open source" data

Data collection is limited to video (visible and infrared) and associated telemetry (e.g., flight path, altitude) necessary for safe flight operations and situational awareness. The UAS will capture real-time video to assist pilots in navigating safely and assessing authorized scenes. These recordings are utilized solely for legitimate law enforcement purposes, including criminal investigations, administrative reviews, and training, in strict accordance with state laws and Department policy.

7. Data Security

Information about the steps that can be taken to ensure adequate security measures to safeguard the data collected or generated from unauthorized access or disclosure

The Department will implement and maintain comprehensive data security protocols to preserve the integrity, confidentiality, and lawful use of UAS videos. Video recording will occur only during authorized operations and will not include continuous or passive surveillance. All recorded data will be stored securely on an internal hard drive and/or SD cards prior to upload to BPD's evidence database. Access to videos will be limited to authorized personnel with a legitimate law enforcement or administrative need. Any release or access to videos by third parties requires prior authorization and will be limited to legally authorized agencies or pursuant to a valid court order.

8. Fiscal Cost

The fiscal costs for the Surveillance Technology, including initial purchase, personnel and other ongoing costs, including to the extent practicable costs associated with compliance with this and other reporting and oversight requirements, as well as any current or potential sources of funding;

The cost ranges below represent estimates. Costs are subject to change at the time of purchase based on the number of units obtained, lease or purchase terms, contract lengths, and bundling options.

The anticipated source of funding is the Department's existing operating budget. We expect that the use of this technology, in combination with other investigative and situational-awareness tools, will reduce the need for overtime by improving the efficiency of investigations and real-time response, generating savings that can offset ongoing

subscription costs. In addition, we anticipate that vendors may offer this capability at a reduced cost if it is bundled with other technology or services already procured by the Department, further limiting the net fiscal impact.

Initial Cost:

- Purchase of 4 interior and 4 outdoor field-deployed UAS : Total \$44,500-\$150,000
- Lease of PSB-based DFR (Year 1): \$100,000-\$200,000
- Radar (Year 1): \$0-\$150,000
- Dock Installation: \$0-\$15,000.

Cost of Use:

- Each individual use of the UAS incurs a negligible financial cost, limited primarily to the electricity required to recharge the aircraft batteries. The operational cost is absorbed within the existing salary of the trained Pilot in Command (PIC) and does not require additional overtime or specialized funding. For the DFR program, the annual lease covers unlimited flights, meaning there is no incremental cost for high-frequency usage.

Costs of Potential Adverse Impacts:

- Costs of adverse impacts could include property damage caused by a malfunctioning drone, but the experience of other agencies with drones and similar programs indicates that such incidents are extremely rare. Furthermore, strict adherence to FAA maintenance schedules, pre-flight inspections, and pilot training requirements serves to minimize the risk of malfunction or operator error. Any costs associated with accidental damage or liability claims would be addressed through the City's existing claims process.
- Costs of compliance with reporting and oversight requirements: financial risks related to Surveillance Technology Ordinance compliance are minimal given that the City is allowed 90 days to cure any issues. Furthermore, strict adherence to the Use Policy will further mitigate liability. The cost of compliance with BMC 2.99 and 2.100 will be absorbed into the existing salary costs of PD staff.

Annual and Ongoing Costs:

- DFR Lease: \$100,000-\$200,000 per year.
- Radar: \$150,000 per year.
- Parts/Maintenance (for purchased units): \$2,000 per year.

Training Costs:

- Personnel: the operational cost is absorbed within the existing salary of the participating officers. The efficiencies produced by this technology will likely result in time savings and reduced overtime.
- Training (4 primary pilots): \$24,000.
- Training (8 additional pilots): \$48,000.

Maintenance and Storage Costs:

- Parts/maintenance for purchased units: \$2,000 per year.
- Parts/maintenance for leased units: included.

Upgrade Costs:

- UAS hardware upgrades are often included in the lease or purchase agreement.

9. Third Party Dependence and Access

Whether use or maintenance of the technology will require data gathered by the technology to be handled or stored by a third-party vendor on an ongoing basis, and whether a third party may have access to such data or may have the right to sell or otherwise share the data in aggregated, disaggregated, raw or any other formats

All UAS data with evidentiary value will be uploaded and stored on Axon's Evidence.com platform in line with existing departmental protocol for evidence collection. 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.

BPD will only share UAS data with other law enforcement agencies on a case-by-case basis in connection with an active investigation, or in response to a lawful judicial warrant or court order in compliance with state and local law.

10. Alternatives

A summary and general assessment of potentially viable alternative methods (whether involving the use of a new technology or not), if any, considered before deciding to propose acquiring the Surveillance Technology

In the absence of a UAS program, the department would be limited to less effective and more costly alternatives. If we were to gain the same level of operational support, we could attempt to increase the amount of officers to match the coverage and responsiveness of aerial support. However that is not feasible at this time due to well established challenges in hiring and training suitable candidates. It would also not address underlying efficiency issues in that ground-based units lack the elevated perspective needed for efficient searches, crowd monitoring, and scene management, and offer reduced capacity to maintain time and distance for de-escalation. This can heighten the potential for confrontational encounters and diminish effectiveness in pursuits or rapidly evolving incidents.

Additionally, taking no action would leave existing operational challenges unaddressed. The department would continue to rely on outside agencies for aerial support, risking delays in critical moments. Without its own UAS capability, the department would forgo enhancements in officer safety and public protection, while falling behind regional peers who have already adopted this widely accepted and increasingly standard public safety tool.

11. Experience of Other Entities

To the extent such information is available, a summary of the experience of comparable government entities with the proposed technology, including any unanticipated financial or community costs and benefits, experienced by such other entities

The Alameda County Sheriff's Office has operated its UAS program since 2015 and only reports a single community complaint, which was ultimately deemed unrelated to drone activity. The agency implemented a public transparency portal and documented multiple operational successes, including enhanced officer safety, improved suspect apprehension, efficient crime scene documentation, and the successful location of missing persons.

The Hayward Police Department launched its UAS program in March 2022. Since then, the department has conducted 75 deployments without any citizen complaints or unexpected financial impacts. The program has been integral in reducing risk during critical incidents.

The Fremont Police Department began using UAS technology in 2017 and now maintains a fleet of 16 drones operated by 25 trained personnel. The department reports no community complaints, maintains regular updates to its transparency portal, and is currently developing its Drone as First Responder (DFR) capability. Fremont Police report that the

program delivers significant operational advantages and has become an integrated part of its modern policing strategy.

These examples illustrate the increasing regional adoption and effectiveness of UAS programs across local police departments and reinforce their role as a valuable and accepted tool in contemporary law enforcement.

Attachment 13

**Impact Statement and Policy 709 Update — Unmanned
Aerial System**

Attachments to ODPa Memorandum Dated October 16, 2026: “Review of BPD
Surveillance Technology Proposals and Policy Revisions”

Background

The Berkeley Police Department (BPD) seeks to acquire a comprehensive Unmanned Aerial System (UAS) program to enhance public safety operations and improve incident response times. This acquisition includes three distinct capabilities: interior-capable drones for searching confined spaces, field-deployed drones carried in patrol vehicles for immediate on-scene situational awareness, and a "Drone as a First Responder" (DFR) system capable of launching from a rooftop docking station. While UAS technology offers broad applications across various City departments such as for wildfire monitoring and disaster response, this Impact Statement specifically addresses the use of this equipment by the Police Department for law enforcement purposes.

This document satisfies the requirements of AB 481 for "approval of the governing body, by an ordinance adopting military equipment use policy" for a specific type of military equipment: "unmanned, remotely piloted, powered aerial... vehicle" (AB 481). It also satisfies the requirements of BMC 2.100 for "a publicly released, written document that includes..." sections covering description, purpose, fiscal cost, impact, mitigations, alternatives, and third-party dependence of the equipment.

1. Description

A description of each type of Controlled Equipment, the quantity sought, its capabilities, expected lifespan, intended uses and effects, and how it works, including product descriptions from the manufacturer of the Controlled Equipment.

The following are descriptions of drone models that are representative of a broader range of drones used for the same purposes.

Description:

The Unmanned Aerial System (UAS) described in this appendix consists of ~~four~~ three ~~different types~~ categories of deployment models- interior field-deployed, outdoor field-deployed, and Drone as First Responder (DFR)- and aircraft, including attached cameras, and internal components to support the safe and effective operation of the systems. ~~Two of them are traditional UAS and two of them would allow the implementation of a "Drone as a First Responder" (DFR) system.~~ The UAS are the following models Examples of UAS models in each category are:

- Interior field-deployed: Avata 2 / Brinc Lemur / Skydio R10: This UAS would be used for tactical operations and searches within interior confined spaces such as a warehouse, commercial building or residence.
- Outdoor field-deployed: DJI Matrice 4T / Brinc Responder / Skydio X10: This UAS would be used for patrol operations to rapidly respond to the scene of an incident and provide real-time video and situational awareness to officers responding to the scene. These systems would include the UAS, batteries, and software integration with our current CAD system.
- DFR: DJI Matrice 4TD / Flock Alpha / Brinc Responder / Skydio X10: This UAS would be dedicated to DFR response to rapidly respond to the scene of an incident and provide real-time video and situational awareness to officers responding to the scene. It would also include the installation of two charging and telecommunications docks on the roof of the Public Safety Building. ~~Within two years, this UAS would be replaced with Flock Alpha UAS and a battery swapping dock.~~

Quantity:

Our initial purchase recommendation for drones is:

- Interior field-deployed: 4 units
- Outdoor field-deployed: 4 units
- DFR: 2 units

Ongoing inventory counts will be updated in the Annual Police Equipment Report as required by BMC 2.100.

Capabilities:

- Interior fielded-deployed UAS are a compact system designed for operation in confined interior spaces. It allows officers to remotely search buildings during high-risk alarms or warrant services, minimizing the need for officers to physically enter potentially hazardous environments without prior visual assessment.
- Outdoor field-deployed UAS are a field-deployed unit carried by patrol officers for immediate operational support. It features high-resolution thermal and zoom sensors ideal for locating missing persons in complex terrain or tracking fleeing suspects to prevent dangerous ground pursuits.
- DFR UAS systems are capable of autonomous dispatch to calls for service, often arriving before ground units. This capability allows for the rapid verification of

incidents, potentially allowing officers to downgrade their response or clear unfounded calls without physical police presence. They provide real-time situational awareness to responding officers and facilitate safer approaches and de-escalation strategies.

Lifespan:

The expected lifespan of the above UAS models is approximately 3 years.

Uses and Effects:

Authorized operators may deploy the UAS in accordance with Unmanned Aerial Systems Use Policy 611.5 Permitted Use and 611.6 Prohibited Use.

How it Works:

Remote controllers would be used to operate each type of UAS. They provide a live video feed and ensure the safe and effective operations of the UAS. Digital media cards would be installed in the UAS and would store the video footage from the flights. The DFR system includes the installation of two charging and telecommunications docks.

Manufacturers' Descriptions:

"DJI Avata 2 is a compact and portable FPV camera drone equipped with built-in propeller guards. The aircraft uses both GNSS and a Vision System, allowing for stable hovering and smooth aerobatic maneuvers while flying both indoors and out."

"Fly with confidence inside thanks to LEMUR 2's hardware and flight software capabilities. Quickly deployable; Shatter glass to breach windows; Stable flight with 360° position hold; Pushes open ajar doors"

"Skydio R10: The ease, durability and low operational cost of small consumer drones popular for indoor use, with the onboard lighting, communications and cloud integrations your mission demands. Launch, command, stream, and upload—everything needed to get the job done, built in."

"The DJI Matrice 4 Thermal drone introduces a compact, intelligent drone for professional use. Equipped with a thermal camera, enhanced sensing, and a laser range finder, this drone offers safer and more reliable operations. The Matrice 4T is ideal for industries including electricity, emergency response, public safety, and forestry conservation."

“Responder: A powerful aerial tool for public safety agencies – built right here in the USA. 42min Flight Time; 40X Total Zoom; 640PX Thermal Camera; 4G Teleoperations”

“Skydio X10: The best sensors for a drone this small, piloted by the most advanced AI in the sky. To get the data you need, wherever and whenever you need it. 45mph Max flight speed. 40min Max flight time. <40sec Deployment time. IP55 Certified against dust and water.”

"The DJI Matrice 4TD is a professional-grade thermal drone designed for rapid, accurate intelligence across utility inspections, solar and wind maintenance, industrial monitoring, public safety, and search-and-rescue missions. Combining high-resolution thermal imaging with a visual camera, this dual-spectrum platform reveals details invisible to conventional sensors, allowing teams to detect overheating equipment, identify hotspots in solar arrays, monitor turbine performance, and locate heat signatures during emergency operations. Rugged, IP-rated construction and extended flight endurance ensure reliable performance in challenging environments, making the M4TD a mission-ready solution for demanding field conditions."

"Flock Alpha sets a new standard for rapid response in public safety. American-made and NDAA-compliant, Flock Alpha is purpose-built for DFR, enhancing speed, coverage area, and camera power in a fully integrated solution."

2. Purpose

The specific purpose or purposes that each type of Controlled Equipment is intended to achieve.

The primary objective of the UAS program is to leverage technology to preserve life and enhance safety.

- By providing an aerial vantage point, the UAS allows officers to create time and distance from a threat. This provides opportunities for negotiation and de-escalation that are not possible when officers are forced to make split-second decisions face-to-face with a suspect.
- The UAS allows for the remote assessment of hazardous scenes (e.g., suspicious devices, armed individuals), reducing the physical risk to officers and bystanders.
- UAS can rapidly clear calls for service (such as unfounded reports), allowing patrol officers to remain available for genuine emergencies and reducing police presence where it is not needed.

3. Fiscal Cost

The fiscal cost of each type of Controlled Equipment, including the initial costs of obtaining the equipment, the costs of each proposed use, the costs of potential adverse impacts, and the annual, ongoing costs of the equipment, including operating, training, transportation, storage, maintenance, and upgrade costs.

The costs below represent estimates. Costs are subject to change at the time of purchase.

Initial Cost:

- Purchase of ~~4 interior and 4 outdoor~~ field-based-deployed UAS (~~Avata 2 & Matrice 4T~~): Total \$44,500-~~\$150,000~~
- Lease of PSB-based DFR (Year 1): \$100,000-~~\$200,000~~
- Radar (Year 1): ~~included-\$0-\$150,000~~
- Dock Installation: ~~\$0~~-\$15,000.

Cost of Use:

- Each individual use of the UAS incurs a negligible financial cost, limited primarily to the electricity required to recharge the aircraft batteries. The operational cost is absorbed within the existing salary of the trained Pilot in Command (PIC) and does not require additional overtime or specialized funding. For the DFR program, the annual lease covers unlimited flights, meaning there is no incremental cost for high-frequency usage.

Costs of Potential Adverse Impacts:

- Costs of adverse impacts could include property damage caused by a malfunctioning drone, but the experience of other agencies with drones and similar programs indicates that such incidents are extremely rare. Furthermore, strict adherence to FAA maintenance schedules, pre-flight inspections, and pilot training requirements serves to minimize the risk of malfunction or operator error. Any costs associated with accidental damage or liability claims would be addressed through the City's existing claims process. Financial risks related to Surveillance Technology Ordinance compliance are minimal given that the City is allowed 90 days to cure any issues.

Annual and Ongoing Costs:

- DFR Lease: \$1~~0025~~,000-~~\$200,000~~ per year (~~includes upgrade to Flock Alpha~~).

BERKELEY POLICE DEPARTMENT BMC 2.100 IMPACT STATEMENT AND POLICY 709 UPDATE – UNMANNED AERIAL SYSTEM

- Radar: \$150,000 per year.
- Parts/Maintenance (for purchased units): \$2,000 per year.

Training Costs:

- Training (4 primary pilots): \$24,000.
- Training (8 additional pilots): \$48,000.

Maintenance and Storage Costs:

- Parts/maintenance for purchased units: \$2,000 per year.
- Parts/maintenance for leased units: included.

Upgrade Costs:

- ~~DFR-UAS hardware~~ upgrades are often included in the lease or purchase agreement. ~~Within two years, this UAS would be replaced with Flock Alpha UAS and a battery-swapping dock.~~

4. Impact

An assessment specifically identifying any potential impacts that the use of Controlled Equipment might have on the welfare, safety, civil rights, and civil liberties of the public.

Welfare and Safety

The use of UAS technology will provide the Berkeley Police Department with an industry-standard tool that significantly enhances operational safety and efficiency. The UAS will improve response times to critical emergencies and calls for service, particularly those hampered by traffic congestion or geographic barriers. By providing rapid, aerial situational awareness, the UAS allows officers to assess threats and locate suspects before physical engagement. This capability allows officers to use time and distance to formulate de-escalation strategies, thereby reducing the likelihood of dangerous encounters for both officers and the community.

Civil Rights and Civil Liberties

The Department acknowledges that UAS operations involve inherent privacy considerations, including the risk of inadvertently capturing footage of private areas (e.g., backyards or through windows) or uninvolved community members. To address this, the Department has established strict prohibitions against random surveillance or targeting

individuals based on protected characteristics. While the aerial vantage point provides critical safety data, the Department's policies prioritize civil liberties by restricting recording to authorized missions and mandating that cameras be diverted away from private spaces when not actively engaged in a call for service, as detailed in the "Mitigations" section below.

5. Mitigations

Specific, affirmative technical and procedural measures that will be implemented to safeguard the public from such impacts.

To safeguard the public's welfare and civil liberties, the Department will implement the following affirmative technical and procedural measures:

- All DFR cameras will be programmed to orient toward the horizon (preventing ground recording) while in transit to a call for service. The camera will only point down upon arrival at the authorized scene.
- All UAS flights are logged, and flight data is auditable. Video data is stored on secure, encrypted servers (Evidence.com) with strict chain-of-custody controls.
- The UAS will not be equipped with facial recognition software or weapons of any kind.
- As required by BMC 2.99 and BMC 2.100, the Department will publish data regarding deployments on an annual basis.
- Information including flight logs and incident type will be published on a publicly accessible transparency portal shortly after the conclusion of a flight, typically within 1 hour after docking.
- The program is subject to review by the Police Accountability Board and approval by the City Council via the Annual Military Equipment Report and the Annual Surveillance Technology Report.

6. Alternatives

Alternative method or methods by which the Police Department can accomplish the purposes for which the Controlled Equipment is proposed to be used, and rationale for selection over alternative methods.

Berkeley-Specific Need Assessment

In response to Council's May 7, 2026 referral, the Department provides the following baseline data.

Aerial need (referral item 5a). Incidents in which an aerial perspective would have been useful cannot be reliably identified from existing records, because the Department has had no aerial capability to measure against and no category in CAD or RMS that captures this need. Two indicators are available. First, Special Response Team operations, which almost always would benefit from aerial or interior drone support, occur roughly 5 to 15 times per year. Second, the approved use policy authorizes drone deployment on a broad range of calls for service, so the limiting factor for the DFR program will be operational capacity (aircraft, docks, pilots, airspace, and weather), not the number of qualifying incidents. The Department will log every deployment by call type shortly after they conclude and in the annual report filed under BMC 2.99.020(2)(d). As data around uses becomes available, the department can assess ongoing need.

External aerial support (5b). The Department has historically encountered delays and availability problems whenever outside aerial support is needed. Each time, staff must contact multiple agencies to find one with an available aircraft or drone team, and support typically arrives two or more hours after the initial request. Because of these delays, the Department often does not request aerial support at all, since it would arrive too late to affect the incident.

Officer safety baseline (5c). The Department's use of force records provide the baseline for assessing officer safety. The program is intended to improve situational awareness before officers arrive, so the Department can deploy exactly the right resources to de-escalate each situation instead of responding prepared for the worst case. In some cases, aerial verification will mean no officer needs to be sent at all. The time and distance afforded to officers by UAS should mean fewer use-of-force incidents, so that count is the most direct available measure. In 2025, the Department recorded 275 use-of-force incidents.

Call-for-service response times (5d). Median response times for 2025 were: Priority 1, 7 minutes; Priority 2, 18 minutes; Priority 3, 54 minutes; Priority 4, 55 minutes. Priority level reflects a combination of call type and call status (in progress, just prior, or cold report). The DFR program is designed to arrive at calls in about 2 minutes, giving the Department aerial awareness of a scene well before ground units can arrive. For lower priority calls, DFR can also confirm whether an incident is ongoing and needs an officer, allowing some calls to be cleared without dispatching a patrol unit. This would ensure more units remain available for deployment.

Crime clearance rates (5e). Clearance rate is the percentage of reported crimes cleared within one year of being reported. Clearance rates for 2025 were: homicide, 100%; felony sexual assault, 32%; robbery, 49%; felony assault, 63%; burglary, 12%; theft, 20%; vehicle theft, 11%; arson, 41%.

No reasonable alternative. The baseline data above shows that the Department's current means of obtaining aerial awareness, and of reaching calls quickly, do not meet the need. Outside aerial support is too slow to be used in most incidents. Ground units take a median of 7 minutes to reach a Priority 1 call and 54 to 55 minutes to reach a Priority 3 or 4 call, while the DFR program is designed to arrive in about 2 minutes and can resolve some lower priority calls without dispatching an officer at all. The alternatives to a Department-operated UAS program are addressed below.

In the absence of a UAS program, the department would be limited to less effective and more costly alternatives. If we were to gain the same level of operational support, we could attempt to increase the amount of officers to match the coverage and responsiveness of aerial support. However, that is not feasible at this time due to well established challenges in hiring and training suitable candidates. It would also not address underlying efficiency issues in that ground-based units lack the elevated perspective needed for efficient searches, crowd monitoring, and scene management, and offer reduced capacity to maintain time and distance for de-escalation. This can heighten the potential for confrontational encounters and diminish effectiveness in pursuits or rapidly evolving incidents.

Additionally, taking no action would leave existing operational challenges unaddressed. The department would continue to rely on outside agencies for aerial support, risking delays in critical moments. Without its own UAS capability, the department would forgo enhancements in officer safety and public protection, while falling behind regional peers who have already adopted this widely accepted and increasingly standard public safety tool.

7. Third Party Dependence

Whether use or maintenance of the Controlled Equipment will require the engagement of third party service providers.

All UAS data will be uploaded and stored on Axon's Evidence.com platform in line with existing departmental protocol for evidence collection. 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.

8. Legal and Procedural Rules

Authorized use must comply with state, federal laws, and Policy 611 Unmanned Aerial System (UAS) Operations.

9. Training

The UAS Supervisor/Program Coordinator will coordinate training of Pilots in Command and Visual Observers. The training course and materials will be approved through the training staff. An approved department instructor will oversee all training. Each training session will be documented and forwarded to the Policy and Training Bureau Sergeant.

Attachment 14

Acquisition Report — Investigative Software

Attachments to ODPa Memorandum Dated October 16, 2026: “Review of BPD
Surveillance Technology Proposals and Policy Revisions”

Background

The Berkeley Police Department (BPD) seeks to implement Investigative Software that enables authorized BPD personnel to search, correlate, and visualize records the Department already maintains or is otherwise authorized to access, in a single secure interface, to support active criminal investigations, serious traffic investigations, and the review of critical incidents and natural disasters.

The Department intends to procure the Investigative Software through a competitive process. The Investigative Software operates above existing approved data sources; it does not itself capture audio, video, location, biometric, or other surveillance data from the public.

Nothing in this report or in the accompanying Surveillance Use Policy modifies, supersedes, or relaxes any provision of any approved Surveillance Use Policy or Police Equipment Use Policy that governs any technology or information source integrated into the Platform. Each integrated source continues to be governed by its own approved policy, including but not limited to that policy's authorized and prohibited uses, retention schedule, data-access rules, data-sharing rules, and oversight requirements. In the event of any conflict between this report or the accompanying Surveillance Use Policy and the approved policy of an integrated source, the more protective provision controls. This report and the accompanying Surveillance Use Policy do not authorize any new collection of data, any new retention of data, any new sharing of data, or any new use of data that would not be permitted under the integrated source's own approved policy.

To the extent that it might be required, this document satisfies the requirements of BMC 2.99 for “publicly-released written report produced prior to acquisition... that includes...” sections covering description, purpose, location, impact, mitigation, data types and sources, data security, fiscal cost, third party dependence and access, alternatives, and experience of other entities of the equipment.

1. Description

Information describing the Surveillance Technology and how it works, including product descriptions from manufacturers

Description:

An Investigative Software is a cloud-hosted software system that sits above existing data sources and provides authorized users a single, audited interface through which to search, link, visualize, and analyze records that today must be queried separately from each source system. The Investigative Software does not itself capture audio, video, location,

biometric, or other surveillance data from the public. It is the layer on top, and not a sensor or collector.

Functionally, an Investigative Software of this category combines two operational layers. The integration layer connects approved internal systems (such as Computer-Aided Dispatch, Records Management, and Digital Evidence Management) and approved external data sources to a common, indexed workspace. The analytics layer provides search, link analysis, case-to-case matching, mapping, timeline construction, and structured workflows over the integrated data, enabling authorized personnel to identify connections among records that would be difficult or impractical to identify through manual cross-system queries.

How it Works:

Approved data sources are connected to the Investigative Software through secure, authenticated integrations (typically encrypted API connections or encrypted data exports). Records from each source are indexed and made searchable through a single interface. When an authorized user runs a query tied to a specific BPD case or incident number, the Investigative Software returns matching records from the connected sources and may display relationships among them. Face Recognition Technology is prohibited.

Manufacturers' Descriptions:

The following are manufacturers' descriptions of investigative software platforms that are representative of a broader range of platforms that are used for the same purposes and are not intended to express a preference for any particular vendor.

"Peregrine's full-stack platform transforms disconnected data into complete operational context. Built around your reality, it puts actionable intelligence in the hands of every person in your organization."

"Flock Nova: Search Once. Act Faster. A real-time investigative and operations platform that helps teams find context, coordinate work, and move cases forward."

"The Mark43 platform enables agencies to operate efficiently across desktop, mobile data terminals (MDT), and mobile devices, providing real-time access to operational data and workflows. The system is designed to be scalable and maintenance-free, supporting secure information sharing and collaboration across public safety teams."

2. Purpose

Information on the proposed purpose(s) for the Surveillance Technology

The proposed purposes of the Investigative Software are limited to:

- Supporting specific and active criminal investigations.

- Supporting serious traffic-related investigations.
- To support police misconduct investigations.
- Responding to and reviewing critical incidents and natural disasters.

Each individual query of the Investigative Software must, in addition, fall within the authorized purposes of the source policy governing the data being queried. The Investigative Software may not be used for any general intelligence-gathering, for monitoring of First Amendment-protected activity, or for any other purpose not enumerated above.

3. Location

The general location(s) it may be deployed and reasons for deployment

The Investigative Software is a cloud-hosted software application. It is not installed at any physical location in public space and does not involve installation of any new hardware in the field. Access is limited to authorized BPD personnel using Department-issued or Department-authorized devices on the Department's network. Connected internal data sources reside on existing Department systems. Connected external data sources, where authorized, reside with their respective owners or operators and are accessed only through the Platform's secure interface.

4. Impact

An assessment identifying potential impacts on civil liberties and civil rights including but not limited to potential disparate or adverse impacts on any communities or groups

Although the Investigative Software itself collects no new data from the public, the aggregation and easier searchability of data already authorized for the Department's access raises civil-rights and civil-liberties considerations that warrant transparent acknowledgment and specific safeguards. The Department identifies the following potential impacts and addresses each through the mitigations described in Section 5 and through the accompanying Surveillance Use Policy.

- Combining records that are each individually permissible to hold can produce a more revealing picture of a person's movements, associations, and activities than any single record. The Investigative Software addresses this by limiting connected data sources to those enumerated in Section 6, by requiring that every query be tied to a specific BPD case or incident, and by auditing all queries.
- BMC 2.99.030(5) prohibits the City from obtaining, retaining, requesting, accessing, or using Face Recognition Technology or information obtained from Face Recognition Technology. Some Investigative Software vendors offer face-comparison, face-matching, or face-clustering features. Any such feature shall be

disabled in the Department's deployment, shall not be enabled by the vendor without explicit Council approval under BMC 2.99, and any inadvertent receipt of Face Recognition output shall be handled in accordance with BMC 2.99.030(5).

- Some underlying data sources reflect historical patterns of police contact, which in Berkeley and elsewhere have not fallen evenly across communities. A tool that makes those records easier to query can, if used carelessly, reinforce those patterns. Mitigations include the case-number-tied query requirement, the prohibition on general intelligence-gathering and dragnet searches in the accompanying Surveillance Use Policy, and the audit-log requirement that records the user, time, source, case number, and reason for each query.
- Investigative Software vendors typically offer the ability to share case data with other participating agencies. Under the accompanying Surveillance Use Policy, the Investigative Software does not create independent authority to share data with any third party; any sharing of data that originates from a connected surveillance technology source is governed by that source's approved Surveillance Use Policy or Police Equipment Use Policy. Berkeley's sanctuary policies, the California Values Act (Gov. Code §§ 7282.5, 7284.2 et seq.), AB 1184, AB 352, AB 1242, SB 345, and BPD Policy 423 therefore continue to govern data accessed through the Platform.
- The Investigative Software permits queries of publicly available open-source data when tied to a specific active investigation. Open-source data can implicate First Amendment-protected activity and produce inaccurate or biased results. The accompanying Surveillance Use Policy addresses this by requiring that every query be tied to a specific case or incident and by prohibiting general intelligence-gathering and dragnet searches.
- Publicly available reporting in 2024 and 2025 has documented that at least one Investigative Software vendor explored sourcing data from data breaches and dark-web marketplaces. The accompanying Surveillance Use Policy prohibits the ingestion of any data the vendor obtained from stolen-data sources, breach-origin sources, or unauthorized aggregations, and requires written vendor representation confirming that no such data is present in the Department's instance.
- There is a risk that integrating multiple technologies into a single platform could implicitly relax the protections in any one technology's existing approved policy. The accompanying Surveillance Use Policy expressly addresses this risk: it does not modify any integrated source's existing policy, and where the Platform's rules and a source's rules conflict, the more protective provision controls.

5. Mitigations

Information regarding technical and procedural measures that can be implemented to appropriately safeguard the public from any impacts identified

The Department will implement the following technical and procedural mitigations, each of which is also embodied in the accompanying Surveillance Use Policy:

- Face Recognition Technology and any face-comparison or face-identification feature shall be disabled and shall not be enabled, used, or queried.
- Every query shall be associated with a specific BPD case number or incident number, a case type, and/or a documented reason, recorded in the Platform's audit log.
- The Investigative Software shall not be configured to ingest, and the Department shall not authorize the ingestion of, any data the vendor obtained from data breaches, dark-web marketplaces, or unauthorized aggregations. Vendor written representation shall be obtained at contract execution.
- Connected data sources are limited to those enumerated in Section 6 of this report.
- For each connected source, the source's existing approved Surveillance Use Policy or Police Equipment Use Policy continues to control. Where the Platform's rules and the source's rules conflict, the more protective rule applies.
- The Investigative Software does not create independent authority to share data with any third party. All third-party data sharing is governed by the approved policy of the connected source from which the data originates.
- The Investigative Software shall be hosted in a CJIS-compliant environment with Multi-Factor Authentication, role-based access controls, and encryption in transit and at rest.
- The Investigative Software shall generate an audit log of every access event.
- All Investigative Software output shall be treated as an investigative lead only and shall be independently corroborated before any enforcement, charging, or detention decision.

6. Data Types and Sources

A list of the sources of data proposed to be collected, analyzed, or processed by the Surveillance Technology, including "open source" data

The Investigative Software does not itself collect data from the public. The Investigative Software analyzes data from the connected sources enumerated below. Each connected source is, at all times, governed by its own approved policy in addition to this policy, and the more protective provision controls. The annual report filed with City Council pursuant to BMC 2.99.020(2)(d) shall include a current list of all data sources connected to the Investigative Software.

Authorized Connected sources

- BPD Computer-Aided Dispatch (CAD) records.
- BPD Records Management System (RMS) reports and supplements.
- BPD Digital Evidence Management System metadata, and case-specific content.
- Automated License Plate Reader (ALPR) data.
- Fixed video camera data.
- Unmanned Aerial Systems (UAS) data.
- Opt-in case-linkage data voluntarily shared by other participating law-enforcement agencies.
- NIBIN (National Integrated Ballistic Information Network) ballistic-evidence data, accessed by federally authorized BPD personnel in connection with firearm investigations.
- Publicly available open-source data.
- Any future surveillance technology approved by Council through the STO process.

Excluded Sources

The following sources shall not be connected to the Platform:

- Face Recognition Technology data.
- Federal immigration enforcement databases, and any data feed whose primary purpose is to support civil immigration enforcement.
- Out-of-state criminal databases queried for the purpose of supporting laws that restrict or criminalize reproductive rights or the provision or receipt of gender-affirming care, consistent with California law.
- Any data the vendor obtained from data breaches, dark-web marketplaces, or unauthorized aggregations. Vendor written representation that no such data is present in the Department's instance shall be obtained at contract execution.

7. Data Security

Information about the steps that can be taken to ensure adequate security measures to safeguard the data collected or generated from unauthorized access or disclosure

The Investigative Software shall use a multi-layered security architecture to preserve the integrity and confidentiality of the data:

- Access shall require secure login credentials with Multi-Factor Authentication (MFA).
- Access shall be restricted to authorized personnel and audited for compliance.
- The storage environment shall comply with CJIS standards.
- Evidentiary data downloaded for investigations shall be stored in the Department's digital evidence system and retained according to state law.
- Vendor obligations including prompt notification of any security incident or data breach, contractual financial penalties for unauthorized disclosures, restrictions on vendor use of City data, and survival of City data-handling protections after contract termination, as set forth in the procurement contract.

8. Fiscal Cost

The fiscal costs for the Surveillance Technology, including initial purchase, personnel and other ongoing costs, including to the extent practicable costs associated with compliance with this and other reporting and oversight requirements, as well as any current or potential sources of funding;

The costs below represent estimates. The anticipated source of funding is the Department's existing operating budget. We expect that the use of this technology, in combination with other investigative and situational-awareness tools, will reduce the need for overtime by improving the efficiency of investigations and real-time response, generating savings that can offset ongoing subscription costs. In addition, we anticipate that vendors may offer this investigative software at reduced or no additional cost when it is bundled with other technology or services already procured by the Department, further limiting the net fiscal impact.

Initial Cost:

- Initial year subscription cost is estimated at \$75,000 to \$150,000, depending on vendor selection, connected source count, and feature set. Funding will be identified through the City's standard budgeting and appropriation processes.

Cost of Use:

- Operational use is absorbed within existing salaries of investigators and analysts. The Investigative Software is intended to reduce the time officers and analysts spend on cross-system queries.

Costs of Potential Adverse Impacts:

- Potential costs include data-breach liability, claims of privacy violation, and litigation costs associated with civil-rights claims. These risks are mitigated by the

contractual financial-penalty clause to be negotiated into the procurement contract, by CJIS-compliant hosting, by the prohibitions on Face Recognition and excluded data sources, and by strict audit and supervisory review.

- Costs of compliance with reporting and oversight requirements: potential costs could arise from data breach litigation or claims of privacy violation. However, the reliance on voluntary consent to access cameras that already are in place as well as strict audit logs minimizes this risk. Strict adherence to the Use Policy will further mitigate liability. The cost of compliance with BMC 2.99 will be absorbed into the existing salary costs of PD staff.

Annual and Ongoing Costs:

- Continued operation beyond the initial year is estimated at \$75,000 to \$150,000 per year, subject to vendor selection and Council appropriation. Any continuation beyond the initial term will require a separate contract authorization by Council.

Training Costs:

- Personnel: The operational cost is absorbed within the existing salary of the investigating officers and this increased efficiency will likely result in time savings. Initial and ongoing training is to be included in the vendor subscription and absorbed into regular in-service training hours.

Maintenance and Storage Costs:

- Maintenance of the Investigative Software is included in the subscription.

Upgrade Costs:

- Software upgrades are included in the annual subscription model.

9. Third Party Dependence and Access

Whether use or maintenance of the technology will require data gathered by the technology to be handled or stored by a third-party vendor on an ongoing basis, and whether a third party may have access to such data or may have the right to sell or otherwise share the data in aggregated, disaggregated, raw or any other formats

The Investigative Software does not create independent authority to share surveillance technology data with any third party. Surveillance technology accessed through the Investigative Software that originates from a connected source may only be shared with any non-City entity in accordance with the approved Surveillance Use Policy or Police Equipment Use Policy that governs that connected source. All restrictions on sharing contained in those approved policies including any applicable provisions regarding sanctuary protections, federal immigration enforcement, out-of-state reproductive-rights

or gender-affirming-care enforcement and vendor disclosure apply to the data when it is accessed through the Platform.

The procurement contract shall provide that the City retains ownership of all of its data and any anonymized derivatives, that the vendor is prohibited from selling, sharing, or distributing City data without explicit City authorization, that the vendor may disclose City data to a government agency only upon a legal request and with the City's written consent, that consistent with the California Values Act and BPD Policy 423 the vendor may not provide City data to federal immigration authorities in response to an administrative subpoena or similar request without a court order, that the vendor must promptly notify the City of any security incident or data breach, and that City ownership and control of its data survives contract termination.

10. Alternatives

A summary and general assessment of potentially viable alternative methods (whether involving the use of a new technology or not), if any, considered before deciding to propose acquiring the Surveillance Technology

Status quo (no platform). Investigators continue to query each source system separately and reconcile results manually. This preserves the strictest separation between systems but materially slows investigations where ballistic, ALPR, and case-report data must be combined quickly, and makes it harder to detect serial offenses that span multiple report categories.

In-house data integration. The City could build its own integration layer across CAD, RMS, and Digital Evidence Management. This option offers maximum control but is fiscally and technically prohibitive within the relevant timeframe and would not, on its own, provide the case-linkage benefits available from opt-in inter-agency data sharing.

11. Experience of Other Entities

To the extent such information is available, a summary of the experience of comparable government entities with the proposed technology, including any unanticipated financial or community costs and benefits, experienced by such other entities

Investigative Software platforms of this category are in use by a range of California and out-of-state agencies, including municipal police departments, county sheriffs, and state-level criminal-justice entities. State-level deployments include statewide criminal-justice data-sharing platforms in at least one state, supported by an analytics vendor in this category.

Publicly available reporting has identified concerns with certain configurations of Investigative Software products in other jurisdictions, including: default-on use of face-matching features in some vendor deployments; reports that one vendor explored sourcing

data from breaches and dark-web marketplaces before publicly stating it would not do so; default-on inter-agency sharing settings, including with federal agencies in apparent violation of state sanctuary laws; and inadequate audit-log review by adopting agencies. The mitigations in this report and the accompanying Surveillance Use Policy are designed specifically to address each of these concerns.

Several California municipalities have adopted public use policies for analogous integration or analytics platforms within the past year. Those policies share certain core features: a defined data-source list, prohibitions on face recognition, mandatory audit logs, and deference to the source-system policies that govern each integrated data source. The Department has reviewed those policies and has incorporated analogous protections in the accompanying Surveillance Use Policy. Where peer policies have been criticized, including by civilian oversight bodies, the principal concerns have been insufficient restriction on inter-agency sharing and lack of explicit prohibitions on stolen-data ingestion. The accompanying Surveillance Use Policy addresses each of these concerns directly by deferring third-party data sharing to the approved policies of the connected sources from which the data originates, and by prohibiting ingestion of any data the vendor obtained from data breaches, dark-web marketplaces, or unauthorized aggregations.

Attachment 15

**Policy 1307 — Surveillance Use Policy—Investigative
Software**

Attachments to ODPa Memorandum Dated October 16, 2026: “Review of BPD
Surveillance Technology Proposals and Policy Revisions”

Berkeley Police Department
Law Enforcement Services Manual

Policy
1307

Berkeley Police Department
Law Enforcement Services Manual

Surveillance Use Policy - Investigative Software

1307.1 PURPOSE

This policy provides guidance for the use of Investigative Software by the Berkeley Police Department (BPD). The purpose of the Investigative Software is to enable authorized BPD personnel to search, correlate, and visualize records that the Department already maintains or is otherwise authorized to access, in support of specific and active criminal investigations, firearm and gun-violence investigations, serious traffic investigations, police misconduct investigations, and review of critical incidents and natural disasters.

The Investigative Software integrates and enables analysis of data from sources that are separately approved under BMC Chapter 2.99 and governed by their own approved Surveillance Use Policies, authorized for the Department's possession or access by state or federal law, or otherwise authorized for the Department's use. The Investigative Software itself does not capture audio, video, location, biometric, or other surveillance data from the public; it is the workspace through which already-authorized data is queried. This policy expressly prohibits querying or sharing data for the purpose of supporting federal civil immigration enforcement or for the purpose of supporting the enforcement of laws that restrict or criminalize reproductive rights, abortion, or the provision or receipt of gender-affirming care.

1307.2 AUTHORIZED USE

Only BPD members who have received training on this policy, on the approved Surveillance Use Policies of the connected sources that the member will access through the Platform, on BPD Policy 423 (Immigration Law), and on applicable state restrictions on reproductive-rights and gender-affirming-care data sharing, and who have then been granted access by an administrator, may access the Platform. Every query shall be associated with a specific BPD case number or incident number, a case type, and/or a documented reason, recorded in the Platform's audit log.

The Investigative Software may only be accessed and used by authorized BPD personnel and such access will be for the following purposes only:

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

Each query of the Investigative Software must, in addition, fall within the authorized purposes of the approved policy that governs the connected source being queried. If a connected source's policy authorizes its data only for specified investigative uses, the Investigative Software shall not be used to query that data for any other use.

Prohibited Uses

The following uses of the Investigative Software are prohibited:

- Use of Face Recognition Technology, or any feature that performs automated or semi-

Berkeley Police Department

Law Enforcement Services Manual

automated identification or verification of an individual based on the individual's face.

- General intelligence-gathering, dragnet searches, or any query that is not tied to a specific BPD case or incident.
- Use to harass, intimidate, or retaliate against any individual or group.
- Querying or sharing data for the purpose of supporting federal civil immigration enforcement. Consistent with BPD Policy 423, state law, and the City's sanctuary ordinance (BMC 13.114), data accessed through the Investigative Software may not be shared with federal immigration authorities except as required by court order, and any such request shall be reported to the Chief of Police and to Council within 10 days.
- Querying or sharing data with law-enforcement agencies from other states for the purpose of supporting the enforcement of laws that restrict or criminalize reproductive rights, abortion, or the provision or receipt of gender-affirming care.
- Use of Investigative Software output as the sole basis for any enforcement action. Platform-generated correlations, links, and matches shall be treated as investigative leads only and shall be independently corroborated before any arrest, detention, or charging decision.
- Any use for personal, political, commercial, or non-law-enforcement purposes.
- Any use that is prohibited by the approved Surveillance Use Policy or Police Equipment Use Policy of a connected source whose data is being queried.

1307.3 DATA COLLECTION AND CONNECTED SOURCES

The Investigative Software does not itself collect data from the public. The Investigative Software analyzes data from the connected sources enumerated below. Each connected source is, at all times, governed by its own approved policy in addition to this policy, and the more protective provision controls. The annual report filed with City Council pursuant to BMC 2.99.020(2)(d) shall include a current list of all data sources connected to the Investigative Software.

Authorized Connected Sources

- BPD Computer-Aided Dispatch (CAD) records.
- BPD Records Management System (RMS) reports and supplements.
- BPD Digital Evidence Management System metadata, and case-specific content.
- Automated License Plate Reader (ALPR) data.
- Fixed video camera data.
- Unmanned Aerial Systems (UAS) data.
- Opt-in case-linkage data voluntarily shared by other participating law-enforcement agencies.
- NIBIN (National Integrated Ballistic Information Network) ballistic-evidence data, accessed by federally authorized BPD personnel in connection with firearm investigations.
- Publicly available open-source data
- Any future surveillance technology approved by Council through the STO process.

Excluded Sources

The following sources shall not be connected to the Platform:

- Face Recognition Technology data.

Berkeley Police Department
Law Enforcement Services Manual

-
- Federal immigration enforcement databases, and any data feed whose primary purpose is to support civil immigration enforcement.
 - Out-of-state criminal databases queried for the purpose of supporting laws that restrict or criminalize reproductive rights or the provision or receipt of gender-affirming care, consistent with California law.
 - Any data the vendor obtained from data breaches, dark-web marketplaces, or unauthorized aggregations. Vendor written representation that no such data is present in the Department's instance shall be obtained at contract execution.

1307.4 DATA ACCESS

Access to the Investigative Software shall be limited to sworn personnel and professional staff whose assignment requires investigative or analytical support, including patrol officers conducting initial investigations, whose access has been approved by the Chief of Police or their designee, who have completed required training and have a current and documented investigative need. A user's access to a connected source through the Investigative Software shall not exceed the access that the user would have to that source directly under the source's own approved policy. The vendor will retain no right access, use, sell or otherwise share Investigative Software data for any purpose without BPD's written consent.

1307.5 DATA PROTECTION

This program shall utilize a multi-layered security architecture to preserve the integrity and confidentiality of the data:

- Access shall require secure login credentials with Multi-Factor Authentication (MFA).
- Access shall be restricted to authorized personnel and audited for compliance.
- The storage environment shall comply with CJIS standards.
- Evidentiary data downloaded for investigations shall be stored in the Department's digital evidence system and retained according to state law.
- Vendor obligations including prompt notification of any security incident or data breach, contractual financial penalties for unauthorized disclosures, restrictions on vendor use of City data, and survival of City data-handling protections after contract termination, as set forth in the procurement contract.

1307.6 CIVIL LIBERTIES AND RIGHTS PROTECTION

To protect against use of the Investigative Software in ways that would violate or infringe upon civil rights or civil liberties, including but not limited to potential disparate or adverse impacts on any community or group, the following safeguards apply:

- Face Recognition Technology is prohibited.
- Every query must be tied to a specific BPD case or incident.
- Investigative Software output shall be treated as an investigative lead only and shall be independently corroborated before any enforcement, charging, or detention decision.
- All other access, retention, sharing, training, and audit provisions of this policy serve to protect against unauthorized use of the Investigative Software and the data accessed through it.

1307.7 DATA RETENTION

Data accessed through the Investigative Software but not downloaded or saved by the Department is not retained by the Department independently of the connected source. The retention schedule of

Berkeley Police Department

Law Enforcement Services Manual

the connected source from which the data was obtained continues to control.

Data downloaded or saved by the Department in connection with a specific case shall be stored in the Department's digital evidence system and retained in accordance with state law and existing Departmental evidence-retention protocols.

1307.8 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 records derived from the Investigative Software shall be processed in the same manner as requests for department public records pursuant to Policy 804. Records that are the subject of a court order or subpoena shall be processed in accordance with the established department subpoena process.

1307.9 THIRD-PARTY DATA-SHARING

The Investigative Software does not create independent authority to share surveillance technology data with any third party. Surveillance technology accessed through the Investigative Software that originates from a connected source may only be shared with any non-City entity in accordance with the approved Surveillance Use Policy or Police Equipment Use Policy that governs that connected source. All restrictions on sharing contained in those approved policies including any applicable provisions regarding sanctuary protections, federal immigration enforcement, out-of-state reproductive-rights or gender-affirming-care enforcement and vendor disclosure apply to the data when it is accessed through the Platform.

The procurement contract shall provide that the City retains ownership of all of its data and any anonymized derivatives, that the vendor is prohibited from selling, sharing, or distributing City data without explicit City authorization, that the vendor may disclose City data to a government agency only upon a legal request and with the City's written consent, that consistent with the California Values Act, BMC 13.114, and BPD Policy 423 the vendor may not provide City data to federal immigration authorities in response to an administrative subpoena or similar request without a court order, that the vendor must promptly notify the City of any security incident or data breach, and that City ownership and control of its data survives contract termination.

1307.10 TRAINING

All BPD members authorized to access the Investigative Software shall receive appropriate training before access is granted, and refresher training not less than annually. Training shall include:

- Use of the Investigative Software.
- This policy and BMC Chapter 2.99.
- The approved Surveillance Use Policy and Police Equipment Use Policy of every connected source that the member will access through the Platform.
- BPD Policy 423 (Immigration Law), BMC 13.114 (Sanctuary Ordinance), the California Values Act, and applicable state restrictions on reproductive-rights and gender-affirming-care data sharing.
- State and federal law on privacy, search and seizure, and the use of analytics in criminal investigations.
- The limitations of Investigative Software output, including the requirement that all Platform-generated correlations be treated as leads and independently corroborated.
- Identification and avoidance of disparate-impact and bias risks.

Records utilized in investigations shall be collected pursuant to Policy 802 (Property and Evidence) and retained pursuant to Policy 804 (Records Maintenance).

Berkeley Police Department
Law Enforcement Services Manual

1307.11 AUDITING AND OVERSIGHT

The Investigative Software generates a site log each time the system is accessed. Audits will be conducted on a regular basis, at least twice a year. As part of the audit, the Offices of Strategic Planning and Accountability (OSPA) will confirm that BPD does not enter any direct data sharing agreements or give direct access to outside agencies.

BPD will enforce against prohibited uses of the Investigative Software 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 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.

1307.12 MAINTENANCE

Maintenance of the Investigative Software shall be provided by the vendor under the procurement contract. Maintenance of integrated internal systems remains the responsibility of the respective system vendors.

Off-Agenda Item 1
Policy Review Status Updates

Updated October 14, 2026



POLICY REVIEW STATUS REPORT

Guiding Authority

Section 125(3)(a)(1) and Section 125(17)(a) of the Berkeley City Charter¹

Case Load Overview

As of October 14, 2026, the Police Accountability Board (PAB) has two (2) active policy reviews. The ODPa has received three (3) additional policy complaints that will present during the October 21, 2026 PAB Meeting.

Policy Review Number	2025-PR-0001
Policy Topic	Contact Between Complaint Subject Officer and Complainant During Calls for Service
Relevant Policy	BPD Policy 1004 "Anti-Retaliation" BPD Policy 1010 "Personnel Complaints"
Status	Open
Date Presented to the PAB	02/19/2025
Anticipated Completion	The review is currently being evaluated to determine the appropriate next steps and timeline for completion.
Assigned To	Chair Cayetano & Board Member Sharma
Summary	
The Complainant reported two interactions with BPD in January 2025, involving officers who were either subjects of their prior complaints to the PAB or involved in other litigation. They expressed concerns about potential retaliation or bias, believing they should not interact with officers they had previously filed complaints against.	
Activity Report	
On September 9, 2026, this policy review was reassigned to Chair Cayetano and Board Member Sharma. ODPa staff has transmitted the material relevant to the review.	

¹ Berkeley City Charter: <https://berkeley.municipal.codes/Charter/125>

Updated October 14, 2026

Policy Review Number	2025-PR-0004
Policy Topic	Public Recording of Police Activity
Relevant Policy	BPD Policy 426 "Public Recording of Police Activity"
Status	Open
Date Presented to the PAB	6/25/2025
Anticipated Completion	The review is currently being evaluated to determine the appropriate next steps and timeline for completion.
Assigned To	ODPA
Summary	
The Complainant expressed concerns with the Berkeley Police Department's General Order D-2, "Public Recording of Police Activity," (now BPD Policy 426) following an incident on June 4, 2025, in which they allege they were physically prevented by three officers from observing and documenting police activity at 8th and Harrison Street. The Complainant argues that the policy fails to clearly affirm the First Amendment rights of onlookers and does not adequately direct officers to limit the use of "police lines" to situations where such restrictions are necessary for officer safety or to protect the integrity of an investigation.	
Activity Report	
On September 23, 2026, the policy complaint was reassigned to ODPA staff after the scope of the review was reevaluated. The PAB requested that PAB complete the review within the next six months per the guidance in its policy manual.	

Off-Agenda Item 2

Legislative Updates Relevant to the PAB's Work



MEMORANDUM

Date: October 16, 2026
To: Honorable Members of the Police Accountability Board
From: Mary Opler, Director of Police Accountability
Jose Murillo, ODPa Policy Analyst
Subject: Legislative Updates

The purpose of this memorandum is to provide a legislative update to the PAB, enabling them to stay informed about changes in local, state, and federal law.

State Legislative Updates¹

The following bills are being proposed in the state of California regarding peace officers:

NAME OF LEGISLATION	STATUS	SUMMARY/PURPOSE
AB 1537 (Bryan) – Peace Officers: Secondary Employment	09/30/26 - Vetoed by Governor.	Prohibits peace officers from engaging in part-time or any other form of secondary employment for the United States (U.S.) Department of Homeland Security (DHS) or any other entity that engages in immigration enforcement
AB 1544 (Krell) – Court proceedings: media access	09/27/26 – Approved by the Governor. Chaptered by Secretary of State - Chapter 520, Statutes of 2026.	Clarifies and strengthens public access rights to court proceedings by prohibiting officials from restricting entry to open court settings—except as necessary to maintain order—makes violations enforceable under the Bane Act, and affirms that existing access rights are not limited or reduced.

¹ <https://post.ca.gov/Status-of-Current-Legislation>

AB 1627 (Avila Farias) - Public employment: disqualifications	09/29/26 - <i>Approved by the Governor. Chaptered by Secretary of State - Chapter 739, Statutes of 2026.</i>	Disqualifies a person previously employed by the United States Immigration and Customs Enforcement (ICE) or specified out-of-state corrections departments, during specified time periods, from being employed as a peace officer
AB 1896 (Gonzalez) – Public employment: disqualifications	09/30/26 - <i>Vetoed by Governor.</i>	Amends various existing laws relating to disqualification from public employment, minimum standards relating to peace officers, and adds certain criteria for an individual employed by an entity that engaged in immigration enforcement on or after January 20, 2025, to January 20, 2029, except as provided, among other provisions.
AB 2347 (Ahrens) – Commission on Peace Officer Standards and Training: hate crime training and guidelines	05/14/2026 - <i>In committee: Held under submission.</i>	Requires the Peace Officer Standards and Training Commission (POST) to conduct a comprehensive review of hate crimes training programs and adopt evidence-based training requirements to fill any gaps in the handling of hate crimes, as specified.
SB 691 (Wahab) – Body-worn cameras: policies	09/20/26 - <i>Approved by the Governor. Chaptered by Secretary of State. Chapter 416, Statutes of 2026.</i>	This bill requires, on or before July 1, 2027, each law enforcement agency that has a body-worn camera policy to update that policy to include a procedure for emergency service personnel to request, prior to any public release, the redaction of evidentiary and nonevidentiary recordings of a patient undergoing medical or psychological evaluation, procedure, or treatment by emergency service personnel.
SB 1105 (Perez) – Law Enforcement	09/30/26 - <i>Vetoed by the Governor. In Senate. Consideration of Governor's veto pending.</i>	Current law grants limited arrest authority—and in some cases peace officer status—to federal law enforcement under specific conditions. This bill removes those authorities and prohibits California agencies from participating in joint task forces involving profiling, while requiring

	Attorney General approval and compliance standards for interagency agreements.
--	--

Additional legislation pertaining to public safety in the state of California may be monitored here: <https://legiscan.com/CA/legislation> . ODPa staff will continuously monitor new legislation and update the PAB throughout the year.

The BPD’s Policy and Training Bureau issues an annual legislative update that summarizes legal changes impacting law enforcement. Unless stated otherwise, the changes outlined in the updates took effect in January of the corresponding year. The following BPD Policies include the legislative updates for 2026.

SOURCE	LINK
BPD Policy 1507 “2026 Legislative & Case Law Update”	https://berkeleyca.gov/sites/default/files/2026-02/RELEASE_20260127_T171031_Berkeley%20PD%20Policy%20Manual.pdf#Page=1061
The California Peace Officers Association also provides a yearly California Legislative and Legal Digest.	https://cpoa.org/wp-content/uploads/2024/11/2025-Legislative-Legal-Digest.pdf

Lexipol Policy Updates

The following Lexipol policies have been updated since the PAB’s October 7, 2026 meeting:

BPD POLICY	DESCRIPTION OF CHANGES
1203 “Smoking Ordinance – Chapter 12.70 BMC”	Updates wording, punctuation, formatting, and street-name references in the smoking pollution control policy.
321 “Standards of Conduct”	Revises Section 321.5.6 regarding unauthorized disclosure of confidential or protected information, including language prohibiting disclosure of a human trafficking victim’s name, address, or image except as authorized by law. Also makes minor formatting and terminology corrections.
601 “Sexual Assault Investigations”	Removes references to Bay Area Women Against Rape (BAWAR), including the specific requirement to notify BAWAR when a victim is transported to Highland Hospital for a forensic medical examination. Retains the victim-

	advocate advisement and notification to Highland’s Sexual Assault Response Team. Revises victim-rights and confidentiality language and DNA database references.
419 “Field Training Officer Program”	Changes the timing for issuing the Field Training Manual from before Orientation Training to the beginning of the Orientation Training Phase. Updates gender-neutral terminology and makes minor punctuation corrections.

Berkeley City Council & Council Committee Meeting Updates

The following items are under consideration by the City Council or its committees and are relevant to the PAB:

October 27, 2026 Regular City Council Meeting

Item #	Item Description	Recommendation
5	Contract No. 32500002 Amendment: Community Initiatives Live Free USA for Gun Violence Intervention and Prevention Services	Authorize a contract amendment adding \$257,548 in Byrne State Crisis Intervention Program grant funding, bringing the total not-to-exceed amount to \$2,874,768; extending the term through December 31, 2027; and updating the scope of services and budget.
7	Contract: Insight Public Sector, Inc. dba Aurelian for Non-Emergency Call-Taking Software	Authorize a contract for non-emergency call-taking software and services for the Emergency Communications Center, from December 1, 2026 through April 30, 2028, in an amount not to exceed \$197,642.
13	Revenue Grant: California Office of Traffic Safety (OTS) for the 2026–2027 “Selective Traffic Enforcement Program (STEP)” Grant	Authorize acceptance of a \$200,000 OTS grant for October 1, 2026 through September 30, 2027, and execution of related revenue agreements and amendments. Funding supports BPD traffic enforcement overtime, related benefits, equipment, and training.

Off-Agenda Item 3
List of Remaining 2026 PAB Meetings

Remaining 2026 Police Accountability Board Meetings

City of Berkeley – Police Accountability Board

The following are the remaining scheduled Police Accountability Board meetings for calendar year 2026, based on the 2026 PAB Meeting Calendar.

Meeting Date
October 21, 2026
November 4, 2026
December 9, 2026