BERKELEY CITY COUNCIL PUBLIC SAFETY COMMITTEE
SPECIAL MEETING

Tuesday, June 2, 2026
2:00 PM

2180 Milvia Street, Berkeley, CA 94704

Teleconference Location – 16 Garden Street, Cambridge, MA 02138

Committee Members:

Councilmembers Rashi Kesarwani, Shoshana O'Keefe, and Brent Blackaby
Alternate: Mayor Adena Ishii

This meeting will be conducted in a hybrid model with both in-person and virtual attendance. Attend this meeting remotely using Zoom. To request to speak, use the "raise hand" function in Zoom. To join by phone: Dial **1-669-254-5252 or 1-833-568-8864 (Toll Free)** and enter **Meeting ID: 165 580 2142**. To provide public comment, Press *9 and wait to be recognized by the Chair. To submit a written communication for the Committee's consideration and inclusion in the public record, email policycommittee@berkeleyca.gov. All Committee meetings are recorded.

This meeting will be conducted in accordance with the Brown Act, Government Code Section 54953. Any member of the public may attend this meeting, however, if you are feeling sick, please do not attend the meeting in person.

Pursuant to the City Council Rules of Procedure and State Law, the presiding officer may remove, or cause the removal of, an individual for disrupting the meeting. Prior to removing an individual, the presiding officer shall warn the individual that their behavior is disrupting the meeting and that their failure to cease their behavior may result in their removal. The presiding officer may then remove the individual if they do not promptly cease their disruptive behavior. "Disrupting" means engaging in behavior during a meeting of a legislative body that actually disrupts, disturbs, impedes, or renders infeasible the orderly conduct of the meeting and includes, but is not limited to, a failure to comply with reasonable and lawful regulations adopted by a legislative body, or engaging in behavior that constitutes use of force or a true threat of force.

California Government Code Section 84308 (Levine Act) Parties to a proceeding involving a license, permit, or other entitlement for use are required to disclose if they made contributions over $500 within the prior 12 months to any City employee or officer. Parties and participants with a financial interest are prohibited from making more than $500 in contributions to a decisionmaker for the 12 months after the final decision is rendered on the proceeding. The above contribution disclosures and restrictions do not apply when the proceeding is competitively bid, or involves a personnel or labor contract. For more information, see Government Code Section 84308.

AGENDA

Roll Call

Minutes for Approval

Draft minutes for the Committee's consideration and approval.

1. Minutes - March 23, 2026

Committee Action Items

The public may comment on each item listed on the agenda for action as the item is taken up. The Chair will determine the number of persons interested in speaking on each item. Up to ten (10) speakers may speak for two minutes. If there are more than ten persons interested in speaking, the Chair may limit the public comment for all speakers to one minute per speaker. Speakers are permitted to yield their time to one other speaker, however no one speaker shall have more than four minutes.

Following review and discussion of the items listed below, the Committee may continue an item to a future committee meeting, or refer the item to the City Council.

2. Surveillance Technology Ordinance Submissions for Community Video Streams and Investigative Software, Pursuant to Council Direction of May 7, 2026 *(Item contains supplemental material)*
From: City Manager
Referred: May 7, 2026
Due: October 22, 2026
Recommendation: Adopt a Resolution to:
1. Accept the Surveillance Acquisition Report and approve the Surveillance Use Policy (BPD Policy 1306) for Community Video Streams, pursuant to Berkeley Municipal Code (B.M.C.) Chapter 2.99.
2. Accept the Surveillance Acquisition Report and approve the Surveillance Use Policy (BPD Policy 1307) for Investigative Software, pursuant to B.M.C. Chapter 2.99.
Financial Implications: See Report
Contact: Jennifer Louis, Police, (510) 981-5900

Unscheduled Items

These items are not scheduled for discussion or action at this meeting. The Committee may schedule these items to the Action Calendar of a future Committee meeting.

- **None**

Items for Future Agendas

- **Requests by Committee Members to add items to the next agenda**

Adjournment

~~~~~~

Written communications addressed to the Public Safety Committee and submitted to the City Clerk Department will be distributed to the Committee in advance of the meeting and retained as part of the official record.

This meeting will be conducted in accordance with the Brown Act, Government Code Section 54953 and applicable Executive Orders as issued by the Governor that are currently in effect. Members of the City Council who are not members of the standing committee may attend a standing committee meeting even if it results in a quorum being present, provided that the non-members only act as observers and do not participate in the meeting. If only one member of the Council who is not a member of the committee is present for the meeting, the member may participate in the meeting because less than a quorum of the full Council is present. Any member of the public may attend this meeting. Questions regarding public participation may be addressed to the City Clerk Department (510) 981-6900.

COMMUNICATION ACCESS INFORMATION:
This meeting is being held in a wheelchair accessible location. To request a disability-related accommodation(s) to participate in the meeting, including auxiliary aids or services, please contact the Disability Services specialist at ada@berkeleyca.gov, (510) 981-6418 (V), or (510) 981-6347 (TDD) at least three business days before the meeting date. Attendees at public meetings are reminded that other attendees may be sensitive to various scents, whether natural or manufactured, in products and materials. Please help the City respect these needs.

~~~~~~

I hereby certify that the agenda for this meeting of the Standing Committee of the Berkeley City Council was posted at the display case located near the walkway in front of the Maudelle Shirek Building, 2134 Martin Luther King Jr. Way, as well as on the City's website, on May 29, 2026.

Mark Numainville, City Clerk

Communications

Communications submitted to City Council Policy Committees are on file in the City Clerk Department at 2180 Milvia Street, 1st Floor, Berkeley, CA, and are available upon request by contacting the City Clerk Department at (510) 981-6908 or policycommittee@berkeleyca.gov.

01

BERKELEY CITY COUNCIL PUBLIC SAFETY COMMITTEE
SPECIAL MEETING MINUTES

Monday, March 23, 2026
2:00 PM

2180 Milvia Street Berkeley, CA 94704

Teleconference Location – 1619 Edith Street, Berkeley CA 94703

Committee Members:

Councilmembers Rashi Kesarwani, Shoshana O'Keefe, and Brent Blackaby
Alternate: Mayor Adena Ishii

This meeting will be conducted in a hybrid model with both in-person and virtual attendance. Attend this meeting remotely using Zoom. To request to speak, use the "raise hand" function in Zoom. To join by phone: Dial **1-669-254-5252 or 1-833-568-8864 (Toll Free)** and enter **Meeting ID: 160 131 2385**. To provide public comment, Press *9 and wait to be recognized by the Chair. To submit a written communication for the Committee's consideration and inclusion in the public record, email policycommittee@berkeleyca.gov. All Committee meetings are recorded.

This meeting will be conducted in accordance with the Brown Act, Government Code Section 54953. Any member of the public may attend this meeting, however, if you are feeling sick, please do not attend the meeting in person.

Pursuant to the City Council Rules of Procedure and State Law, the presiding officer may remove, or cause the removal of, an individual for disrupting the meeting. Prior to removing an individual, the presiding officer shall warn the individual that their behavior is disrupting the meeting and that their failure to cease their behavior may result in their removal. The presiding officer may then remove the individual if they do not promptly cease their disruptive behavior. "Disrupting" means engaging in behavior during a meeting of a legislative body that actually disrupts, disturbs, impedes, or renders infeasible the orderly conduct of the meeting and includes, but is not limited to, a failure to comply with reasonable and lawful regulations adopted by a legislative body, or engaging in behavior that constitutes use of force or a true threat of force.

California Government Code Section 84308 (Levine Act) Parties to a proceeding involving a license, permit, or other entitlement for use are required to disclose if they made contributions over $500 within the prior 12 months to any City employee or officer. Parties and participants with a financial interest are prohibited from making more than $500 in contributions to a decisionmaker for the 12 months after the final decision is rendered on the proceeding. The above contribution disclosures and restrictions do not apply when the proceeding is competitively bid, or involves a personnel or labor contract. For more information, see Government Code Section 84308.

MINUTES

Roll Call: 2:04 p.m.

Present: Kesarwani, O'Keefe, Blackaby

Minutes for Approval

Draft minutes for the Committee's consideration and approval.

1. Minutes - February 19, 2026
Action: M/S/C (O'Keefe/Blackaby) to approve the February 19, 2026 minutes.
Vote: All Ayes.

Committee Action Items

The public may comment on each item listed on the agenda for action as the item is taken up. The Chair will determine the number of persons interested in speaking on each item. Up to ten (10) speakers may speak for two minutes. If there are more than ten persons interested in speaking, the Chair may limit the public comment for all speakers to one minute per speaker. Speakers are permitted to yield their time to one other speaker, however no one speaker shall have more than four minutes.

Following review and discussion of the items listed below, the Committee may continue an item to a future committee meeting, or refer the item to the City Council.

2. Resolution Rescinding Resolution No. 51,408-N.S. Restricting the Use of Air Support and Canine Units And Updating Mutual Aid Policies
From: Councilmember Kesarwani (Author)
Referred: November 17, 2025
Due: May 26, 2026
Recommendation: Adopt a resolution to rescind Resolution No. 51,408-N.S. which currently restricts the use of helicopters and police canine units by the Berkeley Police Department (BPD) and to update policies authorizing BPD to deploy these resources through mutual aid agreements directly with external agencies. The revised policy framework will replace the prior requirement for City Manager approval with post-deployment notification, ensuring rapid and effective responses during critical incidents. The policy will continue to explicitly prohibit the use of canines for crowd control.
Financial Implications: See report
Contact: Rashi Kesarwani, Councilmember, District 1, (510) 981-7110
Action: 11 speakers. M/S/C (Blackaby/O'Keefe) to send the item with a Qualified Positive recommendation to Council that includes: 1) clarifying Section 3(a) to more clearly define the purposes for which the canine team may be deployed, and 2) attaching the communication from the Police Accountability Board to the agenda item for consideration by the full City Council.
Vote: All Ayes.

Unscheduled Items

These items are not scheduled for discussion or action at this meeting. The Committee may schedule these items to the Action Calendar of a future Committee meeting.

- **None**

Items for Future Agendas

- **None**

Adjournment

Action: M/S/C (O'Keefe/Blackaby) to adjourn the meeting.
Vote: All Ayes.

Adjourned at 2:59 p.m.

I hereby certify that the foregoing is a true and correct record of the Public Safety Committee meeting held on March 23, 2026.

_____
Wendy Sorensen, Assistant City Clerk

Communications

Communications submitted to City Council Policy Committees are on file in the City Clerk Department at 2180 Milvia Street, 1st Floor, Berkeley, CA, and are available upon request by contacting the City Clerk Department at (510) 981-6908 or policycommittee@berkeleyca.gov.

02

ACTION CALENDAR

June 30, 2026

To: Honorable Mayor and Members of the City Council

From: Paul Buddenhagen, City Manager

Submitted by: Jennifer Louis, Chief of Police

Subject: Surveillance Technology Ordinance Submissions for Community Video Streams and Investigative Software, Pursuant to Council Direction of May 7, 2026

RECOMMENDATION

Adopt a Resolution to:

1. Accept the Surveillance Acquisition Report and approve the Surveillance Use Policy (BPD Policy 1306) for Community Video Streams, pursuant to Berkeley Municipal Code (B.M.C.) Chapter 2.99.
2. Accept the Surveillance Acquisition Report and approve the Surveillance Use Policy (BPD Policy 1307) for Investigative Software, pursuant to B.M.C. Chapter 2.99.

CURRENT SITUATION AND ITS EFFECTS

On May 7, 2026, the City Council took action on a package of public safety technology items, including several items subject to the Surveillance Technology Ordinance (STO). With respect to Community Video Streams, the Council referred the Surveillance Acquisition Report and Surveillance Use Policy to the Public Safety Policy Committee (PSPC) for further review prior to Council action. With respect to Investigative Software, the Council directed the Berkeley Police Department (BPD), in consultation with the Police Accountability Board (PAB), to initiate an RFP process for each of the components included in the technology package and for their integration.

Under the STO, no surveillance technology subject to B.M.C. Chapter 2.99 may be acquired, used, or made the subject of an agreement until the City Council has accepted a Surveillance Acquisition Report and approved a Surveillance Use Policy for that technology.

Approval of these use policies and acquisition reports does not signify commitment to any single vendor, nor does it limit council's ability to make edits to the use policies or acquisition report prior to granting contract authority.

BACKGROUND

The STO requires the City Manager to submit a Surveillance Acquisition Report and obtain Council approval of a Surveillance Use Policy prior to acquiring, using, or

entering into agreements involving surveillance technology. Each Surveillance Use Policy must address the twelve elements set forth in B.M.C. 2.99.020(4): purpose; authorized use; data collection; data access; data protection; civil liberties and rights protection; data retention; public access; third-party data-sharing; training; auditing and oversight; and maintenance.

Community Video Streams (Policy 1306). The Community Video Streams integration enables authorized BPD personnel to access video footage from privately-owned cameras that have been voluntarily registered and shared with the Department by their owners. Cameras remain owned and controlled by community members, who may revoke access at any time. BPD does not own, install, or maintain the cameras. The integration allows authorized personnel to virtually canvass areas for evidence and gain real-time situational awareness during in-progress incidents without the cost of installing new City-owned cameras. The Surveillance Use Policy addresses each of the twelve elements required by B.M.C. 2.99.020(4) and includes a pre-integration review process to verify camera placement and field of view before any feed is connected.

Investigative Software (Policy 1307). Investigative Software is a query-layer platform that enables authorized BPD personnel to search, correlate, and visualize records the Department already maintains or is otherwise authorized to access. Authorized connected sources will include Computer-Aided Dispatch records, Records Management System reports, digital evidence metadata, Automated License Plate Reader data, fixed video camera data, Unmanned Aerial Systems data, National Integrated Ballistic Information Network data, opt-in case-linkage data from participating agencies, publicly available open-source data, and any future surveillance technology approved by Council under the STO. The Platform does not itself capture audio, video, location, biometric, or other surveillance data from the public; it analyzes data already collected through other approved means. The Surveillance Use Policy expressly prohibits Face Recognition Technology, general intelligence-gathering or dragnet queries, queries not tied to a specific BPD case or incident, queries or sharing in support of federal civil immigration enforcement, and queries or sharing in support of out-of-state laws restricting reproductive rights or gender-affirming care. The policy further provides that for any query, the more protective provision of either Policy 1307 or the Use Policy for a connected source, where one exists, controls.

RATIONALE FOR RECOMMENDATION

Adoption of the recommended Resolution completes the STO process for both Community Video Streams and Investigative Software. Both technologies have been designed and described in their respective documents to meet the civil liberties and rights protections required by B.M.C. Chapter 2.99, including the prohibition on Face Recognition Technology, restrictions on use in support of federal civil immigration enforcement consistent with the California Values Act and BPD Policy 423, and restrictions on use in support of out-of-state laws restricting reproductive rights or the provision or receipt of gender-affirming care.

ENVIRONMENTAL SUSTAINABILITY AND CLIMATE IMPACTS

There are no identifiable environmental effects or climate impacts associated with the act of adopting this resolution.

FISCAL IMPACTS OF RECOMMENDATION

None as a direct result of this action. Contract authority for Community Video Streams and for Investigative Software will be requested separately, following completion of the procurement process.

CONTACT PERSON

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

ATTACHMENTS

1. Resolution
2. Surveillance Acquisition Report- Community Video Streams
3. BPD Policy 1306: Surveillance Use Policy- Community Video Streams
4. BPD Policy 355: Community Video Streams
5. Surveillance Acquisition Report- Investigative Software
6. BPD Policy 1307: Surveillance Use Policy- Investigative Software

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

RESOLUTION ACCEPTING SURVEILLANCE ACQUISITION REPORTS AND APPROVING SURVEILLANCE USE POLICIES FOR COMMUNITY VIDEO STREAMS AND INVESTIGATIVE SOFTWARE

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

WHEREAS, the Surveillance Technology Ordinance requires the City Council to accept a Surveillance Acquisition Report and approve a Surveillance Use Policy prior to the acquisition or use of any surveillance technology subject to the ordinance, or to entering into an agreement to acquire, share, or otherwise use such technology or the information it provides; and

WHEREAS, on May 7, 2026, by Resolution No. 72,254–N.S., the City Council referred the Surveillance Acquisition Report and Surveillance Use Policy for Community Video Streams to the Public Safety Policy Committee for further review prior to Council action; and

WHEREAS, on May 7, 2026, by Resolution No. 72,254–N.S., the City Council directed the City Manager to initiate, in consultation with the Police Accountability Board and the Berkeley Police Department, a Request for Proposals process for each of the components of the public safety technology proposal and for their integration; and

WHEREAS, the Berkeley Police Department has prepared and submitted Surveillance Acquisition Reports and Surveillance Use Policies for Community Video Streams and Investigative Software addressing each of the twelve elements required by B.M.C. 2.99.020(4); and

NOW, THEREFORE, BE IT RESOLVED by the Council of the City of Berkeley that:

1. The Surveillance Acquisition Report for Community Video Streams is hereby accepted, and the Surveillance Use Policy for Community Video Streams (BPD Policy 1306) is hereby approved, pursuant to B.M.C. Chapter 2.99.
2. The Surveillance Acquisition Report for Investigative Software is hereby accepted, and the Surveillance Use Policy for Investigative Software (BPD Policy 1307) is hereby approved, pursuant to B.M.C. Chapter 2.99.

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 descriptions are provided by Flock Safety, which is one vendor capable of delivering this integration.

"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."

"Registering your camera lets law enforcement know you have footage that could help during a criminal investigation. Places a pin on your local law enforcement's camera map... Integrating your business cameras gives law enforcement secure, live access to video streams and the ability to download footage when it's needed as evidence, or for a real-time crisis response."

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.

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.

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 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. Hardware costs and integration costs are paid by the private camera owners.

Initial Cost:

- Hardware: $0 (Cameras are owned by private entities).
- Software Integration: Estimated $30 per stream per year paid by camera owners.
- For the first four years of integration, operating costs are covered through the department's existing agreement with Flock for the FlockOS platform. Thereafter, the annual subscription cost is estimated to be $65,000.

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.

Annual and Ongoing Costs:

- No ongoing costs are incurred by the Department.

Training Costs:

- 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.

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

In December 2025, the City of Oakland City Council voted 7-1 to approve a similar program under their "Community Safety Camera Systems" policy. OPD has established strict governance that explicitly prohibits the use of the technology for facial recognition, harassment, or immigration enforcement.

Regional jurisdictions like Alameda County, Vacaville, and Elk Grove also utilize fixed surveillance cameras and video integration as tools for public safety and crime deterrence which reflects a regional standard for the use of such technology in modern policing. San Francisco has publicized substantial public safety benefits associated with this technology used in concert with drones as a first responder and automated license plate readers.

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.

(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 federal 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.

1306.3 DATA COLLECTION

Data collection is limited to camera footage and associated metadata voluntarily provided by community members. 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 Streams Policy. 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.

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 1306.4 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.

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.

Evidentiary data downloaded for investigations is stored in the Department's digital evidence system. Once downloaded, data is retained in accordance with state law and existing Departmental evidence retention protocols.

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

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 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.

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 biennial. 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.

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 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 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.

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

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.

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.

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. Once downloaded, data is retained in accordance with state law and existing Departmental evidence retention protocols.

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

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.

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.

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 biennial. 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.

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 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.

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.

“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.

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 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.

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.

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:

- 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.

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-

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 policies, 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.

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.

1307.4 DATA ACCESS

Access to the Investigative Software shall be limited to BPD personnel 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.

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 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 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), 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).

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 biennial. 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.

ADENA ISHII
MAYOR OF BERKELEY

2180 Milvia Street
Berkeley, CA 94704
Tel: (510) 981-7100
TDD: (510) 981-6903
mayor@berkeleyca.gov

REVISED AGENDA MATERIAL
for Supplemental #2

Meeting Date: March 24, 2026

Item Number: 26

Item Description: Public Safety Technology: Surveillance Technology Ordinance and Police Equipment Ordinance Approvals, Policy Updates, and Contract Authority

Submitted by: Mayor Adena Ishii (Co-Author), Councilmember Cecilia Lunaparra (Co-Author), and Councilmember Igor Tregub (Co-Sponsor)

This supplemental material aims to balance the value of surveillance technology with Berkeley's commitment to privacy, civil liberties, and Sanctuary City status. Additionally, in response to reported security failures in neighboring jurisdictions, this supplemental clarifies how these technologies work and codifies legislative intent. These recommendations stem from comprehensive community engagement, feedback from the Police Accountability Board (PAB), and extensive conversations with the Office of the Director of Police Accountability and the Berkeley Police Department. In light of these considerations, this item refers the Community Video Stream (CVS) acquisition report and surveillance use policy to the Public Safety Committee for review; recommends limiting the retention period for non-evidentiary footage and strengthening oversight for Unmanned Aerial Systems (UAS); increase auditing and reporting cadence for Fixed Cameras in Surveillance Use Policy; and explicitly opposes the renewal, approval, or authorization of any contract with Flock Safety.

The original item requests authorization for acquisition, use, and/or contracting of the following technologies: Unmanned Aerial System (UAS), Community Video Stream (CVS), Fixed cameras, Investigative software, and Automatic License Plate Readers. The following table summarizes this supplemental’s recommendations.

	Approve/approve with amendments	Refer back to Staff	Reject
Unmanned Aerial System (UAS)	✓Surveillance Use Policy ✓Military Equipment Use Policy	↩Acquisition Report ↩Military Equipment Impact Statement	✗Flock Contract
Community Video Stream (CVS)	—	↩Acquisition Report ↩Surveillance Use Policy	✗Flock Contract
Fixed cameras	✓Surveillance Use Policy	—	✗Flock Contract
Investigative software	—	—	✗Flock Contract
Automatic License Plate Readers (ALPR)	—	—	✗Flock Contract

Proposed revisions and recommendations:

Surveillance Technology Ordinance (BMC 2.99)

1. **Refer the Community Video Stream Acquisition Report and Surveillance Use Policy to the Public Safety Policy Committee (PSPC) for further review; request that the City Manager work at the committee level to address the PAB's concerns and clarify operational ambiguity:**
   This is the first time this item has been presented to the Berkeley City Council. Given the unknown operational implications, additional clarification and feedback are advantageous for a more robust understanding. During review at the PSPC, staff should address the following Police Accountability Board[1] recommendations and authors' questions:

   a. Add an explicit prohibition on surveillance of First Amendment activity, unless there is a clear, articulable, and imminent public safety threat that is actively occurring;
   b. Specify concrete data retention periods with the four elements required by BMC 2.99.020.4(g);
   c. Conduct a disparate impact analysis addressing whether camera coverage is concentrated in areas with particular demographic characteristics;
   d. Supplement Section 11 of the Acquisition Report to disclose adverse findings from comparable jurisdictions;
   e. Update immigration-related search reporting to match the 72-hour

[1]https://berkeleyca.gov/sites/default/files/2026-03/March%2018%2C%202026%20PAB%20Recommendations_Surveillance%20Tech.pdf

standard and named recipients in Policy 351 section 351.6 per our Sanctuary City Ordinance;

f. Consider developing a use policy to address combined cross-platform use of all integrated technologies, regardless of vendor used, including ALPR, fixed cameras, community video streams, and drones;
g. Institute semiannual audits of CVS–similar to Council directive on fixed cameras established in July 2025[2];
h. Analyze the data governance and security risks of community camera integration.

2. **Amend the Surveillance Use Policy for the Unmanned Aerial System to include the following provisions:**

   a. **Reduce the non-evidentiary drone footage retention period to five (5) days**
   Pursuant to the proposed UAS surveillance use policy, uses of the UAS are limited to de-escalation, tactical safety, emergency response, operational efficiency related to calls for services, and investigation. As a result, much of the footage captured by drones is responsive, not passive, and therefore distinct from other surveillance technologies and retention timelines. To balance data security with operational efficiency, we propose a reduced footage retention period of five (5) days, aligning with Oakland's policy.

   b. **Amend audit timelines to require a monthly audit and a semiannual audit report**
   Require monthly audits with a semiannual (twice a year) published audit report. The PAB recommended a monthly audit to ensure potential violations are caught early. The City Council directed staff to change the audit report timeline from biennial (once every two years) to semiannual at their July 2025 meeting.[3] These audits should be sent to the PAB.

   c. **Add supervisory approval for all UAS deployments except for DFR**
   To enhance internal oversight for drone use, supervisory approval for all deployment protocols should be added. DFR protocols may be excluded from these specific service constraints to maintain operational speed.

   d. **Specify authorized use cases**
   It is important to reduce ambiguity around when a UAS deployment is permitted. Accordingly, this supplemental material proposes amending the language from "Authorized operators may deploy the UAS in the following circumstances" to: "Authorized operators ***shall only*** deploy the UAS in the

[2] https://berkeleyca.gov/sites/default/files/city-council-meetings/2025-07-22%20Annotated%20Agenda%20-%20Council.pdf
[3] https://berkeleyca.gov/sites/default/files/city-council-meetings/2025-07-22%20Annotated%20Agenda%20-%20Council.pd,

following circumstances."

e. **Refer to the City Manager to develop defined performance metrics to measure and report on the efficacy of the technology**
BPD should develop performance metrics aligned with the goals of the use policy to better evaluate the technology's effectiveness. The performance metrics should relate to the stated goals of the technology and should quantify the program's success in:
   i. Operational efficiency: Reducing officer overtime.
   ii. Personnel safety: Enhancing officer protection.
   iii. Crime mitigation: Deterring both violent and non-violent offenses.
   iv. Investigative success: Improving clearance rates and solving crimes.

f. **Refer to the City Manager to create a consolidated UAS operations and data governance policy**
Consolidate Policies 611 and 1303 to create a single UAS Operations and Data Governance Policy to ensure clear lines of accountability and enhance document and version control.

g. **Refer to the City Manager the UAS Surveillance Acquisition Report for research and analysis of alternative surveillance technology vendors capable of meeting the City of Berkeley's safety and surveillance needs while balancing the need for privacy and civil liberties protections**
The UAS Surveillance Acquisition Report references Flock technology. As a result, this supplemental material recommends referring the report to the City Manager to identify alternative vendors. The accompanying Use Policy is recommended for approval with the recommendations enumerated in bullet 2.

Provisions 2f, 2g, and 2h may be taken up after Council approval of the UAS Surveillance Use Policy.

3. **Amend the Surveillance Use Policy for Fixed Cameras to include the following provision:**
   a. **Amend audit timelines to require a monthly audit and a semiannual audit report**
   Require monthly audits with a semiannual (twice a year) published audit report. The PAB recommended a monthly audit to ensure potential violations are caught early. The City Council directed staff to change the audit report timeline from biennial to semiannual at their July 2025 meeting.[4] The monthly audit reports should be shared with the PAB.

[4]https://berkeleyca.gov/sites/default/files/city-council-meetings/2025-07-22%20Annotated%20Agenda%20-%20Council.pd,

Police Equipment Ordinance (2.100)

4. **Amend the UAS Equipment Use Policy to include the same revisions as the recommendations for the UAS Surveillance Use Policy.**
    - **a.** Reduce footage retention period to five (5) days
    - **b.** Amend audit timelines to require a monthly audit and a semiannual audit report
    - **c.** Add supervisory approval for all deployments except for DFR
    - **d.** Establish a thorough protocol for decertification
    - **e.** Specify authorized use cases

5. **Refer the following request for information to the City Manager to quantify the need for UAS**
   Provide Berkeley-specific data to prove "no reasonable alternative" exists. The following should be considered:
    - **a.** Frequency of incidents for which aerial perspective has historically been needed by call type
    - **b.** Documented historical delays/availability issues when relying on external aerial support
    - **c.** Establish baseline officer injury rates and documented officer safety issues relevant to articulated use cases (quantitative, not just qualitative)
    - **d.** Baseline Call-For-Service (CFS) response time data by call type
    - **e.** Baseline crime clearance rate data by crime type

Approval of the UAS Equipment Use Policy is not contingent upon completion of 5a-5e.

6. **Refer the UAS Military Equipment Impact Statement to the City Manager for research and analysis of alternative surveillance technology vendors capable of meeting the City of Berkeley's safety and surveillance needs while balancing privacy and civil liberties protections**
   The UAS Military Equipment Impact Statement references Flock technology. As a result, this supplemental material recommends referring the report to the City Manager to identify alternative vendors. (The accompanying but distinct UAS Equipment Use Policy is recommended for approval, subject to incorporation of revisions enumerated in recommendation #4 above.)

Contract Authority

7. **Reject any renewal, authorization, approval, or execution of the Flock Safety contract**
   Flock's violations are numerous. In recent years, at least 30 jurisdictions have paused or terminated their Flock contracts due to concerns about impermissible data sharing with federal law enforcement agencies, including federal immigration enforcement agencies.[5] Within California, at least 7 jurisdictions

[5]https://www.npr.org/2026/02/17/nx-s1-5612825/flock-contracts-canceled-immigration-survillance-concerns

have deactivated their cameras or canceled their contracts with Flock. Most alarmingly, in Ventura, CA, an audit found that "out-of-state agencies accessed the Ventura County Sheriff's Office's data more than 364,000 times between February and March [2025] without the department's approval or knowledge."[6] The Sheriff's Office in Ventura County confirmed that it had disabled the "National Look Up" feature within the Flock system, in order to comply with California law, but that the feature had been reactivated without any notice or explanation from Flock.[7]

Several Bay Area cities, including Santa Cruz, Mountain View, and Los Altos Hills, have paused their flock cameras after "discovering that federal agencies could search the camera data, despite the firm's assurances otherwise."[8] The Mountain View Police Department stated in a January 2026 news release that several federal law enforcement agencies accessed its ALPR system data through the use of the "nationwide" search setting that was turned on by Flock without Mountain View Police Department's permission or knowledge[9]. In Los Altos Hills, the City Council voted to "remove its Flock Safety automated license plate reader cameras around town, citing concerns about data privacy, cost considerations, and overall effectiveness."[10] In each of these cities, Flock made contractual commitments to its clients and failed to abide by them.

As a Sanctuary City, the repeated violations of Flock contract terms pose a risk to the community, including but not limited to Berkeley's immigrant residents.

Single-vendor consolidation introduces additional risks. In its March 18, 2026, letter to the City Council, the PAB explains that while there can be operational benefits to a single vendor ecosystem, there are also significant risks in integrating surveillance data and creating dependency on one private company.

Additional Recommendations

8. **Refer to the City Manager to amend Ordinance 2.99 to include a violation/termination clause for surveillance technology vendors.** Establish enforceable mechanisms to sanction surveillance technology vendors for misuse, unauthorized access, or data security failures.

9. **Refer to the City Manager and City Attorney additional contractual language to require a vendor to inform the City of any request for**

[6] https://www.cbsnews.com/losangeles/news/flock-license-plate-readers-shared-data-with-out-of-state-federal-agencies/
[7] *Ibid.*
[8] https://localnewsmatters.org/2026/02/11/alameda-county-flock-cameras-privacy-debate/
[9] https://www.cbsnews.com/sanfrancisco/news/mountain-view-alpr-cameras-use-suspended-automated-license-plate-reader/
[10] https://www.losaltosonline.com/news/los-altos-hills-to-remove-alpr-cameras/article_59f90aa8-14c1-4309-9f7f-12d16c649d9e.html

information (including but not limited to subpoenas, discovery requests, or requests under any federal or state statute to the extent permitted by law) it receives related to City-controlled data and safeguard it to the fullest extent allowed by law.

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

APPROVING SURVEILLANCE TECHNOLOGY, ~~AND~~ POLICE EQUIPMENT ORDINANCE REQUIREMENTS, AND , ~~UPDATED~~ USE POLICIES, ~~AND AUTHORIZING CONTRACTS WITH FLOCK SAFETY~~ FOR PUBLIC SAFETY TECHNOLOGY

~~WHEREAS, the City of Berkeley has adopted BMC 2.99, the Surveillance Technology Ordinance, which requires City Council approval of a Surveillance Acquisition Report and Surveillance Use Policy prior to the acquisition or use of new surveillance technology; and~~

~~WHEREAS, the City of Berkeley has adopted BMC 2.100, the Police Equipment Ordinance, which requires City Council approval of a Police Equipment Impact Statement and Police Equipment Use Policy for controlled military equipment, consistent with AB 481; and~~

~~WHEREAS, the Drone as First Responder (DFR) portion of the Unmanned Aerial Systems program constitutes both a new surveillance technology under BMC 2.99 and controlled military equipment under BMC 2.100, and the Police Department has prepared and published the required Surveillance Acquisition Report, Surveillance Use Policy, Impact Statement, and Police Equipment Use Policy for Council review; and~~

~~WHEREAS, Community Video Streams constitute a new surveillance technology under BMC 2.99, and the Police Department has prepared and published the required Surveillance Acquisition Report and Surveillance Use Policy for Council review; and~~

~~WHEREAS, fixed video cameras were previously approved by Council, and updated Surveillance Use Policies reflecting Council-directed revisions are presented for approval; and~~

~~WHEREAS, the Police Department held a community information session on January 15, 2026, to present and gather feedback on the full suite of public safety technologies, and the Police Accountability Board has had an opportunity to review and provide input on each technology through multiple public meetings; and~~

~~WHEREAS, the City Council accepted the Byrne State Crisis Intervention Program (SCIP) grant award of $1,000,000 on July 29, 2025, which identified investigative software as an eligible expenditure, and Flock Nova falls within that allocation; and~~

~~WHEREAS, the City's existing Flock Safety ALPR contract expires in July 2026, and renewal authority is required to maintain continuity of service; and~~

~~WHEREAS, the City Attorney's Office has negotiated a Master Services Agreement with Flock Safety that includes protections for City data ownership, restrictions on federal access consistent with the City's sanctuary policies, financial penalties for unauthorized~~

~~disclosures, security incident notification requirements, and post-termination data protections, and Flock Safety has accepted every revision proposed by the City Attorney's Office; and~~

~~WHEREAS, funding for the technology suite will come from eliminating up to 6 sworn officer positions, as supported by the Berkeley Police Association, resulting in a net savings to the General Fund; funding for fixed cameras is available in the General Fund allocation designated for surveillance cameras; funding for Flock Nova is available from the BSCC SCIP grant with no General Fund impact; and~~

~~WHEREAS, all prices meet or are below those listed for the same products on the Omnia cooperative purchasing consortium, satisfying the City's competitive procurement requirements; and~~

~~WHEREAS, Flock Safety has offered a 10% discount on new product lines if contracts are executed by the end of March 2026, representing over $100,000 in savings.~~

WHEREAS, the original staff recommendation for Item 26 requested authorization for the acquisition and use of multiple surveillance technologies and the execution of a master services contract with Flock Safety; and

WHEREAS, over the past year, documented security failures and unauthorized data-sharing incidents involving Flock Safety in jurisdictions such as Mountain View and Ventura County have raised significant concerns regarding the vendor's ability to comply with Berkeley's stated goals; and

WHEREAS, the original item requests authorization for acquisition, use, and/or contracting of the following technologies: Unmanned Aerial System (UAS), Community Video Stream (CVS), Fixed cameras, Investigative software, and Automatic License Plate Readers (ALPRS); and

WHEREAS, the revised material recommends that the City Council approve the amended UAS Surveillance Use Policy, the amended UAS Military Equipment Use Policy, and the amended Fixed Camera Surveillance Use Policy; and

WHEREAS, the revised material recommends that Council refer to staff the UAS Acquisition Report and UAS Military Equipment Impact Statement to identify alternative vendors other than Flock Safety; and

WHEREAS, the revised material recommends that Council refer to staff the CVS Acquisition Report and the CVS Surveillance Use Policy for further review and feedback by the Public Safety Policy Committee; and

WHEREAS, the revised material recommends that Council reject any contract renewal, authorization, approval, or execution with Flock Safety.

NOW THEREFORE, BE IT RESOLVED by the Council of the City of Berkeley as follows:

Surveillance Technology Ordinance Approvals

1. The City Council hereby accepts the Surveillance Acquisition Report and approves the amended Surveillance Use Policy for the Unmanned Aerial Systems program.

2. ~~The City Council hereby accepts the Surveillance Acquisition Report and approves the Surveillance Use Policy for Community Video Streams.~~

3. The City Council hereby approves the updated Surveillance Use Policies for fixed video cameras.

Police Equipment Ordinance Approvals

4. The City Council hereby ~~accepts the Police Equipment Impact Statement and~~ approves the Police Equipment Use Policy for unmanned aerial systems.

5. BE IT FURTHER RESOLVED that the Berkeley City Council directs the following referrals to the City Manager for action:

    a. Refer the Community Video Stream Acquisition Report and Surveillance Use Policy to the Public Safety Policy Committee (PSPC) for further review; request that the City Manager work at the committee level to address the PAB's concerns and clarify operational ambiguity.

    b. Refer the UAS Surveillance Acquisition Report to the City Manager for research and analysis of alternative surveillance technology vendors capable of meeting the City of Berkeley's safety and surveillance needs while balancing privacy and civil liberties protections.

    c. Refer the UAS Military Equipment Impact Statement to the City Manager for research and analysis of alternative surveillance technology vendors capable of meeting the City of Berkeley's safety and surveillance needs while balancing privacy and civil liberties protections.

    ~~a.~~d. Refer to the City Manager to amend Ordinance 2.99 to include a violation/termination clause for surveillance technology vendors.

Contract Authority

BE IT FURTHER RESOLVED that the Berkeley City Council finds it in the public interest to reject any renewal, authorization, approval, or execution of a contract with Flock Safety.

~~4. The City Manager is authorized to amend the existing Contract #32400088 with Flock Group, Inc. (Flock Safety) to add Drone as First Responder hardware, software, and services for an initial three-year term, in an amount not to exceed $750,000.~~

~~5. The City Manager is authorized to amend the existing Contract #32400088 with Flock Group, Inc. (Flock Safety) to add fixed surveillance cameras for an initial four-year term, in an amount not to exceed $310,000, with an option to extend for one additional three-year term, for a total amount not to exceed $600,000.~~

~~6. The City Manager is authorized to amend the existing Contract #32400088 with Flock Group, Inc. (Flock Safety) to add Nova investigative software for a one-year term, in an amount not to exceed $75,000, funded by the Byrne State Crisis Intervention Program (SCIP) grant.~~

~~7. The City Manager is authorized to amend the existing Contract #32400088 with Flock Group, Inc. (Flock Safety) to renew Automated License Plate Readers (ALPRs) for a two-year term, in an amount not to exceed $330,000, with an option to extend for an additional two-year term, for a total amount not to exceed $660,000.~~

~~BE IT FURTHER RESOLVED that the total aggregate amount authorized under items 5 through 8 of this Resolution shall not exceed $1,465,000 for the initial contract terms, and shall not exceed $2,085,000 in the event all optional extension terms are exercised, with no individual contract term extending beyond seven years from the date of execution.~~

~~BE IT FURTHER RESOLVED that the City Manager is authorized to execute any amendments to the above contracts and the Master Services Agreement with Flock Safety, provided that any amendments do not increase the total amounts authorized herein and are consistent with the approved Use Policies and Impact Statements.~~

~~BE IT FURTHER RESOLVED that the authorized sworn officer strength of the Berkeley Police Department is hereby reduced by 3 full-time equivalent positions, effective July 1, 2026, with the resulting salary and benefit savings to fund the ongoing technology subscription costs authorized herein, the Senior Crime Analyst conversion, and the permanent funding of the Crime Analyst position that is currently grant-funded.~~

~~BE IT FURTHER RESOLVED that grant funds received under the SCIP grant and used for the Flock Nova contract shall not be used to supplant expenditures controlled by this body.~~

The foregoing Resolution was adopted by the Berkeley City Council on March 24, 2026, by the following vote:

Ayes: Bartlett, Blackaby, Humbert, Kesarwani, Lunaparra, O'Keefe, Taplin, Tregub, and Ishii.

Noes: None.

Absent: None.

_____
Adena Ishii, Mayor

Attest: _____
Mark Numainville, City Clerk

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 ~~may~~ 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 active criminal activity at mass gatherings or special events.

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 ~~60~~ 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 ~~biennial~~ audits of UAS use. A report of these audits shall be published semiannually 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.

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.

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 ~~may~~ 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 active criminal activity at mass gatherings or special events.

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.

611.8 RETENTION REQUIREMENTS

UAS footage should be purged by BPD within 5 ~~60~~ days if it doesn't contain any data of evidentiary value. If the data has evidentiary value, it should be uploaded into BPD's evidence database and kept pursuant to the established retention guidelines set forth in policy 804-Records Maintenance and Release.

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.

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 location

- 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.

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

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

351.5.1 EVIDENTIARY INTEGRITY

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

Electronic trails, including encryption, digital masking of innocent or uninvolved individuals to preserve anonymity, authenticity certificates and date and time stamping, shall be used as appropriate to preserve individual rights and to ensure the authenticity and maintenance of a secure evidentiary chain of custody.

351.6 RELEASE OF VIDEO IMAGES

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

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

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

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

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

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 Flock, 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.

351.7 VIDEO SURVEILLANCE AUDIT

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

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.

(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 City of Berkeley encrypted servers. License plate and facial recognition data hardware is not installed on the cameras and may not be installed or used unless approved by the City council. Audio is a standard feature of the camera, but is deactivated by the system administrator and may not be activated or used unless approved by the City Council. 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. Access to the data must be obtained through the Public Works Department according to this policy and published regulations that limit access and use of data by Public Works and other City Departments and personnel. All system access including system log-in, access duration, and data access points is accessible and reportable and shall be documented by the Public Works Department's authorized administrator. All relevant recordings that are utilized will be collected pursuant to Policy 802, Property and Evidence, and retained pursuant to Policy 804 Records and Maintenance.

1304.6 CIVIL LIBERTIES AND RIGHTS PROTECTION

The Berkeley Police Department is dedicated to the most efficient utilization of its resources and services in its public safety endeavors. The Berkeley Police Department recognizes the need to protect its ownership and control over shared information and to protect the privacy and civil liberties of the public, in accordance with federal and state law. Provisions of this policy, including

1304.4 Data Access, 1304.5 Data Protection, 1304.7 Data Retention, 1304.8 Public Accessand 1304.9 Third Party Data Sharing serve to protect against any unauthorized use of video surveillance camera data. License plate and facial recognition data hardware is not installed on the cameras. Audio is a standard feature of the camera, but is deactivated by the system administrator. These procedures ensure the data is not used in a way that would violate or infringe upon anyone's civil rights and/or liberties, including but not limited to potentially disparate or adverse impacts on any communities or groups.

1304.7 DATA RETENTION

Video surveillance recordings are not government records pursuant to California Government Code 34090 in and of themselves. Except as otherwise permitted in this section, video surveillance recordings shall be purged within one hundred and eighty (180) days of recording. Recordings of incidents involving use of force by a police officer or involving detentions, arrests, or recordings relevant to a formal or informal complaint against a police officer shall be retained for a minimum of two years and one month. Recordings relating to court cases and complaints against BPD sworn officers that are being adjudicated will be manually deleted at the same time other evidence associated with the case is purged in line with the Department's evidence retention policy. Any recordings related to BPD administrative proceedings pursuant to this section shall be maintained until such matter is fully adjudicated, at which time it shall be deleted in line with the Department's evidence retention policy, and any applicable orders from the court. All data will automatically delete after the aforementioned retention period by the System Administrator from Public Works.

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

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 with laws governing evidence;
(b) Other law enforcement personnel as part of an active criminal investigation;
(c) Recorded video images that are the subject of a court order or subpoena shall be processed in accordance with the established department subpoena process

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

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.

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

May 22, 2026

VIA ELECTRONIC MAIL [Email]

Public Safety Policy Committee
PolicyCommittee@berkeleyca.gov
2180 Milvia Street, 1st Floor
Berkeley, CA 94704

Re: PAB Request to Defer Action on Investigative Software Acquisition Report and Proposed Surveillance Use Policy (Policy 1307)

Honorable Members of the Public Safety Policy Committee:

At its meeting on May 20, 2026, the Police Accountability Board voted to request that the Public Safety Committee defer action on the Berkeley Police Department (BPD) Investigative Software Acquisition Report and proposed Surveillance Use Policy (Policy 1307) pending completion of the competitive procurement process the council initiated on May 7, 2026. BPD has represented that the City Attorney's office has advised that compliance with the Surveillance Technology Ordinance is not required for the Investigative Software — a platform that would aggregate data from ALPRs, fixed cameras, drones, and other surveillance systems into a single searchable interface. The Board takes no position on that legal question, but if that is correct, there is no legal deadline driving approval of this policy at this time, and deferral would carry no compliance risk.

On the other hand, advancing the report and policy prior to the initiation of the competitive procurement process directed by the City Council at its May 7 meeting could inadvertently codify system design choices before that process has had the opportunity to surface what Berkeley's requirements should be. Ultimately, some of these requirements should inform the development of policy. As one example, the policy as currently drafted authorizes connection to "opt-in case-linkage data voluntarily shared by other participating law-enforcement agencies" (Section 1307.3) but specifies no technical requirements for how the platform must screen that inbound data to ensure it doesn't import information Berkeley is prohibited from using. The city and community would be better served by a policy that provides more specificity as to that case-linkage process –

the type of specificity that will be identified through the development of an RFP and subsequent vendor analysis.

Sincerely,

Joshua Cayetano

Joshua Cayetano, Chair
Police Accountability Board

Cc: Paul Buddenhagen, City Manager
David White, Deputy City Manager
Jennifer Louis, Chief of Police
Jen Tate, Deputy Chief of Police
Katherine Lee, Interim Director of Police Accountability