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.

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. Community Video Streams is estimated to cost $65,000 annually, and Investigative Software is estimated to cost $75,000 annually, though those costs are sometimes lowered or waived when bundled with other products.

POLICY COMMITTEE RECOMMENDATION

On June 2, 2026, the Public Safety Policy Committee (PSPC) adopted the following action: M/S/C (Blackaby/O'Keefe) to provide feedback to the Berkeley Police Department regarding the proposed Community Video Streams and Investigative Software Surveillance Use Policies with the following requested revisions and clarifications:

1. Clarify how participating camera locations will be verified and address liability considerations if cameras are moved.
2. Develop a process for notifying camera owners when their camera footage is accessed.
3. Remove vendor-specific references from the acquisition report.

4. Clarify policies governing access to real-time/live video monitoring and the circumstances under which such access is authorized.
5. Provide additional information regarding the use of artificial intelligence and ensure human oversight of investigative decisions.
6. Identify data sources used by the investigative software and consider including such information in annual reporting.
7. Clarify which personnel will be authorized to access the investigative software.
8. Strengthen audit provisions to verify authorized use of the software.
9. Incorporate revisions contained in the supplemental materials, including the 72-hour immigration-related language.
10. Clarify that the Community Video Streams program does not include audio recording.
11. Clarify retention periods and liability considerations associated with retained data.

Vote: All Ayes.

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 (CVS), 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.

The Department submitted both technologies to PSPC for committee-level review. PSPC considered both items on June 2, 2026: Community Video Streams as directed by the May 7 Council referral, and Investigative Software offered by the Department to provide a parallel opportunity for committee review and feedback. The substantive results of that review and the corresponding updates the Department proposes to make to the acquisition reports, use policies, and forthcoming RFP are described in the section "Public Safety Policy Committee Review and Proposed Updates" below and detailed in the attached supplemental staff responses.

Both technologies will be part of the forthcoming RFP, which will also include drones, automated license plate readers, and fixed PTZ cameras, with vendors able to make a submission for any single technology or for a combination. As such, this item remains several steps removed from any actual procurement. To avoid confusion, the Department notes that the acquisition reports name and quote example products, but only as representative illustration: B.M.C. 2.99 requires that the reports include a product description, and staff has used a representative example as a template. Actual product specifications will be determined through the RFP process.

The Department is bringing this matter to the City Council at this time for two main reasons:

- To provide additional public meetings for Council members and the community to hear about the technologies, ask questions, and provide guidance.

- To ensure that the RFP process on these items is clear from the start about what Council expectations will be before any contracting occurs.

This item is one step in the STO process; it does not finalize policies, decide specific vendors, or grant contract authority. Council retains the ability to make edits to the use policies or acquisition reports prior to granting contract authority for either technology.

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

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, as well as public identification of integrated cameras.

Investigative Software

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, 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.

Public Safety Policy Committee Review and Proposed Updates

Following PSPC's June 2, 2026 review, the Department proposes updates that respond to the items previously identified in the Mayor's supplemental memorandum[1] referring CVS to PSPC, and to additional items raised by the Committee during its review of both technologies. The complete staff responses are attached.

RFP and Programmatic Updates

- At the request of the PSPC, the Department will include in the RFP a request for vendors to describe the feasibility of notifying camera owners each time BPD personnel access their feed. This is not a minimum requirement for vendor selection but will be evaluated as a value-added feature that could enhance owner trust and program transparency.

- The Department's approach to AI features in any integrated system is defined by intended use rather than by technical architecture. The Department's intent, applied regardless of the underlying technology, is that no investigative action be initiated or executed without affirmative human review and authorization, and that any AI-generated output be treated as an investigative lead only, requiring independent corroboration before any enforcement, charging, or detention decision. These principles will be operationalized through the RFP, which will require vendors to describe how their system supports human-in-the-loop operation and to identify any actions the system is capable of performing without real-time human authorization.

- Liability questions referred to the City Attorney's Office. Staff has referred two liability questions arising from the Committee's review to the City Attorney's Office: (1) whether a standing direct integration changes the liability or records analysis when BPD accesses footage a camera owner has retained beyond BPD's own retention period, as compared to obtaining the same footage through traditional physical canvassing; and (2) the City's exposure during any period in which it unknowingly received a stream from a camera that had been repositioned to capture a protected area, assuming prompt disconnection upon discovery. Staff will report the City Attorney's response to Council in the appropriate venue.

[1] https://berkeleyca.gov/sites/default/files/2026-05/2026-05-07%20BAC_Flock_Supplemental_Item26_5_07_2026Meeting.pdf

Acquisition Report and Surveillance Use Policy Updates

The department has proposed updated policy language in redline in the attached STO documents to accomplish the following:

- To generalize references in the CVS acquisition report and to clarify that no vendor selection has been made or is implied.
- To require prompt disconnection of any integrated camera found to have been repositioned to capture an area where a reasonable expectation of privacy exists.
- To clarify that real-time access to live video streams is permitted only when there is an active CAD incident or call for service; the associated incident number must be entered in the system log prior to initiating live viewing, and access shall terminate upon closure of that incident.
- To expressly prohibit the integration of any audio capture or transmission through the CVS system, consistent with the Department's intent that the system handle video only.
- To require that the annual report filed with City Council pursuant to B.M.C. 2.99.020(2)(d) include a current list of all data sources connected to the Investigative Software.
- To include 72-hour federal-disclosure language for cross-policy consistency with Policy 351.6, covering instances in which federal agencies are provided with BPD-owned data held by a vendor, alongside the existing ten-day reporting requirement for federal immigration access requests.
- To require that, as part of each audit, OSPA review a sample of system access logs to verify that queries were associated with a valid case or incident number, conducted by an authorized user, and consistent with the authorized uses enumerated in the policy.
- To clarify the audit cadence will be “twice a year”.

RATIONALE FOR RECOMMENDATION

Adoption of the recommended Resolution completes the STO process for both Community Video Streams and Investigative Software and reflects the results of PSPC's June 2, 2026 review and the updates described above. 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. Approval of these use policies and acquisition reports does not signify commitment to any single vendor and does not limit Council's ability to make edits to the use policies or acquisition reports prior to granting contract authority.

ENVIRONMENTAL SUSTAINABILITY AND CLIMATE IMPACTS

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

CONTACT PERSON

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

ATTACHMENTS

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

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, on June 2, 2026, the Public Safety Policy Committee reviewed the Surveillance Acquisition Report and Surveillance Use Policy for Community Video Streams as referred by the Council, as well as the Surveillance Acquisition Report and Surveillance Use Policy for Investigative Software submitted by the Department for committee review, and the Department has revised those documents to reflect the Committee's review as described in this item and in the attached supplemental staff responses; 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

WHEREAS, these Surveillance Acquisition Reports and Surveillance Use Policies may require further refinement after the Police Department selects a vendor that responds to the Request for Proposals; and

WHEREAS, the City Council retains discretion to request that the Police Department make further edits to the Use Policies and Acquisition Reports after the City selects a vendor and before the City grants contract authority for either technology.

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" (BMC 2.99.030(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.~~ The following are manufacturers' descriptions of investigative software platforms that are representative of a broader range of platforms that are used for the same purposes and are not intended to express a preference for any particular vendor.

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

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

2. Purpose

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

The proposed purpose of accessing community video streams is to provide real-time awareness and investigative capacity in following use cases:

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

3. Location

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

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

- Integration will be prioritized for cameras owned by businesses and non-residential commercial property owners in major thoroughfares and districts, such

as the Elmwood, Solano, Telegraph, Fourth Street, and Downtown business districts.

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

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

4. Impact

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

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

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

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

5. Mitigations

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

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

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

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

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

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

6. Data Types and Sources

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

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

7. Data Security

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

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

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

8. Fiscal Cost

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

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

Initial Cost:

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

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

Annual and Ongoing Costs:

- ~~No ongoing costs are incurred by the Department.~~Annual subscription cost for the platform to integrate the streams is estimated to be $65,000.

Training Costs:

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

Maintenance and Storage Costs:

- Maintenance of the software platform is included in the subscription.

Maintenance of physical cameras is the responsibility of the private owners.

Upgrade Costs:

- Software upgrades are included in the annual subscription model.

9. Third Party Dependence and Access

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

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

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

The CVS integration is provided through a third-party platform vendor, but the Department maintains no standing pool of community video stream data with the vendor: non-evidentiary video remains on the camera owner's system, and the Department retains footage only when it is downloaded as evidence, after which it is held in the Department's own digital evidence system and governed by the Department's evidence-retention and immigration policies. The vendor may access the data only to operate the platform. No non-City entity, including any federal agency, is

granted direct access to the camera registry or video feeds; a non-City law enforcement agency may obtain only retained evidentiary footage through standard evidence sharing protocols with pre-authorization from the Investigations Captain, and only for a specific active criminal investigation supported by valid legal process, with any recipient bound by this policy, the Department's Immigration Law Policy, and the bar on using the footage to enforce other states' laws restricting reproductive or gender-affirming care.

10. Alternatives

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

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

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

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

A final alternative would be not acquiring access to community video streams. Without this technology, the Department would forgo enhancements in investigative efficiency and would continue to rely on slower, manual methods that may result in the loss of critical evidence or loss of available personnel power.

11. Experience of Other Entities

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

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

Policy
1306

Berkeley Police Department
Law Enforcement Services Manual

Surveillance Use Policy - Community Video Streams

1306.1 PURPOSE

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

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

1306.2 AUTHORIZED USE

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

Community video streams may be accessed and reviewed by authorized BPD personnel for the following purposes:

(a) To support specific and active criminal investigations.

(b) To support serious traffic-related investigations.

(c) To support police misconduct investigations, and

(d) To respond to and review critical incidents or natural disasters.

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

The following are prohibited uses of the video surveillance system:

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

(b) Community video streams shall not intentionally be used to invade the

privacy of individuals or observe areas where a reasonable expectation of privacy exists.

(c) Community video streams shall not be used in an unequal or discriminatory manner and shall not target protected individual characteristics including, but not limited to race, ethnicity, national origin, religion, disability, gender or sexual orientation.

(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.

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

(h) Community video streams shall not capture or transmit audio; any camera integrated into the Department's system must be configured for video only.

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

1306.3 DATA COLLECTION

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

1306.4 DATA ACCESS

Access to community video streams data shall be limited to BPD personnel utilizing the camera database for uses described above and pursuant to the Community Video Streams Policy. BPD members seeking access to the video surveillance system shall obtain the approval of the Investigations Division Captain, or their designee. Members accessing the database must follow the necessary logging mechanisms, such as case number and case type when querying the database.

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

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

1306.5 DATA PROTECTION

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

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

1306.6 CIVIL LIBERTIES AND RIGHTS PROTECTION

The Berkeley Police Department is dedicated to the most efficient utilization of its resources and services in its public safety endeavors. The Berkeley Police Department recognizes the need to protect its ownership and control over shared information and to protect the privacy and civil liberties of the public, in accordance with federal and state law. Provisions of this policy, including 1306.2 Authorized Use, 1306.4 Data Access, 1306.5 Data Protection, 1306.7 Data Retention, 1306.8 Public Access, 1306.9 Third Party Data Sharing, and 1306.13 Pre-Integration Review serve to protect against any unauthorized use of community video streams. The use of facial recognition technology on any community video stream is prohibited. These procedures ensure the data is not used in a way that would violate or infringe upon anyone's civil rights and/or liberties, including but not limited to potentially disparate or adverse impacts on any communities or groups. The Department will assess after implementation whether the distribution of integrated cameras reflects a pattern that could suggest a disparate impact, and will address any such pattern identified through the ordinance's Annual Report.

1306.7 DATA RETENTION

The Department acknowledges that the Community Video Stream integration relies on

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

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

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

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

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

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

1306.8 PUBLIC ACCESS

Data collected by the Department and used in a police report shall be made available to the public in accordance with D~~d~~epartment 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 D~~d~~epartment 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 D~~d~~epartment 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.

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

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

1306.10 TRAINING

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

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

1306.11 AUDITING AND OVERSIGHT

The community video streams software generates a site log each time the system is accessed. The video surveillance software generates a site log each time the system is accessed. The site log is broken down by server, device, user or general access. The site log is kept on the server for two years and is exportable for reporting. Community video stream audits will be conducted on a regular basis, at least ~~biennial~~twice a year. As part of the audit, OSPA will confirm that BPD does not enter any direct data sharing

agreements or give direct access to outside agencies. A log of any instance of when surveillance footage has been shared, including date, time, reasons for search, and any recipient agencies. As part of each audit, OSPA shall review a sample of system access logs to verify that queries were associated with a valid case or incident number, conducted by an authorized user, and consistent with the authorized uses enumerated in this policy.

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

The audit shall be documented in the form of an internal department memorandum to the Chief of Police. The memorandum shall include any data errors found so that such errors can be corrected. After review by the Chief of Police, the memorandum and any associated documentation shall be 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.

1306.12 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.

1306.13 MAINTENANCE

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

1306.14 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.
4.5. Upon discovery that an integrated camera has been repositioned to capture an area where a reasonable expectation of privacy exists, the Department shall immediately pause that camera's integration until the camera is positioned in compliance with this policy.

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.
- Upon discovery that an integrated camera has been repositioned to capture an area where a reasonable expectation of privacy exists, the Department shall immediately pause that

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

355.4 VIDEO SUPERVISION

Access to community video streams camera data shall be limited to Berkeley Police Department (BPD) personnel utilizing the camera database for uses authorized above, with technical assistance from Public Works Department and Department of Information Technology personnel. Information may be shared in accordance with Sections 355.6 or 1304.9 below. BPD members seeking access to the camera system shall obtain the approval of the Investigations Division Captain, or their designee.

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

355.4.1 VIDEO LOG

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

355.4.2 PROHIBITED ACTIVITY

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

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

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

Community video streams systems and recordings are subject to the Berkeley Police Department's Immigration Law Policy, and hence may not be shared with federal immigration enforcement officials, unless required by federal law.

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

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

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

Department's system must be configured for video only.

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

355.5 STORAGE AND RETENTION OF MEDIA

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

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

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

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

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

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

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.

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

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

355.7 COMMUNITY VIDEO STREAMS AUDIT

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

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

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

355.8 TRAINING

All BPD members authorized to access community video streams systems shall receive appropriate training. Training should include guidance on the use of cameras, associated 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 and are not intended to express a preference for any particular vendor.

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

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

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

2. Purpose

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

The proposed purposes of the Investigative Software are limited to:

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

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

3. Location

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

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

4. Impact

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

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

- Combining records that are each individually permissible to hold can produce a more revealing picture of a person's movements, associations, and activities than any single record. The Investigative Software addresses this by limiting connected data sources to those enumerated in Section 6, by requiring that every query be tied to a specific BPD case or incident, and by auditing all queries.
- BMC 2.99.030(5) prohibits the City from obtaining, retaining, requesting, accessing, or using Face Recognition Technology or information obtained from Face Recognition Technology. Some Investigative Software vendors offer face-comparison, face-matching, or face-clustering features. Any such feature shall be disabled in the Department's deployment, shall not be enabled by the vendor without explicit Council approval under BMC 2.99, and any inadvertent receipt of Face Recognition output shall be handled in accordance with BMC 2.99.030(5).
- Some underlying data sources reflect historical patterns of police contact, which in Berkeley and elsewhere have not fallen evenly across communities. A tool that

makes those records easier to query can, if used carelessly, reinforce those patterns. Mitigations include the case-number-tied query requirement, the prohibition on general intelligence-gathering and dragnet searches in the accompanying Surveillance Use Policy, and the audit-log requirement that records the user, time, source, case number, and reason for each query.

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

5. Mitigations

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

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

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

6. Data Types and Sources

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

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

Authorized Connected sources

- BPD Computer-Aided Dispatch (CAD) records.
- BPD Records Management System (RMS) reports and supplements.
- BPD Digital Evidence Management System metadata, and case-specific content.
- Automated License Plate Reader (ALPR) data.

- Fixed video camera data.
- Unmanned Aerial Systems (UAS) data.
- Opt-in case-linkage data voluntarily shared by other participating law-enforcement agencies.
- NIBIN (National Integrated Ballistic Information Network) ballistic-evidence data, accessed by federally authorized BPD personnel in connection with firearm investigations.
- Publicly available open-source data.
- Any future surveillance technology approved by Council through the STO process.

Excluded Sources

The following sources shall not be connected to the Platform:

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

7. Data Security

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

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

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

8. Fiscal Cost

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

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

Initial Cost:

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

Cost of Use:

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

Costs of Potential Adverse Impacts:

- Potential costs include data-breach liability, claims of privacy violation, and litigation costs associated with civil-rights claims. These risks are mitigated by the contractual financial-penalty clause to be negotiated into the procurement contract, by CJIS-compliant hosting, by the prohibitions on Face Recognition and excluded data sources, and by strict audit and supervisory review.

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

Annual and Ongoing Costs:

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

Training Costs:

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

Maintenance and Storage Costs:

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

Upgrade Costs:

- Software upgrades are included in the annual subscription model.

9. Third Party Dependence and Access

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

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

sanctuary protections, federal immigration enforcement, out-of-state reproductive-rights or gender-affirming-care enforcement and vendor disclosure apply to the data when it is accessed through the Platform.

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

10. Alternatives

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

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

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

11. Experience of Other Entities

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

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

Publicly available reporting has identified concerns with certain configurations of Investigative Software products in other jurisdictions, including: default-on use of face-matching features in some vendor deployments; reports that one vendor explored sourcing data from breaches and dark-web marketplaces before publicly stating it would

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

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

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

1307.3 DATA COLLECTION AND CONNECTED SOURCES

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

Authorized Connected Sources

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

Excluded Sources

The following sources shall not be connected to the Platform:

- Face Recognition Technology data.

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

1307.5 DATA PROTECTION

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

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

1307.6 CIVIL LIBERTIES AND RIGHTS PROTECTION

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

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

1307.7 DATA RETENTION

Data accessed through the Investigative Software but not downloaded or saved by the Department is not retained by the Department independently of the connected source. The retention schedule of the connected source from which the data was obtained continues to control.

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

1307.8 PUBLIC ACCESS

Data collected and used in a police report shall be made available to the public in accordance with department policy and applicable state or federal law. Requests for records derived from the Investigative Software shall be processed in the same manner as requests for department public records pursuant to Policy 804. Records that are the subject of a court order or subpoena shall be processed in accordance with the established department subpoena process.

1307.9 THIRD-PARTY DATA-SHARING

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

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

1307.10 TRAINING

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

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

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

1307.11 AUDITING AND OVERSIGHT

The Investigative Software generates a site log each time the system is accessed. Audits will be conducted on a regular basis, at least twice a year~~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.

SUPPLEMENTAL

AGENDA MATERIAL

for Supplemental Packet 2

Meeting Date: June 2, 2026

Item Number:

Item Description: Council Directed STO Approvals

Submitted by: City Manager Paul Buddenhagen

This document provides staff's initial responses to the sub-items identified in the Mayor's Supplemental Memorandum referring the Community Video Streams (CVS) Acquisition Report and Surveillance Use Policy to the Public Safety Policy Committee (PSPC). Staff welcomes the opportunity for additional committee-level dialogue and intends to work collaboratively with the PSPC, the Police Accountability Board (PAB), and stakeholders to refine the policy framework prior to final Council action.

PURPOSE

This document provides staff's initial responses to the sub-items identified in the Mayor's Supplemental Memorandum referring the Community Video Streams (CVS) Acquisition Report and Surveillance Use Policy (Policy 1306) to the Public Safety Policy Committee (PSPC). Staff welcomes the opportunity for additional committee-level dialogue and intends to work collaboratively with the PSPC, the Police Accountability Board (PAB), and stakeholders to refine the policy framework prior to final Council action at the end of the Request for Proposals (RFP) process.

Staff responses are organized by sub-item lettered (a) through (h) as listed in the Mayor's referral. Where a concern is substantially addressed by existing policy language, staff identifies the relevant provision. Where additional work is warranted, staff describes the approach and anticipated timeline.

RESPONSES

a. First Amendment Protections

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.

Staff Response:

Staff concurs that an explicit First Amendment protection provision strengthens the policy and provides important clarity for both officers and the public. Policy 1306 currently prohibits use of community video streams in an "unequal or discriminatory manner" targeting protected characteristics and restricts access to specific authorized use cases (active criminal investigations, serious traffic investigations, police misconduct investigations, and critical incidents). However, the policy does not include an affirmative, standalone prohibition on surveilling constitutionally protected activity such as protests, demonstrations, or other expressive assemblies.

Staff proposes adding the following language to Policy 1306.2 (Authorized Use) or as a new stand-alone subsection:

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

b. Data Retention Periods

Specify concrete data retention periods with the four elements required by BMC 2.99.020.4(g).

Staff Response:

BMC 2.99.020.4(g) requires that data retention schedules address: (1) the length of time data is retained; (2) the basis for that period; (3) who may authorize extensions; and (4) procedures for destruction upon expiration.

Policy 1306.7 (Data Retention) currently delegates retention of non-evidentiary footage to the camera owner's own schedule, and provides that evidentiary footage is retained "in accordance with state law and existing Departmental evidence retention protocols." This approach reflects the unique architecture of the CVS program- BPD does not own or continuously store video; it only downloads footage when it is relevant to an active investigation. Once downloaded, footage is managed under existing evidence retention rules applicable to all digital evidence.

In an effort to explicitly enumerate the four BMC 2.99.020.4(g) elements for the evidentiary footage category. Staff proposes to revise Policy 1306.7 to address each element as follows:

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

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

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

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

c. Disparate Impact Analysis

Conduct a disparate impact analysis addressing whether camera coverage is concentrated in areas with particular demographic characteristics.

Staff Response:

Staff agrees this is an important transparency and equity measure and commits to conducting a disparate impact analysis as part of the program's implementation framework. Because the CVS program is voluntary and camera locations are

determined entirely by private owners who opt in, the Department does not control the geographic distribution of integrated cameras. Nonetheless, the Acquisition Report acknowledges that deployment priorities will focus on major commercial corridors (Elmwood, Solano, Telegraph, Fourth Street, Downtown) and facilities with mass-casualty response needs.

As the program begins to incorporate video streams, staff will list those locations on our website and will proceed to conduct an analysis mapping camera coverage against census tract-level demographic data, including race/ethnicity, income, and primary language. This analysis will:

- Identify whether opt-in participation is disproportionately concentrated in or absent from areas with particular demographic characteristics;
- Assess whether the Department's prioritization criteria- focused on major commercial corridors- creates patterns of disparate coverage;
- Recommend mitigation measures if disparate patterns are identified, which may include affirmative outreach to underrepresented business districts or geographic restrictions on targeted enrollment efforts.

Staff proposes to incorporate analysis findings into the BMC 2.99 annual report to Council. The methodology and findings will be published on the City's website consistent with the transparency requirements of Policy 1306.13 and BMC 2.99.

d. Adverse Findings from Comparable Jurisdictions

Supplement Section 11 of the Acquisition Report to disclose adverse findings from comparable jurisdictions.

Staff Response:

Staff recommends adding the following text in Section 11 of the Acquisition Report:

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

amendment assemblies, and biennial OSPA review. The features that generated controversy elsewhere- always-on monitoring, facial recognition, and the absence of oversight- are excluded here by design."

e. Immigration-Related Search Reporting

Update immigration-related search reporting to match the 72-hour standard and named recipients in Policy 351 section 351.6 per our Sanctuary City Ordinance.

Staff Response:

The two provisions in Policy 351.6 cover different events. The ten-day requirement applies to requests for immigration-enforcement access- and Policy 1306.9 already carries it. The 72-hour requirement applies when a federal agency is actually given BPD-owned data held by a vendor. That event does not arise under CVS: BPD holds no standing pool of community video stream data with a vendor. The only CVS data the Department controls is evidentiary footage in its digital evidence system, already governed by evidence-retention and immigration policies.

Staff can add parallel 72-hour language (City Manager, City Attorney, City Council) for cross-policy consistency if the Committee prefers.

f. Cross-Platform Integrated Technology Use Policy

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.

Staff Response:

BMC 2.99 structures acquisition reports and use policies on a technology-by-technology basis. Under the current ordinance, staff is not positioned to adopt a single use policy governing combined cross-platform use. Staff would welcome Council direction and a process to amend BMC 2.99 to enable such a framework. The Investigative Software use policy addresses how to use a platform that interacts with multiple surveillance technologies, but does not alter the primary use polices for each technology in any way.

g. Semiannual Audits

Institute semiannual audits of CVS — similar to Council directive on fixed cameras established in July 2025.

Staff Response:

Staff has always interpreted Policy 1306.11 as requiring a regular twice-yearly cadence consistent with the July 2025 fixed-camera directive. Staff will change “biennial” to “twice a year” to remove the ambiguity.

h. Data Governance and Security Risk Analysis

Analyze the data governance and security risks of community camera integration.

Staff Response:

The Acquisition Report addresses data security in Sections 5 and 7 and Policy 1306 in Sections 1306.5 and 1306.9. Staff requests clarification from the authors on the specific data governance or security risks they wish to see analyzed beyond those provisions, so the analysis can be scoped appropriately.

--

Additional concern: Third Party Access

BMC 2.99.020.3.i requires that an acquisition report have information about 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 surveillance data or may otherwise sell or share it in any form. BMC 2.99.020.4.i similarly requires a use policy to have information about “if and how a non-City entity can access or use the information, including any required justification or legal standard necessary to do so and any obligations imposed on the recipient of the information.”

Staff Response:

Staff recommends adding the following text to the Acquisition Report and Surveillance Use Policy:

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