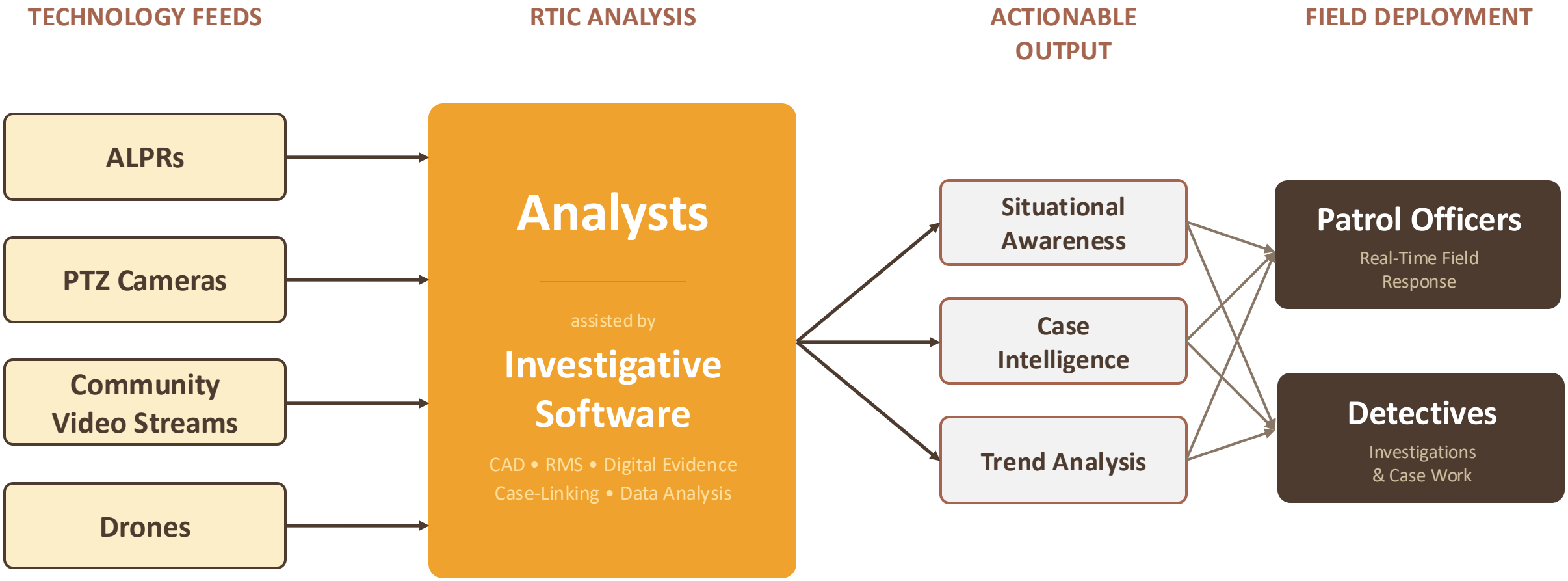
Public Safety Technology Update

March 24, 2026

Real-Time Information Center (RTIC)

How technology feeds support analysts and field operations



***Research**: RTIC's are proven resource multipliers. Peer-reviewed studies show 66% better odds of clearance for cases supported by RTIC. Peer agencies report 25% of drone calls cleared without dispatching officers.*

Renewals + Updates

ALPRs

120+
Arrests and leads in 2025

Contract Renewal

- 52 cameras cross-referencing plates against hotlists for stolen vehicles, missing persons, felony warrants.
- Real-time alerts to patrol;
- 30-day retention; Federal access blocked.
- Approved July 2023. No policy changes.

PTZ Cameras

16
Council-approved cameras

Policy Update with Council-directed revisions.

- Located in business districts with high pedestrian traffic.
- Objective video evidence for prosecution; real-time situational awareness; visual deterrence.
- 180-day retention; no external direct access to data.
- Approved July 2025. Updated policies reflect Council-directed revisions.

Field-Deployed UAS

0
Injuries or complaints reported

Policy Update to allow dept purchase

- On-scene aerial views and interior building assessment during high-risk searches, warrants, and emergencies.
- Increases ability to de-escalate.
- Evidence retained according to department retention policy
- Council approved mutual aid UAS. Contract authority for BPD-owned units requested.

Investigative Software

$0
General Fund impact

Grant-Funded • 1yr

- Centralizes existing databases like CAD, RMS, and digital evidence into one searchable platform for case-linking.
- Directly supports the Gun Violence Intervention and Prevention Program.
- 100% funded by Byrne SCIP grant accepted July 2025. No General Fund impact.

Community Video Streams

$0
City hardware cost.
Cameras are privately owned

- **How it Works**
  - Opt-in program: business and non-residential commercial building camera integration allowing BPD to view security feeds during specific incidents. No City-purchased cameras.
  - Pre-integration review with in-person site assessment
  - On site public notification signage. All camera locations published on City website.
- **Public Safety Benefit**
  - Replaces the slow, manual process of canvassing to locate cameras and request footage after a crime.
  - Real-time visual awareness of scenes before officer arrival.
  - Improves coordination in response to active calls for service like a robbery or active shooter.
- **Privacy Protections**
  - Access restricted to active investigations. Camera owners retain ownership; can revoke access at any time.
  - Facial recognition strictly prohibited. All accesses logged and auditable.
  - Cannot be accessed by outside agencies.
  - Any data with evidentiary value is downloaded to department's secure evidence collection system.

Drone as a First Responder

25%
Calls cleared without a patrol unit

~2 mins
Avg. drone response time

- **How it Works**
  - Drones launch from docking stations on the roof of the Public Safety Building and fly directly to the scene.
  - Analysts see live aerial video and relay what they see to responding officers.
  - All hardware is installed and maintained by Flock under a subscription. No City infrastructure required.
- **Public Safety Benefit**
  - Rapid first-on-scene capability for police, fire, and EMS.
  - Greater certainty enables better tactical planning and facilitates de-escalation.
  - Resource multiplier: extends operational capacity without expanding headcount.
- **Privacy Protections**
  - Launched only for specific calls; never random patrol. Cameras face horizon until on scene.
  - All flight paths logged and publicly available on transparency portal within ~1 hour of docking.
  - Drones will never be weaponized. No facial recognition.
  - Data downloaded to department's secure evidence collection system

Why do we need these technologies?

Resource Multiplier

- Staffing challenges- running well below authorized strength
- Budget constraints- funded by reducing 3 positions, ~$160K/yr net savings
- Bringing multiple technologies into an ecosystem streamlines operations

Investigative Impact

- High-quality leads
- Faster apprehension of suspects
- Improves clearance rates- 66% better odds with RTIC support (peer-reviewed research)
- Strengthens case investigations- real-time data correlation across cameras, drones, ALPRs, and community video

Community Impact

- Victim closure and justice- cases solved faster, dangerous offenders off the street sooner
- Data-driven policing- officers arrive with information, not uncertainty
- Crime deterrent
- Thriving and vibrant community- better public safety outcomes with constrained resources

Why we are recommending Flock Safety

Single Ecosystem

- One dashboard, one audit trail, one MSA.
- Consolidated alerts and oversight
- Native real-time data correlation- impossible with fragmented multi-vendor systems.

Fiscal Advantage

- 10% discount on new product lines (DFR, PTZ) if executed by end of March 2026- over $100K in savings.
- Subscription model includes hardware, maintenance, and upgrades- no City-owned infrastructure to manage.

Vendor Comparison

- No other single vendor delivers ALPRs, fixed cameras, DFR, analytics, and community video integration.
- Drone camera quality and connectivity is far superior to all other competitors.
- Every city in Alameda county uses Flock ALPR. Network effect multiplies public safety value.
- Other vendors require City-owned hardware, lack real-time alerting, or cannot match Flock's technical support and included upgrades.
- Axon came closest but its ALPR/camera hardware is untested and the software lacks real-time alerts and hotlist support- core to BPD operations.

How do we mitigate potential risk

Technical Security

- End-to-end encryption across all product lines.
- SOC 2 certified, CJIS compliant infrastructure.
- All access logged and auditable.
- Flock must promptly notify City of any security incident and describe scope and corrective steps.

Sanctuary Protections

- Federal agencies require a court order to access data. Administrative subpoenas are insufficient.
- Consistent with Sanctuary City Ordinance.
- Flock has stopped federal data-sharing pilot programs nationally and introduced restrictive-by-default permission controls.

Master Services Agreement

- City Attorney's Office negotiated MSA accepted in full by Flock - every redline the City proposed was accepted.
- City owns all data, including anonymized derivatives. Flock prohibited from selling, sharing, or distributing City data.
- Contractual financial penalties for data breaches or unauthorized disclosures, mirroring framework approved by Oakland Council in December 2025.
- City's data ownership and control survives contract termination.
- Department supports additional terms being considered.

Recommended Actions

STO Approvals (BMC 2.99)

- Accept Acquisition Reports + Use Policies: UAS and Community Video Streams
- Approve updated Use Policies: Fixed Video Cameras

Police Equipment (BMC 2.100)

- Accept Impact Statement + Use Policy: Unmanned Aerial Systems

Contract Authority

- Amend contract to include:
  - DFR
  - PTZ Cameras
  - Investigative Software
  - ALPR renewal

POLICE ACCOUNTABILITY BOARD

Police Accountability Board's Surveillance Technology Recommendations for Item 26

Berkeley City Council · March 24, 2026

CORE RECOMMENDATION

Defer final action on the three surveillance items.

BPD's proposal to (1) authorize a drone-as-first-responder program, (2) integrate Community Video Streams, and (3) combine license plate readers, fixed cameras, community video feeds, and aerial drones on a single integrated platform under a single vendor ***represents the largest expansion of BPD's surveillance capacity in Berkeley's history.***

A decision of this magnitude demands thoughtful deliberation and review. This burden has not yet been satisfied.

Berkeley Crime Trends

The case for urgency has not been made.

Robberies	Shootings	Commercial Burglaries	Vehicle Thefts	Catalytic Converter Thefts
2024 → 2025	2024 → 2025	2024 → 2025	2024 → 2025	2024 → 2025
20%↓	40%↓	31%↓	46%↓	21%↓
2021 → 2025	2021 → 2025	2021 → 2025	2021 → 2025	2021 → 2025
33%↓	70%↓	13%↓	48%↓	57%↓

■ Year-over-year change (2024→2025) ■ Five-year change (2021→2025) Source: 2025 BPD Annual Report

WHY NOT NOW?

Four reasons action is premature.

01 **Concerns with Flock Safety and the lack of a documented vendor selection process.**

The record contains no criteria used to evaluate Flock Safety against alternatives and no justification for choosing a single-vendor approach for Berkeley's entire surveillance infrastructure.

02 **Inadequate review time**

BPD submitted the full MSA to the PAB a day before the March 11 meeting. CVS policies had only a single PAB meeting for consideration. The public has had no more time than the PAB to review these policies or the proposed overall surveillance architecture.

03 **No combined system assessment**

Each of the four programs was evaluated individually. The integrated ecosystem - ALPR, fixed cameras, CVS, and drones - has never been assessed as a whole.

04 **Too many unresolved issues including actions needed for regulatory compliance**

The PAB identified ~30 material issues: MSA provisions undisclosed in any acquisition report, policy non-compliance with regulatory requirements across all three program areas, inadequate notification standards, insufficient vendor sanctions, and a liability framework that would leave Berkeley without appropriate remedy in a major data breach.

Why Flock Safety?

BPD proposes Flock Safety as the sole vendor for Berkeley’s integrated surveillance platform.

FLOCK SAFETY

Flock Safety: BPD Justifications and PAB Concerns

BPD Justifications

- **Fully integrated, centralized surveillance system**
  ALPR, cameras, CVS, and drones on one platform under one vendor.
- **More advanced drone technology**
  Flock's drone-as-first-responder (DFR) platform claimed to offer superior capabilities for BPD.

PAB Concerns

- **Concentration risks**
  Operational dependency, vendor lock-in, and magnified privacy impact from a single integrated platform.
- **Experience of other jurisdictions**
  Over 50 jurisdictions have walked away from Flock over privacy and data-sharing failures.
- **Flaws in the Master Services Agreement**
  Perpetual data licenses, no exit rights, and no consent required for new features.
- **Conflict with Sanctuary City commitments**
  Flock's network model creates structural risk of federal immigration agency access.
- **Lack of documented vendor selection process**

RECOMMENDED ACTION 1 OF 4

Complete a consolidated BMC 2.99 assessment for the full ecosystem.

A single operator could identify a vehicle by plate, pull fixed and community camera footage, and dispatch a drone in real time. When ALPR, cameras, CVS, and drones integrate on one platform, the combined tracking capability far exceeds what any individual program authorization contemplated.

CONCENTRATION RISKS THE REPORT MUST ADDRESS

Operational Dependency

One vendor controlling hardware, software, and data storage across multiple critical systems means any outage, security incident, or policy change can impair several core capabilities simultaneously.

Weakened Governance Leverage

Consolidation makes it significantly harder to negotiate privacy terms, conduct independent audits, or manage data parameters. The city's leverage diminishes once multiple systems depend on the same vendor.

Cost Lock-In Over Time

Initial bundled pricing shifts bargaining power to the vendor. Subscription increases, hardware costs, license fees, and add-on charges become difficult to resist once switching is operationally disruptive and expensive.

Integration Magnifies Privacy Impact

Combined ALPR, camera, and drone data on one platform creates tracking capability that significantly exceeds what any individual program authorization contemplated and what no single BMC 2.99 review has evaluated.

Additional factors to be considered in consolidated assessment:

- Combined data access capabilities and cross-program data rights
- Adequacy of audit mechanisms to detect platform-wide unauthorized access
- Corrected "experience of other entities" documentation, including adverse findings from comparable jurisdictions
- BPD's need for dedicated technology staffing to competently manage the ecosystem

RECOMMENDED ACTION 2 OF 4

If Council Chooses to Contract With Flock Safety, Renegotiate the Flock Master Services Agreement.

The MSA contains provisions that leave Berkeley without basic protections:

- An irrevocable service license and perpetual anonymized data license that survive contract termination
- No city consent required before Flock activates new platform features including convoy tracking, predict-a-path, and Flock Nova
- No termination-for-convenience right. Berkeley cannot exit without proving material breach
- No post-termination data deletion requirement for city-associated data
- No city consent required before Flock assigns the agreement to an affiliate or acquirer

RECOMMENDED ACTION 2 OF 4

Strengthen the MSA penalty amendment.

As Submitted

- $75,000 penalty per violation is sole and exclusive remedy, eliminating legal recourse
- Lookup tool carve-out exempts the exact mechanism behind the Mountain View, Ventura, and other similar incidents
- Federal task force carve-out creates proxy-access loophole

What's Needed

- $200,000–$290,000 per violation. Flock accepted this range in Oakland and Richmond
- Delete the lookup tool carve-out entirely
- Preserve full legal remedies where actual harm exceeds penalty amount
- Require individual written authorization by Berkeley for any federal access

There is no basis for Berkeley accepting a lower standard than peer cities have already negotiated.

CVS, UAS, and Fixed Camera Use Policies

BPD Policies 351, 355, 611, 709, 1303, and 1306

Surveillance programs under review: policies and governing law

Type of Surveillance Tool	Applicable BPD Policies	Relevant Laws
Community Video Streams	Policy 355, Policy 1306, and Acquisition Report	BMC 2.99 (STO) & Berkeley's Sanctuary City Commitments
External Fixed Video Surveillance Cameras	Policy 351	BMC 2.99 & Berkeley's Sanctuary City Commitments
Unmanned Aerial System (UAS)	Policy 611, Policy 709, Policy 1303, and Acquisition Report	BMC 2.99 (STO), BMC 2.100 (Military Equipment), AB 481 (Military Equipment), and Berkeley's Sanctuary City Commitments

RECOMMENDED ACTION 3 OF 4

Correct policy deficiencies across all programs.

Policies 351, 355, 611, 709, 1303, and 1306 share common deficiencies:

No First Amendment protections

Only UAS Use Policy prohibits using Flock technology to monitor protests, political assemblies, or protected activity.

Inconsistent notification standards

Triggering criteria for notifying of non-California and federal agency access vary across programs and must be standardized at 72 hours.

Insufficient auditing requirements

Audit requirements are inconsistent, and insufficient, across all programs.

No enforceable vendor sanctions

Policies do not include legally enforceable penalties against Flock for unauthorized access, unauthorized feature activation, or data security violations.

Drone policies carry additional concerns: inadequate use restrictions, fiscal discrepancies, and unresolved FCC Covered List issues for the proposed foreign-produced fleet.

Surveillance Use Policy - Unmanned Aerial System (UAS)

BPD proposes Flock Safety as the sole vendor for Berkeley's integrated surveillance platform.

Eight critical deficiencies must be addressed before any drone program can advance.

Authorized Uses Too Broad

UAS Use Policy lists permitted uses (e.g., active pursuits, missing persons) but does not limit DFR to those uses. PAB recommends explicit permitted uses and limiting DFR to a closed list for a pilot period. The permissive language allows deployment for any purpose not expressly prohibited, creating broad operational discretion with no warrant or exigency requirement for most deployments.

Data Retention Too Broad

UAS Use Policy sets a uniform 60-day retention period for all footage regardless of evidentiary value. PAB recommends tailoring retention periods to achieve the specific permitted purpose, most of which are serviced by immediate video confirmation. Long data retention periods raises privacy concerns, constitutional policing issues, and exposure to federal immigration enforcement.

Oversight & Accountability Gaps

Require supervisory approval before each deployment. Mandate logging of reason for deployment and recording times.

No Performance Baseline

No framework to evaluate program effectiveness. Require metrics before authorization: CFS response time, crime clearance rates, use-of-force rates, and demographic distribution.

No Clear Decertification Procedure & Complaint Intake Process

UAS Use Policy contains no process for revoking officer certification. Repeat violations carry no defined consequence. Also no mechanism exists for community members to report concerns about drone deployments or request review of incidents. Accountability requires an accessible intake channel.

First Amendment Concerns

UAS Policy would authorize use to respond to “active criminal activity at mass gatherings or special events.” PAB is concerned that this offers broad discretion in light of expansive definition of what could constitute ”criminal activity” (i.e. refusing to follow unlawful dispersal order) and could chill protected First Amendment speech.

FCC Covered List Risk

December 2025 FCC action designates foreign-produced drones as national security risks. BPD’s proposed fleet is affected. Equipment authorization status must be confirmed before procurement.

Three-Policy Structure Creates Gaps

Policies 709, 611, and 1303 are interlocked through circular cross-references, creating confusion and version-control and accountability risks. Policy 709 must be self-contained for AB 481 purposes.

PATH FORWARD

The PAB is ready to support this work and to expedite review once conditions are met.

1. Complete and publish the consolidated BMC 2.99 ecosystem assessment.
2. If Council decides to contract with Flock, renegotiate the MSA.
3. Correct deficiencies across all six submitted policies.
4. If Council to authorize drone program, approve PAB's recommendations for Drone Use Policy

BEN BARTLETT
CITY COUNCILMEMBER, DISTRICT 3

REVISED AGENDA MATERIAL
for Supplemental Packet 3

Meeting Date: March 24, 2026

Item Number: 26

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

Submitted by: Councilmember Ben Bartlett
"Good of the City" Analysis:

The purpose of this supplemental material is to clearly define the legal boundaries within which the City may utilize Automated License Plate Reader (ALPR) Technology and other Surveillance Services. The supplemental will ensure that any vendors who are contracted to provide ALPR and Surveillance technology services operate within specific parameters that will safeguard residents' privacy, civil rights, and Berkeley's Sanctuary City Ordinance, while maintaining City control of access and usage of data generated from the technology. The supplemental will incorporate "Good of the City" provisions to ensure full transparency, control, and accountability in the deployment and operation of the technology. These provisions will include strict mutuality of contractual obligations, materially increased penalties for any unauthorized data access or disclosure, and a clear private right of action for affected individuals, including statutory damages and injunctive relief.

Consideration of supplemental or revised agenda material is subject to approval by a two-thirds vote of the City Council. (BMC 2.06.070)

A minimum of 42 copies must be submitted to the City Clerk for distribution at the Council meeting. This completed cover page must accompany every copy.

Copies of the supplemental/revised agenda material may be delivered to the City Clerk Department by 12:00 p.m. the day of the meeting. Copies that are ready after 12:00 p.m. must be delivered directly to the City Clerk at Council Chambers prior to the start of the meeting.

Supplements or Revisions submitted pursuant to BMC § 2.06.070 may only be revisions of the original report included in the Agenda Packet.

2180 Milvia Street, Berkeley, Floor 5, CA 94704 ● Tel: (510) 981-7130 ● E-Mail: bbartlett@cityofberkeley.info

ACTION CALENDAR
March 24, 2026

To: Honorable Mayor and Members of the City Council

From: Councilmember Ben Bartlett

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

RECOMMENDATION

Adopt revisions to the Flock Safety Master Services Agreement (MSA) to strengthen City control, protect data ownership, prohibit unauthorized sharing, remove perpetual licensing rights, enhance privacy safeguards, authorize termination for convenience, require Council approval for key changes, establish enforceable remedies, create a private right of action, include a mutual morality clause, and mandate data deletion upon termination.

CURRENT SITUATION AND ITS EFFECTS

Proposed revisions and recommendations should be added to the Flock Safety Master Services Agreement (MSA) before executing the Flock Safety MSA:

1. **§2.4 CITY CONTROL OF PLATFORM CHANGES**

   Replace with:

   2.4 Platform Changes. Flock shall not implement, activate, or deploy any modification, enhancement, or new functionality that affects data collection, analysis, sharing, access, or retention without the Customer's prior written approval, which shall require approval by the Berkeley City Council.

   This includes, without limitation, features involving predictive analytics, pattern recognition, vehicle tracking, network sharing, or integration with third-party systems.

   All data sharing settings shall be disabled by default. Any deviation must be expressly approved in writing by Customer and publicly disclosed.

2. **§4.1 (Customer Data License) REMOVING IRREVOCABLE**

   Replace with:

   4.1 Customer Data. As between Flock and Customer, all right, title, and interest in and to Customer Data shall remain exclusively with Customer. Customer grants to Flock a limited, non-exclusive, royalty-free, non-transferable license to use Customer Data solely to provide the Flock Services to Customer during the Term.

2180 Milvia Street, Berkeley, Floor 5, CA 94704 ● Tel: (510) 981-7130 ● E-Mail: bbartlett@cityofberkeley.info

This license shall automatically terminate upon expiration or termination of this Agreement. Flock shall have no right to retain, use, or access Customer Data thereafter except as expressly required by law and only for the minimum period required.

3. **§4.2 Customer Generated Data CLOSES THE LOOPHOLE**

   Add at the end:

   Notwithstanding anything to the contrary, Customer Generated Data shall not be used, shared, or accessed for any purpose other than providing Services to Customer, and shall not be subject to any broader rights under Section 4.3 or elsewhere in this Agreement.

4. **§4.3 REMOVING PERPETUAL RIGHTS**

   Replace with:

   4.3 Anonymized Data. Flock may create Anonymized Data solely for the purpose of providing Services to Customer during the Term.

   Flock shall have no right to use Anonymized Data for product development, commercialization, or any purpose unrelated to Services provided to Customer.

   All rights granted under this Section shall terminate upon expiration or termination of this Agreement. Flock shall delete all Anonymized Data derived from Customer Data in accordance with Section [Data Deletion].

5. **New Section Data Sharing Restrictions**

   X. **Data Access and Sharing Restrictions**.

   - **a.** Flock shall not disclose, provide access to, or enable access to Customer Data to any third party, including any federal agency, except pursuant to a specific, written authorization issued by Customer for each individual request.
   - **b.** Access by federal personnel embedded within or assigned to any state or local agency shall be prohibited unless expressly authorized in writing by Customer for each instance of access.
   - **c.** Use of any shared lookup, query, or network-based access tool that permits third-party querying of Customer Data is prohibited unless explicitly approved in writing by Customer.
   - **d.** Indirect access, including access facilitated through another agency, shall be deemed a violation of this Agreement.

6. **ADD: TERMINATION FOR CONVENIENCE**

X Termination for Convenience. Customer may terminate this Agreement at any time, with or without cause, upon thirty (30) days' written notice. Customer shall not be obligated to pay for any Services not rendered after the effective date of termination.

7. **§11.3 (Assignment) COB CONTROLS**

Replace the second sentence with:

Notwithstanding the foregoing, Flock may not assign this Agreement to any affiliate, successor, or acquirer without the prior written consent of Customer, which shall not be unreasonably withheld and shall require City Council approval.

8. **§11.15 Morality Mutual Morality / Misconduct Clause**

Customer shall have the right to terminate this Agreement immediately upon written notice if Flock, its officers, or affiliates are indicted, found liable for violations of law, or determined by Customer to have engaged in unauthorized data access, sharing, or misuse.

9. **Replace the Amendment "Unauthorized Sharing" section entirely:**

Unauthorized Access; Remedies.

a. Any unauthorized access, disclosure, sharing, or use of Customer Data ("Unauthorized Access") shall constitute a material breach of this Agreement.
b. For each Unauthorized Access event, Flock shall pay Customer liquidated damages in the amount of **One Million Dollars ($1,000,000)** per violation, or **Ten Thousand Dollars ($10,000) per affected record**, whichever is greater.
c. Each individual query, access event, or data retrieval shall constitute a separate violation.
d. The remedies set forth herein are cumulative and shall not be deemed the sole or exclusive remedy. Customer retains all rights at law and in equity, including the right to seek injunctive relief.
e. Flock acknowledges that unauthorized access to surveillance data creates irreparable harm. Customer shall be entitled to immediate injunctive relief without the requirement to post bond.

10. ADD: PRIVATE RIGHT OF ACTION

Private Right of Action.

Any individual whose data, image, likeness, or identifying information is accessed, disclosed, or used in violation of this Agreement shall have a direct right of action against Flock.

Flock agrees that such individuals may bring claims for statutory damages of not less than **$5,000 per violation**, actual damages, punitive damages where permitted, and reasonable attorneys' fees and costs.

Flock expressly waives any argument that it is not a data controller or that such individuals lack privity under this Agreement.

11. ADD: Mandatory Data Deletion

Data Deletion.

Within thirty (30) days of termination or expiration of this Agreement, Flock shall permanently delete all Customer Data, Customer Generated Data, and any derivatives thereof, including Anonymized Data.

Flock shall certify such deletion in writing, signed by an officer of the company.

No data may be retained for product development, machine learning, or any other purpose.

ADENA ISHII
MAYOR OF BERKELEY

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

REVISED AGENDA MATERIAL
for Supplemental #2

Meeting Date: March 24, 2026

Item Number: 26

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

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

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

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

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

Proposed revisions and recommendations:

Surveillance Technology Ordinance (BMC 2.99)

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

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

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

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

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

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

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

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

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

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

following circumstances."

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

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

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

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

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

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

Police Equipment Ordinance (2.100)

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

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

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

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

Contract Authority

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

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

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

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

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

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

Additional Recommendations

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Surveillance Technology Ordinance Approvals

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

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

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

Police Equipment Ordinance Approvals

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

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

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

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

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

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

Contract Authority

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

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

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

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

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

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

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

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

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

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

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

Noes: None.

Absent: None.

_____
Adena Ishii, Mayor

Attest: _____
Mark Numainville, City Clerk

Policy
1303

Law Enforcement Services Manual

Surveillance Use Policy-Unmanned Aerial System (UAS)

1303.1 PURPOSE

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

1303.2 AUTHORIZED USE

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

1. To provide real-time situational awareness during high-risk or critical incidents, such as barricaded suspects, hostage situations, active shooters, the apprehension of armed and dangerous suspects, the pre-planning and service of a warrant allowing officers to create time and distance to formulate de-escalation strategies, facilitate safe tactical planning, and reduce the need for immediate physical engagement.

2. To assist in locating lost, missing, or injured persons during search and rescue operations.

3. To rapidly respond to calls for service to verify the nature of the incident, potentially determining that a law enforcement response is unnecessary for unfounded reports or low-priority incidents, thereby acting as a resource multiplier and keeping patrol officers available for other calls.

4. To locate fleeing suspects to effectively contain perimeters and reduce the need for dangerous ground-based foot pursuits.

5. To track fleeing vehicles from a safe distance, allowing patrol units to de-escalate or terminate dangerous ground pursuits while maintaining visual contact.

6. To clear interior buildings or confined spaces remotely to prevent potentially violent encounters between officers and hidden suspects.

7. To assist the Fire Department with fire mitigation and suppression, hazardous materials releases, or disaster response and recovery.

8. To remotely inspect potential explosive devices or hazardous objects.

9. To document complex crime scenes, accident scenes, or areas where an aerial perspective is critical for the investigation.

10. To respond to active criminal activity at mass gatherings or special events.

11. To mitigate hazards caused by other UAS interfering with emergency operations.

12. For pilot certification training and maintenance of proficiency.

13. To address other unforeseen exigent circumstances where there is an imminent threat to public safety, provided the deployment is consistent with the general privacy and safety principles of this policy.

1303.3 PROHIBITED USE

The UAS shall not be used:

1. To conduct random or arbitrary surveillance activities. This prohibition includes, but is not limited to, first amendment assemblies in accordance with Policy 428 First Amendment Assemblies.

2. To target a person based solely on actual or perceived characteristics, such as race, ethnicity, national origin, religion, sex, sexual orientation, gender identity or expression, economic status, age, cultural group, or disability.

3. To harass, intimidate, or discriminate against any individual or group.

Furthermore, the UAS shall not be equipped with:

1. Facial recognition software

2. Biometric analysis capabilities

3. Weapons of any kind, including lethal or non-lethal munitions.

1303.4 DATA COLLECTION

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

1303.5 DATA ACCESS

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

1303.6 DATA PROTECTION

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

1303.7 CIVIL LIBERTIES AND RIGHTS PROTECTIONS

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

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

1. Absent a warrant or exigent circumstances, operators and observers shall adhere to FAA regulations and shall not intentionally record or transmit images of any location where a person would have a reasonable expectation of privacy (e.g., residence, yard, enclosure).

2. Operators and observers shall take reasonable precautions to avoid inadvertently recording or transmitting images of uninvolved community members or areas where there is a reasonable expectation of privacy. Cameras shall be diverted away from private spaces when not actively engaged in a permitted use.

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

1303.8 DATA RETENTION

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

1303.9 PUBLIC ACCESS

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

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

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

1303.10 THIRD PARTY DATA SHARING

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

1303.11 TRAINING

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

1303.12 AUDITING AND OVERSIGHT

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

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

Intentional violation of this policy may serve as grounds for disciplinary action pursuant to the Policy 1010, Personnel Complaints policy.

1303.13 MAINTENANCE

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

Policy
611

Berkeley Police Department

Law Enforcement Services Manual

Unmanned Aerial System (UAS) Operations

611 PURPOSE AND SCOPE

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

611.1 DEFINITIONS

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

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

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

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

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

611.2 POLICY

Unmanned aerial systems may be utilized for the purpose of enhancing the department's mission to safeguard our diverse community by enabling remote visual assessment and real-time situational awareness in the situations specified in this policy. Any use of a UAS will also be in strict accordance with BMC 13.114 Sanctuary City Ordinance, constitutional and privacy rights, and FAA regulations.

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

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

611.3 PRIVACY

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

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

1) Absent a warrant or exigent circumstances, operators and observers shall adhere to FAA regulations and shall not intentionally record or transmit images of any location where a person would have a reasonable expectation of privacy (e.g., residence, yard, enclosure).

2) Operators and observers shall take reasonable precautions to avoid inadvertently recording or transmitting images of uninvolved community members or areas where there is a reasonable expectation of privacy. Cameras shall be diverted away from private spaces when not actively engaged in a permitted use.

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

611.4 PROGRAM COORDINATOR

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

611.5 PERMITTED USE

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

1) To provide real-time situational awareness during high-risk or critical incidents, such as barricaded suspects, hostage situations, active shooters, the apprehension of armed and dangerous suspects, the pre-planning and service of a warrant allowing officers to create time and distance to formulate de-escalation strategies, facilitate safe tactical planning, and reduce the need for immediate physical engagement.

2) To assist in locating lost, missing, or injured persons during search and rescue operations.

3) To rapidly respond to calls for service to verify the nature of the incident, potentially determining that a law enforcement response is unnecessary for unfounded reports or low-priority incidents, thereby acting as a resource multiplier and keeping patrol officers available for other calls.

4) To locate fleeing suspects to effectively contain perimeters and reduce the need for dangerous ground-based foot pursuits.

5) To track fleeing vehicles from a safe distance, allowing patrol units to de-escalate or terminate dangerous ground pursuits while maintaining visual contact.

6) To clear interior buildings or confined spaces remotely to prevent potentially violent encounters between officers and hidden suspects.

7) To assist the Fire Department with fire mitigation and suppression, hazardous materials releases, or disaster response and recovery.

8) To remotely inspect potential explosive devices or hazardous objects.

9) To document complex crime scenes, accident scenes, or areas where an aerial perspective is critical for the investigation.

10) To respond to active criminal activity at mass gatherings or special events.

11) To mitigate hazards caused by other UAS interfering with emergency operations.

12) For pilot certification training and maintenance of proficiency.

13) To address other unforeseen exigent circumstances where there is an imminent threat to public safety, provided the deployment is consistent with the general privacy and safety principles of this policy.

611.6 PROHIBITED USE

1) The UAS shall not be used:

   a) To conduct random or arbitrary surveillance activities. This prohibition includes, but is not limited to, first amendment assemblies in accordance with Policy 428 First Amendment Assemblies.

   b) To target a person based solely on actual or perceived characteristics, such as race, ethnicity, national origin, religion, sex, sexual orientation, gender identity or expression, economic status, age, cultural group, or disability.

   c) To harass, intimidate, or discriminate against any individual or group.

2) Furthermore, the UAS shall not be equipped with:

   a) Facial recognition software

b) Biometric analysis capabilities

c) Weapons of any kind, including lethal or non-lethal munitions.

611.7 TRAINING

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

611.8 RETENTION REQUIREMENTS

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

611.9 RELEASE OF RECORDINGS

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

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

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

External Fixed Video Surveillance Cameras

351.1 PURPOSE AND SCOPE

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

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

351.2 POLICY

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

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

351.3 OPERATIONAL GUIDELINES

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

351.3.1 PLACEMENT REVIEW AND MONITORING

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

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

Current City Council approved location

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

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

(a) To support specific and active criminal investigations.

(b) To support serious traffic-related investigations.

(c) To support police misconduct investigations,

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

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

351.3.2 FIXED CAMERA MARKINGS

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

351.3.3 INTEGRATION WITH OTHER TECHNOLOGY

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

351.4 VIDEO SUPERVISION

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

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

351.4.1 VIDEO LOG

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

351.4.2 PROHIBITED ACTIVITY

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

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

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

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

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

351.5 STORAGE AND RETENTION OF MEDIA

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

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

351.5.1 EVIDENTIARY INTEGRITY

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

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

351.6 RELEASE OF VIDEO IMAGES

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

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

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

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

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

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

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

351.7 VIDEO SURVEILLANCE AUDIT

The video surveillance software generates a site log each time the system is accessed. The site log is broken down by server, device, user or general access. The site log is kept on the server for two years and is exportable for reporting. System audits will be conducted by the Office of Strategic Planning and Accountability (OSPA) on a regular basis, at least monthly ~~biennial~~. A report of these audits shall be published semiannually, and should be sent to the Police Accountability Board. As part of the audit, OSPA will confirm that BPD doesn't enter any direct data sharing agreements or give direct access to outside agencies. A log of any instance of when surveillance footage has been shared, including date, time, reasons for search, and any recipient agencies.

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

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

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

351.8 TRAINING

All department members authorized to operate or access video surveillance systems shall receive appropriate training. Training should include guidance on the use of cameras, associated software, and review of relevant policies and procedures, including this policy, as well as review of relevant City of Berkeley laws and regulations. Training should also address state and federal law related to the use of video surveillance equipment and privacy. All relevant recordings that are utilized will be collected pursuant to Policy 802, Property and Evidence, and retained pursuant to Policy 804, Records and Maintenance.

351.9 MAINTENANCE

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

Policy
1304

Berkeley Police Department

Law Enforcement Services Manual

Surveillance Use Policy-External Fixed Video Surveillance Cameras

1304.1 PURPOSE

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

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

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

1304.2 AUTHORIZED USE

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

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

(a) To support specific and active criminal investigations.

(b) To support serious traffic-related investigations.

(c) To support police misconduct investigations, and

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

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

The following are prohibited uses of the video surveillance system:

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

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

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

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

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

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

1304.3 DATA COLLECTION

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

1304.4 DATA ACCESS

Access to video surveillance cameras data shall be limited to BPD personnel utilizing the camera database for uses described above and pursuant to Use Policy 351, with technical assistance from Public Works Department and Department of Information Technology personnel. Information may be shared in accordance with 1304.9 below. BPD members seeking access to the video surveillance system shall obtain the approval of the Investigations Division Captain, or their designee.

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

1304.5 DATA PROTECTION

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

1304.6 CIVIL LIBERTIES AND RIGHTS PROTECTION

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

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

1304.7 DATA RETENTION

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

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

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

1304.8 PUBLIC ACCESS

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

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

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

1304.9 THIRD-PARTY DATA-SHARING

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

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

Requests for recorded video from the Office of Director of Police Accountability and Police Accountability Board shall be referred to the Investigations Division Captain, or their designee, for release in accordance with Charter Article XVIII, Section 125, Subdivision (20)(a). The Chief of Police will report any request from federal immigration authorities, vendor, or any non-local agency to access data for federal immigration enforcement purposes within 10 days of receiving the request.

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

1304.10 TRAINING

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

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

1304.11 AUDITING AND OVERSIGHT

The video surveillance software generates a site log each time the system is accessed. The site log is broken down by server, device, user or general access. The site log is kept on the server for two years and is exportable for reporting. External fixed video surveillance camera system audits will be conducted by the Office of Strategic Planning and Accountability (OSPA) on a regular basis, at least monthly ~~biennial~~. A report of these audits will be published semiannually and sent to the Police Accountability Board. As part of the audit, OSPA will confirm that BPD doesn't enter any direct data sharing agreements or give direct access to outside agencies. A log of any instance of when surveillance video and/or audio data has been shared, including date, time, reasons for search, and any recipient agencies.

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

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

1304.12 ACCOUNTABILITY

All saved data will be safeguarded and protected by both procedural and technological means. The Berkeley Police Department will observe the following safeguards regarding access to and use of stored data:

(a) Non-law enforcement requests for access to stored external fixed video surveillance camera data shall be processed according to the Records Maintenance and Release Policy in accordance with applicable law.

(b) All external fixed video surveillance camera data downloaded to any workstation or server shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time.

(c) Berkeley Police Department members approved to access external fixed video surveillance camera data under these guidelines are permitted to access the data for legitimate California law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action.

(d) Aggregated external fixed video surveillance camera data not related to specific criminal investigations shall not be released to any local, state or federal agency or entity without the consent of the Chief of Police or City Manager.

(e) Measures will be taken to ensure the accuracy of external fixed video surveillance camera information. Errors discovered in external fixed video surveillance camera data collected by external fixed video surveillance camera units shall be marked, corrected or deleted in accordance with the type and severity of the error in question.

(f) Such external fixed video surveillance camera data may be released to other authorized and verified law enforcement officials and agencies for legitimate California law enforcement purposes.

(g) Every external fixed video surveillance camera browsing inquiry must be documented by either the associated Berkeley Police case number or incident number, and/or a reason for the inquiry. For security or data breaches, see the Records Release and Maintenance Policy.

1304.13 MAINTENANCE

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

Berkeley City Councilmember
Mark Humbert, District 8
2180 Milvia Street, 5th Floor
Berkeley, CA 94704
mhumbert@cityofberkeley.info
www.MarkHumbert.com

SUPPLEMENTAL AGENDA MATERIAL

for Supplemental Packet 2

Meeting Date: **March 24, 2026**

Item Number: **26**

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

Submitted by: **Councilmember Humbert;**
Councilmember O'Keefe;
Councilmember Taplin;
Councilmember Kesarwani

Directs the City Manager and City Attorney to add requirements for the Flock Safety Master Services Agreement (MSA) that accomplish the following: (1) increase the financial penalty for unauthorized data sharing from $75,000 to $150,000 per violation; (2) establish a termination for convenience right under which the City is not refunded for payments already made but is not obligated for the remaining contract value; (3) limit Flock's license to use anonymized data to the term of the Agreement rather than in perpetuity; (4) require Flock to obtain the City's prior written consent before making any changes to the City's data-sharing settings or configurations; (5) make revisions to the Special Terms section to clarify the MSA may not be modified without City Council approval; and (6) remove the Amendment and incorporate provisions on restrictions on data sharing into the MSA and stipulate such provisions shall not be modified by subsequent Flock amendment or attachments without further City Council approval.

Berkeley City Councilmember
Mark Humbert, District 8
2180 Milvia Street, 5th Floor
Berkeley, CA 94704
mhumbert@cityofberkeley.info
www.MarkHumbert.com

ACTION CALENDAR
March 24, 2026

To: Members of the Berkeley City Council

From: Councilmember Mark Humbert (Author);
Councilmember Shoshana O'Keefe (Co-Author);
Councilmember Terry Taplin (Co-Author);
Councilmember Rashi Kesarwani (Co-Author)

Subject: Item 26. Public Safety Technology: Surveillance Technology Ordinance and Police Equipment Ordinance Approvals, Policy Updates, and Contract Authority

RECOMMENDATION

Adopt the following additional requirements for the Flock Safety Master Services Agreement (MSA). The City Manager and City Attorney shall ensure, prior to execution of the MSA, that the Agreement incorporates provisions that accomplish the following: (1) increase the financial penalty for unauthorized data sharing from $75,000 to $150,000 per violation; (2) establish a termination for convenience right under which the City is not refunded for payments already made but is not obligated for the remaining contract value; (3) limit Flock's license to use anonymized data to the term of the Agreement rather than in perpetuity; (4) require Flock to obtain the City's prior written consent before making any changes to the City's data-sharing settings or configurations; (5) revise the Special Terms section to clarify the MSA may not be modified without City Council approval; and (6) remove the Amendment and incorporate provisions on restrictions on data sharing into the MSA and stipulate such provisions shall not be modified by subsequent Flock amendment or attachments without further City Council approval. (See additional detail below.)

FINANCIAL IMPLICATIONS

None. The proposed amendments do not alter the contract price. The termination for convenience provision would limit the City's financial exposure in the event of early termination by ensuring no further payments are owed beyond those already made.

CURRENT SITUATION AND ITS EFFECTS

On March 11, 2026, the Police Accountability Board (PAB) forwarded a letter to the City Council raising concerns about the proposed Flock Safety contract, including the vendor's data-sharing practices, its relationships with federal agencies, and the adequacy of existing contractual safeguards. On March 18, 2026, Mayor Ishii convened a community meeting at which residents voiced similar concerns regarding data privacy, the scope of Flock's license to use City data, and the City's ability to exit the contract if circumstances change.

In light of the PAB's recommendations and the concerns raised by community members, this supplemental proposes the following six targeted amendments to the MSA to materially strengthen the City's position.

The City Manager should work with the City Attorney and Flock to incorporate language substantially similar to the following into the Agreement:

1. The current draft MSA includes a $75,000 per-violation penalty for unauthorized sharing of Customer Data. Increasing this amount to $150,000 per violation serves as a more meaningful deterrent and better reflects the City's expectations around data stewardship.
2. Adding a provision allowing the City to terminate the Agreement for convenience upon thirty (30) days' written notice. Under this provision, fees already paid to Flock would be non-refundable (excepting any penalties), but the City would not be liable for any remaining payments that would otherwise come due under the contract. This structure gives the City a clear exit path if it determines the services are no longer in the City's interest.
3. The current draft grants Flock a license to use anonymized data derived from Customer Data and Customer Generated Data. This license should be expressly limited to the Term of the Agreement, rather than extending in perpetuity. Restricting the duration of this license ensures that Flock's right to use anonymized data ends when the contractual relationship ends, consistent with the City's interest in maintaining long-term control over information derived from its operations.
4. Specify that Flock shall not make any hardware/software modifications that change the scope of data access or sharing without obtaining the City's prior written consent. Routine maintenance, bug fixes, and security patches that do not affect the scope of data access or sharing would not require prior consent. This safeguard addresses community concerns that platform-level configuration changes could inadvertently expand data access without the City's knowledge or approval.
5. Revise the Special Terms section to require that any changes to the MSA subsequent to its final execution by City staff will require action by the City Council.
6. Remove the Amendment at the end of the MSA and integrate provisions regarding data access, sharing, and security into the main body of the MSA, and prohibit any subsequent changes to these provisions by way of amendments, addenda, "customer agreements," or attachments, unless approved by additional Council action. These integrated provisions should ensure that Flock is prohibited from providing any City data in response to a legal request or demand without notifying the City and obtaining the City's written consent to disclosure. This prohibition shall not apply if and only if Flock is both required by law to produce the data in response to the request or demand and prohibited by law from informing the City about the request or demand.

BACKGROUND

The six amendments recommended above are responsive to community concerns and are consistent with the City's obligations under Berkeley Municipal Code Chapter 2.99 and the City's Sanctuary City policies. Staff believes these provisions are achievable and, based on discussions with Flock to date, expects the vendor to accept them. Adopting these requirements would allow Council to act on the MSA without a return to Council for further approval.

ENVIRONMENTAL SUSTAINABILITY AND CLIMATE IMPACTS

None (relative to original item).

CONTACT PERSON

Councilmember Mark Humbert — mhumbert@berkeleyca.gov, 510-981-7180

Brent Blackaby
Councilmember District 6

SUPPLEMENTAL AGENDA MATERIAL

for Supplemental Packet 2

Meeting Date: **March 24, 2026**

Item Number: **#26**

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

Submitted by: **Councilmember Blackaby**

Recommending requirements for the Flock Safety Master Services Agreement (MSA) and a referral to the City Manager for additional BPD reporting during implementation and early months of operation.

2180 Milvia Street, Berkeley, CA 94704 Tel: 510.981.7160 TDD: 510.981.6903 Fax: 510.981.7166
E-Mail: *Bblackaby@berkeleyca.gov*

Brent Blackaby
Councilmember District 6

ACTION CALENDAR
March 24, 2026

To: Honorable Mayor and Members of the City Council

From: Councilmember Blackaby

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

RECOMMENDATION

Adopt additional requirements to the Flock Safety Master Services Agreement (MSA) to reduce the risk of unauthorized data sharing, increase accountability of Flock around system performance and data privacy, and maximize contract flexibility for the City.

In addition, make a referral to the City Manager for more frequent BPD Public Safety Technology program reports to maximize oversight during implementation and reduce the chances of long-undetected data breaches.

FINANCIAL IMPLICATIONS

None.

CURRENT SITUATION AND ITS EFFECTS

Before executing the Flock Safety Master Services Agreement (MSA), the following requirements should be added to the MSA:

1. Increase the penalty Flock pays if they cause an unauthorized sharing, from $75,000 to $150,000 per violation. (FLOCK GROUP INC. AMENDMENT, p.89)

2. Allow the City of Berkeley to terminate the MSA for convenience at any time.

3. Ensure contract is structured for annual payments instead of paying in full up-front for the life of the contract; if City decides to terminate the contract early, no subsequent future payments will be made.

More frequent BPD Public Safety Technology program reports should also take place as off-agenda memos from City Manager to City Council that can be moved to Action Calendar during Council meetings:

1. Quarterly reports until installation is complete, including but not limited to:

a. Update on installation progress and timeline for each component including Unmanned Aerial Systems, Community Video Streams, fixed cameras, ALPRs, Flock Nova software, and Real-Time Information Center (RTIC)
b. Early results for any components that go live before full system is operational
c. Any issues or concerns that arise during installation

2. Monthly reports once the system is in use, for the first six months of operation, including but not limited to:
    a. Early results and performance evaluation of each component
    b. Any issues or concerns observed
    c. Proposed solutions or fixes
    d. Short case-studies or synopses of major cases supported using the new technology

3. Thereafter, align with existing practices for auditing and reporting on ALPR technology
    a. Include audits for all RTIC surveillance components as part of the existing biennial (2x/year) audit process for ALPRs, shared with PAB within 30 days of completion of each audit
    b. Include review of all RTIC surveillance components in the Annual Surveillance Technology report.

BACKGROUND

Public Safety Technology plays a critical role in supporting the Berkeley Police Department's investigations, enhancing officer safety, and strengthening overall public safety. However, Flock's documented unauthorized sharing of surveillance data underscores the need for more robust safeguards in the Master Services Agreement, as well as enhanced program reporting, to ensure full transparency and informed oversight as we move forward with this contract.

ENVIRONMENTAL SUSTAINABILITY AND CLIMATE IMPACTS

None.

CONTACT PERSON

Councilmember Brent Blackaby Council District 6 510-981-7160

Office of the City Manager

ACTION CALENDAR
May 7, 2026
(Continued from March 24, 2026)

To: Honorable Mayor and Members of the City Council

From: Paul Buddenhagen, City Manager

Submitted by: Jennifer Louis, Chief of Police

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

RECOMMENDATION

Adopt a Resolution authorizing the following actions:

Surveillance Technology Ordinance (BMC 2.99)

1. Accept the Surveillance Acquisition Report and approve the Surveillance Use Policy for the Unmanned Aerial Systems (UAS) program.

2. Accept the Surveillance Acquisition Report and approve the Surveillance Use Policy for Community Video Streams.

3. Approve updated Surveillance Use Policies for fixed video cameras, reflecting Council-directed revisions to previously approved technology.

Police Equipment Ordinance (BMC 2.100)

4. Accept the Police Equipment Impact Statement and approve the Police Equipment Use Policy for UAS.

Contract Authority

5. Authorize the City Manager to amend the existing contract with Flock Safety to add Drone as First Responder (DFR) hardware, software, and services for an initial three-year term, in an amount not to exceed $750,000.

6. Authorize the City Manager to amend the existing contract with Flock Safety to add Condor PTZ fixed surveillance cameras for an initial four-year term, in an amount not to exceed $310,000, with an option to extend for one additional three-year term, for a total not to exceed $600,000.

7. Authorize the City Manager to amend the existing contract with Flock Safety to add Flock Nova investigative software for a one-year term, in an amount not to exceed $75,000, funded by the Byrne State Crisis Intervention Program (SCIP) grant previously accepted by Council on July 29, 2025.

8. Authorize the City Manager to amend the existing contract with Flock Safety to renew Automated License Plate Readers (ALPRs) for a two-year term, in an amount not to exceed $330,000, with an option to extend for an additional two-year term, for a total not to exceed $660,000.

SUMMARY

This item requests City Council approval to advance the Berkeley Police Department's (BPD) public safety technology program through a consolidated set of actions. Only two of the technologies presented here are new to the City: the Drone as First Responder (DFR) program and a Community Video Streams integration. All other items involve renewals, extensions, or policy updates to technologies previously reviewed and approved by Council.

Consolidating these actions into a single item reflects the operational and fiscal advantages of maintaining the City's public safety technology within one integrated platform. Flock Safety is the sole vendor capable of delivering these capabilities under a single Master Services Agreement (MSA), which has been extensively negotiated by the City Attorney's Office and includes contractual protections that exceed the vendor's standard terms. Flock has offered a 10% discount on new products if the City executes by the end of March 2026, representing over $100,000 in total savings. All prices meet or are below those listed for the same products on the Omnia cooperative purchasing consortium, which is the procurement mechanism used for this acquisition.

FISCAL IMPACTS OF RECOMMENDATION

The total maximum financial commitment across all contracts is as follows:

- **DFR Program:** Not to exceed $750,000 over three years.

- **Fixed Cameras:** Not to exceed $310,000 over the initial four-year term ($600,000 if the three-year option is exercised). Funding for the initial term is available in the General Fund allocation previously designated for surveillance cameras and transferred into the Police Department's current fiscal year's budget.

- **Flock Nova:** Not to exceed $75,000 for one year. This expenditure is fully funded by the BSCC Byrne State Crisis Intervention Program (SCIP) grant of $1,000,000 accepted by Council on July 29, 2025. The grant application identified $125,504 for investigative software; this contract falls within that allocation. No General Fund impact.

- **ALPR Renewal:** Not to exceed $330,000 for two years ($660,000 if the two-year option is exercised).

At launch, the General Fund impact of this technology package is substantially offset by funding already in place. The PTZ camera contracts are funded by General Fund allocations previously designated for surveillance cameras and already transferred into the Police Department's current fiscal year budget. The Flock Nova contract is fully covered by the BSCC Byrne SCIP grant, with no General Fund impact. The City is therefore launching a comprehensive public safety technology upgrade with General Fund savings in the near term.

The ongoing subscription costs for the DFR program and ALPR renewal, the conversion of a Crime Analyst position to a new Senior Crime Analyst classification, and permanent funding of a Crime Analyst position (currently grant-funded through FY 27) will be funded through the permanent reduction of 3 sworn officer positions. At roughly $288,000–$292,000 per position in salary and benefits, 3 FTEs generate approximately $870,000 in savings per year. This exceeds the combined annual subscription costs for both programs, resulting in an average savings of about $160,000 to the General Fund each year even as the City deploys expanded capability. This approach has been reviewed and supported by the Berkeley Police Association.

The contracts are structured as annual subscriptions billed at signing for the first year and annually thereafter. Flock Safety has offered a 10% discount on new product lines (DFR, PTZ cameras, and Nova) if contracts are executed by the end of March 2026, representing over $100,000 in total savings across the combined contract terms. The ALPR renewal is priced at the existing contract rate. All prices meet or are below those listed for the same products on the Omnia cooperative purchasing consortium, which is the procurement mechanism the City is using for this acquisition and which satisfies the City’s competitive procurement requirements.

CURRENT SITUATION AND ITS EFFECTS

This consolidated public safety technology package advances the Strategic Plan goal to create a resilient, safe, connected, and prepared city.

The Berkeley Police Department currently operates 52 Flock Safety Automated License Plate Reader (ALPR) cameras under a contract that expires in July 2026. Council has previously authorized fixed video surveillance cameras on multiple occasions, most recently approving a transition to Flock Safety’s solar-powered Condor PTZ cameras on March 18, 2025, with the Surveillance Acquisition Report formally accepted on July 22,

2025. At the November 18, 2025, City Council meeting, the council directed staff to explore a Drone as First Responder program to improve public safety outcomes.

This item brings together the regulatory approvals, policy updates, and contract authority needed to move forward on all items. Rather than presenting each technology as a separate Council item over many months, this consolidated approach reflects the reality that these tools operate within a single platform and that unified procurement delivers significant fiscal, operational, and oversight advantages.

BACKGROUND

Legislative History

The technologies in this item are governed by two local ordinances and state law. BMC 2.99, the Surveillance Technology Ordinance, requires a Surveillance Acquisition Report and Use Policy for any new surveillance technology or material change to an existing one. BMC 2.100, the Police Equipment Ordinance (as amended and in effect as of March 12, 2026), requires an Impact Statement and Use Policy for controlled military equipment consistent with AB 481. The UAS program is subject to both ordinances. Community Video Streams and fixed cameras are subject to BMC 2.99. The ALPR renewal involves no new technology and no policy changes; it requires only contract authority.

Council action on each technology to date:

- **ALPRs:** Surveillance Acquisition Report accepted and Use Policy approved July 2023. Contract authority approved October 2023 and executed July 2024, expiring July 2026. No new approvals required beyond contract renewal authority.

- **Fixed Cameras:** Originally authorized December 2021, and again January 2024. Transition to Flock Safety approved March 2025. Surveillance Acquisition Report for Flock Condor cameras accepted July 2025. Updated Use Policies presented here reflect Council-directed revisions and require Council approval.

- **Drones:** Surveillance Acquisition Report accepted and Use Policy approved June 2023. These policies authorize BPD to request field-deployed UAS from outside agencies through mutual aid for specified circumstances. Council directed staff to explore a department run UAS program, including DFR, in November 2025. This item presents the Surveillance Acquisition Report, updated Use Policy, Impact Statement for BPD to acquire and use both field-deployed and DFR drones, and contract authority for recurring DFR costs.

- **Community Video Streams:** This technology was discussed at BPD’s January 2026 community meeting. This item presents the Surveillance Acquisition Report and Use Policy to Council for the first time. These materials were submitted to the

Police Accountability (PAB) in February 2026, and discussed during their subsequent regular public meetings.

- **Flock Nova:** Funded by the Byrne SCIP grant accepted by Council on July 2025, which identified investigative software as an eligible expenditure for the City's Gun Violence Intervention and Prevention Program.

Community Engagement

Every technology in this item has been subject to extensive community engagement and civilian oversight. The Police Accountability Board (PAB) has had the opportunity to review, discuss, and provide recommendations on each technology through public meetings, consistent with the deliberative process contemplated by the Surveillance Technology Ordinance and the Police Equipment Ordinance. A timeline of key engagement milestones follows:

- **ALPRs:** The PAB received the ALPR Surveillance Acquisition Report and Use Policy for review in May 2023. After independent review by the ODPA, the PAB held a special meeting in June 2023 to discuss the proposed policies. The Public Safety Policy Committee held a special meeting later in June 2023 to discuss the ALPR policies and voted to send a qualified positive recommendation to Council on the condition that PAB concerns be addressed. Council approved the Surveillance Acquisition Report and Use Policy in July 2023 and approved the ALPR contract in October 2023. The PAB received a BPD presentation on ALPR operations and data-sharing practices in November 2024.

- **Fixed Cameras:** The PAB reviewed the proposed surveillance camera policies in March 2023 and provided written recommendations. The Public Safety Policy Committee received updates on camera and drone policies in March 2023. Council discussed the camera use policies in May 2023 and approved the final use policy in June 2023. In January 2024, Council voted to approve additional camera locations. Council approved revised camera locations and the vendor transition to Flock Safety in March 2025, and the PAB reviewed the revised locations and vendor transition at its March 2025 meeting. In July 2025, Council heard from BPD and Flock Safety about data security and data-sharing before accepting the Surveillance Acquisition Report, with Council members directing additional safeguards including language from the PAB to limit system access and data sharing. Council continued its consideration of the fixed camera program at its September 2025 meeting, during which concerns about federal data access were raised and the vote was continued to allow additional review.

- **Drones:** The PAB first reviewed proposed UAS policies for borrowing drones through mutual aid in February 2023, after BPD provided draft policies and an acquisition report in January 2023. The earlier UAS policies were included in the June 2023 Council surveillance ordinance item alongside fixed camera policies. The PAB took up the Drone as First Responder issue at its September 2025 meeting and

voted to partner with UC Berkeley's Criminal Law & Justice Center to assess operational, legal, and oversight considerations. The Public Safety Policy Committee reviewed the DFR proposal in October 2025 and voted to send a positive recommendation to Council. At its November 2025 meeting, the PAB discussed data security concerns related to the Flock platform. The Council directed staff to explore a DFR program in November 2025 after a meeting in which Councilmembers posed detailed questions about data practices, recording policies, and privacy safeguards. The ODPA prepared a preliminary analysis of DFR technology, presented to the PAB at its December 2025 meeting. BPD presented the DFR Impact Statement and Use Policy to the PAB at its February 2026 meeting.

- **Community Meeting - January 15, 2026:** The Police Department held a well-attended open community information session on January 15, 2026, to discuss the full suite of current and proposed public safety technologies. The session, which received extensive local news coverage, described how fixed cameras, ALPRs, drones, and community video streams work in practice, the data protections in place for existing technology, and the safeguards planned for proposed new tools. Community members asked questions and provided feedback that informed the policies and contract terms presented here.

Throughout this process, the PAB has served its function as an independent civilian oversight body. While the PAB and BPD have not always agreed- and the Department respects the Board's independence to reach its own conclusions- the iterative process of presentation, questioning, public comment, and written recommendations has produced stronger policies. The engagement record on these technologies spans more than three years and 23 public meetings across the Police Accountability Board, Public Safety Policy Committee, City Council, and BPD-hosted community meeting.

Why Flock Safety

Staff conducted an extensive evaluation of available vendors for each technology category before recommending Flock Safety as the City's consolidated platform. The evaluation considered product capability, data security, contract flexibility, pricing, interoperability, and the vendor's responsiveness to the City's legal and policy requirements.

Product quality across categories

Flock Safety offers fully featured, field-proven products in every category the City seeks: license plate readers, fixed video surveillance, drone-as-first-responder, investigative analytics, and community camera integration. No other single vendor can deliver all of these capabilities. Staff evaluated competing products from Axon, Skydio, Brinc, Avigilon and others. Axon came closest to matching Flock's breadth, but its ALPR and fixed camera software currently offers only search capability and does not support alerts or hotlists, which are features that have added significant public safety value for the

City, particularly for real-time response. Other vendors required the City to own and maintain hardware, lacked real-time alerting, or could not provide the level of technical support and product upgrades that Flock delivers as part of its subscription model.

Single ecosystem advantage

Operating all public safety technology on a single platform creates substantial benefits for the City. From an oversight and audit perspective, a unified system means one dashboard, one set of access logs, one audit trail, and one point of accountability. This simplifies compliance with BMC 2.99, BMC 2.100, and AB 481 reporting requirements, and makes it easier to conduct regular audits. Operationally, officers benefit from a single login, consolidated alerts across camera types, and the ability to correlate data from ALPRs, fixed cameras, drones, and community streams in one workflow.

Contract and legal terms

The City Attorney's Office has negotiated a single Master Services Agreement with Flock Safety that governs all product lines. Every redline proposed by the City Attorney's Office was accepted by Flock. The MSA includes protections that go well beyond the vendor's standard terms of service:

- The City owns all of its data, including anonymized derivatives. Flock is prohibited from selling, sharing, or distributing City data without explicit City authorization.

- Flock may disclose data to a government agency only upon a legal request and with the City's written consent. Consistent with the City's sanctuary policies, footage cannot be provided to federal immigration authorities in response to an administrative subpoena or similar request without a court order.

- Flock has agreed to include contractual financial penalties for data breaches or unauthorized disclosures, mirroring the framework approved by the Oakland City Council in December 2025 for its Flock agreement.

- Flock must promptly notify the City of any security incident or data breach and describe the scope and corrective steps.

- The City's ownership and control of its data survives contract termination.

These terms would apply uniformly across all product lines under the MSA so there are consistent protections whether the City is using ALPRs, fixed cameras, drones, or analytics software.

Responsiveness to community and City concerns

Throughout the negotiation process, Flock Safety has demonstrated a willingness to align its practices with Berkeley's values. When the City Attorney's Office flagged concerns about federal access to data, Flock worked with staff to craft contract language that reflects the City's sanctuary city ordinance and state privacy law. When staff raised questions about data-sharing defaults based on reporting from other jurisdictions, Flock provided transparent answers and made platform changes so that settings are restrictive by default.

Staff independently confirmed with agencies that had experienced publicized issues that all concerns stemmed from default settings that were permissive out of the box, not from vendor overrides or policy violations. Flock has also stopped its federal data-sharing pilot programs nationally and introduced additional permission controls in response to community feedback from jurisdictions across the country. The company's willingness to accept every legal redline from the City Attorney's Office, proactively offer a financial penalty clause, and work iteratively with staff over time reflects an alignment of incentives and accountability.

Fiscal advantage

Flock has offered the City a 10% discount on new product lines- DFR, PTZ cameras, and Nova- if contracts are executed by the end of March 2026, representing over $100,000 in total savings. The ALPR renewal is priced at the existing contract rate. All prices across every product line meet or are below those listed for the same products on the Omnia cooperative purchasing consortium, which is the competitively bid procurement vehicle the City is using for this acquisition.

A consolidated procurement also reduces administrative overhead: one MSA, one vendor relationship, one procurement cycle, and one set of invoices, rather than managing separate agreements with multiple vendors. For reference, Alameda County is preparing a similar consolidated Flock procurement package for consideration later this year.

Technology Descriptions

Drone as First Responder (DFR) - New Technology

The DFR program provides BPD with drone dispatch capability integrated into the FlockOS platform. The system includes DJI Matrice 4TD drones with Dock 3 charging stations and Aerodome radar for detect-and-avoid capability. Drones launch from rooftop docking stations and can arrive at the scene of a call for service before ground units, providing real-time aerial video to dispatchers and responding officers. Within two years, the DJI hardware will be replaced with Flock's American-made, NDAA-compliant Alpha drone. The DFR Impact Statement and Use Policy are attached.

Community Video Streams - New Technology

This capability allows BPD to view live or recorded video from private cameras whose owners have voluntarily registered and opted in to share access. The system does not involve the City purchasing or installing any cameras. Instead, it uses Flock Safety's software to map registered camera locations and, with explicit owner permission, route video feeds to BPD's FlockOS dashboard. Before any camera is activated, BPD must complete a pre-integration review including an in-person site assessment and public notification signage. All integrated cameras will be published on the City website. Camera owners retain ownership and can revoke access at any time. Facial recognition is strictly prohibited. All BPD accesses of the streams are logged and auditable, and are restricted to the uses described in the attached use policies. The Surveillance Acquisition Report and Use Policy are attached.

Fixed Video Cameras (Pan-Tilt-Zoom) - Previously Approved, Policy Update

Solar-powered PTZ cameras installed and maintained by Flock Safety under a subscription model. The Surveillance Acquisition Report was accepted by Council on July 22, 2025. The updated Use Policies presented here incorporate Council-directed revisions and require Council approval before contract execution.

Nova - Grant-Funded Investigative Software

Nova is a data analysis platform that centralizes records from the department's computer-aided dispatch (CAD), records management system (RMS), and digital evidence management system. It also provides access to open-source intelligence and shared inter-agency data to support case-linking and firearm case resolution. This tool is funded by the SCIP grant and directly supports the City's Gun Violence Intervention and Prevention Program.

Automated License Plate Readers (ALPRs) - Contract Renewal

The City's existing network of 52 Flock Safety ALPR cameras. The current contract expires in July 2026. This item requests authority to renew for two years with an option for an additional two-year extension. No changes to the previously approved Surveillance Acquisition Report or Use Policy are proposed.

How It All Comes Together: A Real-Time Information Center

The technologies described above are not standalone tools. They are components of a single, integrated real-time information center (RTIC) that BPD will build around FlockOS. When a 911 call comes in, analysts can simultaneously dispatch a drone to the scene for aerial video, pull up nearby ALPR and fixed camera feeds, check community-registered cameras for relevant angles, and cross-reference vehicle or suspect information through Nova analytics- all from one dashboard, in real time.

To design and operationalize this workflow, BPD will seek to hire a Senior Crime Analyst and permanently fund a Crime Analyst position (currently grant funded) using savings generated by the reduction in sworn officer positions to manage the RTIC on an ongoing basis. In preparation for those roles, BPD is currently developing the operational infrastructure the analyst will rely on: building the operational workflows that connect each data stream, designing standard operating procedures for how dispatchers, analysts, and officers interact with the feeds, and ensuring strict compliance with the City's data policies and access controls. This approach is the core reason the single-platform strategy matters. Fragmented systems from multiple vendors would make real-time correlation impossible without extensive custom integration work. FlockOS provides it natively, and the analysts are the people turning that capability into a functioning operation.

An RTIC is designed to function as a resource multiplier, which is particularly important given BPD’s ongoing staffing challenges and the City’s constrained budget environment. Rather than requiring additional patrol officers or dispatchers to monitor each data source independently, the platform allows a single analyst to synthesize information across all systems simultaneously and surface actionable information to officers already in the field. This means BPD can extend its operational capacity without a proportional increase in personnel costs. At a time when the city is managing a significant structural deficit and recruiting, hiring, and retaining sworn officers remains difficult and expensive, an RTIC enables the department to do more with its existing workforce by directing resources more precisely, reducing reactive deployment, and improving response times without expanding headcount.

ENVIRONMENTAL SUSTAINABILITY AND CLIMATE IMPACTS

The ALPR and PTZ cameras operate on solar power and battery systems thereby limiting the carbon footprint of public safety operations. The DFR program may also reduce vehicle emissions by decreasing the number of patrol car dispatches to calls that can be assessed aerially.

RATIONALE FOR RECOMMENDATION

Approving this item allows the City to move forward on a comprehensive, integrated public safety technology program that has been years in development. Each component has either been previously reviewed and approved by Council or is presented here for the first time with full documentation under the applicable ordinances.

The consolidation into a single vendor platform is not merely a matter of administrative convenience. It is a deliberate choice to maximize oversight, simplify compliance, and ensure that every piece of technology the Police Department operates is governed by the same contractual protections, the same audit infrastructure, and the same accountability mechanisms. A single MSA, negotiated to the City’s specifications by the City Attorney’s Office and accepted in full by Flock, provides a durable legal framework

that protects the City's data, upholds its sanctuary policies, and holds the vendor to financial consequences for violations.

The proposed technology suite, funded by permanently eliminating 3 officer positions, will result in a net savings of about $160,000 per year to the General Fund after accounting for all technology subscription costs and the Crime Analyst positions, while providing response capabilities that multiply the effectiveness of public safety resources. That coupled with the 10% discount offered by Flock for execution by March 2026 provides a compelling fiscal incentive to act now, and the vendor's track record of responsiveness to this City's legal, policy, and community concerns gives staff confidence that this partnership will serve Berkeley well.

ALTERNATIVE ACTIONS CONSIDERED

Staff assessed and considered procuring each technology category from a different vendor. This approach was rejected because it would fragment oversight across multiple platforms, require separate MSAs with varying levels of data protection, increase administrative burden, and forgo the ecosystem discount. Staff also evaluated specific competing products, most notably from Axon, whose ALPR and fixed camera products currently lack the alerting and hotlist capabilities that are central to BPD's real-time response model. Maintaining the status quo- renewing the ALPR contract alone and deferring all other technologies- was considered but would leave Council-directed initiatives unfulfilled and forfeit the consolidated pricing advantage.

CONTACT PERSON

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

ATTACHMENTS

1. Resolution
2. Surveillance Acquisition Report: Unmanned Aerial Systems
3. Surveillance Use Policy (Policy 1303): Unmanned Aerial Systems
4. Police Equipment Impact Statement (Policy 709): Unmanned Aerial Systems
5. Police Equipment Use Policy (Policy 611): Unmanned Aerial Systems
6. Surveillance Acquisition Report: Community Video Streams
7. Surveillance Use Policies (Policies 355 and 1306): Community Video Streams
8. Updated Surveillance Use Policies (Policies 351 and 1304): Fixed Video Cameras
9. Master Services Agreement
10. Financial Penalties Amendment

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

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

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

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

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

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

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

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

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

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

WHEREAS, the City Attorney’s Office has negotiated a Master Services Agreement with Flock Safety that includes protections for City data ownership, restrictions on federal access consistent with the City’s sanctuary policies, financial penalties for unauthorized disclosures, security incident notification requirements, and post-termination data

protections, and Flock Safety has accepted every revision proposed by the City Attorney's Office; and

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

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

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

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

Surveillance Technology Ordinance Approvals

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

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

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

Police Equipment Ordinance Approvals

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

Contract Authority

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

6. The City Manager is authorized to amend the existing Contract #32400088 with Flock Group, Inc. (Flock Safety) to add fixed surveillance cameras for an initial four-

year term, in an amount not to exceed $310,000, with an option to extend for one additional three-year term, for a total amount not to exceed $600,000.

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

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

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

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

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

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

Background

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

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

1. Description

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

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

Description:

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

- Avata 2: This UAS would be used for tactical operations and searches within interior confined spaces such as a warehouse, commercial building or residence.
- DJI Matrice 4T: This UAS would be used for patrol operations to rapidly respond to the scene of an incident and provide real-time video and situational awareness to officers responding to the scene. These systems would include the UAS, batteries, and software integration with our current CAD and Flock systems.

- DJI Matrice 4TD / Flock Alpha: This UAS would be dedicated to DFR response to rapidly respond to the scene of an incident and provide real-time video and situational awareness to officers responding to the scene. It would also include the installation of two charging and telecommunications docks on the roof of the Public Safety Building. Within two years, this UAS would be replaced with Flock Alpha UAS and a battery swapping dock.

How it Works:

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

Manufacturers' Descriptions:

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

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

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

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

2. Purpose

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

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

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

3. Location

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

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

4. Impact

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

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

5. Mitigations

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

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

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

6. Data Types and Sources

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

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

7. Data Security

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

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

8. Fiscal Cost

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

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

Initial Cost:

- Purchase of field-based UAS (Avata 2 & Matrice 4T): Total $44,500.
- Lease of PSB-based DFR (Year 1): $100,000.
- Radar (Year 1): included.
- Dock Installation: $15,000.

Cost of Use:

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

Costs of Potential Adverse Impacts:

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

Annual and Ongoing Costs:

- DFR Lease: $125,000 per year (includes upgrade to Flock Alpha).
- Radar: $150,000 per year.
- Parts/Maintenance (for purchased units): $2,000 per year.

Training Costs:

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

Maintenance and Storage Costs:

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

Upgrade Costs:

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

9. Third Party Dependence and Access

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

All UAS data will be uploaded and stored on Axon's Evidence.com platform in line with existing departmental protocol for evidence collection. Axon complies with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union and Switzerland to the United States

(collectively, "Privacy Shield"). Axon has certified to the U.S. Department of Commerce that it adheres to the Privacy Shield Principles.

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

10. Alternatives

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

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

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

11. Experience of Other Entities

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

The Alameda County Sheriff's Office has operated its UAS program since 2015 and only reports a single community complaint, which was ultimately deemed unrelated to drone activity. The agency implemented a public transparency portal and documented multiple

operational successes, including enhanced officer safety, improved suspect apprehension, efficient crime scene documentation, and the successful location of missing persons.

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

The Fremont Police Department began using UAS technology in 2017 and now maintains a fleet of 16 drones operated by 25 trained personnel. The department reports no community complaints, maintains regular updates to its transparency portal, and is currently developing its Drone as First Responder (DFR) capability. Fremont Police report that the program delivers significant operational advantages and has become an integrated part of its modern policing strategy.

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

Policy
1303

Law Enforcement Services Manual

Surveillance Use Policy-Unmanned Aerial System (UAS)

1303.1 PURPOSE

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

1303.2 AUTHORIZED USE

Authorized operators may deploy the UAS in the following circumstances:

1. To provide real-time situational awareness during high-risk or critical incidents, such as barricaded suspects, hostage situations, active shooters, the apprehension of armed and dangerous suspects, the pre-planning and service of a warrant allowing officers to create time and distance to formulate de-escalation strategies, facilitate safe tactical planning, and reduce the need for immediate physical engagement.

2. To assist in locating lost, missing, or injured persons during search and rescue operations.

3. To rapidly respond to calls for service to verify the nature of the incident, potentially determining that a law enforcement response is unnecessary for unfounded reports or low-priority incidents, thereby acting as a resource multiplier and keeping patrol officers available for other calls.

4. To locate fleeing suspects to effectively contain perimeters and reduce the need for dangerous ground-based foot pursuits.

5. To track fleeing vehicles from a safe distance, allowing patrol units to de-escalate or terminate dangerous ground pursuits while maintaining visual contact.

6. To clear interior buildings or confined spaces remotely to prevent potentially violent encounters between officers and hidden suspects.

7. To assist the Fire Department with fire mitigation and suppression, hazardous materials releases, or disaster response and recovery.

8. To remotely inspect potential explosive devices or hazardous objects.

9. To document complex crime scenes, accident scenes, or areas where an aerial perspective is critical for the investigation.

10. To respond to active criminal activity at mass gatherings or special events.

11. To mitigate hazards caused by other UAS interfering with emergency operations.

12. For pilot certification training and maintenance of proficiency.

13. To address other unforeseen exigent circumstances where there is an imminent threat to public safety, provided the deployment is consistent with the general privacy and safety principles of this policy.

1303.3 PROHIBITED USE

The UAS shall not be used:

1. To conduct random or arbitrary surveillance activities. This prohibition includes, but is not limited to, first amendment assemblies in accordance with Policy 428 First Amendment Assemblies.

2. To target a person based solely on actual or perceived characteristics, such as race, ethnicity, national origin, religion, sex, sexual orientation, gender identity or expression, economic status, age, cultural group, or disability.

3. To harass, intimidate, or discriminate against any individual or group.

Furthermore, the UAS shall not be equipped with:

1. Facial recognition software

2. Biometric analysis capabilities

3. Weapons of any kind, including lethal or non-lethal munitions.

1303.4 DATA COLLECTION

Data collection shall be limited to video (visible and infrared) and associated telemetry

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

1303.5 DATA ACCESS

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

1303.6 DATA PROTECTION

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

1303.7 CIVIL LIBERTIES AND RIGHTS PROTECTIONS

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

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

1. Absent a warrant or exigent circumstances, operators and observers shall adhere to FAA regulations and shall not intentionally record or transmit images of any location where a person would have a reasonable expectation of privacy (e.g., residence, yard, enclosure).

2. Operators and observers shall take reasonable precautions to avoid inadvertently recording or transmitting images of uninvolved community members or areas where there is a reasonable expectation of privacy. Cameras shall be diverted away from private spaces when not actively engaged in a permitted use.

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

1303.8 DATA RETENTION

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

1303.9 PUBLIC ACCESS

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

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

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

1303.10 THIRD PARTY DATA SHARING

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

1303.11 TRAINING

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

1303.12 AUDITING AND OVERSIGHT

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

The Office of Strategic Planning and Accountability shall conduct biennial audits of UAS use.

Intentional violation of this policy may serve as grounds for disciplinary action pursuant to the Policy 1010, Personnel Complaints policy.

1303.13 MAINTENANCE

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

Background

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

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

1. Description

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

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

Description:

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

- Avata 2: This UAS would be used for tactical operations and searches within interior confined spaces such as a warehouse, commercial building or residence.

- DJI Matrice 4T: This UAS would be used for patrol operations to rapidly respond to the scene of an incident and provide real-time video and situational awareness to officers responding to the scene. These systems would include the UAS, batteries, and software integration with our current CAD and Flock systems.
- DJI Matrice 4TD / Flock Alpha: This UAS would be dedicated to DFR response to rapidly respond to the scene of an incident and provide real-time video and situational awareness to officers responding to the scene. It would also include the installation of two charging and telecommunications docks on the roof of the Public Safety Building. Within two years, this UAS would be replaced with Flock Alpha UAS and a battery swapping dock.

Quantity:

Our initial purchase recommendation for drones is:

- DJI Avata 2: 4 units
- DJI Matrice 4T: 4 units
- DJI Matrice 4TD: 2 units
- Flock Alpha: 1 unit to replace the 2 Matrice 4TDs within 2 years

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

Capabilities:

- The Avata 2 is a compact system designed for operation in confined interior spaces. It allows officers to remotely search buildings during high-risk alarms or warrant services, minimizing the need for officers to physically enter potentially hazardous environments without prior visual assessment.
- The Matrice 4T is a field-deployed unit carried by patrol officers for immediate operational support. It features high-resolution thermal and zoom sensors ideal for locating missing persons in complex terrain or tracking fleeing suspects to prevent dangerous ground pursuits.
- The Matrice 4TD and Flock Alpha serve as the core of the Drone as First Responder (DFR) program. These systems are capable of autonomous dispatch to calls for service, often arriving before ground units. This capability allows for the rapid verification of incidents, potentially allowing officers to downgrade their response or clear unfounded calls without physical police presence. They provide real-time

situational awareness to responding officers and facilitate safer approaches and de-escalation strategies.

Lifespan:

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

Uses and Effects:

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

How it Works:

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

Manufacturers' Descriptions:

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

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

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

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

2. Purpose

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

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

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

3. Fiscal Cost

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

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

Initial Cost:

- Purchase of field-based UAS (Avata 2 & Matrice 4T): Total $44,500.
- Lease of PSB-based DFR (Year 1): $100,000.
- Radar (Year 1): included.
- Dock Installation: $15,000.

Cost of Use:

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

Costs of Potential Adverse Impacts:

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

Annual and Ongoing Costs:

- DFR Lease: $125,000 per year (includes upgrade to Flock Alpha).
- Radar: $150,000 per year.
- Parts/Maintenance (for purchased units): $2,000 per year.

Training Costs:

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

Maintenance and Storage Costs:

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

Upgrade Costs:

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

4. Impact

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

Welfare and Safety

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

Civil Rights and Civil Liberties

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

5. Mitigations

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

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

- All DFR cameras will be programmed to orient toward the horizon (preventing ground recording) while in transit to a call for service. The camera will only point down upon arrival at the authorized scene.

- All UAS flights are logged, and flight data is auditable. Video data is stored on secure, encrypted servers (Evidence.com) with strict chain-of-custody controls.
- The UAS will not be equipped with facial recognition software or weapons of any kind.
- As required by BMC 2.99 and BMC 2.100, the Department will publish data regarding deployments on an annual basis.
- Information including flight logs and incident type will be published on a publicly accessible transparency portal shortly after the conclusion of a flight, typically within 1 hour after docking.
- The program is subject to review by the Police Accountability Board and approval by the City Council via the Annual Military Equipment Report and the Annual Surveillance Technology Report.

6. Alternatives

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

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

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

7. Third Party Dependence

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

All UAS data will be uploaded and stored on Axon's Evidence.com platform in line with existing departmental protocol for evidence collection. Axon complies with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union and Switzerland to the United States (collectively, "Privacy Shield"). Axon has certified to the U.S. Department of Commerce that it adheres to the Privacy Shield Principles.

8. Legal and Procedural Rules

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

9. Training

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

Policy
611

Berkeley Police Department

Law Enforcement Services Manual

Unmanned Aerial System (UAS) Operations

611 PURPOSE AND SCOPE

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

611.1 DEFINITIONS

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

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

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

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

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

611.2 POLICY

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

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

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

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

611.3 PRIVACY

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

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

1) Absent a warrant or exigent circumstances, operators and observers shall adhere to FAA regulations and shall not intentionally record or transmit images of any location where a person would have a reasonable expectation of privacy (e.g., residence, yard, enclosure).

2) Operators and observers shall take reasonable precautions to avoid inadvertently recording or transmitting images of uninvolved community members or areas where there is a reasonable expectation of privacy. Cameras shall be diverted away from private spaces when not actively engaged in a permitted use.

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

611.4 PROGRAM COORDINATOR

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

611.5 PERMITTED USE

Authorized operators may deploy the UAS in the following circumstances:

1) To provide real-time situational awareness during high-risk or critical incidents, such as barricaded suspects, hostage situations, active shooters, the apprehension of armed and dangerous suspects, the pre-planning and service of a warrant allowing officers to create time and distance to formulate de-escalation strategies, facilitate safe tactical planning, and reduce the need for immediate physical engagement.

2) To assist in locating lost, missing, or injured persons during search and rescue operations.

3) To rapidly respond to calls for service to verify the nature of the incident, potentially determining that a law enforcement response is unnecessary for unfounded reports or low-priority incidents, thereby acting as a resource multiplier and keeping patrol officers available for other calls.

4) To locate fleeing suspects to effectively contain perimeters and reduce the need for dangerous ground-based foot pursuits.

5) To track fleeing vehicles from a safe distance, allowing patrol units to de-escalate or terminate dangerous ground pursuits while maintaining visual contact.

6) To clear interior buildings or confined spaces remotely to prevent potentially violent encounters between officers and hidden suspects.

7) To assist the Fire Department with fire mitigation and suppression, hazardous materials releases, or disaster response and recovery.

8) To remotely inspect potential explosive devices or hazardous objects.

9) To document complex crime scenes, accident scenes, or areas where an aerial perspective is critical for the investigation.

10) To respond to active criminal activity at mass gatherings or special events.

11) To mitigate hazards caused by other UAS interfering with emergency operations.

12) For pilot certification training and maintenance of proficiency.

13) To address other unforeseen exigent circumstances where there is an imminent threat to public safety, provided the deployment is consistent with the general privacy and safety principles of this policy.

611.6 PROHIBITED USE

1) The UAS shall not be used:

    a) To conduct random or arbitrary surveillance activities. This prohibition includes,

but is not limited to, first amendment assemblies in accordance with Policy 428 First Amendment Assemblies.

b) To target a person based solely on actual or perceived characteristics, such as race, ethnicity, national origin, religion, sex, sexual orientation, gender identity or expression, economic status, age, cultural group, or disability.

c) To harass, intimidate, or discriminate against any individual or group.

2) Furthermore, the UAS shall not be equipped with:

a) Facial recognition software

b) Biometric analysis capabilities

c) Weapons of any kind, including lethal or non-lethal munitions.

611.7 TRAINING

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

611.8 RETENTION REQUIREMENTS

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

611.9 RELEASE OF RECORDINGS

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

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

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

Background

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

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

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

1. Description

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

Description:

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

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

How it Works:

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

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

Manufacturers' Descriptions:

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

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

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

2. Purpose

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

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

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

3. Location

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

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

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

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

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

4. Impact

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

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

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

5. Mitigations

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

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

- Access is strictly permission-based. Camera owners must actively "opt-in" and can revoke access at any time.
- The use of facial recognition technology on any stream is strictly prohibited.
- All system access is logged. The audit trail records the user, date, time, and specific camera accessed as well as the case number and/or reason.
- Data is stored on CJIS-compliant servers.

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

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

6. Data Types and Sources

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

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

7. Data Security

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

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

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

8. Fiscal Cost

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

The costs below represent estimates. Hardware costs and integration costs are paid by the private camera owners.

Initial Cost:

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

Cost of Use:

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

Costs of Potential Adverse Impacts:

- Potential costs could arise from data breach litigation or claims of privacy violation. However, the reliance on voluntary consent to access cameras that already are in place as well as strict audit logs minimizes this risk. Strict adherence to the Use Policy will further mitigate liability.

Annual and Ongoing Costs:

- No ongoing costs are incurred by the Department.

Training Costs:

- Training is included in the software subscription and absorbed into regular in-service training hours.

Maintenance and Storage Costs:

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

Upgrade Costs:

- Software upgrades are included in the annual subscription model.

9. Third Party Dependence and Access

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

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

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

10. Alternatives

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

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

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

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

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

11. Experience of Other Entities

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

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

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

Community Video Streams

355.1 PURPOSE AND SCOPE

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

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

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

355.2 POLICY

The Berkeley Police Department utilizes a community video streams system to enhance its anti-crime strategy, to effectively allocate and deploy personnel, support investigations, and to enhance safety and security in public areas. As specified by this policy, cameras owned by community partners in strategic locations throughout the City may be shared with the Police Department in order to record, deter, and solve crimes, to help the City safeguard against potential threats to the public, and to help manage emergency response situations during natural and human-made disasters, among other uses specified in Section 355.3.1.

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

355.3 OPERATIONAL GUIDELINES

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

355.3.1 PLACEMENT REVIEW AND MONITORING

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

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

- To facilitate rapid response to active shooter events, mass casualty incidents, or other critical public safety threats, the Department may enter into agreements with facilities or

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

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

355.3.2 COMMUNITY VIDEO STREAM CAMERA MARKINGS

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

355.3.3 INTEGRATION WITH OTHER TECHNOLOGY

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

355.3.4 PRE-INTEGRATION REVIEW

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

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

355.4 VIDEO SUPERVISION

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

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

355.4.1 VIDEO LOG

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

355.4.2 PROHIBITED ACTIVITY

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

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

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

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

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

355.5 STORAGE AND RETENTION OF MEDIA

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

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

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

355.5.1 EVIDENTIARY INTEGRITY

All media downloaded and retained pursuant to this Policy shall be treated in the same manner as other evidence. Media shall be accessed, maintained, stored and retrieved in a manner that ensures its integrity as evidence, including strict adherence to chain of custody requirements. Electronic trails, including encryption, digital masking of innocent or uninvolved individuals to preserve anonymity, authenticity certificates and date and time stamping, shall be used as appropriate to preserve individual rights and to ensure the authenticity and maintenance of a secure evidentiary chain of custody.

355.6 RELEASE OF VIDEO IMAGES

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

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

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

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

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

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

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

355.7 COMMUNITY VIDEO STREAMS AUDIT

The community video streams software generates a site log each time the system is accessed. The site log is broken down by server, device, user or general access. The site log is kept on the server for two years and is exportable for reporting. System audits will be conducted by the Office of Strategic Planning and Accountability (OSPA) on a regular basis, at least biennial. As part of the audit, OSPA will confirm that BPD does not enter any direct data sharing agreements or give direct access to outside agencies. A log of any instance of when surveillance footage has been shared, including date, time, reasons for search, and any recipient agencies.

BPD will enforce against prohibited uses of the cameras pursuant to Policy 1010, Personnel Complaints, or other applicable law or policy. The City Manager shall enforce against any

prohibited use of cameras and/or access to data by other City of Berkeley personnel.

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

355.8 TRAINING

All BPD members authorized to access community video streams systems shall receive appropriate training. Training should include guidance on the use of cameras, associated software, and review of relevant policies and procedures, including this policy as well as review of relevant City of Berkeley laws and regulations. Training should also address state and federal law related to the use of video surveillance equipment and privacy. All relevant recordings that are utilized will be collected pursuant to Policy 802 Property and Evidence, and retained pursuant to Policy 804 Records and Maintenance.

355.9 MAINTENANCE

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

Surveillance Use Policy - Community Video Streams

1306.1 PURPOSE

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

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

1306.2 AUTHORIZED USE

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

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

(a) To support specific and active criminal investigations.

(b) To support serious traffic-related investigations.

(c) To support police misconduct investigations, and

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

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

The following are prohibited uses of the video surveillance system:

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

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

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

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

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

(f) Community video streams and recordings that are retained by Berkeley Police Department as evidence shall not be disclosed to law enforcement agencies from other states if the purpose of the request is to support the enforcement of laws that restrict or criminalize reproductive rights or rights regarding the provision or receipt of gender-affirming care.

1306.3 DATA COLLECTION

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

1306.4 DATA ACCESS

Access to community video streams data shall be limited to BPD personnel utilizing the camera database for uses described above and pursuant to the Community Video Streams Policy. BPD members seeking access to the video surveillance system shall obtain the approval of the Investigations Division Captain, or their designee.

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

1306.5 DATA PROTECTION

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

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

1306.6 CIVIL LIBERTIES AND RIGHTS PROTECTION

The Berkeley Police Department is dedicated to the most efficient utilization of its resources and services in its public safety endeavors. The Berkeley Police Department recognizes the need to

protect its ownership and control over shared information and to protect the privacy and civil liberties of the public, in accordance with federal and state law. Provisions of this policy, including 1306.4 Data Access, 1306.5 Data Protection, 1306.7 Data Retention, 1306.8 Public Access, 1306.9 Third Party Data Sharing, and 1306.13 Pre-Integration Review serve to protect against any unauthorized use of community video streams. The use of facial recognition technology on any community video stream is prohibited. These procedures ensure the data is not used in a way that would violate or infringe upon anyone's civil rights and/or liberties, including but not limited to potentially disparate or adverse impacts on any communities or groups.

1306.7 DATA RETENTION

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

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

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

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

1306.8 PUBLIC ACCESS

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

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

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

1306.9 THIRD-PARTY DATA-SHARING

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

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

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

1306.10 TRAINING

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

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

1306.11 AUDITING AND OVERSIGHT

The community video streams software generates a site log each time the system is accessed. The video surveillance software generates a site log each time the system is accessed. The site log is broken down by server, device, user or general access. The site log is kept on the server for two years and is exportable for reporting. Community video stream audits will be conducted on a regular basis, at least biennial. As part of the audit, OSPA will confirm that BPD does not enter any direct data sharing agreements or give direct access to outside agencies. A log of any instance of when surveillance footage has been shared, including date, time, reasons for search, and any recipient agencies.

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

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

1304.12 ACCOUNTABILITY

All saved data will be safeguarded and protected by both procedural and technological means. The Berkeley Police Department will observe the following safeguards regarding access to and use of stored data:

(a) Non-law enforcement requests for access to stored community video streams data shall be processed according to the Records Maintenance and Release Policy in accordance with applicable law.

(b) All community video streams data downloaded to any workstation or server shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time.

(c) Berkeley Police Department members approved to access community video streams data under these guidelines are permitted to access the data for legitimate California law enforcement purposes only, such as when the data relate to a specific criminal

investigation or department-related civil or administrative action.

(d) Aggregated community video streams data not related to specific criminal investigations shall not be released to any local, state or federal agency or entity without the consent of the Chief of Police or City Manager.

(e) Measures will be taken to ensure the accuracy of community video streams information. Errors discovered in community video streams data collected by community video streams units shall be marked, corrected or deleted in accordance with the type and severity of the error in question.

(f) Such community video streams data may be released to other authorized and verified law enforcement officials and agencies for legitimate California law enforcement purposes.

(g) Every community video streams browsing inquiry must be documented by either the associated Berkeley Police case number or incident number, and/or a reason for the inquiry. For security or data breaches, see the Records Release and Maintenance Policy.

1306.12 MAINTENANCE

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

1306.13 PRE-INTEGRATION REVIEW

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

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

External Fixed Video Surveillance Cameras

351.1 PURPOSE AND SCOPE

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

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

351.2 POLICY

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

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

351.3 OPERATIONAL GUIDELINES

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

351.3.1 PLACEMENT REVIEW AND MONITORING

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

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

Current City Council approved locations:

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

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

(a) To support specific and active criminal investigations.

(b) To support serious traffic-related investigations.

(c) To support police misconduct investigations,

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

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

351.3.2 FIXED CAMERA MARKINGS

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

351.3.3 INTEGRATION WITH OTHER TECHNOLOGY

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

351.4 VIDEO SUPERVISION

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

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

351.4.1 VIDEO LOG

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

351.4.2 PROHIBITED ACTIVITY

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

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

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

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

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

351.5 STORAGE AND RETENTION OF MEDIA

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

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

351.5.1 EVIDENTIARY INTEGRITY

All media downloaded and retained pursuant to this Policy shall be treated in the same manner

as other evidence. Media shall be accessed, maintained, stored and retrieved in a manner that ensures its integrity as evidence, including strict adherence to chain of custody requirements. Electronic trails, including encryption, digital masking of innocent or uninvolved individuals to preserve anonymity, authenticity certificates and date and time stamping, shall be used as appropriate to preserve individual rights and to ensure the authenticity and maintenance of a secure evidentiary chain of custody.

351.6 RELEASE OF VIDEO IMAGES

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

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

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

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

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

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

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

351.7 VIDEO SURVEILLANCE AUDIT

The video surveillance software generates a site log each time the system is accessed. The site log is broken down by server, device, user or general access. The site log is kept on the server for two years and is exportable for reporting. System audits will be conducted by the Office of Strategic Planning and Accountability (OSPA) on a regular basis, at least biennial. As part of the audit, OSPA will confirm that BPD doesn't enter any direct data sharing agreements or give direct access to outside agencies. A log of any instance of when surveillance footage has been shared, including date, time, reasons for search, and any recipient agencies.

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

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

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

351.8 TRAINING

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

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

351.9 MAINTENANCE

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

Surveillance Use Policy-External Fixed Video Surveillance Cameras

1304.1 PURPOSE

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

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

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

1304.2 AUTHORIZED USE

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

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

(a) To support specific and active criminal investigations.

(b) To support serious traffic-related investigations.

(c) To support police misconduct investigations, and

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

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

The following are prohibited uses of the video surveillance system:

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

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

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

(d) Video surveillance equipment shall not be used to harass, intimidate or discriminate against any individual or group.
(e) Video surveillance systems and recordings are subject to the Berkeley Police Department's Immigration Law Policy, and hence may not be shared with federal immigration enforcement officials, unless required by federal law.
(f) Video recordings shall not be disclosed to law enforcement agencies from other states if the purpose of the request is to support the enforcement of laws that restrict or criminalize reproductive rights or rights regarding the provision or receipt of gender-affirming care.

1304.3 DATA COLLECTION

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

1304.4 DATA ACCESS

Access to video surveillance cameras data shall be limited to BPD personnel utilizing the camera database for uses described above and pursuant to Use Policy 351, with technical assistance from Public Works Department and Department of Information Technology personnel. Information may be shared in accordance with 1304.9 below. BPD members seeking access to the video surveillance system shall obtain the approval of the Investigations Division Captain, or their designee.

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

1304.5 DATA PROTECTION

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

1304.6 CIVIL LIBERTIES AND RIGHTS PROTECTION

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

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

1304.7 DATA RETENTION

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

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

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

1304.8 PUBLIC ACCESS

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

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

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

1304.9 THIRD-PARTY DATA-SHARING

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

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

(a) The District Attorney's Office for use as evidence to aid in prosecution, in accordance with laws governing evidence;

(b) Other law enforcement personnel as part of an active criminal investigation;

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

Requests for recorded video from the Office of Director of Police Accountability and Police Accountability Board shall be referred to the Investigations Division Captain, or their designee, for release in accordance with Charter Article XVIII, Section 125, Subdivision (20)(a). The Chief of Police will report any request from federal immigration authorities, vendor, or any non-local agency to access data for federal immigration enforcement purposes within 10 days of receiving the request.

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

1304.10 TRAINING

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

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

1304.11 AUDITING AND OVERSIGHT

The video surveillance software generates a site log each time the system is accessed. The site log is broken down by server, device, user or general access. The site log is kept on the server for two years and is exportable for reporting. External fixed video surveillance camera system audits will be conducted by the Office of Strategic Planning and Accountability (OSPA) on a regular basis, at least biennial. As part of the audit, OSPA will confirm that BPD doesn't enter any direct data sharing agreements or give direct access to outside agencies. A log of any instance of when surveillance video and/or audio data has been shared, including date, time, reasons for search, and any recipient agencies.

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

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

Surveillance Use Policy-External Fixed Video Surveillance Cameras

1304.12 ACCOUNTABILITY

All saved data will be safeguarded and protected by both procedural and technological means. The Berkeley Police Department will observe the following safeguards regarding access to and use of stored data:

(a) Non-law enforcement requests for access to stored external fixed video surveillance camera data shall be processed according to the Records Maintenance and Release Policy in accordance with applicable law.

(b) All external fixed video surveillance camera data downloaded to any workstation or server shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time.

(c) Berkeley Police Department members approved to access external fixed video surveillance camera data under these guidelines are permitted to access the data for legitimate California law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action.

(d) Aggregated external fixed video surveillance camera data not related to specific criminal investigations shall not be released to any local, state or federal agency or entity without the consent of the Chief of Police or City Manager.

(e) Measures will be taken to ensure the accuracy of external fixed video surveillance camera information. Errors discovered in external fixed video surveillance camera data collected by external fixed video surveillance camera units shall be marked, corrected or deleted in accordance with the type and severity of the error in question.

(f) Such external fixed video surveillance camera data may be released to other authorized and verified law enforcement officials and agencies for legitimate California law enforcement purposes.

(g) Every external fixed video surveillance camera browsing inquiry must be documented by either the associated Berkeley Police case number or incident number, and/or a reason for the inquiry. For security or data breaches, see the Records Release and Maintenance Policy.

1304.13 MAINTENANCE

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

Master Services Agreement

This Master Services Agreement (this "***Agreement***") is entered into by and between Flock Group, Inc. with a place of business at 1170 Howell Mill Road NW Suite 210, Atlanta, GA 30318 ("***Flock***") and the City of Berkeley ("***Customer***") (each a "***Party***," and together, the "***Parties***") on this the ___ day of _____ 2026. This Agreement is effective on the date of mutual execution ("***Effective Date***"). Parties will sign an Order Form ("***Order Form***") which will describe the Flock Services to be performed and the period for performance, attached hereto as **Exhibit A**. The Parties agree as follows:

RECITALS

WHEREAS, Flock offers a software and hardware situational awareness solution through Flock's technology platform that upon detection is capable of capturing audio, video, image, and recording data and provide notifications to Customer ("***Notifications***");

WHEREAS, Customer desires access to the Flock Services (defined below) on existing devices, provided by Customer, or Flock provided Flock Hardware (as defined below) in order to create, view, search and archive Footage and receive Notifications, via the Flock Services;

WHEREAS, Customer shall have access to the Footage in Flock Services. Pursuant to Flock's standard Retention Period (defined below) Flock deletes all Footage on a rolling thirty (30) day basis, except as otherwise stated on the ***Order Form***. Customer shall be responsible for extracting, downloading and archiving Footage from the Flock Services on its own storage devices; and

WHEREAS, Flock desires to provide Customer the Flock Services and any access thereto, subject to the terms and conditions of this Agreement, solely for the awareness, prevention, and prosecution of crime, bona fide investigations and evidence gathering for law enforcement purposes, ("***Permitted Purpose***").

NOW, THEREFORE, Flock and Customer agree that this Agreement, and any Order Form, purchase orders, statements of work, product addenda, or the like, attached hereto as exhibits and incorporated by reference, constitute the complete and exclusive statement of the Agreement of the Parties with respect to the subject matter of this Agreement, and replace and supersede all prior agreements, term sheets, purchase orders, correspondence, oral or written communications and negotiations by and between the Parties.

1. DEFINITIONS

Certain capitalized terms, not otherwise defined herein, have the meanings set forth or cross-referenced in this Section 1.

1.1 "***Anonymized Data***" means Customer Data or Customer Generated Data permanently stripped of identifying details and any potential personally identifiable information, by commercially available standards which irreversibly alters data in such a way that a data subject (i.e., individual person or entity) can no longer be identified directly or indirectly.

1.2 "***Authorized End User(s)***" means any individual employees, agents, or contractors of Customer accessing or using the Services, under the rights granted to Customer pursuant to this Agreement.

1.3 "***Customer Data***" means the data, media and content provided by Customer through the Services. For the avoidance of doubt, the Customer Data includes Footage and Anonymized Data.

1.4. "***Customer Hardware***" means the third-party camera owned or provided by Customer and any other physical elements that interact with the Embedded Software and the Web Interface to provide the Services.

1.5 "***Embedded Software***" means the Flock proprietary software and/or firmware integrated with or installed on the Flock Hardware or Customer Hardware.

1.6 "***Flock Hardware***" means the Flock device(s), which may include the pole, clamps, solar panel, installation components, and any other physical elements that interact with the Embedded Software and the Web Interface, to provide the Flock Services as specifically set forth in the applicable product addenda.

1.7 "***Flock IP***" means the Services, the Embedded Software, and any intellectual property or proprietary information therein or otherwise provided to Customer and/or its Authorized End Users. Flock IP does not include Footage (as defined below).

1.8 "***Flock Network End User(s)***" means any user of the Flock Services that Customer authorizes access to or receives data from, pursuant to the licenses granted herein.

1.9 "***Flock Services***" means the provision of Flock's software and hardware situational awareness solution, via the Web Interface, for automatic license plate detection, alerts, audio detection, searching image records, video and sharing Footage.

1.10 "***Footage***" means still images, video, audio and other data captured by the Flock Hardware or Customer Hardware in the course of and provided via the Flock Services.

1.11 *"**Hotlist(s)***" means a digital file containing alphanumeric license plate related information pertaining to vehicles of interest, which may include stolen vehicles, stolen vehicle license plates, vehicles owned or associated with wanted or missing person(s), vehicles suspected of being involved with criminal or terrorist activities, and other legitimate law enforcement purposes. Hotlist also includes, but is not limited to, national data (i.e., NCIC) for similar categories, license plates associated with AMBER Alerts or Missing Persons/Vulnerable Adult Alerts, and includes manually entered license plate information associated with crimes that have occurred in any local jurisdiction.

1.12 "***Installation Services***" means the services provided by Flock for installation of Flock Services.

1.13 "***Retention Period***" means the time period that the Customer Data is stored within the cloud storage, as specified in the product addenda.

1.14 "***Vehicle Fingerprint™***" means the unique vehicular attributes captured through Services such as: type, make, color, state registration, missing/covered plates, bumper stickers, decals, roof racks, and bike racks.

1.15 "***Web Interface***" means the website(s) or application(s) through which Customer and its Authorized End Users can access the Services.

2. SERVICES AND SUPPORT

2.1 **Provision of Access.** Flock hereby grants to Customer a non-exclusive, non-transferable right to access the features and functions of the Flock Services via the Web Interface during the Term, solely for the Authorized End Users. The Footage will be available for Authorized End Users to access and download via the Web Interface for the data retention time defined on the Order Form ("***Retention Period***"). Authorized End Users will be required to sign up for an account and select a password and username ("***User ID***"). Customer shall be responsible for all acts and omissions of Authorized End Users, and any act or omission by an Authorized End User which, including any acts or omissions of Authorized End User which would constitute a breach of this agreement if undertaken by Customer. Customer shall undertake reasonable efforts to make all Authorized End Users aware of all applicable provisions of this Agreement and shall cause Authorized End Users to comply with such provisions. Flock may use the services of one or more third parties to deliver any part of the Flock Services, (such as using a third party to host the Web Interface for cloud storage or a cell phone provider for wireless cellular coverage).

2.2 **Embedded Software License.** Flock grants Customer a limited, non-exclusive, non-transferable, non-sublicensable (except to the Authorized End Users), revocable right to use the Embedded Software as it pertains to Flock Services, solely as necessary for Customer to use the Flock Services.

2.3 **Support Services.** Flock shall monitor the Flock Services, and any applicable device health, in order to improve performance and functionality. Flock will use commercially reasonable efforts to respond to requests for support within seventy-two (72) hours. Flock will provide Customer with reasonable technical and on-site support and maintenance services in-person, via phone or by email at support@flocksafety.com (such services collectively referred to as ***"Support Services"***).

2.4 **Upgrades to Platform.** Flock may make any upgrades to system or platform that it deems necessary or useful to (i) maintain or enhance the quality or delivery of Flock's products or services to its agencies, the competitive strength of, or market for, Flock's products or services, such platform or system's cost efficiency or performance, or (ii) to comply with applicable law. Parties understand that such upgrades are necessary from time to time and will not diminish the quality of the services or materially change any terms or conditions within this Agreement.

2.5 **Service Interruption.** Services may be interrupted in the event that: (a) Flock's provision of the Services to Customer or any Authorized End User is prohibited by applicable law; (b) any third-party services required for Services are interrupted; (c) Flock reasonably believes Services are being used for malicious, unlawful, or otherwise unauthorized use; (d) there is a threat or attack on any of the Flock IP by a third party; or (e) scheduled or emergency maintenance necessitates interruption ("***Service Interruption***"). Flock will make commercially reasonable efforts to provide written notice of any Service Interruption to Customer, to provide updates, and to resume providing access to Flock Services as soon as reasonably possible after the event giving rise to the Service Interruption is cured. Flock will have no liability for any damage, liabilities, losses (including any loss of data or profits), or any other consequences that Customer or any Authorized End User may incur as a result of a Service Interruption. To the extent that the Service Interruption is not caused by Customer's direct actions or by the actions of parties associated with the Customer, the time will be tolled by the duration of the Service Interruption (for any continuous suspension lasting at least one full day). For example, in the event of a Service Interruption lasting five (5) continuous days, Customer will receive a credit for five (5) free days at the end of the Term.

2.6 **Service Suspension.** Flock may temporarily suspend Customer's and any Authorized End User's access to any portion or all of the Flock IP or Flock Service if (a) there is a threat or attack on any of the Flock IP by Customer; (b) Customer's or any Authorized End User's use of the Flock IP disrupts or poses a security risk to the Flock IP or any other customer or vendor of Flock; (c) Customer or any Authorized End User is/are using the Flock IP for fraudulent or illegal activities; (d) Customer has violated any term of this provision, including, but not limited to, utilizing Flock Services for anything other than the Permitted Purpose; or (e) any unauthorized access to Flock Services through Customer's account ("***Service Suspension***"). Customer shall not be entitled to any remedy for the Service Suspension period, including any reimbursement, tolling, or credit. If the Service Suspension was not caused by Customer, the Term will be tolled by the duration of the Service Suspension.

2.7 **Hazardous Conditions.** Flock Services do not contemplate hazardous materials, or other hazardous conditions, including, without limit, asbestos, lead, toxic or flammable substances. In the event any such hazardous materials are discovered in the designated locations in which Flock

is to perform services under this Agreement, Flock shall have the right to cease work immediately.

3. CUSTOMER OBLIGATIONS

3.1 **Customer Obligations.** Flock will assist Customer Authorized End Users in the creation of a User ID. Authorized End Users agree to provide Flock with accurate, complete, and updated registration information. Authorized End Users may not select as their User ID, a name that they do not have the right to use, or any other name with the intent of impersonation. Customer and Authorized End Users may not transfer their account to anyone else without prior written permission of Flock. Authorized End Users shall not share their account username or password information and must protect the security of the username and password. Unless otherwise stated and defined in this Agreement, Customer shall not designate Authorized End Users for persons who are not officers, employees, or agents of Customer. Authorized End Users shall only use Customer-issued email addresses for the creation of their User ID. Customer is responsible for any Authorized End User activity associated with its account. Customer shall ensure that Customer provides Flock with up to date contact information at all times during the Term of this agreement. Customer shall be responsible for obtaining and maintaining any equipment and ancillary services needed to connect to, access or otherwise use the Flock Services. Customer shall (at its own expense) provide Flock with reasonable access and use of Customer facilities and Customer personnel in order to enable Flock to perform Services (such obligations of Customer are collectively defined as ***"Customer Obligations"***).

3.2 **Customer Representations and Warranties.** Customer represents, covenants, and warrants that Customer shall use Flock Services only in compliance with this Agreement and all applicable laws and regulations, including but not limited to any laws relating to the recording or sharing of data, video, photo, or audio content.

4. DATA USE AND LICENSING

4.1 **Customer Data.** As between Flock and Customer, all right, title and interest in the Customer Data, belong to and are retained solely by Customer. Customer hereby grants to Flock a limited, non-exclusive, royalty-free, irrevocable, worldwide license to use the Customer Data and perform all acts as may be necessary for Flock to provide the Flock Services to Customer. Flock does not

own Customer Data and shall not use, sell, or share Customer Data except as provided herein or as authorized in writing by Customer.

4.2 **Customer Generated Data.** Flock may provide Customer with the opportunity to post, upload, display, publish, distribute, transmit, broadcast, or otherwise make available, messages, text, illustrations, files, images, graphics, photos, comments, sounds, music, videos, information, content, ratings, reviews, data, questions, suggestions, or other information or materials produced by Customer (**"*Customer Generated Data"***). Customer shall retain whatever legally cognizable right, title, and interest in Customer Generated Data. Customer understands and acknowledges that Flock has no obligation to monitor or enforce Customer's intellectual property rights of Customer Generated Data. Customer grants Flock a limited, non-exclusive, irrevocable, worldwide, royalty-free, license to use the Customer Generated Data for the purpose of providing Flock Services. Flock does not own and shall not use, sell, or share Customer Generated Data except as provided herein or as authorized in writing by Customer.

4.3 **Anonymized Data.** Flock shall have the right to collect, analyze, and anonymize Customer Data and Customer Generated Data in order to create Anonymized Data. Customer hereby grants Flock a limited, non-exclusive, worldwide, perpetual, royalty-free right to use Anonymized Data to improve and enhance the Flock Services and for other development, diagnostic or corrective purposes for other Flock offerings. Parties understand that the aforementioned license is required for continuity of Services. Flock does not own and shall not use, sell, or share Anonymized Data except as provided herein or as authorized in writing by Customer.

4.4 **Security Incidents.** Flock shall promptly notify Customer of any actual or suspected unauthorized access to, disclosure of, or breach of the security of Customer Data ("***Security Incident***"). Such notice shall include a description of the nature and scope of the Security Incident, the date of the Security Incident, the individual(s) who are suspected of having obtained unauthorized access, the types of data affected, and the corrective actions taken or planned.

5. CONFIDENTIALITY; DISCLOSURES

5.1 **Confidentiality.** To the extent required by the California Public Records Act or any other applicable public records law, each Party that receives a public records request (the "***Receiving Party***") understands that the other Party (the "***Disclosing Party***") has disclosed or may disclose business, technical or financial information relating to the Disclosing Party's business (hereinafter referred to as "***Proprietary Information***" of the Disclosing Party). Proprietary Information of Flock includes non-public information regarding features, functionality and performance of the Services. Proprietary Information of Customer includes non-public data provided by Customer to Flock or collected by Flock via Flock Services, which includes but is not limited to geolocation information and environmental data collected by sensors. The Receiving Party agrees: (i) to take the same security precautions to protect against disclosure or unauthorized use of such Proprietary Information that the Party takes with its own Proprietary Information, but in no event less than commercially reasonable precautions, and (ii) not to use (except in performance of the Services or as otherwise permitted herein) or divulge to any third person any such Proprietary Information. The Disclosing Party agrees that the foregoing shall not apply with respect to any information that the Receiving Party can document that (a) is or becomes generally available to the public; or (b) was in its possession or known by it prior to receipt from the Disclosing Party; or (c) was rightfully disclosed to it without restriction by a third party; or (d) was independently developed without use of any Proprietary Information of the Disclosing Party. Nothing in this Agreement will prevent the Receiving Party from disclosing the Proprietary Information pursuant to any judicial order, provided that the Receiving Party gives the Disclosing Party reasonable prior notice of such disclosure to contest such order. At the termination of this Agreement, all Proprietary Information will be returned to the Disclosing Party, destroyed or erased (if recorded on an erasable storage medium), together with any copies thereof, when no longer needed for the purposes above, or upon request from the Disclosing Party, and in any case upon termination of the Agreement. Notwithstanding any termination, all confidentiality obligations for Proprietary Information that is trade secret shall continue in perpetuity or until such information is no longer trade secret.

5.2 **Usage Restrictions on Flock IP.** Flock and its licensors retain all right, title and interest in and to the Flock IP and its components, and Customer acknowledges that it neither owns nor acquires any additional rights in and to the foregoing not expressly granted by this Agreement. Customer further acknowledges that Flock retains the right to use the foregoing for any purpose in

Flock's sole discretion. Customer and Authorized End Users shall not: (i) copy or duplicate any of the Flock IP; (ii) decompile, disassemble, reverse engineer, or otherwise attempt to obtain or perceive the source code from which any software component of any of the Flock IP is compiled or interpreted, or apply any other process or procedure to derive the source code of any software included in the Flock IP; (iii) attempt to modify, alter, tamper with or repair any of the Flock IP, or attempt to create any derivative product from any of the foregoing; (iv) interfere or attempt to interfere in any manner with the functionality or proper working of any of the Flock IP; (v) remove, obscure, or alter any notice of any intellectual property or proprietary right appearing on or contained within the Flock Services or Flock IP; (vi) use the Flock Services for anything other than the Permitted Purpose; or (vii) assign, sublicense, sell, resell, lease, rent, or otherwise transfer, convey, pledge as security, or otherwise encumber, Customer's rights. There are no implied rights.

5.3 **Disclosure of Footage.** Subject to and during the Retention Period, Flock may access, use, preserve and/or disclose the Footage to law enforcement authorities, government officials, and/or third parties, if legally required to do so (e.g., by court order). Flock shall not otherwise share or disclose any Footage to any third party without the written consent of Customer. If Flock receives a legal request or demand (including subpoenas, court orders, or other legal process) seeking access to Footage or other Customer Data, Flock shall, to the extent legally permitted, promptly notify Customer of such request and obtain the written consent of Customer prior to disclosing any such Footage or Customer Data.

6. PAYMENT OF FEES

6.1 **Billing and Payment of Fees**. Customer shall pay the fees set forth in the applicable Order Form based on the billing structure and payment terms as indicated in the Order Form. If Customer believes that Flock has billed Customer incorrectly, Customer must contact Flock no later than thirty (30) days after the closing date on the first invoice in which the error or problem appeared to receive an adjustment or credit. Customer acknowledges and agrees that a failure to contact Flock within this period will serve as a waiver of any claim. If any undisputed fee is more than thirty (30) days overdue, Flock may, without limiting its other rights and remedies, suspend delivery of its service until such undisputed invoice is paid in full. Flock shall provide at least

thirty (30) days' prior written notice to Customer of the payment delinquency before exercising any suspension right.

6.2 **Notice of Changes to Fees.** Flock reserves the right to change the fees for subsequent Renewal Terms by providing sixty (60) days' notice (which may be sent by email) prior to the end of the Initial Term or Renewal Term (as applicable).

6.3 **Late Fees.** If payment is not issued to Flock by the due date of the invoice, an interest penalty of 1.0% of any unpaid amount may be added for each month or fraction thereafter, until final payment is made.

6.4 **Taxes.** Customer is responsible for all taxes, levies, or duties, excluding only taxes based on Flock's net income, imposed by taxing authorities associated with the order. If Flock has the legal obligation to pay or collect taxes, including amount subsequently assessed by a taxing authority, for which Customer is responsible, the appropriate amount shall be invoice to and paid by Customer unless Customer provides Flock a legally sufficient tax exemption certificate and Flock shall not charge customer any taxes from which it is exempt. If any deduction or withholding is required by law, Customer shall notify Flock and shall pay Flock any additional amounts necessary to ensure that the net amount that Flock receives, after any deduction and withholding, equals the amount Flock would have received if no deduction or withholding had been required.

7. TERM AND TERMINATION

7.1 **Term.** The initial term of this Agreement shall be for the period of time set forth on the Order Form (the "***Term***"). Following the Term, the City shall have the option to extend the Agreement as indicated on the Order Form. Aside from this option, the Agreement shall not automatically renew, but rather may be renewed only if specifically authorized by the City Council.

7.2 **Termination.** Upon termination or expiration of this Agreement, Flock will remove any applicable Flock Hardware at a commercially reasonable time period. In the event of any material breach of this Agreement, the non-breaching Party may terminate this Agreement prior to the end of the Term by giving thirty (30) days prior written notice to the breaching Party; provided, however, that this Agreement will not terminate if the breaching Party has cured the breach prior to the expiration of such thirty (30) day period ("***Cure Period***"). Either Party may terminate this

Agreement (i) upon the institution by or against the other Party of insolvency, receivership or bankruptcy proceedings, (ii) upon the other Party's making an assignment for the benefit of creditors, or (iii) upon the other Party's dissolution or ceasing to do business. In the event of a material breach by Flock, and Flock is unable to cure within the ***Cure Period***, Flock will refund Customer a pro-rata portion of the pre-paid fees for Services not received due to such termination.
7.3 **Survival**. The following Sections will survive termination: 1, 3, 4, 5, 6, 7, 8.3, 8.4, 9, 10.1, 11.1 and 11.6.

8. REMEDY FOR DEFECT; WARRANTY AND DISCLAIMER

8.1 **Manufacturer Defect.** Upon a malfunction or failure of Flock Hardware or Embedded Software (a **"*Defect*"**), Customer must notify Flock's technical support team. In the event of a Defect, Flock shall make a commercially reasonable attempt to repair or replace the defective Flock Hardware at no additional cost to the Customer. Flock reserves the right, in its sole discretion, to repair or replace such Defect, provided that Flock shall conduct inspection or testing within a commercially reasonable time, but no longer than seven (7) business days after Customer gives notice to Flock.

8.2 **Replacements.** In the event that Flock Hardware is lost, stolen, or damaged, Customer may request a replacement of Flock Hardware at a fee according to the reinstall fee schedule (https://www.flocksafety.com/reinstall-fee-schedule). In the event that Customer chooses not to replace lost, damaged, or stolen Flock Hardware, Customer understands and agrees that (1) Flock Services will be materially affected, and (2) that Flock shall have no liability to Customer regarding such affected Flock Services, nor shall Customer receive a refund for the lost, damaged, or stolen Flock Hardware.

8.3 **Warranty.** Flock shall use reasonable efforts consistent with prevailing industry standards to maintain the Services in a manner which minimizes errors and interruptions in the Services and shall perform the Installation Services in a professional and workmanlike manner. Services may be temporarily unavailable for scheduled maintenance or for unscheduled emergency maintenance, either by Flock or by third-party providers, or because of other causes beyond Flock's reasonable control, but Flock shall use reasonable efforts to provide advance notice in writing or by e-mail of any scheduled service disruption.

8.4 **Disclaimer.** THE REMEDY DESCRIBED IN SECTION 8.1 ABOVE IS CUSTOMER'S SOLE REMEDY, AND FLOCK'S SOLE LIABILITY, WITH RESPECT TO DEFECTS. FLOCK DOES NOT WARRANT THAT THE SERVICES WILL BE UNINTERRUPTED OR ERROR FREE; NOR DOES IT MAKE ANY WARRANTY AS TO THE RESULTS THAT MAY BE OBTAINED FROM USE OF THE SERVICES. EXCEPT AS EXPRESSLY SET FORTH IN THIS SECTION, THE SERVICES ARE PROVIDED "AS IS" AND FLOCK DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A

PARTICULAR PURPOSE AND NON-INFRINGEMENT. THIS DISCLAIMER ONLY APPLIES TO THE EXTENT ALLOWED BY THE GOVERNING LAW OF THE STATE MENTIONED IN SECTION 11.6.

8.5 **Insurance.** Flock will maintain commercial general liability policies as stated in Exhibit B.

8.6 **Force Majeure.** Parties are not responsible or liable for any delays or failures in performance from any cause beyond their control, including, but not limited to acts of God, changes to law or regulations, embargoes, war, terrorist acts, pandemics (including the spread of variants), issues of national security, acts or omissions of third-party technology providers, riots, fires, earthquakes, floods, power blackouts, strikes, supply chain shortages of equipment or supplies, financial institution crisis, weather conditions or acts of hackers, internet service providers or any other third party acts or omissions.

9. LIMITATION OF LIABILITY; INDEMNITY

9.1 **Limitation of Liability.** NOTWITHSTANDING ANYTHING TO THE CONTRARY, FLOCK, ITS OFFICERS, AFFILIATES, REPRESENTATIVES, CONTRACTORS AND EMPLOYEES SHALL NOT BE RESPONSIBLE OR LIABLE WITH RESPECT TO ANY SUBJECT MATTER OF THIS AGREEMENT OR TERMS AND CONDITIONS RELATED THERETO UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY, PRODUCT LIABILITY, OR OTHER THEORY: (A) FOR LOSS OF REVENUE, BUSINESS OR BUSINESS INTERRUPTION; (B) INCOMPLETE, CORRUPT, OR INACCURATE DATA; (C) COST OF PROCUREMENT OF SUBSTITUTE GOODS, SERVICES OR TECHNOLOGY; (D) FOR ANY INDIRECT, EXEMPLARY, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES; (E) FOR ANY MATTER BEYOND FLOCK'S ACTUAL KNOWLEDGE OR REASONABLE CONTROL INCLUDING REPEAT CRIMINAL ACTIVITY OR INABILITY TO CAPTURE FOOTAGE; OR (F) FOR ANY AMOUNTS THAT, TOGETHER WITH AMOUNTS ASSOCIATED WITH ALL OTHER CLAIMS, EXCEED THE FEES PAID AND/OR PAYABLE BY CUSTOMER TO FLOCK FOR THE SERVICES UNDER THIS AGREEMENT IN THE TWELVE (12) MONTHS PRIOR TO THE ACT OR OMISSION THAT GAVE RISE TO THE LIABILITY, IN EACH CASE, WHETHER OR NOT FLOCK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF

LIABILITY OF SECTION ONLY APPLIES TO THE EXTENT ALLOWED BY THE GOVERNING LAW OF THE STATE REFERENCED IN SECTION 10.6. NOTWITHSTANDING ANYTHING TO THE CONTRARY, THE FOREGOING LIMITATIONS OF LIABILITY SHALL NOT APPLY (I) IN THE EVENT OF GROSS NEGLIGENCE OR WILLFUL MISCONDUCT, OR (II) INDEMNIFICATION OBLIGATIONS.

9.2 **Responsibility.** Each Party to this Agreement shall assume the responsibility and liability for the acts and omissions of its own employees, officers, or agents, in connection with the performance of their official duties under this Agreement. Each Party to this Agreement shall be liable for the torts of its own officers, agents, or employees.

9.3 **Flock Indemnity.** Flock shall indemnify and hold harmless Customer, its agents and employees, from liability of any kind, including claims, costs (including defense) and expenses, on account of: (i) any copyrighted material, patented or unpatented invention, articles, device or appliance manufactured or used in the performance of this Agreement; or (ii) any damage or injury to property or person directly caused by Flock's installation of Flock Hardware, except for where such damage or injury was caused solely by the negligence of the Customer or its agents, officers or employees. Flock's performance of this indemnity obligation shall not exceed the fees paid and/or payable for the services rendered under this Agreement in the preceding twelve (12) months.

10. INSTALLATION SERVICES AND OBLIGATIONS

10.1 **Ownership of Hardware**. Flock Hardware is owned and shall remain the exclusive property of Flock. Title to any Flock Hardware shall not pass to Customer upon execution of this Agreement, except as otherwise specifically set forth in this Agreement. Except as otherwise expressly stated in this Agreement, Customer is not permitted to remove, reposition, re-install, tamper with, alter, adjust or otherwise take possession or control of Flock Hardware. Customer agrees and understands that in the event Customer is found to engage in any of the foregoing restricted actions, all warranties herein shall be null and void, and this Agreement shall be subject to immediate termination for material breach by Customer. Customer shall not perform any acts which would interfere with the retention of title of the Flock Hardware by Flock. Should Customer default on any payment of the Flock Services, Flock may remove Flock Hardware at

Flock's discretion provided that Flock give Customer the opportunity to remove any Customer Data and Customer Generated Data that may be stored on the Flock Hardware before it is returned to Flock. Such removal, if made by Flock, shall not be deemed a waiver of Flock's rights to any damages Flock may sustain as a result of Customer's default and Flock shall have the right to enforce any other legal remedy or right.

10.2 **Deployment Plan**. Flock shall advise Customer on the location and positioning of the Flock Hardware for optimal product functionality, as conditions and locations allow. Flock will collaborate with Customer to design the strategic geographic mapping of the location(s) and implementation of Flock Hardware to create a deployment plan ("***Deployment Plan***"). In the event that Flock determines that Flock Hardware will not achieve optimal functionality at a designated location, Flock shall have final discretion to veto a specific location, and will provide alternative options to Customer.

10.3 **Changes to Deployment Plan.** After installation of Flock Hardware, any subsequent requested changes to the Deployment Plan, including, but not limited to, relocating, re-positioning, adjusting of the mounting, removing foliage, replacement, changes to heights of poles will incur a fee according to the reinstall fee schedule located at (https://www.flocksafety.com/reinstall-fee-schedule). Customer will receive prior notice and confirm approval of any such fees.

10.4 **Customer Installation Obligations**. Customer is responsible for any applicable supplementary cost as described in the Customer Implementation Guide, attached hereto as Exhibit C ("***Customer Obligations***"). Customer represents and warrants that it has, or shall lawfully obtain, all necessary right title and authority and hereby authorizes Flock to install the Flock Hardware at the designated locations and to make any necessary inspections or maintenance in connection with such installation.

10.5 **Flock's Obligations**. Installation of any Flock Hardware shall be installed in a professional manner within a commercially reasonable time from the Effective Date of this Agreement. Upon removal of Flock Hardware, Flock shall restore the location to its original condition, ordinary wear and tear excepted. Flock will continue to monitor the performance of Flock Hardware for the length of the Term. Flock may use a subcontractor or third party to perform certain obligations

under this agreement, provided that Flock's use of such subcontractor or third party shall not release Flock from any duty or liability to fulfill Flock's obligations under this Agreement.

11. MISCELLANEOUS

11.1 **Compliance With Laws.** Parties shall comply with all applicable local, state and federal laws, regulations, policies and ordinances and their associated record retention schedules, including responding to any subpoena request(s) in the manner provided in Section 5.3 of this Agreement.

11.2 **Severability.** If any provision of this Agreement is found to be unenforceable or invalid, that provision will be limited or eliminated to the minimum extent necessary so that this Agreement will otherwise remain in full force and effect.

11.3 **Assignment.** This Agreement is not assignable, transferable or sublicensable by either Party, without prior consent. Notwithstanding the foregoing, either Party may assign this Agreement, without the other Party's consent, (i) to any parent, subsidiary, or affiliate entity, or (ii) to any purchaser of all or substantially all of such Party's assets or to any successor by way of merger, consolidation or similar transaction.

11.4 **Entire Agreement.** This Agreement, together with the Order Form(s), the reinstall fee schedule (https://www.flocksafety.com/reinstall-fee-schedule), and any attached exhibits are the complete and exclusive statement of the mutual understanding of the Parties and supersedes and cancels all previous or contemporaneous negotiations, discussions or agreements, whether written and oral , communications and other understandings relating to the subject matter of this Agreement, and that all waivers and modifications must be in a writing signed by both Parties, except as otherwise provided herein. None of Customer's purchase orders, authorizations or similar documents will alter the terms of this Agreement, and any such conflicting terms are expressly rejected. Any mutually agreed upon future purchase order is subject to these legal terms and does not alter the rights and obligations under this Agreement, except that future purchase orders may outline additional products, services, quantities and billing terms to be mutually accepted by Parties. In the event of any conflict of terms found in this Agreement or any other terms and conditions, the terms of this Agreement shall prevail. Customer agrees that Customer's purchase is neither contingent upon the delivery of any future functionality or features nor

dependent upon any oral or written comments made by Flock with respect to future functionality or feature.

11.5 **Relationship.** No agency, partnership, joint venture, or employment is created as a result of this Agreement and Parties do not have any authority of any kind to bind each other in any respect whatsoever. Flock shall at all times be and act as an independent contractor to Customer.

11.6 **Governing Law; Venue.** This Agreement shall be governed by the laws of the state in which the Customer is located. The Parties hereto agree that venue would be proper in the chosen courts of the State of which the Customer is located. The Parties agree that the United Nations Convention for the International Sale of Goods is excluded in its entirety from this Agreement.

11.7 **Special Terms.** Flock may offer certain special terms which are indicated in the proposal and will become part of this Agreement, upon Customer's prior written consent and the mutual execution by authorized representatives ("***Special Terms***"). To the extent that any terms of this Agreement are inconsistent or conflict with the Special Terms, the Special Terms shall control.

11.8 **Publicity.** Flock has the right to reference and use Customer's name and trademarks and disclose the nature of the Services in business and development and marketing efforts.

11.9 **Feedback.** If Customer or Authorized End User provides any suggestions, ideas, enhancement requests, feedback, recommendations or other information relating to the subject matter hereunder, Agency or Authorized End User hereby assigns to Flock all right, title and interest (including intellectual property rights) with respect to or resulting from any of the foregoing.

11.10 **Export.** Customer may not remove or export from the United States or allow the export or re-export of the Flock IP or anything related thereto, or any direct product thereof in violation of any restrictions, laws or regulations of the United States Department of Commerce, the United States Department of Treasury Office of Foreign Assets Control, or any other United States or foreign Customer or authority. As defined in Federal Acquisition Regulation ("FAR"), section 2.101, the Services, the Flock Hardware and Documentation are "commercial items" and according to the Department of Defense Federal Acquisition Regulation ("DFAR") section 252.2277014(a)(1) and are deemed to be "commercial computer software" and "commercial computer software documentation." Flock is compliant with FAR Section 889 and does not contract or do business with, use any equipment, system, or service that uses the enumerated banned Chinese telecommunication companies, equipment or services as a substantial or essential

component of any system, or as critical technology as part of any Flock system. Consistent with DFAR section 227.7202 and FAR section 12.212, any use, modification, reproduction, release, performance, display, or disclosure of such commercial software or commercial software documentation by the U.S. Government will be governed solely by the terms of this Agreement and will be prohibited except to the extent expressly permitted by the terms of this Agreement.

11.11 **Headings.** The headings are merely for organization and should not be construed as adding meaning to the Agreement or interpreting the associated sections.

11.12 **Authority.** Each of the below signers of this Agreement represent that they understand this Agreement and have the authority to sign on behalf of and bind the Parties they are representing.

11.13 **Conflict.** In the event there is a conflict between this Agreement and any applicable statement of work, or Customer purchase order, this Agreement controls unless explicitly stated otherwise.

11.14 **Superseding of Prior Agreements.** In the event there is a conflict between Section 4.1 through 4.4, Section 5.1 through 5.3, Section 7.3, Section 10.1, or Section 11.1 of this Agreement and corresponding sections of a prior agreement between Flock and Customer, including a prior agreement relating to automated license plate reader ("ALPR") cameras, the terms and conditions of this Agreement shall control.

11.15 **Morality.** In the event Customer or its agents become the subject of an indictment, contempt, scandal, crime of moral turpitude or similar event that would negatively impact or tarnish Flock's reputation, Flock shall have the option to terminate this Agreement upon prior written notice to Customer.

11.16 **Notices.** All notices under this Agreement will be in writing and will be deemed to have been duly given when received, if personally delivered; when receipt is electronically confirmed, if transmitted by email; the day after it is sent, if sent for next day delivery by recognized overnight delivery service; and upon receipt to the address listed on the Order Form (or, if different, below), if sent by certified or registered mail, return receipt requested.

11.17 **Non-Appropriation.** Notwithstanding any other provision of this Agreement, all obligations of the Customer under this Agreement which require the expenditure of funds are conditioned on the availability of funds appropriated for that purpose. Customer shall have the right to terminate this Agreement for non-appropriation with thirty (30) days written notice without penalty or other cost.

FLOCK NOTICES ADDRESS:

1170 HOWELL MILL ROAD, NW SUITE 210

ATLANTA, GA 30318

ATTN: LEGAL DEPARTMENT

EMAIL: legal@flocksafety.com

Customer NOTICES ADDRESS:

ADDRESS: _____

ATTN: _____

EMAIL: _____

EXHIBIT B

INSURANCE

Required Coverage. Flock shall procure and maintain for the duration of this Agreement insurance against claims for injuries to persons or damages to property that may arise from or in connection with the performance of the services under this Agreement and the results of that work by Flock or its agents, representatives, employees or subcontractors. Insurance shall be placed with insurers with a current A. M. Best rating of no less than "A" and "VII". Flock shall obtain and, during the term of this Agreement, shall maintain policies of professional liability (errors and omissions), automobile liability, and general liability insurance for insurable amounts of not less than the limits listed herein. The insurance policies shall provide that the policies shall remain in full force during the life of the Agreement. Flock shall procure and shall maintain during the life of this Agreement Worker's Compensation insurance as required by applicable State law for all Flock employees.

Types and Amounts Required. Flock shall maintain, at minimum, the following insurance coverage for the duration of this Agreement:

(i) **Commercial General Liability** insurance written on an occurrence basis with minimum limits of One Million Dollars ($1,000,000) per occurrence and Two Million Dollars ($2,000,000) in the aggregate for bodily injury, death, and property damage, including personal injury, contractual liability, independent contractors, broad-form property damage, and product and completed operations coverage;

(ii) **Umbrella or Excess Liability** insurance written on an occurrence basis with minimum limits of Ten Million Dollars ($10,000,000) per occurrence and Ten Million Dollars ($10,000,000) in the aggregate;

(iii) **Professional Liability/Errors and Omissions** insurance with minimum limits of Five Million Dollars ($5,000,000) per occurrence and Five Million Dollars ($5,000,000) in the aggregate;

(iv) **Commercial Automobile Liability** insurance with a minimum combined single limit of One Million Dollars ($1,000,000) per occurrence for bodily injury, death, and property coverage, including owned and non-owned and hired automobile coverage; and

(v) **Cyber Liability** insurance written on an occurrence basis with minimum limits of Five Million Dollars ($5,000,000).

flock safety

FLOCK GROUP INC.
AMENDMENT

This amendment (the "**Amendment**") is made between Flock Group Inc. ("**Flock**") and CA - Berkeley PD **("Customer")**, collectively referred to as (the "**Parties**").

1. Scope. This Amendment amends the previously executed agreement between the Parties, dated 12/07/2023, relating to the provision of services by Flock to Customer and any schedules attached thereto or incorporated therein by reference (the "**Agreement**"). This Amendment further amends the agreement between the Parties, dated March __ 2026, relating to the provision of services by Flock to Customer and any schedules attached thereto or incorporated therein by reference (the "**Master Services Agreement**"). The remainder of the Agreement and the Master Services Agreement shall remain in full force and effect.

2. Conflict. In the event of a conflict between this Amendment and the Agreement or any previous amendment, the terms of this Amendment will prevail. However, in the event of a conflict between this Amendment and the Master Services Agreement, the terms of the Master Services Agreement will prevail.

3. Capitalization. Any capitalized terms used in this Amendment will have the same meaning as in the Agreement, unless expressly defined otherwise.

4. Effective Date. This Amendment will become effective when executed by both Parties (the "**Effective Date**").

The Agreement and Master Services Agreement are amended as follows: Unauthorized Sharing. Flock acknowledges the importance of protecting the integrity and security of Customer Data and maintains appropriate technical and organizational safeguards designed to prevent unauthorized disclosure, access, or use of Customer Data ("Unauthorized Sharing"). Flock shall comply with its Policy for Responding to Legal Demands for Customer Data (the "Customer Data Policy"), attached hereto as Attachment "A." Flock shall not disclose, enable access to, or otherwise make available any Customer Data to any unauthorized person or entity, except: (a) where required by applicable law, regulation, subpoena, warrant, or court order, and only in accordance with the Customer Data Policy; (b) in response to an exigent or emergency request consistent with Flock's Evidence Policy and applicable law; or (c) with Customer's prior written consent. Access to Customer Data by individuals deputized or seconded to a federal task force, or by federal personnel embedded within a state or local agency, shall not constitute an Unauthorized Sharing under this Section where (i) such individuals are acting under the control, supervision, or credentials of the Customer or another state or local agency with authorized access approved by Customer; and (ii) access to Customer Data that is initiated, authorized, or facilitated by Customer, including Customer's acceptance of a sharing request or participation in a Lookup tool via the user interface, shall likewise not constitute an Unauthorized Sharing. In the event Flock causes an Unauthorized Sharing, Flock shall pay to Customer, as a penalty, the sum of Seventy Five Thousand Dollars ($75,000) per Violation. For purposes of this Section, a "Violation" means a single, discrete act or incident of unauthorized disclosure or access resulting from Flock's conduct, irrespective of the volume or number of records, cameras, or data elements involved in that same act or incident. The Parties acknowledge and agree that (i) this penalty is intended to serve as a deterrent to unauthorized sharing of Customer Data, by Flock; (ii) this Section does not apply to any disclosure made pursuant to lawful process, emergency, or regulatory compulsion, or as a result of circumvention of Flock's controls, and (iii) the penalty set forth herein constitutes Customer's sole and exclusive remedy for any such Unauthorized Sharing. For avoidance of doubt, nothing in this paragraph shall be construed to limit or abridge Section 5.3 of the Master Services Agreement, or the City's rights with respect to Customer Data, Customer Generated Data, and Anonymized Data pursuant to Sections 4.1, 4.2 and 4.3 of the Master Services Agreement.

By executing this Amendment, Customer represents and warrants that it has read and agrees to all of the terms contained herein.

FLOCK GROUP INC.		CA - Berkeley PD	
By:	_____	By:	_____
Name:	_____	Name:	_____
Title:	_____	Title:	_____
Date:	_____	Date:	_____