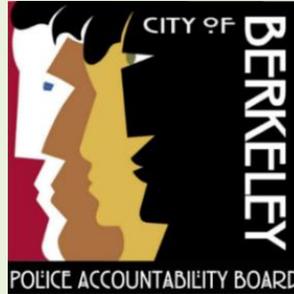Page numbers for this packet are marked in **blue** to distinguish them from the numbering within individual documents.

Board Members

Joshua Cayetano (Chair)	Leah Wilson (Vice-Chair)
Randy Wells	Joshua Buswell-Charkow

Police Accountability Board Recommendations to Council for the March 24, 2026 Regular Meeting—Item 26: Public Safety Technology: Surveillance Technology Ordinance and Police Equipment Ordinance Approvals, Policy Updates, and Contract Authority

Letter 1

Flock Safety — Vendor Concerns, Cumulative Surveillance Architecture,
and Recommendations for Council Action

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

March 18, 2026

VIA ELECTRONIC MAIL [Email]

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

Re: Flock Safety — Vendor Concerns, Cumulative Surveillance Architecture, and Recommendations for Council Action

Dear Honorable Mayor and Councilmembers:

The Police Accountability Board (PAB) submits this letter in connection with three surveillance technology items currently before the city: the proposed Community Video Streams (CVS) program, the updated External Fixed Video Surveillance Camera policy (Policy 351), and the proposed Unmanned Aerial Systems (UAS) program. Each item involves Flock Safety as the sole vendor. Taken together, and in light of the existing contract with Flock for automated license plate reader (ALPR) technology, they would place Berkeley Police Department's (BPD) entire active surveillance infrastructure — license plate readers, fixed cameras, community video feeds, and aerial drones — on a single platform operated by a single company. This letter addresses vendor and contractual concerns that apply across all four use cases, including BPD's existing ALPR program. It also addresses the Flock Safety Master Services Agreement (MSA) governing all BPD programs, submitted to the PAB on the afternoon of March 10, 2026, and reviewed briefly by the PAB in connection with this letter.[1]

I.   **Cumulative Architecture**

The three items now before the city council would add on the same platform on which the ALPR system currently operates: 16 city-owned Condor fixed cameras, voluntary private camera feeds,

---

[1] The PAB's program-specific letters on Community Video Streams, Policy 351, and UAS are submitted separately.

and drones. The combined system would enable a single vendor to identify a vehicle by plate, simultaneously pull fixed and community camera footage of the surrounding area, and dispatch an aerial drone to track that vehicle in real time — all automatically, on one screen, operated by one company. To the PAB's knowledge, no combined assessment of this integrated capability has been conducted.

Figure 1. A Growing Flock Ecosystem
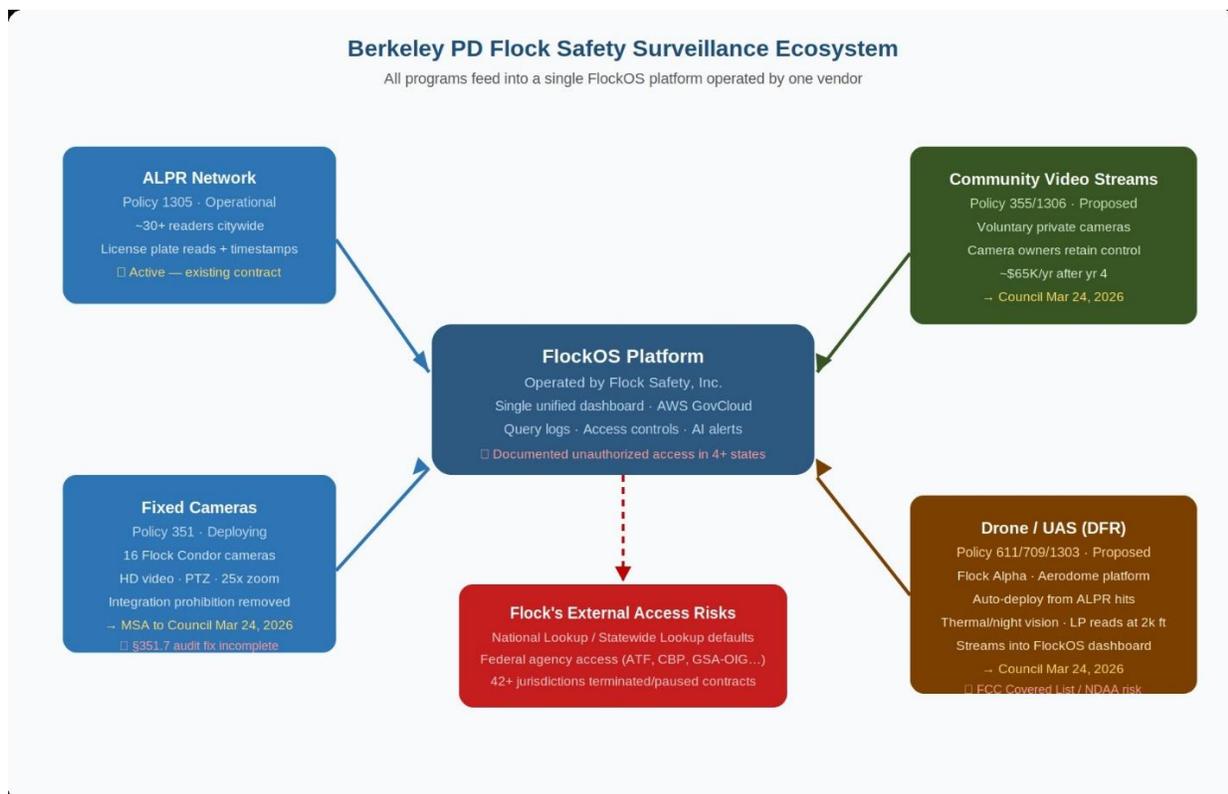
II.   Single-Vendor Concentration Risk

Regardless of the vendor selected, consolidating BPD's entire surveillance infrastructure under a single vendor is likely to deliver operational benefits. The PAB acknowledges these advantages. But the trade-offs deserve equal attention.

Operational dependency. When one vendor controls multiple critical systems — hardware, software, and data storage — any outage, security incident, policy change, or product limitation can impair several core capabilities simultaneously. A problem with Flock's platform is no longer an ALPR problem or a camera problem; it is a total surveillance infrastructure problem.

Weakened governance leverage. Single-vendor consolidation significantly degrades the city's ability to negotiate privacy protections, conduct independent audits, manage data parameters, or enforce limits. Once BPD's operational workflows are built around FlockOS, the practical ability to contest Flock's data practices or demand contractual modifications narrows considerably. The city's leverage is highest before signing — not after.

Cost dependency and lock-in. Flock's bundled pricing creates initial savings, but once the contract is executed and BPD's operations depend on the platform, pricing power shifts to the vendor. Subscription increases, hardware costs, license fees, and add-on charges become difficult to resist when the cost of switching — retraining, new hardware, policy rewrites, data migration — is operationally prohibitive. The MSA's terms on assignment (section 11.3) and data retention after termination (section 4.3) confirm that these risks are real and contractually embedded, not hypothetical.

What happens if Flock fails or is acquired? Flock is a private company that has grown rapidly through venture capital. Section 11.3 of the MSA permits Flock to assign the agreement to any acquirer by merger or asset sale without the city's consent — meaning Berkeley's surveillance data, including years of license plate scans, location history, and video, transfers automatically to any new owner. Section 4.3 of the MSA grants Flock a perpetual license to retain anonymized derivatives of city data even after the contract ends. The city currently has no contractual mechanism to object to either outcome.

III.   Flock Specific Concerns

Community concerns about Flock Safety are grounded in documented incidents:

- **Mountain View (January–February 2026):** Mountain View Police discovered Flock had silently enabled a "nationwide" access setting allowing federal agencies including ATF, the Air Force, and the GSA Inspector General to access local ALPR data in violation of state law and departmental policy. A "statewide lookup" feature had also been silently enabled on 29 of 30 cameras since deployment, allowing approximately 600,000 unauthorized searches by more than 250 California agencies over more than a year. The Police Chief shut down all 30 cameras on February 2, 2026, stating he "personally no longer ha[d] confidence in this particular vendor." The City Council voted unanimously to terminate the contract on February 24, 2026.

- **Berkeley (July 2025):** BPD's own audit identified that external agencies queried Berkeley's Flock ALPR data using the search terms "ICE" and "CBP," enabled by Flock's statewide lookup tool. This was not a hypothetical risk from another jurisdiction — it involved Berkeley's own data.

- **Illinois (August 2025):** The Illinois Secretary of State's audit found Flock violated state law by allowing U.S. Customs and Border Protection to access Illinois license plate data via its National Lookup feature — characterized by one city as "intentional and unauthorized."

- **Oregon:** The city of Eugene discovered Flock reactivated a camera after the department had ordered it shut down. The department learned of the reactivation not from Flock but from a community member.

- **California AG / Oakland / Alameda County:** The California Attorney General sued El Cajon in October 2025 for systematic illegal Flock data sharing with federal agencies. Oakland faced a lawsuit in November 2025 alleging millions of unauthorized external searches of its Flock system, and ultimately approved its Flock contract only after a contested 7–1 vote and significant contractual amendments. Alameda County voted in February 2026 to table a Flock contract extension pending further review.

- **Broader pattern:** At least 42 jurisdictions have terminated or paused Flock contracts. Security researchers found 67 Flock cameras streaming to the open internet without passwords in January 2026. A class action was filed in California on February 26, 2026, alleging Flock violated the California ALPR Privacy Act. The Electronic Frontier Foundation documented agencies logging Flock searches tied to political demonstrations in 2025.

The structural explanation for these incidents is Flock's business model. Flock's value proposition depends on network effects — cross-jurisdictional data sharing and search. The platform's architecture makes broader access easier than the public would expect, and the default settings for features like National Lookup and Statewide Lookup have repeatedly been enabled without notifying client agencies. Flock's own published legal terms permit it to access, use, preserve, or disclose data when it determines this is "reasonably necessary" for legal process, enforcement of agreements, or to address security or technical issues — a self-defined standard that no BPD acquisition report has acknowledged or addressed.

IV. The Flock Master Services Agreement

The proposed MSA governs all BPD Flock programs — including the existing ALPR system, the deployment of fixed cameras (Policy 351), the proposed CVS program, and the proposed UAS program — and was submitted on the afternoon of March 10, 2026, as a supplemental item for the March 11th PAB meeting. The MSA includes meaningful commitments: under sections 4.1 and 4.2, Flock confirms that all right, title, and interest in customer data belongs to the city, and that Flock will not use, sell, or share customer data except as provided in the agreement or authorized in writing by the city. However, the MSA also contains provisions that no BPD acquisition report

disclosed, and that are material to the council's evaluation of both the MSA and the individual programs.

- Section 4.3 of the MSA grants Flock a perpetual, irrevocable, worldwide license to use "Anonymized Data" — defined as data stripped of identifying details under commercially available standards — for its own product development and other Flock offerings. This license survives termination of the agreement. Given that license plate scans combined with location and timestamp data are highly re-identifiable, this is a significant data-use right.

- Section 2.4 grants Flock unilateral authority to make any platform upgrades it deems necessary to maintain competitive strength, without customer consent — the contractual mechanism that enabled silent activation of National Lookup and Statewide Lookup in Mountain View and other jurisdictions.

- Section 9.1 caps Flock's total liability at fees paid in the preceding 12 months (approximately $65,000–$80,000 per program), with no carve-out for negligent misconfigurations that enable unauthorized federal access.

- The MSA gives Berkeley extremely limited grounds to exit the agreement. Under section 7.2, the city may terminate only for Flock's material breach — and only after a 30-day cure period during which Flock may remedy the breach and prevent termination. There is no termination-for-convenience clause: the city cannot simply decide it no longer wishes to use the service and exit. It is locked in for the full contract term unless it can prove a material breach that Flock fails to cure within 30 days. The agreement does not define "material breach," leaving that determination to potential dispute. The city may also terminate if Flock becomes insolvent or ceases to do business (section 7.2), but that is not a meaningful governance tool.

Flock, by contrast, holds termination rights the city does not. Section 11.15 permits Flock to terminate if Berkeley becomes subject to an indictment, scandal, or "crime of moral turpitude" that could tarnish Flock's reputation — a broadly worded, unilateral right with no equivalent running in Berkeley's favor. Berkeley has no reciprocal right to terminate if Flock is indicted, found to have violated state law, or implicated in the kind of unauthorized access incidents documented across dozens of jurisdictions. Flock may also terminate immediately for payment default (section 3). The result is a stark asymmetry: Flock has multiple exit paths; the city has one, and it requires proving a contested legal standard before the right even arises.

The absence of enforceable vendor sanctions compounds the contractual limitations described above. BPD's submitted policies sanction personnel for misuse but establish no legally enforceable

mechanism against Flock for unauthorized access, data sharing violations, or security failures. BMC 2.99.020.4(k) requires legally enforceable sanctions for intentional violations. That requirement is effectively rendered hollow by the MSA's liability cap (section 9.1), which limits Flock's total exposure to approximately one year of fees regardless of the nature or scale of the violation. The council should require both a vendor sanctions provision in the applicable policies and a meaningful liability threshold in the MSA that reflects potential community harm.

V. Recommendations

The PAB respectfully recommends that the city council:

- **Delay the March 24 vote on the Flock MSA to allow meaningful Council deliberation.** The PAB has reviewed the MSA under a very condensed timeframe (having received the MSA less than 27 hours before the March 11 PAB meeting) and identified provisions — including a perpetual anonymized data license (section 4.3), a unilateral platform upgrade authority (section 2.4), an assignment-without-consent clause (section 11.3), a liability cap insufficient to cover the harm of a major unauthorized access incident (section 9.1), and an asymmetric termination clause (section 11.15) — that no BPD acquisition report disclosed. These terms are material to the council's evaluation.

- **Require the following amendments to the MSA as conditions of council approval.** The PAB has identified nine provisions that require amendment before the MSA is approved: (1) narrow the irrevocable license in section 4.1 so that it is expressly limited to service delivery and terminates with the agreement; (2) delete or narrow the perpetual anonymized data license in section 4.3 so that it does not survive contract termination and cannot be used for general product development beyond the city's specific program; (3) amend section 2.4 to require the city's written consent before Flock activates, modifies, or expands platform features affecting data access, sharing, or lookup capabilities; (4) amend section 9.1 to increase or supplement the liability cap for data breach and unauthorized access incidents to reflect the actual potential harm to residents; (5) amend section 11.3 so that Flock's right to assign the agreement to affiliates and acquirers without the city's consent is eliminated or requires prior written consent; (6) add a termination-for-convenience clause giving the city the right to exit the agreement on reasonable notice without having to establish material breach; (7) amend section 11.15 to add a reciprocal termination right for the city if Flock is indicted, found to have violated state or federal law, or is implicated in unauthorized data sharing or platform access violations; (8) add an express obligation for Flock to delete all city-associated data — including anonymized derivatives retained under section 4.3 — upon contract termination, with written certification of deletion; and (9) add a vendor sanctions provision establishing minimum financial penalties for unauthorized data access, unauthorized feature activation, or

data sharing in violation of applicable law, set at a level that exceeds the cost of compliance and is not subject to the general liability cap in section 9.1.

- **Commission a consolidated BMC 2.99 assessment of the full Flock ecosystem.** Each program (ALPR, fixed cameras, CVS, and drones) has been evaluated individually. The combined system — ALPR, fixed cameras, CVS, and drones on a single platform — has not been assessed as a whole. A combined assessment should address Flock's combined data access capabilities, cross-program data rights under the MSA, BPD's needs for dedicated technology staffing to competently support the Flock ecosystem, and adequacy of audit mechanisms to detect platform-wide unauthorized access. BPD should also be directed to supplement the acquisition reports for the UAS and CVS programs to disclose the full terms of the MSA, as required by BMC 2.99.020.3(i).

- **Standardize non-California agency access notification requirement across all Flock programs.** Policy 351 now requires 72-hour notification to the City Manager, City Attorney, and city council when BPD-owned data stored with Flock is given to a federal agency. The community video stream policies require only 10-day notification to an unspecified recipient. Neither standard reflects the full scope of the legal obligation: California SB 34 prohibits sharing of ALPR data with any non-California agency, not only federal agencies. The 72-hour notification standard with named recipients should apply uniformly across all programs on the FlockOS platform and should be triggered by any access by a non-California agency — federal or otherwise.

- **Require proactive access log audits.** The Mountain View breach went undetected for over a year because no one was reviewing Flock's access logs. All BPD Flock policies should require regular proactive audits — at minimum monthly — of platform access logs, with results reported to the PAB.

- **Submit a referral to the City Manager and City Attorney to assess the feasibility, benefits, and risks of amending the Surveillance Technology Ordinance, Berkeley Municipal Code 2.99, to include a private "right to know" and private "right to delete" personal information gathered and stored by Flock Safety and similar vendors.** California SB 362, signed into law in October 2023, strengthened consumer privacy by creating a centralized mechanism ("Delete Request and Opt-Out Platform" or "DROP") that allows end-users to request deletion of all personal information from registered data brokers. Creating a similar system in Berkeley that covers Flock Safety in particular or all data brokers and vendors contracted with Berkeley in general could further strengthen privacy protections for individuals. But applying this concept to surveillance integrated with law enforcement tools would create unique challenges. Because of the potential benefits and challenges, we

recommend that the City Council refer the matter to the City Manager and City Attorney for an operational and legal assessment of the proposal.

Sincerely,

Joshua Cayetano
Joshua Cayetano, Chair
Police Accountability Board

Cc: Paul Buddenhagen, City Manager
       David White, Deputy City Manager
       Jennifer Louis, Chief of Police
       Jen Tate, Deputy Chief of Police
       Jose Murillo, Acting Director of Police Accountability
       Farimah Brown, City Attorney
       Mark Numainville, City Clerk

Letter 2

BPD's Proposed Acquisition and Use of Unmanned Aerial Surveillance Systems (UAS)

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

March 18, 2026

VIA ELECTRONIC MAIL [Email]

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

Re: BPD's Proposed Acquisition and Use of Unmanned Aerial Surveillance Systems (UAS)

Dear Honorable Mayor Ishii and Members of the City Council,

The Police Accountability Board submits the following recommendations regarding the Berkeley Police Department's proposed acquisition and use of unmanned aerial surveillance systems, commonly known as "police drones." This Board does not take the responsibilities before us lightly. We understand that law enforcement in the 21st century requires adopting new tools to effectively address crimes. We also understand that new tools require an appropriate level of accountability. To reach these findings, the PAB was guided by the process and values articulated in the City of Berkeley's Police Equipment Ordinance[1], Surveillance Technology Ordinance[2], and California's Assembly Bill AB 481—all of which emphasize transparency, accountability, and the protection of the community's civil rights and liberties.[3]

Since 1994, the Berkeley Police Department has operated under a Community Involved Policing (CIP) model, an approach premised on partnership with the community and oriented toward addressing underlying conditions that contribute to crime. This approach has led to measurable public-safety outcomes, including reductions in crime and improvements in public trust. The Berkeley Police Department has incorporated this model into its mission, vision, and values, and those commitments are reflected in the recommendations that guide this work.

---

[1] Police Equipment and Community Safety Ordinance: https://berkeley.municipal.codes/BMC/2.100
[2] Acquisition and Use of Surveillance Technology: https://berkeley.municipal.codes/BMC/2.99.010
[3] Assembly Bill 481: https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202120220AB481

While the PAB recognizes the potential benefits of technology in advancing public safety, we are also concerned that the proposals to adopt or enhance a large suite of surveillance technologies can undermine the principles of community policing with an approach that is potentially more invasive and less personal, creating a modern-day panopticon.

We do not believe that the use of technology to support public safety efforts compels this outcome. Our purpose, rather, is to raise concerns to the City Council to proceed carefully and thoughtfully when authorizing relatively new and, in several respects, still statistically unproven applications of emerging technologies, including the use of drones to assist local policing efforts. If such tools are authorized, they should be governed by clear, measurable performance metrics, implemented under transparent and readily understandable policies, constrained with strict budgetary oversight, and subject to meaningful oversight with defined areas of accountability.

We also write to repeat our concern about BPD's proposal to contract all its surveillance needs out to Flock Safety Inc, a company that provides data to federal immigration authorities and has suffered numerous data breaches. Flock's data-sharing practices raise serious concerns for Berkeley, given the City's longstanding commitment to Sanctuary policies. Considering these risks, it is particularly troubling that at least forty-two jurisdictions across the United States have terminated, paused, or declined to enter into contracts with Flock Safety over concerns about unlawful data sharing, privacy violations, and inadequate safeguards against federal access. The PAB does not believe that expanding BPD's reliance on this vendor is consistent with the City's legal obligations, its Sanctuary commitments, and the trust it seeks to maintain with immigrant residents and community members who rely on local government to safeguard their rights and access to services.

Our recommendations are as follows:

1. Increase Compliance with AB 481 Requirements

AB 481 requires a publicly posted Military Equipment Use Policy (Policy 709) and a governing-body finding that the equipment is necessary because no reasonable alternative can achieve the same safety objective for officers and civilians. As drafted, the packet addresses most required categories, but it relies heavily on cross-references and does not build a sufficient evidentiary record to support the statute's requirement that the City Council only approve a proposed use policy if "[t]he military equipment is necessary because there is no reasonable alternative that can achieve the same objective of officer and civilian safety."[4]

Our recommended compliance improvements are:

---

[4] Gov. Code Ch. 12.8 Section 7071(d)(1)(A).

- Strengthen the "necessity/no reasonable alternative" record with City of Berkeley-specific data. The current narrative justification and alternatives discussion are largely qualitative. At minimum, the policy should be supplemented with clear metrics and supporting information addressing:
    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
- Improve compliance with AB-481 complaint-and-concern process requirements.[5] Policy 709 should specify:
    a. A complaint intake channel
    b. Acknowledgement timeline
    c. Substantive response target
    d. Routing (who reviews UAS complaints)
    e. A commitment to include complaint counts and themes in the AB 481 annual report
- Make Policy 709 self-contained with respect to required AB 481-required elements. Even if operational details remain in other policies, Policy 709 should include short summaries of authorized uses, prohibited uses, training prerequisites, audit and compliance structure, and consolidated fiscal disclosure (rather than requiring readers to reconstruct core AB 481 elements from other documents).

2. Identify Performance Metrics Prior to Program Deployment

If Council proceeds with authorization, it should adopt a defined evaluation framework at the outset and incorporate it into AB 481's annual reporting by adding a new subsection to Policy 709 (Performance Reporting) that includes all required metrics. Based on BPD's stated rationale for procuring drones, the metrics should include, at a minimum:

- CFS response time by call type
- Crime clearance rates and outcomes by crime type
- False alarm cancellation rates

---

[5] Gov. Code Ch. 12.8 Section 7070(d)("'Military equipment use policy' means a publicly released, written document governing the use of military equipment by a law enforcement agency or a state agency that addresses, at a minimum, all of the following….(7) For a law enforcement agency, the procedures by which members of the public may register complaints or concerns or submit questions about the use of each specific type of military equipment, and how the law enforcement agency will ensure that each complaint, concern, or question receives a response in a timely manner.")

- Efficient allocation of police resources
- Reduction of officer injury rates

Specific proposed metrics are set forth in Appendix A.

3. Limit Authorized Uses of Drones

Policies 611 and 1303, BPD's proposed UAS use policies, set out broad categories of acceptable use. The PAB recommends a phased approach that begins with a more narrowly defined allowable-use framework. Adopting this approach would prevent generalized-surveillance risk, educate and promote public trust, and make compliance monitoring more workable. It would also ensure the technology is integrated under defined security and privacy controls at the outset—minimizing the risk of data breaches and other compliance failures.

The PAB recommends:

- Limiting drones-as-first-responder (DFR) to a bounded set of call types for a limited pilot period.
- Specific enumeration of high-risk and critical incident categories:
    a. Violent felonies in progress/recently committed
    b. Armed suspect
    c. Missing/at-risk person
    d. Active fire/disaster hazard
    e. Imminent threat to life, plus a narrowly defined 'exigent threat to life' catchall.
- Clarifying under what 'criminal' circumstances in the 'special events/mass gatherings' context a police drone is permitted and including strict prerequisites: written incident-specific threat assessment, supervisor approval, narrow geographic/time bounds, explicit First Amendment safeguards, and a prohibition on generalized crowd monitoring.
- Adding explicit prohibitions to prevent generalized surveillance and proxy profiling: no area sweeps untethered to a specific incident; no pattern monitoring of neighborhoods; no deployment for minor code/quality-of-life violations; no use to monitor constitutionally protected activity absent a judicial warrant and documented exigency.

4. Strengthen Oversight and Accountability Mechanisms

It is important to strengthen oversight and use policies by establishing clear guardrails around when and how the Berkeley Police Department may deploy drones. While we are not submitting redlined versions of the various policies at this time due to the limited timeframe which the PAB has had to review these proposed policies, the PAB recommends:

- Narrowing officer discretion by limiting drone use to specifically enumerated circumstances.

- Requiring supervisory approval before drone deployment, except in urgent threats to public safety, ensuring that the decision to use this technology is not left to the unilateral judgment of an individual operator.

- Requiring drone operators to list the authorized use, the recording start time, and the recording end time after each use.

- Mandating monthly audits conducted by the Office of Strategic Planning and Accountability

- Detailing real consequences for violations of the use policy, including mandatory retraining, potential revocation of operator authorization after repeated violations, and possible disciplinary action if misconduct is found. Specifically, the PAB recommends that the policies:

  o Require three hours of training if an officer violates the UAS use policy
  o Revoke drone use certification and authorization if an operator violates this policy three times in a five-year period.[6]

By defining permissible uses and requiring supervisory approval, these revisions would create a framework that prioritizes civil liberties while ensuring the technology is used only when it provides clear public safety value. Equally important, the revisions would introduce meaningful accountability and oversight mechanisms that limit the potential for misuse. Together, these measures ensure that drone technology operates within a structured system of oversight that emphasizes transparency, responsibility, and adherence to clearly defined rules.

5. Narrow Data Retention to Safeguard Privacy Interests and Align with Operational Purpose

The PAB requests that the Council significantly narrow the data retention window, unless the video footage has evidentiary value. The primary purposes of the drones, as articulated by BPD—real-time situational awareness, confirming whether a law enforcement response is unnecessary, locating fleeing suspects, tracking vehicles from a safe distance, clearing buildings—only require immediate video confirmation, as opposed to a large storage database. Generally, the PAB endorses tailoring retention policies to the authorized uses of each approved surveillance technology, and shortening the retention window for data captured from drones aligns with this philosophy. The PAB recognizes, however, that at least some of the authorized uses may require a longer data retention timeframe. We note that the data retention period in Policy 1303 excludes

---

[6] We note that this last recommendation may trigger meet-and-confer obligations under the Meyers-Milias-Brown Act.

data of evidentiary value, which addresses BPD's concern that restrictive data retention policies would cause BPD to lose access to potential evidence. That carveout prevents BPD from "rummaging" into stored data in an unparticularized or overbroad manner.[7]

These drones would give the BPD the ability to simultaneously surveil large areas, capturing a host of footage of non-consenting Berkeleyans. The drones provide BPD with access to areas traditionally unavailable to law enforcement and at response times that can only be achieved through technological advancement. Further, as the PAB explained to the Council during the discussion of the Flock surveillance cameras last year, limiting the availability of footage is the only way to ensure that federal immigration authorities cannot access that data, even with a valid judicial warrant. If the data does not exist, the City or Flock cannot be compelled to share it.

6. Increase Fiscal Transparency and Accountability

At present, the fiscal information is dispersed between Policy 709 and the impact report, and certain expenses appear inconsistent. In addition, the materials do not clearly disclose lifecycle costs, including LTE connectivity and related infrastructure, data storage, fleet replacement, and the anticipated costs of transitioning to FCC and NDAA compliance, as discussed further in Section 5.

Fiscal recommendations to strengthen disclosure and support an informed decision include:

- Consolidate and reconcile. Create a single fiscal table within Policy 709 with three columns: One Time, Year 1 and Ongoing Annual, and reconcile the identified DFR and radar inconsistencies. See Appendix B
- Disclose full lifecycle costs. Add lifecycle costs that are presently omitted or unclear, including LTE connectivity and related infrastructure, evidence.com (or comparable) data storage, fleet replacement at years 3-4, and any expected subscription inflation/escalators. See Appendix C.
- Address FCC/NDAA transition risk. If replacement with NDAA-compliant alternatives may be required within the stated lifespan, quantify plausible replacement scenarios and the City's resulting fiscal exposure.
- Uphold BPD's commitment to permanently remove 6 sworn officer positions in order to pay for these proposed contracts. The BPD materials publicly provided for the March 24, 2026, City Council Meeting state 3 positions will be eliminated, but BPD informed the PAB at our February 25, 2026, meeting that 6 positions would be eliminated.[8]

7. Facilitate Ease of Governance and Accountability Through Policy Restructure

---

[7] https://wustllawreview.org/2024/07/01/digital-rummaging/
[8] PAB February 25, 2026 Meeting – 18:36: https://www.youtube.com/watch?v=qY9lqFqNeVE.

The packet consists of three interlocking policies (709, 611, and 1303) and an accompanying impact statement. In its current form, the documents incorporate one another through extensive cross-references, making it difficult to determine which provisions are controlling core requirements such as authorized uses, audits, retention, reporting, and fiscal impacts. The structure, in turn, creates avoidable version-control and accountability risks.

Our suggested recommendations:

- Make Policy 709 self-contained for AB 481 purposes. Include all required elements within Policy 709, without requiring cross-references to other policies.
- Add a one-page governance map and a precedence clause to Policy 709. Specify what:
  a. Policy 709 governs
  b. Policy 611 governs
  c. Policy 1303 governs
  d. Which policy controls conflicts
- Eliminate circularity. Policy 611 should not be necessary to understand Policy 709's AB 481 minimum content; Policy 1303 should serve as the definitive source for retention, access, and audit requirements.
- Or consider consolidation as an alternative. Merge Policies 611 and 1303 into a single "UAS" Operations and Data Governance' policy, with Policy 709 serving as the AB 481 wrapper. This would reduce the framework from three policies to two, making it easier for the public (and auditors) to understand the full rule set.

8. Assess FCC Covered List Implications

UC Berkeley Law's Criminal Law & Justice Center identified supply-chain and lifecycle uncertainty arising from the FCC's December 2025 action. On December 22, 2025, the FCC updated its Covered List to include foreign-produced UAS and UAS critical components, based on a national-security determination. The FCC has also emphasized that this action is forward-looking, affects future FCC equipment authorizations and does not require consumers to stop using if they have already purchased.

BPD's proposed drone fleet relies on foreign-produced UAS platforms. The record should therefore address, expressly and with model-specific clarity: (a) whether each proposed model currently holds the necessary FCC equipment authorizations; (b) whether replacement units, upgrades, or successor models could face authorization constraints going forward; and (c) how that risk bears on the asserted three-year service life and on replacement planning.

9. Reassess Plan to Consolidate Surveillance Technology and Services Under Flock

BPD is proposing to use Flock Safety not only for Drone First Responder (DFR) capability, but also for other procured and deployed technologies, including Automated License Plate Readers (ALPRs) and fixed cameras. This degree of vendor concentration raises several concerns. On the one hand, relying on a single vendor like Flock for multiple public-safety technologies can deliver real operational benefits such as: faster integration and implementation, simpler training and support and a unified platform that helps dispatch and investigators work from a unified system. On the other hand, the trade-off is concentrated risk. The ability to switch to another provider becomes expensive, difficult or operationally disruptive. Any outage, security incident, policy change, pricing shift or product limitation can affect multiple critical functions at once. In short, a single-vendor approach can improve operational efficiency, but it needs stronger contractual exit protections and stronger oversight to manage dependency and data-governance risks.

A. Concentration/single-vendor risk creates efficiencies and raises concerns:

- Operational dependency: When one vendor has absolute control over multiple critical systems (hardware, software, and data storage) it creates a dependency risk where the disruption is not confined to one tool but can impair several core capabilities simultaneously.
- Weakened governance leverage: Single vendor consolidation also raises the potential for the City of Berkeley or BPD to negotiate privacy, conduct an audit, manage data parameters, privacy limits or the cost of terminating the relationship becomes much more difficult.
- Cost dependency: The reliance on vendor to manage multiple functions allows for initial upfront savings in the forms of discounts, bundles and service integration. However, once the initial contract is executed the bargaining power shifts to the vendor in the form of fees, subscription increases, hardware and software costs, license fees, add-on charges that the City will have limited ability to negotiate given the disruption and expense associated with switching providers.

B. Flock-specific concerns:

- Flock Safety's value proposition is its network effects capabilities—cross jurisdiction search and data sharing. Even if BPD has strong controls, the platform architecture can make broader access easier than the public would expect.
- Unauthorized or unintended access, including federal use. There continues to be reporting from local jurisdictions alleging federal agencies accessed ALPR data without the local cities consent. As recently as January-February 2026, Mountain View discovered its Flock Safety ALPR data had been accessed outside the city's approved sharing rules, including access by Federal and state agencies.

- At least 42 jurisdictions, including multiple local jurisdictions, have terminated their contract or refused to contract with Flock Safety following reports showing data access by federal immigration enforcement or other federal entities without clear local approval. Many of these jurisdictions have cited a loss of trust with Flock Safety, given the advertent or inadvertent disclosure of data to federal immigration officials without clear local approval and despite existing restrictions.
- Berkeley has already experienced one such breach of trust in July 2025 when Flock Safety enabled a state-wide look-up tool that caused other agencies to query Berkeley data for "ICE" and "CBP".
- Retention creep and secondary use: Flock states "standard" retention is often 30 days but may vary by customer policy; in practice, retention can expand over time (by policy amendments, exceptions, or investigative holds.)
- Integration magnifies and intensifies privacy impact. When ALPR data and drone operations integrate, the combined capability can significantly increase tracking power.
- Legal process discretion included into the vendor's policy. Flock Safety own published policy indicates it may access/use/preserve/disclose LPR data when it believes it is "reasonably necessary" for legal process, enforcement of agreements, or to address security/technical issues.

The question for the City Council is not limited to whether Berkeley "trusts" Flock Safety. It is whether the City is prepared to approve a contract with a vendor whose platform can enable and facilitate federal immigration enforcement in any space where data sharing is not expressly prohibited. In that respect, the risk is structural, not personal. Flock's business model depends, at least in part, on network effects and cooperation with outside agencies, including federal entities. Where sharing is permitted, that cooperation can include providing access to, or facilitating the use of, data that may be used to identify and locate undocumented individuals.

If Berkeley's policy judgment is that City resources and City-enabled systems should not function as an input to civil immigration enforcement, then the Council must confront whether contracting with a vendor structured around broad, networked access is consistent with that commitment.

Approval, if granted, should be conditioned on (1) share-off-by-default network settings with public reporting on any external access, (2) enforceable contractual limits on vendor access/disclosure and rapid breach notification, (3) strict retention limits and audit-ready logs (4) controls on cross-tool integration that could enable tracking, (5) clear exit rights and data portability to prevent lock-in.

The Police Accountability Board recognizes that certain technological tools may offer operational benefits, improving public safety outcomes, and supporting recruitment and retention within the Berkeley Police Department. But recognition of potential utility does not relieve the City of its

duty to ask the threshold question: what, precisely, is driving BPD's demand for expanded power and access to these tools, and why now?

Berkeley's crime patterns since COVID (2020 onward) declined starting in 2024 toward more typical levels.

Key year-over-year changes BPD highlights:

- Robberies: down 20% from 2024 to 2025 (221 → 177).
- Shootings: down 40% from 2024 to 2025 (25 → 15).
- Commercial burglaries: declined 31% from 2024 to 2025 (396 → 274).
- Vehicle thefts: decreased by approximately 46% from 2024to 2025 (1053 → 567).
- Catalytic converter thefts: decreased from 2024 to 2025 (312 → 248).

This question becomes more urgent when the request extends beyond minor implementation of technology to include loosening longstanding restrictions on the Military Equipment Use Policy or reintroducing historically constrained tools, such as access to and use of helicopters and canine deployment. The public is not demanding these expansions. To the contrary, many residents are concerned and are asking why BPD is seeking so much all at once, particularly when reported crime is declining. The burden rests with BPD to justify not only the asserted benefits, but the necessity, and the safeguards, before the City normalizes the expansion of force and surveillance capabilities that may be difficult to unwind.

Respectfully submitted,

Joshua Cayetano

Joshua Cayetano
Chair, Police Accountability Board

Cc: Paul Buddenhagen, City Manager
        David White, Deputy City Manager
        Jennifer Louis, Chief of Police
        Jen Tate, Deputy Chief of Police
        Jose Murillo, Acting Director of Police Accountability
        Farimah Brown, City Attorney
        Mark Numainville, City Clerk

ATTACHMENTS:

1. Appendix A – Breakdown of CFS and UAS
2. Appendix B – Consolidated Cost Table
3. Appendix C – Lifecycle Provisional Cost Estimate
4. Appendix D – Flock ALPR Terminated Paused Contracts
   - Timeline View

Appendix A

1. **Calls for Service (CFS) Response Time by Call Type**

   - Broken out by drone vs. ground units

2. **Crime Clearance Rates by Crime Type**

3. **False Alarm / Cancellation / Downgrade Rates**

   - Percentage of drone deployments resulting in:
     - Ground response cancellation
     - Response downgrade
     - No enforcement action required
   - Break down by call type

4. **Use of Force Rates in Drone-Assisted Incidents**

Track and report:
   - Use-of-force incidents involving drone-assisted calls
   - Compare to similar incidents without drone deployment
   - Break out by force level (hands-on, intermediate, firearm)

5. **Officer Injury and Safety Indicators**

Track:
   - Officer injuries in drone-assisted incidents
   - Near-miss or tactical withdrawal events
   - High-risk entries avoided due to aerial assessment

6. **Equity and Geographic Distribution (Cross-Cutting Metric)**

Track:
   - Deployment counts by *census* tracts or council districts
   - Overlay with demographic indicators

Appendix B – Consolidated Cost Table

Category	Line item	Amount	Notes/discrepancies to reconcile
One-time	Field-based UAS purchase (Avata 2 + Matrice 4T units)	$44,500	Capital purchase
One-time	Dock installation	$15,000	One-time installation
One-time	Pilot training (4 primary + 8 additional)	$72,000	One-time training cost stated; no documentation of ongoing training costs
Year 1	DFR lease (Year 1)	$100,000	Figure appears in impact materials; may conflict with $125,000 annual figure in Policy 709
Year 1	Radar	Included	Stated as included in Year 1 in impact statement; may conflict with separate $150,000 annual cost in Policy 709
Ongoing annual	DFR lease	$125,000 / year	May conflict with $100,000 Year 1 figure; reconcile
Ongoing annual	Radar	$150,000 / year	May conflict with "included" in Year 1 in impact statement; clarify subscription structure
Ongoing annual	Maintenance (purchased units)	$2,000 / year	Recurring

Appendix C – Lifecycle Provisional Cost Estimate

- One-time subtotal (excluding Year 1 lease): approximately $131,500.
- Estimated Year 1 total (one-time + Year 1 lease + annual maintenance): approximately $233,500.
- Estimated steady-state annual cost (DFR lease + radar + maintenance): approximately $277,000/year.

Appendix D – Flock ALPR Terminated Paused Contracts

Agency Name	Agency Type	State	Action Type	Approx Date	Notes	Source URL
Sedona	City	AZ	Program Shut Down	Sept 2025	Permanent Removal	https://www.redrocknews.com/2025/09/09/sedona-ends-flock-license-plate-cameras
Flagstaff	City	AZ	Contract terminated & Cameras Deactivated	Dec 2025	Council Vote to end Program	https://azdailysun.com/news/local/flagstaff-flock-safety-cameras-ended
South Tucson	City	AZ	Contract terminated	Feb 17, 2026	Council voted to terminate contract	https://www.kgun9.com/news/community-inspired-journalism/south-tucson/south-tucson-ends-flock-camera-contract-city-now-

						searching-for-alternatives
Los Alto Hills	City	CA	Cameras turned off, contract to be terminated	Jan 2026	City contracts with Santa Clara County Sheriff	https://www.losaltosonline.com/news/los-altos-hills-to-remove-alpr-cameras/article_59f90aa8-14c1-4309-9f7f-12d16c649d9e.html
Mountain View	City	CA	Cameras turned off during pause (Council vote to decide)	Feb 2026	Police chief shut down/paused Flock ALPRs after discovering a configuration issue that allowed limited outside-agency searching. Council may vote Feb 24.	https://www.mv-voice.com/public-safety/2026/02/02/mountain-view-police-turn-off-license-plate-cameras-after-data-sharing-breach/

Richmond	City	CA	Program paused/shut down (cameras offline)	Dec 2025	Police chief shut down/paused Flock ALPRs after discovering a configuration issue that allowed limited outside-agency searching; described as a pause pending safeguards.	https://richmondside.org/2025/12/09/richmond-license-plate-reader-data-breach/ https://richmondstandard.com/community/2025/12/09/richmond-police-suspend-system-that-automatically-reads-license-plates/
Santa Clara County (Covers Saratoga, Los Altos Hills (see above), and Cupertino)	County	CA	Sheriff prohibited from using Flock APLR	Feb 24, 2026	The unincorporated areas of Saratoga, Cupertino, and Los Altos Hills have to make their own decision to terminate their respective contracts with	https://abc7news.com/post/santa-clara-county-stop-using-flock-safety-cameras-several-cities-privacy-

					Flock (Los Altos has terminated), but the County's vote effectively ends the use of Flock in these three cities because they do not have their own law enforcement agency.	concerns/1864 6060/
Santa Cruz	City	CA	Contracted Terminated	Jan 13, 2025	Council vote to end program	https://www.s antacruzsentin el.com/2026/0 1/13/santa- cruz-votes-to- terminate-its- contract-with- flock-safety/
Windsor	City	CT	Cameras turned off	Feb 17, 2026	Council directed City Manager to turn off cameras, and explore alternate vendors	https://patch.c om/connecticu t/windsor/win dsor-votes-8- 1-shut-down- flock-license-

					and/or a contract that protects data	plate-reader-cameras
Denver	City/County	CO	Proposed extension rejected	May 2025	Council vote against extending contract with flock.	https://www.denverpost.com/2025/05/05/denver-city-council-flock-vote
Coralville	City	IA	Cameras removed, contract terminated	Feb 25, 2026	Council vote to terminate contract, takedown cameras	https://www.kcrg.com/2026/02/25/coralville-removes-flock-cameras-after-council-votes-end-contract/
Oak Park	Village	IL	Contract terminated	Aug 2025	Immediate shutdown	https://oakpark.com/2025/08/05/oak-park-ends-flock-cameras
Evanston	City	IL	Contracted terminated	Sept 2025	Termination notice issued	https://evanstonroundtable.com/2025/09/26/evanston-

Page **19** of **35**

						ends-flock-alpr
Brookline	Town	MA	Police access paused	October 2025	Private Flock system	https://brookline.news/police-pause-flock-access
Cambridge	City	MA	Contracted terminated	2025	Unauthorized installation issues	https://www.cambridgema.gov/Departmentsoffice/news/2025/flock-contract-terminated
Ferndale	City	MI	Contract ended	Nov 2025	Contract ended after two years, not renewed	https://www.freep.com/story/news/local/michigan/2025/11/13/ferndale-ends-flock-cameras
Hillsborough	Town	NC	Contract terminated	Oct 2025	Cameras removed	https://www.newsobserver.com/news/local/article-

						hillsborough-flock
Ithica	City	NY	Contracted terminated	Mar 4, 2026	Council vote to terminate contract	https://www.wskg.org/regional-news/2026-03-04/ithaca-common-council-votes-to-end-contract-with-flock-safety
Poestenkill	Town	NY	Proposal rejected	2024	Town board vote	https://www.timesunion.com/news/article/poestenkill-rejects-flock-cameras
Village of Saranac Lake	Village	NY	Contract Terminated	Mar 11, 2026	Village officials terminated contract	https://www.adirondackexplorer.org/communities/government/saranac-lake-scraps-plan-for-flock-surveillance-cameras-after-

						public-backlash/
Lucas County	County	OH	Attempted rescission	2024	Legal dispute	https://www.toledoblade.com/local/county/2024/01/18/lucas-county-flock-contract
Washington County	County	OK	Agreement rescinded	2024	County roads only	https://m.bartlesvilleradio.com/pages/news/437382024/washington-comay-rescind-agreement-for-flock-cameras
Woodburn	City	OR	Program suspended/paused	Nov 2025	City suspended use for at least two months after community concerns about potential federal/ICE enforcement use.	https://woodburnindependent.com/2025/11/11/woodburn-suspends-flock-safety-license-plate-cameras-amid-concerns-of-federal-ice-enforcement/

Eugene	City	OR	Contract terminated	Dec 2025	Immediate termination	https://www.eugene-or.gov/m/newsflash/Home/Detail/7288?arc=17091
Springfield	City	OR	Cameras not activated; covered pending removal	Oct – Dec 2025	City stated cameras had not been turned on; planned to cover then remove after ending use.	https://www.klcc.org/breaking/2025-12-05/eugene-and-springfield-both-announce-end-of-flock-camera-usage; https://lookouteugene-springfield.com/story/justice/2025/12/05/eugene-announces-termination-of-flock-contract/
Bend	City	OR	Cameras turned off;	Jan 7, 2026	Constituent concerns, data	https://www.opb.org/article/

			won't renew contract		privacy/data collection practices.	2026/01/08/bend-flock-cameras-ai-license-plate-camera-law-enforcement/
Austin	City	TX	Contract ended	July 2025	Not renewed	https://www.kut.org/austin/2025-07-01/austin-ends-flock-cameras
Hays County	County	TX	Contract terminated	Oct 14, 2025	County Commission voted to end contract.	https://www.kvue.com/article/news/local/hays-county/hays-county-contract-flock-license-plate-reader-cameras/269-f7276915-920a-4216-add1-42fbf17a0056

San Marcos	City	TX	Renewal Rejected	Dec 2025	Council direction	https://www.kvue.com/article/news/local/san-marcos-texas-not-renewing-contract-flock-license-plate-reader-cameras/269-2002ef35-d393-4abc-bb6e-eccc01f875f6
Staunton	City	VA	Contract ended	Dec 2025	ALPRs removed	https://www.whsv.com/2026/01/10/city-stauntons-contract-with-flock-safety-officially-terminated/ https://www.whsv.com/2025/12/22/city-staunton-end-relationship-with-flock-safety-remove-license-plate-readers/

Charlottesville	City	VA	Program paused/ cameras turned off	Dec 16, 2025	City Manager ordered Flock ALPR cameras turned off pending review after concerns about cameras operating during a pause.	https://cvillerightnow.com/news/208802-city-ends-flock-pilot-program-over-federal-data-base-concerns/ https://cvillerightnow.com/news/208802-flock-ceo-includes-charlottesville-staunton-in-email-blaming-activists-for-cities-dropping-the-companys-services/
Gig Harbor	City	WA	Contracted not awarded	Mar 24, 2025	Council declined to award proposed contract for Flock ALPR	https://www.thenewstribune.com/news/local/community/gateway/g-news/article302729359.html
Mountainlake Terrace	City	WA	Contract canceled	2024	Unanimous council vote	https://www.heraldnet.com/news/mountla

						ke-terrace-cancels-flock
Redmon	City	WA	Program suspended	2025	Privacy & records concerns. Cameras turned off after ICE arrests near camera	https://www.seattletimes.com/seattle-news/law-justice/redmond-turns-off-flock-safety-cameras-after-ice-arrests/
Olympia	City	WA	Pilot Suspended	2025	Under review	https://www.theolympian.com/news/local/article313365325.html
Sedro-Wooley	City	WA	Program suspended, pending appeal of WA PRA lawsuit	June 2025	Paused while appeals re WA Supreme Court ruling on public records for Flock data	https://www.goskagit.com/scnews/stanwood-sedro-woolley-appeal-ruling-regarding-flock-camera-data/article_689423af-1bc8-423c-8319-e540457fcca4.html

Skamania County	County	WA	Use delayed/turned off	2025	Public records ruling	https://www.kgw.com/article/news/local/washington/skamania-county-shuts-off-flock-cameras-court-ruling/283-8675caf0-f183-4f1f-b5b7-c932f047d687
Stanwood	City	WA	Program Paused	May 2025	Litigation concerns	https://www.heraldnet.com/news/stanwood-flock-paused
Prosser	City	WA	Cameras turned off (under contract through Nov'26)	Jan 26, 2026	Under contract through Nov '26 - press release silent as to renewal	https://www.chronline.com/stories/controversial-flock-license-plate-readers-shut-off-by-another-eastern-washington-city,395347

| Lynnwood | City | WA | Contract terminated | Feb 2026 | City Council votes to terminate contract | https://www.heraldnet.com/2026/02/23/lynnwood-becomes-one-of-the-1st-in-the-state-to-terminate-flock-contract/ |
| Verona | City | WI | Renewal Declined | Nov 2025 | Contract expired | https://www.wkow.com/news/city-of-verona-votes-to-not-renew-flock-cameras/article_083afa08-5b8a-4955-9876-ad8fd2b9f3aa.html |

Appendix D - Timeline View

Agency Name	Agency Type	State	Action Type	Approx. Date	Notes	Source URL
City of Sedona / Sedona PD	City	AZ	Program shut down	Sept 2025	Permanent removal	https://www.redrocknews.com/2025/09/09/sedona-ends-flock-license-plate-cameras
City of Evanston / Evanston PD	City	IL	Contract terminated	Sept 2025	Termination notice issued	https://evanstonroundtable.com/2025/09/26/evanston-ends-flock-alpr
City of Austin	City	TX	Contract ended	July 2025	Not renewed	https://www.kut.org/austin/2025-07-01/austin-ends-flock-cameras
City of Springfield / Springfield Police Department	City	OR	Cameras not activated; covered pending removal	Oct–Dec 2025	City stated cameras had not been turned on; planned to cover then remove after ending use.	https://www.klcc.org/breaking/2025-12-05/eugene-and-springfield-both-announce-end-of-flock-camera-usage; https:/lookouteugene-springfield.com/story/justice/2025/12/05/eugene-announces-termination-of-flock-contract/

City of Oakland	City	CA	Proposal rejected (committee)	2023	Later approved by council	https://oaklandside.org/2023/06/13/oakland-flock-vote
Town of Brookline	Town	MA	Police access paused	2023	Private Flock system	https://brookline.news/police-pause-flock-access
Town of Hillsborough	Town	NC	Contract terminated	2024	Cameras removed	https://www.newsobserver.com/news/local/article-hillsborough-flock
City of Verona	City	WI	Renewal declined	2024	Contract expired	https://madison.com/news/local/verona-flock-renewal-vote
Town of Poestenkill	Town	NY	Proposal rejected	2024	Town board vote	https://www.timesunion.com/news/article/poestenkill-rejects-flock-cameras
Lucas County	County	OH	Attempted rescission	2024	Legal dispute	https://www.toledoblade.com/local/county/2024/01/18/lucas-county-flock-contract
City of Mountlake Terrace	City	WA	Contract canceled	2024	Unanimous council vote	https://www.heraldnet.com/news/mountlake-terrace-cancels-flock
Washington County	County	OK	Agreement rescinded	2024	County roads only	https://www.examiner-enterprise.com/story/news/2024/02/06/

						washington-county-flock
City of Cambridge	City	MA	Contract terminated	2025	Unauthorized installation issues	https://www.cambridgema.gov/Departments/citymanagersoffice/news/2025/flock-contract-terminated
City of Redmond / Redmond PD	City	WA	Program suspended	2025	Privacy & records concerns	https://www.seattletimes.com/seattle-news/politics/redmond-suspends-flock-cameras
City of Olympia	City	WA	Pilot suspended	2025	Under review	https://www.theolympian.com/news/local/article-olympia-flock
Skamania County	County	WA	Use delayed / turned off	2025	Public records ruling	https://www.columbian.com/news/2025/skamania-county-flock
City of Stanwood	City	WA	Program paused	May 2025	Litigation concerns	https://www.heraldnet.com/news/stanwood-flock-paused
City & County of Denver	City/County	CO	Proposed extension rejected	May 2025	Council vote	https://www.denverpost.com/2025/05/05/denver-city-council-flock-vote
Village of Oak Park / Oak Park PD	Village	IL	Contract terminated	Aug 2025	Immediate shutdown	https://oakpark.com/2025/08/05/oak-park-ends-flock-cameras

City of Lynnwood / Lynnwood PD	City	WA	Program paused	Oct 2025	Cameras turned off	https://www.heraldnet.com/news/lynnwood-pauses-flock-cameras
City of Eugene / Eugene Police Department	City	OR	Cameras turned off during pause (later contract terminated)	Oct 2025	During a mid-October pause, cameras were turned off; contract later terminated in early Dec 2025.	https://www.klcc.org/breaking/2025-12-05/eugene-and-springfield-both-announce-end-of-flock-camera-usage; https://lookouteugene-springfield.com/story/latest-news/2025/12/09/flock-activated-camera-during-pause-chief-says-pushing-city-to-axe-contract/
City of Ferndale	City	MI	Contract ended	Nov 2025	Pilot discontinued	https://www.freep.com/story/news/local/michigan/2025/11/13/ferndale-ends-flock-cameras
City of Woodburn	City	OR	Program suspended / paused	Nov 2025	City suspended use for at least two months after community concerns about potential federal/ICE enforcement use.	https://woodburnindependent.com/2025/11/11/woodburn-suspends-flock-safety-license-plate-cameras-amid-concerns-of-

						federal-ice-enforcement/
City of Flagstaff / Flagstaff PD	City	AZ	Contract terminated & cameras deactivated	Dec 2025	Council vote to end program	https://azdailysun.com/news/local/flagstaff-flock-safety-cameras-ended
City of Eugene	City	OR	Contract terminated	Dec 2025	Immediate termination	https://www.opb.org/article/2025/12/02/eugene-ends-flock-alpr
City of Staunton	City	VA	Contract ended	Dec 2025	ALPRs removed	https://www.whsv.com/2025/12/10/staunton-ends-flock-cameras
City of San Marcos	City	TX	Renewal rejected	Dec 2025	Council direction	https://www.kut.org/texas/2025-12-03/san-marcos-flock-cameras
City of Richmond / Richmond Police Department	City	CA	Program paused / shut down (cameras offline)	Dec 2025	Police chief shut down/paused Flock ALPRs after discovering a configuration issue that allowed limited outside-agency searching; described as a pause pending safeguards.	https://richmondside.org/2025/12/09/richmond-license-plate-reader-data-breach/ https://richmondstandard.com/community/2025/12/09/richmond-police-suspend-system-that-automatically-reads-license-plates/
City of Charlottesville /	City	VA	Program paused / cameras turned off	Dec 16, 2025	City Manager ordered Flock ALPR cameras	https://cvillerightnow.com/news/20880

Charlottesville Police Department					turned off pending review after concerns about cameras operating during a pause.	2-charlottesville-turns-off-flock-license-plate-cameras-after-concerns-raised/

Letter 3

BMC 2.99 Compliance Review: Community Video Streams (Policies 355/1306) and External Fixed Video Surveillance Cameras (Policy 351 Redline)
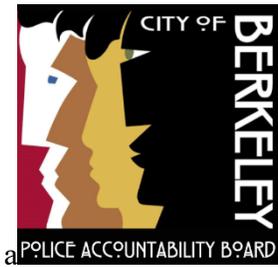
Joshua Cayetano | Chair
Police Accountability Board
JCayetano@berkeleyca.gov

March 18, 2026

VIA ELECTRONIC MAIL [Email]

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

Re: BMC 2.99 Compliance Review: Community Video Streams (Policies 355/1306) and External Fixed Video Surveillance Cameras (Policy 351 Redline)

Dear Mayor and Honorable Councilmembers,

In this letter, the Police Accountability Board (PAB) addresses two surveillance technology items coming before the Berkeley City Council (Council) on March 24, 2026: the proposed Community Video Streams (CVS) program and the redlined Policy 351 governing city-owned fixed cameras. Concerns about Flock Safety as the vendor common to both programs, and about the Flock Safety Master Services Agreement (MSA) submitted to the PAB on March 10, 2026, are addressed in a separate communication to Council (cover letter). This letter focuses on compliance with Berkeley Municipal Code (BMC) Chapter 2.99 requirements specific to the CVS program and Policy 351. The Board also notes that the CVS policies and Surveillance Acquisition Report were provided to the PAB on February 21, 2026, leaving a limited review period before Council consideration, given the scope of the proposed program and its integration with other surveillance technologies on the Flock platform.

In short, pursuant to its authority under BMC 2.99.030(2), the PAB finds that BPD's Surveillance Acquisition Report for Community Video Streams does not meet the requirements under BMC 2.99.020(3) and recommends that BPD resubmit a revised report and recommends approval of BPD's proposed External Fixed Video Surveillance Cameras Use Policy with some modifications.

Recommendations

The PAB recommends that the city council:

- **Community Video Streams — Require the BPD to take additional steps prior to final Council action.** Prior to approving or rejecting the proposal, the PAB recommends that council require the BPD to:
  - (1) add an explicit prohibition on surveillance of First Amendment activity;
  - (2) specify concrete data retention periods with the four elements required by BMC 2.99.020.4(g);
  - (3) conduct a disparate impact analysis addressing whether camera coverage is concentrated in areas with particular demographic characteristics;
  - (4) supplement Section 11 of the Acquisition Report to disclose adverse findings from comparable jurisdictions;
  - (5) update immigration reporting to match the 72-hour standard and named recipients in Policy 351 section 351.6;
  - (6) add rules governing combined cross-platform use of all integrated technologies on the FlockOS platform, including ALPR, fixed cameras, community video streams, and drones;
  - (7) add legally enforceable sanctions for vendor violations; and
  - (8) amend both policies to expressly limit Flock's data use to what is strictly necessary for service delivery, consistent with the MSA amendments recommended in the cover letter.

- **Policy 351 — Approve with modifications.** Council directed a series of modifications to this policy in July 2025. The redline implements most but not all; specifically, section 351.7 must be corrected from "biennial" to "biannual" (twice per year) as Council directed. In addition, the removal of the integration prohibition in section 351.3.3 enables consolidation of all four Flock programs on FlockOS without a fresh BMC 2.99 assessment — the PAB recommends either restoring the prohibition or requiring a new acquisition report addressing the combined-use system before the programs advance to Council (see cover letter); (3) the dual immigration reporting provisions should be reconciled into a single clearly drafted provision; and (4) an explicit First Amendment protection should be added consistent with Policy 428.

- **Both programs — Adopt consistent standards across all Flock policies.** The 72-hour federal access notification with named recipients (City Manager, City Attorney, City Council) in Policy 351 §351.6 should be applied uniformly to Policies 355 and 1306. Audit results for both programs should be reported directly to the PAB. Both programs should

report audits biannual (twice per year) consistent with the Council-directed standard for fixed cameras.

- **Both programs - Establish legally enforceable sanctions against Flock Safety as vendor.** Both the CVS policies and Policy 351 sanction BPD personnel for misuse but establish no enforceable mechanism against Flock for unauthorized access, unauthorized feature activation, or data security violations. BMC 2.99.020.4(k) requires legally enforceable sanctions for intentional violations. This gap should be addressed both through express policy provisions and through the MSA amendments recommended in the cover letter.

- **Both programs - Add explicit First Amendment protection to all applicable policies**. Neither the CVS policies nor the updated Policy 351 contains a prohibition on using the relevant technology to monitor First Amendment assemblies, protests, or political activity. An explicit prohibition consistent with BPD Policy 428 should be added to each policy.

- **Both programs - Require proactive audits of Flock access logs.** The 72-hour federal access notification in section 351.6 is triggered by "discovery" of an incident rather than the incident itself. The Mountain View breach went undetected for over a year because no one was reviewing Flock's access logs. Both programs should require BPD to proactively audit Flock platform access logs on a regular basis so that unauthorized access is detected rather than waited upon. Audit results should be reported directly to the PAB.

PART I: COMMUNITY VIDEO STREAMS — POLICIES 355 AND 1306

I. Background

The Community Video Streams program would allow BPD to access voluntarily registered private cameras through Flock's FlockOS platform via a cloud-based API. Camera owners retain control and can revoke access at any time. The first four years of operating costs are covered under BPD's existing Flock agreement; annual subscription costs are estimated at $65,000 thereafter. BPD submitted Policy 355, Policy 1306, and a Surveillance Acquisition Report to the PAB on February 21, 2026.

The PAB remains concerned about the timing of the submission of proposed policies to the PAB. As the PAB has explained in prior communications, such as its October 28, 2025 correspondence relating to the encryption of police radio channels,[1] the Berkeley Police Department (BPD)

---

[1] October 28, 2025 PAB Letter to Council re: Importance of Proper Vetting for Public Safety Policy Changes – Concerns About Item 18 "Authorization to Encrypt Berkeley Police Department Radio Channels":

continues to provide the PAB with insufficient time to substantively review policies that profoundly impact how policing happens in Berkeley. At the January 27, 2026 City Council meeting, the Council responded to these concerns by increasing the prior review period for policies covered by the Police Equipment Ordinance, BMC 2.100, from 30 to 45 days.[2] The Council also asked Chief Louis to collaborate with the PAB to ensure that it has sufficient time to review policies, given Brown Act agendizing requirements and the cadence of PAB regular meetings.

Chief Louis submitted the CVS policies to the PAB on Saturday, February 21, 2026. Although this was more than 30 days prior to the March 24th Council meeting, the PAB was only able to agendize discussion of this proposal at one PAB meeting due to Brown Act agenda requirements. Had we received this policy only one day earlier, we would have been able to agendize it for the PAB's February 25th meeting, assign a Board member to meet with BPD to discuss, and take additional action. As it were, the PAB considered the policy for the first time as a board at our March 11, 2026 meeting.

The February 21, 2026 submission of the CVS policy did not provide the PAB with sufficient time to research policy issues, discuss potential changes with BPD, hear from outside stakeholders, and reach a final recommendation. Therefore, the PAB only recommends that the Council require BPD to take specific actions that would allow for a fuller analysis but stop short of approving the proposed use and acquisition of the new technology.

II. Procedural Compliance

BPD's submission of Policy 355, Policy 1306, and the Acquisition Report on February 21, 2026, appears procedurally compliant. The three-document package maps to the requirements of BMC 2.99.030.2 and 2.99.030.3, which together require both a Surveillance Use Policy and a Surveillance Acquisition Report to be presented to the PAB before council approval is sought.

III. Acquisition Report — BMC 2.99.020.3

A. Impact Assessment — Section 4 / BMC 2.99.020.3(d)

BMC 2.99.020.3(d) requires an assessment of potential disparate or adverse impacts on communities or groups. The Acquisition Report's Section 4 acknowledges privacy considerations in general terms but does not address whether surveillance activity will be concentrated in areas with particular demographic characteristics. Given that the policy prioritizes integration of cameras in named business improvement districts (Elmwood, Solano, Telegraph, Fourth Street, and Downtown), this omission is a substantive weakness.

---

https://berkeleyca.gov/sites/default/files/documents/2025-10-28%20DPA%20Ltr%20to%20CoB%20Council-%20Radio%20Encryption%20Concerns_Final.pdf

[2] January 27, 2026 Berkeley City Council Regular Meeting Annotated Agenda: https://berkeleyca.gov/sites/default/files/city-council-meetings/2026-01-27%20Annotated%20Agenda%20-%20Council.pdf#Page=11

B. Third Party Dependence — Section 9 / BMC 2.99.020.3(i)

BMC 2.99.020.3(i) requires the Acquisition Report to address whether a third party may have access to data or the right to sell or share it. Section 9 of the Acquisition Report states that evidentiary footage will be stored on Evidence.com and that non-evidentiary data remains with camera owners but does not address what rights Flock holds as the platform operator — a gap that neither the CVS acquisition report nor the fixed camera acquisition report has remedied.

The July 2025 Surveillance Acquisition Report for the Flock Condor fixed cameras addressed the same requirement with identical inadequacy: "The City owns the data. Flock Safety states it will not share or sell customer data." The MSA (section 4.1) does confirm that, as between Flock and the city, all right, title, and interest in customer data belong to and are retained solely by the city — so on that narrow point, the self-attestation is accurate. However, both acquisition reports omitted two critical qualifications. First, the city's ownership coexists with an irrevocable, worldwide license Flock holds to use customer data as necessary to provide its services (section 4.1) — a license the city cannot revoke even if it has concerns about how Flock exercises it. Second, section 4.3 grants Flock the right to anonymize city data and then retain and use those anonymized derivatives under a separate perpetual, royalty-free license for any Flock product development or improvement purpose — a right that survives contract termination. Ownership of the underlying data does not limit what Flock can do with data it has already anonymized. The cover letter details these provisions and recommends specific MSA amendments. Any new consolidated acquisition report for the Flock ecosystem should also address the data shortcomings identified in this section.

C. Experience of Other Entities — Section 11 / BMC 2.99.020.3(k)

BMC 2.99.020.3(k) requires a summary of the experience of comparable entities, "including any unanticipated financial or community costs and benefits." Acquisition Report Section 11 cites Oakland's December 2025 adoption and references Alameda County, Vacaville, Elk Grove, and San Francisco entirely in affirmative terms. No adverse findings are mentioned.

Specifically with respect to community video streams, the public record from the cited jurisdictions tells a different story. Oakland's Privacy Advisory Commission voted 4–2 to recommend that the Council not adopt the policy needed to integrate private cameras into Flock. A lawsuit was filed in Alameda County Superior Court on November 18, 2025 — on the same day the Council's Public Safety Committee first considered the Flock contract, alleging OPD repeatedly violated state law by sharing Flock ALPR data with federal agencies, including the FBI, DEA, and ICE, with audit logs revealing millions of unauthorized external searches. The contract was approved only after a contested 7–1 vote and adoption of significant contractual amendments restricting inter-agency data access. In February 2026, Alameda County voted to table a Flock contract extension pending further review. San Francisco was reported in July 2025 to have shared Oakland's Flock data with federal agencies in apparent violation of SB 34. The California Attorney General sued El Cajon in October 2025 for systematic illegal Flock data sharing with federal agencies. A compliant Section 11 survey would have disclosed this record.

The PAB recommends that the CVS program should not advance to Council until this comparative record is fully and accurately presented, whether in a corrected submission or as part of the consolidated Flock ecosystem acquisition report recommended in the cover letter.

IV. Surveillance Use Policy — BMC 2.99.020.4

A. No First Amendment Prohibition — Section 355.4.2; Section 1306.2 / BMC 2.99.020.4(b)

Neither policy contains an explicit prohibition on using community video streams to monitor First Amendment assemblies, protests, or political activity. BMC 2.99.020.4(b) requires the policy to specify prohibited uses. An explicit prohibition consistent with BPD Policy 428 should be added.

B. Data Retention — Section 1306.7 / BMC 2.99.020.4(g)

BMC 2.99.020.4(g) requires: (1) the time period for which information will be routinely retained; (2) why that period is appropriate; (3) the deletion process; and (4) conditions for extended retention. Section 1306.7 states that evidentiary data is "retained in accordance with state law and existing Departmental evidence retention protocols" and that non-evidentiary data remains with camera owners. It satisfies none of the four requirements. Specific retention language should be added.

C. Third Party Data Sharing — Vendor Rights and Immigration Reporting — Section 355.6; Section 1306.9 / BMC 2.99.020.4(i)

Flock's data rights: The MSA confirms that the city retains ownership of its data, but that ownership coexists with significant Flock license rights — including an irrevocable service license (section 4.1) and a perpetual license to use anonymized derivatives for any Flock product purpose (section 4.3) — that are detailed in the cover letter. Neither Policy 355 nor Policy 1306 acknowledges these terms or establishes any city right to limit or audit how Flock exercises them. This is a gap under BMC 2.99.020.4(i) and 2.99.020.4(d). Both policies should be amended to expressly limit Flock's data use to what is strictly necessary for service delivery.

Immigration reporting: Both policies require the Chief of Police to report any federal immigration enforcement data request within 10 days to an unspecified recipient. Policy 351 — covering the same Flock platform — now requires 72-hour notification to the City Manager, City Attorney, and City Council. There is no basis for the inconsistency. The 72-hour standard with named recipients should be adopted in Policies 355 and 1306.

D. Vendor Sanctions — Section 1306.11 / BMC 2.99.020.4(k)

Section 1306.11 addresses sanctions for BPD personnel violations but does not establish any legally enforceable mechanism against Flock Safety for misuse, unauthorized access, or data security violations. BMC 2.99.020.4(k) requires legally enforceable sanctions for intentional violations. This should be addressed in the policies and in the MSA amendments recommended in the cover letter.

E. Audit Cycle — Section 355.7; Section 1306.11 / BMC 2.99.020.4(k)

Both policies require audits "at least biennial." The Council has already directed a biannual (twice per year) audit standard for the fixed camera program on the same Flock platform. Community video streams should be audited with similar frequency. Both policies should be amended to require biannual audits. Results should be reported directly to the PAB.

F. Cross-Platform Integration — Section 355.3.3

Section 355.3.3 explicitly permits integration of community video streams with ALPR on a shared dashboard, and the redlined Policy 351 removes the prior prohibition on fixed camera integration with ALPR. If the drone program also proceeds, all four programs will be integrated on a single FlockOS platform — a system capable of identifying a vehicle by plate, pulling fixed and community camera footage, and dispatching an aerial drone to track it in real time. Neither the CVS policies nor the acquisition report addresses what rules govern this combined use: permissible query types, logging requirements for cross-technology searches, or safeguards against exceeding individual program authorizations. The cover letter recommends a consolidated BMC 2.99 assessment of the full Flock ecosystem to address these gaps.

PART II: POLICY 351 — EXTERNAL FIXED VIDEO SURVEILLANCE CAMERAS

I. Background and Procedural Context

Policy 351 governs BPD's City-owned fixed external cameras. In March 2025, Council approved 16 new locations and directed a vendor switch from Edgeworth Integration to Flock Safety. On July 22, 2025, the Council adopted Resolution No. 71,903-N.S., accepting the Flock Condor acquisition report and reaffirming the existing 2023 policies, while directing five specific updates. The following issues have been identified upon review of the redlined policy attempting to effectuate the Council's July 2025 action.

II. Key Issues

A. Section 351.3.3 — Integration Prohibition Removed: Critical Policy Reversal

The original Policy 351.3.3 explicitly prohibited integration of the video surveillance system with ALPR, gunshot detection, facial recognition, and other analytical systems. The redline strikes this prohibition entirely and replaces it with permissive language authorizing integration of "technologies not otherwise prohibited," with the explicit example that "integration may occur on a shared access platform where video data and automated license plate reader data are viewable in the same system."

This reversal authorizes the exact integrations the original policy banned, without any fresh BMC 2.99 acquisition report addressing the combined-use capabilities now enabled. The PAB recommends either restoring the prohibition or requiring a new acquisition report for the integrated

system before this policy advances to Council. The cover letter addresses the broader cross-program assessment needed across all four Flock programs.

B. §351.7 — Biannual Audit: Council Directive Not Implemented

Section 351.7 still reads "at least biennial" (every two years) rather than the Council-directed "biannual" (twice per year). This should be corrected. Audit results should also be reported directly to the PAB, not only to the Chief of Police.

C. §351.6 — Immigration Reporting: Improvement, but Inconsistencies Remain

The new 72-hour notification provision — requiring the Police Chief to notify the City Manager, City Attorney, and City Council within 72 hours when BPD-owned data stored with Flock is given to a federal agency — is a meaningful improvement. However, three issues remain:

- The 10-day provision (reporting a federal immigration data request) and the 72-hour provision (reporting actual data transfer) are now both present in Policy 351.6 without reconciliation. The trigger points, recipients, and timelines should be consolidated into a single, clearly drafted provision.
- The 72-hour clock runs from "discovery" of the incident, not from the incident itself. Given that Flock has repeatedly enabled access settings without notifying client agencies, a discovery-triggered clock provides weak protection. BPD should be required to proactively audit Flock access logs on a regular basis to detect unauthorized access before it is "discovered."
- The 72-hour standard in Policy 351 should be applied uniformly to the community video stream policies (355 and 1306), which still require only 10-day notification to an unspecified recipient.

D. Section 351.4.2 — No First Amendment Protection

The prohibited activity section does not include an explicit prohibition on using fixed cameras to monitor First Amendment assemblies or political activity. Several of the newly approved camera locations are in areas with high levels of political demonstrations. An explicit First Amendment protection should be added consistent with Policy 428.

E. Vendor Sanctions — No Enforceable Mechanism Against Flock

Policy 351 establishes sanctions for BPD personnel violations but creates no legally enforceable mechanism against Flock Safety for misuse, unauthorized access, or data security failures. This gap is significant in the context of the fixed camera program: the integration prohibition in section 351.3.3 has been removed, meaning Flock now operates a combined ALPR-video dashboard with broader access to city data than any prior policy authorized. The Eugene, Oregon incident — in which Flock reactivated a camera the department had ordered shut down, and the department learned of it from a community member rather than from Flock — involved fixed cameras specifically. BMC 2.99.020.4(k) requires legally enforceable sanctions for intentional violations.

Page **8** of **11**

That requirement is effectively rendered hollow by the MSA's liability cap (section 9.1), which limits Flock's total exposure to approximately one year of fees regardless of the nature or scale of the violation. This should be addressed in the policies and in the MSA amendments recommended in the cover letter.

III. Compliance Summary Table

Issue	Policy Section	BMC 2.99 Provision	Applies To	Severity
No First Amendment / protest surveillance prohibition	Policy 355 §355.4.2; Policy 1306 §1306.2; Policy 351 §351.4.2	BMC 2.99.020.4(b)	Both programs	Significant
Flock Safety data rights not disclosed — acquisition reports rely on vendor self-attestation only	CVS Acq. Report §9; July 2025 Fixed Camera Acq. Report §9	BMC 2.99.020.3(i); BMC 2.99.020.4(d)	Both programs	Significant
Data retention periods unspecified — defers to 'existing protocols'	Policy 1306 §1306.7	BMC 2.99.020.4(g)	CVS only	Compliance Gap
Immigration reporting: recipient, format, and timeline inadequate; 10-day window inconsistent with 72-hour standard in Policy 351	Policy 355 §355.6; Policy 1306 §1306.9	BMC 2.99.020.4(i)	CVS only	Drafting Deficiency
§351.3.3 integration prohibition struck — enables ALPR-video consolidation on	Policy 351 §351.3.3	BMC 2.99.020.3 / 2.99.030	Fixed cameras only	Critical

Issue	Policy Section	BMC 2.99 Provision	Applies To	Severity
FlockOS without fresh BMC 2.99 assessment				
§351.7 biannual audit fix NOT COMPLETE — still reads 'biennial'; Council-directed fix unimplemented	Policy 351 §351.7	Council directive July 22, 2025	Fixed cameras only	Must Fix
Dual overlapping immigration reporting obligations not reconciled; 72-hour clock runs from 'discovery' not occurrence	Policy 351 §351.6	BMC 2.99.020.4(i)	Fixed cameras only	Drafting Deficiency
Audit results not required to go to PAB; no proactive access log review requirement	Policy 355 §355.7; Policy 1306 §1306.11; Policy 351 §351.7	BMC 2.99.020.4(k)	Both programs	Significant
Experience of other jurisdictions — adverse findings not disclosed	CVS Acq. Report §11	BMC 2.99.020.3(k)	CVS only	Substantive Weakness
No disparate impact analysis for camera concentration in named BIDs	CVS Acq. Report §4	BMC 2.99.020.3(d)	CVS only	Substantive Weakness

IV. Conclusion

For the reasons outlined above, the PAB recommends that the Council does not take final action on the proposed CVS use policies (Policies 355 and 1306) until:

- BPD has satisfied the requirements of BMC 2.99 and submits a revised acquisition report that describes (1) an impact assessment, (2) "the experience of other entities," including "any unanticipated financial or community costs and benefits"; (3) "[a]n 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; (4) an assessment of "third-party dependence and access."

- BPD has integrated the oversight and accountability measures that the Council previously approved into the proposed use policies.

- BPD submits a consolidated acquisition report for the entire Flock ecosystem.

The PAB further recommends that the Council approve the Fixed Surveillance Camera use policy (Policy 351) conditioned on BPD's implementation of the above-recommended changes.

Respectfully submitted,

Joshua Cayetano

Joshua Cayetano
Chair, Police Accountability Board

Cc: Paul Buddenhagen, City Manager
       David White, Deputy City Manager
       Jennifer Louis, Chief of Police
       Jen Tate, Deputy Chief of Police
       Jose Murillo, Acting Director of Police Accountability
       Farimah Brown, City Attorney
       Mark Numainville, City Clerk