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

PUBLIC MEETING MATERIAL

POLICE ACCOUNTABILITY BOARD
REGULAR MEETING AGENDA PACKET
SUPPLEMENTAL NO. 2
MARCH 11, 2026
6:30 PM

Board Members

Joshua Cayetano (Chair)

Leah Wilson (Vice-Chair)

Randy Wells

Joshua Buswell-Charkow

MEETING LOCATION

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

Item 9.b.

Draft PAB Letter to City Council Regarding “Flock Safety: Vendor Concerns, Cumulative Surveillance Architecture, and Recommendations for Council Action,” Proposed by Vice-Chair Wilson.

DRAFT

CITY OF BERKELEY
POLICE ACCOUNTABILITY BOARD

Leah Wilson | Vice Chair
Police Accountability Board
LWilson@berkeleyca.gov

March 11, 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]

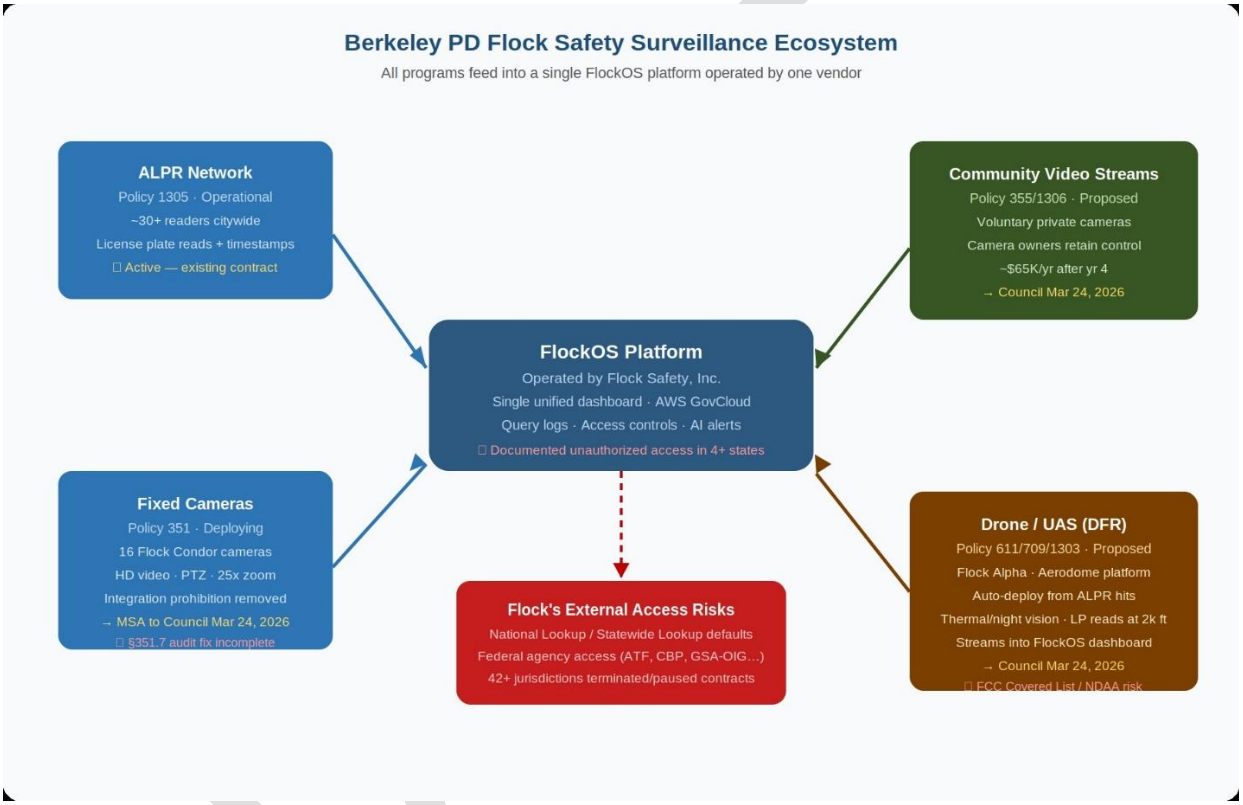
I. The Cumulative Architecture

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



Berkeley PD Flock Safety Surveillance Ecosystem

All programs feed into a single FlockOS platform operated by one vendor

ALPR Network
Policy 1305 · Operational
~30+ readers citywide
License plate reads + timestamps
□ Active — existing contract

Community Video Streams
Policy 355/1306 · Proposed
Voluntary private cameras
Camera owners retain control
~$65K/yr after yr 4
→ Council Mar 24, 2026

FlockOS Platform
Operated by Flock Safety, Inc.
Single unified dashboard · AWS GovCloud
Query logs · Access controls · AI alerts
□ Documented unauthorized access in 4+ states

Fixed Cameras
Policy 351 · Deploying
16 Flock Condor cameras
HD video · PTZ · 25x zoom
Integration prohibition removed
→ MSA to Council Mar 24, 2026
□ §351.7 audit fix incomplete

Flock's External Access Risks
National Lookup / Statewide Lookup defaults
Federal agency access (ATF, CBP, GSA-OIG…)
42+ jurisdictions terminated/paused contracts

Drone / UAS (DFR)
Policy 611/709/1303 · Proposed
Flock Alpha · Aerodome platform
Auto-deploy from ALPR hits
Thermal/night vision · LP reads at 2k ft
Streams into FlockOS dashboard
→ Council Mar 24, 2026
□ FCC Covered List / NDAA risk

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.

II. 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.

III. The Flock Master Services Agreement

The proposed MSA governs all BPD Flock programs — including the existing ALPR system, the deploying 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 11 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.

IV. 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 six 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, 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 the federal 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. There is no principled basis for this inconsistency. The 72-hour standard with named recipients should apply uniformly across all programs on the FlockOS platform.

- **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.

Sincerely,

Leah Wilson, Vice 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

Item 9.c. & 9.d.

Draft PAB Letter to City Council Regarding “BMC 2.99 Compliance Review: Community Video Streams (Policies 355/1306) and External Fixed Video Surveillance Cameras (Policy 351 Redline)”

DRAFT

CITY OF BERKELEY
POLICE ACCOUNTABILITY BOARD

Leah Wilson
Vice Chair, Police Accountability Board
LWilson@berkeleyca.gov

March 11, 2026

VIA ELECTRONIC MAIL [Email]

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

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

Dear Honorable Mayor and Councilmembers:

This letter addresses two surveillance technology items coming before the 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.

Recommendations

The PAB recommends that the city council:

- **Community Video Streams — Approve with modifications.** The PAB recommends approval conditioned on: (1) adding an explicit prohibition on surveillance of First Amendment activity; (2) specifying concrete data retention periods with the four elements required by BMC 2.99.020.4(g); (3) conducting a disparate impact analysis addressing whether camera coverage is concentrated in areas with particular demographic characteristics; (4) supplementing Section 11 of the Acquisition Report to disclose adverse findings from comparable jurisdictions; (5) updating immigration reporting to match the 72-hour standard and named recipients in Policy 351 section 351.6; (6) adding rules governing combined cross-platform use of all integrated technologies on the FlockOS platform, including ALPR, fixed cameras, community video streams, and drones; (7) adding legally enforceable sanctions for vendor violations; and (8) amending 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 adopt biannual (twice per year) audits 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 an 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.

Sincerely,

Leah Wilson, Vice 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:

A. ODPA Memo Titled "Proposed Berkeley Police Department Policies Governing Community Video Streams”