March 11, 2026

To: Berkeley City Council

From: Police Accountability Board

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

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.

DRAFT

- **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.

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.

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.

DRAFT

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.

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 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,

DRAFT

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. Alameda County voted in February 2026 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 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 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."

DRAFT

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 demonstration. 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

DRAFT

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. 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 FlockOS without fresh BMC 2.99 assessment	Policy 351 §351.3.3	BMC 2.99.020.3 / 2.99.030	Fixed cameras only	Critical
§351.7 biannual audit fix NOT COMPLETE — still reads 'biennial'; Council-	Policy 351 §351.7	Council directive July 22, 2025	Fixed cameras only	Must Fix

Issue	Policy Section	BMC 2.99 Provision	Applies To	Severity
directed fix unimplemented				
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