SUPPLEMENTAL

AGENDA MATERIAL

for Supplemental Packet 2

Meeting Date: June 2, 2026

Item Number:

Item Description: Council Directed STO Approvals

Submitted by: City Manager Paul Buddenhagen

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

PURPOSE

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

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

RESPONSES

a. First Amendment Protections

Add an explicit prohibition on surveillance of First Amendment activity, unless there is a clear, articulable, and imminent public safety threat that is actively occurring.

Staff Response:

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

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

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

b. Data Retention Periods

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

Staff Response:

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

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

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

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

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

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

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

<u>c. Disparate Impact Analysis</u>

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

Staff Response:

Staff agrees this is an important transparency and equity measure and commits to conducting a disparate impact analysis as part of the program's implementation framework. Because the CVS program is voluntary and camera locations are determined entirely by private owners who opt in, the Department does not control the geographic distribution of integrated cameras. Nonetheless, the Acquisition Report acknowledges that deployment priorities will focus on major commercial corridors (Elmwood, Solano, Telegraph, Fourth Street, Downtown) and facilities with mass-casualty response needs.

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

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

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

<u>d. Adverse Findings from Comparable Jurisdictions</u>

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

Staff Response:

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

“Community video integration is in active use regionally and nationally; most comparably, the Oakland City Council approved a similar program in December 2025, with comparable tools operating in San Francisco, Alameda County, and other jurisdictions. Criticism of the technology is found with the largest programs: Detroit's Project Green Light and Chicago's Operation Virtual Shield have been faulted for expanding into continuous, citywide monitoring, for pairing camera feeds with facial recognition, and in Chicago's case, for operating with limited regulation or public transparency. These criticisms do not transfer to the program proposed here. The

Department seeks to integrate only voluntarily shared feeds that owners may revoke at any time; live access is limited to active incidents rather than continuous monitoring; facial recognition is prohibited on any stream; and the program operates under the public BMC 2.99 review process, with a published list and map of all integrated cameras, on-site signage, audit logging, express prohibition on use for monitoring first amendment assemblies, and biennial OSPA review. The features that generated controversy elsewhere- always-on monitoring, facial recognition, and the absence of oversight- are excluded here by design."

e. Immigration-Related Search Reporting

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

Staff Response:

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

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

f. Cross-Platform Integrated Technology Use Policy

Consider developing a use policy to address combined cross-platform use of all integrated technologies, regardless of vendor used, including ALPR, fixed cameras, community video streams, and drones.

Staff Response:

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

g. Semiannual Audits

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

Staff Response:

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

h. Data Governance and Security Risk Analysis

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

Staff Response:

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

--

Additional concern: Third Party Access

BMC 2.99.020.3.i requires that an acquisition report have information about whether “use or maintenance of the technology will require data gathered by the technology to be handled or stored by a third-party vendor on an ongoing basis,” and whether a third party may have access to surveillance data or may otherwise sell or share it in any form. BMC 2.99.020.4.i similarly requires a use policy to have information about “if and how a non-City entity can access or use the information, including any required justification or legal standard necessary to do so and any obligations imposed on the recipient of the information.”

Staff Response:

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

“The CVS integration is provided through a third-party platform vendor, but the Department maintains no standing pool of community video stream data with the vendor: non-evidentiary video remains on the camera owner's system, and the Department retains footage only when it is downloaded as evidence, after which it is held in the Department's own digital evidence system and governed by the

Department's evidence-retention and immigration policies. The vendor may access the data only to operate the platform. No non-City entity, including any federal agency, is granted direct access to the camera registry or video feeds; a non-City law enforcement agency may obtain only retained evidentiary footage through standard evidence sharing protocols with pre-authorization from the Investigations Captain, and only for a specific active criminal investigation supported by valid legal process, with any recipient bound by this policy, the Department's Immigration Law Policy, and the bar on using the footage to enforce other states' laws restricting reproductive or gender-affirming care."