

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. 1
September 23, 2026
6:30 PM**

Board Members

Joshua Cayetano (Chair)	Leah Wilson (Vice-Chair)
Joshua Buswell-Charkow	Stephanie Allan
Patrick DeTemple	Jasmina Viteskic
Anay Sharma	Dwayne Phillips (Alternate)

MEETING LOCATION

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

Agenda Item Materials

Item	Description	Page
9.a.	September 18, 2026 Memorandum from Vice-Chair Wilson to the PAB regarding "RFP 26-11794-C, Public Safety Technology – Overview of Solicitation and Summary of the Six Technology Areas it Addresses"	1

Off Agenda Communications

Description	Page
September 21, 2026 PAB Correspondence to the Berkeley City Council Regarding "Surveillance Technology Ordinance Submission for Mutual Aid Air Support"	9

ITEM 9.A.

**SEPTEMBER 18, 2026 MEMORANDUM FROM VICE-CHAIR
WILSON TO THE PAB REGARDING “RFP 26-11794-C, PUBLIC
SAFETY TECHNOLOGY – OVERVIEW OF SOLICITATION AND
SUMMARY OF THE SIX TECHNOLOGY AREAS IT ADDRESSES”**



MEMORANDUM

Date: September 18, 2026
To: Honorable Members of the Police Accountability Board (PAB)
From: Leah Wilson, Vice Chair
Subject: RFP 26-11794-C, Public Safety Technology – Overview of Solicitation and Summary of the Six Technology Areas it Addresses

This memorandum summarizes the six Technology Areas covered by City of Berkeley (City) RFP 26-11794-C.

The Solicitation

The City issued RFP 26-11794-C on July 7, 2026, and proposals were due August 20, 2026. The RFP sought proposals for six separate public safety technologies. This is a modular solicitation: vendors could bid on a single Area, any combination of Areas, or all six. Each Area is scored independently on a 100-point scale; the City may decide not to award in any Area, award by individual Area, by combination, or in whole, and may select more than one vendor.

The base contract term is three years, with extension options exercisable at the City's sole discretion. Where hardware is involved, the City states a preference for an all-inclusive, vendor-managed subscription model. The RFP sets quantities but states no budget, price range, or not-to-exceed amount; cost is worth 10 of the 100 points.

The technologies sought are governed by the City's Surveillance Technology Ordinance (BMC 2.99), the Police Equipment Ordinance (BMC 2.100), the Sanctuary City Contracting Ordinance (BMC 13.105), the Sanctuary City Ordinance (BMC 13.114), and state law including AB 481, SB 34 and SB 54.

Scoring

Each Area is scored out of 100 points on six criteria:

- Data Security, Privacy, and Compliance: 30 points
- Technical Solution and Functional Capabilities: 30 points
- Integration and Interoperability: 10 points
- Implementation, Training, and Support: 10 points

- Company Experience and References: 10 points
- Cost and Price: 10 points

Schedule

Dates are as published and were stated to be subject to change.

- July 7, 2026: RFP issued
- July 20, 2026: Vendor questions due
- July 27, 2026: Addendum A issued with answers to vendor questions
- August 20, 2026: Proposals due
- September 7–25, 2026: Online and in-person vendor demonstrations
- September 30, 2026: Selection process complete
- November 17, 2026: Council approval of contract
- November 18, 2026: Award of contract
- December 1–2, 2026: Contract signed; notice to proceed

The selection committee consists of the Director of the Office of Police Accountability, Board member Pat DeTemple, and me, together with eight sworn and non-sworn Berkeley Police Department personnel. The above-referenced vendor demonstrations concluded the week of September 14, 2026.

The Six Technology Areas

Area 1 – Automated License Plate Readers (ALPR)

What it is. Cameras mounted at fixed locations that photograph every passing vehicle, convert the license plate to text, and record it with a date, time and location. Berkeley currently operates approximately 52 of these. The RFP requires full replacement of that network.

How the technology is used. ALPRs are used in two ways. In real time, each plate read is checked against watch lists – stolen vehicles, felony warrants, missing persons, and plates entered manually by the Department – and an officer receives an alert by app, email or text when a listed plate passes a camera. The officer confirms the plate and the vehicle before acting on the alert; under the RFP an automated alert is an investigative lead that must be independently corroborated, and cannot by itself justify a stop. After the fact, every read is stored in a searchable database, so an investigator who identifies a vehicle through other evidence can run the plate to establish where and when it was seen, or ask which vehicles passed a given location during a given window.

What the RFP requires. Cameras must be deployable where no City electrical power or network infrastructure exists, and vendors must describe how their solution achieves and sustains power and connectivity independent of wired infrastructure, including expected

uptime and maintenance intervals. Each camera must capture at least two lanes of traffic. Search must support full or partial plates with wildcards, date and time ranges, specific cameras, and location with a proximity radius or map-drawn area. Officers must be able to search by vehicle description alone, without a plate. Watch lists must support expiration dates on alerts, with notice before an alert expires, and must flag duplicate entries. Data must purge automatically after 30 days, consistent with the City's ALPR Use Policy. Camera locations must be mapped and publishable on the City website. Vendors must disclose every statewide, national or equivalent lookup network their platform connects to, and confirm participation is opt-in only.

What it does not cover. Faces or people – ALPRs should only read license plates.

Area 2 – Fixed Video Cameras (Pan-Tilt-Zoom)

What it is. A video camera mounted permanently at one location that an operator can pan, tilt and zoom remotely, rather than one that watches a single framed view. The City Council has approved 16 locations for initial deployment under this Area.

How the technology is used. Operators can watch a location live during an incident, moving the camera as they watch. Recorded video can be retrieved after an incident and may be used as evidence in an investigation or prosecution.

What the RFP requires. Pan, tilt and zoom control with configurable fields of view. Live streaming and retrieval of recorded video. Secure access from PC and iOS/Android apps. Remote health monitoring and self-diagnostics so the City knows when a camera is down. A map-based locator of camera positions, publishable on the City website.

What it does not cover. Reading license plates, which is Area 1. Audio recording is prohibited: cameras must either lack audio capability entirely or provide an administrator-controlled setting to disable it permanently off by default.

Area 3 – Drone as First Responder (DFR)

What it is. Drones kept in fixed docking stations. When a call comes in and authorized BPD personnel decide to initiate launch, the DFR is released from its dock, flies to the location in question, and streams video to dispatchers and responding officers. The RFP anticipates two docking stations with associated aircraft and asks for optional pricing for a third.

How the technology is used. A DFR is used to respond to calls for service as authorized by established City policy. Authorized Department personnel initiate the launch; the aircraft then handles takeoff, navigation, return and recharging without a pilot on scene. In some cases the aerial view allows a call to be cleared without officers arriving on scene. The technology can also be deployed in search and rescue and other types of emergency operations.

What the RFP requires. Docking and charging stations supporting launch and return from fixed sites. Detect-and-avoid capability sufficient for safe operation beyond the operator's visual line of sight subject to appropriate authorization. Real-time video and telemetry

streamed to dispatch and field personnel, with integration to computer-aided dispatch where available. Configurable privacy protections during transit to a call — the ability to elevate the camera angle, restrict the field of view, or otherwise limit incidental capture of people and property not associated with the incident. Complete flight logging and an audit trail. Recording, retention and redaction consistent with City policy. NDAA-compliant hardware or a stated migration path and timeline. Identification of all regulatory prerequisites, including FAA Part 107 certification and any waiver required for beyond-line-of-sight or nighttime operation, together with the vendor's role and track record in supporting agencies through FAA approval. Role-based operator controls, pilot training, and maintenance and support for the term. Support for the City's reporting obligations under BMC 2.100 and AB 481.

What it does not cover. Officer-carried drones, which are Area 4. Audio recording is prohibited: the drone must either lack audio capability entirely or provide an administrator-controlled setting to disable it off by default.

Area 4 — Field-Deployed Drones (Unmanned Aerial Systems)

What it is. Portable drones transported in patrol or supervisor vehicles and launched by hand by a trained pilot at an incident scene. The RFP anticipates four outdoor airframes and four indoor airframes designed for GPS-denied interior operations.

How the technology is used. Tactical operations, critical incidents, building searches, crowd and traffic-collision documentation, and natural disaster response, including indoors where GPS is unavailable.

What the RFP requires. Aircraft suitable for rapid field deployment from a vehicle, including transport cases, spare batteries and field-charging equipment. At least one indoor-capable airframe supporting obstacle avoidance and stable flight in confined, GPS-denied spaces. Manual, pilot-operated flight within visual line of sight. Real-time video and telemetry to dispatch and field personnel, with integration to computer-aided dispatch where available. Complete flight logging and an audit trail, with recording, retention and redaction consistent with City policy. NDAA-compliant hardware or a stated migration path. Identification of all regulatory prerequisites, including FAA Part 107 and applicable waivers, and the vendor's role in helping the City obtain them. Role-based operator controls and pilot training. Support for BMC 2.100 and AB 481 reporting. All-inclusive pricing covering airframes, payloads, batteries, transport cases, software, connectivity, maintenance and warranty, priced as two distinct line items with unit pricing for each airframe type.

What it does not cover. Drones launched remotely from a fixed dock, which is Area 3.

Area 5 — Community Video Stream Integration

What it is. Software enabling the Department to view live or recorded video from privately owned cameras whose owners voluntarily register and opt in to share access. The City purchases and installs no cameras under this Area.

How the technology is used. An owner registers a camera on a map and grants permission. When an incident occurs nearby, the Department can see which registered cameras cover the area and, with the owner's permission, view the feed or obtain footage.

What the RFP requires. Camera registration and mapping, with owner opt-in required before any access and the ability for owners to revoke access at any time. Owners retain full ownership of their cameras and footage. A registered feed is routed to the Department only with the owner's explicit permission. Restrictive, privacy-protective settings by default.

What it does not cover. Any City-purchased or City-installed camera. Facial recognition is prohibited. Audio is excluded entirely: the platform may not ingest, transmit or store audio from registered cameras.

Area 6 – Investigative Software

What it is. The platform that the other Areas feed into. It operates in two ways: as a real-time information center – also called a real-time crime center – and as an investigative tool. Berkeley does not operate a real-time information center today; this Area would establish one.

How the technology is used. In real time, the platform brings together license plate reads, fixed-camera video, drone video and community streams alongside computer-aided dispatch data – the live record of calls for service, including location, call type and which units are responding – and records management system data, the Department's system of record for incident and arrest reports, people, vehicles and property, together with other records the platform is able to connect. It presents these on a single dashboard with one sign-on, one set of access logs and one audit trail, so that dispatchers and officers have access to a robust and comprehensive array of information as situations are unfolding or as they respond to calls for service. After the fact, investigators use the platform to search across those same sources and to link related cases. Both functions rest on the same integration; the difference is whether the work is happening during an incident or after it.

What the RFP requires – investigative analytics. Ingestion and integration of structured and unstructured data from dispatch, records management and digital evidence, with vendors identifying supported systems and the integration approach. Auto-refresh of calls for service. Case-linking and entity resolution across connected sources, supporting cross-reference of vehicle and person information. Access to open-source intelligence and shared inter-agency data with configurable access controls, audit logging and security for all shared information. Comprehensive search, data visualization, dashboards, and both predesignated and ad-hoc reporting. Alerts when other users search the same criteria, so that investigations do not unknowingly collide. A "breadcrumbs" or equivalent workflow allowing operators to document the steps taken to reach a conclusion or investigative action. A description of granular inter-agency access controls, and confirmation that inter-agency sharing and deconfliction features are off by default.

What the RFP requires – technology integration platform. A single dashboard correlating multiple live and recorded sources in real time, with single sign-on and consolidated alerts across source types. The ability to customize and drag and drop data and views from maps, camera views, search results, tables and documents. The ability to pop up or highlight a specific camera when a call for service falls within that camera's viewshed. Real-time alerts based on keywords or criteria. Open, documented integrations and APIs to third-party ALPR, camera, drone, analytics and CAD/RMS systems, with known integrations listed. Geospatial mapping, location and radius search, map-drawn search areas, geo-fencing, and alert routing by app, email and text. A dashboard of system productivity – alert volumes, detection and hit volumes, and accuracy ratios – filterable by source, user or system.

What it does not cover. Any cameras or hardware of its own.

Requirements That Apply to All Six Areas

The RFP places a set of cross-cutting requirements on every proposal, regardless of which Areas a vendor bid.

Facial recognition

Prohibited unless expressly authorized by the Berkeley City Council through future council action.

Restrictive by default

Settings must be privacy-protective by default. No data-sharing defaults may be enabled without affirmative City action, and participation in any cross-jurisdictional lookup network – statewide, national or equivalent – is opt-in only. Vendors must disclose every such network their platform supports.

Human review of automated output

All AI-generated output – alerts, matches, classifications and recommendations – is to be treated as an investigative lead only, and must be independently corroborated before any enforcement, charging or detention decision. No investigative action may be initiated solely on the basis of AI output without affirmative human review and authorization. Vendors must identify every action their system can execute without real-time human authorization, and describe the controls available to the City to restrict, audit or disable those functions. Default configurations may not enable enforcement-adjacent automation – such as automatic hotlist sharing, automatic case flagging, or automatic inter-agency notification – without affirmative City configuration.

Auditing

Every system must maintain a detailed audit trail. Specifically, the RFP requires auditing sufficient to identify and track usage by any user at any time; permission and security levels defining user rights and access; and administrator visibility into deployments, queries and hotlists or alerts for all users, including the date, the time, and the reason

given for the query or deployment. The City must be able to run both predesignated and ad-hoc reports on this data and to export audit data. Vendors must describe configurable retention parameters for access logs – how long logs are kept, what each entry captures, whether the City can configure that duration, and whether logs are exportable.

Interoperability

Every component must expose or support documented integrations so the City can correlate data across systems even where Areas are awarded to different vendors. Vendors bidding a single Area must describe the published integrations and APIs available to connect to other systems and to the real-time information center.

Data ownership and accountability

The City owns its data, and that ownership survives termination; the vendor must return or export City data when the agreement ends. The RFP requires agreements to provide a financial penalty of \$290,000 per violation for any unauthorized sharing, disclosure or release of City data, in addition to any other remedy available to the City. Vendors were required either to accept the cross-cutting contractual protections expressly or to identify their proposed exceptions.

**SEPTEMBER 21, 2026 PAB CORRESPONCE TO THE BERKELEY
CITY COUNCIL REGARDING "SURVEILLANCE TECHNOLOGY
ORDINANCE SUBMISSION FOR MUTUAL AID AIR SUPPORT"**



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

September 21, 2026

VIA ELECTRONIC MAIL [Email]

Berkeley City Council
Council@berkeleyca.gov
2180 Milvia Street
Berkeley, California 94704

Re: Surveillance Technology Ordinance Submission for Mutual Aid Air Support

Honorable Mayor Ishii and Members of the City Council,

On behalf of the Police Accountability Board (PAB), I am writing to communicate the Board's recommendation as provided under BMC 2.99.030 regarding the Berkeley Police Department's (BPD) Acquisition Report and Policy 1308 concerning mutual aid air support. The PAB received the materials from the BPD on August 28, 2026, and reviewed them at its regular meeting on September 9, 2026.

Following a majority vote, the PAB recommended approval of the Acquisition Report and Policy 1308 with a minor amendment to Section 1308.11. The amendment is intended to clarify the reporting requirements and eliminate potential ambiguity. The Board's recommended redline is included as Attachment 1.

Accordingly, the PAB respectfully recommends that the City Council approve the Acquisition Report and Policy 1308, subject to the amendment to Section 1308.11 reflected in Attachment 1.

Respectfully submitted,

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
Katherine Lee, Interim Director of Police Accountability

Attachments: 1. PAB's Redline of Policy 1308 Section 11

Attachment 1. PAB's Redline of Policy 1308 Section 11

1308.11 AUDITING AND OVERSIGHT

The Office of Strategic Planning and Accountability (OSPA) shall audit all air support deployments at least twice per year. As part of the audit, OSPA will confirm that BPD has not entered any direct data-sharing arrangements inconsistent with this policy.

BPD will enforce against prohibited uses of Mutual Aid Air Support pursuant to Policy 1010, Personnel Complaints, or other applicable law or policy. The City Manager shall enforce against any prohibited use of air support data by other City of Berkeley personnel.

The audit shall be documented in the form of an internal department memorandum to the Chief of Police. After review by the Chief of Police, the memorandum and any associated documentation shall be placed into the annual report filed with the City Council pursuant to BMC Section 2.99.020(2) and published on the City of Berkeley's website. **The annual report shall include the results of any nonprivileged internal audits, information regarding any violations or potential violations of this policy, and any responsive actions taken.** The annual public report on air support deployments required by the July 14, 2026 resolution shall be transmitted to the City Council and the Police Accountability Board.