MANOHAR RAJU – PUBLIC DEFENDER
MATT GONZALEZ – CHIEF ATTORNEY

SAN FRANCISCO PUBLIC DEFENDER
Greater Than One

SAN FRANCISCO PUBLIC DEFENDER
Greater than one.

San Francisco Police Commission
San Francisco Police Department Headquarters
1245 3rd Street
6th Floor
San Francisco, CA 94158

Sept. 1, 2026

Submitted via Electronic Mail

Re: Vote No on DGO 10.12 to Instead Create a Working Group

Dear President Clay, Vice President Tekkey, and Members of the Commission:

We, the undersigned, write to urge you to vote no on Department General Order 10.12 as written and establish a working group to resolve significant issues and to solicit additional input from the community, experts, and stakeholders. As written, the proposed policy unlawfully expands SFPD's ability to use drones, invites invasions of privacy, chills First Amendment activity, and installs a weak data retention and sharing model.

A working group can resolve these issues and create a policy that reflects best practices and the will of San Francisco voters while minimizing infringement on constitutional rights. Accordingly, and for the reasons set forth below, we urge you to vote no on this draft of the policy and call for a working group to revise the proposed policy.

The Commission Retains the Authority to Revise DGO 10.12

Proposition E did not reduce the Commission to a rubber stamp for any policy SFPD places before it. While Prop E limits the City's ability to impose *new restrictions* on police technology without approval from the Board of Supervisors, it also requires that SFPD use technology *only for legitimate law-enforcement purposes* so long as its use does not impinge on privacy, civil liberties, and constitutionally protected rights. Those commands leave the Commission both the authority and responsibility to implement those principles in this DGO. Moreover, Prop E cannot authorize what the federal or California Constitutions otherwise forbid. Voter approval of police technology does not displace the First and Fourth Amendments or convert potentially unconstitutional surveillance into lawful conduct.

This Commission therefore should zealously scrutinize DGO 10.12 for threats to constitutional rights as it considers whether the policy gives SFPD the operational authority it seeks.[1]

The Policy Expands Drone Usage Beyond Current Statutory Authority

California law expressly classifies an "[u]nmanned, remotely piloted, powered aerial" vehicle as "military equipment"[2] and AB 481 requires a police department's military-equipment policy itself to specify the "purposes and authorized uses" for each type of equipment.[3] Significantly, SFPD must obtain governing-body approval before using existing equipment "for a purpose, in a manner, or by a person not previously approved by the governing body."[4] The Legislature did not merely require elected officials to approve the *purchase of a drone*. It reserved to the applicable governing body (here, the Board of Supervisors) the authority to approve the *purposes and manners* in which it *may be used*, including subsequent expansions.

After Proposition E passed, SFPD submitted an Unmanned Aerial Vehicle (UAV) policy to the Board under AB 481, and the Board approved it.[5] The UAV Policy approved by the Board described the "Authorized Use" of drones: for vehicle pursuits, to assist with active criminal investigations, and for a longer enumerated list of uses that did not include patrols, general surveillance, or use in "any situation in which a member may be deployed."[6]

In 2025, SFPD disclosed that drones were deployed approximately 1,122 times for, among other things, patrols, trainings, and simulations.[7] In less than a year, the Department moved from roughly 350 deployments allowable under the Board-approved policy to more than 1,100 deployments that expressly included patrol or general surveillance outside the scope of the granted authority. In June 2026, the Board unanimously approved SFPD's 2025 Annual Report in a resolution, explicitly authorizing the "continued use of the equipment as described in the 2025 Annual Report."[8]

---

[1] The Chief's Waiver does not foreclose a working group: the Waiver under Administrative Code § 96I.1(b) excuses the separate statutory community-engagement process, while DGO 3.01 treats the community-policy-working-group process as distinct—and the Commission retains authority to direct that a working group be convened.

[2] Gov. Code § 7070(c)(1).

[3] Gov. Code § 7070(d)(2).

[4] Gov. Code § 7071(a)(1)(E).

[5] See Ordinance 233-24, File No. 240636.

[6] San Francisco Police Department, Unmanned Aircraft System (UAS) Proposed Law Enforcement Equipment Use Policy 2 (Sept. 3, 2024), approved by S.F., Cal., Ordinance No. 233-24, § 2(c) (2024).

[7] San Francisco Police Department, Law Enforcement Equipment Policy Pursuant to California Government Code Section 7072: 2025 Annual Report (Jan. 22, 2026), p. 12.

[8] San Francisco Police Department, Law Enforcement Equipment Use Policy – 2025 Annual Report (2026), approved by S.F. Res. No. 390-26, File No. 260626 (July 2, 2026), p. 2.

However, before a law enforcement agency uses military equipment "for a purpose [or] in a manner … not previously approved by the governing body," it must obtain governing-body approval "*by an ordinance* adopting a military equipment use policy" and must do so before engaging in that use.[9] Neither state law nor the San Francisco Charter gives the Board unilateral power to retroactively approve SFPD's expanded drone use, even via an ordinance.

The 2025 Annual Report approved by resolution does not have the same legal effect as an ordinance that state law requires.[10] Perhaps what is most alarming is even if the resolution approving SFPD's existing use *were lawful*, the language in the current draft of DGO 10.12 allows SFPD to use drones "in any situation in which a member may be deployed" *was not approved* in that resolution.

The uncertainty surrounding whether SFPD can now use drones "in any situation in which a member may be deployed" requires the convening a working group to determine the exact parameters of when drones can be deployed.

The Proposed Policy Openly Invites Invasions of Privacy

Competing Instructions on Privacy Will Confuse Officers

The draft policy states that SFPD's "use of UAS will be in strict compliance with constitutional and privacy rights." Yet, it mandates that UAS operators "shall consider the protection" of those same rights only as "a key component" such that the operations must only "take *reasonable precautions* to avoid inadvertently recording or transmitting images where there is a reasonable expectation of privacy." (Emphasis added). The drafted language sits in deep tension with itself: how can a drone pilot both strictly comply with constitutional and privacy rights yet consider those same rights only as a key component of their operation?

That tension leaves officers without meaningful guidance for applying the policy in practice. DGO 10.12 does not define what precautions operators must take to avoid observing or recording areas where people have a reasonable expectation of privacy, when operators must redirect or disable cameras, when zoom or other enhanced capabilities may be used, what must happen to inadvertently captured footage, or what supervisory review is required after a potential privacy intrusion. These are not minor implementation details. They determine whether the DGO's promise of "strict compliance" with constitutional and privacy rights operates as an enforceable limitation or merely an aspiration.

A working group should resolve those questions before the Commission authorizes routine drone operations under an otherwise undefined privacy standard.

---

[9] Gov. Code 7071(a)(1).

[10] See, e.g., *City of Sausalito v. County of Marin* (1970) 12 Cal.App.3d 550, 565–567; *Midway Orchards v. County of Butte* (1990) 220 Cal.App.3d 765, 774–775; *Childhelp, Inc. v. City of Los Angeles* (2023) 91 Cal.App.5th 224.

Near-Constant, Repetitive Surveillance Threatens Constitutionally Protected Rights
The central Fourth Amendment concern with authorizing drones for patrol or general surveillance is that patrol eliminates the investigative predicate that ordinarily limits police surveillance. An incident-driven deployment begins with a reason to use a drone: a reported crime, an emergency, a missing person, a fleeing suspect, or some other defined law-enforcement need. In other words, an enumerated list of operations for which a drone can be deployed. That predicate naturally limits why the drone is deployed, where it should fly, what officers should be looking for, and when the deployment should end. Drones on patrol reverse that sequence. SFPD can deploy the drone first, observe people who are not suspected of anything, and then determine from those observations whether someone warrants further investigation. In practical terms, surveillance ceases to be a tool used in an investigation and becomes a means of looking for something to investigate. It becomes, in short, a surveillance dragnet.

That dragnet also raises substantial concerns under the California Constitution. Article 1, § 13 provides greater protection than the Fourth Amendment in the precise context of police aerial surveillance of residential property. In *People v. Cook*, the California Supreme Court rejected the argument that aerial surveillance was merely a form of routine "street patrol" and held that warrantless police scrutiny of an enclosed backyard from an aircraft violated the state Constitution.[11] The Court warned that "[p]urposeful surveillance from the air simply lays open everything and everyone below—whether marijuana plants, nude sunbathers, or family members relaxing in their lawn chairs—to minute inspection."[12] Drone patrols only sharpen *Cook*'s concern by making purposeful aerial observation cheaper, more persistent, and easier to deploy routinely.

A Fourth Circuit Court of Appeals case illustrates the far end of that continuum—and its limits.[13] The Baltimore Police Department photographed approximately 90 percent of Baltimore for as much as twelve hours per day. Police retained the images and later used them to reconstruct the movements of people and vehicles associated with crimes. The system also integrated aerial information with police dispatch data, fixed surveillance cameras, ShotSpotter, and automatic license plate readers. The Fourth Circuit held that accessing the resulting record

[11] (1985) 41 Cal.3d 373, 381-383.
[12] *Id* at 382; compare *People v. Mayoff* (1986) 42 Cal.3d 1302, 1312, with *California v. Ciraola* (1986) 476 U.S. 207, 214 and *Florida v. Riley* (1989) 488 U.S. 445, upholding limited aerial observations from publicly navigable airspace. Neither federal case, however, addressed the constitutional limits of repeated, technologically enhanced drone surveillance conducted without an incident-specific investigative predicate.
[13] *Leaders of a Beautiful Struggle v. Baltimore Police Department* (4th Cir. 2021) 2 F.4th 330 (en banc), building on *Carpenter v. United States* (2018) 585 U.S. 296, cautions against evaluating technologically enabled surveillance as a series of isolated observations while ignoring the broader picture those observations collectively reveal.

constituted a Fourth Amendment search *because* the system enabled police to deduce all of that person's movements.[14]

Baltimore police did not have to identify everyone it would ultimately investigate before collecting the images. They could preserve movements first and determine later which movements mattered. And once the images had been retained for one investigation, nothing prevented its use in another. The constitutional concern therefore lies in allowing an initially permissible form of observation to develop, without a clear policy boundary, into a system capable of persistent or retrospective tracking.

The Supreme Court's recent decision in *Chatrie v. United States*[15] reinforces that point. The *Chatrie* Court rejected the Government's argument that constitutional protection depended on police examining a sufficiently long period of time. "Even short-term monitoring," the Court explained, can reveal substantial information about an individual's associations, and the constitutional problem was particularly acute where law enforcement could select the information it wanted from an "all-encompassing database."[16] *Chatrie* does not stand for the proposition that every brief drone flight is a search. But it does reject the idea that the constitutional significance of surveillance necessarily turns on how small a portion of a comprehensive record police ultimately examine.

Drone patrol gives SFPD continuing authority to observe first and develop the investigative justification later. The Commission should not rely on the proposition that the most limited possible exercise of patrol authority may be constitutional as justification for granting the broader authority in the first place.

Other California police departments have drawn exactly this line without abandoning operational drone programs:

- ***Chula Vista PD*** expressly prohibits use of its drones for "general surveillance or general patrol operations."
- ***Corona PD*** does not conduct "routine patrol" or "surveillance" flights as a matter of privacy.
- ***Culver City PD*** describes its drone program as "incident driven" and states that its drones "will never be used for routine patrol."
- ***Bakersfield PD*** expressly prohibits drones from conducting "random surveillance activities."

---

[14] *Id.* at 341–46.

[15] (2026) No. 25-112, slip op. at pp. 20–21. Though not about aerial surveillance, the Court held that accessing even a limited period of historical location data can constitute a Fourth Amendment search where police draw from a comprehensive location database. Feeding drone footage from routine patrols into a comprehensive database that SFPD already uses presents a similar constitutional risk.

[16] *Chatrie v. United States (2026)* No. 25-112, slip op. at pp. 20–21 (quoting *United States v. Jones* (2012) 565 U.S. 400, 415 (Sotomayor, J., concurring)).

- ***Woodland PD*** specifically prohibits drones for both "general surveillance" and "general patrol operations."

Those jurisdictions recognize a distinction that drones should not become roving instruments of suspicionless police surveillance. How then should drones be used to the maximum extent allowed under Prop E, state law, and constitutionally protected rights? A working group can properly address those contours.

Suspicionless Drone Surveillance Threatens First Amendment Activity
The Supreme Court has long recognized the "vital relationship between freedom to associate and privacy in one's associations," because government can deter participation by collecting information identifying those who join for political, religious, or social causes.[17]

Drones heighten that concern because they allow police to gather associational information without demanding it directly from an organization or participant. A drone deployed above a demonstration, religious gathering, political meeting, or other protected event can observe the crowd remotely, focus on individuals, record who associates with whom, and potentially maintain observation as people move through or away from the event.

The First Amendment does not prohibit every police observation of activity occurring in public.[18] But that does not mean government surveillance of First Amendment activity is constitutionally insignificant. The Ninth Circuit Court of Appeals distinguished that reasoning when government agents secretly recorded worship services, and the surveillance allegedly caused people to stop attending, participating, and seeking counseling from their churches.[19] The constitutional concern becomes substantially greater when a drone identifies, records, or tracks people engaged in protected activity in ways that deter participation.

DGO 8.10 recognizes that danger and limits officers' involvement in First Amendment activity to legitimate law-enforcement needs and separately regulates video and photographic recording at First Amendment events. Yet, as DPA observed in its recommendation grid to SFPD, the proposed drone policy does not explain when those protections apply to drone operations, does not address generalized surveillance around protests and public assemblies, and does not establish

[17] *NAACP v. Alabama ex rel. Patterson* (1958) 357 U.S. 449, 462–63; see also *Americans for Prosperity Foundation v. Bonta* (2021) 594 U.S. 595, 606–18.
[18] *Laird v. Tatum* (1972) 408 U.S. 1.
[19] *Presbyterian Church (U.S.A.) v. United States* (9th Cir. 1989) 870 F.2d 518, 521–23.

safeguards against operator conduct that could chill protected activity.[20] SFPD's response—that DGO 8.10 is "not directly associated with this policy" and that the Department is "not interested in using this tool to monitor First Amendment participants"[21]—does not resolve the problem. A statement of present intent is not an enforceable limitation on future police authority. And the premise that drones and First Amendment activity are unrelated is difficult to reconcile with SFPD's actual practices: the Department has already deployed drones during First Amendment events.[22]

If SFPD truly does not intend to use drones to monitor people because they protest, worship, organize, associate, speak to the press, or petition their government, the policy should say so. At minimum, DGO 10.12 should make explicit that drone technology does not create an exception to DGO 8.10.

These are precisely the issues a working group should resolve before the Commission approves a policy capable of placing persistent police surveillance above political, religious, and expressive gatherings throughout San Francisco.

Tighten Data Retention and Sharing Requirements

The Commission should not approve a data-retention scheme that looks strict on paper but is riddled with exceptions SFPD itself gets to define. Proposition E allows SFPD to retain "public footage" for up to 30 days and permits access or longer retention when a Captain or higher determines that it is necessary for an open criminal investigation. But retaining footage due to an open criminal investigation does not magically evolve to end the inquiry. The Commission should evaluate whether officers must identify the investigation, the specific footage sought, the factual connection between the two, and why continued access or retention is necessary. In short, the Commission should require a paper trail, impose firm time limits, and require periodic review. Otherwise, the 30-day rule is not much of a rule at all.

The data-sharing provisions present a separate, equally troubling problem. A 30-day retention limit means very little if SFPD can send the footage to another agency and that agency can then retain it, search it, combine it with other surveillance data, or redistribute it under different rules. San Francisco's ordinary surveillance-technology law recognizes that problem and requires policies to address who may receive surveillance data, why they may receive it, and how the

[20] *DGO 10.12 DPA Rec Grid and SFPD Responses, Stage 2*, R2 (S.F. Police Comm'n July 15, 2026).
[21] *Id.*
[22] David Hernandez & Sriharsha Devulapalli, SFPD Has Used Drones Nearly 1,400 Times Since 2024. Here's How, S.F. Chron. (Oct. 16, 2025) (reporting that SFPD flew drones over San Francisco Pride for more than five hours in June 2024).

City will ensure compliance with downstream restrictions.[23] Proposition E exempted drones from that framework.[24] That makes it more—not less—important for DGO 10.12 to supply those protections itself. Any transfer should require a documented lawful purpose, bind the recipient to equivalent restrictions on use, access, retention, deletion, and onward sharing, and create a complete audit trail.

These are not abstract concerns. In July 2026, WIRED reported that an SFPD Skydio sharing link left live drone feeds accessible without authentication for roughly six months, exposing color and thermal video, GPS and telemetry data, pilots' identifying information, and footage involving detentions, residential locations, and unhoused people. And in September 2025, EFF and the ACLU of Northern California alleged that SFPD had given out-of-state agencies direct access to its ALPR database, including agencies in Georgia and Texas, and that multiple searches referenced ICE-related purposes. Different technology, same warning: once SFPD surveillance data leaves the Department's direct control, the risk of misuse, over-retention, and redistribution increases dramatically.

The Commission should not accept a policy that relies on trust where enforceable limits are available. DGO 10.12 should make investigative necessity a real standard, prevent reclassification from swallowing the 30-day rule, and ensure that interagency sharing cannot be used to do indirectly what SFPD could not do directly. If some of those protections require Board approval, then the Commission should identify them and demand that approval rather than approve a policy with the loopholes built in. These complex issues should be examined more fully in a working group.

Conclusion

As currently drafted, DGO 10.12 gives SFPD broad authority to conduct aerial surveillance while leaving critical and practically necessary limits on that authority undefined. The policy impermissibly allows drones to be used for patrol and other open-ended law-enforcement purposes without adequately specifying when surveillance is permissible, how privacy and First Amendment protections apply, what information may be retained, or how that information may be shared. Those gaps create a real risk that drones will evolve from an incident-driven tool into a system of routine surveillance capable of recording sensitive information about where people go, whom they associate with, and what protected activities they participate in.

None of these risks is necessary to preserve the legitimate operational value of drones. Other jurisdictions continue to deploy drones in response to emergencies, reported crimes, and specific investigative needs while prohibiting general

[23] S.F. Admin. Code § 19B.1 (defining "Surveillance Technology Policy," subd. (9)).
[24] S.F. Admin. Code § 96I.2(e).

surveillance and routine patrol and imposing stronger safeguards on protected activity and collected data. San Francisco can do the same.

The Commission should require clear, enforceable limits on when drones may be deployed, how DGO 8.10 and privacy protections apply, how retained footage may be accessed, and when surveillance data may be shared outside the Department. These issues should be resolved before broad drone authority becomes normalized rather than after its consequences become apparent.

For these reasons, we urge the Commission to vote no on DGO 10.12 as currently drafted and convene a Commission-led working group to develop a policy that preserves legitimate drone uses while establishing meaningful protections for privacy, civil liberties, and constitutional rights.

Respectfully submitted,

San Francisco Public Defender's Office
American Civil Liberties Union of Northern California
Center on Juvenile and Criminal Justice
National Harm Reduction Coalition
Women's Housing Coalition
Drug Policy Alliance
Legal Services for Prisoners with Children
Council on American-Islamic Relations, San Francisco Bay Area
The Gubbio Project
California Coalition for Women Prisoners
SF Rising
Chinese for Affirmative Action
GLIDE Foundation
Electronic Frontier Foundation
Community Legal Services in East Palo Alto