



Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109

September 18, 2026

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

Submitted via Electronic Mail

Re: Public Comment on DGO 10.12

Dear Members of the San Francisco Police Commission:

The San Francisco Police Department's (SFPD) revised draft of Department General Order (DGO) 10.12 lacks crucial details around the Department's current and anticipated use of unmanned aerial systems (UASs) and fails to address the capabilities of drones and drone-as-first-responder programs.

SFPD has lobbied for and embraced a "mandate" to "use technology to the maximum extent possible to improve its efficiency and effectiveness in combatting crime, and to reduce dangers to the public, subject to the City's policies to protect privacy and civil liberties," ensuring that the details and foresight embedded in the City's policies on responsible deployment are of utmost importance.

Surveillance technology and its capabilities are rapidly developing. Even in the relatively short time since the March 2024 passage of Proposition E, the capacity to collect, analyze, store, and share information gathered by drones has expanded. The rapid integration of artificial intelligence into police surveillance and investigatory platforms continues to fuel worrying developments that threaten privacy and security.

DGO 10.12 must acknowledge the technological capabilities of today's modern police surveillance network and require additional guardrails. The public deserves clarity and specificity around SFPD's continued use of this technology.

Clarity around Deployment

The revised policy states that "UAVs may be used as an asset in any situation in which a member may be deployed for a public safety response or when a member onviews criminal activity" but fails to define what is meant by a "public safety response." The revised policy also provides a definition of "Drone as First Responders," but it fails to provide any more detail about appropriate DFR deployment. Without appropriate safeguards around deployment and use, drones could be deployed to every call for service, even in situations that are ultimately deemed nonincidents, collecting data along the way that is then stored for 30 days. This type of general patrol could effectively become general surveillance, which SFPD acknowledges is an inappropriate use of their drones and yet is still possible under the vague terms of the current DGO.

Privacy

The revised policy claims that "All UAS operations shall consider the protection of individual civil rights and the reasonable expectation of privacy as a key component in any decision made to deploy a [unmanned aerial vehicle]."

Unfortunately, this policy itself fails to specifically consider how to protect individual privacy and civil liberties in ways that are obvious and commonly detailed in other municipalities' drone policies.

For example, the one and only other point in the policy's "Privacy" section states that "UAS operators shall take reasonable precautions to avoid inadvertently recording or transmitting images of areas where there is a reasonable expectation of privacy, unless authorized by law." Yet the policy fails to identify a single reasonable precaution that an operator should take to achieve this. Given the emphasis placed on the rapidity with which drones will be deployed to calls, the public cannot expect each individual drone operator to consider privacy concerns during each individual call or to apply them in a uniform manner.

SFPD should implement a policy prohibiting the filming or recording of footage during a drone's flight to or from the scene of a call for service, protecting innocent individuals in the drone's path from being recorded and eliminating the possibility that automated license plate reader (ALPR) capabilities or integrated features could be used to identify vehicles or individuals that simply happen to be in a drone's flight path. Other departments have implemented such policies, requiring cameras to be turned off or fixed on a particular spot on the horizon. Strictly limiting the collection of information and footage on a drone would further protect individuals from the privacy risks associated with retroactive analysis of drone footage, future drone capabilities, and the data sharing and data integration facilitated by common police platforms.

Currently, the policy relies on a 30-day retention period for footage unrelated to a criminal investigation. This retention period should be shortened. There is no investigatory reason to maintain footage of innocent people for as long as a month, a period of time in which that information could be shared, duplicated, and misused. Moreover, any footage that is related to a criminal investigation must be limited to the evidentiary portion of the recording; any footage lacking evidentiary value that captures unrelated people or activity during the same flight must not be retained.

Require Oversight of Data Sharing, Duplication, and Added Capabilities

Drone-mounted cameras are capable of collecting video footage that may later be integrated into sophisticated video analytics platforms or may become subject to on-device updates and capabilities.

Currently, the policy fails to address the integration of data and AI analytics being used by law enforcement, and raises the following questions:

- Which other SFPD platforms have access to drone footage?
- Where are copies of drone footage being made?
- How will retention and deletion requirements affect those systems?
- Are partner agencies who receive SFPD's drone footage bound by this policy?

Questions like these are not addressed in DGO 10.12. SFPD uses [Peregrine](#) and other platforms within the City's Real-Time Investigation Center, suggesting that drone footage streams are regularly ingested into other platforms with the capacity to store, analyze, and share data. This policy fails to describe anything like these platforms, only stating that, "Footage collected during UAS operations may be shared by the Program Manager with relevant partner agencies in accordance with laws governing evidence, orders of the Court, MOUs, Charter Authority, state, or local laws." Given the wide data-sharing potential available to law enforcement, this failure to explicitly address how information can further be stored and duplicated is a severe oversight to protecting privacy during drone operations.

Moreover, the policy must address the integration of other technology within drone-mounted cameras. For example, in 2025, drone manufacturers like Flock Safety [quietly added ALPR capabilities](#) to their drones, allowing them to log license plate and vehicle information from their discreet positions hundreds of feet in the air. Increased camera definition combined with video analytics make the transition from a flying camera to an ALPR possible with simply a software update. A drone camera can be one video node in an extensive surveillance network that, with AI

capabilities, allows for search of objects or people in general terms: “a blue Camry” or “a man with a purple backpack.” These capabilities are serious ones, but they may not require new equipment, more money, or any public awareness. SFPD’s drone policy must address this.

Further, it must be made clear that additional equipment and capabilities — such as the use of a drone to facilitate the collection of cell phone information (like through use of cell-site simulators) or for weapon-related reasons — must be disclosed and brought before the appropriate governing body.

Transparency and Compliance with State Law

Drone flight portals are very commonly used to provide transparency. In California, multiple law enforcement agencies — including [Los Angeles Police Department](#) and [Sacramento Police Department](#) — provide the public with detailed information about drone flight paths through transparency portals. In some cases, this is real-time information; in other cases, it is released on a delay. In either case, SFPD must make such transparency a requirement.

The current policy states, “The public may submit public information requests for footage and the Department will defer to the Department’s Legal Division and the Office of the City Attorney to consider the requests.” Drone footage should be subject to public records laws and transparency expectations as a public record created and maintained for public purposes.

Further, SFPD must comply with the requirements of California Government Code § 7072, which mandates annual reporting about current and intended uses of important military equipment, like UAVs. Past reports have failed to describe the DFR program that SFPD was apparently poised to launch after the passage of Prop E, suggesting that, while the department anticipated the use of UAVs, they did not follow state law in doing so.

Conclusion

SFPD’s revised proposal for DGO 10.12 is inadequate in its failure to create operational guidelines that address the way drones are being used and the legitimate privacy concerns associated with airborne surveillance and modern data sharing and analysis capabilities. SFPD has been using drones for two years and presumably gathering experience and information in that time that would help it to draft a more robust policy. This is a responsibility that the department needs to take on.

DGO 10.12 will be an important guiding document for the use of drones and for ensuring protection of individual privacy rights and civil liberties. It should articulate appropriate deployment use, enact restrictions on recording and data sharing, provide and reaffirm public avenues for transparency and oversight, and clearly restrict the addition of surveillance and airborne capabilities. To approve this policy without addressing these provisions would be a disservice to the people of San Francisco.

Respectfully,

Electronic Frontier Foundation