Surveillance Technology Policy

Unmanned Aerial Systems
Police Department

The City and County of San Francisco values privacy and protection of San Francisco residents' civil rights and civil liberties. As required by San Francisco Administrative Code, Section 19B, the Surveillance Technology Policy aims to ensure the responsible use of Unmanned Aerial Systems (UAS), [also referred to as Unmanned Aerial Vehicles (UAV) or Small Unmanned Aerial Systems (sUAS)], itself as well as any associated data, and the protection of City and County of San Francisco residents' civil rights and liberties.

PURPOSE AND SCOPE

Pursuant to the San Francisco Charter, the Police Department is required to preserve the public peace, prevent, and detect crime, and protect the rights of persons and property by enforcing the laws of the United States, the State of California, and the City and County. The Department's mission is to protect life and property, prevent crime and reduce the fear of crime by providing service with understanding, response with compassion, performance with integrity and law enforcement with vision.

The Surveillance Technology Policy ("Policy") defines the way the UAS will be used to support this mission, by describing the intended purpose, authorized and restricted uses, and requirements.

This Policy applies to all department personnel that use, plan to use, or plan to secure UAS, including employees, contractors, and volunteers. Employees, consultants, volunteers, and vendors while working on behalf of the City with the Department are required to comply with this Policy.

POLICY STATEMENT

The authorized use of the surveillance technology for the Department is limited to the following use cases and is subject to the requirements listed in this Policy.

Authorized Use(s): Support first responders and investigators when they can benefit from an aerial perspective during the following specified uses:

- Sideshows (AKA stunt driving) and/or street takeover events where many vehicles and reckless driving are present.
- Major and Critical incidents as defined by SFPD General Order 8.01, including but limited to mass casualty events, natural disasters or Hazardous material incidents.
- High-risk search warrant service.
- Apprehension of armed and dangerous and/or violent suspects.
- Hostage/Crisis Negotiations Team (H/CNT) incidents.
- Pre-planned deployment mapping.
- Search & rescue operations.
- Post-incident crime scene mapping, preservation, and documentation.
- Apprehension of suspects who have fled on foot.
- Auto Burglary and Robbery Abatement Operations.

Surveillance Oversight Review Dates
PSAB Review: August 24, 2023; November 7, 2023. COIT Review: TBD
Board of Supervisors Review: TBD

- When there is probable cause to arrest or reasonable suspicion to detain an occupant of a vehicle and reasonable belief that the operator of the vehicle is likely to flee if a vehicle stop is attempted.
- Department training relating to authorized uses.

UASs may only begin recording upon arrival on scene during one or more of the above listed authorized uses.

Any use of a UAS shall comply with constitutional and privacy rights, the applicable regulations of the Federal Aviation Administration (FAA), CCSF ordinances, SFPD written directives and UAS manufacturers' approved flight manuals.
This surveillance technology may be deployed by sworn members in the Field Operations Bureau and Special Operations Bureau.
The UAS equipment may be deployed in the following locations, based on use case: The City & County of San Francisco, San Francisco Airport property and SFPD led operations in the greater Bay Area.

Prohibitions and Restrictions:

The UAS equipment shall not be used:

- For the purpose of harassing, intimidating or discriminating against any individual or group.
- To monitor individuals based on their race, gender, religion, or sexual orientation.
- For a non-law enforcement related matter.
- In an unsafe manner or in violation with FAA regulations.

The UAS shall not be equipped with weapons of any kind.

The UAS shall not be used as a force option.

Where there are specified and articulable grounds to believe that the UAS may collect evidence of criminal wrongdoing and the UAS is used in a manner that may intrude upon an individual's reasonable expectations of privacy, the Department shall obtain a search warrant prior to conducting the flight, unless a recognized warrant exception exists (exigency, consent etc.), and utilize the UAS in accordance with the authorized use(s) of this policy.

UAS operations shall not exceed 24 hours of continuous monitoring or recording unless addressing prolonged Major or Critical incidents where extensive response and commitment of resources are required.

BUSINESS JUSTIFICATION

Reason for Technology Use

The surveillance technology supports the Department's mission and provides important operational value in the following ways:

Unmanned Aircraft Systems (UAS) may be utilized to improve response times, enhance efficiency, and increase officer safety during high-risk incidents. Enhancing SFPD's capabilities through aerial observation results in the timely apprehension of criminals and safe de-escalation of individuals in crises. Direct aerial observation allows officers to not rely solely on third-hand information passed through dispatch where descriptions of incidents and/or suspects may be unreliable. The firsthand aerial perspective enables officers to respond to incidents

with proportionality, safety, and respect.

Description of Technology

Unmanned Aerial System (UAS) - An unmanned aircraft of any type that is capable of sustaining directed flight, whether preprogrammed or remotely controlled (also referred to as an unmanned aerial vehicle (UAV)), and all the supporting or attached systems designed for gathering information through imaging, recording or any other means.

Generally, a UAS consists of:

- Chassis with several propellers for flight
- Control propellers and other flight stabilization technology
- Radio frequency and antenna equipment to communicate with remote-control unit
- A camera
- Audio recording
- A digital image/video storage system for recording into a digital data memory card
- A remote-control unit
- Battery charging equipment for the aircraft and remote control

UAS models are subject to change with the advancement and update of technology.

The following capture UAS capabilities available to law enforcement agencies: Live streaming and recording through a 4k visual camera or thermal imaging lens, two-way communication via a cell phone SIM card which provides a way to de-escalate hostile situations, battery performance that provides for a longer flight time and protection through adverse weather and temperature conditions. UASs can provide unique benefits that allow for exterior open-air or in building searches as well as overwatch capabilities during incidents.

Due to battery life, the average flight time is 28 minutes.

The expected lifespan of UAS equipment is 150-800 flight hours.

Resident Benefits

The surveillance technology promises to benefit residents in the following ways:

	Benefit	Description
X	Education	UAS presentations can be used to demonstrate its use as a de-escalation tool and how it can be used to safely resolve critical incidents. The Department may use footage for training purposes to improve police response methods.
☐	Community Development	
X	Health	According to the CDC, community violence affects millions of people, and their families, schools, and communities every year. Community violence can cause significant physical injuries and mental health conditions such as depression, anxiety, and post-traumatic stress disorder (PTSD). Successfully prosecuting major crime is an essential part of protecting life and building a healthy community.

X	Environment	UASs can conduct surveys and assessment of collapsed structures, damage and risk assessments, and severity of damage to affected areas including natural disasters.
X	Criminal Justice	To enhance the San Francisco Police Department's mission of protecting lives and property, while increasing transparency by collecting and making data policies and procedures publicly available to the local community and supporting community outreach and engagement.

Department Benefits

The surveillance technology will benefit the department in the following ways:

	Benefit	Description
X	Financial Savings	UASs can be far more time efficient and cost effective when responding to emergency incidents. Alternatives like helicopters are more expensive than UAS technology.
X	Time Savings	UASs reduce the number of staff and time spent responding to calls for service or during authorized uses. UASs allow officers to assess and prioritize calls for service and even clear calls without ever sending ground units.
X	Staff Safety	UASs would be deployed to dangerous or inaccessible locations/incidents instead of personnel. These range from a variety of situations such as Barricaded Subjects, Hostage Situations, or Sniper Situations. UASs enhances de-escalation by providing critical information to formulate tactics proportional to the emergency at hand.
X	Data Quality	UASs can provide an omnipresent perspective at a scene, providing post-incident crime scene mapping, preservation, and documentation.
X	Other	UAS technology creates time and distance to de-escalate critical incidents, reducing risk to the public and officers.

POLICY REQUIREMENTS

This Policy defines the responsible data management processes and legally enforceable safeguards required by the Department to ensure transparency, oversight, and accountability measures. Department use of surveillance technology and information collected, retained, processed, or shared by surveillance technology must be consistent with this Policy; must comply with all City, State, and Federal laws and regulations; and must protect all state and federal Constitutional guarantees.

Specifications: The software and/or firmware used to operate the surveillance technology must be up to date and maintained.

Data Collection: The Department shall only collect data required to execute the authorized use cases. All data collected by the surveillance technology, including PII, shall be classified according to the City's Data Classification Standard.

The surveillance technology collects some or all of the following data type(s):

Data Type(s)	*Format(s)*	*Classification*
Still Image, Thermal Imaging	JPG, DNG, R.JPG, PNG and other formats	Level 3
Video	MP4, MOV, MPG, AVI, and other formats	Level 3

Access: All parties requesting access must adhere to the following rules and processes: SFPD members designated as operators and administrators must be approved to access the UAS and any processed data and information must be related to an investigation.
Technology Division members will be designated to perform tasks essential to the health and functionality of the data storage mechanism, which does not include access to law enforcement sensitive, privileged, or confidential case records or information.

A. Department employees

Once collected, the following roles and job titles are authorized to access and use data collected, retained, processed, or shared by the surveillance technology:

- Non-sworn members with authorization from Chief of Police, or designee.
- Authorized sworn members designated and trained as UAS Operators and Administrators
- Q2-Q4, Police Officer
- Q35-Q37, Assistant Inspector
- Q0380- Q0382, Inspector
- Q50-Q-52, Sergeant
- Q60-Q62, Lieutenant
- Q80-Q82, Captain
- 0488-0490, Commander
- 0400-0402, Deputy Chief
- 0395, Assistant Chief
- 0390, Chief of Police
- 1044, IS Engineer Principal

- 1043, IS Engineer Senior
- 1070, IS Project Director
- 1094, IS System Administrator IV
- 1093, IS System Administrator III
- 8173, Legal Assistant
- 8177, Attorney

B. Members of the public

The Department will comply with the California Public Records Act, the San Francisco Sunshine Ordinance, the requirements of the federal and State Constitutions, and federal and State civil procedure laws and rules.

Collected data that is classified as Level 1-Public data may be made available for public access or release via DataSF's Open Data portal. Open Data has a Public Domain Dedication and License and makes no warranties on the information provided. Once public on Open Data, data can be freely shared, modified, and used for any purpose without any restrictions. Any damages resulting from use of public data are disclaimed.

Members of the public may also request access by submission of a request pursuant to San Francisco's Sunshine Ordinance. No record shall be withheld from disclosure in its entirety unless all information contained in it is exempt from disclosure under express provisions of the California Public Records Act or some other statute.

UAS data associated with a criminal investigation will not be accessible to the public. Members of the public can submit a public information request. The Department will defer to general counsel and the SFPD legal unit to determine whether the request can be fulfilled.

Training:

To reduce the possibility that UAS or its associated data will be misused or used contrary to its authorized use, all individuals requiring access must receive training on data security policies and procedures.
At the very least, the Department shall require all elected officials, employees, consultants, volunteers, and vendors working with the technology on its behalf to read and formally acknowledge all authorized and prohibited uses. The Department shall also require that all individuals requesting data or regularly requiring data access receive appropriate training before being granted access to systems containing PII.

- 40-hours of training in UAV/UAS: Standard Law Enforcement and FAA training may cover the following topics: Applicable regulations, emergency procedures, effects of weather on UAS performance, Tactical UAS deployments, UAS incident debriefs, airborne search techniques, UAS operation at night, Airport regulations, UAS program breakdowns, and

more.

- Current FAA 14 CFR Part 107 - Remote Pilot Certification
- Ongoing annual training as designated by the SFPD UAS Program Manager

Data Security: Department shall secure PII against unauthorized or unlawful processing or disclosure; unwarranted access, manipulation, or misuse; and accidental loss, destruction, or damage. Surveillance technology data collected and retained by the Department shall be protected by the safeguards appropriate for its classification level(s) as defined by the National Institute of Standards and Technology (NIST) security framework 800-53, or equivalent requirements from other major cybersecurity framework selected by the department.

The Department shall ensure compliance with these security standards through the following: SFPD Technology Division will ensure that data security aligns with the FBI's Criminal Justice Information Services Division (CJIS) standards which is an important compliance standard for law enforcement at the local, state, and federal levels, and is designed to ensure data security in law enforcement. The Department maintains compliance with requirements established and enforced by the Department of Justice California Law Enforcement Telecommunications System (CLETS). Our department ensures all contractors and vendors who have access or exposure to Confidential Offender Record Information (CORI) have fulfilled training and background requirements. Click here for CLETS Policies, Practices and Procedures.

Data Storage: The UAS data may be stored in the following location:

- X Local storage (e.g., local server, storage area network (SAN), network attached storage (NAS), backup tapes, etc.)
- ☐ Department of Technology Data Center
- X Software as a Service Product
- X Cloud Storage Provider

Data Sharing: For internal and externally shared data, shared data shall not be accessed, used, or processed by the recipient in a manner incompatible with the authorized use cases stated in this Policy.

Department shall ensure proper administrative, technical, and physical safeguards are in place before sharing data with other CCSF departments, outside government entities, and third-party providers or vendors. *(See Data Security)*

Department shall ensure all PII, and restricted data is de-identified or adequately protected to ensure the identities of individual subjects are effectively safeguarded from entities that do not have authorized access under this policy.

Further, in sharing data, processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership for the purpose of uniquely identifying an individual person, data concerning health or data concerning an individual person's sex life or sexual orientation shall be prohibited.

Each department that believes another agency or department receives or may receive data collected from its use of surveillance technologies should consult with its assigned deputy city attorney regarding their legal obligations.

Before sharing data with any recipients, the Department will use the following procedure to ensure appropriate data protections are in place:

- Confirm the purpose of the data sharing aligns with the department's mission.
- Consider alternative methods other than sharing data that can accomplish the same purpose.
- Redact names, scrub faces, and ensure all PII is removed in accordance with the department's data policies.
- Review of all existing safeguards to ensure shared data does not increase the risk of potential civil rights and liberties impacts on residents.
- Evaluation of what data can be permissibly shared with members of the public should a request be made in accordance with the San Francisco's Sunshine Ordinance.
- Ensure data will be shared in a cost-efficient manner and exported in a clean, machine-readable format.

A. Internal Data Sharing (city agencies):

The department shares the following data with recipients within the City and County of San Francisco:

Data Type	Data Recipient
Video, Still Photos/Images, Thermal Imaging	District Attorney's Office for use as evidence to aid in prosecution, in accordance with laws governing evidence
Video, Still Photos/ Images, Thermal Imaging	Public Defender's Office or criminal defense attorney via the District

	Attorney's Office in accordance with California and federal discovery laws
Video, Still Photos/Images, Thermal Imaging	The Department of Police Accountability in accordance with memorandum of understanding (MOU), Charter authority, state, or local law.

Frequency - Data sharing occurs at the following frequency: As needed.

B. External Data Sharing (non-city agencies):

The department shares the following data with recipients external to the City and County of San Francisco:

Data Type	Data Recipient
Video, Still Photos/Images, Thermal Imaging	Law enforcement partners, as part of a criminal or administrative investigation; Parties to civil litigation, or other third parties, in response to a valid Court Order
Video, Still Photos/Images, Thermal Imaging (redactions made in compliance with Ca. Gov Code 6254)	Media outlets. If footage is not connected with an active investigation and/or approved by chain of command and SFPD legal teams.

Frequency - Data sharing occurs at the following frequency: As needed.

Public records requests can be made at the following link:

https://www.sanfranciscopolice.org/get-service/public-records-request

Data Retention: Department may store and retain raw PII data only as long as necessary to accomplish a lawful and authorized purpose.

The Department's data retention period and justification are as follows:

Retention Period	Retention Justification
UAS recordings relevant to a criminal, civil or administrative manner shall be retained for a minimum of two (2) years. UAS data provided per warrant request to investigators is retained per the department's retention policy and times will vary per offense type. UAS recordings that do not capture incidents relevant to a criminal, civil or administrative manner and are not deemed as material and/or exculpatory evidence may be erased, destroyed, or recycled after a retention period of sixty (60) days.	Material (inculpatory and/or exculpatory) evidence must be preserved. Evidence is material if it is relevant to an important issue in the case, and evidence is exculpatory if it supports a defense or tends to show that a defendant is not guilty of the crime. Retention allows for any appeals process to occur or if further analysis is needed it will be available. Evidence, if deemed relevant to a criminal, civil, or administrative matter may be retained for a minimum period of 2 years and in accordance with federal/state law(s). Examples include: -Incident/Citizen Contact -Misdemeanor Case (including report, statements, cite or arrest) -Runaway- Returned Evidence, if deemed relevant to a criminal, civil, or administrative matter is retained indefinitely, and in accordance with federal/state law(s). Examples include: -Homicide -Violent Felony/DOA -Collision- Major Injury/Fatal -Sex Crimes -Internal Affairs Investigations -Officer Use of Force Note: Evidence in multiple cases will use the longest retention policy for all of the cases.

Exceptions to Retention Period – PII data collected by the surveillance technology may be retained beyond the standard retention period only in the following circumstance(s):

- SFPD is a law enforcement agency and required by state law(s) to retain evidence relevant to a criminal, civil, or administrative matter. In many cases, evidence must be retained for the entire duration of a convicted subject's required custody. PII data retained during an investigation of a crime, is subject to evidence codes, Ca. penal codes, and other state or federal laws.

Data Disposal:	Upon completion of the data retention period, the Department shall dispose of data in the following manner: Data destruction via deleting/wiping/erasing/degaussing or otherwise making the data irretrievable.

COMPLIANCE

Department Compliance

The Department shall oversee and enforce compliance with this Policy according to the respective memorandum of understanding of employees and their respective labor union agreements.
UAS policies shall have the same compliance requirements as all Department Written Directives and Police Commission Resolutions, per the "Sanctions for Violations" section of this policy.

1.) The Department shall assign one individual to serve as the SFPD UAS Program Manager.
2.) The SFPD UAS Program Manager shall assign two individuals to maintain updates and perform required maintenance. A procedural pre-mobilization and post-mobilization safety check will be performed at each operation.
3.) The SFPD UAS Program Manager's Officer in Charge (OIC) shall oversee Policy Compliance by the Department. If allegations arise that a member is not in compliance, the OIC will initiate an investigation and will take the appropriate action which could include an investigation of misconduct by Internal Affairs.

The duties of the SFPD UAS Program Manager include, but are not limited to:
1. Conducting periodic and random audits of UAS video recording equipment.
2. Conducting periodic and random audits of UAS recordings for members' compliance with the policy.
3. Maintaining a deployment log, including date, general location, authorized use, flight duration, case/incident, or CAD #.
4. Maintaining a log of access, duplication, distribution, and deletion.
5. Conducting periodic audits of recordings during deployments based on drone GPS location capabilities, if available, to ensure compliance with this policy.

Allegations of 19B Violations: Members of the public may submit written notice of an alleged violation of Chapter 19B to SFPDChief@sfgov.org. If the Department takes corrective measures in response to such an allegation, the Department will post a notice within 30 days that generally describes the corrective measures taken to address such allegation (https://www.sanfranciscopolice.org/your-sfpd/policies/19b-surveillance-technology-policies). The Department will comply with allegation and misconduct processes as set forth by the city Charter.

If a Department is alleged to have violated the Ordinance under San Francisco Administrative Code Chapter 19B, Department shall post a notice on the Department's website that generally describes any corrective measure taken to address such allegation.

Department is subject to enforcement procedures, as outlined in San Francisco Administrative Code Section 19B.8.

Sanctions for Violations: The San Francisco Police Department will conduct an internal investigation though the Chief of Staff/Internal Affairs (IA) Unit or may refer the case to the Department of Police Accountability. The results of the investigation will be reported to the Chief of Police, who will determine the penalty for instances of misconduct. Under San Francisco Charter section A8.343, the Chief may impose discipline of up to a 10-day suspension on allegations brought by the Internal Affairs Division or the Department of Police Accountability. Depending on the severity of the allegation of misconduct, the Chief or the Department of Police Accountability may elect to file charges with the Police Commission for any penalty greater than the 10-day suspension. Any discipline sought must be consistent with principles of just cause and progressive discipline and in accordance with the SFPD Disciplinary Guidelines.

DEFINITIONS

Personally Identifiable Information	Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.
Raw Data	Information collected by surveillance technology that has not been processed and cleaned of all personal identifiable information. The distribution and use of raw data is tightly restricted.
CAD	Computer Aided Dispatch System (CAD). CAD systems allow public safety operations and communications to be augmented, assisted, or partially controlled by an automated system. It can include, among other capabilities, computer-controlled emergency vehicle dispatching, vehicle status, incident reporting, and management information.
Major Incidents	The SFPD Department General Order (DGO) 8.01 defines a Major Incident as an event involving potential or actual injury, death, or property damage requiring an exceptional emergency response. This includes natural disasters (floods, earthquakes, major fires, etc.) and human-caused emergencies (plane crash, riot, terrorist acts, etc.) that require extensive response and commitment of resources to control or resolve. This definition is subject to change through the Police Commission adoption of an amended DGO. For a specific list of examples, please read the current version of DGO 8.01.
Critical Incidents	The SFPD Department General Order (DGO) 8.01 defines a Critical Incident as any incident with a life-threatening situation, a defined terrain objective, and requiring a coordinated tactical response should be declared as a critical incident. Procedures and guidelines for requesting the Tactical Unit should be followed. This definition is subject to change through the Police Commission adoption of an amended DGO. For a specific list of examples, please read the current version of DGO 8.01.

Pre-planned deployment mapping	This is a process that allows for early review and mapping of potentially dangerous locations related to specific high-risk investigations or operations ahead of deploying officers to that location or ahead of tactical entry to increase officer and subject safety.
Auto Burglary and Robbery Abatement Operations	Planned enforcement actions usually conducted and coordinated by multiple units/teams including investigators, plainclothes teams, and uniformed patrol officers. These operations focus on high crime incidence areas with the goal of identifying and apprehending suspects tied to auto burglaries and robberies (including armed robbery, aggravated robbery etc.)

STANDARD REPORTING OF UAS FLIGHT LOGS

Once the SFPD UAS Program is operational, the Department will post a report of UAS deployments on its public website. The standard reporting will include the date of flight, case, CAD or incident #, flight duration, general location, and the authorized use category. Training flights will not be included in the standard reporting of UAS flight logs. The logs will be updated monthly and shall be publicly posted for a minimum of five years.

ANNUAL REPORTING PURSUANT TO CALIFORNIA ASSEMBLY BILL 481

Unmanned, remotely piloted, powered aerial vehicles are defined by Assembly Bill 481 to be "military equipment" and as such are subject to requirements set forth in Government Code 7070 – 7072. The Board of Supervisors shall determine, based on review of the annual UAS report, whether the UAS equipment complied with the standards set forth in Government Code 7071(d). If the Board of Supervisors determines that SFPD has not complied with Government Code 7071(d) standards, the Board may vote to disapprove a renewal or require modifications to this use policy in a manner that will resolve the lack of SFPD's compliance with Government Code 7071(d).

Pursuant to Government Code 7072(a), SFPD shall submit to the Board of Supervisors an annual military equipment report for each type of military equipment approved by the Board of Supervisors within one year of approval, and annually thereafter for as long as the military equipment is available for use. SFPD shall also publicly post the annual UAS equipment report on its website for as long as the UAS equipment is available for use. The annual UAS equipment report shall, at a minimum, include the following information for the immediately preceding calendar year for the UAS equipment:

(1) A summary of how the UAS was used and the purpose of its use.
(2) A summary of any complaints or concerns received concerning the UAS equipment.
(3) The results of any internal audits, any information about violations of the UAS use policy, and any actions taken in response.
(4) The total annual cost of the UAS equipment including acquisition, personnel, training, transportation, maintenance, storage, upgrade, and other ongoing costs, and from what source funds will be provided for the military equipment in the calendar year following submission of the annual UAS equipment report.
(5) The quantity possessed.

(6) If SFPD intends to acquire additional UAS equipment in the next year and the quantity sought.

Within 30 days of submitting and publicly releasing an annual UAS equipment report pursuant to Government Code 7072, SFPD shall hold at least one well-publicized and conveniently located community meeting through the Police Commission at which the general public may discuss and ask questions regarding the annual UAS Equipment report and SFPD's funding, acquisition, or use of equipment listed in the report.

The Department shall create an internal process to monitor and track all data points relating to the annual reporting requirement.

AUTHORIZATION

Section 19B.4 of the City's Administrative Code states, "It is the policy of the Board of Supervisors that it will approve a Surveillance Technology Policy ordinance only if it determines that the benefits the Surveillance Technology ordinance authorizes outweigh its costs, that the Surveillance Technology Policy ordinance will safeguard civil liberties and civil rights, and that the uses and deployments of the Surveillance Technology under the ordinance will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or Protected Class."

QUESTIONS & CONCERNS

Complaints of Officer Misconduct: Members of the public can register complaints about SFPD activities with the Department of Police Accountability (DPA), 1 South Van Ness Ave, 8th Floor, San Francisco, CA 94103, (415) 241-7711, https://sf.gov/departments/department-police-accountability. DPA, by Charter authority, receives and manages all citizen complaints relating to SFPD use of force misconduct, or allegations that a member has not properly performed a duty. DPA manages, acknowledges, and responds to complaints from members of the public.

Concerns and Inquiries: Department shall acknowledge and respond to complaints and concerns in a timely and organized response, and in the following manner: The Department has included a 19B Surveillance Technology Policy page on its public website: https://www.sanfranciscopolice.org/your-sfpd/policies/19b-surveillance-technology-policies. This page includes an email address for public inquiries: SFPDChief@sfgov.org. This email is assigned to several staff members in the Chief's Office who will respond to inquiries within 48 hours.

Inquiries from City and County of San Francisco Employees: All questions regarding this policy should be directed to the Chief of Police at SFPDChief@sfgov.org. Similarly, questions about other applicable laws governing the use of the surveillance technology or the issues related to privacy should be directed to the Chief of Police at SFPDChief@sfgov.org