Surveillance Impact Report

Non-City Entity Surveillance Cameras
San Francisco Police Department (SFPD)

As required by San Francisco Administrative Code, Section 19B ("19B"), departments must submit a Surveillance Impact Report for each surveillance technology to the Committee on Information Technology ("COIT") and the Board of Supervisors.

The Surveillance Impact Report details the benefits, costs, and potential impacts associated with the Department's use of Non-City Entity Surveillance Cameras (hereinafter referred to as "surveillance technology").

PURPOSE OF THE TECHNOLOGY

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.

This impact report applies to security camera data sharing between SFPD and the following entities: Any non-City entity or individual, through consent, subpoena, search warrant or other court order, who provides SFPD with data access or information acquired through the entity or individual's use of surveillance cameras or surveillance camera networks owned, leased, managed and/or operated by the entity or individual.

The Department shall use the surveillance technology only for the following authorized purposes:

Authorized Use(s):

1. Temporary live monitoring (a) during an exigent circumstance as defined by San Francisco Administrative Code, Section 19B, (b) during Significant Events with public safety concerns only for placement of police personnel due to crowd sizes or other issues creating imminent public safety hazards, or (c) in the course of a specific criminal investigation if an SFPD Captain or member in rank above Captain confirms in writing that the department has credible information of criminal activity and live monitoring is being requested in furtherance of that criminal investigation. Temporary live monitoring will cease, and the connection will be severed within 24 hours after the non-city entity has provided access to SFPD. SFPD shall not record or duplicate the live monitoring feed using any electronic device, including body worn cameras or cell phones. If SFPD observes misdemeanor or felony violations on the live monitoring feed, nothing in this policy ordinance prohibits SFPD from deferring to authorized use No. 2 or No. 3 of this section.
2. Requesting, obtaining, and reviewing historical video footage for purposes of gathering evidence relevant to a specific criminal investigation.

Surveillance Oversight Review Dates
PSAB Review: March 25, 2022 & March 31, 2022
COIT Review: April 7, 2022 & April 21, 2022
Board of Supervisors Approval: September 27, 2022

3. Requesting, obtaining, and reviewing historical video footage for purposes of gathering evidence relevant to an internal investigation regarding officer misconduct.

Prohibitions:

- Surveillance camera footage will not on its own identify an individual, confirm racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, or information concerning an individual person's sex life or sexual orientation.

- SFPD is prohibited from using biometric identification or facial recognition technology in connection with non-City entity surveillance cameras or associated data.

- SFPD is prohibited from live monitoring inside residential dwellings where homeowners/renters have a reasonable expectation of privacy unless one the following conditions exist: Exigency per SF Admin Code 19b.7; a homeowner/renter/individual with legal authority to do so provides consent; or a warrant is issued. If the conditions exist, SFPD shall adhere to the authorized use and reporting provisions relating to temporary live monitoring.

- SFPD is prohibited from monitoring any certain groups or individuals based, in whole or in part, on race, gender, religion, or sexual orientation. Race, color, ethnicity, or national origin may not be used as a motivating factor for initiating police enforcement action.

- SFPD is prohibited from accessing, requesting, or monitoring any surveillance camera live feed during First Amendment activities unless there are exigent circumstances or for placement of police personnel due to crowd sizes or other issues creating imminent public safety hazards. SFPD members are required to comply with SFPD Department General Order (DGO) 8.03 Crowd Control, DGO 8.10 Guidelines for First Amendment Activities and its annual audit requirements, and the SFPD Event Manual to ensure the safety of those attending planned or spontaneous events.

- SFPD members shall not acquire or use surveillance camera footage in cooperation with or assisting U.S. Immigration and Customs Enforcement or U.S. Customs and Border Protection in any investigation, detention, or arrest procedures, public or clandestine, where in any such instance the purpose is the enforcement of federal immigration laws. SFPD complies with SF Administrative Code Chapters 12H "Immigration Status" and 12I "Civil Immigration Detainers" and SFPD General Order (DGO) 5.15 "Enforcement of Immigration Laws".

- SFPD is prohibited from seeking to obtain surveillance footage for purposes of enforcing prohibitions on reproductive care or interstate travel for reproductive care. Except as required by law, SFPD shall not share surveillance footage with any law enforcement agency for purposes of enforcing prohibitions on reproductive care or interstate travel for reproductive care. Unless legally required, SFPD will not share footage with non-California law enforcement agencies**.**

Description of Technology
This is a product description of the technology:

Categories: Residential, Small Business, Commercial Security Camera Systems.

Subcategories: Indoor, Outdoor

Typical Camera Types [Not vendor specific & not an exhaustive list]:

- Box Camera: A Box Style camera is a standalone camera. The name is derived from the shape of the camera.
- Dome Camera: A dome camera is a combination of camera, lens, and ceiling mount packaged in a discreet dome shape.
- PTZ Camera: A PTZ camera contains mechanical controls that allow the operator to remotely pan, tilt, and zoom the camera.
- Bullet Camera: A bullet camera is a combination of camera, lens, and housing packaged in a bullet-style body.
- IP Camera: An IP camera transmits a digital signal using Internet Protocol over a network
- Wireless IP Camera: Wireless IP security cameras offers ease of installation and eliminates the cost of network cabling when adding this camera to your video surveillance system.
- Day/Night Camera: A Day/night camera is a camera used indoor and outdoor for environments with low light conditions.
- Wide Dynamic Cameras: Wide Dynamic Cameras can balance light-levels on a pixel-by-pixel basis
- Smart/Doorbell Cameras: cameras typically affixed to a or inside of a residence.

IMPACT ASSESSMENT

The impact assessment addresses the conditions for surveillance technology approval, as outlined by the Standards of Approval in San Francisco Administrative Code, Section 19B:

1. The benefits of the surveillance technology outweigh the costs.
2. The Department's Policy safeguards civil liberties and civil rights.
3. The uses and deployments of the surveillance technology are not based upon discriminatory or viewpoint-based factors and do not have a disparate impact on any community or Protected Class.

The Department's use of the surveillance technology is intended to support and benefit the residents of San Francisco while minimizing and mitigating all costs and potential civil rights and liberties impacts of residents.

A. Benefits

The Department's use of the surveillance technology has the following benefits for the residents of the City and County of San Francisco:

	Benefit	Description
☐	Education	
☐	Community Development	
☐	Health	Protect safety of residents, visitors of San Francisco.
☐	Environment	
☐	Criminal Justice	Review video footage after a crime has occurred; officer and community safety during live monitoring; corroborate witness statements; investigative tool; provide objective video evidence to the DA's office for prosecutorial functions or provide to the public upon request through a formal process, order, or subpoena.
☐	Jobs	
☐	Housing	
X	Other	Additional benefits include effective public-safety interventions to curb crime and improve livability and wellbeing of communities.

B. Civil Rights Impacts and Safeguards

The Department has considered the potential impacts and has identified the technical, administrative, and physical protections as mitigating measures:

Right to Privacy- Individuals retain certain rights to privacy when they leave private spaces and generally people do not expect or desire for law enforcement to monitor, record, without cause or as a consequence of participating in contemporary society. While SFPD may ask public organizations, private businesses, and individuals to share video that might help in the investigation of a crime, SFPD does not own or operate non-city entity surveillance cameras and as such does not determine placement of these cameras, what is captured or what is recorded. If invertedly provided, SFPD will not rely on facial recognition or biometric software to identify specific persons captured on video that has facial recognition as a component.

Patrons of businesses in this city generally accept that they are being recorded when in or around retail shops and many residents widely accept that they are being recorded by doorbell cameras in residential neighborhoods. While SFPD affirms that individuals have the Right to Privacy and freedom of expression, in conformance with and consistent with federal, state, and local law, officers will only request historical footage that relates to a specific criminal or internal investigation.

The Department will also limit temporary live footage to specific circumstances as not to impede on members of the public and their general desire to not be monitored. Requests for live footage access will be restricted to active criminal or internal investigations and significant events with public safety concerns. Examples include but are not limited to:
Aircraft accident
Homicide suspect location
Active narcotic sales
Missing/abducted person

Riots/Looting/Arson

Requests for live footage must first receive Captain approval.

Another loss of the right to privacy concern relates to individuals or businesses who provide camera footage to the police but do not want to be identified for fear of retaliation from perpetrators. PII of individuals who provided video footage to SFPD for investigative purposes will not be provided to the public unless authorized pursuant to a court order or as authorized by state or federal law. If an individual's surveillance camera footage is included in videos displayed during Officer Involved Shooting (OIS) townhalls, SFPD will notify the individual beforehand.

Loss of Liberty- Surveillance footage could lead to false conclusions or misidentifications of a person as a perpetrator. To mitigate this, SFPD does not rely solely on camera footage to conclude a case or bring charges against a suspect. SFPD must do additional investigative work to understand the full context of a criminal incident by consulting with witnesses and residents, review booking photos, consulting with ALPR reads and reviewing any evidence left at the scene. Footage is a vital tool but cannot replace investigative processes necessary to solve a case.

Warrantless Searches- Surveillance cameras with views covering areas where people may have a reasonable expectation of privacy can pose a civil liberty concern. Absent a search warrant, or recognized warrant exception (e.g., valid consent, exigent circumstances), SFPD members will not monitor live footage or request historical footage from spaces where individuals have a reasonable expectation of privacy.

Equal Protection of the Law- SFPD may request video footage relating to specific criminal activity or incidents and will not request to monitor individuals or groups based on their race, gender, religion, or sexual orientation. SFPD has included specific prohibitions to this policy to ensure parameters around requests for historical footage and temporary live monitoring do not infringe on the rights of individuals.

C. Fiscal Analysis of Costs and Benefits

The Department's use of the surveillance technology yields the following business and operations benefits:

	Benefit	Description
X	Financial Savings	Non-city entity Security Camera Systems do not require Department operational funding and reduce reliance on first-hand accounts by patrol officers or fixed posts, making deployments more effective and efficient.
X	Time Savings	Investigating crimes by gathering evidence can be extremely time consuming. As there are thousands of cameras throughout the city, officers can quickly identify cameras in vicinity of an incident that could potentially aid in the apprehension of the suspect(s) responsible for the crime under investigation. This saves officers valuable time which they

		would otherwise spend going door-to-door attempting to locate witnesses and gathering witness statements.
X	Staff Safety	Non-city entity Security Camera Systems provide situational awareness and increase officer safety, particularly during live video reviews. Officers can approach an active crime scene more safely and determine a strategy to keep members of the public safe during live monitoring of cameras. Officers can determine the precise location and time of the event and whether high-capacity weapons are being used.
X	Data Quality	Non-city entity camera footage provides an objective account of an incident and can corroborate or dispute witness statements, determine whether involved persons may have left the scene of the incident before first responder arrived.
X	Other	Other benefits include accountability. SFPD Internal Affairs may request historical camera footage from a non-city entity during an officer misconduct investigation

The total fiscal cost, including initial purchase, personnel and other ongoing costs is

FTE (new & existing)			N/A
Classification			N/A
	Annual Cost	***Years***	***One-Time Cost***
Total Salary & Fringe	*$0*	-	-
Software	$0	-	-
Hardware/Equipment	$0	-	-
Professional Services	*$0*		-
Training	$0	-	-
Other	$0	-	-
Total Cost [Auto-calculate]			
2.1 Please disclose any current or potential sources of funding (e.g., potential sources = prospective grant recipients, etc.). SIR, ASR			

No cost to the Department

COMPARISON TO OTHER JURISDICTIONS:

Surveillance Camera Registries: The following police departments manage local registry programs for private security cameras owned by individuals and businesses. The Police Departments do not have access to registered cameras but may request a copy of any video captured by registered cameras to assist in the investigation of a crime. Some jurisdictions offer signage noting that surveillance systems are registered with the

police department. The registry also enables officers to quickly identify cameras that could potentially aid in the apprehension of the suspect(s) responsible for the crime under investigation. This saves officers valuable time which they would otherwise spend going door-to-door attempting to locate security footage that could help identify a suspect. Registration is completely voluntary and free of charge. Registrant's personal information is kept confidential by the Police Department and will only be accessed by law enforcement personnel who are investigating. Registration may be withdrawn at any time.

- Albany Police Department: https://www.albanyca.org/Home/Components/News/News/9888/
- Berkely Police Department https://www.cityofberkeley.info/police/security-camera-registry/
- Dublin Police Department: https://dublin.ca.gov/1815/Security-Camera-Registration
- Hayward Police Department: https://www.hayward-ca.gov/police-department/programs/hayward-eyes
- Oakland Police Department: https://www.oaklandca.gov/services/register-your-security-camera
- Union City Police Department: https://cityprotect.com/camera-registration#/agencies

SFPD does not manage a camera registry. The San Francisco District Attorney's office has information about a camera registry managed by the DA's office, found here: https://sfdistrictattorney.org/resources/register-your-camera/

Ring/Neighbors Partnerships: Police Departments can sign an agreement with Amazon's home surveillance equipment company, Ring, to gain special access to the company's Neighbors app. Here is a partial list of Police Department's in surrounding cities/counties who have these agreements in place.

- Alameda County Sheriff's Office
- Daly City Police Department
- Dublin Police Department
- Elk Grove Police Department
- Hayward Police Department

SFPD does not have a Ring/Doorbell Camera Partnership and as such cannot access these cameras without incident expressed consent from homeowner/renter/individual with legal authority at the time of each request.

Public Surveillance Systems: These are a network of several cameras linked to a centralized monitor or location equipped to record the images that were captured. These systems may also be referred to as Police Observation Devises (POD) or Portable Overt Digital Surveillance Systems (PODSS). The benefits include public policy processes, public posting of locations of cameras and law enforcement having direct access to camera footage without third party.

- Sacramento Police Departments: Police Observation Devices (PODs) https://apps.sacpd.org/Releases/liveview.aspx?reference=20161027-141

SFPD does not have or manage PODS, PODSS or any other network of cameras. This is an example of how other law enforcement agencies manage surveillance cameras.

APPENDIX A: Mapped Crime Statistics

The general location(s) cameras be deployed and crime statistics for any location(s):

The SFPD does not have decision making authority for placement of non-city entity surveillance cameras and as such is unable to post general locations of cameras.

The SFPD submits requests through any non-city entity or individual throughout the city and county of San Francisco.

Please see below crime statistics for San Francisco:

https://www.sanfranciscopolice.org/stay-safe/crime-data/crime-dashboard

Surveillance Technology Policy

Non-City Entity Surveillance Cameras
San Francisco Police Department (SFPD)

The City and County of San Francisco values the 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 "Non-City Entity" Security Camera System by Department as well as any associated data to which Department is privy, 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 non-city entity Security Camera System will be used to support department operations.

This Policy applies to all department personnel that use, plan to use, or plan to secure non-city entity security camera systems or data, 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.

Absent a subpoena or search warrant, SFPD access to all systems noted in this Policy will be obtained through the express consent of the individual or entity managing the surveillance system at the time of request. SFPD does not and shall not manage a surveillance camera registry, have public observation devices, or have a Ring/Neighbors or similar partnership agreements.

POLICY STATEMENT

This policy applies to security camera data sharing between SFPD and the following entities:

- Any non-City entity or individual, through consent, subpoena, search warrant or other court order, who provides SFPD with data access or information acquired through the entity's or individual's use of surveillance cameras or surveillance camera networks owned, leased, managed and/or operated by the entity or individual.

Surveillance Oversight Review Dates
COIT Review: April 21, 2022
Board of Supervisors Approval: September 27, 2022

This policy excludes any surveillance cameras that meet both of the following conditions:

- Paid for through a city grant
- Owned by a non-City entity that is under a contractual agreement or memorandum of understanding with the City requiring them to share live feed or historical footage from the camera

These exclusions shall be governed by a separate use policy compliant with the requirements of 19B.

SFPD is limited to the following authorized use(s) and requirements listed in this Policy only.

Authorized Use(s):

1. Temporary live monitoring (a) during an exigent circumstance as defined by San Francisco Administrative Code, Section 19B, (b) during Significant Events with public safety concerns only for placement of police personnel due to crowd sizes or other issues creating imminent public safety hazards, or (c) in the course of a specific criminal investigation if an SFPD Captain or member in rank above Captain confirms in writing that the department has credible information of criminal activity and live monitoring is being requested in furtherance of that criminal investigation. Temporary live monitoring will cease, and the connection will be severed within 24 hours after the non-city entity has provided access to SFPD. SFPD shall not record or duplicate the live monitoring feed using any electronic device, including body worn cameras or cell phones. If SFPD observes misdemeanor or felony violations on the live monitoring feed, nothing in this policy ordinance prohibits SFPD from deferring to authorized use No. 2 or No. 3 of this section.

2. Requesting, obtaining, and reviewing historical video footage for purposes of gathering evidence relevant to a specific criminal investigation.

3. Requesting, obtaining, and reviewing historical video footage for purposes of gathering evidence relevant to an internal investigation regarding officer misconduct.

Prohibitions:

- Surveillance camera footage will not on its own identify an individual, confirm racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, or information concerning an individual person's sex life or sexual orientation.

- SFPD is prohibited from using biometric identification or facial recognition technology in connection with non-City entity surveillance cameras or associated data.

- SFPD is prohibited from live monitoring inside residential dwellings where homeowners/renters have a reasonable expectation of privacy unless one the following

conditions exist: Exigency per SF Admin Code 19b.7; a homeowner/renter/individual with legal authority to do so provides consent; or a warrant is issued. If the conditions exist, SFPD shall adhere to the authorized use and reporting provisions relating to temporary live monitoring.

- SFPD is prohibited from monitoring any certain groups or individuals based, in whole or in part, on race, gender, religion, or sexual orientation. Race, color, ethnicity, or national origin may not be used as a motivating factor for initiating police enforcement action.

- SFPD is prohibited from accessing, requesting, or monitoring any surveillance camera live feed during First Amendment activities unless there are exigent circumstances or for placement of police personnel due to crowd sizes or other issues creating imminent public safety hazards. SFPD members are required to comply with SFPD Department General Order (DGO) 8.03 Crowd Control, DGO 8.10 Guidelines for First Amendment Activities and its annual audit requirements, and the SFPD Event Manual to ensure the safety of those attending planned or spontaneous events.

- SFPD members shall not acquire or use surveillance camera footage in cooperation with or assisting U.S. Immigration and Customs Enforcement or U.S. Customs and Border Protection in any investigation, detention, or arrest procedures, public or clandestine, where in any such instance the purpose is the enforcement of federal immigration laws. SFPD complies with SF Administrative Code Chapters 12H "Immigration Status" and 12I "Civil Immigration Detainers" and SFPD General Order (DGO) 5.15 "Enforcement of Immigration Laws".

- SFPD is prohibited from seeking to obtain surveillance footage for purposes of enforcing prohibitions on reproductive care or interstate travel for reproductive care. Except as required by law, SFPD shall not share surveillance footage with any law enforcement agency for purposes of enforcing prohibitions on reproductive care or interstate travel for reproductive care. Unless legally required, SFPD will not share footage with non-California law enforcement agencies.

BUSINESS JUSTIFICATION

[A description of the product, including vendor and general location of technology]

Categories: Residential, Small Business, Commercial Security Camera Systems.

Subcategories: Indoor, Outdoor

Typical Camera Types [Not vendor specific & not an exhaustive list]:

- Box Camera: A Box Style camera is a standalone camera. The name is derived from the shape of the camera.

- Dome Camera: A dome camera is a combination of camera, lens, and ceiling mount packaged in a discreet dome shape.
- PTZ Camera: A PTZ camera contains mechanical controls that allow the operator to remotely pan, tilt, and zoom the camera.
- Bullet Camera: A bullet camera is a combination of camera, lens, and housing packaged in a bullet-style body.
- IP Camera: An IP camera transmits a digital signal using Internet Protocol over a network
- Wireless IP Camera: Wireless IP security cameras offers ease of installation and eliminates the cost of network cabling when adding this camera to your video surveillance system.
- Day/Night Camera: A Day/night camera is a camera used indoor and outdoor for environments with low light conditions.
- Wide Dynamic Cameras: Wide Dynamic Cameras can balance light-levels on a pixel-by-pixel basis
- Smart/Doorbell Cameras: cameras typically affixed to a or inside of a residence.

Security Cameras supports the Department's mission and provides important operational value in the following ways:

X	Health	Protect safety of visitors and residents of San Francisco.
☐	Environment	
X	Criminal Justice	Review video footage after a crime has occurred; officer and community safety during live monitoring; corroborate witness statements; investigative tool; provide objective video evidence to the DA's office for prosecutorial functions or provide to the public upon request through a formal process, order, or subpoena.
☐	Housing	
X	Other	Effective public-safety interventions to curb crime and improve livability and wellbeing of communities.

In addition, the following benefits are obtained:

Benefit		**Description**
X	Financial Savings	Non-city entity Security Camera Systems do not require Department operational funding and reduce reliance on first-hand accounts by patrol officers or fixed posts, making deployments more effective and efficient.
X	Time Savings	Non-city entity Security Camera Systems may run 24/7, thus decreasing or eliminating building or patrol officer supervision. Reviewing Third

		Party data may also decrease demands on investigative units corroborating first-hand accounts of criminal activity.
X	Staff Safety	Non-city entity Security Camera Systems provide situational awareness and increase officer safety, particularly during live video reviews.
X	Service Levels	Non-city entity Security cameras will enhance effectiveness of incident response, criminal investigations, and result in improved level of service. Criminal activity captured through video can help verify the act of the crime and corroborate whether a suspect has been correctly identified and corroborate witness statements to assist with conviction rates.

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.

Data Collection: Department shall only collect data required to execute the authorized use case. All surveillance technology data shared with Department by Non-city entity, including PII, shall be classified according to the City's Data Classification Standard.

The surveillance technology collects some or all the following data types:

Data Type(s)	*Format(s)*	*Classification*
Video and Images	MP4, AVI, MPEG	Level 4
Date and Time	MP4 or other format	Level 4
Geolocation data	TXT, CSV, DOCX	Level 4

Notification: Departments shall rely on the non-city entity vendor to manage public notifications relating to surveillance technology operation at the site of operations through signage in readily viewable public areas in accordance to Section 19.5 of the Administrative Code.

Access:

Prior to accessing or using data, authorized individuals within the Department receive training in system access and operation, and instruction regarding authorized and prohibited uses.

Access to live views and recorded footage is restricted to members who have receive authorization from their officer and charge and have reviewed this policy, connected written directives, and acknowledged on SFPD Power DMS.

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 with Level 4 classification:

- Non-sworn members, at the direction of Officer in Charge. The Officer in Charge (OIC) is any member working in a supervisorial capacity over a unit, group, or team. The OIC is not rank specific.
- 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

Live monitoring requests shall be limited to the following roles and job titles upon authorization of a Captain (Q80-Q82) rank:

- Q2-Q4, Police Officer
- Q35-Q37, Assistant Inspector
- Q0380- Q0382, Inspector
- Q50-Q-52, Sergeant
- Q60-Q62, Lieutenant
- Q80-Q82, Captain

The approving Captain shall use good faith belief or objectively reasonable reliance on information confirming exigency or misdemeanor or felony violations for the basis of approving or denying live monitoring requests. Upon Board of Supervisors approval of this policy ordinance, the Department will determine a mechanism for the ranks Q2 – Q62 to receive Captain rank approval. The Department's Written Directives Unit shall update the "Permission to Search -Form 468" that may be provided to the non-city entity or individual to substantiate the

consent for SFPD live monitoring request. The non-city entity or individual retains the right to refuse the request.

Live monitoring viewing rights include the following roles and job titles:

- Q2-Q4, Police Officer
- Q50-Q-52, Sergeant
- Q35-Q37, Assistant Inspector
- Q0380- Q0382, Inspector
- Q60-Q62, Lieutenant
- Q80-Q82, Captain
- 0488-0490, Commander
- 0400-0402, Deputy Chief
- 0395, Assistant Chief
- 0390, Chief of Police

B. Members of the public

Members of the public may 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.

Data Security:

Department shall secure any PII received from non-city entity or individuals (or shared by non-city entity) 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.

Departments shall, at minimum, apply the following safeguards to protect surveillance technology information received from non-city entity from unauthorized access and control, including misuse:

- Storage: Any storage of a non-city entity's camera footage must reside in a SFPD specified repository that meets the City's cyber security requirements as well as Department of Justice California Law Enforcement Telecommunications Systems (CLETS) and Criminal Justice Information Services (CJIS) requirements. Video Retrieval Officers may initially store footage provided by a business or individual on a USB or CD. Upon the execution of a city contract with a digital evidence management system vendor, members shall transfer the footage to this system that requires an agency domain and log in. The evidence management system will have a platform that is auditable and can track the source of upload and number of

views. This platform will not be accessible to members of the public or anyone without an approved log-in. This platform will meet the requirements of the Office of Contract Administration ("OCA") who promulgates rules and regulations pursuant to Chapter 21 of the San Francisco Administrative Code. The SFPD Contracting Department shall comply with the requirements of Chapter 21 and cooperate to the fullest extent with OCA in the Acquisition of Commodities and Services.

- Audits: SFPD members shall note in the chronological record of investigation ("chron") time/date surveillance footage was requested, approved, or denied by non-city entity, and in the case of live monitoring requests, SFPD members shall note in an incident report and/or the chron the captain's approval, date/time of access, duration of access and outcome of access. Upon implementation of the internal records management system, SFPD members shall note this information in this system. This data will serve as the Department's audit log, which is electronically accessible for on-demand audits
- Reporting: SFPD shall submit an annual surveillance report as outlined in SF Administrative Code Sections 19B.1 and 19B.6. Upon adoption of the non-city entity surveillance camera policy ordinance, SFPD shall submit a quarterly report tracking live monitoring requests to the Police Commission, copying the Clerk of the Board of Supervisors.

  The quarterly report shall identify whether each request was granted or denied by the Captain or member in rank above Captain; the justification for granting the request if it was granted, including the reason(s) why the Captain or member in rank above Captain found the information credible; whether the request was granted by the non-City entity; the total costs to the Department, including any staff time and other costs, associated with the request and usage; felony and misdemeanor crime statistics for the census tract surrounding the camera used for live monitoring for the month prior to the live monitoring as well as the month following live monitoring; whether the images were used to bring criminal charges; the types of charges brought; and the results of the charges.

  The reporting requirement shall commence 60 days after the first full quarter following adoption and every quarter thereafter. After the first two years of quarterly reports to the Commission, the Department will thereafter submit a bi-annual report.

  The Department understands that the Board of Supervisors intends to direct the Budget and Legislative Analyst to evaluate the efficacy of the Policy based on a review of the SFPD's quarterly reports and any other information relevant to making such an evaluation.

Data Sharing:	The Non-city entity is the custodian of its Surveillance Technology data. The non-city entity may share such data with the Department or other entities solely at its discretion. Data is shared by non-city entity with the Department on the following schedule: X Upon Request X As needed *A. Internal (City Entity) Data Sharing* Department shares the following data with the recipients: -District Attorney's Office for use as evidence to aid in prosecution, in accordance with laws governing evidence. -Public Defender's Office or criminal defense attorney via the District Attorney's Office in accordance with California and federal discovery laws. -The Department of Police Accountability per Section 4.136(j) of the Sn Francisco Charter -Other City agencies impacted by a criminal incident captured by the surveillance camera footage. Data sharing occurs at the following frequency: As needed *B. External (Non-City Entity) Data Sharing* Department shares the following data with the recipients: -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; Media may receive redacted footage relating to Officer Involved Shooting Townhall meetings or other public safety issues requiring the public's awareness or assistance. To ensure that entities receiving data collected by the surveillance technology comply with the Surveillance Technology Policy, Department shall: Comply with all applicable laws, rules, and regulations, including but not limited to, to the extent applicable, the California Values Act (Government Code Section 7284 et seq.) which prohibits state and local law enforcement agencies from engaging certain acts related to immigration enforcement. If determined by Department's general counsel or SFPD's legal division, surveillance camera footage can be disclosed in response to a public

information request. Based on legal advice, the department will redact PII as it may be considered investigative/evidentiary material. The Department may use its discretion when releasing investigative/evidentiary material per SFPD DGO 3.16.

Data sharing occurs at the following frequency: As needed

Data Retention:

Department may store and retain PII data shared by the non-city entity only as long as necessary to accomplish a lawful and authorized purpose. Records shall be purged according to the current San Francisco Police Department Records Retention and Destruction Schedule which calls for destruction of intelligence files two years from the last date of entry with the following exceptions:

a) Information may be maintained if it is part of an ongoing investigation or prosecution.

b) All investigative files shall be maintained according to CA Penal Code, Evidence Code, department retention guidelines and according to state and federal law.

c) Records showing violation of these guidelines shall not be destroyed or recollected for the purpose of avoiding disclosure.

The Department's data retention period is as follows:

- Security Camera data shared with Department by a non-City entity will be stored only for the period necessary for investigation, prosecution, or litigation following an incident. All historical footage is associated with a specific criminal investigation and is tagged as evidence. This data shall be retained as required by State evidence retention laws. Camera footage associated with an officer misconduct or Officer Involved Shooting (OIS) investigation shall be maintained in perpetuity.
- Any historical video not tagged into evidence and subject to the use requirements of Chapter 19B shall be deleted within 90 days.

Data may be stored in the following location:

☒ Local storage (e.g., local server, storage area network (SAN), network-attached storage (NAS), backup tapes, etc.)

☐ Department of Technology Data Center

☐Software as a Service Product

☒Cloud Storage Provider

Data Disposal:	The Police Department does not have a contract or legal agreement with a non-city entity governing non-city entity data use, including but not limited to non-city entity party data use, sharing, signage, retention, and/or disposal. Upon completion of the data retention period, Department shall dispose of data in the following manner: - Delete from local storage - Delete from USB thumb drive or disk if not associated with investigative file
Training:	To reduce the possibility that surveillance technology or its associated data will be misused or used contrary to its authorized use, all individuals requiring access on behalf of Department must receive training on data security policies and procedures. Other trainings may include: California Peace Officer Standards and Training (POST): - LD 15 Laws of Arrest - LD 16 Search and Seizure - LD 17 Presentation of Evidence - LD 23 Crimes in Progress - LD 26 Critical Incidents - LD 30 Crime Scenes, Evidence, and Forensics - LD 42 Cultural Diversity/Discrimination - LD 43 Terrorism Awareness - PC 872 (b) Hearsay Testimony SF City & County Employee Portal - Cybersecurity Training SFPD Training Options - Critical Mindset Coordinated Response Training - DGO 8.10 Guidelines for First Amendment Activities - Video Retrieval Training - Crowd Control Training

COMPLIANCE

Department shall oversee and enforce compliance with this Policy according to the respective memorandum of understanding of employees and their respective labor union agreement.

Allegations of 19B Violations:
Members of the public may submit written notice of an alleged violation of Chapter 19B to SFPDChief@sfgov.org.

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. The Department will comply with allegation and misconduct processes as set forth by the city Charter

Sanctions for violations of this Policy include the following:
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 (PII):	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.
Significant Events:	These are large or high-profile events in the city where SFPD Special Events Unit and Traffic Company manage street closures, barricades, and crowd management; Special Investigations Division (SID) manages dignitary escorts; or Homeland Security Unit (HSU)/Special Ops is assigned to thwart potential terrorist or criminal attacks. These units may require and request additional deployment efforts during these high-profile events based on activity detected during live monitoring which allows for situational awareness and the ability to coordinate resources based on information obtained.

Exigent Circumstances:	See Admin Code Sec. 19B.1

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. DPA manages, acknowledges, and responds to complaints from members of the public.

Concerns and Inquiries: Department shall acknowledge and respond to concerns in a timely manner. To do so, 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.

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

Sunset Provision: Unless reauthorized by ordinance, this policy shall expire fifteen months after the effective date of Ordinance File No. 220606.
Effective Date: Ordinance File No. 220606 becomes effective 30 days after enactment. Enactment occurs when the mayor signs the ordinance, the mayor returns the ordinance unsigned or does not sign the ordinance withing ten days of receiving it, or the Board of Supervisors overrides the mayor's veto of the ordinance.