File No. 210559 **Committee Item No.** 3
Board Item No. 17

COMMITTEE/BOARD OF SUPERVISORS

AGENDA PACKET CONTENTS LIST

Committee: Rules Committee **Date** July 19, 2021

Board of Supervisors Meeting **Date** July 27, 2021

Cmte Board

Cmte	Board	
☐	☐	**Motion**
☐	☐	**Resolution**
x	X	**Ordinance**
x	X	**Legislative Digest**
☐	☐	**Budget and Legislative Analyst Report**
☐	☐	**Youth Commission Report**
☐	☐	**Introduction Form**
x	X	**Department/Agency Cover Letter and/or Report**
☐	☐	**Memorandum of Understanding (MOU)**
☐	☐	**Grant Information Form**
☐	☐	**Grant Budget**
☐	☐	**Subcontract Budget**
☐	☐	**Contract/Agreement**
☐	☐	**Form 126 - Ethics Commission**
☐	☐	**Award Letter**
☐	☐	**Application**
☐	☐	**Form 700**
☐	☐	**Vacancy Notice**
☐	☐	**Information Sheet**
☐	☐	**Public Correspondence**

OTHER **(Use back side if additional space is needed)**

xx ☐	X	Surveillance Impact Reports (various departments)
xx ☐	X	Surveillance Technology Policy (various departments)
☐	☐	
☐	☐	
☐	☐	
☐	☐	
☐	☐	
☐	☐	
☐	☐	

Completed by: Victor Young **Date** July 15, 2021
Completed by: _____ **Date** _____

BOARD of SUPERVISORS

City Hall
1 Dr. Carlton B. Goodlett Place, Room 244
San Francisco 94102-4689
Tel. No. 554-5184
Fax No. 554-5163
TDD/TTY No. 554-5227

M E M O R A N D U M

RULES COMMITTEE

SAN FRANCISCO BOARD OF SUPERVISORS

TO: Supervisor Aaron Peskin, Chair
Rules Committee

FROM: Victor Young, Assistant Clerk

DATE: July 19, 2021

SUBJECT: **COMMITTEE REPORT, BOARD MEETING**
Tuesday, July 20, 2021

The following file should be presented as a **COMMITTEE REPORT** at the Board Meeting on Tuesday, July 20, 2021. This item was acted upon at the Rules Committee Meeting on Monday, July 19, 2021, at 10:00 a.m., by the votes indicated.

Item No. 73 File No. 210559

[Administrative Code - Approval of Surveillance Technology Policies for Multiple City Departments]

Ordinance approving Surveillance Technology Policies governing the use of 1) Audio Recorders (ShotSpotter) by the Police Department, 2) Automatic License Plate Readers by the Airport, Public Works, Recreation and Park Department, and Police Department, 3) Drones by the Fire Department, Port, Public Works, Public Utilities Commission, Recreation and Park Department, and Department of Technology, 4) Security Cameras by the Airport, Arts Commission, Asian Art Museum, Department of Child Support Services, City Administrator, Department of Technology, Department of Emergency Management, Fire Department, Department of Homelessness and Supportive Housing, Department of Human Resources, Human Services Agency, Library, Municipal Transportation Agency, Port, Public Utilities Commission, Department of Public Health, Recreation and Park Department, Rent Board, and War Memorial, and 5) Radio Frequency Identification by the Library; making required findings in support of said approvals; and amending the Administrative Code to require departments to post each Board-approved Surveillance Technology Policy on the department website.

RECOMMENDED AS AMENDED AS A COMMITTEE REPORT

Vote: Supervisor Rafael Mandelman - Aye
Supervisor Connie Chan - Aye
Supervisor Aaron Peskin - Aye

c: Board of Supervisors
Angela Calvillo, Clerk of the Board
Alisa Somera, Legislative Deputy Director
Anne Pearson, Deputy City Attorney

AMENDED IN COMMITTEE
7/19/21

FILE NO. 210559 ORDINANCE NO.

[Administrative Code - Approval of Surveillance Technology Policies for Multiple City Departments]

Ordinance approving Surveillance Technology Policies governing the use of 1) Audio Recorders (ShotSpotter) by the Police Department, 2) Automatic License Plate Readers by the Airport, Department of Public Works, Recreation and Parks Department, and Police Department, 3) Drones by the Fire Department, Port, Department of Public Works, Public Utilities Commission, Recreation and Parks Department, and Department of Technology, 4) Security Cameras by the Airport, Arts Commission, Asian Art Museum, Department of Child Support Services, City Administrator, Department of Technology, Department of Emergency Management, Fire Department, Department of Homelessness and Supportive Housing, Department of Human Resources, Human Services Agency, Library, Municipal Transportation Agency, Port, Public Utilities Commission, Department of Public Health, Recreation and Parks Department, Rent Board, and War Memorial, and 5) Radio Frequency Identification by the Library; making required findings in support of said approvals; and amending the Administrative Code to require departments to post each Board-approved Surveillance Technology Policy on the department website.

NOTE: **Unchanged Code text and uncodified text** are in plain Arial font.
Additions to Codes are in *single-underline italics Times New Roman font*.
Deletions to Codes are in ~~*strikethrough italics Times New Roman font*~~.
Board amendment additions are in double-underlined Arial font.
Board amendment deletions are in ~~strikethrough Arial font~~.
Asterisks (* * * *) indicate the omission of unchanged Code subsections or parts of tables.

Be it ordained by the People of the City and County of San Francisco:

Section 1. Background.

(a) Administrative Code Chapter 19B ("Chapter 19B"), established in 2019 with the enactment of Ordinance Nos. 103-19 and 107-19, requires that City Departments obtain Board of Supervisors approval of a Surveillance Technology Policy to use existing Surveillance Technology; but Chapter 19B permits Departments that already were in the possession of or using Surveillance Technology to continue to possess and use the Surveillance Technology and the sharing of data from the Surveillance Technology, until such time as the Board approves a Surveillance Technology Policy for such Departments.

(b) Beginning in August 2019, and continuing over the following several months, Departments submitted to the Committee on Information Technology ("COIT") inventories of their existing Surveillance Technology and also, for existing Surveillance Technology, submitted a Surveillance Impact Report.

(c) Following receipt of the inventories and Surveillance Impact Reports, COIT and its subcommittee, the Privacy and Surveillance Advisory Board ("PSAB"), conducted multiple public hearings at which COIT and PSAB considered both the inventories and Surveillance Impact Reports for existing Surveillance Technology. Following those hearings, COIT developed Surveillance Technology Policies for multiple Departments, covering five categories of Surveillance Technology:

(1) Audio Recorder (ShotSpotter)

(2) Automatic License Plate Readers (ALPR)

(3) Drones (Unmanned Aircraft Systems)

(4) Security Cameras

(5) Radio Frequency Identification (RFID)

(e) COIT, together with PSAB, developed Department-specific Surveillance Technology Policies as well as a consolidated Surveillance Technology Policy for use by multiple Departments, in those five categories. COIT has recommended that the Board of

Supervisors approve the Surveillance Technology Policies delineated in Sections 2 through 6 of this ordinance. This ordinance approves those proposed Surveillance Technology Policies, each of which is available in Board File No. 210559 and is incorporated herein by reference.

(f) Terms used in this ordinance have the meaning set forth in Chapter 19B.

Section 2. Audio Recorder (ShotSpotter): Police Department.

(a) Current Status. The Police Department ("SFPD") currently possesses and uses Audio Recorder ("ShotSpotter").

(b) Purpose. SFPD uses ShotSpotter to record gunshot sounds in order to locate the origin of the gunshots and also to find shell casings evidence. [

(c) Surveillance Impact Report. SFPD submitted to COIT a Surveillance Impact Report for ShotSpotter. A copy of the SFPD Surveillance Impact Report for ShotSpotter is in Board File No. 210559, and is incorporated herein by reference.

(d) Public Hearings. Between August 28, 2020 and January 21, 2021, inclusive, COIT and PSAB conducted a total of five public hearings at which they considered the ShotSpotter Surveillance Impact Report and developed a Surveillance Technology Policy for ShotSpotter. A copy of the Surveillance Technology Policy for SFPD's use of ShotSpotter ("ShotSpotter Policy") is in Board File No. 210559, and is incorporated herein by reference.

(e) COIT Recommendation. On January 21, 2021, COIT voted to recommend the ShotSpotter Policy to the Board of Supervisors for approval.

(f) Findings. The Board of Supervisors hereby finds that ShotSpotter's benefits outweigh its costs and risks, that the ShotSpotter Policy will safeguard civil liberties and civil rights, and that the uses and deployments of ShotSpotter, as set forth in the ShotSpotter Policy, will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or Protected Class.

(g) Approval of Policy. The Board of Supervisors hereby approves the ShotSpotter Policy under which SFPD may continue to possess and use ShotSpotter.

Section 3. Automatic License Plate Readers ("ALPR"): Four Departments (Airport, Department of Public Works, Police Department, Recreation and Parks Department).

(a) Current Status. The following Departments currently possess and use Automatic License Plate Readers:

Airport ("SFO")

Department of Public Works ("DPW")

Recreation and Parks Department ("RPD")

SFPD

(b) SFO.

(1) Purpose. SFO uses an ALPR known as the Ground Transportation Management System ("GTMS") to (A) track the activity of permitted commercial ground transportation at the San Francisco International Airport; (B) collect trip fees in the event an operator's transponder fails to read; and (C) support SFO and local, state, federal, and regional public safety departments in the identification of vehicles associated with targets of investigations, including locating stolen, wanted, and other vehicles that are the subject of investigation, and locating victims, witnesses, suspects, and others associated with a law enforcement investigation.

(2) Surveillance Impact Report. SFO submitted to COIT a Surveillance Impact Report for GTMS. A copy of the SFO Surveillance Impact Report for GTMS is in Board File No. 210559, and is incorporated herein by reference.

(3) Public Hearings. On September 25, 2020 and February 4, 2021, COIT and PSAB conducted a total of two public hearings at which they considered the Surveillance

Impact Report and developed a Surveillance Technology Policy for GTMS. A copy of the Surveillance Technology Policy for SFO's use of GTMS ("GTMS Policy") is in Board File No. 210559, and is incorporated herein by reference.

(4) COIT Recommendation. On February 4, 2021, COIT voted to recommend the GTMS Policy to the Board of Supervisors for approval.

(5) Findings. The Board of Supervisors hereby finds that GTMS' benefits outweigh its costs and risks, that the GTMS Policy will safeguard civil liberties and civil rights, and that the uses and deployments of GTMS, as set forth in the GTMS Policy, will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or Protected Class.

(6) Approval of Policy. The Board of Supervisors hereby approves the GTMS Policy under which SFO may continue to possess and use GTMS.

(c) DPW.

(1) Purpose. DPW uses an ALPR known as the OnSight Portable License Plate Reader ("OnSight") to discourage illegal dumping onto City streets.

(2) Surveillance Impact Report. DPW submitted to COIT a Surveillance Impact Report for OnSight. A copy of the DPW Surveillance Impact Report for OnSight is in Board File No. 210559, and is incorporated herein by reference.

(3) Public Hearings. Between July 24, 2020 and September 17, 2020, inclusive, COIT and PSAB conducted a total of three public hearings at which they considered the Surveillance Impact Report and developed a Surveillance Technology Policy for OnSight. A copy of the Surveillance Technology Policy for DPW's use of Onsight ("OnSight Policy") is in Board File No. 210559, and is incorporated herein by reference.

(4) COIT Recommendation. On September 17, 2020, COIT voted to recommend the OnSight Policy to the Board of Supervisors for approval.

(5) Findings. The Board of Supervisors hereby finds that OnSight's benefits outweigh its costs and risks, that the OnSight Policy will safeguard civil liberties and civil rights, and that the uses and deployments of OnSight, as set forth in the OnSight Policy, will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or Protected Class.

(6) Approval of Policy. The Board of Supervisors hereby approves the OnSight Policy under which DPW may continue to possess and use Onsight.

(d) RPD.

(1) Purpose. RPD uses an ALPR ("RPD ALPR") to (A) support local, state, federal, and regional public safety departments in the identification of vehicles associated with targets of criminal investigations, including investigations of serial crimes; (B) protect the public and RPD staff at special events from misconduct and/or violent confrontations; and (C) protect critical infrastructure sites from vandalism, theft, and damage.

(2) Surveillance Impact Report. RPD submitted to COIT a Surveillance Impact Report for the RPD ALPR. A copy of the RPD Surveillance Impact Report for the RPD ALPR is in Board File No. 210559, and is incorporated herein by reference.

(3) Public Hearings. Between August 28, 2020 and February 4, 2021, inclusive, COIT and PSAB conducted a total of three public hearings at which they considered the Surveillance Impact Report and developed a Surveillance Technology Policy for the RPD ALPR. A copy of the Surveillance Technology Policy for RPD's use of the RPD ALPR ("RPD ALPR Policy") is in Board File No. 210559, and is incorporated herein by reference.

(4) COIT Recommendation. On February 4, 2021, COIT voted to recommend the RPD ALPR Policy to the Board of Supervisors for approval.

(5) Findings. The Board of Supervisors hereby finds that the RPD ALPR's benefits outweigh its costs and risks, that the RPD ALPR Policy will safeguard civil liberties

and civil rights, and that the uses and deployments of the RPD ALPR, as set forth in the RPD ALPR Policy, will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or Protected Class.

(6) Approval of Policy. The Board of Supervisors hereby approves the RPD ALPR Policy under which RPD may continue to possess and use the RPD ALPR.

(e) SFPD.

(1) Purpose. SFPD uses an ALPR ("SFPD ALPR") to (A) locate stolen, wanted, and/or other vehicles that are the subject of investigation; (B) apprehend wanted persons subject to arrest warrants or who are otherwise lawfully sought by law enforcement; (C) locate victims, witnesses, suspects, missing children, adults, and/or elderly individuals, including in response to Amber Alerts and Silver Alerts and others associated with a law enforcement investigation; (D) assist with criminal investigations initiated by local, state, and regional public safety departments by identifying vehicles associated with targets of criminal investigations; (E) identify potential threats to critical infrastructure sites; and (F) investigate major crimes as authorized by law.

(2) Surveillance Impact Report. SFPD submitted to COIT a Surveillance Impact Report for the SFPD ALPR. A copy of the SFPD Surveillance Impact Report for the SFPD ALPR is in Board File No. 210559, and is incorporated herein by reference.

(3) Public Hearings. Between August 14, 2020 and January 21, 2021, inclusive, COIT and PSAB conducted a total of four public hearings at which they considered the Surveillance Impact Report and developed a Surveillance Technology Policy for the SFPD ALPR. A copy of the Surveillance Technology Policy for SFPD's use of the SFPD ALPR ("SFPD ALPR Policy") is in Board File No. 210559, and is incorporated herein by reference.

(4) COIT Recommendation. On January 21, 2021, COIT voted to recommend the SFPD ALPR Policy to the Board of Supervisors for approval.

(5) Findings. The Board of Supervisors hereby finds that the SFPD ALPR's benefits outweigh its costs and risks, that the SFPD ALPR Policy will safeguard civil liberties and civil rights, and that the uses and deployments of the SFPD ALPR, as set forth in the SFPD ALPR Policy, will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or Protected Class.

(6) Approval of Policy. The Board of Supervisors hereby approves the SFPD ALPR Policy under which the SFPD may continue to possess and use the SFPD ALPR.

Section 4. Drones (Unmanned Aircraft Systems): Six Departments (Department of Public Works, Department of Technology, Fire Department, Port, Public Utilities Commission, and Recreation and Parks Department).

(a) Current Status. The following Departments currently possess and use Drones, which are also known as Unmanned Aircraft Systems ("Drones"):

DPW

Department of Technology ("DT")

Fire Department ("Fire")

Port

Public Utilities Commission ("PUC")

RPD

(b) DPW.

(1) Purpose. DPW uses Drones ("DPW Drones") for (A) disaster preparedness and response; (B) environmental monitoring and documentation; (C) inspections and surveys of DPW properties and assets; (D) inspections and documentation of DPW projects; and (E) surveying and mapping data collection.

(2) Surveillance Impact Report. DPW submitted to COIT a Surveillance Impact Report for DPW Drones. A copy of the Surveillance Impact Report for DPW Drones is in Board File No. 210559, and is incorporated herein by reference.

(3) Public Hearings. Between February 28, 2020 and July 17, 2021, inclusive, COIT and PSAB conducted a total of three public hearings at which they considered the Surveillance Impact Report and developed a Surveillance Technology Policy for DPW Drones. A copy of the Surveillance Technology Policy for DPW's use of Drones ("DPW Drone Policy") is in Board File No. 210559, and is incorporated herein by reference.

(4) COIT Recommendation. On July 17, 2020, COIT voted to recommend the DPW Drone Policy to the Board of Supervisors for approval.

(5) Findings. The Board of Supervisors hereby finds that the benefits of DPW Drones outweigh their costs and risks, that the DPW Drone Policy will safeguard civil liberties and civil rights, and that the uses and deployments of DPW Drones, as set forth in the DPW Drone Policy, will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or Protected Class.

(6) Approval of Policy. The Board of Supervisors hereby approves the DPW Drone Policy under which DPW may continue to possess and use DPW Drones.

(c) DT.

(1) Purpose. DT uses Drones ("DT Drones") for (A) video production, including the capture of video stills and photographs as elements of SFGovTV's video productions, in order to broadcast completed videos on SFGovTV's cable channels and YouTube account; and (B) the development of marketing and promotional videos for City Departments.

(2) Surveillance Impact Report. DT submitted to COIT a Surveillance Impact Report for DT Drones. A copy of the Surveillance Impact Report for DT Drones is in Board File No. 210559, and is incorporated herein by reference.

(3) Public Hearings. Between February 28, 2020 and July 17, 2021, inclusive, COIT and PSAB conducted a total of three public hearings at which they considered the Surveillance Impact Report and developed a Surveillance Technology Policy for DT Drones. A copy of the Surveillance Technology Policy for DT's use of Drones ("DT Drone Policy") is in Board File No. 210559, and is incorporated herein by reference.

(4) COIT Recommendation. On July 17, 2020, COIT voted to recommend the DT Drone Policy to the Board of Supervisors for approval.

(5) Findings. The Board of Supervisors hereby finds that the benefits of DT Drones outweigh their costs and risks, that the DT Drone Policy will safeguard civil liberties and civil rights, and that the uses and deployments of DT Drones, as set forth in the DT Drone Policy, will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or Protected Class.

(6) Approval of Policy. The Board of Supervisors hereby approves the DT Drone Policy under which PUC may continue to possess and use PUC Drones.

(d) Fire.

(1) Purpose. Fire uses Drones ("Fire Drones") for (A) disaster response assessment and district surveys; (B) building fire reconnaissance; (C) search and rescue; and (D) training assessment and evaluation.

(2) Surveillance Impact Report. Fire submitted to COIT a Surveillance Impact Report for Fire Drones. A copy of the Surveillance Impact Report for Fire Drones is in Board File No. 210559, and is incorporated herein by reference.

(3) Public Hearings. Between February 28, 2020 and July 17, 2021, inclusive, COIT and PSAB conducted a total of three public hearings at which they considered the Surveillance Impact Report and developed a Surveillance Technology Policy for Fire Drones.

A copy of the Surveillance Technology Policy for Fire's use of Drones ("Fire Drone Policy") is in Board File No. 210559, and is incorporated herein by reference.

(4) COIT Recommendation. On July 17, 2020, COIT voted to recommend the Fire Drone Policy to the Board of Supervisors for approval.

(5) Findings. The Board of Supervisors hereby finds that the benefits of Fire Drones outweigh their costs and risks, that the Fire Drone Policy will safeguard civil liberties and civil rights, and that the uses and deployments of the Fire Drones, as set forth in the Fire Drone Policy, will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or Protected Class.

(6) Approval of Policy. The Board of Supervisors hereby approves the Fire Drone Policy under which Fire may continue to possess and use the Fire Drones.

(e) Port.

(1) Purpose. The Port uses Drones ("Port Drones") for (A) disaster response and recovery by providing high resolution images during response and recovery operations after a disaster; (B) facility inspections by providing high resolution images during engineering and environmental surveys and assessments of Port properties; and (C) marketing by capturing Port Drones footage to be used in marketing materials for the promotion of activities and opportunities at the Port.

(2) Surveillance Impact Report. The Port submitted to COIT a Surveillance Impact Report for Port Drones. A copy of the Surveillance Impact Report for Port Drones is in Board File No. 210559, and is incorporated herein by reference.

(3) Public Hearings. Between February 28, 2020 and July 17, 2021, inclusive, COIT and PSAB conducted a total of three public hearings at which they considered the Surveillance Impact Report and developed a Surveillance Technology Policy for Port Drones.

A copy of the Surveillance Technology Policy for the Port's use of Drones ("Port Drone Policy") is in Board File No. 210559, and is incorporated herein by reference.

(4) COIT Recommendation. On July 17, 2020, COIT voted to recommend the Port Drone Policy to the Board of Supervisors for approval.

(5) Findings. The Board of Supervisors hereby finds that the benefits of Port Drones outweigh their costs and risks, that the Port Drone Policy will safeguard civil liberties and civil rights, and that the uses and deployments of Port Drones, as set forth in the Port Drone Policy, will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or Protected Class.

(6) Approval of Policy. The Board of Supervisors hereby approves the Port Drone Policy under which Port may continue to possess and use Port Drones.

(f) PUC.

(1) Purpose. The PUC uses Drones ("PUC Drones") for (A) construction management, including inspection of project sites for contract and environmental compliance; (B) environmental monitoring and documentation, including monitoring of vegetation type and health, wildlife, and streams and reservoirs; (C) inspections, including conducting surveys and assessments of San Francisco PUC properties and assets, including surveys of bay and ocean outfalls, large wastewater collections, and power lines; (D) disaster relief to record footage of damage and assess the role PUC may play in responding to such disasters; and (E) marketing and public education, including capturing footage of the watershed.

(2) Surveillance Impact Report. The PUC submitted to COIT a Surveillance Impact Report for PUC Drones. A copy of the Surveillance Impact Report for PUC Drones is in Board File No. 210559, and is incorporated herein by reference.

(3) Public Hearings. Between February 28, 2020 and July 17, 2021, inclusive, COIT and PSAB conducted a total of three public hearings at which they considered the

Surveillance Impact Report and developed a Surveillance Technology Policy for PUC Drones. A copy of the Surveillance Technology Policy for PUC's use of Drones ("PUC Drone Policy") is in Board File No. 210559, and is incorporated herein by reference.

(4) COIT Recommendation. On July 17, 2020, COIT voted to recommend the PUC Drone Policy to the Board of Supervisors for approval.

(5) Findings. The Board of Supervisors hereby finds that the benefits of PUC Drones outweigh their costs and risks, that the PUC Drone Policy will safeguard civil liberties and civil rights, and that the uses and deployments of PUC Drones, as set forth in the PUC Drone Policy, will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or Protected Class.

(6) Approval of Policy. The Board of Supervisors hereby approves the PUC Drone Policy under which PUC may continue to possess and use PUC Drones.

(g) RPD.

(1) Purpose. RPD uses Drones ("RPD Drones") for (A) disaster preparedness and response, including post-disaster mitigation, logistical support for emergency routing, life safety, and cleanup efforts, and protection of physical assets, public spaces, and human life; (B) environmental monitoring and documentation; (C) inspection and surveys of properties and assets; (D) inspection and documentation of projects; and (E) data collection for surveys and mapping.

(2) Surveillance Impact Report. RPD submitted to COIT a Surveillance Impact Report for RPD Drones. A copy of the Surveillance Impact Report for RPD Drones is in Board File No. 210559, and is incorporated herein by reference.

(3) Public Hearings. Between February 28, 2020 and July 17, 2021, inclusive, COIT and PSAB conducted a total of three public hearings at which they considered the Surveillance Impact Report and developed a Surveillance Technology Policy for RPD Drones.

A copy of the Surveillance Technology Policy for RPD's use of Drones ("RPD Drone Policy") is in Board File No. 210559, and is incorporated herein by reference.

(4) COIT Recommendation. On July 17, 2020, COIT voted to recommend the RPD Drone Policy to the Board of Supervisors for approval.

(5) Findings. The Board of Supervisors hereby finds that the benefits of RPD Drones outweigh their costs and risks, that the RPD Drone Policy will safeguard civil liberties and civil rights, and that the uses and deployments of RPD Drones, as set forth in the RPD Drone Policy, will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or Protected Class.

(6) Approval of Policy. The Board of Supervisors hereby approves the RPD Drone Policy under which RPD may continue to possess and use RPD Drones.

Section 5. Security Cameras: Nineteen Departments.

(a) Current Status. The following Departments currently possess and use security cameras:

SFO

Arts Commission

Asian Art Museum

Department of Child Support Services ("DCSS")

City Administrator

DT

Department of Emergency Management ("DEM")

Fire

Department of Homelessness and Supportive Housing (DHSH")

Department of Human Resources ("DHR")

Human Services Agency (“HSA”)

Library

Municipal Transportation Agency (“MTA”)

Port

PUC

Department of Public Health (“DPH”)

RPD

Rent Board

War Memorial

As set forth below, COIT developed a consolidated security camera policy for use by 16 of the above 19 Departments that currently use security cameras, and Department-specific policies for the remaining three (MTA, Library, and PUC).

(b) Consolidated Departments Security Camera Policy.

(1) COIT developed a security camera policy for the Departments listed below, which, for purposes of this Section 5, shall be referred to as the “Consolidated Departments”:

SFO

Arts Commission

Asian Art Museum

DCSS

City Administrator

DT

DEM

Fire

DHSH

DHR

HSA

Port

DPH

RPD

Rent Board

War Memorial

(2) Purpose. The Consolidated Departments use security cameras for (A) live monitoring of their property; (B) recording of video and images; (C) reviewing camera footage in the event of an incident; and (D) providing video footage and images to law enforcement or other authorized persons following an incident or upon request.

(3) Surveillance Impact Report. The Consolidated Departments submitted to COIT Surveillance Impact Reports for their use of security cameras. A copy of the Surveillance Impact Reports for the Consolidated Departments' security cameras is in Board File No. 210559, and is incorporated herein by reference.

(4) Public Hearings. Between November 13, 2020 and March 18, 2021, inclusive, COIT and PSAB conducted a total of six public hearings at which they considered the Surveillance Impact Reports submitted by the Consolidated Departments and developed a Surveillance Technology Policy for the Consolidated Departments' security cameras. A copy of the Surveillance Technology Policy for the Consolidated Departments' Security Cameras ("Consolidated Departments Security Camera Policy") is in Board File No. 210559, and is incorporated herein by reference.

(5) COIT Recommendation. On July 17, 2020, COIT voted to recommend the Consolidated Departments Security Camera Policy to the Board of Supervisors for approval.

(6) Findings. The Board of Supervisors hereby finds that the benefits of the Consolidated Departments' security cameras outweigh their costs and risks, that the

Consolidated Departments Security Camera Policy will safeguard civil liberties and civil rights, and that the uses and deployments of the Consolidated Departments' security cameras, as set forth in the Consolidated Departments Security Camera Policy, will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or Protected Class.

(7) Approval of Policy. The Board of Supervisors hereby approves the Consolidated Departments Security Camera Policy under which the Consolidated Departments may continue to possess and use the Consolidated Departments' security cameras.

(c) MTA Security Cameras.

(1) Purpose. MTA uses security cameras ("MTA Security Cameras") for (A) live monitoring of MTA property; (B) recording of video and images; (C) reviewing camera footage in the event of an incident; (D) providing video footage and images to law enforcement or other authorized persons following an incident or upon request; and (E) enforcing parking and driving violations.

(2) Surveillance Impact Report. MTA submitted to COIT a Surveillance Impact Report for MTA Security Cameras. A copy of the Surveillance Impact Report for MTA Security Cameras is in Board File No. 210559, and is incorporated herein by reference.

(3) Public Hearings. On February 12, 2021 and March 18, 2021, COIT and PSAB conducted a total of two public hearings at which they considered the Surveillance Impact Report and developed a Surveillance Technology Policy for MTA Security Cameras. A copy of the Surveillance Technology Policy for MTA's use of MTA Security Cameras ("MTA Security Camera Policy") is in Board File No. 210559, and is incorporated herein by reference.

(4) COIT Recommendation. On March 18, 2021, COIT voted to recommend the MTA Security Camera Policy to the Board of Supervisors for approval.

(5) Findings. The Board of Supervisors hereby finds that the benefits of MTA Security Cameras outweigh their costs and risks, that the MTA Security Camera Policy will safeguard civil liberties and civil rights, and that the uses and deployments of MTA Security Cameras, as set forth in the MTA Security Camera Policy, will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or Protected Class.

(6) Approval of Policy. The Board of Supervisors hereby approves the MTA Security Camera Policy under which MTA may continue to possess and use MTA Security Cameras.

(d) Library Security Cameras.

(1) Purpose. The Library uses security cameras ("Library Security Cameras") for (A) live monitoring of Library property to protect the safety of Library staff, patrons, and facilities; (B) recording of video and images; (C) reviewing camera footage in the event of an incident; and (D) providing video footage and images to law enforcement or other authorized persons following an incident or upon request.

(2) Surveillance Impact Report. The Library submitted to COIT a Surveillance Impact Report for Library Security Cameras. A copy of the Surveillance Impact Report for Library Security Cameras is in Board File No. 210559, and is incorporated herein by reference.

(3) Public Hearings. On February 12, 2021 and March 18, 2021, COIT and PSAB conducted a total of two public hearings at which they considered the Surveillance Impact Report and developed a Surveillance Technology Policy for Library Security Cameras. A copy of the Surveillance Technology Policy for the Library's use of Library Security Cameras ("Library Security Camera Policy") is in Board File No. 210559, and is incorporated herein by reference.

(4) COIT Recommendation. On March 18, 2021, COIT voted to recommend the Library Security Camera Policy to the Board of Supervisors for approval.

(5) Findings. The Board of Supervisors hereby finds that the benefits of Library Security Cameras outweigh their costs and risks, that the Library Security Camera Policy will safeguard civil liberties and civil rights, and that the uses and deployments of Library Security Cameras, as set forth in the Library Security Camera Policy, will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or Protected Class.

(6) Approval of Policy. The Board of Supervisors hereby approves the Library Security Camera Policy under which the Library may continue to possess and use Library Security Cameras.

(d) PUC Security Cameras.

(1) Purpose. The PUC uses security cameras ("PUC Security Cameras") to (A) deter malicious behavior directed at PUC facilities, employees, or personnel working on behalf of the PUC; (B) capture potential or actual malicious behavior by or against PUC facilities, employees, or personnel working on behalf of the PUC; (C) provide evidence to support incident investigations; (D) provide real-time monitoring of operations and critical equipment at PUC facilities; and (E) support PUC health and safety requirements and objectives..

(2) Surveillance Impact Report. The PUC submitted to COIT a Surveillance Impact Report for PUC Security Cameras. A copy of the Surveillance Impact Report for PUC Security Cameras is in Board File No. 210559, and is incorporated herein by reference.

(3) Public Hearings. Between February 26, 2021 and March 18, 2021, inclusive, COIT and PSAB conducted a total of three public hearings at which they considered the Surveillance Impact Report and developed a Surveillance Technology Policy for PUC Security Cameras. A copy of the Surveillance Technology Policy for the PUC's use of PUC

Security Cameras ("PUC Security Camera Policy") is in Board File No. _210559, and is incorporated herein by reference.

(4) COIT Recommendation. On March 18, 2021, COIT voted to recommend the PUC Security Camera Policy to the Board of Supervisors for approval.

(5) Findings. The Board of Supervisors hereby finds that the benefits of PUC Security Cameras outweigh their costs and risks, that the PUC Security Camera Policy will safeguard civil liberties and civil rights, and that the uses and deployments of PUC Security Cameras, as set forth in the PUC Security Camera Policy, will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or Protected Class.

(6) Approval of Policy. The Board of Supervisors hereby approves the PUC Security Camera Policy under which the PUC may continue to possess and use PUC Security Cameras.

Section 6. Radio Frequency Identification ("RFID")

(a) Current Status. The Library currently possesses and uses RFID.

(b) Purpose. The Library uses RFID to (1) passively tag library material for inventory management and circulation functions; (2) allow staff to check in and check out material and trigger holds; (3) allow patrons to check out material; (4) allow staff to confirm the current inventory on the library's shelves; and (5) check and sort material in order to sort the items into carts and bins for delivery to other floors and branches.

(c) Surveillance Impact Report. The Library submitted to COIT a Surveillance Impact Report for RFID. A copy of the Surveillance Impact Report for RFID is in Board File No. 210559, and is incorporated herein by reference.

(d) Public Hearings. On January 24, 2020 and February 20, 2020, COIT and PSAB conducted a total of two public hearings at which they considered the Surveillance Impact Report and developed a Surveillance Technology Policy for the Library RFID. A copy of the Surveillance Technology Policy for the Library's RFID ("Library RFID Policy") is in Board File No. 210559, and is incorporated herein by reference.

(e) COIT Recommendation. On February 20, 2020, COIT voted to recommend the Library RFID Policy to the Board of Supervisors for approval.

(f) Findings. The Board of Supervisors hereby finds that the Library's RFID benefits outweigh its costs and risks, that the Library RFID Policy will safeguard civil liberties and civil rights, and that the uses and deployments of the Library RFID, as set forth in the Library RFID Policy, will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or Protected Class.

(g) Approval of Policy. The Board of Supervisors hereby approves the Library RFID Policy under which the Library may continue to possess and use the Library RFID.

Section 7. The Administrative Code is hereby amended by adding Section 19B.10, to read as follows:

SEC. 19B.10. POSTING OF BOARD-APPROVED SURVEILLANCE TECHNOLOGY POLICIES; APPENDIX.

(a) Each Department shall post each Surveillance Technology Policy for that Department that has been approved by the Board of Supervisors in accordance with this Chapter 19B, on the Department's website within 10 days of the Board's approval of the policy.

(b) There shall be an Appendix to this Chapter 19B, which shall contain a record of all Surveillance Technology Policies approved by the Board of Supervisors in accordance with this

Chapter 19B. Upon approval by ordinance of a Surveillance Technology Policy, the City Attorney shall cause said policy to be identified in said Appendix.

Section 8. Effective Date. This ordinance shall become 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 within ten days of receiving it, or the Board of Supervisors overrides the Mayor's veto of the ordinance.

APPROVED AS TO FORM:
DENNIS J. HERRERA, City Attorney

By: /s/ Jana Clark
JANA CLARK
Deputy City Attorney

n:\govern\as2021\1900636\01544280.docx

FILE NO. 210559

LEGISLATIVE DIGEST
(Revised 7/19/21)

[Administrative Code - Approval of Surveillance Technology Policies for Multiple City Departments]

Ordinance approving Surveillance Technology Policies governing the use of 1) Audio Recorders (ShotSpotter) by the Police Department, 2) Automatic License Plate Readers by the Airport, Department of Public Works, Recreation and Parks Department, and Police Department, 3) Drones by the Fire Department, Port, Department of Public Works, Public Utilities Commission, Recreation and Parks Department, and Department of Technology, 4) Security Cameras by the Airport, Arts Commission, Asian Art Museum, Department of Child Support Services, City Administrator, Department of Technology, Department of Emergency Management, Fire Department, Department of Homelessness and Supportive Housing, Department of Human Resources, Human Services Agency, Library, Municipal Transportation Agency, Port, Public Utilities Commission, Department of Public Health, Recreation and Parks Department, Rent Board, and War Memorial, and 5) Radio Frequency Identification by the Library; making required findings in support of said approvals; and amending the Administrative Code to require departments to post each Board-approved Surveillance Technology Policy on the department website.

Existing Law

Existing law, Administrative Code Chapter 19B ("Chapter 19B"), governs the acquisition and use of surveillance technology by City departments. Chapter 19B requires each department possessing or using surveillance technology before the effective date of Chapter 19B (May 30, 2019) to submit an inventory of its existing surveillance technology to the Committee on Information Technology ("COIT"). Chapter 19B further requires that COIT publicly post the inventories on COIT's website. Chapter 19B also requires that each department submit a proposed policy for the use of existing surveillance technology to the Board of Supervisors for approval by ordinance, but permits departments to use existing surveillance technology until such time as the Board enacts an ordinance approving a surveillance technology policy. Chapter 19B further requires that the Board of Supervisors approve a surveillance technology policy ordinance only if it determines that the benefits of the surveillance technology outweigh its costs, that the policy will safeguard civil liberties and civil rights, and that the uses and deployments of the surveillance technology will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or protected class.

Amendments to Current Law

This ordinance would approve surveillance technology policies governing multiple departments' use of existing surveillance technologies, and find for each that the benefits of the surveillance technology outweigh its costs and risks, that the policy will safeguard civil liberties and civil rights, and that the uses and deployments of the surveillance technology will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or protected class. Specifically, this ordinance would approve five categories of surveillance technology policies used by multiple departments as follows:

1) Audio Recorders (ShotSpotter) -
    Police Department
2) Automatic License Plate Readers -
    Airport
    Department of Public Works
    Recreation and Parks Department
    Police Department
3) Drones
    Fire Department
    Port
    Department of Public Works
    Public Utilities Commission
    Recreation and Parks Department
    Department of Technology
4) Security Cameras
    Airport
    Arts Commission
    Asian Art Museum
    Department of Child Support Services
    City Administrator
    Department of Technology
    Department of Emergency Management
    Fire Department
    Department of Homelessness and Supportive Housing
    Department of Human Resources
    Human Services Agency
    Library Department
    Municipal Transportation Agency
    Port
    Public Utilities Commission
    Department of Public Health
    Recreation and Parks Department
    Rent Board
    War Memorial

City and County of San Francisco

Committee on Information Technology

July 19, 2021

Agenda

- COIT Overview
- CCSF Privacy & Surveillance Landscape
- Work to Date: Section 19B Compliance
- Recommendations to 19B

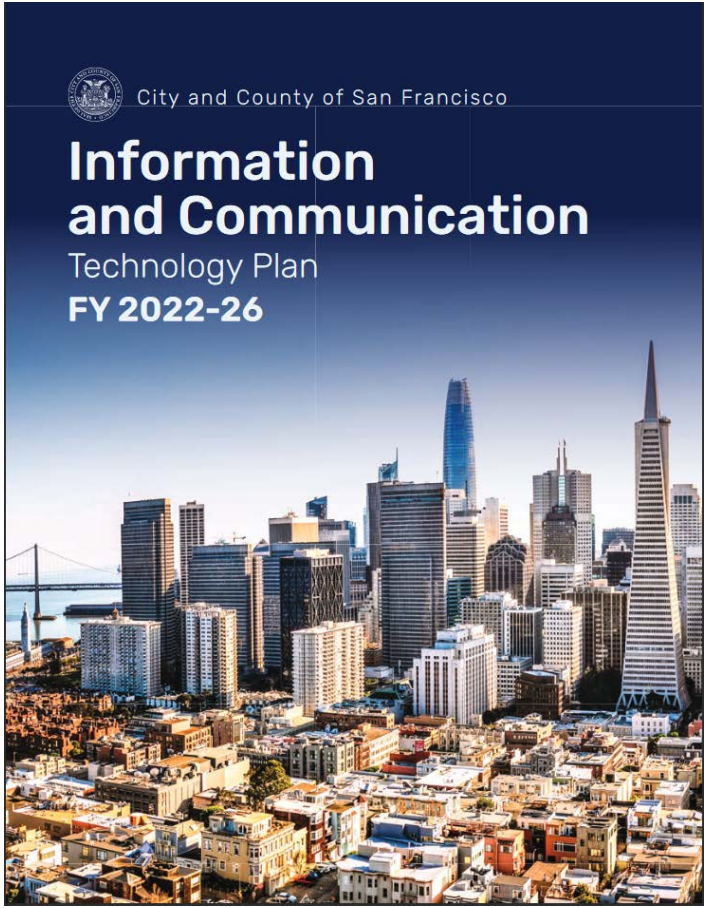
COIT Overview

We are the City & County of San Francisco's technology governance body.

COIT's structure is intended to provide a forum for City leadership to coordinate and collaborate. Through regular public meetings, COIT is also a vehicle to share with residents and the public the state of technology in the City.

Responsibilities

- Five-year technology plan
- Annual Budget
- Portfolio Management
- Technology Policy



CCSF Privacy & Surveillance Landscape

Examples of Data/ Privacy Regulations…

HIPAA – Health Insurance Portability and Accounting Act

FERPA – Family Educational Rights and Privacy Act

CJIS – Criminal Justice Information Services

PCI DSS – Payment Card Industry Data Security Standard

History: COIT Data/ Privacy Policies

Cybersecurity (2016) – Policy, training and awareness, and requirements

Data Governance (2017) – Data Classification Standard

Drones (2017) – Limited Authorized Use

All COIT Policies are available at:

https://sf.gov/information/coit-policy

Data Lifecycle

Created by Barudak Lier
from Noun Project

Collect

Created by Gregor Cresnar
from Noun Project

Process
&
Use

Created by Тимур Миннапеев
from Noun Project

Share

Created by Astatine Lab
from Noun Project

Storage

Created by Pikselan
from Noun Project

Dispose

Upcoming Policy Development

- Data Minimization Guideline
- Public Noticing Standards
- Privacy Policies for digital services

Section 19B Compliance

Section 19B Department Requirements

- Surveillance Inventory (deadline August 29, 2019)
- Impact Report
- Surveillance Technology Policy
- Annual Report

Section 19B Definition of Duties

COIT's role is to:

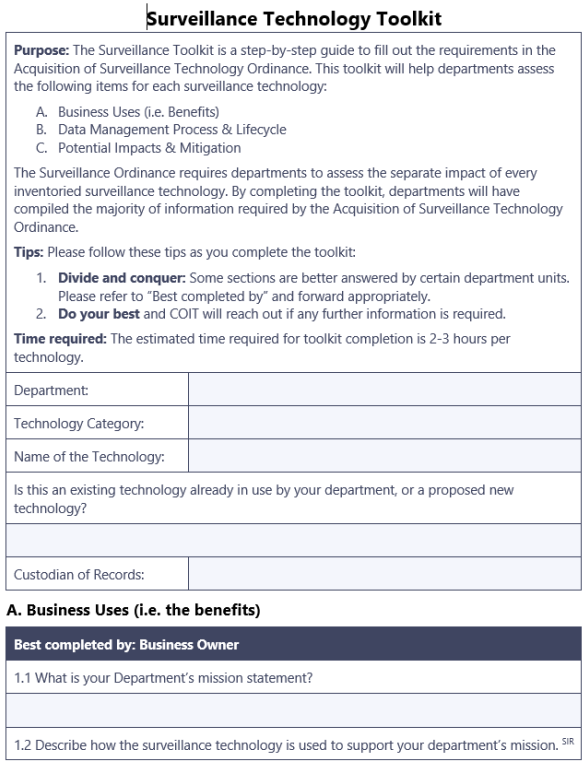
- Post the surveillance inventory available at: https://sf.gov/resource/2020/surveillance-technology-inventory
- Work with departments on Impact Report and Policy
- Conduct public hearings and recommend action to the Board of Supervisors
- Post annual surveillance reports

SURVEILLANCE INVENTORY CATEGORY	NUMBER (2021)_
Ads and Notifications	12
Audio Recorders	3
Automatic License Plate Readers	5
Biometric Processing	8
Camera	58
Drone	6
Location Management	10
Misc	26
RFID/ Toll Reader	4
Smart City Sensor	3
Social Media Monitoring	33
Total	**168**

Surveillance Toolkit

COIT's Toolkit aims to achieve:

- A robust impact assessment
- Streamline submission of all Ordinance requirements
- Minimize implementation burden
- Inform the Board of Supervisors' decision assessing whether the benefits of each surveillance technology outweigh the costs.



Surveillance Technology Toolkit

Purpose: The Surveillance Toolkit is a step-by-step guide to fill out the requirements in the Acquisition of Surveillance Technology Ordinance. This toolkit will help departments assess the following items for each surveillance technology:

A. Business Uses (i.e. Benefits)
B. Data Management Process & Lifecycle
C. Potential Impacts & Mitigation

The Surveillance Ordinance requires departments to assess the separate impact of every inventoried surveillance technology. By completing the toolkit, departments will have compiled the majority of information required by the Acquisition of Surveillance Technology Ordinance.

Tips: Please follow these tips as you complete the toolkit:

1. **Divide and conquer:** Some sections are better answered by certain department units. Please refer to "Best completed by" and forward appropriately.
2. **Do your best** and COIT will reach out if any further information is required.

Time required: The estimated time required for toolkit completion is 2-3 hours per technology.

Department:	
Technology Category:	
Name of the Technology:	
Is this an existing technology already in use by your department, or a proposed new technology?	
Custodian of Records:	

A. Business Uses (i.e. the benefits)

Best completed by: Business Owner
1.1 What is your Department's mission statement?
1.2 Describe how the surveillance technology is used to support your department's mission. SIR

Civil Liberties & Civil Rights Impact

What are privacy impacts?

NIST Privacy Framework

- Dignity Loss
- Discrimination
- Economic Loss
- Loss of Autonomy
- Loss of Liberty
- Physical Harm
- Loss of Trust

How do we mitigate impact?

Potential actions

- Administrative
- Technical
- Physical

Privacy & Surveillance Advisory Board

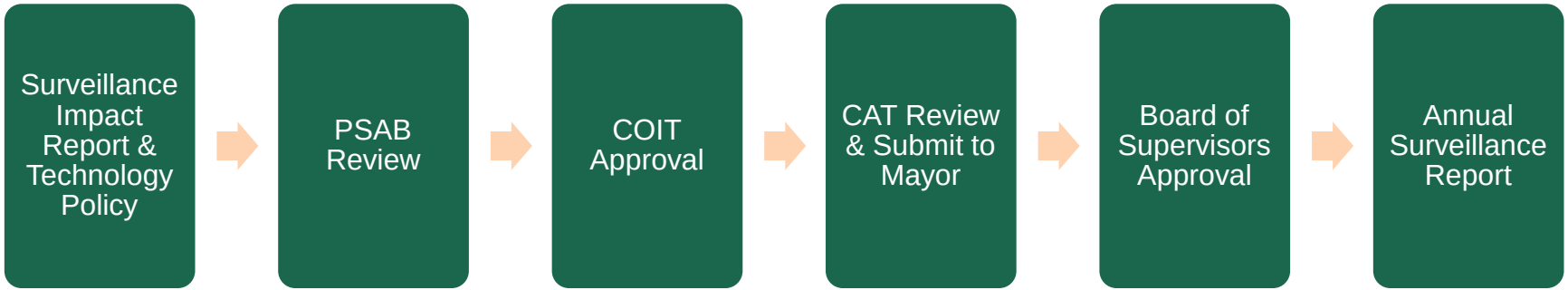
Public Hearings:

- 2nd and 4th Friday of each month

Membership:

Chair – Office of Contract Administration	Juvenile Probation
City Services Auditor	San Francisco International Airport
Controller	Committee on Information Technology
DataSF	Public Member
Department of Technology	

Review Process



Calendar Review

Number of public meetings since August 2019:

- 20 PSAB meetings
- 8 COIT meetings

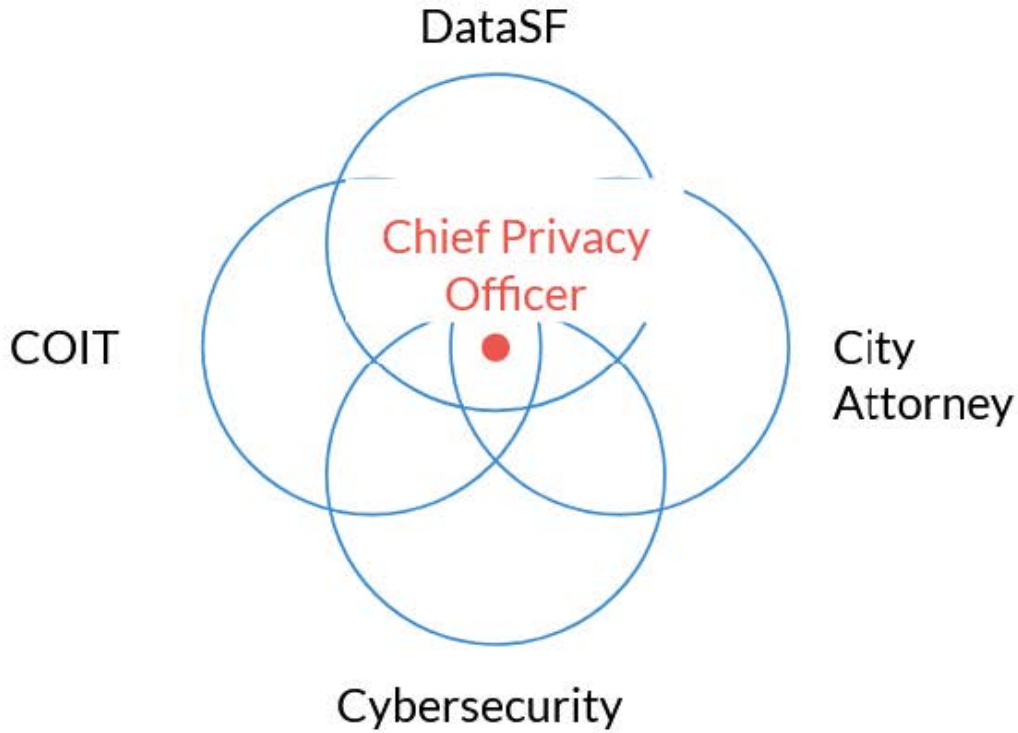
COIT APPROVALS	TECHNOLOGY
February 20, 2020	RFID (SFPL)
July 17, 2020	Drones
January 21, 2021	Audio Recorder ALPR (Police)
February 4, 2021	ALPR
March 18, 2021	Security Cameras

Recommendations to 19B

Recommendation 1: Hire In-House Expertise

Some activities of a **Chief Privacy Officer (CPO)**:

- **Procurement**: City contracts should include privacy requirements, especially for third-party vendors with sensitive data.
- **Privacy by Design**: We need to embed privacy practices in the design of City products.
- **Trainings**: City staff need better training on privacy practices.


DataSF
Chief Privacy Officer
COIT
City Attorney
Cybersecurity

Recommendation 2: Citywide Policy

Current State:

- Current process is administrative burdensome and redundant.

Recommendation:

- A single citywide policy per technology category.
- Department's to create subsequent requirements on top of citywide baseline.

Recommendation 3: 19B Amendments

Current State:

- Definition of surveillance technology is overbroad.
- IT Infrastructure or services where consent is obtained considered surveillance technology.

Recommendation

- Refinement of definition and/or additional exemptions.

Thank You!

5) Radio Frequency Identification
Library Department.

This ordinance also would amend Chapter 19B to require that departments post each Board approved surveillance technology policy on the department's website within 10 days of the Board's approval of the policy.

Background

This ordinance includes amendments approved by the Rules Committee at their July 19, 2021.

n:\govern\as2021\1900636\01544289.docx

Chapter 19B. Upon approval by ordinance of a Surveillance Technology Policy, the City Attorney shall cause said policy to be identified in said Appendix.

Section 8. Effective Date. This ordinance shall become 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 within ten days of receiving it, or the Board of Supervisors overrides the Mayor's veto of the ordinance.

APPROVED AS TO FORM:
DENNIS J. HERRERA, City Attorney

By: /s/ Jana Clark
JANA CLARK
Deputy City Attorney

n:\govern\as2021\1900636\01544280.docx

Surveillance Impact Report

Audio Recorder - ShotSpotter, Inc. ("ShotSpotter")
San Francisco Police Department

As required by San Francisco Administrative Code, Section 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 ShotSpotter, Inc. ("ShotSpotter").

DESCRIPTION OF THE TECHNOLOGY

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.

In line with its mission, the Department uses ShotSpotter, Inc. ("ShotSpotter") which enables SFPD to be aware of gunshots in the absence of witnesses and/or reports to 911 of gunshots. The ShotSpotter system notifies SFPD of verified gunshot events, which expedites police and ambulance response rates to incidents involving illegal gunfire to help locate victims, witnesses, evidence (casings, bullets, firearms) and suspects.

It shall be the policy of the SFPD to properly utilize ShotSpotter to enhance the Department's ability to respond to and investigate violent crimes involving illegal gunfire.

SFPD shall use ShotSpotter, Inc. ("ShotSpotter") only for the following authorized purposes:

Authorized Use(s):

1. Gunshot detection: Record gunshot sounds and use sensors to locate the origin of the gunshots. Patrol Officers receive gunshot alerts to respond to crime scene.

2. Investigators use ShotSpotter Investigative Portal reports to find shell casing evidence on scene and to further analyze the incident.

All use cases not defined as an authorized use are prohibited.

A ShotSpotter alert will not, on its own, identify an individual, reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, information concerning an individual person's sex life or sexual orientation. Recordings of ambient noise, or any other sound outside of verified gunshots shall be prohibited for use in any investigation and shall not cause police enforcement.

Surveillance Oversight Review Dates
COIT Review: January 21, 2021
Board of Supervisors Review: TBD

TECHNOLOGY DETAILS

The following a is product description of ShotSpotter, Inc. ("ShotSpotter"):

ShotSpotter Inc. is a California-based company that operates ShotSpotter Flex, a proprietary technology that uses sensors strategically placed in a geographic coverage area to detect, locate, and analyze gunshots, and notify law enforcement. ShotSpotter places acoustic sensors high above the street, typically on buildings. The sensors connect over a private commercial cellular wireless communications network in real-time to the ShotSpotter hosted servers. After a loud, impulsive sound is captured and located by 3 or more ShotSpotter Sensors, an incident is created and a short snippet of audio is sent to the ShotSpotter Incident Review Center (IRC) via secure, high-speed network connections for real-time verification that it is a gunshot. ShotSpotter professional reviewers analyze the audio soundwave visually, and listen to the sound to confirm whether it is gunfire or non-gunfire (e.g. fireworks, car back fire, helicopter, construction etc.). If it is validated as a gunshot, an alert is published and sent directly to the Customer's dispatch center, PSAP, mobile/patrol officers, and any other relevant safety or security personnel, as determined by the Customer (SFPD). The process from trigger pull to published alert takes on average 34 seconds.

Investigative Lead Summary ("ILS"): ShotSpotter provides an on-demand report for investigators available through the ShotSpotter Respond Application. The Investigative Lead Summary (ILS) provides useful details about the approximate location, timing, and sequence of each shot fired during an incident (similar to a DFR below, but not a court-admissible document)

Detailed Forensic Report ("DFR"): ShotSpotter will provide a DFR for any ShotSpotter-detected incidents, including Reviewed Alerts. The DFR is intended to be a court-admissible document used by attorneys as part of a court case for the exact, verified timing, sequence and location of each shot fired.

How It Works:

ShotSpotter uses acoustic sensors that are strategically placed in an array of approximately 20-25 sensors per square mile. These sensors are connected wirelessly to ShotSpotter's centralized, cloud-based application to reliably detect and accurately triangulate (locate) gunshots. Each acoustic sensor captures the precise time and audio associated with impulsive sounds that may represent gunfire. This data, from multiple sensors, is used to locate the incident, which is then filtered by sophisticated machine algorithms to classify the event as a potential gunshot. Expertly trained acoustic analysts, who are located and staffed in ShotSpotter's 24x7 Incident Review Center, then further qualify those highlighted incidents. These analysts ensure and confirm that the events are in fact gunfire. In addition, the analysts can append the alert with other critical intelligence such as whether a fully-automatic weapon was fired or whether multiple shooters are involved. This process typically takes no more than 45 seconds from the time of the actual shooting to the digital alert (with the precise location identified as a dot on a map) popping onto a screen of a computer in the 911 Call Center or on a police officer's smartphone or mobile laptop. There are three components to the ShotSpotter system:

1. Gunshot Location Detection (GLD) Sensors: Sensors are installed in different coverage areas in San Francisco.

2. ShotSpotter Incident Review Center (IRC): Sensors send acoustic information to the cloud where computer-based machine-learning algorithms are used to analyze the sound. If the sound and visual audio signature match gunfire, the incident file is then passed along to the IRC. Acoustic experts at the IRC review incidents within seconds and provide additional information (e.g. multiple shooters, high caliber weapon, automatic weapon). Confirmed gunshots are pushed out to Communications (dispatch) as well as to the SFPD ShotSpotter software system within seconds.

3. ShotSpotter User Software: SFPD authorized personnel can receive ShotSpotter alerts and access historical gunshot incident details for more in-depth investigative analysis using desktop-based, web-based or mobile applications.

All data collected or processed by ShotSpotter, Inc. will be handled or stored by an outside provider or third-party vendor on an ongoing basis. Specifically, data will be handled by ShotSpotter to ensure the Department may continue to use the technology.

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:

A. The benefits of the surveillance technology outweigh the costs.

B. The Department's Policy safeguards civil liberties and civil rights.

C. 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 public safety of visitors and 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 ShotSpotter has the following benefits for the residents of the City and County of San Francisco:

☐	Education	
☐	Community Development	
X	Health	Quicker response and medical assistance for victims of gun violence which is believed to have more positive survival outcomes
☐	Environment	
X	Criminal Justice	ShotSpotter notifications help make the department aware of gunfire events they would have otherwise not have known about. In 2019, only 15% of SF gunfire incidents were called into 911. ShotSpotter alerts enable a fast, precise officer response to unreported gunfire to render aid to victims of a gunshot, secure critical evidence, and apprehend armed individuals.

- Jobs
- Housing
- Other

Additional benefits include:

The Crime Gun Intelligence Center (CGIC) program: CGICs are an interagency collaboration among local police departments, the U.S. Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), and other partners such as state and local prosecutors, to identify perpetrators of gun crime for immediate investigation, apprehension, and prosecution. The SFPD CGIC partnership reduces turnaround times for evidence analysis and improve SFPD's capabilities for connecting guns to crimes that may appear unrelated and more effectively identified guns used in multiple and cross jurisdictional shooting incidents. The Urban Institute has shown that ShotSpotter significantly improves the collection of evidence in the form of shell casings for gun crimes. These casings can be fed into the ATF's NIBIN database to connect gun crimes and identify potential suspects.

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:

ShotSpotter acoustic sensors use ordinary microphones that are similar to ones found in cellphones. They are placed high above the street and are not positioned, tuned or specialized to pick up human voices. The sensors "listen" for gunshot-like sounds and trigger only when detecting an impulsive sound that is instantaneous and sharp. When at least three different sensors detect a gunshot-like sound at the same time and determine a location, they send a short audio snippet to ShotSpotter headquarters that includes 1 second of sound prior to the incident (to establish a baseline of ambient noise), the incident itself and 1 second after. Upon detecting a likely gunshot, trained ShotSpotter personnel listen to a short computer-generated audio snippet of the gunfire to double check that it is actually gunfire. It is highly unusual for a human voice to be included in a snippet. For this to occur, the voice must be loud enough to be heard over the gunfire. In addition, there is no personally identifiable information in any audio snippet.

Since 2012, only authorized ShotSpotter employees have access to audio from sensors. They can only access it under a strict set of conditions and can only provide police a short audio snippet. In 2019 ShotSpotter commissioned an independent privacy audit by the Policing Project at NYU Law School. This end-to-end assessment conducted by objective privacy professionals concluded that ShotSpotter presents an "extremely low risk of audio surveillance". The Policing Project based this finding upon the short amount of audio that is temporarily stored on sensors, the short length of audio snippets that are permanently stored as evidence and the internal controls the company uses to restrict access to audio for authorized employees only.

Human voices and street noise will never trigger a sensor because they do not produce an instantaneous sharp sound and they are not loud enough to be picked up by three or more sensors. That being said, street noise that can include human voices could be captured by a sensor temporarily. All sensor audio, however, is permanently deleted after 30 hours and never

heard by a human unless it was accompanied by a loud, impulse sound thought to be a gunshot. Live streaming of audio is not possible.

Technology and operational mitigations:

• ShotSpotter, not SFPD, is responsible for determining the location(s) for installation of acoustic sensors. Sensors are placed high above the ground typically on top of buildings or sometimes lampposts. At this height, there is more limited ability to pick up street level sounds clearly.

Determining locations: ShotSpotter works with police agencies using their historical crime data on shootings to determine the desired physical boundaries of the coverage area for the gunshot detection technology. Once the coverage area is set, trained ShotSpotter operations personnel, who are experienced with wide-area array sensor design, use an analytical process to determine how many sensors are needed and where they should be placed in order to achieve reliable detection throughout the area. Factors that go into final sensor location selection include:

- Desired sensor density based on the unique geographical, topographical, and ambient acoustic features of the coverage area
- Relative distance and spacing between other sensors
- Height of building or structure (to better "hear to the horizon" and thus minimize acoustic signal attenuation from far away gunfire)
- Availability of reliable power
- Adequate cellular coverage, signal strength and latency for communications
- Written permission from the property owner to install a sensor

• The sensors are not capable of audio streaming – neither ShotSpotter nor SFPD can listen in on street level sounds in real-time.

• The system permanently deletes all audio that is temporarily stored on the sensor after 30 hours.

• The system only triggers an incident to send downstream when 3 or more sensors hear a loud, impulsive sound. Sensors cannot be triggered by human voices because voices are not impulsive enough or loud enough to be heard by 3 sensors which may be 800 meters or more apart. Thus, the audio of a human voice that may be captured by 1 sensor would be permanently deleted after 30 hours and no police or ShotSpotter employee will have heard that sound.

• If a sound is loud enough and sharp enough to possibly be a gunshot and is detected by 3 or more sensors and a location is able to be determined, the system pulls a short audio snippet of the sound plus 1 second of ambient noise prior to the incident and 1 second after. This audio is interpreted by a machine at first and then reviewed by an acoustic analyst at ShotSpotter Headquarters who is only presented with the audio snippet and is under significant time pressure to process the incident as either a gunshot or to dismiss as a non-gunshot and get on to the next incident. All incidents, whether determined to be a gunshot or non-gunshot, are permanently and securely stored in the cloud to serve as both evidence and to train the machine classifier in the future.

• ShotSpotter security protocols also mitigate gunshot detection data access. ShotSpotter does not provide extended audio to SFPD or any police agency; they will not provide this access even if requested. Additionally, ShotSpotter does not provide actual precise locations of the sensors to SFPD.

• As previously mentioned, the sensors are constantly listening for gunshot-like sounds and storing what is captured for 30 hours (was 72 hours before July 2019), and then deleting the data unless triggered to send the data to the ShotSpotter Cloud for analysis. The 30-hour buffer allows SFPD to request data within 24 hours in cases where gunshots have been identified by police but not picked up by the system or if there is a need to verify if there were other gunshots prior to the authenticated event.

• ShotSpotter policy stipulates that only a limited number of authorized forensic engineers can access the storage buffer of a sensor to retrieve prior recorded data within that 30-hour window and search for other gunshot impulsive sound events. To avoid listening to recorded data on a sensor in a haphazard way, the search for a missing gunshot is first done visually through a secure interface looking for the prevalence of electrical "pulses" strong enough to be a gunshot that occurred around the time of the incident in question.

•Upon receiving a gunshot alert SFPD authorized personnel may find that a voice has been recorded along with gunshot sound, but such voice data is only associated with the actual gunshot data and has no personally identifiable information built in. There is no way to tag any voice audio that is unintentionally recorded when connected to a gunshot.

•SFPD takes data security seriously and safeguards GDT System data by both procedural and technological means. Only authorized and trained personnel are permitted access to the system. The system always requires user and password ID for login. Furthermore, only personnel specifically designated by the Chief or Chief-designee have access to the system desktop applications which provide access to any historical downloadable data.

•ShotSpotter data collected by SFPD shall not be used for the enforcement of Immigration Laws. SFPD complies with SF Admin Code Section 12H and 12I.

C. Fiscal Analysis of Costs and Benefits

The Department's use of ShotSpotter, Inc. yields the following business and operations benefits:

	Benefit	Description
☐	Financial savings	
X	Time savings	If a 911 caller reports a gunshot incident, it usually takes several minutes to capture and relay the information to officers often with imprecise data on the exact location. With ShotSpotter, officers receive alerts within 60 seconds of trigger pull with closest address data enabling a faster response to a crime scene to potentially save victims.

X	Staff safety	Officers can approach a crime scene more safely with ShotSpotter alerts knowing the precise location and time of the event and whether there are multiple shooters or high capacity weapons being used.
X	Improved data quality	Only 15% of gunshot incidents in SF have an accompanying 911 call (2019). Without ShotSpotter there would be no police response to 85% of gun crime representing over 850 incidents. However, with ShotSpotter, virtually all incidents are captured with an exact location enabling the department to better protect and serve the community.
☐	Other	

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

FTE (new & existing)			-
Classification			-
	Annual Cost	***Years***	***One-Time Cost***
Total Salary & Fringe	$0	-	-
Software	$0	-	-
Hardware/Equipment	$0	-	-
Professional Services	$545,938	4	-
Training	$0	-	-
Other	$0	-	-
Total Cost [Auto-calculate]			**$ 2,183,752**
2.1 Please disclose any current or potential sources of funding (e.g. potential sources = prospective grant recipients, etc.). SIR, ASR			
SFPD operational budget			

The Department funds its use and maintenance of the surveillance technology through SFPD operational budget.

COMPARISON TO OTHER JURISDICTIONS

Sample results reported from other cities:

- Oakland, CA: ShotSpotter Policy approved by the Oakland Privacy Commission in November 2019.
- Las Vegas Metro Police pilot report indicates 342 gunshot incidents were identified by ShotSpotter in first 9 months of use that the PD would not have known about and a 26% reduction in violent crime. Expanded coverage area to all known hotspots.[1]
- Cincinnati cites a 48% reduction in shootings[2]
- Newport News reports a 13% reduction in shootings with ShotSpotter[3]
- Greenville, NC reports a 33% reduction in gun violence injuries using ShotSpotter[4]
- Chicago cites a drop of over 40% in shootings in the Englewood District in the first year after installation[5]
- Camden County, NJ–46% reduction in homicides by shooting[6]
- Denver–103 arrests and 84-gun recoveries over the course of 3 years[7]
- Bakersfield–22 arrests in first 9 months[8]
- Pittsburgh – 48 arrests and 83 victims found with help of ShotSpotter in 3 years[9]

[1] https://www.youtube.com/watch?v=bK8_oEjQ-gs&t=23s
[2] https://www.wcpo.com/news/crime/shootings-down-nearly-50-percent-in-cincinnati-this-year-police-say
[3] https://www.dailypress.com/news/crime/dp-nw-newport-news-police-2019-year-20200128-p6z2jetrkfd7ljhw6cvblfopxe-story.html
[4] https://www.witn.com/content/news/Greenville-Police-credit-Shot-Spotter-for-lower-crime-stats--567247521.html
[5] https://www.chicagotribune.com/news/breaking/ct-met-superintendent-eddie-johnson-chicago-violence-20171116-story.html
[6] https://www.phillymag.com/news/2015/04/02/camden-reduces-gunfire-by-48-percent/
[7] https://www.thedenverchannel.com/news/crime/denver-police-to-test-shotspotter-system-in-4-different-neighborhoods-with-live-gunfire
[8] https://bakersfieldnow.com/news/local/is-shotspotter-working-in-bakersfield
[9] https://www.post-gazette.com/local/city/2018/03/14/Pittsburgh-City-Council-ShotSpotter-expansion-Wendell-Hissrich-North-Side-Jason-Lando-Darlene-Harris-Deborah-Gross/stories/201803140183

APPENDIX A: Surveillance Impact Report Requirements

The following section shows all Surveillance Impact Report requirements in order as defined by the San Francisco Administrative Code, Section 19B.

1. Information describing the Surveillance Technology and how it works, including product descriptions from manufacturers.

ShotSpotter uses acoustic sensors that are strategically placed in an array of approximately 20 sensors per square mile. These sensors are connected wirelessly to ShotSpotter's centralized, cloud-based application to reliably detect and accurately triangulate (locate) gunshots. Each acoustic sensor captures the precise time and audio associated with impulsive sounds that may represent gunfire. This data, from multiple sensors, is used to locate the incident, which is then filtered by sophisticated machine algorithms to classify the event as a potential gunshot. Expertly trained acoustic analysts, who are located and staffed in ShotSpotter's 24x7 Incident Review Center, then further qualify those highlighted incidents. These analysts ensure and confirm that the events are in fact gunfire. In addition, the analysts can append the alert with other critical intelligence such as whether a fully automatic weapon was fired and whether the shooter is on the move. This process typically takes no more than 45 seconds from the time of the actual shooting to the digital alert (with the precise location identified as a dot on a map) popping onto a screen of a computer in the 911 Call Center or on a police officer's smartphone or MDT (vehicle mobile display terminals) There are three components to the ShotSpotter system:
1. Gunshot Location Detection (GLD) Sensors: Sensors are installed in different coverage areas in San Francisco.
2. ShotSpotter Headquarters (HQ): Sensors send acoustic information to HQ where computer-based machine-learning algorithms are used to analyze the sound. If the sound and visual audio signature match gunfire, the incident file is then passed along to the Incident Review Center (IRC). Acoustic experts at the IRC review incidents within seconds and provide additional information (e.g. number of gunshots, number of guns, types of guns). Confirmed gunshots are pushed out to Communications (dispatch) as well as to the SFPD ShotSpotter software system within seconds.
3. The SFPD ShotSpotter Software System: This system is cloud-based and desktop-based; SFPD authorized personnel can use internet browsers to connect to the ShotSpotter system via SFPD computers. Certain authorized personnel use desktop applications that connect to the ShotSpotter system for more in-depth gunshot analysis.

ShotSpotter Inc. ("SST") is a California-based company that operates ShotSpotter Flex (hereafter referred to as "ShotSpotter"), a proprietary technology that uses sensors strategically placed around a geographic area to detect, locate, and analyze gunshots, and notify law enforcement. ShotSpotter is the most widely used gunshot detection technology in the United States, currently operating in more than 100 jurisdictions. SST's primary customers are local law enforcement agencies. ShotSpotter is gunshot detection technology that uses sophisticated acoustic sensors to detect, locate and alert law enforcement agencies and security personnel about illegal gunfire incidents in real-time. The digital alerts include a precise location on a map (latitude/longitude) with corresponding data such as the address, number of rounds fired, type of gunfire, etc. delivered to any browser-enabled smartphone or mobile laptop device as well as police vehicle MDC or desktop. This information is key to better protecting officers by providing them with increased tactical awareness. It also enables law enforcement agencies to better connect with their communities and bolsters their mission to protect and serve. The ShotSpotter system employs acoustic sensors strategically placed in specified areas (commonly referred to as a "coverage area.") When a gun is fired, the sensors detect the firing of the weapon. The audio triangulation of multiple installed sensors then pinpoints a gunfire location and sends the audio file and triangulation information to

ShotSpotter Headquarters (HQ) for gunshot verification. Verified gunshots and related information are then sent to SFPD in real-time so that SFPD may notify responding officers where guns were fired.

2. Information on the proposed purpose(s) for the Surveillance Technology.

The ShotSpotter system enables SFPD to be aware of gunshots in the absence of witnesses and/or reports of gunshots. The ShotSpotter system notifies SFPD of verified gunshot events, which allows SFPD to quickly respond to gunshots and related violent criminal activity. ShotSpotter expedites police and ambulance response rates to incidents involving illegal gunfire which expedite the location of victims, witnesses, evidence and suspects.

The Crime Gun Intelligence Center (CGIC) Unit conducts a re-canvass of ShotSpotter notifications when multiple gunshots are detected and cartridge cases are not recovered. Returning the following day to re-canvass the neighborhood may encourage witnesses to come forward and provide information as opposed to immediately following the shooting incident. The increased attention to the investigation of shots fired in the neighborhood may aid in building community trust.

3. If applicable, the general location(s) it may be deployed and crime statistics for any location(s).

Sensors are currently in the following neighborhoods: Bayview, Western Addition, Sunnydale/Visitation Valley, Bernal Dwellings/Bernal Heights, Potrero Hill and South of Market

4. An assessment identifying any potential impact on civil liberties and civil rights and discussing any plans to safeguard the rights of the public.

ShotSpotter acoustic sensors use ordinary microphones that are similar to ones found in cellphones. They are placed high above the street and are not positioned, tuned or specialized to pick up human voices. The sensors "listen" for gunshot-like sounds and trigger only when detecting an impulsive sound that is instantaneous and sharp. When at least three different sensors detect a gunshot-like sound at the same time and determine a location, they send a short audio snippet to ShotSpotter headquarters that includes 1 second of sound prior to the incident (to establish a baseline of ambient noise), the incident itself and 1 second after. Upon detecting a likely gunshot, trained ShotSpotter personnel listen to a short computer-generated audio snippet of the gunfire to double check that it is actually gunfire. It is highly unusual for a human voice to be included in a snippet. For this to occur, the voice must be loud enough to be heard over the gunfire. In addition, there is no personally identifiable information in any audio snippet.

Since 2012, only authorized ShotSpotter employees have access to audio from sensors, they can only access it under a strict set of conditions and can only provide police a short audio snippet.

In 2019 ShotSpotter commissioned an independent privacy audit by the Policing Project at NYU Law School. This end-to-end assessment conducted by objective privacy professionals concluded that ShotSpotter presents an "extremely low risk of audio surveillance". The Policing Project based this finding upon the short amount of audio that is temporarily stored on sensors, the short length of audio snippets that are permanently stored as evidence and the internal controls the company uses to restrict access to audio for authorized employees only.

Human voices and street noise will never trigger a sensor because they do not produce an instantaneous sharp sound and they are not loud enough to be picked up by three or more sensors. That being said, street noise that can include human voices could be captured by a sensor temporarily. All sensor audio, however, is permanently deleted after 30 hours and never heard by a human unless it was accompanied by a loud, impulse sound thought to be a gunshot. Live streaming of audio is not possible.

Technology and operational mitigations:

- ShotSpotter, not SFPD, is responsible for determining the location(s) for installation of acoustic sensors. Sensors are placed high above the ground typically on top of buildings or sometimes lampposts. At this height, there is more limited ability to pick up street level sounds clearly.
- The sensors are not capable of audio streaming – neither ShotSpotter nor SFPD can listen in on street level sounds in real-time.
- The system permanently deletes all audio that is temporarily stored on the sensor after 30 hours.
- The system only triggers an incident to send downstream when 3 or more sensors hear a loud, impulsive sound. Sensors cannot be triggered by human voices because voices are not impulsive enough or loud enough to be heard by 3 sensors which may be 800 meters or more apart. Thus, the audio of a human voice that may be captured by 1 sensor would be permanently deleted after 30 hours and no police or ShotSpotter employee will have heard that sound.
- If a sound is loud enough and sharp enough to possibly be a gunshot and is detected by 3 or more sensors and a location is able to be determined, the system pulls a short audio snippet of the sound plus 1 second of ambient noise prior to the incident and 1 second after. This audio is interpreted by a machine at first and then reviewed by an acoustic analyst at ShotSpotter Headquarters who is only presented with the audio snippet and is under significant time pressure to process the incident as either a gunshot or to dismiss as a non-gunshot and get on to the next incident. All incidents, whether determined to be a gunshot or non-gunshot, are permanently and securely stored in the cloud to serve as both evidence and to train the machine classifier in the future.
- ShotSpotter security protocols also mitigate gunshot detection data access. ShotSpotter does not provide extended audio to SFPD or any police agency; they will not provide this access even if requested. Additionally, ShotSpotter does not provide actual precise locations of the sensors to SFPD.
- As previously mentioned, the sensors are constantly listening for gunshot-like sounds and storing what is captured for 30 hours (was 72 hours before July 2019), and then deleting the data unless triggered to send the data to the ShotSpotter Cloud for analysis. The 30-hour buffer allows SFPD to request data within 24 hours in cases where gunshots have been identified by police but not picked up by the system or if there is a need to verify if there were other gunshots prior to the authenticated event.
- ShotSpotter policy stipulates that only a limited number of authorized forensic engineers can access the storage buffer of a sensor to retrieve prior recorded data within that 30-hour window and search for other gunshot impulsive sound events. To avoid listening to recorded data on a sensor in a haphazard way, the search for a missing gunshot is first done visually through a secure interface looking for the prevalence of electrical "pulses" strong enough to be a gunshot that occurred around the time of the incident in question.
- Upon receiving a gunshot alert SFPD authorized personnel may find that a voice has been recorded along with gunshot sound, but such voice data is only associated with the actual gunshot data and has no personally identifiable information built in. There is no way to tag any voice audio that is unintentionally recorded when connected to a gunshot.

5. Whether use or maintenance of the technology will require data gathered by the technology to be handled or stored by a third-party vendor on an ongoing basis.

Handled by third-party vendor, ongoing: true

Vendor name: ShotSpotter

Special data handling required: true

6. A summary of the experience, if any, other governmental entities have had with the proposed technology, including information about its effectiveness and any known adverse information about the technology such as anticipated costs, failures, or civil rights and civil liberties abuses.

Sample results reported from other cities:

- Oakland, CA: ShotSpotter Policy approved by the Oakland Privacy Commission in November 2019.
- Las Vegas Metro Police pilot report indicates 342 gunshot incidents were identified by ShotSpotter in first 9 months of use that the PD would not have known about and a 26% reduction in violent crime. Expanded coverage area to all known hotspots.
- Cincinnati cites a 48% reduction in shootings
- Newport News reports a 13% reduction in shootings with ShotSpotter
- Greenville, NC reports a 33% reduction in gun violence injuries using ShotSpotter
- Chicago cites a drop of over 40% in shootings in the Englewood District in the first year after installation
- Camden County, NJ–46% reduction in homicides by shooting
- Denver–103 arrests and 84-gun recoveries over the course of 3 years
- Bakersfield–22 arrests in first 9 months
- Pittsburgh – 48 arrests and 83 victims found with help of ShotSpotter in 3 years

APPENDIX B: SFPD District Stations Included in ShotSpotter Service Area

Southern Station (Company B)
Bayview Station (Company C)
Mission Station (Company D)
Northern Station (Company E)
Ingleside Station (Company H)
Tenderloin Station (Company J)

APPENDIX C: Firearm Homicide by District Station, year over year 9/20/2020

District	2019	2020
Central	0	1
Southern	1	1
Bayview	7	7
Mission	3	4
Northern	3	0
Park	0	0
Richmond	0	0
Ingleside	1	4
Taraval	0	0
Tenderloin	2	5
Total	**17**	**22**

APPENDIX D: Violent Crime Zone Identification, 2008 Report

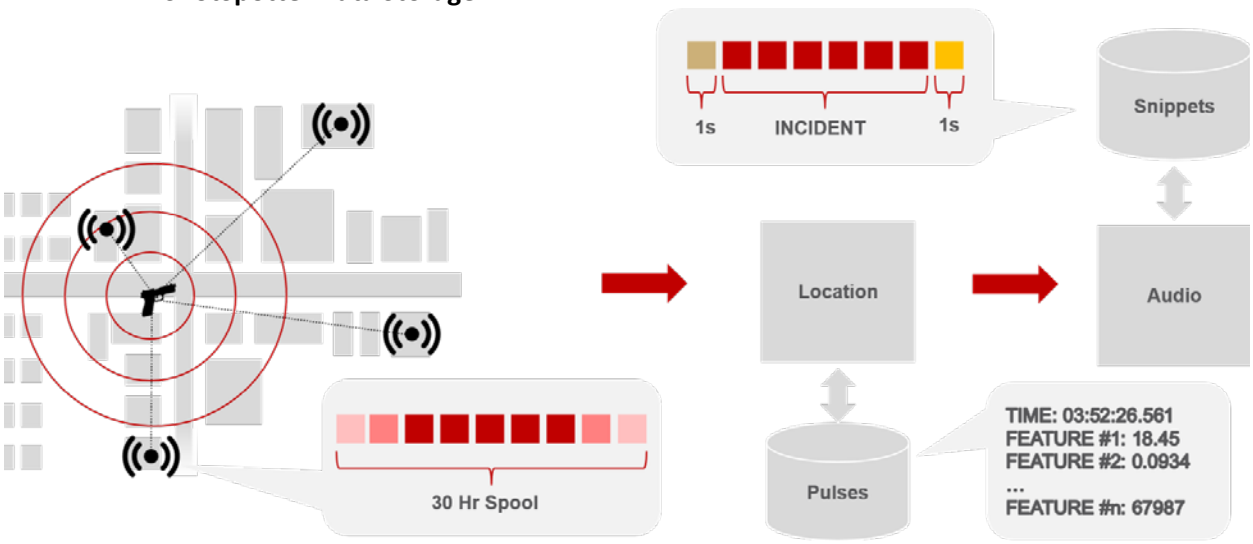
In 2008, SFPD's Crime Analysis Unit (CAU) identified five zones where the majority of violent crimes were taking place. The below five zones are included in the ShotSpotter Service Area.

- Zone 1: Tenderloin/SOMA
- Zone 2: Western Addition
- Zone 3: Mission District
- Zone 4: Bayview District
- Zone 5: Visitacion Valley

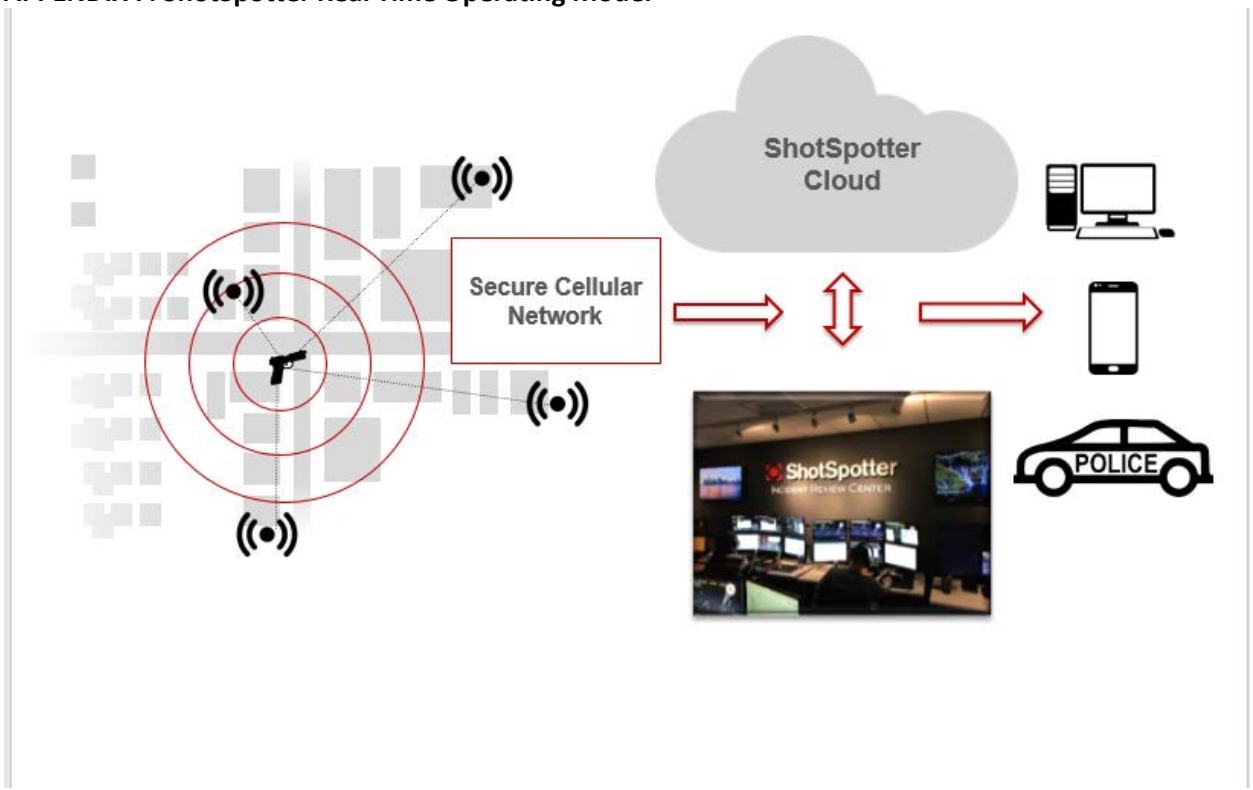
SFPD VIOLENT CRIME REDUCTION ZONES

Source: Violent Crime Reduction Strategy
Prepared by Crime Analysis Unit
08/20/2008

APPENDIX E: ShotSpotter Data Storage



APPENDIX F: ShotSpotter Real Time Operating Model



Surveillance Technology Policy

Audio Recorder - ShotSpotter, Inc. ("ShotSpotter")
San Francisco 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 ShotSpotter, Inc. ("ShotSpotter") 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

The Department's mission is: In order protect life and property, prevent crime and reduce the fear of crime, we will provide service with understanding, response with compassion, performance with integrity and law enforcement with vision.

The Surveillance Technology Policy ("Policy") defines the manner in which the ShotSpotter, Inc. ("ShotSpotter") will be used to support this mission, by describing the intended purpose, authorized and restricted uses, and requirements.

This Policy applies to all to department personnel that use, plan to use, or plan to secure ShotSpotter, Inc. ("ShotSpotter"), 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 ShotSpotter, Inc. ("ShotSpotter") technology for the Department is limited to the following use cases and is subject to the requirements listed in this Policy.

Authorized Use(s):

1. Gunshot detection: Record gunshot sounds and use sensors to locate the origin of the gunshots. Patrol Officers receive gunshot alerts to respond to crime scene.

2. Investigators use ShotSpotter Investigative Portal reports to find shell casing evidence on scene and to further analyze the incident.

All use cases not defined as an authorized use are prohibited.

A ShotSpotter alert will not, on its own, identify an individual, reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, information concerning an individual person's sex life or sexual orientation. Recordings of ambient noise, or any other sound outside of verified gunshots shall be prohibited for use in any investigation and shall not cause police enforcement.

Surveillance Oversight Review Dates
COIT Review: January 21, 2021
Board of Supervisors Review: TBD

BUSINESS JUSTIFICATION

ShotSpotter, Inc. ("ShotSpotter") supports the Department's mission and provides important operational value in the following ways:

The ShotSpotter system enables SFPD to be aware of gunshots in the absence of witnesses and/or reports to 911 of gunshots. The ShotSpotter system notifies SFPD of verified gunshot events, which expedites police and ambulance response rates to incidents involving illegal gunfire. ShotSpotter Alerts help SFPD locate victims, witnesses, evidence and suspects.

It shall be the policy of the SFPD to properly utilize ShotSpotter to enhance the Department's ability to respond to and investigate violent crimes involving illegal gunfire.

In addition, ShotSpotter, Inc. ("ShotSpotter") promises to benefit residents in the following ways:

☐	Education	
☐	Community Development	
☒	Health	Gun violence and its impacts are a public health concern. Preventing gun violence is an essential component to building health communities.
☐	Environment	
☒	Criminal Justice	ShotSpotter notifications help make the department aware of gunfire events they would have otherwise not have known about. In 2019, only 15% of SF gunfire incidents were called into 911. ShotSpotter alerts enable a fast, precise officer response to unreported gunfire to render aid to victims of a gunshot, secure critical evidence, and apprehend armed individuals.
☐	Jobs	
☐	Housing	
☐	Other	

ShotSpotter, Inc. ("ShotSpotter") will benefit the department in the following ways:

Benefit		Description
☐	Financial Savings	
☒	Time Savings	If a 911 caller reports a gunshot incident, it usually takes several minutes to capture and relay the information to officers often with imprecise data on the exact location. With ShotSpotter, officers receive alerts within 60 seconds of trigger pull with closest address

		data enabling a faster response to a crime scene to potentially save victims.
☒	Staff Safety	Officers can approach a crime scene more safely with ShotSpotter alerts knowing the precise location and time of the event and whether there are multiple shooters or high capacity weapons being used.
☒	Data Quality	Only 15% of gunshot incidents in SF have an accompanying 911 call (2019). Without ShotSpotter there would be no police response to 85% of gun crime representing over 850 incidents. However, with ShotSpotter, virtually all incidents are captured with an exact location enabling the department to better protect and serve the community.
☐	Other	

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 kept up to date and maintained.
Safety:	Surveillance technology must be operated in a safe manner. Surveillance technology should not be operated in a way that infringes on resident civil rights, including privacy, or causes personal injury or property damage.
Data Collection:	Departments shall minimize the use, collection, and retention of Personally Identifiable Information (PII) to what is strictly necessary to accomplish the intended purpose of the surveillance technology. Department shall only collect data required to execute the authorized use case. All data collected by the surveillance technology, including PII, shall be classified according to the City's Data Classification Standard. Should information be incidentally collected that is not necessary to accomplish the intended purpose of the surveillance technology, including information that may be used to identify persons or private information, Department shall remove all incidental PII from raw data.

Data types can take the form video, audio, still images. Data formats can take the form of XML, PDF, HTML, Plain Text, JPEG, etc.

The surveillance technology collects the following data types:

Data Type(s)	*Format(s)*	*Classification*
acoustic	.wav format	Level 3

Data Stored by ShotSpotter Related to Gunshot Incident

Data field	Explanation
o **ShotSpotter Incident ID**	Unique ShotSpotter incident ID
o **CAD ID**	Police Computer Aided Dispatch ID
o **Trigger date/time**	
o **Latitude**	Location data in relation to the gunshot incident: the angular distance of a place north or south of the earth's equator, usually expressed in degrees and minutes
o **Longitude**	Location data in relation to the gunshot incident: the angular distance of a place east or west of the meridian at Greenwich, England, or west of the standard meridian of a celestial object, usually expressed in degrees and minutes.
o **Incident Type/Classification**	Single Gunshot, Multiple Gunshot, Possible Gunshot
o **Number of rounds**	# shots fired
o **Dispatch address**	Reverse lookup of nearest street address from latitude/longitude using parcel data, Google
o **City and state**	
o **Area**	Beat/District
o **Audio Snippet**	Gunshot plus up to 1 second before and after to establish ambient noise level
o **Reviewer tags**	Manually entered data from a ShotSpotter incident reviewer for situational awareness such as multiple shooters, automatic weapon or high capacity weapon
o **Report**	Investigative Lead Summary that details location and sequence of shots fired

o **Comments**	Publishing time, acknowledgement from ShotSpotter Incident Review center; any modification to classification

Notification:	Publicly posted signage near the location of the technology is not feasible as the technology is not physically guarded and because of the intent of the technology to detect illegal gunfire the unguarded and unprotected technology is susceptible to vandalism and attempts to disable the intent of the technology.
Access:	All parties requesting access must adhere to the following rules and processes: Authorized personnel may access the browser-based ShotSpotter system via vehicle computers to only access the cloud-based system. SFPD members also have the option to activate ShotSpotter app on their Department issued mobile phones. Authorized personnel must always gain access through a login/password-protected system which records all login access. SFPD has no direct access to actual ShotSpotter sensors. Only ShotSpotter-specified support engineers can use a technology to access the data in the sensors prior to the 30-hour deletion period, if investigators need to search for previous gunshots. SFPD may request data within the first 24 hours, prior to the 30-hour deletion period. 1. Authorized personnel may access the ShotSpotter system via vehicle computers and receive notifications of verified ShotSpotter activations. SFPD may also notify authorized personnel of ShotSpotter activations. Authorized personnel may respond to such notifications based upon priorities as mandated by their supervisors. 2. The ShotSpotter system shall only be used for official law enforcement purposes. 3. Only specifically authorized personnel authorized by the Chief or Chief designee (e.g. personnel with SFPD's Investigations Division) will have access to historical ShotSpotter system data via desktop ShotSpotter system applications. The ShotSpotter system may be used for authorized patrol and investigation purposes. Contacting individuals at locations where ShotSpotter activations occur shall be conducted in accordance with applicable law and policy. 4. Accessing data collected by the ShotSpotter system requires a right to know and a need to know. A right to know is the legal authority to receive information pursuant to a court order, statutory law, or case law. A need to know is a compelling reason to request information such as direct involvement in an investigation or assignment to a unit which responds to gunshot calls (e.g. Patrol Division). 5. Members approved to access ShotSpotter system data may only use data for legitimate law enforcement purposes only, such as when the data relate to

gunshots, a specific criminal investigation or department-related civil or administrative action.

6. All verified ShotSpotter system activations are entered into SFPD's computer-aided dispatch (CAD) record management system (RMS) with ShotSpotter system specific ID numbers. Authorized personnel can then query the CAD/RMS system for any and all ShotSpotter system activations.

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. Employee Job Classification & Title: Individuals designated by the Chief or Chief-designee can include the following: Police Service Aide (PSA), PSA Supervisor, Police Officer, Sergeant, Lieutenant, Captain, Crime Analyst, Deputy Chief, Commanders, Assistant Chief, Chief of Police, Media Relations Unit members or specifically designated civilian staff.

- The Department and ShotSpotter

The following providers are required to support and maintains the surveillance technology and its associated data to ensure it remains functional:

- ShotSpotter

B. Members of the public

ShotSpotter data is classified as Level 3, Sensitive and public release is restricted, however each request submitted by a member of the public will be reviewed to determine whether the data can be released. SFPD shall comply with the requirements of the federal and State Constitutions, and federal and State civil procedure laws and rules.

Data Security:	To protect surveillance technology information from unauthorized access and control, including misuse, Departments shall, at minimum, apply the following safeguards: The Department must have a subscription to ShotSpotter system and only has access to Reviewed Alerts delivered via the Investigator Portal password-protected internet portal and user interface supplied by ShotSpotter. ShotSpotter has limited or eliminated audio access for several positions (including SST executives) whose access to audio was not essential. To address, deter and detect possible misuse, ShotSpotter requires supervisor approval before a ShotSpotter employee is permitted to download extended audio. For every instance in which a ShotSpotter employee accesses stored sensor audio, ShotSpotter requires its employees to document what audio was accessed, who accessed the audio, and who approved the download, the law enforcement officer making the request, and the evidentiary basis for the request. Supervisory personnel regularly review this

audit trail to ensure that audio is being accessed only when necessary and according to proper procedures. These regular reviews assess which law enforcement agencies may be using the process at a much higher rate, ShotSpotter personnel who listen to a significantly longer duration of audio, or other patterns that may require corrective action.

ShotSpotter's privacy policy can be accessed here: https://www.shotspotter.com/privacy-policy

Data Sharing:

SFPD will endeavor to ensure that other agencies or departments that may receive data collected by [the Surveillance Technology Policy that it operates] will act in conformity with this Surveillance Technology Policy.

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.

SFPD 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)

SFPD shall ensure all PII and restricted data is de-identified or adequately protected to ensure the identities of individual subjects are effectively safeguarded.

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 shared data will be done in a cost-efficient manner and exported in a clean, machine-readable format.

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

SFPD 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.

The Department currently participates in the following sharing practices:

A. Internal Data Sharing

Department shares the following data with the recipients:

- San Francisco District Attorney's Office
- San Francisco Public Defender's Office

Data sharing occurs at the following frequency:

- Frequency depends on cases/incidents

B. External Data Sharing

Department shares the following data with the recipients:

- CGIC Partners
- US Attorney.
- ShotSpotter data will only be shared with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law.

Data sharing occurs at the following frequency:

- As-needed

To ensure that entities receiving data collected by the surveillance technology comply with the Surveillance Technology Policy, Department shall:

- Direct the request to ShotSpotter. ShotSpotter may offer redacted data that complies with the Right to Know Law Request and/or Open Public Records Act/Freedom of Information Act, ShotSpotter and its confidential, proprietary Data and records are protected under the exemptions expressly defined in the Public Records Act, Evidence Code and California Civil Code as follows:

ShotSpotter gunfire alert Data and records are a trade secret, and are exempt from disclosure pursuant to Evidence Code section 1060 which refers to subdivision (d) of Section 3426.1 of the California Civil Code for the definition of trade secret, as follows:

ShotSpotter keeps the gunfire alert Data and records confidential and secret by not releasing them to the public and by including Data restriction rights and confidentiality clauses in all customer agreements. Further, locations of specific sensors, gunshots at or near specific locations, and actual locations of areas covered is a matter of public safety and will not be released under any conditions.

Additionally, the data is protected as some or all can be involved in on-going criminal investigations.

Data Retention:	Department may store and retain raw PII data only as long as necessary to accomplish a lawful and authorized purpose. Please list data retention schedules based on the following categories: • Permanent records (i.e., records that are essential): shall be retained and preserved indefinitely • Current records (i.e., records for operational necessity, ready reference, convenience): record retention schedules may vary but generally less than 10 years • Storage records (i.e., records retained offsite): record retentions may vary but generally less than 10 years • Criminal Investigative file retention schedule is subject to evidence laws, CA penal code and statute of limitations. The Department's data retention period and justification are as follows: • ShotSpotter: The sensors delete all acoustic data after 30 hours unless the gunshot-like impulsive acoustic event sends the data to ShotSpotter for analysis. Only verified gunshot data (all impulsive acoustic events loud enough to be heard by multiple sensors and where a location can be calculated) is maintained in perpetuity, both by ShotSpotter HQ as well as on SFPD desktop applications. ShotSpotter does not collect PII data and as such PII data shall not be kept in a form which permits identification of data subjects. ShotSpotter maintains verified gunshot data indefinitely. • SFPD: Records shall be purged according to the current San Francisco Police Department Records Retention and Destruction Schedule which calls for destruction of intelligence files every two years from the last date of entry with the following exceptions: a) a. Information may be maintained if it is part of an ongoing investigation or prosecution. b) b. All written memoranda requesting authorization to commence an investigation and subsequent authorizations shall be maintained for not less than five years after termination of the investigation.

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

It shall be the policy of the SFPD that once the requisite retention period for a record has passed, the record shall be destroyed unless there are particular circumstances that dictate that the record be retained.

It shall be the policy of the SFPD to work with contractors providing off-site storage of records to ensure that records are destroyed once the requisite time period for retention has passed

Data will be stored in the following location:

- ☐ Local storage
- ☐ Department of Technology Data Center
- X Software as a Service Product
- ☐ Cloud Storage Provider

Access to ShotSpotter Historical Incidents if Contract is Terminated:

SFPD has access to and the ability to download historical data at any time during the term of the Agreement using the Investigator Portal. Per the service contract with ShotSpotter, SFPD may not, without the prior written consent of ShotSpotter, merge, combine integrate or bundle the Software or the Data, in whole or in part, with other software, hardware, data, devices, systems, technologies, products, services, functions or capabilities. If/When the Department desires to terminate the ShotSpotter contract, SFPD may follow the process as set forth by ShotSpotter, to request to own the service area's historical data. The associated cost may require the Department to submit a request through the city and county's budget process.

This data shall be subject to the retention period as stated above.

Data Disposal:

Upon completion of the data retention period, Department shall dispose of data in the following manner:

Practices: Audio is only temporarily stored (30 hours), and then a very select amount of audio is retained only if the computer algorithm or human reviewer detects an impulsive acoustic event loud enough to be heard by multiple sensors and where a location can be calculated. All other audio is routinely purged from ShotSpotter's systems.

Processes and Applications: The ShotSpotter real-time Incident Review Center (IRC) will review at least 90% of all gunfire incidents within 60 seconds. This human review is intended to confirm or change the machine classification of the incident type, and, depending on the reviewer's confidence level that the incident is or may be gunfire, will result in an alert ("Reviewed Alert") sent to the Customer's dispatch center, patrol car mobile data terminals (MDT), and officer

	smartphones (via the ShotSpotter App), based on the following criteria: High confidence incident is gunfire; If uncertain an incident is gunfire, it is published as Probable Gunfire.
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 must receive training on data security policies and procedures. The ShotSpotter Gun Shot Detection Program Manager shall oversee the training program for any members with access to the ShotSpotter system and data.

CONSIDERATIONS FOR SERVICE AREA EXPANSION

The current service area was defined in part by a Violent Crime Reduction Strategy report prepared by SFPD's Crime Analysis Unit(CAU) in 2008. This report determined areas that experienced highest incidences of gun violence and identified five crime reduction zones. SFPD created a Zone Enforcement Strategy based on a study titled "Police Innovation and Crime Prevention: Lessons Learned from Police Research over the Past 20 Years" by Anthony A. Braga, Ph.D. and Davis L. Weisenburd Ph.D. The Zone Enforcement Strategy focused on deploying resources in identified zones to reduce or mitigate crime. ShotSpotter's service area which covers the areas identified in the study.

The Investigations Bureau along with the CAU will continue to review the weekly citywide shooting logs and the annual ShotSpotter report to determine whether there is a year over year increase, over a period of three years, in fatal and non-fatal shooting incidents in non-service areas. If there is a sustained increase in shootings in the non-service area, the Investigations Bureau will make a recommendation to the Chief of Police to consider expanding the ShotSpotter Service Area.

ANNUAL PUBLIC REPORTING

SFPD shall issue an annual gun violence report which will include ShotSpotter data. The first annual report will be issued on February 1, 2022 and will be issued on the 1st day of February every year, thereafter. The report will be posted on the SFPD public website, through San Francisco Open Data- DataSF and if requested, will be reported to the Police Commission on an annual basis.

The current SFPD Gun Violence Report lists the following data sets:

- Year-to-date gunfire numbers (four previous years and current YTD)
- Number of shooting victims (non-fatal)
- Number of Homicides with Firearm
- Total Number of Gun Violence Victims

The Annual ShotSpotter report may also include the following:

- Number of SFPD responses due to ShotSpotter alerts only

- Number of SFPD responses due to 911 calls only
- Number of SFPD responses due to ShotSpotter and 911 calls
- Total number of ShotSpotter incidents in coverage area
- Year-end gunfire event totals per District Station

COMPLIANCE

Department shall oversee and enforce compliance with this Policy using the following methods:

Surveillance Technology Policies shall have the same compliance requirements as all Department Written Directives and Police Commission Resolutions.

Department shall assign the following personnel to oversee Policy compliance by the Department and third-parties:

Deputy Chief of Investigations and the Commander of Investigations in addition, each member of the Department belongs to a chain of command. The Officer in Charge (OIC) of that chain of command is responsible for overseeing compliance with all SFPD written directives and the surveillance technology polices. 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.

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. 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 DPA. Depending on the severity of the allegation of misconduct, the Chief or the DPA 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.

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.

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 a surveillance technology that has not been processed and cleaned of all personal identifiable information. The distribution and use of raw data is tightly restricted.
Exigent Circumstances	An emergency involving imminent danger of death or serious physical injury to any person that requires the immediate use of Surveillance Technology or the information it provides.
Trade Secret	"Trade secret" means information, including a formula, pattern, compilation, program, device, method, technique, or process, that: 1.) Derives independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use; and 2.) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

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

Public:

Members of the public can register complaints about SFPD activities with the Department of Police Accountability (DPA). 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.

Department shall acknowledge and respond to concerns in a timely and organized response. To do so, Department shall:

Update the SFPD public website to include surveillance technology policies and will include a general email for public inquiries. The general email box will be assigned to a staff member 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.

APPENDIX A: Surveillance Technology Policy Requirements

The following section shows all Surveillance Technology Policy requirements in order as defined by the San Francisco Administrative Code, Section 19B.

1. A description of the product and services addressed by the Surveillance Technology, including the identity of any provider(s) whose services are essential to the functioning or effectiveness of the Surveillance Technology equipment or services for the intended purpose.

ShotSpotter manages the cloud-based service with a subscription service which provides the SFPD with access to the following:

- Gunshot Alerts
- Apps for Dispatch, Patrol Officers, Investigators, and District Station Personnel
- Incident Review Center
- Investigative Lead Summary
- Investigator Portal
- Detailed Forensic Report

ShotSpotter Inc. is a California-based company that operates ShotSpotter Flex, a proprietary technology that uses sensors strategically placed around a geographic area to detect, locate, and analyze gunshots, and notify law enforcement. ShotSpotter is the most widely used gunshot detection technology in the United States, currently operating in nearly 100 jurisdictions across the country.

ShotSpotter uses acoustic sensors that are strategically placed in an array of approximately 20 sensors per square mile. These sensors are connected wirelessly to ShotSpotter's centralized, cloud-based application to reliably detect and accurately triangulate (locate) gunshots. Each acoustic sensor captures the precise time and audio associated with impulsive sounds that may represent gunfire. This data, from multiple sensors, is used to locate the incident, which is then filtered by sophisticated machine algorithms to classify the event as a potential gunshot. Expertly trained acoustic analysts, who are located and staffed in ShotSpotter's 24x7 Incident Review Center, then further qualify those highlighted incidents. These analysts ensure and confirm that the events are in fact gunfire. In addition, the analysts can append the alert with other critical intelligence such as whether a full automatic weapon was fired and whether the shooter is on the move. There are three components to the ShotSpotter system:
1. Gunshot Location Detection (GLD) Sensors: Sensors are installed in different coverage areas in San Francisco.

2. ShotSpotter Headquarters (HQ): Sensors send acoustic information to HQ where computer-based machine-learning algorithms are used to analyze the sound. If the sound and visual audio signature match gunfire, the incident file is then passed along to the Incident Review Center (IRC). Acoustic experts at the IRC review incidents within seconds and provide additional information (e.g. number of gunshots, number of guns, types of guns). Confirmed gunshots are pushed out to Communications (dispatch) as well as to the SFPD ShotSpotter software system within seconds.

3. The SFPD ShotSpotter Software System: This system is cloud-based and desktop-based; SFPD authorized personnel can use internet browsers to connect to the ShotSpotter system via SFPD computers. Certain authorized personnel use desktop applications that connect to the ShotSpotter system for more in-depth gunshot analysis.

2. A description of the purpose(s) for which the Surveillance Technology equipment or services are proposed for acquisition, including the type of data that may be collected by the Surveillance Technology equipment or services.

Technology Use:
The ShotSpotter system enables SFPD to be aware of gunshots in the absence of witnesses and/or reports to 911 of gunshots. The ShotSpotter system notifies SFPD of verified gunshot events, which expedites police and ambulance response rates to incidents involving illegal gunfire which will help locate victims, witnesses, evidence (casings, bullets, blood etc.,) and suspects.

PII:
false

3. The uses that are authorized, the rules and processes required prior to such use, and uses of the Surveillance Technology that will be expressly prohibited.

Authorized Uses:

Gunshot detection: Record gunshot sounds and use sensors to locate the origin of the gunshots.

3.) Patrol Officers receive gunshot alerts to respond to crime scene.
4.) Investigators use ShotSpotter reports to find shell casing evidence on scene and to further analyze the incident .

Rules:
Prohibited Uses:
1. Unauthorized members using an authorized members log in to access historical ShotSpotter system data via desktop ShotSpotter system applications.

2. Using the ShotSpotter system for anything other than official law enforcement purposes.

3. Using ambient noise or any other sound outside of verified gunshots for use in any investigation.

4. Authorized members accessing data collected by the ShotSpotter system absent a right to know and a need to know. A right to know is the legal authority to receive information pursuant to a court order, statutory law, or case law. A need to know is a compelling reason to request information such as direct involvement in an investigation or assignment to a unit which responds to gunshot calls (e.g. Patrol Division).

5. Authorized members approved to access ShotSpotter system data using data for illegitimate purposes

4. A description of the formats in which information collected by the Surveillance Technology is stored, copied, and/or accessed.

Data Type	Formats STP
acoustic	.wav format Mp3

5. The specific categories and titles of individuals who are authorized by the Department to access or use the collected information, including restrictions on how and under what circumstances data collected with Surveillance Technology can be analyzed and reviewed, and the rules and processes required prior to access or use of the information.

Employee Job Classification & Title: Individuals designated by the Chief or Chief-designee can include the following: Police Service Aide (PSA), PSA Supervisor, Police Officer, Sergeant, Lieutenant, Captain, crime analyst, Deputy Chief, Commanders, Assistant Chief, Chief of Police, Media Relations Unit members or specifically designated civilian staff.

1. Authorized personnel may access the ShotSpotter system via vehicle computers and receive notifications of verified ShotSpotter activations. SFPD may also notify authorized personnel of ShotSpotter activations. Authorized personnel may respond to such notifications based upon priorities as mandated by their supervisors.

2. The ShotSpotter system shall only be used for official law enforcement purposes.

3. Only specifically authorized personnel authorized by the Chief or Chief designee (e.g. personnel with SFPD's Investigations Division) will have access to historical ShotSpotter system data via desktop ShotSpotter system applications. The ShotSpotter system may be used for authorized patrol and investigation purposes. Contacting individuals at locations where ShotSpotter activations occur shall be conducted in accordance with applicable law and policy.

4. Accessing data collected by the ShotSpotter system requires a right to know and a need to know. A right to know is the legal authority to receive information pursuant to a court order, statutory law, or case law. A need to know is a compelling reason to request information such as direct involvement in an investigation or assignment to a unit which responds to gunshot calls (e.g. Patrol Division).

5. Members approved to access ShotSpotter system data may only use data for legitimate law enforcement purposes only, such as when the data relate to gunshots, a specific criminal investigation or department-related civil or administrative action.

6. All verified ShotSpotter system activations are entered into computer-aided dispatch (CAD) record management system (RMS) with ShotSpotter system specific ID numbers. Authorized personnel can then query the CAD/RMS system for any and all ShotSpotter system activations.

Department:
SFPD and ShotSpotter
If applicable, contractor or vendor name:
ShotSpotter

Rules and processes required prior to data access or use:

The department must have a subscription to ShotSpotter system and only has access to Reviewed Alerts delivered via the Investigator Portal password-protected internet portal and user interface supplied by ShotSpotter.

ShotSpotter has limited or eliminated audio access for several positions (including SST executives) whose access to audio was not essential. To address, deter and detect possible misuse, ShotSpotter requires supervisor approval before a ShotSpotter employee is permitted to download extended audio. For every instance in which a ShotSpotter employee accesses stored sensor audio, ShotSpotter requires its employees to document what audio was accessed, who accessed the audio, and who approved the download, the law enforcement officer making the request, and the evidentiary basis for the request. Supervisory personnel regularly review this audit trail to ensure that audio is being accessed only when necessary and according to proper procedures. These regular reviews assess which law enforcement agencies may be using the process at a much higher rate, ShotSpotter personnel who listen to a significantly longer duration of audio, or other patterns that may require corrective action.

ShotSpotter's privacy policy can be accessed here: https://www.shotspotter.com/privacy-policy

6. The general safeguards that protect information from unauthorized access, including encryption and access control mechanisms.

Only authorized and trained personnel are permitted access to the system. The system always requires user and password ID for login. Furthermore, only personnel specifically designated by the Chief or Chief-designee have access to the system desktop applications which provide access to any historical downloadable data Authorized personnel may access the ShotSpotter system via vehicle computers and receive notifications of verified ShotSpotter activations. All verified ShotSpotter system activations are entered into SFPD's computer-aided dispatch (CAD) record management system (RMS) with ShotSpotter system specific ID numbers. Authorized personnel can then query the CAD/RMS system for any and all ShotSpotter system activations. The ShotSpotter verified activations entered into CAD/RMS require personnel to have level two CAD access which must adhere to the California Law Enforcement Telecommunications System (CLETS) guidelines.

7. The limited time period, if any, that information collected by the Surveillance Technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s) enumerated in the Surveillance Technology Policy, the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond that period

Retention:
ShotSpotter: The sensors delete all acoustic data after 30 hours unless the gunshot-like impulsive acoustic event sends the data to ShotSpotter for analysis. All impulsive acoustic events loud enough to be heard by three or more sensors and where a location can be calculated are maintained in perpetuity, both by ShotSpotter HQ as well as on SFPD desktop applications.
SFPD: Records shall be purged according to the current San Francisco Police Department Records Retention and Destruction Schedule which calls for destruction of intelligence files every 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 written memoranda requesting authorization to commence an investigation and subsequent authorizations shall be maintained for not less than five years after termination of the investigation.
c. Records showing violation of these guidelines shall not be destroyed or recollected for the purpose of avoiding disclosure.

Reason for retention:
ShotSpotter policy and SFPD retention schedule.
Deletion process:
It shall be the policy of the SFPD that once the requisite retention period for a record has passed, the record shall be destroyed unless there are particular circumstances that dictate that the record be retained. It shall be the policy of the SFPD work with contractors providing off-site storage of hardcopy records to ensure that records are destroyed once the requisite time period for retention has passed.

Retention exemption conditions:
ShotSpotter maintains all impulsive events loud enough to be heard by three or more sensors and where a location can be calculated indefinitely.

8. How collected information can be accessed or used by members of the public, including criminal defendants

Will the data be accessible to the public:

Members of the public and media may submit a public information request to the Department, however, ShotSpotter keeps the gunfire alert data and records confidential and secret by not releasing them to the public and by including Data restriction rights and confidentiality clauses in all customer agreements. Further, locations of specific sensors, gunshots at or near specific locations, and actual locations of areas covered is a matter of public safety and will not be released under any conditions. Additionally, the data is protected as some or all can be involved in on-going criminal investigations.

Criminal defendants may request to access the ShotSpotter data per the rules of criminal procedure around discovery and inspection. Accessibility will be determined by the courts.

How it can be requested by members of the public: https://www.sanfranciscopolice.org/get-service/public-records-request

9. Which governmental agencies, departments, bureaus, divisions, or units that may receive data collected by the Surveillance Technology operated by the Department, including any required justification or legal standard necessary to share that data and how it will ensure that any entity receiving such data complies with the Surveillance Technology Policy.

Name of agency: San Francisco District Attorney's Office, San Francisco Public Defender's Office, US Attorney, CGIC Partners, City Attorney. ShotSpotter data will only be shared with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law.
Justification: Law Enforcement purposes/on-going criminal investigations or prosecutorial process.

10. The training required for any individual authorized to use the Surveillance Technology or to access information collected by the Surveillance Technology

Training required:
true
Description of training:
The ShotSpotter Gun Shot Detection Program Manager shall oversee the training program for any members with access to the ShotSpotter system and data. Additionally, the Manager shall ensure all members with access have reviewed the Surveillance Technology Policy for ShotSpotter.

11. The mechanisms to ensure that the Surveillance Technology Policy is followed, including internal personnel assigned to ensure compliance with the policy, internal recordkeeping of the use of the technology or access to information collected by the technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the sanctions for violations of the policy

Process for responding to complaints from members of the public:
The Department of Police Accountability (DPA), by Charter authority, receives and manages all citizen complaints relating to the police department.
Complaints that come to the Department from members of the public will be forwarded to the DPA.
Oversight process:
Should a violation of ShotSpotter occur, San Francisco Police Department will conduct an internal investigation though the Chief of Staff/Internal Affairs (IA) Unit. The results of the investigation will be reported to the Chief of Police, who will consider in determining the charges 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

DPA. Depending on the severity of the allegation of misconduct, the Chief or the DPA may elect to file charges with the Police Commission. Any discipline sought must be consistent with principles of just cause and progressive discipline.

Compliance personnel titles:
SFPD Investigations Commander and Deputy Chief, SFPD and ShotSpotter. In addition, each member of the Department belongs to a chain of command. The Officer in Charge (OIC) of that chain of command is responsible for overseeing compliance with all SFPD policies.

Restrictions:
1. Authorized personnel may access the ShotSpotter system SFPD may also notify authorized personnel of ShotSpotter activations. Authorized personnel may respond to such notifications based upon priorities as mandated by their supervisors.
2. The ShotSpotter system shall only be used for official law enforcement purposes.
3. Only specifically authorized personnel authorized by the Chief or Chief designee (e.g. personnel with SFPD's Investigations Division) will have access to historical ShotSpotter system data via desktop ShotSpotter system applications. The ShotSpotter system may be used for authorized patrol and investigation purposes. Contacting individuals at locations where ShotSpotter activations occur shall be conducted in accordance with applicable law and policy.
4. Accessing data collected by the ShotSpotter system requires a right to know and a need to know. A right to know is the legal authority to receive information pursuant to a court order, statutory law, or case law. A need to know is a compelling reason to request information such as direct involvement in an investigation or assignment to a unit which responds to gunshot calls (e.g. Patrol Division).
5. Members approved to access ShotSpotter system data may only use data for legitimate law enforcement purposes only, such as when the data relate to gunshots, a specific criminal investigation or department-related civil or administrative action.
6. All verified ShotSpotter system activations are entered into SFPD's computer-aided dispatch (CAD) record management system (RMS) with ShotSpotter system specific ID numbers. Authorized personnel can then query the CAD/RMS system for any and all ShotSpotter system activations.

12. What procedures will be put in place by which members of the public can register complaints or concerns, or submit questions about the deployment or use of a specific Surveillance Technology, and how the Department will ensure each question and complaint is responded to in a timely manner.

Complaint procedures:
Complaints from members of the public will be forwarded to the Department of Police Accountability(DPA) for investigation. DPA manages complaint responses.
Departmental follow-up process:
DPA manages the complaint follow- up process. Surveillance Technology Policies will have the same procedural authority as any Departmental Written Directive. Non-compliance can result in progressive discipline or sustained complaints.
Members of the public can register complaints with the Department of Police Accountability https://sfgov.org/dpa/complaints. *Members of the public can register questions and concerns or submit questions via calls or emails at 311.org.*

Allegation procedures:

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

Surveillance Impact Report

San Francisco International Airport
Automated License Plate Readers (ALPR) – Ground Transportation Management System (GTMS)

As required by San Francisco Administrative Code, Section 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 Automated License Plate Readers ("ALPR") – Ground Transportation Management System ("GTMS").

DESCRIPTION OF THE TECHNOLOGY

The Department's ("Airport") mission is to provide an exceptional airport service to our communities.

In line with its mission, the Airport has historically used electronic toll readers and other technologies to monitor commercial ground transportation activity at the Airport. The PIPS Technology™ ("PIPS") ALPR - GTMS solution serves as a secondary source of ensuring commercial ground transportation database information is correct. This is an essential component of a comprehensive and efficient transportation system. Ground transportation activity at the Airport continues to grow in line with air passenger activity. In FY2019, there were over 6,500 (non TNC) vehicles permitted to operate at the Airport, with almost 3,000,000 pickups and drop-offs completed. The primary use for Landside ALPR - GTMS is to capture the activity of permitted commercial ground transportation at the Airport. The ALPR - GTMS acts as a failsafe if the Automated Vehicle Identification (AVI) readers malfunction and fails to read the transponder the Airport affixes to certain types of permitted vehicles. It assists in dispute resolution in the event that the operator challenges the transponder data (i.e., number of trips the operator has made to the Airport) collected from the AVI. Additional uses include tracking permitted operators that are not issued transponders, such as TNC vehicles and long-distance bus carriers; tracking unpermitted operators who solicit passengers for rides; and assisting public safety agencies in investigations.

Airport shall use ALPR - GTMS only for the following authorized purposes:

Authorized Use(s):

1. Tracking the activity of permitted commercial ground transportation at the Airport. Also used as a secondary method for collecting trip fees in the event an operator's transponder fails to read.
2. To support the Airport and local, state, federal, and regional public safety departments in the identification of vehicles associated with targets of investigations, including locating stolen, wanted, and or other vehicles that are the subject of investigation; and/or locating victims, witnesses, suspects, and others associated with a law enforcement investigation.

Any use(s) not identified in the Authorized Use(s) above are strictly prohibited.

Surveillance Oversight Review Dates

COIT Review: February 4, 2021
Board of Supervisors Review: TBD

Technology Details

The following a is product description of ALPR - GTMS

The Landside division currently has one (1) P357, side-fire camera and (20) 3M PIPS P392+ Spikelet cameras. P392 Spikelet is a fully-integrated number plate recognition unit incorporating camera (s), illuminator and data and image processing within a single sealed enclosure. The unit comprises a monochrome camera surrounded by two sets of infrared LEDs. PIPS patented filter/flash technique provides suppression of headlights and bright sunlight. Field-by-field control of camera parameters allows the use of patented 'triple flash' technique to reduce any problems of plate to plate variability.

A. How It Works

To function, ALPR - GTMS technology automates the processing of vehicle license plate information by transforming license plate images into alphanumeric characters with optical recognition software and storing those images, plate information and related metadata, including time and geo-location information. ALPR - GTMS:

- uses specially designed cameras mounted on gantries at the airport's entry points to capture digital images of approaching vehicles as they drive into the airport. The database records images and compares them with known operators;
- transforms the images into alphanumeric characters with optical character recognition (OCR) software;
- stores the images, plate information, and related metadata in a restricted-access database;
- compares the transformed license plate characters to databases of AVI reads for billing purposes; and
- archives photo evidence and metadata in support of citations (issued by the Airport's Ground Transportation Unit for vehicles violating the Airport's Rules and Regulations) issued ("hits") according to evidence retention standards consistent with City and State law.

All data collected or processed by ALPR - GTMS will be handled or stored by an outside provider or third-party vendor on an ongoing basis. Specifically, data will be handled by IBI Group, LLC to ensure the Airport may continue to use the technology.

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:

A. The benefits of the surveillance technology outweigh the costs.
B. The Airport's Policy safeguards civil liberties and civil rights.
C. 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 Airport'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 Airport's use of ALPR - GTMS has the following benefits for the residents of the City and County of San Francisco:

☐	Education	
☐	Community Development	
☐	Health	
X	Environment	Traffic congestion studies: ALPR - GTMS can be used to conduct studies on traffic volumes and patterns, with the potential to mitigate environmental impacts of traffic congestion on residents.
X	Criminal Justice	ALPR - GTMS can be used to support identification of vehicles as a part of law enforcement investigations.
☐	Jobs	
☐	Housing	
X	Other	Public Safety: ALPR - GTMS can be used to locate stolen, wanted, and or other vehicles that are the subject of investigation, and can improve overall roadway safety for residents using Airport roadways. Trip fees by permitted operators: ALPR - GTMS can be used to track vehicles and collect trip fees to offset impacts of commercial vehicles on Airport roadways and to improve roadway conditions for residents accessing the Airport.

B. Civil Rights Impacts and Safeguards

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

Administrative

- Commercial ground transportation operators acknowledge notice of GTMS policies and procedures, which include the Airport's use of ALPR and Electronic Toll Readers, by signing the Airport permit. In addition, in compliance with California Civil Code § 1798.90.5, the Airport shall notify the public of the ALPR – GTMS surveillance technology operation by posting the ALPR – GTMS privacy and usage policy on FLYSFO.
- Policies and procedures applicable to all Airport employees.

- SFO ITT team has documented polices regarding cybersecurity, networks and servers, and computer and software usage.
- Training provided to all Airport software users, including in-person or virtual training session that includes system overview and use of reporting modules.

Technical

- All network equipment and servers containing sensitive data are maintained in a secured location and accessible only to Airport badged, authorized personnel.
- Servers and network equipment are continuously monitored.
- ITT maintains a log of successful and unsuccessful logon attempts, changes in user accounts, whether user logs have been modified, network threats, and resource access.
- All SFO workstations and servers are patched regularly.
- All data stored on the servers are backed up regularly and a copy saved offsite.
- SFO's network is protected behind a firewall and data transmitted outside SFO's network to SFO cloud-based partners are encrypted via SSL/TLS. Data at rest offsite are also encrypted.

Physical

All Electronic Toll Readers and ALPRs are installed within locked equipment enclosures. Access to the enclosures is limited to Airport badged, authorized service technicians with SFO's ITT Tech Shop or TransCore, LP.

C. Fiscal Analysis of Costs and Benefits

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

Benefit		Description
☐	Financial Savings	
X	Time Savings	Without the ALPR - GTMS technology, the Airport would need to deploy a manually staffed ground transportation operation. This alternative has not been thoroughly explored for feasibility. At minimum however, team members would be required to be assigned to all entry lanes, exit lanes, curbside zones, and staging lots during 24/7 operations. Team members would conduct manual verification of registration through visual observance of permits and decals, and conduct traffic counts. The ALPR - GTMS removes the necessity of staffing for this purpose.
☐	Staff Safety	

X	Data Quality	The ALPR - GTMS technology is verified against the AVI technology to verify that all permitted vehicles' trips have been documented for tracking and fee assessment purposes, in case the AVI malfunctions and fails to read the airport affixed transponder. The ALPR - GTMS is also used in concert with AVI to confirm whether a commercial vehicle on Airport roadways is a permitted operator.
X	Other	The ALPR - GTMS technology enables the Airport to assess trip fees on permitted Commercial ground transportation operators. In 2019, the Airport collected a total of $64,815,649 in trip fees from ground transportation operators.

Number of FTE (new & existing)	0.10 Existing		
Classification	7318 Electronic Maintenance Technician (Support)		
	Annual Cost	***Years***	***One-Time Cost***
Total Salary & Fringe	$17,286	1	-
Software		-	-
Hardware/Equipment	*$0* *Break/Fix included in the GTMS Support contract*		$241,560 (15 PIPS Technology™ cameras, power supply, and enclosures)
Professional Services	*$340,000* *(GTMS Support, includes ALPR-GTMS)*	*1*	$8,261,227 (One-time cost to implement GTMS, includes ALPR-GTMS)
Training	-	-	-
Other	$250,000	1	$250,000
Subtotals	$607,286		$19,846,051
Total Cost	*$20,453,337 with 1 Year Recurring Cost*		

2.1 Please disclose any current or potential sources of funding (e.g. potential sources = prospective grant recipients, etc.). [SIR, ASR]
• Ongoing Support = Annual Airport Opex Budget • Future Lifecycle Refresh = Airport Capex Budget

The Airport funds its use and maintenance of the surveillance technology through:

Ongoing Support = Annual Airport Opex Budget Future Lifecycle Refresh = Airport Capex Budget.

COMPARISON TO OTHER JURISDICTIONS

ALPR - GTMS are currently utilized by other governmental entities for similar purposes.

APPENDIX A: Mapped Crime Statistics

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

The technology is deployed at various airport roadways and inspection areas, six (6) locations, including:

- Domestic and International Terminals, inbound roadways, departures, and arrivals level
- North Access Road
- Ground Transportation Unit inspection area

Surveillance Technology Policy

San Francisco International Airport
Automated License Plate Readers (ALPR) – Ground Transportation Management System (GTMS)

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 Automated License Plate Readers ("ALPR") – Ground Transportation Management System ("GTMS") 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

The Department's ("SFO" or "Airport") mission is to provide an exceptional airport in service to our communities.

The Surveillance Technology Policy ("Policy") defines the manner in which the ALPR – GTMS will be used to support this mission, by describing the intended purpose, authorized and restricted uses, and requirements.

This Policy applies to all to department personnel that use, plan to use, or plan to secure ALPR – GTMS, 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 ALPR – GTMS technology for the Department is limited to the following use cases and is subject to the requirements listed in this Policy.

Authorized Use(s):

1. To track the activity of permitted commercial ground transportation at the Airport. Also used as a secondary method for collecting trip fees in the event an operator's transponder fails to read.
2. To support the Airport and local, state, federal, and regional public safety departments in the identification of vehicles associated with targets of investigations, including locating stolen, wanted, and or other vehicles that are the subject of investigation; and/or locating victims, witnesses, suspects, and others associated with a law enforcement investigation.

Prohibited use cases include any uses not stated in the Authorized Use Case section.

Departments may use information collected only for legally authorized purposes, and may not use that information to unlawfully discriminate against people based on race, ethnicity, political opinions, religious or philosophical beliefs, trade union membership, gender, gender identity, disability status, sexual orientation or activity, or genetic and/or biometric data. Additionally,

departments may not use automated systems to scan footage and identify individuals based on any of the categories listed in the preceding sentence.

BUSINESS JUSTIFICATION

ALPR – GTMS supports the Department's mission and provides important operational value in the following ways:

The Airport has historically used electronic toll readers and other technologies to monitor commercial ground transportation activity at the Airport. The PIPS Technology™ ("PIPS") ALPR – GTMS solution serves as a secondary source of ensuring commercial ground transportation database information is correct. This is an essential component of a comprehensive and efficient transportation system. Ground transportation activity at the Airport continues to grow in line with air passenger activity. In FY2019, there were over 6,500 (non TNC) vehicles permitted to operate at the Airport, with almost 3,000,000 pickups and drop-offs completed.

The primary use for Landside ALPR – GTMS is to capture the activity of permitted commercial ground transportation at the Airport. The ALPR – GTMS acts as a failsafe if the Automated Vehicle Identification (AVI) readers malfunctions and fails to read the transponder the Airport affixes to certain types of permitted vehicles. It assists in dispute resolution in the event that the operator challenges the transponder data (i.e., number of trips the operator has made to the Airport) collected from the AVI.

Additional uses include tracking permitted operators that are not issued transponders, such as TNC vehicles and long distance bus carriers; tracking unpermitted operators who solicit passengers for rides; and assisting public safety agencies in investigations.

In addition, ALPR – GTMS promises to benefit residents in the following ways:

☐	Education	
☐	Community Development	
☐	Health	
X	Environment	Traffic congestion studies: ALPR – GTMS can be used to conduct studies on traffic volumes and patterns, with the potential to mitigate environmental impacts of traffic congestion on residents.
X	Criminal Justice	ALPR – GTMS can be used to support identification of vehicles as a part of law enforcement investigations.
☐	Jobs	
☐	Housing	
X	Other	Public Safety: ALPR – GTMS can be used to locate stolen, wanted, and or other vehicles that are the subject of investigation, and can improve overall roadway safety for residents using Airport roadways.

	Trip fees by permitted operators: ALPR – GTMS can be used to track vehicles and collect trip fees to offset impacts of commercial vehicles on Airport roadways and to improve roadway conditions for residents accessing the Airport.

In addition, the following benefits are obtained:

Benefit		Description
☐	Financial Savings	
X	Time Savings	Without the ALPR – GTMS technology, the Airport would need to deploy a manually staffed ground transportation operation. This alternative has not been thoroughly explored for feasibility. At minimum however, team members would be required to be assigned to all entry lanes, exit lanes, curbside zones, and staging lots during 24/7 operations. Team members would conduct manual verification of registration through visual observance of permits and decals, and conduct traffic counts. The ALPR – GTMS removes the necessity of staffing for this purpose.
☐	Staff Safety	
X	Data Quality	The ALPR – GTMS technology is verified against the AVI technology to verify that all permitted vehicles' trips have been documented for tracking and fee assessment purposes, in case the AVI malfunctions and fails to read the airport affixed transponder. The ALPR – GTMS is also used in concert with AVI to confirm whether a commercial vehicle on Airport roadways is a permitted operator.
X	Other	The ALPR – GTMS technology enables the Airport to assess trip fees on permitted Commercial ground transportation operators. In 2019, the Airport collected a total of $64,815,649 in trip fees from ground transportation operators.

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 kept up to date and maintained.
Safety:	Surveillance technology must be operated in a safe manner. Surveillance technology should not be operated in a way that infringes on resident civil rights, including privacy, or causes personal injury or property damage.
Data Collection:	Departments shall minimize the use, collection, and retention of Personally Identifiable Information (PII) to what is strictly necessary to accomplish the intended purpose of the surveillance technology. Department shall only collect data required to execute the authorized use case. All data collected by the surveillance technology, including PII, shall be classified according to the City's Data Classification Standard. Should information be incidentally collected that is not necessary to accomplish the intended purpose of the surveillance technology, including information that may be used to identify persons or private information, Department shall remove all incidental PII from raw data. The surveillance technology collects the following data types:

Data Type(s)	*Format(s)*	*Classification*
Company's registered DBA Permit Type Location of record Date and Time of record	.xml, .pdf, .html, .jpg, .xml	Level 2
Images of license plates	.jpg, .xml	Level 3
Date & time image taken	.jpg, .xml	Level 3

Notification:	The commercial ground transportation operators acknowledge notice of GTMS policies and procedures, which include the Airport's use of ALPR and Electronic Toll Readers, by signing the Airport permit. In addition, in compliance with California Civil Code § 1798.90.5, the Airport shall notify the public of the ALPR – GTMS surveillance technology operation by posting the ALPR – GTMS privacy and usage policy on FLYSFO.

The public notice shall include the following items in its public notice:

- Information on the surveillance technology
- Description of the authorized use
- Type of data collected
- Will persons be individually identified
- Data retention
- Department identification
- Contact information

Access:

All parties requesting access must adhere to the following rules and processes:

Use of the Ground Transportation Management System (GTMS) software is required for data access. Agreement and adherence to the City and County of San Francisco's and Airport's computer and data information systems policies, supervisor approval for use, and GTMS Administrator approval for use. Request for system access is to be submitted through SFO's ITT Help Desk ServiceNow online request form. Access can be limited and varied dependent on software system user role. GTMS Administrator and ITT to determine and provide permissions on user role. Training to be provided once software is installed on computer or laptop.

Data can only be accessed through the permissions-controlled GTMS software. The data is to be used for trip and revenue analysis for internal purposes. Information deemed low risk such as Permit Type i.e. Limousine, Taxi, trip counts may be aggregated and shared with the public, other airports, and transportation industries. The public may request trip and revenue information through a public records request.

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.

- 1825 Principal Administrative Analyst II
- 1823 Senior Administrative Analyst
- 1822 Administrative Analyst
- 7315 Automotive Machinist Assistant Supervisor
- (2) 5290 Transportation Planner IV
- 7381 Automotive Mechanic
- 0931 Manager III, Airport – Landside Operations

The following providers are required to support and maintains the surveillance technology and its associated data to ensure it remains functional:

- TransCore
- LP IBI Group, LLC

B. Members of the public

Airport 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. Anyone, including criminal defendants, may access such data. 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, including by criminal defendants.

Members of the public, including criminal defendants, 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.

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).

To protect surveillance technology information from unauthorized access and control, including misuse, Departments shall, at minimum, apply the following safeguards:

Data can only be accessed through the permissions-controlled GTMS software. Users must provide unique computer login credentials such as username and password to access the data. Passwords must comply with the City and County of San Francisco cyber security requirements. The following protocols shall be followed to ensure data security:

- All network equipment and servers containing sensitive data are maintained in a secured
- location accessible only to Airport badged, authorized personnel.
- Servers and network equipment are continuously monitored.

- ITT maintains a log of successful and unsuccessful logon attempts, changes in user accounts, whether user logs have been modified, network threats, and resource access.
- All SFO workstations and servers are patched regularly.
- All sensitive data stored on the servers are backed up regularly and a copy saved offsite
- SFO's network is protected behind a firewall and data transmitted outside SFO's network to SFO cloud-based partners are encrypted via SSL/TLS. Data at rest offsite are also encrypted.

Data Sharing:

Airport 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.

Airport will endeavor to ensure that other agencies or departments that may receive data collected by ALPR – GTMS Technology will act in conformity with this Surveillance Technology Policy.

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.

Airport 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)

Airport shall ensure all PII and restricted data is de-identified or adequately protected to ensure the identities of individual subjects are effectively safeguarded.

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

The Department currently participates in the following sharing practices:

A. Internal and External Data Sharing

- GTMS Users for review of matching license plates and electronic toll reads;
- District Attorney's Office in accordance with the law; and
- Public Defender's Office or criminal defense attorney in accordance with California discovery laws; law enforcement agencies as part of a criminal or administrative investigation; Parties to civil litigation, or other third parties when required under law.

Data sharing occurs at the following frequency:

- On request in accordance with the law, or during SFO presentations on topics related to ground transportation activity.

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

X Confirm the purpose of the data sharing aligns with the department's mission.

X Consider alternative methods other than sharing data that can accomplish the same purpose.

X Redact names, scrub faces, and ensure all PII is removed in accordance with the department's data policies.

X Review of all existing safeguards to ensure shared data does not increase the risk of potential civil rights and liberties impacts on residents.

X 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.

X Ensure shared data will be done in a cost-efficient manner and exported in a clean, machine-readable format.

B. Department shares the following data with the recipients:

- Aggregated trip counts and revenue by permit types. Data constituting PII or other sensitive information will be shared with law enforcement agencies in accordance with the law, and with parties involved in criminal, civil or administrative proceedings as required under law.

To ensure that entities receiving data collected by the surveillance technology comply with the Surveillance Technology Policy, Department shall:

- Data collected is primarily to be accessed by internal stakeholders within the Airport department. All Airport users are to comply with the Airport's computer and cybersecurity polices, as agreed upon through daily computer sign-in. Data shared with external entities or other City and County departments are to fall within the Level 2 category of non-sensitive data for the business purposes of improved commercial ground transportation and analyses. Information within the Level 3 low-moderate risk category must be requested through the public records request process, and the data is reviewed prior to disclosure to ensure that it is subject to disclosure under the Public Records Act and the Sunshine Ordinance.

- 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.

Data Retention:

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

- Data is active for 18 months in the production server, then 4.5 years in cloud storage.
- Airport server storage size limits retention on production server
- Airport Data Retention Policy requires 4.5 years
- Data would only be retained longer than above if/when the City Attorney issued a litigation hold letter to the Airport.

PII data shall not be kept in a form which permits identification of data subjects for any longer than is necessary for the purposes for which the personal data are processed. PII data collected by the surveillance technology may be retained beyond the standard retention period only in the following circumstance(s):

Departments must establish appropriate safeguards for PII data stored for longer periods.

Data will be stored in the following location:

- Local storage
- Cloud Storage Provider

Data Disposal:

Upon completion of the data retention period, Department shall dispose of data in the following manner:

Practices: Data is consolidated on the local storage and moved to cloud provider for long term storage. Local drives are overwritten with new data. Cloud storage data is deleted.

Processes and Applications: Not applicable for this technology solution.

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 must receive training on data security policies and procedures.

At the very least, 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. 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.

In-person or virtual training session that includes system overview and use of reporting modules.)

COMPLIANCE

Department shall oversee and enforce compliance with this Policy using the following methods:

The Airport's Information Technology and Telecommunications (ITT) and Government Affairs & Policy teams will both govern and oversee compliance of the policy. Any resulting policy is to be shared with the Airport community with follow-up items, if any, documented.

Department shall assign the following personnel to oversee Policy compliance by the Department and third-parties.

- Manager of ITT Business Services
- Senior, Landside Transportation Planner

Sanctions for violations of this Policy include the following:

- Airport Commission employees will be disciplined for violation of the Ordinance subject to meeting and conferring with the unions representing Airport Commission employees.

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.

EXCEPTIONS

Only in exigent circumstances or in circumstances where law enforcement requires surveillance technology data for investigatory or prosecutorial functions may data collected, retained or processed by the surveillance technology be shared with law enforcement.

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.
Sensitive Data:	Data intended for release on a need-to-know basis. Data regulated by privacy laws or regulations or restricted by a regulatory agency or contract, grant, or other agreement terms and conditions.

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

Public:

Complaints or concerns can be submitted to the Department by completing a Contact SFO Form found on FLYSFO.COM. The submissions are reviewed by the Airport Guest Services team and forwarded to the Airport stakeholder team responsible for follow-up, as necessary, on the topic of concern or comment. Additionally, the Airport Commission holds bi-monthly public meetings where the public may register complaints or concerns during the Public Comment section of the calendared agenda.

Department shall acknowledge and respond to complaints and concerns in a timely and organized response. To do so, Department shall:

- Include in the daily tasks and job duties of Landside staff and its contractors to respond to complaints and concerns submitted by the commercial transportation.
- Consistent with these duties, Landside staff responds to all inquiries from commercial passenger transportation providers.
- In addition, the Airport's Guest Services team dedicates a staff to address complaints and concerns from the public.
- Any matters brought to the Airport are tracked from initial receipt of communication through closure of follow-up actions, if any.

City and County of San Francisco Employees:

All questions regarding this policy should be directed to the employee's supervisor or to the director. Similarly, questions about other applicable laws governing the use of the surveillance technology or the issues related to privacy should be directed to the employee's supervisor or the director.

Surveillance Impact Report

OnSight Portable License Plate Reader
Public Works

As required by San Francisco Administrative Code, Section 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 OnSight Portable License Plate Reader.

DESCRIPTION OF THE TECHNOLOGY

The Department's mission is: We Care for and build the City's assets for the People of San Francisco.

In line with its mission, the Department uses OnSight Portable License Plate Reader to Keeping the streets clean is a major challenge with ongoing illegal dumping. The License plate reader will allow us to capture illegal dumping and follow up with the bad actors.

Public Works shall use OnSight Portable License Plate Reader only for the following authorized purposes:

Authorized Use(s):

To follow up on illegal dumping onto City Streets

The following use cases are expressly prohibited.

- Anything outside of illegal dumping cases .

Department technology is located District 10.

TECHNOLOGY DETAILS

The following a is product description of OnSight Portable License Plate Reader

IR/Starlight Hybrid Camera Sensor. 21"lx15"Wx9"D Weight 25lbs.

A. How It Works

To function, OnSight Portable License Plate Reader Powered by solar with a battery, it captures data from vehicles in day or night to read the license plate. A 12 MM camera lens is paired with a LTE SIM Card to record the license plate information for a maximum of 30 days.

All data collected or processed by OnSight Portable License Plate Reader will be handled or stored by an outside provider or third-party vendor on an ongoing basis. Specifically, data will be handled byV5 Systems to ensure the Department may continue to use the technology.

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:

A. The benefits of the surveillance technology outweigh the costs.

B. The Department's Policy safeguards civil liberties and civil rights.

C. 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 [Technology name] has the following benefits for the residents of the City and County of San Francisco:

☐ Education	
☐ Community Development	
☐ Health	
☑ Environment	Illegal dumping affects adjacent neighbors and businesses. This will allow us to catch and prevent future illegal dumping in these neighborhoods.
☐ Criminal Justice	
☐ Jobs	
☐ Housing	
☐ Other	

Additional benefits include:

- Easily deployed to any outdoor environment without need for trenching. Can be used on either A/C or solar power. Web based user interface for easy accessing of information.

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:

Data will only be looked at if illegal dumping occurs. Data will only be used if violation occurs. No data on other individuals will be looked at, or used.

Authorization to review the footage will come from the Deputy Director of Operations in form of written approval for reviewing of the footage. Cameras will only be placed in an

area capturing images of an identified, documented illegal dumping location. Any incidental information seen will not be kept or used

The placement of these cameras is intended to improve the quality of life in the community and will only be placed in areas where we have a clear illegal dumping problem that is impacting the community.

Hotspots of illegal dumping are identified through the following sources:

- 311
- Employee observations
- Email complaints from constituents

C. *Fiscal Analysis of Costs and Benefits*

The Department's use of OnSight Portable License Plate Reader yields the following business and operations benefits:

Benefit	Description
☑ Financial savings	It would be very costly to pay for humans to sit at night to catch illegal dumpers
☐ Time savings	
☑ Staff safety	We won't have to put staff in direct harm confronting illegal dumpers, won't have to have staff working at night in remote locations.
☑ Improved data quality	The camera lens provides accurate license plate data. If we were relying on a human they might misread the plate during low-light conditions.
☐ Other	

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

FTE (new & existing)	.01, .1, .1		
Classification	1042, 1093, 1010, 7281, 7345, 0941, 0954		
	Annual Cost	***Years***	***One-Time Cost***
Total Salary & Fringe	$30,403.34	5	$5,740.8
Software	$0	0	$0
Hardware/Equipment	$0	0	$99,000

Professional Services	$0	0	$0
Training	$0	0	$0
Other	$0	0	$10,000
Total Cost [Auto-calculate]	$114,740.8		
2.1 Please disclose any current or potential sources of funding (e.g. potential sources = prospective grant recipients, etc.). SIR, ASR			
add-back funding from D10 Supervisor			

The Department funds its use and maintenance of the surveillance technology through add-back funding from D10 Supervisor.

COMPARISON TO OTHER JURISDICTIONS

OnSight Portable License Plate Reader are currently utilized by other governmental entities for similar purposes.

APPENDIX A: Surveillance Impact Report Requirements

The following section shows all Surveillance Impact Report requirements in order as defined by the San Francisco Administrative Code, Section 19B.

1. Information describing the Surveillance Technology and how it works, including product descriptions from manufacturers.

Powered by solar with a battery, it captures data from vehicles in day or night to read the license plate. A 12 MM camera lens is paired with a LTE SIM Card to record the license plate information for a maximum of 30 days.

IR/Starlight Hybrid Camera Sensor. 21"lx15"Wx9"D Weight 25lbs

2. Information on the proposed purpose(s) for the Surveillance Technology.

Keeping the streets clean is a major challenge with ongoing illegal dumping. The License plate reader will allow us to capture illegal dumping and follow up with the bad actors.

Easily deployed to any outdoor environment without need for trenching. Can be used on either A/C or solar power. Web based user interface for easy accessing of information.

3. If applicable, the general location(s) it may be deployed and crime statistics for any location(s).

District 10

4. An assessment identifying any potential impact on civil liberties and civil rights and discussing any plans to safeguard the rights of the public.

Data will only be looked at if illegal dumping occurs. Data will only be used if violation occurs. No data on other individuals will be looked at, or used.

5. The fiscal costs for the Surveillance Technology, including initial purchase, personnel and other ongoing costs, and any current or potential sources of funding.

Number of FTE (new & existing)	.01, .1, .1
Classification	1042, 1093, 1010, 7281, 7345, 0941, 0954
Total Salary & Fringe	$5,740.8
Software	$0
Hardware/Equipment	$99,000
Professional Services	$0

Training	$0
Other	$10,000
Total Cost [Auto-calculate]	$114,740.8

add-back funding from D10 Supervisor

6. Whether use or maintenance of the technology will require data gathered by the technology to be handled or stored by a third-party vendor on an ongoing basis.

Handled by third-party vendor, ongoing: true

Vendor name: V5 Systems

Special data handling required: true

7. A summary of the experience, if any, other governmental entities have had with the proposed technology, including information about its effectiveness and any known adverse information about the technology such as anticipated costs, failures, or civil rights and civil liberties abuses.

APPENDIX B: Mapped Crime Statistics

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

District 10

Surveillance Technology Policy

OnSight Portable License Plate Reader
Public Works

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 OnSight Portable License Plate Reader 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

The Department's mission is to care for and build the City's assets for the People of San Francisco

The Surveillance Technology Policy ("Policy") defines the manner in which the OnSight Portable License Plate Reader will be used to support this mission, by describing the intended purpose, authorized and restricted uses, and requirements.

This Policy applies to all to department personnel that use, plan to use, or plan to secure OnSight Portable License Plate Reader, 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 OnSight Portable License Plate Reader technology for the Department is limited to the following use cases and is subject to the requirements listed in this Policy.

Authorized Use(s):

Discourage illegal dumping onto City Streets.

Prohibited use cases include any uses not stated in the Authorized Use Case section.

Further, processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data 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.

Surveillance Oversight Review Dates

COIT Review: September 17, 2020

Board of Supervisors Review: TBD

BUSINESS JUSTIFICATION

OnSight Portable License Plate Reader supports the Department's mission and provides important operational value in the following ways:

Keeping the streets clean is a major challenge with ongoing illegal dumping. The License plate reader will allow us to capture illegal dumping and discourage illegal dumping.

Public Works has two License Plate Readers that are currently mounted on a pole on our facility for proof of concept. Public Works' intention is to attach additional License Plate Readers to buildings in neighborhoods at the request of, or with permission from the property owner. The Supervisor's office is working on identifying participants.

Hotspots of illegal dumping are identified through the following sources:

- 311
- Employee observations
- Email complaints from constituents

In addition, OnSight Portable License Plate Reader promises to benefit residents in the following ways:

☐	Education	
☐	Community Development	
☐	Health	
☐	Environment	Illegal dumping affects adjacent neighbors and businesses. This will allow us to catch and prevent future illegal dumping in these neighborhoods.
☐	Criminal Justice	
☐	Jobs	
☐	Housing	
☐	Other	

OnSight Portable License Plate Reader will benefit the department in the following ways:

Benefit		Description
☐	Financial Savings	It would be very costly to pay for humans to sit at night to catch illegal dumpers
☐	Time Savings	

☐	Staff Safety	We won't have to put staff in direct harm confronting illegal dumpers, won't have to have staff working at night in remote locations.
☐	Data Quality	The camera lens provides accurate license plate data. If we were relying on a human they might misread the plate during low-light conditions.
☐	Other	

Other benefits include Easily deployed to any outdoor environment without need for trenching. Can be used on either A/C or solar power. Web based user interface for easy accessing of information.

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 kept up to date and maintained.
Safety:	Surveillance technology must be operated in a safe manner. Surveillance technology should not be operated in a way that infringes on resident civil rights, including privacy, or causes personal injury or property damage.
Data Collection:	Departments shall minimize the use, collection, and retention of Personally Identifiable Information (PII) to what is strictly necessary to accomplish the intended purpose of the surveillance technology. Department shall only collect data required to execute the authorized use case. All data collected by the surveillance technology, including PII, shall be classified according to the City's Data Classification Standard. Should information be incidentally collected that is not necessary to accomplish the intended purpose of the surveillance technology, including information that may be used to identify persons or private information, Department shall remove all incidental PII from raw data. Data types can take the form video, audio, still images. Data formats can take the form of XML, PDF, HTML, Plain Text, JPEG, etc. The surveillance technology collects the following data types and formats:

- Video in MOV format
- Still images from cameras in PDF format

The surveillance technology collects the following data types:

Data Type(s)	*Format(s)*	*Classification*
License Plate	AVI	Level 3
Facial features	AVI	Level 3

The technology does not use facial recognition but does take photos/videos that may capture facial features. This technology will only be used to pursue enforcement of illegal activity. Facial features and license plate information will only be shared with relevant law enforcement for enforcement purposes.

Notification:

Departments shall notify the public of intended surveillance technology operation at the site of operations through signage in readily viewable public areas. Department notifications shall identify the type of technology being used and the purpose for such collection.

Department includes the following items in its public notice:

☒ Information on the surveillance technology
☐ Description of the authorized use
☐ Type of data collected
☐ Will persons be individually identified
☐ Data retention
☒ Department identification
☐ Contact information

Access:

All parties requesting access must adhere to the following rules and processes (please refer to the data sharing section to ensure all information covered in that section is also included below): evidence of illegal dumping

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.

- 7281 Operations Supervisor 2, Public Works

The following providers are required to support and maintains the surveillance technology and its associated data to ensure it remains functional:

- V5 Systems

B. Members of the public

Public Works 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.

Data collected by surveillance technology will not be made available to members of the public, including criminal defendants.

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. Anyone, including criminal defendants, may access such data. 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, including by criminal defendants.

Members of the public, including criminal defendants, 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.

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). To protect surveillance technology information from unauthorized access and control, including misuse, Departments shall, at minimum, apply the following safeguards: Supervisors will be monitored
Data Sharing:	Public Works 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.

Public Works will endeavor to ensure that other agencies or departments that may receive data collected by OnSight Portable License Plate Readers will act in conformity with this Surveillance Technology Policy.

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.

Public Works 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)

Public Works shall ensure all PII and restricted data is de-identified or adequately protected to ensure the identities of individual subjects are effectively safeguarded.

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

The Department currently participates in the following sharing practices:

A. Internal and External Data Sharing

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 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 shared data will be done in a cost-efficient manner and exported in a clean, machine-readable format.

Department shares the following data with the recipients:

- Public Works may share data with SFPD, CAT

Data sharing occurs at the following frequency:

- As needed

Public Works may share data with SFPD and the District Attorney to pursue criminal charges.

Data Retention:

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

Please list data retention schedules (i.e., x type of data will be retained for 1 year) based on the following categories:

- Permanent records (i.e., records that are essential): shall be retained and preserved indefinitely
- Current records (i.e., records for operational necessity, ready reference, convenience): record retention schedules may vary but generally less than 10 years
- Storage records (i.e., records retained offsite): record retentions may vary but generally less than 10 years

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

Maximum of 30 days	Only need it long enough to confirm responsible parties

PII data shall not be kept in a form which permits identification of data subjects for any longer than is necessary for the purposes for which the personal data are processed. PII data collected by the surveillance technology may be retained beyond the standard retention period only in the following circumstance(s):

- n/a

Departments must establish appropriate safeguards for PII data stored for longer periods.

Data will be stored in the following location:

☐ Local storage
☐ Department of Technology Data Center
☐ Software as a Service Product
☑ Cloud Storage Provider

Data Disposal:

Upon completion of the data retention period, Department shall dispose of data in the following manner:

	Practices: Automatic overwrite after 30 days Processes and Applications: n/a
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 must receive training on data security policies and procedures. At the very least, 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. 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.

COMPLIANCE

Department shall oversee and enforce compliance with this Policy using the following methods:

Deputy Director for Operations is responsible for monitoring compliance

Department shall assign the following personnel to oversee Policy compliance by the Department and third-parties:

Deputy Director for Operations

Sanctions for violations of this Policy include the following:

Removal or shutting down of technology until violations are resolved

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.

EXCEPTIONS

Only in exigent circumstances or in circumstances where law enforcement requires surveillance technology data for investigatory or prosecutorial functions may data collected, retained or processed by the surveillance technology be shared with law enforcement.

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 a surveillance technology that has not been processed and cleaned of all personal identifiable information. The distribution and use of raw data is tightly restricted.
Exigent Circumstances	An emergency involving imminent danger of death or serious physical injury to any person that requires the immediate use of Surveillance Technology or the information it provides.

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

Public:

Complaints or concerns can be submitted to the Department by:

All complaints or concerns should be routed through 311.org

Department shall acknowledge and respond to complaints and concerns in a timely and organized response. To do so, Department shall:

Respond to 311 within required SLA

City and County of San Francisco Employees:

All questions regarding this policy should be directed to the employee's supervisor or to the director. Similarly, questions about other applicable laws governing the use of the surveillance technology or the issues related to privacy should be directed to the employee's supervisor or the director.

APPENDIX A: Surveillance Technology Policy Requirements

The following section shows all Surveillance Technology Policy requirements in order as defined by the San Francisco Administrative Code, Section 19B.

1. A description of the product and services addressed by the Surveillance Technology, including the identity of any provider(s) whose services are essential to the functioning or effectiveness of the Surveillance Technology equipment or services for the intended purpose.

Powered by solar with a battery, it captures data from vehicles in day or night to read the license plate. A 12 MM camera lens is paired with a LTE SIM Card to record the license plate information for a maximum of 30 days.

IR/Starlight Hybrid Camera Sensor. 21"lx15"Wx9"D Weight 25lbs

V5 Systems

2. A description of the purpose(s) for which the Surveillance Technology equipment or services are proposed for acquisition, including the type of data that may be collected by the Surveillance Technology equipment or services.

Technology Use:

Keeping the streets clean is a major challenge with ongoing illegal dumping. The License plate reader will allow us to capture illegal dumping and follow up with the bad actors.

PII:

true

3. The uses that are authorized, the rules and processes required prior to such use, and uses of the Surveillance Technology that will be expressly prohibited.

Authorized Uses:

Only to follow up on illegal dumping onto City Streets

Rules:

anything outside of illegal dumping cases

Prohibited Uses:

only where illegal dumping was confirmed

4. A description of the formats in which information collected by the Surveillance Technology is stored, copied, and/or accessed.

Data Type	Formats STP
License Plate	AVI
Facial features	AVI

5. The specific categories and titles of individuals who are authorized by the Department to access or use the collected information, including restrictions on how and under what circumstances data collected with Surveillance Technology can be analyzed and reviewed, and the rules and processes required prior to access or use of the information.

Employee Job Classification & Title:

only where illegal dumping was confirmed

Department:

Public Works

If applicable, contractor or vendor name:

V5 Systems

Rules and processes required prior to data access or use:

Supervisors will be monitored

6. The general safeguards that protect information from unauthorized access, including encryption and access control mechanisms.

only where illegal dumping was confirmed

7. The limited time period, if any, that information collected by the Surveillance Technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s) enumerated in the Surveillance Technology Policy, the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond that period

Retention:

only need it long enough to confirm responsible parties

Reason for retention:

n/a

Deletion process:

only need it long enough to confirm responsible parties

Retention exemption conditions:

n/a

8. How collected information can be accessed or used by members of the public, including criminal defendants

Will the data be accessible to the public:

Maximum of 30 days

How it can be accessed:

9. Which governmental agencies, departments, bureaus, divisions, or units that may receive data collected by the Surveillance Technology operated by the Department, including any required justification or legal standard necessary to share that data and how it will ensure that any entity receiving such data complies with the Surveillance Technology Policy.

Name of agency: Public Works may share data with SFPD, CAT

Justification:

10. The training required for any individual authorized to use the Surveillance Technology or to access information collected by the Surveillance Technology

Training required:

false

Description of training:

11. The mechanisms to ensure that the Surveillance Technology Policy is followed, including internal personnel assigned to ensure compliance with the policy, internal recordkeeping of the use of the technology or access to information collected by the technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the sanctions for violations of the policy

Training required:

false

Process for responding to complaints:

Deputy Director for Operations

Oversight process:

Removal or shutting down of technology until violations are resolved

Compliance personnel titles:

7281 Operations Supervisor 2, Public Works

Restrictions:

only where illegal dumping was confirmed

12. What procedures will be put in place by which members of the public can register complaints or concerns, or submit questions about the deployment or use of a specific Surveillance Technology, and how the Department will ensure each question and complaint is responded to in a timely manner.

Complaint procedures:

respond to 311 within required SLA

Departmental follow-up process:

Larry Stringer, Deputy Director for Operations is responsible for monitoring compliance

Members of the public can register complaints/concerns or submit questions via calls or emails at 311.org.

Surveillance Impact Report

Recreation & Parks Department
Automatic License Plate Reader (ALPR)

As required by San Francisco Administrative Code, Section 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 ALPR.

DESCRIPTION OF THE TECHNOLOGY

The Department's mission is: to provide enriching recreational activities, maintain beautiful parks and preserve the environment for the well-being of our diverse community.

In line with its mission, the Department uses ALPR to ALPRs are used to protect the public and our staff in our parks and playgrounds and at special events. In addition, ALPRs are used to protect our critical infrastructure sites.

Recreation and Parks shall use ALPR only for the following authorized purposes:

Authorized Use(s):

1. To support local, state, federal, and regional public safety departments in the identification of vehicles associated with targets of criminal investigations, including investigations of serial crimes
2. To protect the public and our staff at special events from misconduct and/or violent confrontations.
3. To protect critical infrastructure sites from vandalism, theft and damage.

Prohibited use cases include any uses not stated in the Authorized Use Case section.

Further, processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, gender, gender identity, disability status, or an individual person's sex life or sexual orientation, and the processing of genetic data and/or biometric data for the purpose of uniquely identifying an individual person shall be prohibited.

Department technology is located Poles or facilities where there is a view of park assets (eg. Parking lots, park roads). ALPRs are not located on public streets.

Surveillance Oversight Review Dates
COIT Review: February 4, 2021
Board of Supervisors Review: TBD

Technology Details

The following a is product description of ALPR

- ARES 2 Line LPR ARES server Exacqvision Video Management System Note: 1. RecPark does not consistently monitor the cameras. RecPark only reviews the video files after an incident has occurred. 2. ALPRs only generate video / image files. The license plate images taken by the ALPRs are not transformed into alphanumeric characters and stored with any related metadata.

A. How It Works

To function, ALPR Automated license plate readers (ALPRs) are high-speed, computer-controlled camera systems. ALPRs automatically capture all license plate numbers that come into view, along with the location, date, and time. ALPRs will be mounted on a pole or on a RecPark facility, and monitor parks, playgrounds, and RecPark facilities.

Data collected or processed by ALPR will not be handled or stored by an outside provider or third-party vendor on an ongoing basis. The Department will remain the sole Custodian of Record.

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:

- The benefits of the surveillance technology outweigh the costs.
- The Department's Policy safeguards civil liberties and civil rights.
- 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.

B. Benefits

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

☐	Education	
☐	Community Development	
☐	Health	
☐	Environment	
X	Criminal Justice	Coordination with law enforcement or first responders for all approved requests. Approved requests include criminal activities

		such as auto burglaries, personal theft, assaults, robberies, vehicle theft, and vehicle accidents.
☐	Jobs	
☐	Housing	
X	Other	Public Safety - to protect the public and our staff in our parks and playgrounds and at special events.

C. Civil Rights Impacts and Safeguards

The Department has considered the potential impacts and has identified technical, administrative, and physical protections as mitigating measures. Through operationalization of the ALPR Surveillance Policy, the following will be implemented:

1. Administrative Safeguards - All ALPR data will be captured in a request management software solution. Data will include information about ALPR procurement, ALPR attributes, approved requestors of surveillance data, and all requests for Surveillance data. In addition, there will be knowledge articles describing step by step instructions on how to collect and send the data to the requestor.

2. Technical Safeguards - ALPR Data cannot be accessed unless by an approved requestor, and only for approved requests. Access to ALPR data is limited to 8210 and above management levels in the Park Ranger unit. Violation of the policy will be subject to standard RecPark departmental policies, which may include disciplinary action up to and including termination.

3. Physical Safeguards - Hardware is secured in the server room, where there is limited physical access. Additionally, there is limited access to the software that stores and retrieves the ALPR data. Fiscal Analysis of Costs and Benefits

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

Benefit		**Description**
☐	Financial Savings	
☐	Time Savings	
X	Staff Safety	To protect our staff in our parks and playgrounds, and at special events.
☐	Data Quality	

FTE (new & existing)	1 (5% max time - only when requested)	
Classification	8210 - Head Park Ranger	
	Annual Cost	***One-Time Cost***
Total Salary & Fringe	*$5,000*	-
Software	**-**	$1,000
Hardware/Equipment	-	$5,000
Professional Services	-	$1,000
Training	-	-
Other	-	-
Total Cost		***$7,000***

The Department funds its use and maintenance of the surveillance technology through

- Operational funds.

COMPARISON TO OTHER JURISDICTIONS

ALPR are currently utilized by other governmental entities for similar purposes.

APPENDIX A: Mapped Crime Statistics

Poles or facilities where there is a view of park assets (eg. Parking lots, park roads). ALPRs are not located on public streets.

Surveillance Technology Policy

Recreation & Parks Department
Automatic License Plate Reader (ALPR)

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 ALPR 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

The Department's mission is: to provide enriching recreational activities, maintain beautiful parks and preserve the environment for the well-being of our diverse community.

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

This Policy applies to all to department personnel that use, plan to use, or plan to secure ALPR, 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 ALPR technology for the Department is limited to the following use cases and is subject to the requirements listed in this Policy.

Authorized Use(s):

1. To support local, state, federal, and regional public safety departments in the identification of vehicles associated with targets of criminal investigations, including investigations of serial crimes
2. To protect the public and our staff at special events from misconduct and/or violent confrontations.
3. To protect critical infrastructure sites from vandalism, theft and damage.

Prohibited use cases include any uses not stated in the Authorized Use Case section.

Departments may use information collected only for legally authorized purposes, and may not use that information to unlawfully discriminate against people based on race, ethnicity, political opinions, religious or philosophical beliefs, trade union membership, gender, gender identity, disability status, sexual orientation or activity, or genetic and/or biometric data. Additionally, departments may not use automated systems to scan footage and identify individuals based on any of the categories listed in the preceding sentence.

BUSINESS JUSTIFICATION

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

- ALPRs are used to protect the public and our staff in our parks and playgrounds and at special events. In addition, ALPRs are used to protect our critical infrastructure sites.

In addition, ALPR promises to benefit residents in the following ways:

	▪ Education	
	▪ Community Development	
	▪ Health	
	▪ Environment	
X	Criminal Justice	Coordination with law enforcement or first responders for all approved requests. Approved requests include criminal activities such as auto burglaries, personal theft, assaults, robberies, vehicle theft, and vehicle accidents.
	▪ Jobs	
	▪ Housing	
X	Other	Public Safety - to protect the public and our staff in our parks and playgrounds and at special events.

In addition, the following benefits are obtained:

Benefit		Description
	▪ Financial Savings	
	▪ Time Savings	
X	Staff Safety	To protect our staff in our parks and playgrounds, and at special events.
	▪ Data Quality	
	▪ Service Levels	

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 kept up to date and maintained.
Safety:	Surveillance technology must be operated in a safe manner. Surveillance technology should not be operated in a way that infringes on resident civil rights, including privacy, or causes personal injury or property damage.
Data Collection:	Departments shall minimize the use, collection, and retention of Personally Identifiable Information (PII) to what is strictly necessary to accomplish the intended purpose of the surveillance technology. Department shall only collect data required to execute the authorized use case. All data collected by the surveillance technology, including PII, shall be classified according to the City's Data Classification Standard. Should information be incidentally collected that is not necessary to accomplish the intended purpose of the surveillance technology, including information that may be used to identify persons or private information, Department shall remove all incidental PII from raw data. The surveillance technology collects the following data types:

Data Type(s)	*Format(s)*	*Classification*
Images of license plates	AVI, MOV, MP3, JPG	Level 3
Date & time image taken	AVI, MOV, MP3, JPG	Level 3

Notification:	Departments shall notify the public of intended surveillance technology operation at the site of operations through signage in readily viewable public areas. Department notifications shall identify the type of technology being used and the purpose for such collection. The Department's public notice will include the following items:

- Information on the surveillance technology
- Description of the authorized use
- Type of data collected
- Will persons be individually identified
- Data retention
- Department identification
- Contact information

Access:

All parties requesting access must adhere to the following rules and processes: RecPark does not consistently monitor the cameras. RecPark only reviews the video files after an incident has occurred. Request may come from RecPark or law enforcement.

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.

- 8210 - Head Park Ranger, SF Rec Park

The following providers are required to support and maintains the surveillance technology and its associated data to ensure it remains functional:

B. Members of the public

Recreation and Parks 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. Anyone, including criminal defendants, may access such data. 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, including by criminal defendants.

Members of the public, including criminal defendants, 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.

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). To protect surveillance technology information from unauthorized access and control, including misuse, Departments shall, at minimum, apply the following safeguards: ALPR data shall only be utilized for legitimate park enforcement purposes, or at the request other law enforcement agencies. Access to ALPR data is limited to 8210 and above management levels in the Park Ranger unit.
Data Sharing:	Recreation and Parks 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. Recreation and Parks will endeavor to ensure that other agencies or departments that may receive data collected by [the Surveillance Technology Policy that it operates] will act in conformity with this Surveillance Technology Policy. 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. Recreation and Parks 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) Recreation and Parks shall ensure all PII and restricted data is de-identified or adequately protected to ensure the identities of individual subjects are effectively safeguarded. Each department that believes another agency or department receives or may receive data collected from its use of STs should consult with its assigned deputy city attorney regarding their response. *A. Internal Data Sharing* Department shares the following data with the recipients: The department does not share surveillance technology data with other departments or entities inside the City and County of San Francisco. Data sharing occurs at the following frequency: Upon request. Before sharing data with any recipients, the Department will use the following procedure to ensure appropriate data protections are in place:

The Department currently participates in the following sharing practices:

X	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.
X	Redact names, scrub faces, and ensure all PII is removed in accordance with the department's data policies.
X	Review of all existing safeguards to ensure shared data does not increase the risk of potential civil rights and liberties impacts on residents.
X	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.
X	Ensure data will be shared in a cost-efficient manner and exported in a clean, machine-readable format.

B. External Data Sharing

Department shares the following data with the recipients:

- Approved requests from other law enforcement agencies e.g. SFPD, District Attorney, Public Defender. Approved requests include criminal activities such as auto burglaries, personal theft, assaults, robberies, vehicle theft, and vehicle accidents.

Data sharing occurs at the following frequency:

- Upon 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:

- ALPR video files will be retained for 30-60 days (depending upon the hardware capacity).
- Hardware capacity (files are overwritten when storage is full).

PII data shall not be kept in a form which permits identification of data subjects for any longer than is necessary for the purposes for which the personal data are processed. PII data collected by the surveillance technology may be retained beyond the standard retention period only in the following circumstance(s):

	Any requested files will be saved in the request management software used to manage all requests for surveillance technology. The files will be maintained for up to two years or if a case has been closed. Departments must establish appropriate safeguards for PII data stored for longer periods. 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 X Software as a Service Product ▪ Cloud Storage Provider
Data Disposal:	Upon completion of the data retention period, Department shall dispose of data in the following manner: Practices: All ALPR data is stored in the local hardware and is delated 30-60 days from the date it was collected. The system overwrites the data when hard drive is full. There is no manual deletion of any data. For any requested data that is stored in the request management software used to manage all requests for surveillance technology, there will be a process to delete the data after two years if still available. Processes and Applications: None
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 must receive training on data security policies and procedures. At the very least, 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. 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. Training is provided by the installation vendor - Microbiz.

COMPLIANCE

Department shall oversee and enforce compliance with this Policy using the following methods:

IT will work closely with the Park Rangers to ensure that the Surveillance Technology Policy for ALPRs will be supported. Procurement of all technical hardware and software is led by IT. Additionally, asset and request management of all ALPRs is led by IT.

Department shall assign the following personnel to oversee Policy compliance by the Department and third-parties.

Lieutenant Marcus Santiago (SFRPRD Park Ranger), Christine Nath (SFRPRD CIO)

Sanctions for violations of this Policy include the following:

Violation of the policy will be subject to standard RecPark departmental policies, which may include disciplinary action up to and including termination.

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.

EXCEPTIONS

Only in exigent circumstances or in circumstances where law enforcement requires surveillance technology data for investigatory or prosecutorial functions may data collected, retained or processed by the surveillance technology be shared with law enforcement.

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.
Sensitive Data:	Data intended for release on a need-to-know basis. Data regulated by privacy laws or regulations or restricted by a regulatory agency or contract, grant, or other agreement terms and conditions.

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

Public:

Complaints or concerns can be submitted to the Department by

Members of the public can register complaints/concerns or submit questions to San Francisco Recreation and Parks through several ways: 1.) Send written correspondence to McLaren Lodge in Golden Gate Park, 501 Stanyan Street, San Francisco, CA 94117; 2.) Call to the RPD Front Desk 415-831-2700; 3.) Send an email to rpdinfo@sfgov.org; 4.)Contact 311.

Department shall acknowledge and respond to complaints and concerns in a timely and organized response. To do so, Department shall:

All ALPR calls/complaints from the public received via mail or via call to the RPD Front Desk are routed to the RPD IT HelpDesk and logged in our department's request management system. Any requests from 311 are received in our department's dispatch system and routed to the RPD IT HelpDesk which then is logged in the request management system.

Once the request is tracked in the request management system, IT will work with all relevant parties to ensure completion.

Review of open / closed requests occur with the CIO on a weekly basis.

City and County of San Francisco Employees:

All questions regarding this policy should be directed to the employee's supervisor or to the director. Similarly, questions about other applicable laws governing the use of the surveillance technology or the issues related to privacy should be directed to the employee's supervisor or the director.

Surveillance Impact Report

San Francisco Police Department
Automated License Plate Readers (ALPR)

As required by San Francisco Administrative Code, Section 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 ALPR.

DESCRIPTION OF THE TECHNOLOGY

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.

In line with its mission, the Department uses ALPR readers which allow for automatic and efficient identification of license plates that may be associated with criminal activity or missing persons. The quick identification of a license plate allows SFPD to respond to an associated crime, recover a victim's vehicle, investigate a crime and lawfully apprehend suspects.

SFPD shall use ALPR only for the following authorized purposes:

Authorized Use(s):

1. Locate stolen, wanted, and or other vehicles that are the subject of investigation
2. To apprehend wanted persons with arrest warrants or who are otherwise lawfully sought by law enforcement.
3. To locate victims, witnesses, suspects, missing children, adults, and/or elderly individuals, including in response to Amber Alerts and Silver Alerts and others associated with a law enforcement investigation.
4. To assist with criminal investigations initiated by local, state, federal, and regional public safety departments by identifying vehicles associated with targets of criminal investigations.
5. Identify potential threats to critical infrastructure sites.
6. For other law enforcement purposes as authorized by law: Investigations of major crimes.

The following use cases are expressly prohibited.

- An ALPR alert will not, on its own, identify an individual, reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, information concerning an individual person's sex life or sexual orientation
- An ALPR hit on its own will not substantiate law enforcement response or contact. Contacting an individual solely based on an ALPR alert in the absence of confirming disposition of the vehicle (stolen or recovered), verifying that the observed license plate number matches the ALPR data, and verifying the reason a vehicle or owner is wanted or of interest shall be prohibited.

Surveillance Oversight Review Dates

COIT Review: January 21, 2021
Board of Supervisors Review: TBD

- No SFPD member shall access ALPR data for any use other than the authorized use cases herein.
- ALPR scanning is limited to vehicles exposed to public view.
- No content captured by ALPR cameras other than license plate and vehicle information, geo- location, and time date of capture, shall constitute cause for police enforcement.

Technology Details

The following a is product description of ALPR

Stationary/Fixed, Semi-Stationary, Mobile and smartphone mobile application ALPR Systems and ALPR Systems assist on-street patrol officers checking for criminal activity by capturing and analyzing license plates against known databases. This compact, rugged system has been IP67 certified and mounts securely below the lightbar for limited visual interference. Features and Benefits Offers high resolution coverage for a full lane of traffic with up to two concurrent vehicles in the field of view. Instantly checks captured plates against one or more databases of interest to immediately alert officers of hits. Increases spatial awareness for improved officer safety. Enhances proactive, preventative enforcement by enabling more intelligent investigations and data sharing across jurisdictions. Back Office System Software stores all collected data in a central location to support data analysis, data queries and reporting for law enforcement investigations (in accordance with each jurisdiction's data retention policy). System Components Mobile ALPR Camera(s) – Each System has 1 to 4 dual (IR and color) mobile cameras. Mobile ALPR Processor – Each processor simultaneously supports up to 4 mobile cameras.

Brackets – A variety of camera mounting brackets for various vehicles and light-bar designs. In-car software – PAGIS software provides the graphical user interface (GUI) and in-car application. It compares ALPR images against federal, local or customized hotlists and sends alert when a match occurs.

How It Works

To function, ALPR Vehicle-mounted Automated License Plate Recognition (ALPR) technology shall be used to automate the processing of vehicle license plate information by translating the images license plate into alphanumeric characters with optical recognition software and storing those images, plate information and related metadata, including time and geo-location information. Vehicle-mounted Automated License Plate Recognition (ALPR) technology automates the processing of vehicle license plate and compliance information. Specifically, ALPR: uses specially-designed cameras mounted on Marked patrol vehicles and unmarked vehicles to capture digital images from surrounding vehicles as they drive through the streets; transforms the images into alphanumeric characters with optical character recognition (OCR) software to enable;

Searches full plates, with color pictures of identified vehicles for plate read verification
Partial plate searches that return possible matches to assist with identifying suspects' vehicles
stores the images, plate information, and related metadata in a restricted-access database;
compares the transformed license plate characters to databases of license plates of interest to operators;
archives photo evidence and metadata in support of citations issued ("hits") according to evidence retention standards consistent with City and State law;
ALPR Mobile Applications are uploaded onto patrol officers' Department issued smartphones and eliminate dedicated ALPR vehicles, hardware, and infrastructure and has ability to integrate into the ALPR reporting systems.

Fixed/Stationary ALPR Cameras are in a fixed location, such as permanently affixing the cameras to traffic lights, telephone poles, or at the entrances of facilities or freeway exit ramps. If cameras are pointed opposite each other, or can be repositioned remotely, law enforcement can know which direction a driver is traveling. Authorization shall be given for continuous deployment of a fixed ALPR (e.g., positioning the ALPR at a specific stationary location), in which case the authorization shall remain in force and effect unless and until rescinded or modified by the Chief of Police or his/her designee.

Semi-Stationary ALPR Cameras are located on a trailer and towed into place at strategic locations throughout the city. When parked, they function much like stationary cameras, capturing the license plates of moving vehicles that pass within view. Semi-Stationary ALPRs can be moved to different locations as operational needs change.

All data collected or processed by ALPR will be handled or stored by an outside provider or third-party vendor on an ongoing basis. Specifically, data will be handled by NCRIC's vendor to ensure the Department may continue to use the technology.

How SFPD Uses ALPR

- The Northern California Regional Intelligence Center (NCRIC) ALPR repository: NCRIC is a Federal, State, Local public safety government program that connects regional law enforcement partners. The Northern California region includes 15 counties. Each law enforcement partner's respective ALPR technology will collect ALPR data and house this data into one central repository. This data consists of license plate image, geo-location, time and date of capture and will create an alert for any license plate associated with a stolen, wanted or of interest vehicle. The central repository can be accessed by NCRIC approved agencies. NCRIC uses a vendor (currently listed as Back Office Server Software (BOSS)) which is available on SFPD Network so approved SFPD members may access the ALPR database for investigative purposes.

- Patrol officers driving marked vehicles or plain clothed officers driving unmarked vehicles outfitted with ALPR technology: The ALPR will scan license plates and may trigger an ALPR alert. The officers use the information from the alert and check it against California Law Enforcement Telecommunications System (CLETS). CLETS is the computer network that connects public safety agencies across the state to criminal histories, driver records, and other databases. "Hot sheets" or "hot lists" are housed in CLETS. The officer confirms through CLETS, the disposition of the license plate (stolen, recovered, attached to person of interest etc.). Once information is verified, the patrol officer may make contact with the vehicle, if occupied, or may begin an investigation, if unoccupied.
- SFPD does not have access to, own, lease or use Stationary ALPR cameras or Smartphone ALPR applications. The Department will comply with the ALPR Surveillance Technology Policy, authorized use cases, prohibitions and impact report should the Department acquire or procure either the Stationary or Mobile application ALPR systems.

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:

- The benefits of the surveillance technology outweigh the costs.
- The Department's Policy safeguards civil liberties and civil rights.
- 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 ALPR has the following benefits for the residents of the City and County of San Francisco:

☐	Education	
☐	Community Development	
☐	Health	
☐	Environment	
X	Criminal Justice	On-street enforcement of: Stolen Vehicles; Amber Alerts; Silver Alerts; Unregistered Vehicles; Wanted Criminals; Parking

	Violations; Be on the Lookout (BOLO). Investigation tool for law enforcement inter-agency collaboration.

- ☐ Jobs
- ☐ Housing

Civil Rights Impacts and Safeguards

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

ALPR System Efficiencies are 98% with a correct Read Rate of 95% resulting in high validity of documentation of incidents. Highly effective read rates protect individuals and civil liberties by ensuring proper, correct capturing of information. SFPD recognizes that all people have a right to privacy and are committed to protecting and safeguarding this constitutional right, and that ALPR could raise concerns regarding real and/or perceived threats to civil liberties and privacy. Specifically, the Department and NCRIC recognize the following actual or potential public concerns:

Identity capture. The public may be concerned that ALPR will capture personally identifiable information (PII) without notice or consent. Although ALPR does not independently generate information that identifies vehicle occupants, license plate information can be used to determine the registered owner through a law enforcement investigation. In addition, contextual information like vehicle occupants, immediate surroundings, building addresses or pedestrians may be pictured. While contextual images are captured they are not searchable/indexed/scanned in the ALPR database. As a result, it is possible that individuals with access to this data could do additional research to identify an individual who may have been captured in the contextual color image. SFPD policy (Dept. Bulletin15-221) and NCRIC policy prohibit the use of ALPR data for anything other than legitimate law enforcement purposes. A license plate number identifies a specific vehicle, not a specific person. The potential to link to an identifiable person can only be realized through a separate step (inquiry to DMV etc.). Without this extra step, the license plate number and time/location data attached are not personally identifying. The investigative process identifies individuals while the ALPR system only automates the collection of the license plate numbers. Patrol vehicles outfitted with ALPR technology are constantly reassigned to District Stations based on operational need. ALPR outfitted vehicles are not concentrated in any one neighborhood in San Francisco.

ALPR data collected by SFPD and hosted by NCRIC is not used for the enforcement of Immigration Laws. SFPD complies with SF Admin Code Section 12H and 12I.

Misidentification. The public may be concerned that, if ALPR data is widely accessible and inaccurate, individuals may be misidentified as the person driving a vehicle that is violating parking rules, or is a criminal suspect. This could lead to improper government actions against such individuals. SFPD does

not make ALPR data widely accessible and uses ALPR to detect a vehicle, not the driver. The investigative step is required to identify an individual. The ALPR system does not identify the individual. Activity monitoring or non-relevant data. The public may be concerned that ALPR data will enable individuals' behaviors to be revealed to and/or monitored by DOT or other government agencies, their partners or affiliates, companies interested in targeted marketing, and/or the public. Such concerns may include basic information about when individuals are in certain locations, as well as concerns about what government or individuals may infer from this data (i.e. marital fidelity, religious observance, or political activity). Although ALPR data is gathered from public places, this could conflict with an individual's expectation of locational privacy. SFPD policy (Dept. Bulletin 15-221 and DGO 10.08) and existing NCRIC user policy prohibit the use of ALPR data for anything other than legitimate law enforcement purposes. ALPR systems are restricted to law enforcement personnel with a lawful purpose for using the system and are not shared with private sector companies and is considered exempt from disclosure under Ca. Public Records Act.

B. Fiscal Analysis of Costs and Benefits

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

Benefit		Description
☐	Financial Savings	
☐	Time Savings	
☐	Staff Safety	
☐	Data Quality	
☐	Other	

Number of FTE (new & existing)	2
Classification	Q-60 and Q-2

	Annual Cost	***Years***	***One-Time Cost***
Total Salary & Fringe			
Software			
Hardware/Equipment			$15,000
Professional Services			
Training			
Other			
Total Cost			***$15,000***

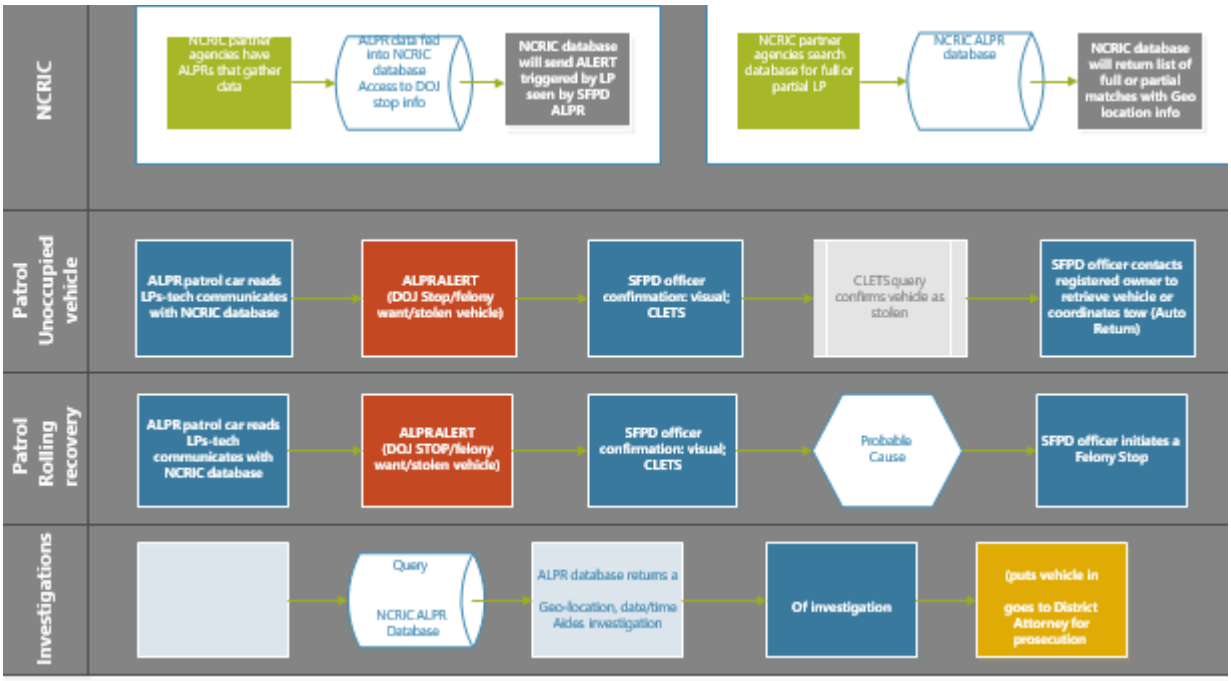
The Police Department funds its use and maintenance of the surveillance technology through:

- Aside from SFPD fleet operational budget, Vehicle Theft Abatement Funds (as defined by California Vehicle Code Section 9250.14) have been utilized to purchase and maintain these units in the past. There is no cost associated with NCRIC database access.

COMPARISON TO OTHER JURISDICTIONS

Other governmental entities and NCRIC partner agencies utilize ALPR data for similar purposes. NCRIC's area of responsibility includes the following counties: Del Norte, Humboldt, Mendocino, Sonoma, Lake, Napa, Marin, Contra Costa, San Francisco, San Mateo, Alameda, Santa Cruz, Santa Clara, San Benito and Monterey.

APPENDIX A: SFPD Use of ALPR Data



Appendix B: "Hot List" or "Hot Sheets" Definition Relating to ALPR Data Accessed by SFMTA

Stolen vehicles and stolen plates in the City and County of San Francisco as reported through Police Incident Reports and available through CABLE/CLETS

Appendix C: "Hot Lists" Categories That May Trigger ALPR Alerts, If ALPR Technology Is So Configured

For SFPD ALPR usage, "Hot List" refers to license plates that are associated with "DOJ Stop/Felony Wants". "DOJ Stop/Felony Want" are listed as follows:

- Stolen Vehicles
- Stolen Plates
- Felony Wants (Homicide, Domestic Violence, Kidnapping, Aggravated Assault, shootings etc.)
- Missing Person
- Protection Order
- Sex Offenders
- Canadian Stolen Plate
- Violent Gang Terrorist Organization File (VGTOF)
- Violent Offender
- Wanted Persons

Appendix D: Annual Reporting

Per SF Admin Code Section 96A.3, SFPD is required to quarterly report on specific data relating to Stops, Searches, Arrests and Use of Force. The Stop Data is collected via the California Department of Justice Stop Data Collection System (DCS). For purposes of reporting stop, search and associated demographic data, the report draws upon definitions provided by the state as part of AB953's regulatory implementation. The quarterly report requirements are established through state and local law codes and do not consider ALPR Alert tracking.

SFPD shall create administrative mechanisms and a reporting structure, if the technology capabilities allow, to track ALPR alerts and subsequent law enforcement action. The first annual report will be issued on January 30, 2022 and will be issued on the 30th day of January every year, thereafter. The report will be posted on the SFPD public website, through San Francisco Open Data- DataSF and if requested, will be reported to the Police Commission on an annual basis.

The annual report may include the following data sets:

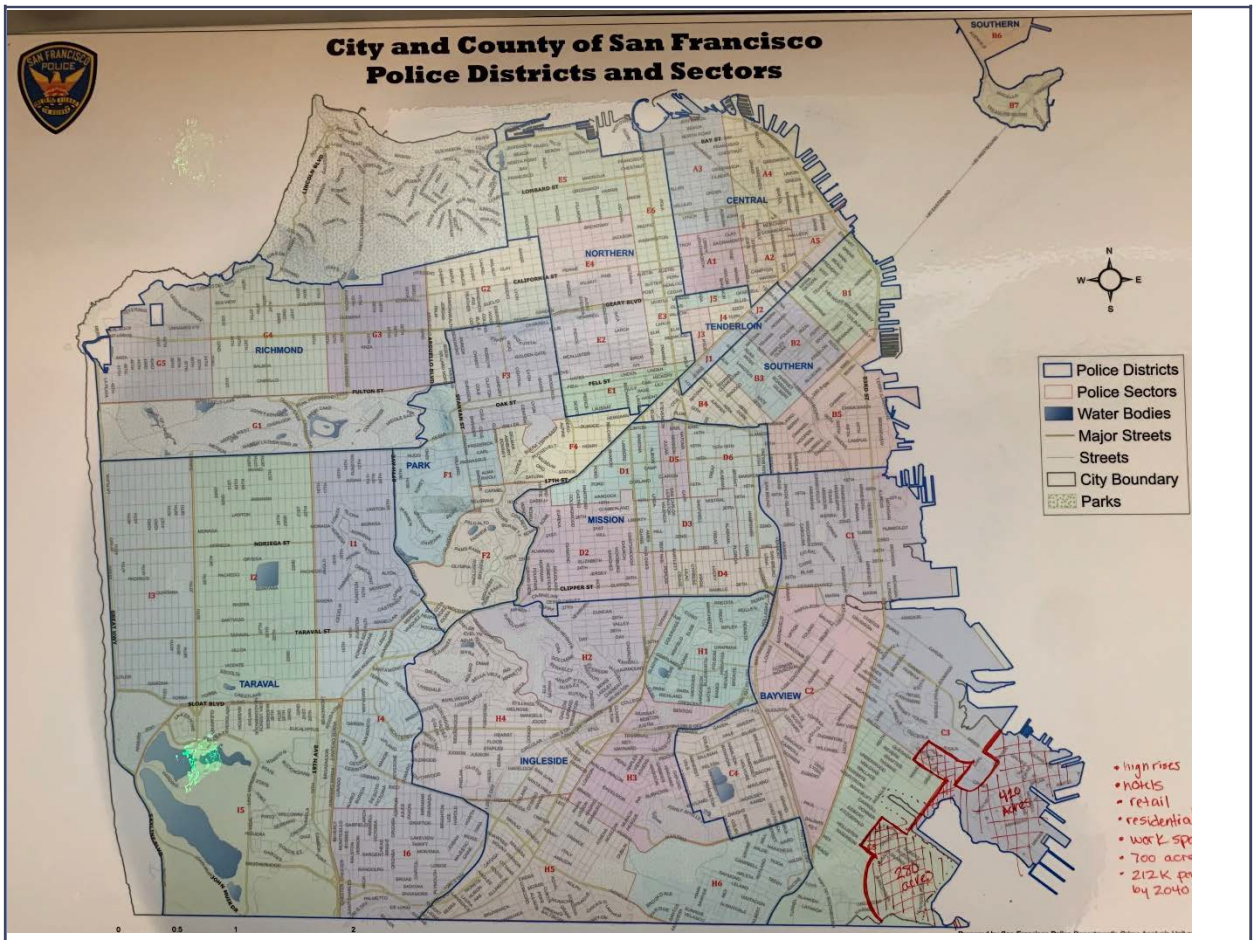
- Total Number of ALPR devices used
- Total number of traffic stops due to ALPR alerts and corresponding category of DOJ Stop/Felony want
- District Station Jurisdiction of traffic stops due to ALPR alerts
- Total number of manually entered ALPR canvas searches
- District Station Jurisdiction of manually entered ALPR canvas searches
- Number of stolen vehicles recovered due to ALPR alerts
- Number of Missing Persons (Silver/Amber Alerts) associated with a vehicle's license plate number
- Number of Missing Persons (Silver/Amber Alerts) associated with a vehicle's license plate number, located using ALPR
- Total Number of investigations aided by ALPR

Appendix F: SFPD Sector Patrol Map

The City of San Francisco is covered by ten (10) Police Districts: Central, Southern, Bayview, Mission, Northern, Park, Richmond, Ingleside, Taraval and Tenderloin. Each Police District includes sectors for police patrol. Each sector is patrolled during the day shift, swing shift and midnight shift, each shift overlapping the other. The patrol vehicles equipped with ALPR may be distributed across any of the sectors at any given time.

Sectors for Police Patrol by Station:

Central Station: A1- A5 Southern Station: B1-B5 Bayview Station: C1-C3 Mission Station: D1-D6 Northern Station: E1-E6 Park Station: F1-F4 Richmond Station: G1- G5 Ingleside Station: H1-H6 Taraval Station: I1-I6 Tenderloin Station: J1-J5


City and County of San Francisco
Police Districts and Sectors
SOUTHERN
CENTRAL
NORTHERN
RICHMOND
TENDERLOIN
SOUTHERN
PARK
MISSION
TARAVAL
BAYVIEW
INGLESIDE
Police Districts
Police Sectors
Water Bodies
Major Streets
Streets
City Boundary
Parks
• high rises
• hotels
• retail
• residentia
• work sp
• 700 acr
• 212K p
by 2040
410 Acres
250 acres

Surveillance Technology Policy

San Francisco Police Department
Automated License Plate Readers (ALPR)

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 ALPR 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

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 manner in which the ALPR will be used to support this mission, by describing the intended purpose, authorized and restricted uses, and requirements.

This Policy applies to all to department personnel that use, plan to use, or plan to secure ALPR 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

POLICY STATEMENT

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

Authorized Use(s):

1. Locate stolen, wanted, and or other vehicles that are the subject of investigation
2. To apprehend wanted persons subject to arrest warrants or who are otherwise lawfully sought by law enforcement.
3. To locate victims, witnesses, suspects, missing children, adults, and/or elderly individuals, including in response to Amber Alerts and Silver Alerts and others associated with a law enforcement investigation.
4. To assist with criminal investigations initiated by local, state and regional public safety departments by identifying vehicles associated with targets of criminal investigations.
5. Counter-terrorism: Identify potential threats to critical infrastructure sites.
6. For other law enforcement purposes as authorized by law: Investigations of major crimes.

Prohibited use cases include any uses not stated in the Authorized Use Case section.

Departments may use information collected only for legally authorized purposes, and may not use that information to unlawfully discriminate against people based on race, ethnicity, political

Surveillance Oversight Review Dates
COIT Review: January 21, 2021
Board of Supervisors Review: TBD

opinions, religious or philosophical beliefs, trade union membership, gender, gender identity, disability status, sexual orientation or activity, or genetic and/or biometric data. Additionally, departments may not use automated systems to scan footage and identify individuals based on any of the categories listed in the preceding sentence.

- An ALPR alert alone does not substantiate law enforcement response or contact. Contacting an individual solely based on an ALPR alert in the absence of confirming disposition of the vehicle (stolen or recovered), verifying that the observed license plate number matches the ALPR data, and verifying the reason a vehicle or owner is wanted or of interest shall be prohibited.
- No SFPD member shall access ALPR data for any use other than the authorized use cases herein
- ALPR scanning is limited to vehicles exposed to public view.
- No content captured by ALPR cameras other than license plate and vehicle information, geo-location, and time date of capture, shall constitute cause for police enforcement.

BUSINESS JUSTIFICATION

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

ALPR readers allow for automatic and efficient identification of license plates that may be associated with criminal activity or missing persons. The identification of a license plate allows SFPD to recover a victim's vehicle, investigate a crime and lawfully apprehend suspects. SFPD is able to protect life and property using this technology.

In addition, ALPR promises to benefit residents in the following ways:

☐	Education	
☐	Community Development	
☐	Health	
☐	Environment	
X	Criminal Justice	On-street enforcement of: Stolen Vehicles; Amber Alerts; Unregistered Vehicles; Wanted Criminals; Parking Violations; Be on the Lookout (BOLO), assists criminal investigations
☐	Jobs	
☐	Housing	

In addition, the following benefits are obtained:

Benefit		Description
☐	Financial Savings	
X	Time Savings	
X	Staff Safety	
☐	Data Quality	

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 kept up to date and maintained.
Safety:	Surveillance technology must be operated in a safe manner. Surveillance technology should not be operated in a way that infringes on resident civil rights, including privacy, or causes personal injury or property damage.
Data Collection:	Departments shall minimize the use, collection, and retention of Personally Identifiable Information (PII) to what is strictly necessary to accomplish the intended purpose of the surveillance technology. Department shall only collect data required to execute the authorized use case. All data collected by the surveillance technology, including PII, shall be classified according to the City's Data Classification Standard. Should information be incidentally collected that is not necessary to accomplish the intended purpose of the surveillance technology, including information that may be used to identify persons or private information, Department shall remove all incidental PII from raw data.

The surveillance technology collects the following data types:

Data Type(s)	*Format(s)*	*Classification*
Digital images of vehicle license plates and their associated vehicles	Encoded and stored in SQL	Level 3
Date and time the license plate passes a digital-image site where an ALPR is located	SQL server datetime	Level 3

Notification: Decals identifying that ALPR is in use will be placed on marked patrol vehicles outfitted with ALPR. Decals will not be placed on unmarked vehicles outfitted with ALPR, as it poses operational and officer safety issues. Posted signs are not logistically feasible as marked patrol vehicles are constantly reassigned based on operational needs, which fluctuate.

The public notice shall include the following items in its public notice:

- X Type of technology in use
- Information on the surveillance technology
- Description of the authorized use
- Type of data collected
- Will persons be individually identified
- Data retention
- Department identification
- Contact information

Access: All parties requesting access must adhere to the following rules and processes: US DOJ's

*California Law Enforcement Telecommunications System (CLETS) rules and regulations, NCRIC ALPR policy, Dept. Bulletin 15-221 and DGO 10.08, SFPD members must be approved to access the ALPR data and the data must be tied to an investigation and per.

*CLETS is the computer network that connects public safety agencies across the state to criminal histories, driver records, and other databases. DOJ grants each public safety agency's access.

Officers shall not stop a vehicle solely based on an ALPR alert. Before stopping a vehicle based on an ALPR alert for a stolen or felony want, the officer conducting the stop shall:

1. Visually verify the alphanumeric characters on the plate of the suspect vehicle to be detained, AND
2. Verify through CLETS or through the Department of Emergency Management (dispatch has CLETS access) that the license plate on the vehicle to be detained is currently listed on the DOJ database as stolen or wanted.

Other ALPR alerts (e.g. 852 "auto boost", 459 "burglary", 10-43 "of interest to special investigation", etc.) do not provide officers with justification to conduct a traffic stop or detain a vehicle and the occupants. Sufficient probable cause has not been established to stop a "vehicle of interest" that is the focus of a criminal investigation.

These alerts may provide officers with additional instructions or information when a vehicle is located.

Officers should follow the instructions on the alert, use discretion, and have independent probable cause to justify a traffic stop.

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.

- Sworn members, Civilian Crime analysts, Radio Shop Technicians (access to hardware)

The following providers are required to support and maintains the surveillance technology and its associated data to ensure it remains functional:

- NCRIC hosts the ALPR data repositories. Vehicle Theft Abatement Funds pay for maintenance.

B. Members of the public

ALPR data is classified as Level 3 Sensitive. ALPR data has previously been deemed as exempt from the California Public Records Act, however each request submitted by a member of the public will be reviewed to determine whether the data can be released. SFPD shall comply with the requirements of the Federal and State Constitutions, and federal and State civil procedure laws and rules.

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). To protect surveillance technology information from unauthorized access and control, including misuse, Departments shall, at minimum, apply the following safeguards: Northern California Regional Intelligence Center (NCRIC) hosts the ALPR data collected by SFPD equipment. Only Authorized SFPD members with an account can access the repository of data via the Back Office Server Software (BOSS) application. SFPD Information Technology Division and Special Investigations Division will not grant user access to ALPR data unless they are approved to do so. All SFPD members are required to comply with CLETS and department written directives. Non-compliance may result in progressive discipline measures.
Data Sharing:	If the ALPR data is not exempt from California Public Records Act, SFPD 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. SFPD will endeavor to ensure that other agencies or departments that may receive data collected by [the Surveillance Technology Policy that it operates] will act in conformity with this Surveillance Technology Policy. 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. SFPD 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) SFPD shall ensure all PII and restricted data is de-identified or adequately protected to ensure the identities of individual subjects are effectively safeguarded. Each department that believes another agency or department receives or may receive data collected from its use of STs should consult with its assigned deputy city attorney regarding their response.

The Department currently participates in the following sharing practices:

A. Internal and External 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 discovery laws
- Data sharing occurs at the following frequency: as-needed

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

X 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.

X 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 shared data will be done in a cost-efficient manner and exported in a clean, machine-readable format.

B. External Data Sharing:

Department shares the following data with the recipients:

- NCRIC 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.
- Data sharing occurs at the following frequency: as-needed.

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.).

If Department's general counsel determines ALPR data can be disclosed in response to a public information request, the department will redact PII as it will be considered investigative/evidentiary material. The Department may use its discretion when releasing investigative/evidentiary material per SFPD DGO 3.16.

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:

SFPD defers to the NCRIC retention standard: ALPR records are maintained for 12 months from capture. If a record is connected to a criminal investigation or criminal intelligence file it may be retained for 5 years.

ALPR Technology data associated with a criminal investigation may be downloaded onto an electronic storage device or printed. Downloaded, copied, and printed data shall be maintained in accordance with applicable local, state and federal evidentiary laws, to include retaining the data through the adjudication of a case in a recognized court of law, as well as allotment of time for an appeals process and statute of limitations.

ALPR does not collect PII data and as such PII data shall not be kept in a form which permits identification of data subjects

Departments must establish appropriate safeguards for PII data stored for longer periods.

Data will be stored in the following location:

- ☐ Local storage
- ☐ Vendor managed storage
- ☐ Department of Technology Data Center
- ☐ Software as a Service Product
- ☐ Cloud Storage Provider

Data Disposal: Upon completion of the data retention period, Department shall dispose of data in the following manner:

Practices: ALPR data are cleared after 1 year from capture unless associated with a criminal investigation.

	Processes and Applications: If ALPR data is associated with a criminal investigation and must be disposed of due to retention schedule, confidential information shall be disposed of according to SFPD Department Notice 20-166: https://www.sanfranciscopolice.org/sites/default/files/2020-08/SFPDNotice20.116.20200804.pdf CLETS Information (print-outs, CDs, Flash Drives, Diskettes or any other storage media) no longer has a necessary law enforcement purpose, members shall dispose of it in the following manner: • Hard copies and print-outs - with the exception of staples and paper clips - shall be placed in the gray colored Shred Works shredding bins. Facility Coordinators, or other designated SFPD employees, shall ensure that these bins are always located in a secure area of the SFPD facility. • If a member has stored CLETS Information on any electronic storage media, the member shall be responsible for its proper destruction.
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 must receive training on data security policies and procedures. At the very least, 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. 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. NCRIC provides training information to the Department.

COMPLIANCE

Department shall oversee and enforce compliance with this Policy using the following methods:

These policies will have the same compliance requirements as all Department Written Directives and Police Commission Resolutions.

The Department shall assign the following personnel to oversee Policy compliance by the Department and third-parties: Deputy Chief of Investigations, Lieutenant of Special Investigations Division.

In addition, each member of the department belongs to a chain of command. The Officer in Charge (OIC) of that chain of command is responsible for overseeing compliance with all SFPD written directives and the surveillance technology polices. 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.

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. 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 DPA. Depending on the severity of the allegation of misconduct, the Chief or the DPA 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.

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.

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.
Sensitive Data:	Data intended for release on a need-to-know basis. Data regulated by privacy laws or regulations or restricted by a regulatory agency or contract, grant, or other agreement terms and conditions.
Exigent Circumstances	An emergency involving imminent danger of death or serious physical injury to any person that requires the immediate use of Surveillance Technology or the information it provides.

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

Public:

Members of the public can register complaints with the Department of Police Accountability (DPA). 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.

Department shall acknowledge and respond to concerns in a timely and organized response. To do so, Department shall:

SFPD will update the SFPD public website to include surveillance technology policies and will include a general email address for public inquiries. The general email box will be assigned to a staff member in the Chief's Office.

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.

1. A description of the product and services addressed by the Surveillance Technology, including the identity of any provider(s) whose services are essential to the functioning or effectiveness of the Surveillance Technology equipment or services for the intended purpose.

Vehicle-mounted Automated License Plate Recognition (ALPR) technology shall be used to automate the processing of vehicle license plate information by transforming images into alphanumeric characters with optical recognition software and storing those images, plate information and related metadata, including time and geo-location information.
Vehicle-mounted Automated License Plate Recognition (ALPR) technology automates the processing of vehicle license plate and compliance information. Specifically, ALPR:
uses specially-designed cameras mounted on law enforcement vehicles to capture digital images of license plates and vehicles as they drive through the streets;
alphanumeric characters are translated using optical character recognition (OCR) software to enable;

- Searches full plates, with color pictures of identified vehicles for plate read verification
- Partial plate searches that return possible matches to assist with identifying suspects' vehicles
- stores the images, plate information, and related metadata in a restricted-access database;
- compares the license plate characters with state, local law enforcement and customized hotlists;

Mobile ALPR Systems
Mobile ALPR Systems assist on-street patrol officers checking for criminal activity by capturing and analyzing license plates against known databases. The cameras are mounted securely below the lightbar for limited visual interference.

Features and Benefits
Offers high resolution coverage for a full lane of traffic with up to two concurrent vehicles in the field of view.
Instantly checks captured plates against one or more databases of interest to immediately alert officers of hits.
Increases spatial awareness for improved officer safety.
Enhances proactive, preventative enforcement by enabling more intelligent investigations. ALPR database stores all collected data in a central location to support data analysis, data queries and reporting for law enforcement investigations.

System Components
Mobile ALPR Camera(s) – Each System has 1 to 4 dual (IR and color) mobile cameras.
Mobile ALPR Processor – Each processor simultaneously supports up to 4 mobile cameras.
Brackets – A variety of camera mounting brackets for various vehicles and light-bar designs.
In-car software – PAGIS software provides the graphical user interface (GUI) and in-car application. It compares ALPR images against federal, local or customized hotlists and sends alert when a match occurs.

Other Existing ALPR Systems Available
Stationary – Cameras may be permanently affixed to a specific location like a traffic light, telephone pole or at entrances of facilities or freeway exit ramps.
Semi-Stationary – ALPR system is located on a trailer which can be moved to different locations as operational needs change.
Smartphone Applications – Mobile applications can be uploaded onto patrol officer's Department issued smartphones and use the smartphone's camera capabilities.

SFPD does not have access to, own, lease or use Stationary ALPR cameras or Smartphone ALPR applications. The Department will comply with the ALPR Surveillance Technology Policy, authorized use cases, prohibitions and impact report should the Department acquire or procure either the Stationary or Mobile application ALPR systems.

2. A description of the purpose(s) for which the Surveillance Technology equipment or services are proposed for acquisition, including the type of data that may be collected by the Surveillance Technology equipment or services.

Technology Use:

ALPR readers allow for automatic and efficient identification of license plates that may be associated with criminal activity or missing persons. The identification of a license plate allows SFPD to act quickly and respond to an associated crime, recover a victim's vehicle, investigate a crime and lawfully apprehend suspects. SFPD is able to protect life and property using this technology.

PII:

False. PII is not collected by ALPR technology

3. The uses that are authorized, the rules and processes required prior to such use, and uses of the Surveillance Technology that will be expressly prohibited.

Authorized Uses:

Locate stolen, wanted, and or other vehicles that are the subject of investigation

To locate victims, witnesses, suspects, missing children, adults, and/or elderly individuals, including in response to Amber Alerts and Silver Alerts and others associated with a law enforcement investigation.

To assist with criminal investigations initiated by local, state, federal, and regional public safety departments by identifying vehicles associated with targets of criminal investigations.

Counter-terrorism: Identify potential threats to critical infrastructure sites.

For other law enforcement purposes as authorized by law: Investigations of major crimes.

Rules:

Prohibited Uses:

1. Officers shall not stop a vehicle solely based on an ALPR alert. Before stopping a vehicle based on an ALPR alert for a stolen or felony want, the officer conducting the stop shall:
   Visually verify the alphanumeric characters on the plate of the suspect vehicle to be detained, AND
   Verify through the Department of Emergency Management (dispatch) or through a Ca. DOJ's California Law Enforcement Telecommunications System (CLETS) computer return that the license plate on the vehicle to be detained is currently listed on the DOJ database as stolen or wanted.
   Other ALPR alerts (e.g. 852,459, 10-43, etc.) do not provide officers with justification to conduct a traffic stop or detain a vehicle and the occupants. Sufficient probable cause has not been established to stop a "vehicle of interest" that is the focus of a criminal investigation.

These alerts may provide officers with additional instructions or information when a vehicle is located. Officers should follow the instructions on the alert, use discretion, and have independent probable cause to justify a traffic stop.

2. No SFPD member shall access ALPR data for any use other than the authorized use cases herein
3. Manual entry to trigger an ALPR alert, such as for canvassing or locating a victim, witness or missing person, shall be prohibited except to aid in an active investigation or active criminal court case.
4. ALPR scanning is limited to vehicles exposed to public view.
5. No content captured by ALPR cameras other than license plate and vehicle information, geo-location information, and time date of capture, shall constitute cause for police enforcement.

4. A description of the formats in which information collected by the Surveillance Technology is stored, copied, and/or accessed.

Data Type	Formats STP
Digital images of vehicle license plates and their associated vehicles	Encoded and stored in SQL
Date and time the license plate passes a digital-image site where an ALPR is located	SQL server datetime

5. The specific categories and titles of individuals who are authorized by the Department to access or use the collected information, including restrictions on how and under what circumstances data collected with Surveillance Technology can be analyzed and reviewed, and the rules and processes required prior to access or use of the information.

Employee Job Classification & Title: Police Officers, investigators, Sergeants, Crime Analysts, Lieutenants of SID, or their designee, Deputy Chief of Investigations, Assistant Chiefs and Chief of Police

Department:

SFPD

If applicable, contractor or vendor name:

NCRIC, NICRIC database vendor and NCRIC partner agencies

Rules and processes required prior to data access or use:

NCRIC hosts the ALPR data repositories accessed by a database provided by a vendor available on the SFPD Network for approved users. SFPD IT and SID do not provide access to SFPD members who are not approved users. All SFPD members are required to comply with department written directives. Non-compliance results in progressive discipline measures as outlined under the Compliance Section of this Policy.

6. The general safeguards that protect information from unauthorized access, including encryption and access control mechanisms.

All users of NCRIC ALPR equipment or accessing NCRIC ALPR Data are required to acknowledge that they have read and understood the NCRIC ALPR Policy prior to use of the ALPR System. Only law enforcement NCRIC partners have access to the database.

7. The limited time period, if any, that information collected by the Surveillance Technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s) enumerated in the Surveillance Technology Policy, the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond that period

Retention:

NCRIC advises ALPR data retention of 12 months. If a record is connected to a criminal investigation or criminal intelligence file it may be retained for five years.

ALPR Technology data associated with a criminal investigation may be downloaded onto an electronic storage device or printed. Downloaded, copied, and printed data shall be maintained in accordance with applicable local, state and federal evidentiary laws, to include retaining the data through the adjudication of a case in a recognized court of law, as well as allotment of time for an appeals process and statute of limitations.

Reason for retention:

NICRIC policy and SFPD Retention schedule

Deletion process:

NCRIC advises ALPR data retention of 12 months from date of capture. If a record is connected to a criminal investigation or criminal intelligence file it may be retained for 5 years.

ALPR Technology data associated with a criminal investigation may be downloaded onto an electronic storage device or printed. Downloaded, copied, and printed data shall be maintained in accordance with applicable local, state and federal evidentiary laws, to include retaining the data through the adjudication of a case in a recognized court of law, as well as allotment of time for an appeals process and statute of limitations.

Retention exemption conditions:

if general counsel determines that ALPR data can be disclosed in response to a public information request, the department will redact information linked to an individual as it will be considered investigative material.

8. How collected information can be accessed or used by members of the public, including criminal defendants

Will the data be accessible to the public:

ALPR 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.
How it can be accessed: https://www.sanfranciscopolice.org/get-service/public-records-request

9. Which governmental agencies, departments, bureaus, divisions, or units that may receive data collected by the Surveillance Technology operated by the Department, including any required justification or legal standard necessary to share that data and how it will ensure that any entity receiving such data complies with the Surveillance Technology Policy.

Name of agency: 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 discovery laws; Other law enforcement offices as part of a criminal or administrative investigation; Parties to civil litigation, or other third parties, in response to a valid Court Order; From NCRIC: Only law enforcement personnel that have access to the ALPR database and have: 1. Agreed to the NCRIC privacy policy and non-disclosure agreement. 2. A criminal case or incident number/name. 3. A lawful purpose with a need to know and right to know the information.

ALPR data collected by SFPD and hosted by NCRIC is not used for the enforcement of Immigration Laws. SFPD complies with SF Admin Code Section 12H and 12I.

Justification: Past and current practice associated with the NCRIC partnership

10. The training required for any individual authorized to use the Surveillance Technology or to access information collected by the Surveillance Technology

Training required:

true

Description of training:

Only persons trained in the use of the NCRIC ALPR system, including its privacy and civil liberties protections, shall be allowed access to NCRIC ALPR Data. Training content shall consist of:
- Legal authorities, developments, and issues involving the use of ALPR Data and technology
- Current NCRIC Policy regarding appropriate use of NCRIC ALPR systems;
- Evolution of ALPR and related technologies, including new capabilities and associated risks;
- Technical, physical, administrative, and procedural measures to protect the security of ALPR Data against unauthorized access or use; and
- Practical exercises in the use of the NCRIC ALPR system

Training shall be updated as technological, legal, and other changes that affect the use of the NCRIC ALPR system occur. In no case shall a person utilize the NCRIC ALPR system if he/she has not completed training in more than a year.

11. The mechanisms to ensure that the Surveillance Technology Policy is followed, including internal personnel assigned to ensure compliance with the policy, internal recordkeeping of the use of the technology or access to information collected by the technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the sanctions for violations of the policy

Oversight process:

Should a member of the department uncover a violation of ALPR, they will notify the Internal Affairs Unit which will conduct an internal investigation through the Chief of Staff/Internal Affairs Unit. The results of the investigation will be reported to the Chief of Police, who may take disciplinary or policy/procedure action as indicated in the Compliance section of this policy.

Compliance personnel titles:

Q-60 Lieutenant in Special Investigations Division (SID) and Deputy Chief of Investigations, SFPD

12. What procedures will be put in place by which members of the public can register complaints or concerns, or submit questions about the deployment or use of a specific Surveillance Technology, and how the Department will ensure each question and complaint is responded to in a timely manner.

Complaint procedures:

Complaints from members of the public will be forwarded to the Department of Police Accountability (DPA) for investigation. DPA manages the complaint responses.

Departmental follow-up process:

DPA manages the complaint follow- up process. The Surveillance Technology Polices will have the same procedural authority as any Department Written Directive. Non-compliance can result in progressive discipline or sustained complaints.

Members of the public can register complaints with the Department of Police Accountability https://sfgov.org/dpa/complaints. *Members of the public can register questions and concerns or submit questions via calls or emails at 311.org*

Allegation procedures:

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 that generally describes the corrective measures taken to address such allegation.

If the Department finds the allegation to be unfounded and subsequently does not take corrective measures, the Department may respond to the complainant directly confirming the justified use of the technology.

Surveillance Impact Report

Public Works
Unmanned Aircraft Systems (Drones)

As required by San Francisco Administrative Code, Section 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 Unmanned aerial vehicles ("UAV" or "Drone" technology).

DESCRIPTION OF THE TECHNOLOGY

The Department's mission is to: enhance the quality of life in San Francisco as responsible stewards of the public's physical assets by providing outstanding service in partnership with the community. We design, build, manage, maintain, green, protect and improve the City's public spaces (infrastructure, public right of way and facilities) with skill, pride, innovation, and responsiveness.

In line with its mission, the Department uses Unmanned aerial vehicles ("UAV" or "Drone" technology) to Drone technology will support our mission through the following:

1. In times of disaster preparedness or post-disaster mitigation, drones will provide critical emergency response functions such as logistical support for emergency routing, life safety, and cleanup efforts, not only assisting in protecting physical assets and public spaces but human life as well;
2. Drones will support the maintenance efforts of City-owned street trees pursuant to our mission of greening and improving City public spaces;
3. Drones will support the objective of maintaining city owned properties and landscapes by safely providing detailed photographic data and documentation to assist in the planning of corrective or new construction work by roofers, architects, engineers, electricians, PMs, CMs and other personnel.

Public Works shall use Unmanned aerial vehicles ("UAV" or "Drone" technology) only for the following authorized purposes:

1. Disaster preparedness and response
2. Environmental monitoring and documentation
3. Inspect/Survey properties & assets
4. Project inspection and documentation
5. Surveying/Mapping data collection

Prohibited use cases include any uses not stated in the Authorized Use Case section.

Departments may use information collected from technology only for legally authorized purposes, and may not use that information to unlawfully discriminate against people based on race, ethnicity, political opinions, religious or philosophical beliefs, trade union membership, gender, gender identity, disability status, sexual orientation or activity, or genetic and/or biometric data. Additionally,

departments may not use automated systems to scan footage and identify individuals based on any of the categories listed in the preceding sentence.

Department technology may be deployed in the following locations, based on use case:

- **For city and trees data collection**: Neighborhoods, parks, and other areas within San Francisco where City-owned street trees are located.
- **For asset/building data collection**: Islais Creek & Lefty O'Doul bridges, roadway structures such as retaining walls or stairs or bridges, rooftops of City properties where solar panels or other equipment such as HVAC are located, or exterior walls of buildings, including schools, Police and Fire stations, public libraries, and other City owned buildings, infrastructure, and facilities.
- **For Public Works project education/marketing/promotions**: various locations involving Public Works right-of-way or facility construction or repairs.
- **For surveying/mapping activity**: survey site locations along streetscapes, landscape areas, steep hillsides and cliffs, at bridges and fixed structures such as piers, etc.
- **During disaster/emergency response operations**: Disaster areas, emergency evacuation routes, and other areas within San Francisco requiring Public Works safety response operations.

TECHNOLOGY DETAILS

The following is a product description of Drones or Unmanned Aerial Vehicles:

- Phantom 4 RTK is an aerial survey drone that combines centimeter-level navigation and positioning with a high-performance imaging system for use during surveying, mapping or inspection operations.
- Intel Falcon 8+ is designed to provide consistent, stable flights with weak GPS signals, high winds as well as resistance to magnetic field.
- Falcone 8+ drone can provide detailed data for orthography and 3D reconstruction, with millimeter accuracy for ground sample distance. Unique, patented "V-shaped design enables a greater than 180-degree view from top to bottom. Falcon 8+ system can be configured as a closed system with isolated, on-board data storage that does not transmit data over the public internet.
- The Leica Aibot AX20 is built on a DJI UAV platform which can accommodate various sensor payloads for surveying, mapping and construction aerial data capture solutions.
- DJI Mavic 2 Enterprise Dual is an aerial survey drone that combines navigation and positioning with a high-performance imaging system for use during surveying, mapping or inspection operations.

A. How It Works

To function, Drones or Unmanned Aerial Vehicles incorporate unmanned, remotely-operated aircraft with onboard visual recording equipment, for the purpose of capturing images from an aerial perspective.

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:

- The benefits of the surveillance technology outweigh the costs.
- The Department's Policy safeguards civil liberties and civil rights.
- 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 Drone technology has the following benefits for the residents of the City and County of San Francisco:

X	Education	Drone imagery to promote Public Works projects and demonstrate use of tax dollars on projects.
▪	Community Development	
▪	Health	
X	Environment	Drone imagery to collect data on street-trees for maintenance and safety reasons.
▪	Criminal Justice	
▪	Jobs	
▪	Housing	
X	Other	Public Safety: to inspect tree canopies for damaged limbs (fall risks), to provide support when determining safety routes during emergencies, to collect data and information during emergencies (particularly in the event of loss of cellular communications) and during post-disaster cleanup operations.

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:

Public Works strives to mitigate all potential civil rights impacts through responsible technology and associated data use policies and procedures and intends to use drones and their associated data exclusively for authorized uses cases. All other uses, including surveillance of San Francisco residents or groups, are expressly prohibited. Public Works drone operators/pilots will be prohibited from

intentionally capturing data that can be used to identify individuals. Auto license plate information shall also not be deliberately captured.

To mitigate the risk of potential embarrassment, emotional distress, self-censorship or diminished civic engagement by SF residents whose personal information may be unintentionally captured, Public Works requires the "scrubbing" or otherwise obscuring/blurring (through use of image editing software) of all collected data to remove facial images or other personally identifiable information unintentionally captured by aerial drones.

All collected data, irrespective of the location of data capture or the identifying characteristics of captured persons, is subject to the same scrubbing processes and procedures. The image software scrubbing process obscures and blurs all data using either built-in AI recognition settings or through manual efforts by software operator. To protect drone data from potential breach, misuse or abuse that may result in civil rights impacts, data is maintained on secure, department-owned servers.

Only persons authorized to utilize the raw data may access the information and are required to maintain records of access using a drone data access log. Only data that has been edited to remove PII will be shared and stored on servers, and sharing will only occur with partner CCSF agencies for whom Public Works has been contracted to provide inspection, maintenance, repair, or construction services.

To further protect data and any personal resident information captured by a drone, all raw data will be permanently erased after it has been processed and edited to blur or obscure human features and license plate information. To mitigate any potential impacts to residents' physical safety or economic loss through property damage, all SFPW drone operators must have valid UAV pilot certifications.

C. Fiscal Analysis of Costs and Benefits

The Department's use of Drones or Unmanned Aerial Vehicles yields the following business and operations benefits:

Benefit		Description
X	Financial Savings	Drones can be far more time efficient and cost effective when conducting asset inspections, by mitigating the need for traffic control, expensive scaffolding/swing stage or other equipment, and can provide more detailed photographs/videos of the assets or areas in need of maintenance or repairs than can be done manually, minimizing labor costs.
X	Time Savings	Deploying a drone can provide time savings over setting up and employing equipment such as scaffolds/swing stages/scissor-lift vehicles, etc.
X	Staff Safety	Drones can be deployed to dangerous locations instead of personnel, such as rooftops, at the sides of building/bridges, along cliff areas or areas prone to erosion.

X	Data Quality	Some locations which are difficult to access by personnel may be more easily photographed using drone technology, thereby achieving better data.

Number of FTE (new & existing)	Estimate 4 existing employees: Mapping staff: 10 hrs/wk; Structural Section staff: 2 hrs/wk; Yard staff: 3 hrs/wk; Architectural staff: 4 hrs/wk		
Classification	Surveyors (5310-14); Engineers (5201-18); Stationary Engineers (7333-35); BUF Inspectors (3435); Architectural Administrator (5120); Architects (5260-74)		
	Annual Cost	***Years***	***One-Time Cost***
Total Salary & Fringe	*$148,000*	1	*$148,000*
Software	*$15,000*	1	$15,000
Hardware/Equipment	*$35,000*	1	$35,000
Professional Services	*$30,000*	1	$30,000
Training	*$5,000*	*1*	*$5,000*
Other			
Total Cost			***$233,800***

The Department funds its use and maintenance of the surveillance technology through:

- Personnel: Staff time devoted to use of drone for Inter-departmental work such as inspecting another agency's building can be charged to that agency as a line item cost. Time used to inspect Public Works assets will be charged as any other labor costs associated with project or inspection work.
- Equipment: Funding to pay for cost of equipment purchase/lease and license for software to remove PII has been requested as part of the FY21 budget initiative process.

COMPARISON TO OTHER JURISDICTIONS

Unmanned aerial vehicles ("UAV" or "Drone" technology) are currently utilized by other governmental entities for similar purposes.

APPENDIX A: DPW Drone Checklist (Snapshot)

Drone Checklist for Drone Flight PMs, pilots, and data editors:

Item Number	Activity Category	Sub Category	Who	What	How	Where	When
1	Pre-flight	Policy Review	• Drone Pilot (Public Works staff and/or 3rd party contractor) • Project Manager	Review of Public Works Drone Policy ***note:*** *as of 2.27.20 "Public Works Drone Policy" is CCSF Employee Drone Policy; will be replaced by Public Works Surveillance Technology Policy upon COIT review and approval*	• Distribute electronic or paper copy of Policy to all parties for review.	Policy Statement for Drone Pilots and PMs (PW and Contractors)	• Public Works staff: prior to flight • Contractor: at contract execution AND prior to flight
2	Pre-flight	COIT notification	• Drone Flight Project Manager ("PM")	Submission of Flight Summary Form	• Complete and submit "Flight Summary Form" at Drone Usage Reporting sharepoint site.	CCSF Drone Usage Reporting site	24 hours in advance of flight
3	Pre-flight	Public notification	• PM/Rachel Gordon	Posting of Public Notices	• Complete "Public Notice template" form • Submit completed notice to Rachel Gordon for posting at location.	Public Notice	24 hours in advance of flight

Surveillance Technology Policy

Public Works
Unmanned Aircraft Systems (Drones)

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 vehicles ("UAV" or "Drone" technology) 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

The Department's mission is to: enhance the quality of life in San Francisco as responsible stewards of the public's physical assets by providing outstanding service in partnership with the community. We design, build, manage, maintain, green, protect and improve the City's public spaces (infrastructure, public right of way and facilities) with skill, pride, innovation, and responsiveness.

The Surveillance Technology Policy ("Policy") defines the manner in which the Unmanned aerial vehicles or Drone technology 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 Unmanned aerial vehicles or Drone technology, including employees, suppliers, contractors, and volunteers while working on behalf of the City with the Department.

POLICY STATEMENT

Unmanned Aerial Vehicles and Drone technology for the Department is limited to the following use cases and is subject to the requirements listed in this Policy.

Authorized Use(s):

1. Disaster preparedness and response
2. Environmental monitoring and documentation
3. Inspect/Survey properties & assets
4. Project inspection and documentation
5. Surveying/Mapping data collection

Prohibited use cases include any uses not stated in the Authorized Use Case section.

Departments may use information collected from technology only for legally authorized purposes, and may not use that information to unlawfully discriminate against people based on race, ethnicity, political opinions, religious or philosophical beliefs, trade union membership, gender, gender identity, disability status, sexual orientation or activity, or genetic and/or biometric data. Additionally, departments may not use automated systems to scan footage and identify individuals based on any of the categories listed in the preceding sentence.

Surveillance Oversight Review Dates
COIT Review: July 17, 2020
Board of Supervisors Review: TBD

BUSINESS JUSTIFICATION

Unmanned aerial vehicles and Drone technology supports the Department's mission and provides important operational value in the following ways:

1. In times of disaster preparedness or post-disaster mitigation, drones will provide critical emergency response functions such as logistical support for emergency routing, life safety, and cleanup efforts, not only assisting in protecting physical assets and public spaces but human life as well;
2. Drones will support the maintenance efforts of City-owned streets and trees pursuant to our mission of greening and improving City public spaces;
3. Drones will support the objective of maintaining city owned properties and landscapes by safely providing detailed photographic data and documentation to assist in the planning of corrective or new construction work by roofers, architects, engineers, electricians, PMs, CMs and other personnel.

In addition, unmanned aerial vehicles and Drone technology promises to benefit residents in the following ways:

X	Education	Drone imagery to promote Public Works projects and demonstrate use of tax dollars on projects.
▪	Community Development	
▪	Health	
X	Environment	Drone imagery to collect data on street-trees for maintenance and safety reasons.
▪	Criminal Justice	
▪	Jobs	
▪	Housing	
X	Other	Public Safety: to inspect tree canopies for damaged limbs (fall risks), to provide support when determining safety routes during emergencies, to collect data and information during emergencies (particularly in the event of loss of cellular communications) and during post-disaster cleanup operations.

In addition, the following benefits are obtained:

Benefit		**Description**
X	Financial Savings	Drones can be far more time efficient and cost effective when conducting asset inspections, by mitigating the need for traffic control, expensive scaffolding/swing stage or other equipment, and can provide more detailed photographs/videos of the assets or areas in need of maintenance or repairs than can be done manually, minimizing labor costs.

X	Time Savings	Deploying a drone can provide time savings over setting up and employing equipment such as scaffolds/swing stages/scissor-lift vehicles, etc.
X	Staff Safety	Drones can be deployed to dangerous locations instead of personnel, such as rooftops, at the sides of building/bridges, along cliff areas or areas prone to erosion.
X	Data Quality	Some locations which are difficult to access by personnel may be more easily photographed using drone technology, thereby achieving better data.

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.

Specifications:	The software and/or firmware used to operate the surveillance technology must be kept up to date and maintained.
Safety:	Surveillance technology must be operated in a safe manner. Surveillance technology should not be operated in a way that infringes on resident civil rights, including privacy, or causes personal injury or property damage.
Data Collection:	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. Departments shall minimize the use, collection, and retention of Personally Identifiable Information (PII) to what is strictly necessary to accomplish the intended purpose of the surveillance technology. Department shall only collect data required to execute the authorized use case. All data collected by the surveillance technology, including PII, shall be classified according to the City's Data Classification Standard. Should information be incidentally collected that is not necessary to accomplish the intended purpose of the surveillance technology, including information that may be used to identify persons or private information, Department shall remove all incidental PII from raw data. The surveillance technology collects some or all of the following data types:

Data Type(s)	*Format(s)*	*Classification*

Images/video of CCSF projects, assets, trees, etc.	JPGE, MOV, AVI	Level 1
Images/video of CCSF projects, assets, trees, etc.	JPGE, MOV, AVI	Level 2

Notification:

Departments shall notify the public of intended surveillance technology operation at the site of operations through signage in readily viewable public areas. Department notifications shall identify the type of technology being used and the purpose for such collection.

Department includes the following items in its public notice:

- X Information on the surveillance technology
- X Description of the authorized use
- X Type of data collected
- X Will persons be individually identified
- X Data retention
- X Department identification
- X Contact information

Access:

All parties requesting access must adhere to the following rules and processes (please refer to the data sharing section to ensure all information covered in that section is also included below): Distinctive personal features or license plate information collected inadvertently (if any) will be blurred using an approved editing software prior to use or storage of images (drone "data") for any business purposes. Once PII have been obscured or removed from images, data may be used by department based on use cases identified above and may be stored on servers for future use. RAW (unedited) data shall not be used or retained.

Data must always be scrubbed of PII as stated above prior to use.

A. Department employees

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.

1. 7333-35 Stationary Engineer
2. 5310-13 Surveyor class series
3. 5201-18 Engineers class series

4. 1823-27 Analyst class series
5. 0922-0954 Manager class series
6. 3435 BUF Inspectors
7. 5120 Architectural Administrator
8. 5260-74 Architect Class Series
9. San Francisco Public Works: Bureau of Street Use & Mapping, Bureau of Urban Forestry, Bureau of Building Repair, Bureau of Engineering, Bureau of Architecture, Streets and Environmental Services, Streets and Sewer Repair

Contractors: The following providers are required to support and maintain the surveillance technology and its associated data to ensure it remains functional:

- At this point, Public Works does not anticipate using specific contractors whose services may be required
- However, if Public Works does use contractors, they will follow Public Works' Surveillance Technology Policy

B. Members of the public

Public Works 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. Anyone, including criminal defendants, may access such data. 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, including by criminal defendants.

Members of the public, including criminal defendants, 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.

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).

To protect surveillance technology information from unauthorized access and control, including misuse, Departments shall, at minimum, apply the following safeguards:

- Only authorized drone operators or PM may access unedited data.

Data Sharing:	Public Works will endeavor to ensure that other agencies or departments that may receive data collected by Department of Public Work's unmanned aerial vehicles policy will act in conformity with this Surveillance Technology Policy. 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. Public Works 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) Public Works shall ensure all PII and restricted data is de-identified or adequately protected to ensure the identities of individual subjects are effectively safeguarded. Each department that believes another agency or department receives or may receive data collected from its use of STs should consult with its assigned deputy city attorney regarding their response. Before sharing data with any recipients, the Department will use the following procedure to ensure appropriate data protections are in place: X Confirm the purpose of the data sharing aligns with the department's mission. X Consider alternative methods other than sharing data that can accomplish the same purpose. X Redact names, scrub faces, and ensure all PII is removed in accordance with the department's data policies. X Review of all existing safeguards to ensure shared data does not increase the risk of potential civil rights and liberties impacts on residents. X 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. X Ensure data will be shared in a cost-efficient manner and exported in a clean, machine-readable format. Public Works 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 The Department currently participates in the following sharing practices: *A. Internal Data Sharing:*

Department shares the following data with the recipients: The department does not share surveillance technology data containing non-obscured ("raw" or unedited) PII with other departments or entities inside the City and County of San Francisco.

Data sharing occurs at the following frequency: N/A

B. External Data Sharing:

Department shares the following data with the recipients:

- In emergency scenarios, Public Works may provide data to departments such as SFMTA, SFPUC, SF Port, SF Airport, SFDBI, and public access based on the Sunshine Ordinance. This data will be scrubbed and all PII will be removed, per Public Works' data processing protocols.

Data sharing occurs at the following frequency: Data sharing will vary by case.

To ensure that entities receiving data collected by the surveillance technology comply with the Surveillance Technology Policy, Department shall:

- Public Works will process raw data collected by drones as expeditiously as possible, removing or obscuring all PII. Only post-processed (i.e., "scrubbed") data will be maintained by Public Works per federal (FEMA) and state (OES) and local reimbursement and investigation requirements. Unedited data shall be deleted upon completion of processing.

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:

- Public Works will process raw data collected by drones as expeditiously as possible, and will commit to remove or obscure all PII within one year of collection. Only post-processed (i.e., "scrubbed") data will be maintained by Public Works per federal (FEMA) and state (OES) and local reimbursement and investigation requirements. Unedited data shall be deleted upon completion of processing.
- Scrubbed data will be maintained in Public Works servers for historical purposes.

PII data shall not be kept in a form which permits identification of data subjects for any longer than is necessary for the purposes for which the personal data are processed. PII data collected by the surveillance technology may be retained beyond the standard retention period only in the following circumstance(s): N/A

Departments must establish appropriate safeguards for PII data stored for longer periods.

Data will 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
- Software as a Service Product

X Cloud Storage Provider

Data Disposal: Upon completion of the data retention period, Department shall dispose of data in the following manner:

Practices:

1. Raw (unprocessed) data will be collected by the drone in the field, and stored on an onboard storage disc (i.e, "SD" card).
2. Raw data (from the drone disc) will be downloaded from onboard storage disc onto secure Public Works servers by Drone Data Editor.
3. Still or video frames will be identified for use by the appropriate Public Works data consumer (based upon pre-approved Public Works use cases.)

Such data may include, as examples, images of buildings and structures, overhead images of topographic features, images of City tree canopy/limbs, and/or video images featuring Public Works project locations for use in Public Works TV episodes or other promotional materials.

Once the subject image frames, still and/or video, have been identified for business needs, the Public Works Data editor will review all selected frames and identify each instance of PII (faces or license plates). All instances of PII will be blurred or obscured using editing software, such that no recognizable human features or license plate information remain.

After processing and saving of edited data, all raw data will be permanently erased. Before replacing the SD storage cards into the drone, data editor will ensure the discs are completely free of all data.

Processes and Applications: All instances of PII will be blurred or obscured using editing software, such that no recognizable human features or distinctly identifying information remain.

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 to unedited data with PII present must receive training on data security policies and procedures.

At the very least, 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. 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.

Data editors will be trained to properly utilize the editing software to ensure that all PII has been removed from still or video drone images before those images are released to other agencies or the public, or stored on servers for long term retention.

COMPLIANCE

Department shall oversee and enforce compliance with this Policy using the following methods:

1. Two individuals will be assigned to maintain updates and perform required maintenance. A procedural pre-mobilization and post-mobilization safety check will be performed at each operation.
2. Department shall assign one or more of the following personnel to oversee Policy compliance by the Department and third-parties.
    a. Senior Administrative Analyst,
    b. BSM Deputy Bureau Manger,
    c. BOE Deputy Bureau Manager,
    d. BOE structural section manager,
    e. BOA Deputy Bureau Manager,
    f. BUF Deputy Bureau Manager,
    g. Architectural Administrator,
    h. Architects and Engineers

Sanctions for violations of this Policy include the following:

1. First offense: violator shall be verbally notified by Public Works management of nature of violation.
2. Second offense: violator shall be notified in writing of second offence and privileges to operate drone hardware shall be suspended for 60 days.
3. Third offense: (following reinstatement of operator privileges): violator shall be permanently banned from drone operations and disciplinary action may be taken depending upon the severity of second/third offences.

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.

EXCEPTIONS

Only in exigent circumstances or in circumstances where law enforcement requires surveillance technology data for investigatory or prosecutorial functions may data collected, retained, or processed by the surveillance technology be shared with law enforcement.

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.
Sensitive Data:	Data intended for release on a need-to-know basis. Data regulated by privacy laws or regulations or restricted by a regulatory agency or contract, grant, or other agreement terms and conditions.
Exigent Circumstances	An emergency involving imminent danger of death or serious physical injury to any person that requires the immediate use of Surveillance Technology or the information it provides.

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

Public:

Complaints or concerns can be submitted to the Department by members of the public can register complaints / concerns or submit questions at San Francisco Public Works Bureau of Street-Use and Mapping (BSM) 1155 Market Street, 3rd Floor San Francisco, CA 94103, 415-554-5810 or via calls/emails to 311.org. As of July 15, Public Works will be located at 49 South Van Ness, Suite 300, San Francisco, CA 94102.

Department shall acknowledge and respond to complaints and concerns in a timely and organized response. To do so, Department shall:

Constituent calls and complaints to the Bureau of Street-Use and Mapping (BSM) are received by counter personnel and routed to the bureau's Drone Program manager. Program manager will discuss concerns or complaints with constituent, enter details regarding nature of conversation on excel spreadsheet stored in Public Works shared drive, referred to as the drone Constituent Feedback Log ("CFL"). If additional action is required or requested by caller, Public Works commits to a follow-up (by email or telephone) within 48 hours. Department shall be prepared to host a viewing of edited imagery if caller is insistent, to demonstrate that no PII was collected. Depending upon the urgency or sensitivity of call, Drone Program manager shall notify bureau of details and discuss resolution before follow-up with caller. The final outcome and action(s) taken shall be logged onto CFL.

Public Works drone operators and Public Works management shall review log on a quarterly basis to discuss best practices, evaluate for learning lessons and opportunities to improve and refine the drone use program based on caller complaints, concerns and other community feedback.

City and County of San Francisco Employees:

All questions regarding this policy should be directed to the employee's supervisor or to the director. Similarly, questions about other applicable laws governing the use of the surveillance technology or the issues related to privacy should be directed to the employee's supervisor or the director.

Surveillance Impact Report

Department of Technology
Unmanned Aircraft Systems (Drones)

As required by San Francisco Administrative Code, Section 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 Unmanned Aerial Vehicle (UAV) or Drone Technology.

DESCRIPTION OF THE TECHNOLOGY

The Department's mission is: To provide innovative, reliable, and secure business solutions that support and empower City agencies and departments in their delivery of high-quality government services for the public.

In line with its mission, the Department uses Unmanned Aerial Vehicles or Drone Technology to:

1. The Department of Technology's video channel SFGovTV provides the public critical information about government and civic life program through cable channels and web streaming. Drone technology will allow SFGovTV to produce improved video programming. Specifically, drone technology will allow the station to capture of video and still photographs as elements of the City video productions program.

Technology shall use Unmanned Aerial Vehicle or Drone Technology only for the following authorized purposes:

1. The drone technology is authorized for use during Video production, specifically the capture of video stills and photographs as elements of SFGovTV's video productions. The completed videos will be broadcast on SFGovTV's cable channels and made available on the station's YouTube account. Marketing and promotional videos created for other City departments may also feature drone footage or photographs.

Prohibited use cases involve any uses not stated in the Authorized Use Case section.

Use of drone technology to intentionally capture images of a personal nature will always be prohibited.

Department Technology's Unmanned Aerial Vehicles or Drones will be used wherever outdoor footage may provide public with added understanding of City operations, such as parks, plazas and other facilities.

Surveillance Oversight Review Dates
COIT Review: July 17, 2020
Board of Supervisors Review: TBD

Technology Details

The following is a product description of Drones or Unmanned Aerial Vehicles:

- Mavic 2 Pro with Hasselblad Camera: Made in Sweden, Hasselblad cameras are renowned for their iconic ergonomic design, uncompromising image quality, and Swedish craftsmanship. Since 1941, Hasselblad cameras have captured some of the world's most iconic images – including the first moon landing. Co-engineered in partnership with Hasselblad after two years of tireless research, the Mavic 2 Pro comes equipped with the all-new Hasselblad L1D-20c camera. The L1D-20c possesses Hasselblad's unique Hasselblad Natural Colour Solution (HNCS) technology, 5 helping users to capture gorgeous 20-megapixel aerial shots in stunning color detail.

A. How It Works

To function, Unmanned Aerial Vehicle or Drone Technology Drone technology incorporates unmanned, remotely operated aircraft with onboard visual recording equipment, for the purpose of capturing images from an aerial perspective.

Data collected or processed by Unmanned Aerial Vehicle or Drone Technology will not be handled or stored by an outside provider or third-party vendor on an ongoing basis. The Department will remain the sole Custodian of Record.

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:

- The benefits of the surveillance technology outweigh the costs.
- The Department's Policy safeguards civil liberties and civil rights.
- 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 Drone technology has the following benefits for the residents of the City and County of San Francisco:

- Education
- Community Development
- Health
- Environment

- Criminal Justice
- Jobs
- Housing

X	Other	Civic Engagement SFGovTV's use of drone technology will allow residents to have an improved view of City operations and civic life.

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:

DT strives to mitigate all potential civil rights impacts through responsible technology and associated data use policies and procedures and intends to use drones and their associated data exclusively for the aforementioned authorized uses cases. All other uses, including surveillance of San Francisco residents or groups, are expressly prohibited.

Department policy stipulates that drone operators/pilots are not authorized to intentionally capture data than can identify individuals. Auto license plate information shall also not be deliberately captured.

To mitigate the risk of potential embarrassment, emotional distress, self-censorship or diminished civic engagement by SF residents whose personal information may be unintentionally captured, DT will require the "scrubbing" or otherwise obscuring/blurring (through use of image editing software) any collected data of facial images, license plates or other personally identifiable information unintentionally captured by aerial drones.

All collected data, irrespective of the location of data capture or the identifying characteristics of captured persons, is subject to the same scrubbing processes and procedures. The image software scrubbing process obscures and blurs all data using either built-in AI recognition settings or through manual efforts by software operator.

To protect drone data from potential breach, misuse or abuse that may result in civil rights impacts, data is maintained on secure, department-owned servers. Only persons authorized to utilize the raw data may access the information and are required to maintain records of access by completing the drone data access log described in section 3.23. Only data that has been edited to remove PII will be used in SFGovTV programming.

To further protect data and any personal resident information captured by a drone, all raw data will be permanently erased after it has been processed and edited to blur or obscure human features and license plate information. To mitigate any potential impacts to residents' physical safety or economic loss through property damage, all DT drone operators receive pilot training and are required to sign the Department's Drone Use Policy.

C. Fiscal Analysis of Costs and Benefits

The Department's use of Drones or Unmanned Aerial Vehicles yields the following business and operations benefits:

Benefit		Description
X	Financial Savings	Drones will be far more cost effective than alternative methods of original aerial photography. By mitigating the need for traffic control, expensive scaffolding/swing stage or other equipment, and other means that can be done manually, Drones minimize labor costs.
X	Time Savings	Drones do not require as much time for set-up as other aerial alternatives.
X	Staff Safety	Drones expose staff to much less risk than alternatives such as constructing and climbing scaffolding or manned aircraft.

- Data Quality

Number of FTE (new & existing)	0.2 FTE		
Classification	Media Production Specialist (1767)		
	Annual Cost	***Years***	***One-Time Cost***
Total Salary & Fringe			$33,850
Software			
Hardware/Equipment			$2,500
Professional Services			
Training			*$1,800*
Other			
Total Cost			*$36,350*

The Department funds its use and maintenance of the surveillance technology through

- Staff time devoted to video programming produced using drones will be charged to departments/agencies for which programming is being produced.

COMPARISON TO OTHER JURISDICTIONS

Drones or Unmanned Aerial Vehicles are currently utilized by other governmental entities for similar purposes.

Surveillance Technology Policy

Department of Technology
Unmanned Aircraft Systems (Drones)

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 Vehicle (UAV) or Drone Technology (referred to hereafter as "Drones") 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

The Department of Technology's (DT's) mission is to: provide innovative, reliable, and secure business solutions that support and empower City agencies and departments in their delivery of high-quality government services for the public.

The Surveillance Technology Policy ("Policy") defines the manner in which the Drone technology will be used to support this mission, by describing the intended purpose, authorized and restricted uses, and requirements.

This Policy applies to all to department personnel that use, plan to use, or plan to secure Drone technology, 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

Unmanned Aerial Vehicles and Drone technology for the Department is limited to the following use cases and is subject to the requirements listed in this Policy.

Authorized Use(s):

1. Drone technology is authorized for use during Video production, specifically the capture of video stills and photographs as elements of SFGovTV's video productions. The completed videos will be broadcast on SFGovTV's cable channels and made available on the station's YouTube account. Marketing and promotional videos created for other City departments may also feature drone footage or photographs.

Prohibited use cases include any uses not stated in the Authorized Use Case section.

Departments may use information collected from technology only for legally authorized purposes, and may not use that information to unlawfully discriminate against people based on race, ethnicity, political opinions, religious or philosophical beliefs, trade union membership, gender, gender identity, disability status, sexual orientation or activity, or genetic and/or biometric data. Additionally, departments may not use automated systems to scan footage and identify individuals based on any of the categories listed in the preceding sentence.

Surveillance Oversight Review Dates
COIT Review: July 17, 2020
Board of Supervisors Review: TBD

BUSINESS JUSTIFICATION

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

The DT's video channel SFGovTV provides the public critical information about government and civic life program through cable channels and web streaming. Drone technology will allow SFGovTV to produce improved video programming. Specifically, drone technology will allow the station to capture video and still photographs as elements of the City video productions program.

In addition, unmanned aerial vehicles and Drone technology promises to benefit residents in the following ways:

- Education
- Community Development
- Health
- Environment
- Criminal Justice
- Jobs
- Housing

X	Other	Civic Engagement SFGovTV's use of drone technology will allow residents to have an improved view of City operations and civic life.

In addition, the following benefits are obtained:

Benefit		Description
X	Financial Savings	Drones will be far more cost effective than alternative methods of original aerial photography. By mitigating the need for traffic control, expensive scaffolding/swing stage or other equipment, and other means that can be done manually, Drones will minimize labor costs.
X	Time Savings	Drones do not require as much time for set-up as other aerial alternatives.
X	Staff Safety	Drones expose staff to much less risk than alternatives such as constructing and climbing scaffolding or manned aircraft.

- Data Quality

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 kept up to date and maintained.
Safety:	Surveillance technology must be operated in a safe manner. Surveillance technology should not be operated in a way that infringes on resident civil rights, including privacy, or causes personal injury or property damage. To ensure physical safety of the public, DT will operate drones in a manner consistent with the San Francisco Film Commission's guidelines for filming with a drone in all drone flight that is on, from, within and over City property. https://filmsf.org/filming-droneuas
Data Collection:	Department shall minimize the use, collection, and retention of Personally Identifiable Information (PII) to what is strictly necessary to accomplish the intended purpose of the surveillance technology. Department shall only collect data required to execute the authorized use case. All data collected by the surveillance technology, including PII, shall be classified according to the City's Data Classification Standard. Should information be incidentally collected that is not necessary to accomplish the intended purpose of the surveillance technology, including information that may be used to identify persons or private information, Department shall remove all incidental PII from raw data. The surveillance technology collects some or all of the following data types:

Data Type(s)	*Format(s)*	*Classification*
Photographic and video data (no audio) of assets, landscapes, etc.	JPEG, PNG, MOV, AVI, CSV	Level 1

Notification:	Department shall notify the public of intended surveillance technology operation at the site of operations through signage in readily viewable public areas. Department notifications shall identify the type of technology being used and the purpose for such collection.

Department includes the following items in its public notice:

X Information on the surveillance technology

X Description of the authorized use

X Type of data collected

X Will persons be individually identified

X Data retention

X Department identification

X Contact information

Access:

All parties requesting access must adhere to the following rules and processes (please refer to the data sharing section to ensure all information covered in that section is also included below):

1. Distinctive personal features or license plate information collected inadvertently (if any) will be blurred using an approved editing software prior to use or storage of images (drone "data") for any business purposes.
2. Once PII have been obscured or removed from images, data may be used by department based on use cases identified above, and may be stored on servers for future use. RAW (unedited) data shall not be used or retained.

Data must always be scrubbed of PII as stated above prior to use.

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.

1767 Media Production Specialist , Technology

B. Members of the public

Technology 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.

Data collected by surveillance technology will be made available to members of the public, including criminal defendants. Data can be accessed by the public in the following ways:

1. Scrubbed data will be available through channels and web streaming.

Anyone, including criminal defendants, may access such data.

	Members of the public, including criminal defendants, 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.
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). To protect surveillance technology information from unauthorized access and control, including misuse, Departments shall, at minimum, apply the following safeguards: Only authorized drone operator(s) and General Manager may access unedited data.
Data Sharing:	Technology will endeavor to ensure that other agencies or departments that may receive data collected by DT's Drones will act in conformity with this Surveillance Technology Policy. 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. Technology 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). Technology shall ensure all PII and restricted data is de-identified or adequately protected to ensure the identities of individual subjects are effectively safeguarded. 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 response. Before sharing data with departments requesting data not-contained in programming via cablecast or video streaming, DT will use the following procedure to ensure appropriate data protections are in place: X Confirm the purpose of the data sharing aligns with the department's mission. X Consider alternative methods other than sharing data that can accomplish the same purpose. X Redact names, scrub faces, and ensure all PII is removed in accordance with the department's data policies.

X	Review of all existing safeguards to ensure shared data does not increase the risk of potential civil rights and liberties impacts on residents.
X	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.
X	Ensure data will be shared in a cost-efficient manner and exported in a clean, machine-readable format.

For Departments accessing data contained in programming via cablecast or video streaming, DT 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.
X	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.
X	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.

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.

The Department currently participates in the following sharing practices:

A. Internal Data Sharing:

Department shares the following data with the recipients:

- We anticipate that programming will be shared with various departments
- Data scrubbed of any inadvertently collected PII will be disclosed

Data sharing occurs at the following frequency: Continuously

B. External Data Sharing:

Department shares the following data with the recipients:

- Scrubbed data will be integrated in video programming. DT anticipates that video programming which includes video captured by drone will be publicly available through cable channels and web video streaming.

Data sharing occurs at the following frequency: Continuously.

To ensure that entities receiving data collected by the surveillance technology comply with the Surveillance Technology Policy, Department shall:

1. Raw data collected by drones will be scrubbed of any inadvertently collected PII as soon as possible and deleted as soon as possible.
2. Seek to delete metadata stored on the drone within 24 hours of capture and in all circumstances delete within 72 hours.

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:

- Raw data collected by drones will be scrubbed of any inadvertently collected PII as soon as possible and deleted as soon as possible.
- Programming using scrubbed data are considered permanent records and will be archived indefinitely.

Programming is intended as an enduring record of city operations.

Departments must establish appropriate safeguards for PII data stored for longer periods.

Departments must establish appropriate safeguards for PII data stored for longer periods.

Data will 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
- Software as a Service Product

X Cloud Storage Provider

Data Disposal:

Upon completion of the data retention period, Department shall dispose of data in the following manner:

1. Raw (unprocessed) data will be collected by the drone in the field, and stored on an onboard storage disc (i.e, "SD" card). Raw data (from the drone disc) will be downloaded from onboard storage disc onto secure DT device. Still or video frames will be identified for use by the SFGovTV producer. Such data may include, as examples, images of buildings and structures, overhead images of topographic features.
2. Once the subject image frames, still and/or video, have been identified for business needs, the producer editor will review all selected frames and identify each instance of PII (faces or license plates). All instances of PII will be blurred or obscured using editing software, such that no recognizable human features or license plate information remain.
3. Before replacing the SD storage cards into the drone, data editor will ensure the discs are completely free of all data.

Processes and Applications: All instances of PII will be blurred or obscured using editing software, such that no recognizable human features or license plate information remain.

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 must receive training on data security policies and procedures.

At the very least, 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. With the exception of data shared through cable cast, web steaming or other distribution of programming, 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.

Drone data collection and use shall be explained in Departmental Drone Policy. All authorized users must sign off on policy prior to use.

COMPLIANCE

Department shall oversee and enforce compliance with this Policy using the following methods:

1. One individual with that has reviewed and signed the drone policy and received drone flight certification will be responsible for compliance with policies, procedures and record keeping.
2. Department shall assign the following personnel to oversee Policy compliance by the Department and third-parties:
    a. General Manager, SFGTV

Sanctions for violations of this Policy include the following:

- First offense: violator shall be verbally notified by DT management of nature of violation.
- Second offense: violator shall notified in writing of second offence and privileges to operate drone hardware shall be suspended for 60 days.
- Third offense: (following reinstatement of operator privileges): violator shall be permanently banned from drone operations and disciplinary action may be taken depending upon the severity of second/third offences.

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.

EXCEPTIONS

Only in exigent circumstances or in circumstances where law enforcement requires surveillance technology data for investigatory or prosecutorial functions may data collected, retained or processed by the surveillance technology be shared with law enforcement.

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.
Sensitive Data:	Data intended for release on a need-to-know basis. Data regulated by privacy laws or regulations or restricted by a regulatory agency or contract, grant, or other agreement terms and conditions.
Exigent Circumstances	An emergency involving imminent danger of death or serious physical injury to any person that requires the immediate use of Surveillance Technology or the information it provides.

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

Public:

Complaints or concerns can be submitted to the Department:

Members of the public can register complains, concerns or ask questions by calling (415) 554-4188, emailing sfgovtv@sfgov.org or going to 311.org

Department shall acknowledge and respond to complaints and concerns in a timely and organized response. To do so, Department shall:

- SFGovTV will monitor drone program related complaints and respond within two business days.

City and County of San Francisco Employees:

All questions regarding this policy should be directed to the employee's supervisor or to the director. Similarly, questions about other applicable laws governing the use of the surveillance technology or the issues related to privacy should be directed to the employee's supervisor or the director.

Surveillance Impact Report

Fire Department
Unmanned Aircraft Systems (Drones)

As required by San Francisco Administrative Code, Section 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 Drones or Unmanned Aerial Vehicles.

DESCRIPTION OF THE TECHNOLOGY

The Department's mission is: to protect the lives and property of the people of San Francisco from fires, natural disasters, and hazardous materials incidents; to save lives by providing emergency medical services; to prevent fires through prevention and education programs; and to provide a work environment that values health, wellness and cultural diversity and is free of harassment and discrimination.

In line with its mission, the Department uses Drones or Unmanned Aerial Vehicles to facilitate saving lives and property, enhance Firefighter safety and improve emergency response actions by providing aerial reconnaissance and observation to the Incident Commander to support strategic and tactical decisions at emergencies, major incidents and/or disasters. The SFFD will use uniformed personnel or an authorized contractor to operate the Drone

Fire Department shall use Drones or Unmanned Aerial Vehicles only for the following authorized purposes:

1. Disaster Response: Assessment and District Surveys
2. Emergency Response: Building Fire Reconnaissance
3. Search & Rescue: Aerial or water borne drones.
4. Training: Assessment and evaluation of emergency response

The following use cases are expressly prohibited:

- Use of drone technology to intentionally capture images of a personal nature will always be prohibited.

Fire Department Drone technology is located in the following areas: Disaster areas, emergency evacuation routes, and other areas within San Francisco requiring Fire Department safety response operations.

Surveillance Oversight Review Dates
COIT Review: July 17, 2020
Board of Supervisors Review: TBD

Technology Details

The following is a product description of Drones or Unmanned Aerial Vehicles:

DJI Matrice 210 is an aerial survey drone that is equipped with both an aerial zoom and thermal camera. First responders can now quickly locate missing people in remote areas and plan the safest approach path.

A. How It Works

To function, Drones or Unmanned Aerial Vehicles incorporate unmanned, remotely-operated aircraft with onboard visual recording equipment, for the purpose of capturing images from an aerial perspective.

Data collected or processed by Drones or Unmanned Aerial Vehicles will not be handled or stored by an outside provider or third-party vendor on an ongoing basis. The Department will remain the sole Custodian of Record.

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:

- The benefits of the surveillance technology outweigh the costs.
- The Department's Policy safeguards civil liberties and civil rights.
- 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 Drone technology has the following benefits for the residents of the City and County of San Francisco:

X	Education	Drone imagery to promote Fire Department safety messaging and disaster preparedness
▪	Community Development	
▪	Health	
X	Environment	Drone imagery to identify any hazardous material response and mitigation
▪	Criminal Justice	
▪	Jobs	
▪	Housing	

X	Other	Public Safety: emergency response as indicated in authorized use cases

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:

The San Francisco Fire Department strives to mitigate all potential civil rights impacts through responsible technology and associated data use policies and procedures. The Fire Department intends to use drones and their associated data exclusively for aforementioned authorized uses cases. All other uses, including surveillance of San Francisco residents or groups, are expressly prohibited.

To protect drone data from potential breach, misuse or abuse that may result in civil rights impacts, data is maintained on secure, department-owned servers. Only persons authorized to utilize the raw data may access the information and are required to maintain records of access by completing the drone data access log described in section 3.23.

Only data that has been edited to remove PII will be shared and stored on servers, and sharing will only occur with partner CCSF agencies on a case by case basis or as required by law. To mitigate any potential impacts to residents' physical safety or economic loss through property damage, all SFFD drone operators receive pilot training and are required to sign the Department's Drone Use Policy.

Recorded data will not be collected, disseminated or retained solely for the purpose of monitoring activities protected by the U.S. Constitution, such as the First Amendment's protections of religion, speech, press, assembly, and redress of grievances (e.g., protests, demonstrations). Collection, use, dissemination, or retention of recorded data should not be based solely on individual characteristics (e.g., race, ethnicity, national origin, sexual orientation, gender identity, religion, age, or gender), which is a violation of the law.

C. Fiscal Analysis of Costs and Benefits

The Department's use of Drones or Unmanned Aerial Vehicles yields the following business and operations benefits:

Benefit		Description
X	Financial Savings	Drones can be far more time efficient and cost effective when conducting emergency response and gaining rapid situational awareness in a disaster.
X	Time Savings	Deploying a drone can provide time savings locating victims in a variety of environments as well as gain situational awareness and hazard assessment.

X	Staff Safety	Drones can be deployed to dangerous locations instead of personnel, such as rooftops, at the sides of building/bridges, along cliff areas or areas prone to erosion.
X	Data Quality	Dome locations which are difficult to access by personnel may be more easily photographed using drone technology, thereby achieving better data.

Number of FTE (new & existing)	0		
Classification	n/a		
	Annual Cost	***Years***	***One-Time Cost***
Total Salary & Fringe	*$5,000*	1	0
Software	*$1,000*	1	*$1,000*
Hardware/Equipment		1	$25,000
Professional Services		1	
Training	*$1,000*		
Other			
Total Cost			*$26,000*

The Department funds its use and maintenance of the surveillance technology through

- This project was initially funded by a Homeland Security grant, but further costs would be relegated to the Department's general fund budget.

COMPARISON TO OTHER JURISDICTIONS

Drones or Unmanned Aerial Vehicles are currently utilized by other governmental entities for similar purposes.

Surveillance Technology Policy

Fire Department
Unmanned Aircraft Systems (Drones)

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 Drones or Unmanned Aerial Vehicles 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

The Department's mission is to: to protect the lives and property of the people of San Francisco from fires, natural disasters, and hazardous materials incidents; to save lives by providing emergency medical services; to prevent fires through prevention and education programs; and to provide a work environment that values health, wellness and cultural diversity and is free of harassment and discrimination.

The Surveillance Technology Policy ("Policy") defines the manner in which the Drones or Unmanned Aerial Vehicles will be used to support this mission, by describing the intended purpose, authorized and restricted uses, and requirements.

This Policy applies to all to department personnel that use, plan to use, or plan to secure Drones or Unmanned Aerial Vehicles, 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 Drones or Unmanned Aerial Vehicles technology for the Department is limited to the following use cases and is subject to the requirements listed in this Policy.

Authorized Use(s):

1. Disaster Response: Assessment and District Surveys
2. Emergency Response: Building Fire Reconnaissance
3. Search & Rescue: Aerial or water borne drones.
4. Training: Assessment and evaluation of emergency response

Prohibited use cases include any uses not stated in the Authorized Use Case section.

Departments may use information collected from technology only for legally authorized purposes, and may not use that information to unlawfully discriminate against people based on race, ethnicity, political opinions, religious or philosophical beliefs, trade union membership, gender, gender identity, disability status, sexual orientation or activity, or genetic and/or biometric data. Additionally, departments may not use automated systems to scan footage and identify individuals based on any of the categories listed in the preceding sentence.

Surveillance Oversight Review Dates
COIT Review: July 17, 2020
Board of Supervisors Review: TBD

BUSINESS JUSTIFICATION

Drones or Unmanned Aerial Vehicles support the Department's mission and provides important operational value in the following ways:

The mission of the SFFD Drone Program is to facilitate saving lives and property, enhance Firefighter safety and improve emergency response actions by providing aerial reconnaissance and observation to the Incident Commander to support strategic and tactical decisions at emergencies, major incidents and/or disasters. The SFFD will use uniformed personnel or an authorized contractor to operate the Drone.

In addition, Drones or Unmanned Aerial Vehicles promise to benefit residents in the following ways:

X	Education	Drone imagery to promote Fire Department safety messaging and disaster preparedness
▪	Community Development	
▪	Health	
X	Environment	Drone imagery to identify any hazardous material response and mitigation
▪	Criminal Justice	
▪	Jobs	
▪	Housing	
X	Other	Public Safety: emergency response as indicated in authorized use cases

In addition, the following benefits are obtained:

Benefit		Description
X	Financial Savings	Drones can be far more time efficient and cost effective when conducting emergency response and gaining rapid situational awareness in a disaster.
X	Time Savings	Deploying a drone can provide time savings locating victims in a variety of environments as well as gain situational awareness and hazard assessment.
X	Staff Safety	Drones can be deployed to dangerous locations instead of personnel, such as rooftops, at the sides of building/bridges, along cliff areas or areas prone to erosion.
X	Data Quality	Some locations which are difficult to access by personnel may be more easily photographed using drone technology, thereby achieving better data.

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 kept up to date and maintained.
Safety:	Surveillance technology must be operated in a safe manner. Surveillance technology should not be operated in a way that infringes on resident civil rights, including privacy, or causes personal injury or property damage
Data Collection:	Departments shall minimize the use, collection, and retention of Personally Identifiable Information (PII) to what is strictly necessary to accomplish the intended purpose of the surveillance technology. Department shall only collect data required to execute the authorized use case. All data collected by the surveillance technology, including PII, shall be classified according to the City's Data Classification Standard. Should information be incidentally collected that is not necessary to accomplish the intended purpose of the surveillance technology, including information that may be used to identify persons or private information, Department shall remove all incidental PII from raw data. The surveillance technology collects some or all of the following data types:

Data Type(s)	*Format(s)*	*Classification*
Photographic and video data (no audio) of assets, landscapes, etc.	JPEG, PNG, MOV, AVI, CSV	Level 2

Notification:	Departments shall notify the public of intended surveillance technology operation at the site of operations through signage in readily viewable public areas. Department notifications shall identify the type of technology being used and the purpose for such collection. Because of the urgent nature of fighting fires, Fire Department will likely not be able to implement public noticing. In these scenarios, Fire Department may implement public noticing after the fact or may seek other options of letting the public know about Drone use.

Department includes the following items in its public notice:

X Information on the surveillance technology

X Description of the authorized use

X Type of data collected

X Will persons be individually identified

X Data retention

X Department identification

X Contact information

Access:

All parties requesting access must adhere to the following rules and processes (please refer to the data sharing section to ensure all information covered in that section is also included below):

- Distinctive personal features or license plate information collected inadvertently (if any) will be blurred using an approved editing software prior to use or storage of images (drone "data") for any business purposes.

- Once PII have been obscured or removed from images, data may be used by department based on use cases identified above and may be stored on servers for future use. RAW (unedited) data shall not be used or retained.

Data must always be scrubbed of PII as stated above prior to public use.

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:

- Drone Program Manager, Fire Department Operations
- It is possible drone contractors may be retained as part of a professional services contract.

B. Members of the public

Fire 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. Anyone, including criminal defendants, may access such data. 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, including by criminal defendants.

	Members of the public, including criminal defendants, 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.
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). To protect surveillance technology information from unauthorized access and control, including misuse, Departments shall, at minimum, apply the following safeguards: - Only authorized drone operators or MIS may access unedited data.
Data Sharing:	Fire Department will endeavor to ensure that other agencies or departments that may receive data collected by SFFD's Drone Policy will act in conformity with this Policy. 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. Fire 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) Fire Department shall ensure all PII and restricted data is de-identified or adequately protected to ensure the identities of individual subjects are effectively safeguarded. Further, in sharing data, processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data 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 response. Before sharing data with any recipients, the Department will use the following procedure to ensure appropriate data protections are in place:

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

Fire 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.

The Department currently participates in the following sharing practices:

A. Internal Data Sharing:

The department does not share surveillance technology data with other departments or entities inside the City and County of San Francisco.

B. External Data Sharing:

The department does not share surveillance technology data externally with entities outside the City and County of San Francisco.

The Fire Department will process raw data collected by drones as expeditiously as possible, removing or obscuring all PII. Only post-processed (i.e., "scrubbed") data will be maintained by the Fire Department per federal (FEMA) and state (OES) and local reimbursement and investigation requirements. Unedited data shall be deleted upon completion of processing.

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:

- The Fire Department will process raw data collected by drones as expeditiously as possible, removing or obscuring all PII. Only post-

processed (i.e., "scrubbed") data will be maintained by the Fire Department per federal (FEMA) and state (OES) and local reimbursement and investigation requirements. Unedited data shall be deleted upon completion of processing.

- Scrubbed data will adhere to the SFFD Records Management Policy. The Fire Department will consider images collected with surveillance technology as current records and, unless required for an ongoing investigation, they will be retained for period of 1 year.

PII data shall not be kept in a form which permits identification of data subjects for any longer than is necessary for the purposes for which the personal data are processed. PII data collected by the surveillance technology may be retained beyond the standard retention period only in the following circumstance(s):

- N/A

Departments must establish appropriate safeguards for PII data stored for longer periods.

Data will 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

▪ Cloud Storage Provider

Data Disposal: Upon completion of the data retention period, Department shall dispose of data in the following manner:

Practices:

- Raw (unprocessed) data will be collected by the drone in the field, and stored on an onboard storage disc (i.e, "SD" card). Raw data (from the drone disc) will be downloaded from onboard storage disc onto secure Fire Department servers by Drone Data Editor.
- Once the subject image frames, still and/or video, have been identified for business needs, the Fire Department Data editor will review all selected frames and identify each instance of PII (faces or license plates). All instances of PII will be blurred or obscured using editing software, such that no recognizable human features or license plate information remain.
- After processing and saving of edited data, all raw data will be permanently erased. Before replacing the SD storage cards into the drone, data editor will ensure the discs are completely free of all data.

	Processes and Applications: All instances of PII will be blurred or obscured using editing software, such that no recognizable human features or license plate information remain.
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 must receive training on data security policies and procedures. At the very least, 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. 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. Drone data collection and use shall be explained in Departmental Drone Policy. All authorized users must sign off on policy prior to use.

COMPLIANCE

Department shall oversee and enforce compliance with this Policy using the following methods:

- Drone Operators will be assigned to maintain updates and perform required maintenance. A procedural pre-mobilization and post-mobilization safety check will be performed at each operation.
- Department shall assign the following personnel to oversee Policy compliance by the Department and third-parties.
    - Supervisor- Management of Information Services

Sanctions for violations of this Policy include the following:

- First offense: violator shall be verbally notified by Fire Department management of nature of violation.
- Second offense: violator shall be notified in writing of second offence and privileges to operate drone hardware shall be suspended for 60 days.
- Third offense: (following reinstatement of operator privileges): violator shall be permanently banned from drone operations and disciplinary action may be taken depending upon the severity of second/third offences.

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.

EXCEPTIONS

Only in exigent circumstances or in circumstances where law enforcement requires surveillance technology data for investigatory or prosecutorial functions may data collected, retained or processed by the surveillance technology be shared with law enforcement.

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.
Sensitive Data:	Data intended for release on a need-to-know basis. Data regulated by privacy laws or regulations or restricted by a regulatory agency or contract, grant, or other agreement terms and conditions.
Exigent Circumstances	An emergency involving imminent danger of death or serious physical injury to any person that requires the immediate use of Surveillance Technology or the information it provides.

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

Public:

Department Members of the public can register complaints/concerns or submit questions via calls or emails at 311.org, or to the Department directly at FireAdministration@sfgov.org or 415-558-3200.

Department shall acknowledge and respond to complaints and concerns in a timely and organized response. To do so, Department shall:

Constituent calls and complaints to the Fire Department are routed to the Drone Program manager. Program manager will discuss concerns or complaints with constituent and record details regarding nature of conversation. If additional action is required or requested by caller, the Fire Department commits to a follow-up (by email or telephone) in a timely manner.

Drone Program Manager, drone operators, and Fire Department management shall review log on a quarterly basis to discuss best practices, evaluate for learning lessons and opportunities to improve and refine the drone use program based on caller complaints, concerns and other community feedback.

City and County of San Francisco Employees:

All questions regarding this policy should be directed to the employee's supervisor or to the director. Similarly, questions about other applicable laws governing the use of the surveillance technology or the issues related to privacy should be directed to the employee's supervisor or the director.

Surveillance Impact Report

Port
Unmanned Aircraft Systems (Drones)

As required by San Francisco Administrative Code, Section 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 Unmanned Aerial Vehicles or Drones.

DESCRIPTION OF THE TECHNOLOGY

The Department's mission is: to manage the waterfront as the gateway to a world-class city and advances environmentally and financially sustainable maritime, recreational, and economic opportunities to serve the City, Bay Area region, and California.

In line with its mission, the Department uses Unmanned Aerial Vehicles or Drones to accomplish the following:

1. Drones will provide the Port Department Operations Center (DOC) with high resolution images during response and recovery operations after a disaster.
2. Drones will provide high resolution images during engineering and environmental surveys and assessments of Port properties
3. Drones will support the development of marketing materials for the promotion of activities and opportunities at the Port.

Port shall use Unmanned Aerial Vehicles or Drones only for the following authorized purposes:

1. Disaster response and recovery: Provide DOC with high resolution images during response and recovery operations after a disaster.
2. Facility Inspections: Provide high resolution images during engineering and environmental surveys and assessments of Port properties.
3. Marketing: Capture Drone footage to be used in marketing materials for the promotion of activities and opportunities at the Port.

Prohibited use cases involve any uses not stated in the Authorized Use Case section.

Port Drones are located in the following areas:

- Drones may be deployed at any Port property or facility along the seven and one-half miles of Port property between Aquatic Park in the North and Heron's Head Park in the South.

Surveillance Oversight Review Dates
COIT Review: July 17, 2020
Board of Supervisors Review: TBD

Technology Details

The following is a product description of Unmanned Aerial Vehicles or Drones:

Phantom 4 RTK is an aerial survey drone that combines centimeter-level navigation and positioning with a high-performance imaging system for use during surveying, mapping or inspection operations.

A. How It Works

To function, Unmanned Aerial Vehicles or Drones incorporate unmanned, remotely operated aircraft with onboard visual recording equipment, for the purpose of capturing images from an aerial perspective.

All data collected or processed by Unmanned Aerial Vehicles or Drones will be handled or stored by an outside provider or third-party vendor on an ongoing basis. Specifically, data will be handled by Baseline Environmental or another City Compliant Vendor to ensure the Department may continue to use the technology.

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:

- The benefits of the surveillance technology outweigh the costs.
- The Department's Policy safeguards civil liberties and civil rights.
- 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 Drone technology has the following benefits for the residents of the City and County of San Francisco:

X	Education	Drone imagery will be used to provide materials to residents by promoting Port efforts to advance improvements in the environment, social equity, and quality of life for San Francisco residents and visitors.
▪	Community Development	
▪	Health	
X	Environment	Drone imagery will be used to conduct environmental surveys of Port property and open space. Drone imagery may be used during an Oil Spill response to monitor environmentally sensitive sites and to conduct shoreline assessments
▪	Criminal Justice	

- Jobs
- Housing

X	Other	Drone imagery will be used in the Port's DOC to provide situational awareness and common operating pictures during an emergency response.

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:

The Port strives to mitigate all potential civil rights impacts through responsible technology and associated data use policies and procedures and intends to use drones and their associated data exclusively for authorized uses cases. All other uses, including surveillance of San Francisco residents or groups, are expressly prohibited.

Port Contractors will be prohibited from intentionally capturing data that can be used to identify individuals. Auto license plate information shall also not be deliberately captured. To mitigate the risk of potential embarrassment, emotional distress, self-censorship or diminished civic engagement by SF residents whose personal information may be unintentionally captured, the Port requires the "scrubbing" or otherwise obscuring/blurring (through use of image editing software) of all collected data to remove facial images or other personally identifiable information unintentionally captured by aerial drones.

All collected data, irrespective of the location of data capture or the identifying characteristics of captured persons, is subject to the same scrubbing processes and procedures. The image software scrubbing process obscures and blurs all data using either built-in AI recognition settings or through manual efforts by software operator.

To protect drone data from potential breach, misuse or abuse that may result in civil rights impacts, data is maintained on secure, department-owned servers. Only persons authorized to utilize the raw data may access the information and are required to maintain records of access using a drone data access log. Only data that has been edited to remove PII will be shared and stored on servers. To mitigate any potential impacts to residents' physical safety or economic loss through property damage, all Port Contractors operating drones must have valid Unmanned Aerial Vehicle pilot certifications.

C. Fiscal Analysis of Costs and Benefits

The Department's use of Drones or Unmanned Aerial Vehicles yields the following business and operations benefits:

Benefit		Description
X	Financial Savings	Drones can be far more time efficient and cost effective when conducting asset inspections, by mitigating the need for traffic control, expensive scaffolding/swing stage or other equipment, and can provide more detailed photographs/videos of the assets or areas in need of maintenance or repairs than can be done manually, minimizing labor costs.
X	Time Savings	Deploying a drone can provide time savings over setting up and employing equipment such as scaffolds/swing stages/scissor-lift vehicles, etc.
X	Staff Safety	Drones can be deployed to dangerous locations instead of personnel, such as rooftops, at the sides of building/bridges, along cliff areas or areas prone to erosion.
X	Data Quality	Some locations which are difficult to access by personnel may be more easily photographed using drone technology, thereby achieving better data.

Number of FTE (new & existing)	0		
Classification	n/a		
	Annual Cost	***Years***	***One-Time Cost***
Total Salary & Fringe			
Software			
Hardware/Equipment			
Professional Services	*$9,999*	1	
Training			
Other			
Total Cost			***$9,999***

The Department funds its use and maintenance of the surveillance technology through

- Port operating budget.

COMPARISON TO OTHER JURISDICTIONS

Drones or Unmanned Aerial Vehicles are currently utilized by other governmental entities for similar purposes.

Surveillance Technology Policy

Port

Unmanned Aircraft Systems (Drones)

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 Vehicles or Drones 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

The Department's mission is to: manages the waterfront as the gateway to a world-class city and advances environmentally and financially sustainable maritime, recreational, and economic opportunities to serve the City, Bay Area region, and California

The Surveillance Technology Policy ("Policy") defines the manner in which the Unmanned Aerial Vehicles or Drones will be used to support this mission, by describing the intended purpose, authorized and restricted uses, and requirements.

This Policy applies to all to department personnel that use, plan to use, or plan to secure Unmanned Aerial Vehicles or Drones, 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 Unmanned Aerial Vehicles or Drones technology for the Department is limited to the following use cases and is subject to the requirements listed in this Policy.

Authorized Use(s):

1. Disaster response and recovery: Provide DOC with high resolution images during response and recovery operations after a disaster.
2. Facility Inspections: Provide high resolution images during engineering and environmental surveys and assessments of Port properties.
3. Marketing: Capture Drone footage to be used in marketing materials for the promotion of activities and opportunities at the Port.

Prohibited use cases include any uses not stated in the Authorized Use Case section.

Departments may use information collected from technology only for legally authorized purposes, and may not use that information to unlawfully discriminate against people based on race, ethnicity, political opinions, religious or philosophical beliefs, trade union membership, gender, gender identity, disability status, sexual orientation or activity, or genetic and/or biometric data. Additionally, departments may not use automated systems to scan footage and identify individuals based on any of the categories listed in the preceding sentence.

Surveillance Oversight Review Dates

COIT Review: July 17, 2020

Board of Supervisors Review: TBD

BUSINESS JUSTIFICATION

Unmanned Aerial Vehicles or Drones supports the Department's mission and provides important operational value in the following ways:

1. Drones will provide the Port Department Operations Center (DOC) with high resolution images during response and recovery operations after a disaster.
2. Drones will provide high resolution images during engineering and environmental surveys and assessments of Port properties.
3. Drones will support the development of marketing materials for the promotion of activities and opportunities at the Port.

In addition, Unmanned Aerial Vehicles or Drones promises to benefit residents in the following ways:

X	Education	Drone imagery will be used to provide materials to residents by promoting Port efforts to advance improvements in the environment, social equity and quality of life for San Francisco residents and visitors.
▪	Community Development	
▪	Health	
X	Environment	Drone imagery will be used to conduct environmental surveys of Port property and open space. Drone imagery may be during an Oil Spill response to monitor environmentally sensitive sites and to conduct shoreline assessments
▪	Criminal Justice	
▪	Jobs	
▪	Housing	
X	Other	Drone imagery will be used in the Port's DOC to provide situational awareness and common operating picture during an emergency response.

In addition, the following benefits are obtained:

Benefit		Description
X	Financial Savings	Drones can be far more time efficient and cost effective when conducting asset inspections, by mitigating the need for traffic control, expensive scaffolding/swing stage or other equipment, and can provide more detailed photographs/videos of the assets or areas in need of maintenance or repairs than can be done manually, minimizing labor costs.

X	Time Savings	Deploying a drone can provide time savings over setting up and employing equipment such as scaffolds/swing stages/scissor-lift vehicles, etc.
X	Staff Safety	Drones can be deployed to dangerous locations instead of personnel, such as rooftops, at the sides of building/bridges, along cliff areas or areas prone to erosion.
X	Data Quality	Some locations which are difficult to access by personnel may be more easily photographed using drone technology, thereby achieving better data.

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 kept up to date and maintained.
Safety:	Surveillance technology must be operated in a safe manner. Surveillance technology should not be operated in a way that infringes on resident civil rights, including privacy, or causes personal injury or property damage.
Data Collection:	Departments shall minimize the use, collection, and retention of Personally Identifiable Information (PII) to what is strictly necessary to accomplish the intended purpose of the surveillance technology. Department shall only collect data required to execute the authorized use case. All data collected by the surveillance technology, including PII, shall be classified according to the City's Data Classification Standard. Should information be incidentally collected that is not necessary to accomplish the intended purpose of the surveillance technology, including information that may be used to identify persons or private information, Department shall remove all incidental PII from raw data. The surveillance technology collects some or all of the following data types:

Data Type(s)	***Format(s)***	***Classification***
Photographic and video data of Port	JPEG, PNG, MIOV, AVI, CSV	Level 2

	properties and facilities		
	Photographic and video of Port properties and facilities including critical maritime transportation system infrastructure regulated by the Maritime Transportation Security Act	JPEG, PNG, MIOV, AVI, CSV	Level 4

Notification: Departments shall notify the public of intended surveillance technology operation at the site of operations through signage in readily viewable public areas. Department notifications shall identify the type of technology being used and the purpose for such collection.

Department includes the following items in its public notice:

- X Information on the surveillance technology
- X Description of the authorized use
- X Type of data collected
- X Will persons be individually identified
- X Data retention
- X Department identification
- X Contact information

Access: All parties requesting access must adhere to the following rules and processes (please refer to the data sharing section to ensure all information covered in that section is also included below): Distinctive personal features or license plate information collected inadvertently (if any) will be blurred using an approved editing software prior to use or storage of images (drone "data") for any business purposes. Once PII have been obscured or removed from images, data may be used by department based on use cases identified above and may be stored on servers for future use. RAW (unedited) data shall not be used or retained.

Data must always be scrubbed of PII as stated above prior to use.

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.

- 0931 Manager III
- 0953 Chief Harbor Engineer 0923 Manager II
- 0922 Manager I, Port- Planning & Environment Port- Engineering Port- Executive

The following providers are required to support and maintains the surveillance technology and its associated data to ensure it remains functional:

- Baseline Environmental or another City Compliant Vendor

B. Members of the public

Port 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. Anyone, including criminal defendants, may access such data. 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, including by criminal defendants.

Members of the public, including criminal defendants, 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.

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).

To protect surveillance technology information from unauthorized access and control, including misuse, Departments shall, at minimum, apply the following safeguards:

- Only authorized personnel may access unedited data. Data will be encrypted and password protected.

Data Sharing:	Port will endeavor to ensure that other agencies or departments that may receive data collected by Drones will act in conformity with this Surveillance Technology Policy. 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. Port 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). Port shall ensure all PII and restricted data is de-identified or adequately protected to ensure the identities of individual subjects are effectively safeguarded. Each department that believes another agency or department receives or may receive data collected from its use of STs should consult with its assigned deputy city attorney regarding their response. Before sharing data with any recipients, the Department will use the following procedure to ensure appropriate data protections are in place: X Confirm the purpose of the data sharing aligns with the department's mission. X Consider alternative methods other than sharing data that can accomplish the same purpose. X Redact names, scrub faces, and ensure all PII is removed in accordance with the department's data policies. X Review of all existing safeguards to ensure shared data does not increase the risk of potential civil rights and liberties impacts on residents. X 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. X Ensure data will be shared in a cost-efficient manner and exported in a clean, machine-readable format. 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.

The Department currently participates in the following sharing practices:

A. Internal Data Sharing:

The department does not share surveillance technology data with other departments or entities inside the City and County of San Francisco.

Data sharing occurs at the following frequency: N/A

B. External Data Sharing:

Data sharing occurs at the following frequency:

- Dependent on services

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:

- The Port will not maintain records of raw, unprocessed drone data once the business purpose has been accomplished. The Port may store raw data up to a maximum of one year.
- The Port 2017 Drone Policy as approved by the Port Commission and COIT.

PII data shall not be kept in a form which permits identification of data subjects for any longer than is necessary for the purposes for which the personal data are processed. PII data collected by the surveillance technology may be retained beyond the standard retention period only in the following circumstance(s):

Exceptions to the standard must be supported with documentation and a clear rationale, and maintained by department staff to be reviewed by COIT.

Departments must establish appropriate safeguards for PII data stored for longer periods.

Data will be stored in the following location:

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

X Department of Technology Data Center

X Software as a Service Product

X Cloud Storage Provider

Data Disposal: Upon completion of the data retention period, Department shall dispose of data in the following manner:

	Practices: Raw data will be erased from all storage devices and servers after one year Processes and Applications: All instances of PII will be blurred or obscured using editing software, such that no recognizable human features or license plate information remain.
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 must receive training on data security policies and procedures. At the very least, 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. 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. Training applicable to: Port personnel and vendors on the Surveillance Technology Policy and the Port 2017 Drone Policy.

COMPLIANCE

Department shall oversee and enforce compliance with this Policy using the following methods:

- Training applicable to Port personnel and vendors on the Surveillance Technology Policy and the Port 2017 Drone Policy

Department shall assign the following personnel to oversee Policy compliance by the Department and third-parties:

- Security and Emergency Planning Manager

Sanctions for violations of this Policy include the following:

- Progressive discipline as per the Port's Personnel Policies and Procedures Manual, CCSF Personnel Policies and applicable employee memorandums of agreement.

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.

EXCEPTIONS

Only in exigent circumstances or in circumstances where law enforcement requires surveillance technology data for investigatory or prosecutorial functions may data collected, retained or processed by the surveillance technology be shared with law enforcement.

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.
Sensitive Data:	Data intended for release on a need-to-know basis. Data regulated by privacy laws or regulations or restricted by a regulatory agency or contract, grant, or other agreement terms and conditions.
Exigent Circumstances	An emergency involving imminent danger of death or serious physical injury to any person that requires the immediate use of Surveillance Technology or the information it provides.

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

Public:

Complaints or concerns can be submitted to the Department by:

Members of the public can register complaints/concerns or submit questions via calls or emails at 311.org or to the Port's 24-hour telephone number 415-274-0400

Department shall acknowledge and respond to complaints and concerns in a timely and organized response. To do so, Department shall:

- As per the Port of San Francisco Personnel Policies and Procedures Manual

City and County of San Francisco Employees:

All questions regarding this policy should be directed to the employee's supervisor or to the director. Similarly, questions about other applicable laws governing the use of the surveillance technology or the issues related to privacy should be directed to the employee's supervisor or the director.

Surveillance Impact Report

Public Utilities Commission
Unmanned Aircraft Systems (Drones)

As required by San Francisco Administrative Code, Section 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 Unmanned Aerial Vehicles or Drone technology.

DESCRIPTION OF THE TECHNOLOGY

The Department's mission is: to provide our customers with high quality, efficient and reliable water, power, and sewer services in a manner that is inclusive of environmental and community interests, and that sustains the resources entrusted to our care. San Francisco Public Utilities Commission provides retail drinking water & wastewater services to the City of San Francisco, wholesale water to three Bay Area counties, green hydroelectric & solar power to Hetch Hetchy electricity customers, and power to the residents & businesses of San Francisco through the CleanPowerSF program.

In line with its mission, the Department uses Unmanned Aerial Vehicles or Drone technology to: enable more efficient use of City resources and improved ability to inspect, manage and protect City infrastructure and natural resources.

Public Utilities Commission shall use Unmanned Aerial Vehicles or Drone technology only for the following authorized purposes:

1. Construction Management: Examples include inspection of project sites for contract and environmental compliance.
2. Environmental Monitoring & Documentation: Examples include monitoring of vegetation type and health, wildlife, and streams/reservoirs.
3. Inspections: Conducting surveys and assessments of SFPUC properties and assets. Examples include survey of bay and ocean outfalls, inspection of large wastewater collections and power line surveys.
4. Disaster Relief: Drones may be used in disaster relief to record footage of damage and assess the role PUC may play in responding to such disasters.
5. Marketing and Public Education: Drones may be used to capture footage of the watershed, as an example, to be used in public education and/or marketing materials.

Prohibited use cases involve any uses not stated in the Authorized Use Case section.

SFPUC UAV operations will always be consistent with our approved use cases in SFPUC Drone Policy. SFPUC shall not exchange raw drone data containing PII between City departments, or disclose such data to the public, except for exigent public safety needs or as required by law.

Department technology is located SFPUC watersheds and SFPUC construction sites.

Surveillance Oversight Review Dates
COIT Review: July 17, 2020
Board of Supervisors Review: TBD

Technology Details

The following is a product description of Unmanned Aerial Vehicles or Drone technology:

The DJI Phantom 4 Pro is an aerial survey drone that combines centimeter-level navigation and positioning with a high-performance imaging system for use during surveying, mapping or inspection operations.

A. How It Works

To function, Unmanned Aerial Vehicles or Drone technology utilizes an unmanned aircraft flown by a pilot via a ground control system, or autonomously through use of an on-board flight computer, communication links, or other any additional equipment, for the purpose of capturing images from an aerial perspective.

Data collected or processed by the Unmanned Aerial Vehicles will not be handled or stored by an outside provider or third-party vendor on an ongoing basis. The Department will remain the sole Custodian of Record.

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:

- The benefits of the surveillance technology outweigh the costs.
- The Department's Policy safeguards civil liberties and civil rights.
- 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 Drone technology has the following benefits for the residents of the City and County of San Francisco:

X	Education	Education: Drone imagery to promote SFPUC projects and educate the public and on our mission and operations.
▪	Community Development	
▪	Health	
▪	Environment	
▪	Criminal Justice	
▪	Jobs	

- Housing

X	Other	Public Safety: Efficient inspection of critical infrastructure (dams, sewer infrastructure, power lines) helps ensure infrastructure is operating safely, minimizing overall risk of failure.

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:

- SFPUC utilization of Drone technology is limited to monitoring assets and infrastructure on SFPUC owned lands and private property. Staff and consultants participating in SFPUC drone operations take precautions to ensure PII is not captured. If incidental PII is captured, data is scrubbed to remove any identifying information.

C. Fiscal Analysis of Costs and Benefits

The Department's use of Unmanned Aerial Vehicles ("UAV" or Drone technology) yields the following business and operations benefits:

Benefit		Description
X	Financial Savings	Drones are more efficient and cost effective than traditional methods. In environmental monitoring example, for an 8,000 ft fountain thistle site, it would take an estimated 120 labor hours to collect data if done by individuals counting plants, using traditional methods, costing an estimated $120,000. With a drone it would take two people less than two days and cost about $22,000, including labor and equipment.
X	Time Savings	Performing manual infrastructure inspections and environmental monitoring adds significant time to operations. See specific fountain thistle example above.
X	Staff Safety	See construction management and inspection examples above. Using a drone to capture imagery keeps staff out of dangerous and compromising situations (high structure inspections)
X	Data Quality	Some locations which are difficult to access by personnel may be more easily photographed using drone technology, providing improved overall data.

Number of FTE (new & existing)	2-4 employees, roughly 15-20 hours/month.		
Classification	1770 photographer, 1824 Principal Analyst, 9922 Public Service Aide		
	Annual Cost	***Years***	***One-Time Cost***
Total Salary & Fringe	*$30,364*		
Software			
Hardware/Equipment			$4,000
Professional Services	*$10,000*		
Training			
Other			
Total Cost			***$44,364***

The Department funds its use and maintenance of the surveillance technology through operating budget.

COMPARISON TO OTHER JURISDICTIONS

Unmanned Aerial Vehicles or Drone technology are currently utilized by other governmental entities for similar purposes.

Surveillance Technology Policy

Public Utilities Commission
Unmanned Aircraft Systems (Drones)

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 Vehicles or Drone technology 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

The Department's mission is to: provide our customers with high quality, efficient and reliable water, power, and sewer services in a manner that is inclusive of environmental and community interests, and that sustains the resources entrusted to our care. San Francisco Public Utilities Commission provides retail drinking water & wastewater services to the City of San Francisco, wholesale water to three Bay Area counties, green hydroelectric & solar power to Hetch Hetchy electricity customers, and power to the residents & businesses of San Francisco through the CleanPowerSF program.

The Surveillance Technology Policy ("Policy") defines the manner in which the Unmanned Aerial Vehicles or Drone technology will be used to support this mission, by describing the intended purpose, authorized and restricted uses, and requirements.

This Policy applies to all to department personnel that use, plan to use, or plan to secure Unmanned Aerial Vehicles or Drone technology, 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 Unmanned Aerial Vehicles or Drone technology for the Department is limited to the following use cases and is subject to the requirements listed in this Policy.

Authorized Use(s):

1. Construction Management: Examples include inspection of project sites for contract and environmental compliance.
2. Environmental Monitoring & Documentation: Examples include monitoring of vegetation type and health, wildlife, and streams/reservoirs.
3. Inspections: Conducting surveys and assessments of SFPUC properties and assets. Examples include survey of bay and ocean outfalls, inspection of large wastewater collections and power line surveys.
4. Disaster Relief: Drones may be used in disaster relief to record footage of damage and assess the role PUC may play in responding to such disasters.
5. Marketing and Public Education: Drones may be used to capture footage of the watershed, as an example, to be used in public education and/or marketing materials.

Surveillance Oversight Review Dates
COIT Review: July 17, 2020
Board of Supervisors Review: TBD

Prohibited use cases include any uses not stated in the Authorized Use Case section.

Departments may use information collected from technology only for legally authorized purposes, and may not use that information to unlawfully discriminate against people based on race, ethnicity, political opinions, religious or philosophical beliefs, trade union membership, gender, gender identity, disability status, sexual orientation or activity, or genetic and/or biometric data. Additionally, departments may not use automated systems to scan footage and identify individuals based on any of the categories listed in the preceding sentence.

BUSINESS JUSTIFICATION

Unmanned Aerial Vehicles or Drone technology supports the Department's mission and provides important operational value in the following ways:

The use of Drone technology enables more efficient use of City resources and improved ability to inspect, manage and protect City infrastructure and natural resources.

In addition, Drone technology promises to benefit residents in the following ways:

X	Education	Education: Drone imagery to promote SFPUC projects and educate the public and on our mission and operations.
▪	Community Development	
▪	Health	
▪	Environment	
▪	Criminal Justice	
▪	Jobs	
▪	Housing	
X	Other	Public Safety: Efficient inspection of critical infrastructure (dams, sewer infrastructure, power lines) helps ensure infrastructure is operating safely, minimizing overall risk of failure.

In addition, the following benefits are obtained:

Benefit		Description
X	Financial Savings	Drones are more efficient and cost effective than traditional methods. In environmental monitoring example, for an 8,000 ft fountain thistle site, it would take an estimated 120 labor hours to collect data if done by individuals counting plants, using traditional methods, costing an estimated $120,000. With a drone it would take two people less than two days and cost about $22,000, including labor and equipment.

X	Time Savings	Performing manual infrastructure inspections and environmental monitoring adds significant time to operations. See specific fountain thistle example above.
X	Staff Safety	See construction management and inspection examples above. Using a drone to capture imagery keeps staff out of dangerous and compromising situations (high structure inspections)
X	Data Quality	Some locations which are difficult to access by personnel may be more easily photographed using drone technology, providing improved overall data.

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 kept up to date and maintained.
Safety:	Surveillance technology must be operated in a safe manner. Surveillance technology should not be operated in a way that infringes on resident civil rights, including privacy, or causes personal injury or property damage.
Data Collection:	Departments shall minimize the use, collection, and retention of Personally Identifiable Information (PII) to what is strictly necessary to accomplish the intended purpose of the surveillance technology. Department shall only collect data required to execute the authorized use case. All data collected by the surveillance technology, including PII, shall be classified according to the City's Data Classification Standard. Should information be incidentally collected that is not necessary to accomplish the intended purpose of the surveillance technology, including information that may be used to identify persons or private information, Department shall remove all incidental PII from raw data. The surveillance technology collects some or all of the following data types:

Data Type(s)	*Format(s)*	*Classification*
Photographic and video data of	JPEG, PNG, MOV, AVI, CSV	Level 2

	assets, landscapes and property
Notification:	Departments shall notify the public of intended surveillance technology operation at the site of operations through signage in readily viewable public areas. Department notifications shall identify the type of technology being used and the purpose for such collection. Department includes the following items in its public notice: X Information on the surveillance technology X Description of the authorized use X Type of data collected X Will persons be individually identified X Data retention X Department identification X Contact information
Access:	All parties requesting access must adhere to the following rules and processes (please refer to the data sharing section to ensure all information covered in that section is also included below): SFPUC Drone Policy must be reviewed and signed by all SFPUC drone operators and any individuals with access to drone data that may contain Personal Identifiable Information. Contractor Provisions: If entering into a contract with a third party to operate drones, the contract shall include the following requirements: • Ownership and handling of City Data: "City Data" includes without limitation all data collected, used, maintained, processed, stored, or generated by or on behalf of the City, including as the result of the use of the services provided by a contractor. The City retains ownership and rights to City Data, including derivative works made from City Data and the licensing applied to the data. Contractors must treat City Data using the same Privacy and Data Security requirements that apply to CCSF employees. • Unauthorized use prohibited - Engaging in the unauthorized use of drones or activities that are inconsistent with this Policy may be grounds for termination of the relevant contract, as well as applicable monetary fines and penalties. • Signatures – This Drone Policy must be reviewed and signed by all drone operators, including contractors

- Insurance required – Contractor drone operators must provide proof of liability insurance commensurate with current SFPUC insurance requirements for contractors.

The SFPUC shall restrict access to any raw (i.e., unprocessed) drone footage that contains PII to authorized City staff (i.e., authorized employees and contractors) only. Distribution of raw drone data containing PII to other City departments shall be for the purpose of cleansing and processing data only. In all other circumstances, the SFPUC shall not exchange raw drone data containing PII between City departments, or disclose such data to the public, except for exigent public safety needs or as required by law.

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.

- 1770 Photographer, San Francisco Public Utilities Commission: Construction Management Bureau

B. Members of the public

Public Utilities Commission 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.

Data collected by surveillance technology will not be made available to members of the public, including criminal defendants.

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. Anyone, including criminal defendants, may access such data. 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, including by criminal defendants.

Members of the public, including criminal defendants, 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.

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).

To protect surveillance technology information from unauthorized access and control, including misuse, Departments shall, at minimum, apply the following safeguards:

- Should PII that is not related to the authorized purpose be incidentally collected through use of drones, the SFPUC shall remove all PII from the raw footage, or destroy the raw footage, within one year of collection. Exceptions to this one-year limit must be supported with documentation and a clear rationale, and maintained by SFPUC staff to be reviewed by COIT.

Data Sharing:	Public Utilities Commission will endeavor to ensure that other agencies or departments that may receive data collected by PUC's Drone technology will act in conformity with this Surveillance Technology Policy. 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. Public Utilities Commission 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) Public Utilities Commission shall ensure all PII and restricted data is de-identified or adequately protected to ensure the identities of individual subjects are effectively safeguarded. 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 response. Before sharing data with any recipients, the Department will use the following procedure to ensure appropriate data protections are in place: X Confirm the purpose of the data sharing aligns with the department's mission. X Consider alternative methods other than sharing data that can accomplish the same purpose. X Redact names, scrub faces, and ensure all PII is removed in accordance with the department's data policies. X 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.

Public Utilities Commission 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.

The Department currently participates in the following sharing practices:

A. Internal Data Sharing:

The department does not share surveillance technology data with other departments or entities inside the City and County of San Francisco.

B. External Data Sharing:

The department does not share surveillance technology data with other departments or entities outside the City and County of San Francisco.

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:

In accordance with the SFPUC Records Management Policy, data and video footage collected during drone operations will fall into one of the following categories:

1. Permanent Records: Records that are permanent or essential shall be retained and preserved indefinitely. Examples include: Drone video footage data collected for environmental monitoring and documentation.
2. Current Records: Records for which operational necessity, ready reference, convenience or other reasons are retained in the office space and equipment of the SFPUC. Examples include: Drone video footage data collected for construction management and inspections.
3. Storage Records: Records that are retained offsite. Typically, Current or Permanent records that have ceased to have immediate operational value, but which have a retention/lifecycle period that requires continued custodianship. Examples include: Drone video footage data collected for encroachments on the pipeline rights of way; until encroachment is removed.

PII data shall not be kept in a form which permits identification of data subjects for any longer than is necessary for the purposes for which the personal data are

processed. PII data collected by the surveillance technology may be retained beyond the standard retention period only in the following circumstance(s):

Environmental Monitoring: All data is kept for the lifetime of the project as it informs future trends and management, and is invaluable for monitoring population trends and habitat conditions for rare species.

Departments must establish appropriate safeguards for PII data stored for longer periods.

Data will 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
- Software as a Service Product
- Cloud Storage Provider

Data Disposal:	Upon completion of the data retention period, Department shall dispose of data in the following manner: Processes and Applications: All instances of PII will be blurred or obscured using editing software, such that no recognizable human features or license plate information remain.
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 must receive training on data security policies and procedures. At the very least, 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. 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. Drone data collection, dissemination and distribution is explained in SFPUC Drone Policy. All authorized users (staff and contractors) must sign off on policy prior to use.

COMPLIANCE

Department shall oversee and enforce compliance with this Policy using the following methods:

- For Drones, all flights are routed to SFPUC Emergency Planning and Security for approval, then inputted into the Open Data Portal 24 hours prior to flight.
- Department shall assign the following personnel to oversee Policy compliance by the Department and third-parties.
    - SFPUC Emergency Planning staff.

Sanctions for violations of this Policy include the following:

- Per SFPUC Drone Policy: "Engaging in the unauthorized use of drones or activities that are inconsistent with this Policy may be grounds for termination of the relevant contract, as well as applicable monetary fines and penalties."

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.

EXCEPTIONS

Only in exigent circumstances or in circumstances where law enforcement requires surveillance technology data for investigatory or prosecutorial functions may data collected, retained or processed by the surveillance technology be shared with law enforcement.

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.
Sensitive Data:	Data intended for release on a need-to-know basis. Data regulated by privacy laws or regulations or restricted by a regulatory agency or contract, grant, or other agreement terms and conditions.
Exigent Circumstances	An emergency involving imminent danger of death or serious physical injury to any person that requires the immediate use of Surveillance Technology or the information it provides.

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

Public:

Complaints, concerns, or questions may be submitted via the San Francisco Public Utilities Commission website https://www.sfwater.org/

Members of the public can send us an email to info@sfwater.org or call the General Inquiries phone number (415) 554-3289.

They may also send a letter via post to 525 Golden Gate Avenue, 10th floor, San Francisco, CA 94102.

Department shall acknowledge and respond to complaints and concerns in a timely and organized response. To do so, Department shall:

- Calls would be received by customer service personnel and routed to SFPUC Emergency Planning and Security for additional follow up.

City and County of San Francisco Employees:

All questions regarding this policy should be directed to the employee's supervisor or to the director. Similarly, questions about other applicable laws governing the use of the surveillance technology or the issues related to privacy should be directed to the employee's supervisor or the director.

Surveillance Impact Report

Recreation and Parks
Unmanned Aircraft Systems (Drones)

As required by San Francisco Administrative Code, Section 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 Unmanned aerial vehicles or Drone technology.

DESCRIPTION OF THE TECHNOLOGY

The Department's mission is to: provide enriching recreational activities, maintain beautiful parks and preserve the environment for the well-being of our diverse community.

In line with its mission, the Department uses Unmanned aerial vehicles Drone technology to:

1. In times of disaster preparedness or post-disaster mitigation, drones will provide critical emergency response functions such as logistical support for emergency routing, life safety, and cleanup efforts, not only assisting in protecting physical assets and public spaces but human life as well
2. Drones may support the maintenance and construction efforts by providing detailed photographic data of City-owned assets managed by RPD:
    - 4,113 acres of recreational and open space,
    - 3,400 acres within San Francisco,
    - 671 marina slips,
    - 220 neighborhood parks,
    - 179 playgrounds and play areas,
    - 82 recreation centers and clubhouses,
    - 72 basketball courts and 151 tennis courts,
    - 59 soccer/playfields (and growing),
    - 1 Family Camp.

Recreation and Parks shall use Unmanned aerial vehicles or Drone technology only for the following authorized purposes:

1. Disaster preparedness and response
2. Environmental monitoring and documentation
3. Inspect/Survey properties & assets
4. Project inspection and documentation
5. Surveying/Mapping data collection

Prohibited use cases include any use case not mentioned in the Authorized Uses section above.

The following use cases are expressly prohibited:

Surveillance Oversight Review Dates
COIT Review: July 17, 2020
Board of Supervisors Review: TBD

- Use of drone technology to intentionally capture images of a personal nature will always be prohibited. No PII (Personnel Identifiable Information) will be captured.

Department technology is located at RPD capital project sites, RPD buildings, parks, playgrounds, open space areas, recreation sites (e.g. courts).Use of drone technology to intentionally capture images of a personal nature will always be prohibited.

TECHNOLOGY DETAILS

The department has decided to contract out our UAV services so the equipment will vary from vendor to vendor. To date, we have not had any drone flights. Upcoming flights may include the Margaret Hayward Playground Improvement project, and the Garfield Pool Renovation project.

A. How It Works

To function, Unmanned aerial vehicles or Drone technology incorporates unmanned, remotely operated aircraft with onboard visual recording equipment, for the purpose of capturing images from an aerial perspective.

All data collected or processed by Unmanned aerial vehicles or Drone technology will be handled or stored by an outside provider or third-party vendor on an ongoing basis. Specifically, data will be handled by:

The department has decided to contract out our UAV services so the equipment will vary from vendor to vendor. To date, we have not had any drone flights. Upcoming flights may include the Margaret Hayward Playground Improvement project, and the Garfield Pool Renovation project.

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:

- The benefits of the surveillance technology outweigh the costs.
- The Department's Policy safeguards civil liberties and civil rights.
- 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 Drones has the following benefits for the residents of the City and County of San Francisco:

- Education
- Community Development

	▪ Health	
X	Environment	To inspect trees and other park features for project and/ or maintenance related work.
	▪ Criminal Justice ▪ Jobs ▪ Housing	
X	Other	To inspect trees and other park features to ensure public safety

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:

Drone operators/pilots are not authorized to intentionally capture data than can identify individuals. Auto license plate information shall also not be deliberately captured. To mitigate the risk of potential embarrassment, emotional distress, self-censorship or diminished civic engagement by SF residents whose personal information may be unintentionally captured, the department requires the "scrubbing" or otherwise obscuring/blurring (through use of image editing software) any collected data of facial images, license plates or other personally identifiable information unintentionally captured by aerial drones.

All collected data, irrespective of the location of data capture or the identifying characteristics of captured persons, is subject to the same scrubbing processes and procedures. The image software scrubbing process obscures and blurs all data using either built-in AI recognition settings or through manual efforts by software operator.

All recorded video will be stored on secured servers in the DT data center at 200 Paul Street data and data systems are physically protected, such as security systems, video surveillance, door and window locks, secured server and computer locations, and policies about mobile devices and removing hardware/software from certain locations.

To protect drone data from potential breach, misuse or abuse that may result in civil rights impacts, data is maintained on secure, department-owned servers. Only persons authorized to utilize the raw data may access the information and are required to maintain records of access using a drone data access log. Only data that has been edited to remove PII will be shared and stored on servers. Additionally, all contractors will be required to have a valid FAA-issued Unmanned Aerial Vehicle license.

C. Fiscal Analysis of Costs and Benefits

The Department's use of Drones or Unmanned Aerial Vehicles yields the following business and operations benefits:

Benefit		Description
X	Financial Savings	Mitigating the need for traffic control, expensive scaffolding/swing stage or other equipment, and can provide more detailed photographs/videos of the assets or areas in need of maintenance or repairs than can be done manually, minimizing labor costs.
X	Time Savings	Deploying a drone can provide time savings over setting up and employing equipment such as scaffolds/swing stages/scissor-lift vehicles, etc.
X	Staff Safety	Drones can be deployed to dangerous locations instead of personnel, such as rooftops, at the sides of building/bridges, along cliff areas or areas prone to erosion.
X	Data Quality	Locations which are difficult to access by personnel may be more easily photographed using drone technology, thereby achieving better data.

Number of FTE (new & existing)	1		
Classification	1090 and 5500 series		
	Annual Cost	***Years***	***One-Time Cost***
Total Salary & Fringe	*$5,000*		
Software			
Hardware/Equipment			
Professional Services			$20,000
Training			
Other			
Total Cost			***$25,000***

The Department funds its use and maintenance of the surveillance technology through:

- Capital funds will be utilized for Capital projects; Operational funds for operational activities.

COMPARISON TO OTHER JURISDICTIONS

Drones or Unmanned Aerial Vehicles are currently utilized by other governmental entities for similar purposes.

Surveillance Technology Policy

Recreation and Parks
Unmanned Aircraft Systems (Drones)

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 vehicles or Drone technology 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

The Department's mission is to: provide enriching recreational activities, maintain beautiful parks and preserve the environment for the well-being of our diverse community.

The Surveillance Technology Policy ("Policy") defines the manner in which the Unmanned aerial vehicles or Drone technology will be used to support this mission, by describing the intended purpose, authorized and restricted uses, and requirements.

This Policy applies to all to department personnel that use, plan to use, or plan to secure Unmanned aerial vehicles or Drone technology, 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 Unmanned aerial vehicles Drone technology for the Department is limited to the following use cases and is subject to the requirements listed in this Policy.

Authorized Use(s):

1. Disaster preparedness and response: In times of disaster preparedness or post-disaster mitigation, drones will provide critical emergency response functions such as logistical support for emergency routing, life safety, and cleanup efforts, not only assisting in protecting physical assets and public spaces but human life as well
2. Environmental monitoring and documentation
3. Inspect/Survey properties & assets
4. Project inspection and documentation
5. Surveying/Mapping data collection

Prohibited use cases include any uses not stated in the Authorized Use Case section.

Departments may use information collected from technology only for legally authorized purposes, and may not use that information to unlawfully discriminate against people based on race, ethnicity, political opinions, religious or philosophical beliefs, trade union membership, gender, gender identity, disability status, sexual orientation or activity, or genetic and/or

biometric data. Additionally, departments may not use automated systems to scan footage and identify individuals based on any of the categories listed in the preceding sentence.

BUSINESS JUSTIFICATION

Unmanned aerial vehicles or Drone technology supports the Department's mission and provides important operational value in the following ways:

Drone technology will support RPD's mission through the following ways:

1. In times of disaster preparedness or post-disaster mitigation, drones will provide critical emergency response functions such as logistical support for emergency routing, life safety, and cleanup efforts, not only assisting in protecting physical assets and public spaces but human life as well;
2. Drones may support the maintenance and construction efforts by providing detailed photographic data of City-owned assets managed by RPD:
    - 4,113 acres of recreational and open space,
    - 3,400 acres within San Francisco,
    - 671 marina slips,
    - 220 neighborhood parks,
    - 179 playgrounds and play areas,
    - 82 recreation centers and clubhouses,
    - 72 basketball courts and 151 tennis courts,
    - 59 soccer/playfields (and growing),
    - 1 Family Camp.

In addition, unmanned aerial vehicles or Drone technology) promises to benefit residents in the following ways:

	▪ Education	
	▪ Community Development	
	▪ Health	
X	Environment	To inspect trees and other park features for project and/ or maintenance related work.
	▪ Criminal Justice	
	▪ Jobs	
	▪ Housing	
X	Other	To inspect trees and other park features to ensure public safety.

In addition, the following benefits are obtained:

Benefit	Description

X	Financial Savings	Mitigating the need for traffic control, expensive scaffolding/swing stage or other equipment, and can provide more detailed photographs/videos of the assets or areas in need of maintenance or repairs than can be done manually, minimizing labor costs.
X	Time Savings	Deploying a drone can provide time savings over setting up and employing equipment such as scaffolds/swing stages/scissor-lift vehicles, etc.
X	Staff Safety	Drones can be deployed to dangerous locations instead of personnel, such as rooftops, at the sides of building/bridges, along cliff areas or areas prone to erosion.
X	Data Quality	Locations which are difficult to access by personnel may be more easily photographed using drone technology, thereby achieving better data.

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 kept up to date and maintained.
Safety:	Surveillance technology must be operated in a safe manner. Surveillance technology should not be operated in a way that infringes on resident civil rights, including privacy, or causes personal injury or property damage.
Data Collection:	Departments shall minimize the use, collection, and retention of Personally Identifiable Information (PII) to what is strictly necessary to accomplish the intended purpose of the surveillance technology. Department shall only collect data required to execute the authorized use case. All data collected by the surveillance technology, including PII, shall be classified according to the City's Data Classification Standard. Should information be incidentally collected that is not necessary to accomplish the intended purpose of the surveillance technology, including information that may be used to identify persons or private information, Department shall remove all incidental PII from raw data.

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

Data Type(s)	*Format(s)*	*Classification*
Images / videos of RPD capital project sites, RPD buildings, parks, playgrounds, open space areas, recreation sites (e.g. courts)	MOV, AVI, MP3	Level 2
Images / videos of RPD capital project sites, RPD buildings, parks, playgrounds, open space areas, recreation sites (e.g. courts)	MOV, AVI, MP3	Level 3

Notification: Departments shall notify the public of intended surveillance technology operation at the site of operations through signage in readily viewable public areas. Department notifications shall identify the type of technology being used and the purpose for such collection.

Department includes the following items in its public notice:

- X Information on the surveillance technology
- X Description of the authorized use
- X Type of data collected
- X Will persons be individually identified
- X Data retention
- X Department identification
- X Contact information

Access: All parties requesting access must adhere to the following rules and processes (please refer to the data sharing section to ensure all information covered in that section is also included below):

- Distinctive personal features or license plate information collected inadvertently (if any) will be blurred using an approved editing

software prior to use or storage of images (drone "data") for any business purposes. Once PII have been obscured or removed from images, data may be used by department based on use cases identified above, and may be stored on servers for future use. RAW (unedited) data shall not be used or retained.

- Data must always be scrubbed of PII as stated above prior to use.

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.

- 0900 Manager Class Series, 5500 Project Manager Class Series , Recreation and Park Department

The following providers are required to support and maintains the surveillance technology and its associated data to ensure it remains functional:

- The department has decided to contract out our UAV services so the equipment will vary from vendor to vendor. To date, we have not had any drone flights. Upcoming flights may include the Margaret Hayward Playground Improvement project, and the Garfield Pool Renovation project.

B. Members of the public

Recreation and Parks 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.

Data collected by surveillance technology will not be made available to members of the public, including criminal defendants.

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. Anyone, including criminal defendants, may access such data. 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, including by criminal defendants.

Members of the public, including criminal defendants, 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.

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). To protect surveillance technology information from unauthorized access and control, including misuse, Departments shall, at minimum, apply the following safeguards: - Only authorized drone operators or PM may access unedited data.
Data Sharing:	Recreation and Parks will endeavor to ensure that other agencies or departments that may receive data collected by Drones will act in conformity with this Surveillance Technology Policy. 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. Recreation and Parks 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) Recreation and Parks shall ensure all PII and restricted data is de-identified or adequately protected to ensure the identities of individual subjects are effectively safeguarded. Each department that believes another agency or department receives or may receive data collected from its use of Drones should consult with its assigned deputy city attorney regarding their response. Before sharing data with any recipients, the Department will use the following procedure to ensure appropriate data protections are in place: X Confirm the purpose of the data sharing aligns with the department's mission. X Consider alternative methods other than sharing data that can accomplish the same purpose. X Redact names, scrub faces, and ensure all PII is removed in accordance with the department's data policies. X Review of all existing safeguards to ensure shared data does not increase the risk of potential civil rights and liberties impacts on residents.

X	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.
X	Ensure data will be shared in a cost-efficient manner and exported in a clean, machine-readable format.

Recreation and Parks 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.

The Department currently participates in the following sharing practices:

A. Internal Data Sharing:

The department does not share surveillance technology data with other departments or entities inside the City and County of San Francisco.

B. External Data Sharing:

The department does not share surveillance technology data externally with entities outside the City and County of San Francisco.

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:

- Permanent records - stored permanently
- Current records - 2 years or as needed e.g. active capital projects
- Storage records - 2 years

PII data shall not be kept in a form which permits identification of data subjects for any longer than is necessary for the purposes for which the personal data are processed. PII data collected by the surveillance technology may be retained beyond the standard retention period only in the following circumstance(s):

- For capital construction projects, data may be stored for the duration of the project; for all others, data may be retained beyond this point on an as needed basis

Departments must establish appropriate safeguards for PII data stored for longer periods.

Data will be stored in the following location:

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

X Department of Technology Data Center

- Software as a Service Product
- Cloud Storage Provider

Data Disposal:	Upon completion of the data retention period, Department shall dispose of data in the following manner: Practices: Normal file deletion and formatting of hard disks will be used to dispose of the data. Processes and Applications: The department will use a third party vendor for all data scrubbing and de-identification
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 must receive training on data security policies and procedures. At the very least, 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. 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. RPD intends to utilize contractors for drone flights. Contractors must be knowledgeable about data editing practices to ensure that all PII has been removed prior to release.

COMPLIANCE

Department shall oversee and enforce compliance with this Policy using the following methods:

- IT will be the central point of coordination for drone flights. IT has drafted and supports a departmental Surveillance Technology Policy for Drones, which includes a procedural pre-mobilization and post-mobilization checklist which will be performed at each operation.

Department shall assign the following personnel to oversee Policy compliance by the Department and third-parties.

- RPD Chief Information Officer

Sanctions for violations of this Policy include the following:

- First Offense: Violators shall be verbally notified by the Recreation and Park Department's management of nature of the violation.

- Second offense: violator shall be notified in writing of second offence and privileges to operate drone hardware shall be suspended for 60 days.
- Third offense: (following reinstatement of operator privileges): violator shall be permanently banned from drone operations and disciplinary action may be taken depending upon the severity of second/third offences.

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.

EXCEPTIONS

Only in exigent circumstances or in circumstances where law enforcement requires surveillance technology data for investigatory or prosecutorial functions may data collected, retained or processed by the surveillance technology be shared with law enforcement.

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.
Sensitive Data:	Data intended for release on a need-to-know basis. Data regulated by privacy laws or regulations or restricted by a regulatory agency or contract, grant, or other agreement terms and conditions.
Exigent Circumstances	An emergency involving imminent danger of death or serious physical injury to any person that requires the immediate use of Surveillance Technology or the information it provides.

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

Public:

Complaints or concerns can be submitted to the Department by:

Members of the public can register complaints/concerns or submit questions to San Francisco Recreation and Parks through several ways: 1.) Send written correspondence to McLaren Lodge in Golden Gate Park, 501 Stanyan Street, San Francisco, CA 94117; 2.) Call to the RPD Front Desk 415-831-2700; 3.) Send an email to rpdinfo@sfgov.org; 4.) Contact 311.

All drone-related calls/complaints from the public received via mail or via call to the RPD Front Desk are routed to the RPD IT HelpDesk and logged in our department's request management system. Any requests from 311 are received in our department's dispatch system and routed to the RPD IT HelpDesk which then is logged in the request management system.

Once the request is tracked in the request management system, IT will work with all relevant parties to ensure completion.

City and County of San Francisco Employees:

All questions regarding this policy should be directed to the employee's supervisor or to the director. Similarly, questions about other applicable laws governing the use of the surveillance technology or the issues related to privacy should be directed to the employee's supervisor or the director.

Surveillance Impact Report

San Francisco International Airport
Security Cameras (Pre-Security Closed-Circuit Television)

As required by San Francisco Administrative Code, Section 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 Airport's use of surveillance cameras.

DESCRIPTION OF THE TECHNOLOGY

The Airport's mission is to provide an exceptional airport in service to our communities.

In line with its mission, the Airport shall use security cameras in its Closed-Circuit Television (CCTV) system only for the following authorized purposes:

Authorized Use(s):

1. Live monitoring.
2. Recording of video and images in the event of an incident.
3. Reviewing camera footage.
4. Providing video footage/images to law enforcement or other authorized persons following an incident, or upon request, when the footage is subject to disclosure pursuant to a Public Records Act request.

Prohibited use cases include any uses not stated in the Authorized Use Case section.

Further, processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, gender, gender identity, disability status, or an individual person's sex life or sexual orientation, and the processing of genetic data and/or biometric data for the purpose of uniquely identifying an individual person shall be prohibited.

Airport technology may be deployed in the following locations, based on use case:

Inside terminal buildings (pre-security) and terminal curbs adjacent to Terminal roadways.

Surveillance Oversight Review Dates
COIT Review: March 18, 2021
Board of Supervisors Review: TBD

Technology Details

The following is a product description:

The Airport uses Verint Video Management Software (VMS) and, primarily, Pelco Analog and Digital Pan-Tilt-Zoom (PTZ) and fixed cameras.

A. How It Works

The primary function of the CCTV is to record live video feed of various areas of the Airport.

Data collected or processed by security cameras will be handled and stored by an outside provider or third-party vendor on an ongoing basis.

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 Airport'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 Airport'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 Airport's use of Closed-Circuit Television (CCTV) has the following benefits for residents

	▪ Education	
	▪ Community Development	
X	Health	Protect safety of staff, patrons, and facilities while promoting an open and welcoming environment.
	▪ Environment	
X	Criminal Justice	Review video footage after a security incident; provide video evidence to law enforcement or the public upon request by formal process, order, or subpoena.
	▪ Jobs	
	▪ Housing	
	▪ Other – Public Safety	The technology helps ensure the safety of the 49,000+ people who work at the Airport and the 58 million people (pre-COVID) who fly to and from SFO every year.

B. Civil Rights Impacts and Safeguards

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

The Airport's use of CCTV is restricted to those identified Authorized Use Cases. The Airport retains CCTV footage for 1 year, consistent with state law. Video files are only released through subpoena, a public records act request, to assist law enforcement with an investigation and to assist Airport personnel in the investigation of claims.

Further, Airport Rules & Regulations and policies restrict use of CCTV. Airport personnel who monitor CCTV must maintain a current Airport badge and be trained in the proper use of cameras and footage. Contractors that handle and access video footage are required to execute a Corporate and Individual NDA.

Data is housed in servers located in secured areas that are only accessible by approved and badged employees. Cloud access to data is administered by Airport badged employees with access to cloud services that enables continuous monitoring of the Airport account activity.

C. Fiscal Analysis of Costs and Benefits

The Airport's use of surveillance cameras yields the following business and operations benefits:

Benefit		**Description**
X	Financial Savings	Airport CCTV saves on salary costs for Airport staff and SFPD-AB patrol officers.
X	Time Savings	Airport CCTV provides real-time feeds that run 24/7, thus eliminating lengthy physical surveillance of Airport facilities
X	Staff Safety	Security cameras provide advance view of an incident to better prepare those responding to an incident.
X	Data Quality	Security cameras run 24/7/365 which maximizes the Airport's ability to capture video of incidents. Video can be used to verify the accuracy of written reports regarding the incident.

The following provides the cost of operations funded by Airport revenues from airlines, concessions, and federal grants:

Number of FTE (new & existing)	Equivalent to 2.95 FTE Existing	
Classification	*1041, Network Engineer - Asst. 20%* *1042, Network Engineer - Journey 20%* *1042, System Engineer - Journey 25%* *1043, Network Engineer - Senior 20%* *1043, System Engineer - Senior 10%* *1044, Network Engineer - Principal 15%* *1044, Network Engineer - Principal 20%* *1044, System Engineer - Principal 25%* *1070, IS Project Director 5%* *7308, Cable Splicer 20%* *7318, Electronic Maint Tech 100%* *7318, Electronic Maint Tech 15%*	
	Annual Cost	***One-Time Cost***
Total Salary & Fringe	*Based on Feb 2021 Salaries* ***~$533,000***	
Software	*Combined in the Maint/Support cost. See below*	*Combined in the hardware cost*
Hardware/Equipment		*$5,753,387*
Professional Services		*2 Juniper Network Resident Engineer:* ***$165,325***
Training		
Other	*Verint Video Mgmt System Maint/Support:* ***$213,333*** *G4S Integration Svc:* ***$152,000*** *BART CCTV VIDSYS View - Lic & Support:* ***$24,177***	*Construction:* ***$11,343,264*** *Incl. roadside infrastructure to incl. gantries and LPR*
Total Cost	***$922,510***	***$17,261,976***

The Airport funds its use and maintenance of the surveillance technology through

Airport Operating Funds, Capital Funds, and Federal Grants.

COMPARISON TO OTHER JURISDICTIONS

CCTV solutions are used by other governmental entities, including Airports, for similar purposes.

Appendix A: Crime Statistics

Department: Airport

Section 19B requires each department in their Surveillance Impact Report to respond to the following question if applicable, "the general location(s) [of the surveillance technology] may be deployed and crime statistics for any location(s)."

The Airport operates approximately 3,500 Security Cameras located in SFO Domestic Terminals, International Terminal, terminal curbsides, courtyards, and surrounding buildings on SFO campus.

The department maintained an internal incident log for 2020:

CATEGORY	# of Incidents	% of Incidents
Abandoned Property	1	1%
Assault & Battery	5	6%
Burglary	3	4%
Contempt of Court	1	1%
Controlled Substance	4	5%
Controlled Substance - Transport	24	29%
Criminal Threat	1	1%
Disorderly Conduct	1	1%
Disturbing the Peace	1	1%
Firearm	4	5%
Grand Theft	9	11%
Jaywalking	1	1%
Petty Theft	4	5%
Robbery	1	1%
Suicide Attempt	1	1%
Theft – Vehicle	3	4%
Traffic Accident	5	6%
Trespassing	7	8%
Vandalism	4	5%
Welfare & Institution	3	4%
TOTAL	**83**	

Surveillance Impact Report

Arts Commission
Security Cameras

As required by San Francisco Administrative Code, Section 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 surveillance cameras.

DESCRIPTION OF THE TECHNOLOGY

Established by charter in 1932, the San Francisco Arts Commission is the City agency that champions the arts as essential to daily life by investing in a vibrant arts community, enlivening the urban environment and shaping innovative cultural policy.

In line with its mission, the Department shall use security cameras only for the following authorized purposes:

Authorized Use(s):

1. Live monitoring.
2. Recording of video and images in the event of an incident.
3. Reviewing camera footage.
4. Providing video footage/images to law enforcement or other authorized persons following an incident.

Prohibited use cases include any uses not stated in the Authorized Use Case section.

Further, processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, gender, gender identity, disability status, or an individual person's sex life or sexual orientation, and the processing of genetic data and/or biometric data for the purpose of uniquely identifying an individual person shall be prohibited.

Department technology may be deployed in the following locations, based on use case:

Main Gallery: 401 Van Ness Avenue, Suite 126

African American Art & Culture Complex: 762 Fulton Street

Bayview Opera House: 4705 3rd Street

Mission Cultural Center for Latino Arts: 2868 Mission Street

SOMArts: 934 Brannan Street

Surveillance Oversight Review Dates
COIT Review: March 18, 2021
Board of Supervisors Review: TBD

Technology Details

The following lists product description:

Main Gallery: 6 cameras.

African American Art & Culture Complex: 9 cameras.

Bayview Opera House: 12 cameras (Exacqvision).

Mission Cultural Center for Latino Arts: 28 cameras.

SOMArts: 15 cameras (Exacqvision)

A. How It Works

To function, the technology's primary functions are to provide live views and record video footage to dedicated, secure servers. The system is comprised of multiple cameras connected by data cables and infrastructure to the server. The footage is recorded on the server and stored for a limited amount of time.

Data collected or processed by security cameras will not be handled or stored by an outside provider or third-party vendor on an ongoing basis. The Department will remain the sole Custodian of Record.

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 security cameras has the following benefits for the residents of the City and County of San Francisco:

- Education
- Community Development

X	Health	Protect safety of staff, patrons, and facilities while promoting an open and welcoming environment.

- Environment

X	Criminal Justice	Review video footage after a security incident; provide video evidence to law enforcement or the public upon request by formal process, order, or subpoena.

- Jobs
- Housing
- Other

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:

Surveillance Camera systems pose potential risks to civil liberties in respect to dignity loss and loss of liberty.

An individual could be embarrassed or experience emotional distress if cameras capture behaviors, appearances, or circumstances by which they might feel humiliated. Examples include views of someone exhibiting an emotional outburst, a person's clothing or hair being disheveled, or someone having their physique ridiculed or leered at. Risks for loss of dignity are reduced by restricting access to live views, as well as recorded footage, to a limited number of authorized staff. In addition, the cameras do not pan, tilt or zoom, thus removing possible temptation for system operators to use those features to follow or enhance views of individuals. Audio is also not recorded or enabled.

Loss of liberty could potentially occur if a person were to be misidentified as the perpetrator of a crime or other incident, making them subject to wrongful arrest. An innocent person might be similar in appearance to someone who committed an offense. Surveillance images could reinforce other circumstantial evidence tying the wrong person to a criminal incident. As an example, someone might be wearing clothing like clothing worn by someone seen leaving an office where a theft had just occurred. Loss of liberty risks due to misidentification of a subject in surveillance video is mitigated by restricting access to live views and recorded footage to authorized personnel.

C. Fiscal Analysis of Costs and Benefits

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

Benefit		**Description**
X	Financial Savings	Department Security Camera Systems will save on building or patrol officers.
X	Time Savings	Department Security Camera Systems will run 24/7, thus eliminating building or patrol officer supervision

X	Staff Safety	Security cameras help identify violations of Department Patron Code of Conduct and provide assurance that staff safety is emphasized and will be protected at their place of employment.
X	Data Quality	Security cameras run 24/7/365 so full-time staffing is not required to subsequently review footage of security incidents. Data resolution can be set by level and is currently set to high resolution.

Number of FTE (new & existing)	$40,288. Cost for Hardware/Equipment and installation at our 4 Cultural Centers.	
Classification	N/A	
	Annual Cost	***One-Time Cost***
Software		868
Hardware/Equipment		30,006
Professional Services		0
Training		*0*
Other		9,002
Total Cost		***40,288***

The Department funds its use and maintenance of the surveillance technology through

Annual Facilities Maintenance budget.

COMPARISON TO OTHER JURISDICTIONS

Surveillance Camera Technologies are currently utilized by other governmental entities for similar purposes.

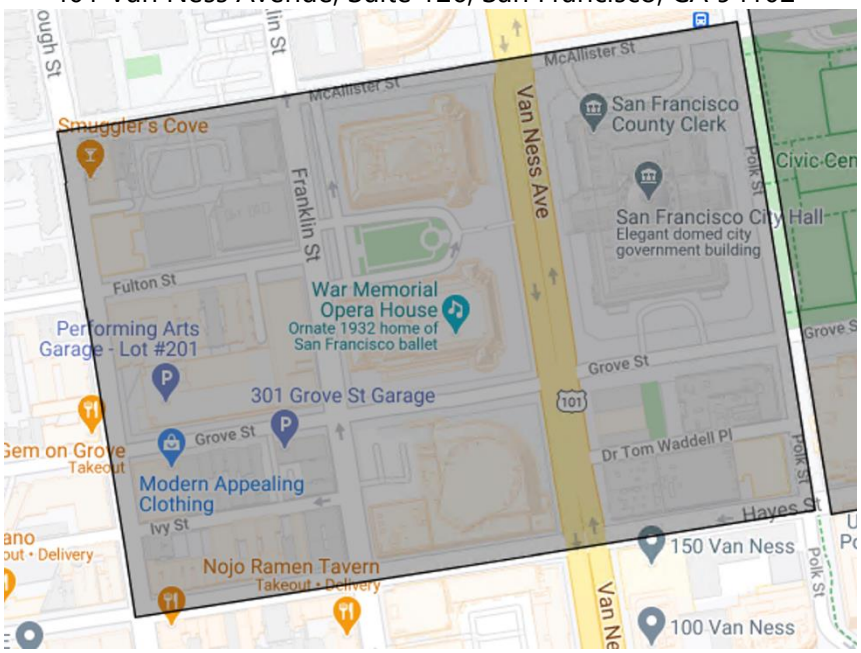
Appendix A: Crime Statistics

Department: Arts Commission

Section 19B requires each department in their Surveillance Impact Report to respond to the following question if applicable, "the general location(s) [of the surveillance technology] may be deployed and crime statistics for any location(s)."

The Arts Commission operates a total of 6 Security Cameras at the following locations:

- 401 Van Ness Avenue, Suite 126, San Francisco, CA 94102



[Image description: The image shows a screenshot of a mapped area around the Arts Commission building.]

Incident Category	Number of SFPD Incidents	Percent
	1	0.001701
Arson	1	0.001701
Assault	29	0.04932
Burglary	65	0.110544
Courtesy Report	1	0.001701
Disorderly Conduct	2	0.003401
Drug Offense	5	0.008503
Embezzlement	1	0.001701
Fire Report	1	0.001701
Forgery And Counterfeiting	1	0.001701
Fraud	10	0.017007
Larceny Theft	250	0.42517

Liquor Laws	1	0.001701
Lost Property	15	0.02551
Malicious Mischief	67	0.113946
Miscellaneous Investigation	3	0.005102
Missing Person	3	0.005102
Motor Vehicle Theft	30	0.05102
Non-Criminal	15	0.02551
Offences Against The Family And Children	7	0.011905
Other	8	0.013605
Other Miscellaneous	32	0.054422
Other Offenses	2	0.003401
Recovered Vehicle	1	0.001701
Robbery	5	0.008503
Stolen Property	3	0.005102
Suspicious Occ	4	0.006803
Traffic Violation Arrest	5	0.008503
Vandalism	2	0.003401
Vehicle Impounded	1	0.001701
Warrant	10	0.017007
Weapons Offense	7	0.011905

Information on crime statistics in 2020 in this area is provided by the San Francisco Police Department. Statistics are taken from a 1-block radius around the location of cameras. All information is obtained through the San Francisco Open Data Portal: https://datasf.org/opendata/

In addition, the department maintains an internal incident log which is available on request.

Surveillance Impact Report

Asian Art Museum
Security Cameras

As required by San Francisco Administrative Code, Section 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 surveillance cameras.

DESCRIPTION OF THE TECHNOLOGY

Our Mission is to inspire new ways of thinking by connecting diverse communities to historical and contemporary Asian art and culture though our world-class collection, exhibitions and programs.

In line with its mission, the Asian Art Museum utilizes the surveillance camera system to increase security officer capacity directly related to public safety. The technology enhances the department's ability to provide a safe and welcoming environment to patrons, visitors, and staff. The system is also used to help protect the priceless collection of art owned by the City of San Francisco.

The Asian Art Museum shall use security cameras only for the following authorized purposes:

Authorized Use(s):

1. Live monitoring.
2. Recording of video and images in the event of an incident.
3. Reviewing camera footage.
4. Providing video footage/images to law enforcement or other authorized persons following an incident.

Prohibited use cases include any uses not stated in the Authorized Use Case section.

Further, processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, gender, gender identity, disability status, or an individual person's sex life or sexual orientation, and the processing of genetic data and/or biometric data for the purpose of uniquely identifying an individual person shall be prohibited.

Department technology may be deployed in the following locations, based on use case:

Security camera systems will be placed in public facing areas to cover artwork, entrances and exits, as well as exterior locations to protect the museum and staff.

Surveillance Oversight Review Dates
COIT Review: March 18, 2021
Board of Supervisors Review: TBD

Technology Details

The following is a product description of the surveillance system at the Asian Art Museum:

The museum uses several different models of IP based cameras. The footage is stored on internally located servers, and the software is ExacqVision.

A. How It Works

The technology's primary functions are to provide live views and record motion video footage to a dedicated secure server. The system is comprised of multiple cameras connected to the server. The footage is recorded on the server and stored for various amounts of time based on server size and motion recording.

Data collected or processed by the Asian Art Museum surveillance camera system will not be handled or stored by an outside provider or third-party vendor on an ongoing basis. The Department will remain the sole Custodian of Record.

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 Asian Art Museum surveillance cameras system has the following benefits for the residents of the City and County of San Francisco:

	▪ Education	
	▪ Community Development	
X	Health	Protect safety of staff, patrons, and facilities while promoting an open and welcoming environment.
	▪ Environment	
X	Criminal Justice	Review video footage after a security incident; provide video evidence to law enforcement or the public upon request by formal process, order, or subpoena.

- Jobs
- Housing

X	Other	Public Safety - Assists security department investigating Asian Art Museum code of conduct violations and/or criminal acts. - Provides a mechanism to augment foot patrols, prevent criminal acts, and assist anyone requiring emergency help.

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:

The Asian Art Museum believes that the surveillance camera system poses potential risks to civil liberties in respect to dignity loss and loss of liberty.

And individual could be embarrassed or experience emotional distress if cameras capture certain behaviors, appearances, or circumstances by which they might feel humiliated. Examples include views of someone exhibiting an emotional outburst, a person's clothing or hair being disheveled, or having their physique ridiculed or leered at. Risks for loss of dignity are reduced by restricting access to live views, as well as recorded footage, to a limited number of trained security staff. Audio is not recorded or enabled.

Loss of liberty could potentially occur if a person were to be misidentified as the perpetrator of a crime or other incident, making them subject to wrongful arrest. An innocent person might be similar in appearance to someone who committed an offense. Surveillance images could reinforce other circumstantial evidence tying the wrong person to a criminal incident. As an example, someone might be wearing clothing similar to someone seen leaving an office where a theft had just occurred. Loss of liberty risks due to misidentification of a subject in surveillance video is mitigated by restricting access to live views and recorded footage to a limited number of trained personnel.

Release of camera footage to outside agencies or internal use is through the approval of the security management team. The technology is password protected to eliminate unauthorized use.

C. Fiscal Analysis of Costs and Benefits

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

Benefit		**Description**
X	Financial Savings	Help mitigate potential incidents that have a financial impact. These include but are not limited to medical response, theft, and vandalism.
X	Time Savings	Department Security Camera Systems will run 24/7, and are monitored from a security control room reducing response time to incidents or need for service.

X	Staff Safety	Security cameras help identify violations of department code of conduct or other applicable rules and laws. Enhances security staff's ability to observe patrons, visitors and staff members requiring assistance. Can help mitigate or prevent dangerous incidents.
X	Data Quality	Security cameras run 24/7/365 so full-time staffing is not required to subsequently review footage of security incidents. Recording is set to motion allowing for higher quality recording without compromising data storage.

Number of FTE (new & existing)	Control room is staffed 24 hours per day monitoring cameras, security and life safety systems. 4.2 FTE.	
Classification	8226 and 8202 for monitoring. 8228 and 0922 for review	
	Annual Cost	***One-Time Cost***
Software		
Hardware/Equipment	*20-30k*	500k
Professional Services		
Training		
Other		
Total Cost	***20-30k***	*500k*

The Department funds its use and maintenance of the surveillance technology through:

- Non-City funding on an annual maintenance. Upgrades through capital requests.
- The Asian Art Museum started upgrading the camera system in 2014. This project took several years to complete. The funding was primarily thought COIT funding, with some funds received from City capital. Additional funding was through the museum Foundation (non-City funds).

COMPARISON TO OTHER JURISDICTIONS

Surveillance technologies like the Asian Art Museum surveillance camera system are currently utilized by other governmental entities for similar purposes.

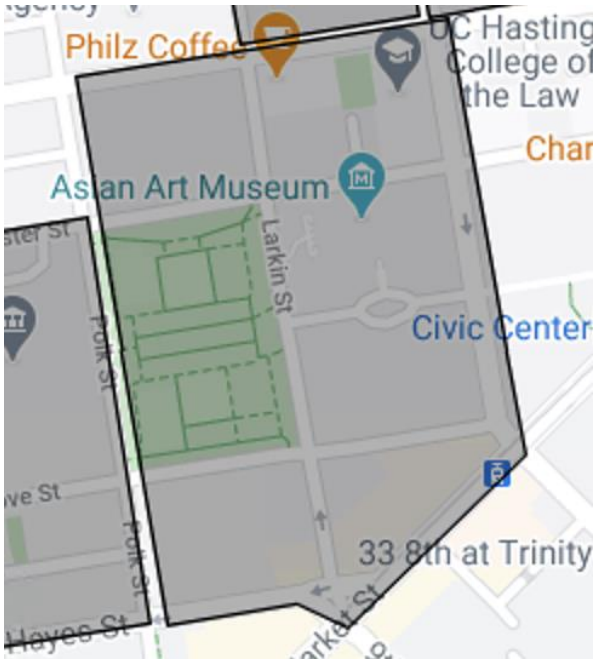
Appendix A: Crime Statistics

Department: Asian Art Museum

Section 19B requires each department in their Surveillance Impact Report to respond to the following question if applicable, "the general location(s) [of the surveillance technology] may be deployed and crime statistics for any location(s)."

The Asian Art Museum operates a total of 242 Security Cameras at the following location:

- 200 Larkin Street, San Francisco, CA 94102



[Image description: The image shows a screenshot of a mapped area around the Asian Art Museum building.]

Incident Category	Number of SFPD Incidents	Percent
	5	0.002798
Arson	1	0.00056
Assault	123	0.06883
Burglary	23	0.012871
Courtesy Report	5	0.002798
Disorderly Conduct	16	0.008954
Drug Offense	640	0.358142
Drug Violation	1	0.00056
Fire Report	1	0.00056
Forgery And Counterfeiting	7	0.003917
Fraud	25	0.01399

Larceny Theft	159	0.088976
Lost Property	26	0.01455
Malicious Mischief	63	0.035255
Miscellaneous Investigation	9	0.005036
Missing Person	19	0.010632
Motor Vehicle Theft	33	0.018467
Non-Criminal	137	0.076665
Offences Against The Family And Children	29	0.016228
Other	31	0.017348
Other Miscellaneous	148	0.08282
Other Offenses	15	0.008394
Prostitution	1	0.00056
Recovered Vehicle	13	0.007275
Robbery	43	0.024063
Sex Offense	3	0.001679
Stolen Property	2	0.001119
Suspicious Occ	37	0.020705
Traffic Collision	4	0.002238
Traffic Violation Arrest	34	0.019026
Vandalism	3	0.001679
Vehicle Impounded	1	0.00056
Warrant	104	0.058198
Weapons Carrying Etc	13	0.007275
Weapons Offense	13	0.007275

Information on crime statistics in 2020 in this area is provided by the San Francisco Police Department. Statistics are taken from a 1-block radius around the location of cameras. All information is obtained through the San Francisco Open Data Portal: https://datasf.org/opendata/

In addition, the department maintained an internal incident log in 2020:

Asian Art Museum Statistics	CY2020
Assault/Battery	4
Burglary	0
Fire	4
Homicide	0
Medical	25
Robbery	0
Shooting	0
Stabbing	3

Drug activity	3500
Theft	0
Vandalism	29
Vehicle accident	5
Total	**3570**

Surveillance Impact Report

Child Support Services
Security Cameras

As required by San Francisco Administrative Code, Section 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 surveillance cameras.

DESCRIPTION OF THE TECHNOLOGY

The San Francisco Department of Child Support Service's (SFDCSS or Department) mission is to empower parents to provide support for their children by furnishing child support services in the form of location of parents, establishment of parenting and support obligations and enforcement of support obligations, thereby contributing to the wellbeing of families and children.

In line with its mission, the Department uses Sonitrol Security System to protect against unauthorized access to confidential customer data, and for customer and employee safety. Sonitrol monitors physical access to the facility where customer information resides to detect and respond to physical security incidents.

In line with its mission, the Department shall use security cameras only for the following authorized purposes:

Authorized Use(s):

1. Live monitoring.
2. Recording of video and images in the event of an incident.
3. Reviewing camera footage.
4. Providing video footage/images to law enforcement or other authorized persons following an incident.

Prohibited use cases include any uses not stated in the Authorized Use Case section.

Further, processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, gender, gender identity, disability status, or an individual person's sex life or sexual orientation, and the processing of genetic data and/or biometric data for the purpose of uniquely identifying an individual person shall be prohibited.

Department technology may be deployed in the following locations, based on use case:

Points of entries, public lobby, and Intake/Interview areas.

Surveillance Oversight Review Dates
COIT Review: March 18, 2021
Board of Supervisors Review: TBD

Technology Details

The following is a product description of Sonitrol Security System:

Sonitrol's verified alarms are sound-based – not motion-based – so when an alarm is triggered, our monitoring professionals can actually listen to determine whether a break-in is in progress, or whether a false alarm has occurred. If it is a break-in, Sonitrol staff immediately dispatch police and relay real-time information to the responding officers. If it is a false alarm, Sonitrol staff simply reset the system without contacting the police. Because of this ability to verify alarms, Sonitrol has the highest apprehension rate and the lowest false alarm rate in the industry.

A. How It Works

To function, Sonitrol Security System monitors building access and safety using surveillance cameras at points of entries, public lobby, and Intake/Interview areas.

Data collected or processed by security cameras is not handled or stored by an outside provider or third-party vendor on an ongoing basis. The Department will remain the sole Custodian of Record.

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 security cameras has the following benefits for the residents of the City and County of San Francisco:

- Education
- Community Development

X	Health	Protect safety of staff, patrons, and facilities while promoting an open and welcoming environment.

- Environment

X	Criminal Justice	Review video footage after a security incident; provide video evidence to law enforcement or the public upon request by formal process, order, or subpoena.

- Jobs
- Housing
- Other

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:

- Administrative Safeguards: Departmental access is restricted to SFDCSS IT, SFDCSS Executive Management, SFDCSS HR and Allied Security Guards. Upon request, SFDCSS IT will provide access to video footage to the above mentioned, as well as SFPD personnel. All staff and contractors are required to complete annual training, sign annual confidentiality forms and submit to Live Scan background checks to meet minimum employment requirements.

- Technical Safeguards: SFDCSS follows restricted access protocols. Only IT Manager and IT Administrators have access to stored video footage and access point records. To protect data from potential breach, misuse or abuse that may result in impacts to the public, data is maintained on secure, department-owned servers. Server backup transmission is secured in accordance with Federal, State and local regulations. Only persons authorized to utilize the data may access the information and are required to maintain records of access. Data is provided to Executive Management, HR and SFPD upon request. Lobby Security Guard personnel have view-only access and monitor live footage during business hours.

- Physical Safeguards: Data can only be accessed onsite at SFDCSS – 617 Mission Street or, in the event of a disaster, our secondary backup appliance is stored at SFO. The data and data systems are secured during transmission and during rest in accordance with Federal, State and Local regulations.

C. Fiscal Analysis of Costs and Benefits

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

Benefit		**Description**
X	Financial Savings	Department Security Camera Systems will save on building or patrol officers.
X	Time Savings	Department Security Camera Systems will run 24/7, thus eliminating building or patrol officer supervision

X	Staff Safety	Security cameras help identify violations of Department Patron Code of Conduct and provide assurance that staff safety is emphasized and will be protected at their place of employment.
X	Data Quality	Security cameras run 24/7/365 so full-time staffing is not required to subsequently review footage of security incidents. Data resolution can be set by level and is currently set to high resolution.

Number of FTE (new & existing)	2 guards *40hr/week*52 weeks*$31.84hr	
Classification	N/A (Security guard contractor hired by HSA)	
	Annual Cost	***One-Time Cost***
Software	$0	
Hardware/Equipment	$7,290.42	
Professional Services	$4,872.24	
Training	$0	
Other	$0	
Total Cost	$144,662.66	

The Department funds its use and maintenance of the surveillance technology through state and federal subvention and receives no county general fund dollars.

COMPARISON TO OTHER JURISDICTIONS

Sonitrol Security System are currently utilized by other governmental entities for similar purposes.

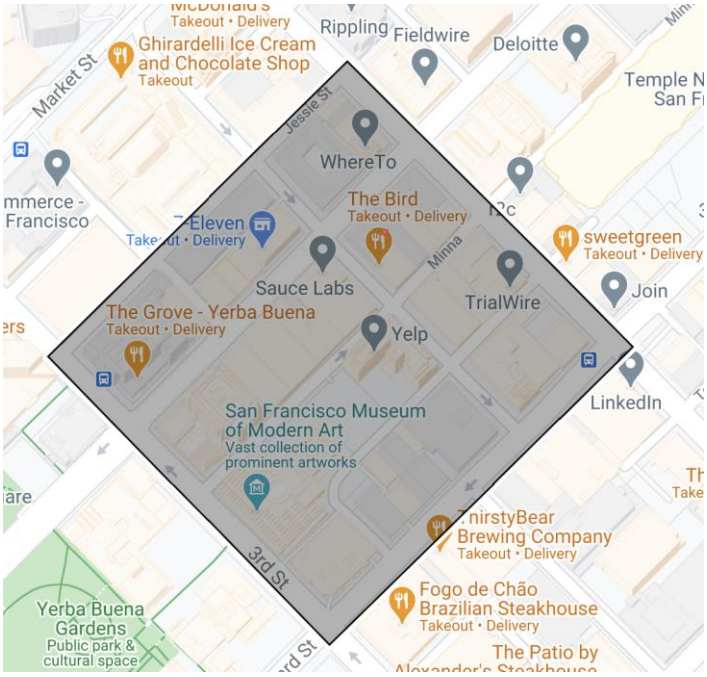
Appendix A: Crime Statistics

Department: Child Support Services

Section 19B requires each department in their Surveillance Impact Report to respond to the following question if applicable, "the general location(s) [of the surveillance technology] may be deployed and crime statistics for any location(s)."

The Child Support Services Department operates a total of 8 Security Cameras at the following locations:

- 617 Mission Street, San Francisco, CA 94105



[Image description: The image shows a screenshot of a mapped area around the Child Support Services building.]

Incident Category	Number of SFPD Incidents	Percent
	2	0.004751
Arson	1	0.002375
Assault	33	0.078385
Burglary	48	0.114014
Disorderly Conduct	6	0.014252
Drug Offense	1	0.002375
Fire Report	2	0.004751
Fraud	13	0.030879
Homicide	1	0.002375
Larceny Theft	111	0.263658

Lost Property	11	0.026128
Malicious Mischief	50	0.118765
Miscellaneous Investigation	2	0.004751
Missing Person	3	0.007126
Motor Vehicle Theft	12	0.028504
Non-Criminal	25	0.059382
Offences Against The Family And Children	4	0.009501
Other	4	0.009501
Other Miscellaneous	39	0.092637
Other Offenses	1	0.002375
Recovered Vehicle	3	0.007126
Robbery	17	0.04038
Stolen Property	3	0.007126
Suspicious Occ	3	0.007126
Traffic Collision	2	0.004751
Traffic Violation Arrest	6	0.014252
Vandalism	3	0.007126
Warrant	11	0.026128
Weapons Carrying Etc	3	0.007126
Weapons Offense	1	0.002375

Information on crime statistics in 2020 in this area is provided by the San Francisco Police Department. Statistics are taken from a 1-block radius around the location of cameras. All information is obtained through the San Francisco Open Data Portal: https://datasf.org/opendata/

In addition, the department maintains an internal incident log which is available on request.

Surveillance Impact Report

Real Estate Division of the City Administrator's Office
Security Cameras

As required by San Francisco Administrative Code, Section 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 Real Estate Division's use of surveillance cameras.

I. DESCRIPTION OF THE TECHNOLOGY

The Real Estate Division acquires and manages the City Administrator's real estate portfolio ensuring optimal use of City owned vacant, improved and leased properties for the highest public use and benefit, generating maximum revenue and overall financial return, and providing real estate services and assistance to the Mayor, Board of Supervisors, City departments and City residents with expertise, efficient and commitment.

In line with its mission, the Division utilizes Surveillance Camera Systems to increase deputy sheriff/security officer capacity directly related to public safety and well-being and to protect the City's property. The technology enhances the Division's ability to provide a safe, secure and welcoming environment to staff and visitors to its facilities.

The Division shall use security cameras only for the following authorized purposes:

Authorized Use(s):

1. Live monitoring.
2. Recording of video and images in the event of an incident.
3. Reviewing camera footage.
4. Providing video footage/images to law enforcement or other authorized persons following an incident.

Prohibited use cases include any uses not stated in the Authorized Use Case section.

Further, processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, gender, gender identity, disability status, or an individual person's sex life or sexual orientation, and the processing of genetic data and/or biometric data for the purpose of uniquely identifying an individual person shall be prohibited.

Surveillance Oversight Review Dates
COIT Review: March 18, 2021
Board of Supervisors Review: TBD

A. Facilities

The Division currently has technology deployed in the following locations:

Office of Chief Medical Examiner	1 Newhall	Public Interior, Exterior, All Exterior Doors, Lobby, Within halls
1 South Van Ness		Public Interior, Exterior, Garage
Permit Center/Office Building	49 South Van Ness	Public Interior, Exterior
1650 Mission		Public Interior, Exterior, Garage
25 Van Ness		Public Interior (Lobby), Exterior
Central Shops	450 Toland	Public Interior, Exterior
Central Shops	555 Selby	Public Interior, Exterior
City Hall	1 Dr. Carlton B. Goodlett Place	Public Interior, Interior Mayor's Office, Exterior
Animal Care and Control	1419 Bryant	Under construction Interior/Exterior
Hall of Justice	850 Bryant	Freight Back Door and Hallway, Exterior

B. Technology Details

The following is a product description:

Cameras: Arecont, Axis, Bosch, Avigilon, Pelco, Samsung, Sony, Panasonic, and Vivotek
Server: Avigilon Control Center (ACC) Video management system, ExacqVision
Software: Avigilon, ExacqVision, ACC Video Management Software,
Access Control Systems: Honeywell-Pro Watch (Monitor and operate RFID readers, door sensors, requests to exit triggers (REX) (push to exit buttons), horns and locks 24 hours a day

i. How It Works

To technology's primary functions are to provide live views and record video footage to a dedicated, secure server (stored in security closets or IDFs). The systems are comprised of multiple cameras connected by data cables and infrastructure to the server. The footage is recorded on the server and stored for a specific amount of time.

Most cameras are programmed to record only when motion is detected; when the motion ends the recording stops. Old archives are continuously erased automatically as new archives are recorded.

Data collected or processed by RED's security cameras and systems is self-contained and discrete. They do not share information with other City or private databases. It will not be handled or stored by an outside provider or third-party vendor on an ongoing basis. The Division will remain the sole Custodian of Record.

II. 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 Division'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 Division's use of security cameras has the following benefits for the residents of the City and County of San Francisco:

▪	Education	
▪	Community Development	
X	Health	Protect safety of staff, patrons, and facilities while promoting an open and welcoming environment.
▪	Environment	
X	Criminal Justice	Review video footage after a security incident; provide video evidence to law enforcement or the public upon request by formal process, order, or subpoena.
▪	Jobs	
▪	Housing	
X	Other	City Code of Conduct Violations/Criminal Acts – assists security and DHR investigations; Augments security foot patrols, deters criminal behavior, assists with emergency response

B. Civil Rights Impacts and Safeguards

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

The Real Estate Division understands and has considered the potential impacts on civil liberties and civil rights as set forth in the draft National Institute of Standards and Technology (NIST) Privacy Framework. To mitigate same and prevent potential breach, misuse or abuse, RED's maintains robust administrative, technical, physical, and operational security practices.

- Data is maintained on secure, Division-owned servers.
- No outside vendor uses, processes, or stores data captured and archived by the Avigilon or Exacqvision systems.
- Vendors have no direct administrative or maintenance access to databases or services. If access is needed (for testing, maintenance, repair), they are accompanied by an approved and authorized RED staff member who logs into the device and remains onsite.
- Archived video records are available in proprietary formats. Avigilon files can only be viewed with an accompanying PC compatible video player. Exacqvision files are self-contained within a PC executable viewer.
- Date and time information are available by using these viewers.
- All video from Avigilon archives is watermarked to guard against post-export manipulation.
- Most cameras are programmed to record only when motion is detected; when the motion begins, recording begins, and when the motion ends, the recording stops. No other video analytics such as facial recognition or other biometrics are employed by RED.
- These systems are self-contained, discrete, and do not share information with other databases.
- RED has a request form and procedure for requests for recorded video, with both Director and City Attorney, District Attorney, Subpoena, or Sheriff's Counsel approval.
- RED has logs of all requests to review video which include date, time, and requestor along with approval for same.
- Only authorized and trained staff may view live feeds, review footage and obtain footage for approved requests.
- Buildings, cameras, servers and related equipment are physically secured by various measures including building security systems, door locks, alarm systems, log in requirements and cameras.

C. Fiscal Analysis of Costs and Benefits

The Division's use of surveillance cameras yields the following business and operations benefits:

Benefit		Description
X	Financial Savings	Department Security Camera Systems reduce the staff needed for building security and/or deputy sheriffs – usually overnight patrol officers.
X	Staff Safety	Security cameras help identify violations of the City's Staffs' Code of Conduct, Building Rules and Regulations, and provide assurance that staff safety is emphasized and will be protected at their place of

	employment. Provides alerts of emergency situations, persons requiring help and/or injured, mitigate dangerous incidents as they occur.

	Annual Cost	***One-Time Cost***
Software	$25,000	$37,000
Hardware/Equipment	$50,000	$871,000 (to allow for 1 year of storage)
Professional Services	$20,000	$25,000
Training	$5,000	
Other/Personnel Sheriffs (City Hall, OCME) Security Guards (Vendors) 8211 - 1 8207 – Card Readers/Vendors	 $1,225,000 $2,215,840 $ 70,000 $437,500 $130,000	
Total Cost	**$4,178,340**	**$933,000**

The Department funds its use and maintenance of the surveillance technology through its annual budget and requests for capital improvements (COIT).

III. COMPARISON TO OTHER JURISDICTIONS

RED's Surveillance Camera Technologies are currently utilized by other city departments and governmental entities for similar purposes.

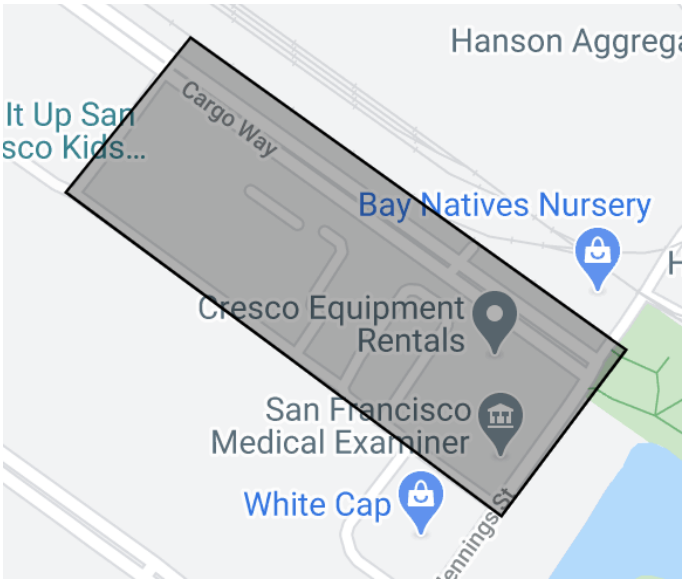
Appendix A: Crime Statistics

Department: City Administrator's Office – Real Estate Division

Section 19B requires each department in their Surveillance Impact Report to respond to the following question if applicable, "the general location(s) [of the surveillance technology] may be deployed and crime statistics for any location(s)."

The City Administrator's Office – Real Estate Division operates a total of 511 Security Cameras at the following locations:

- Medical Examiner, 1 Newhall Street, San Francisco, CA 94124

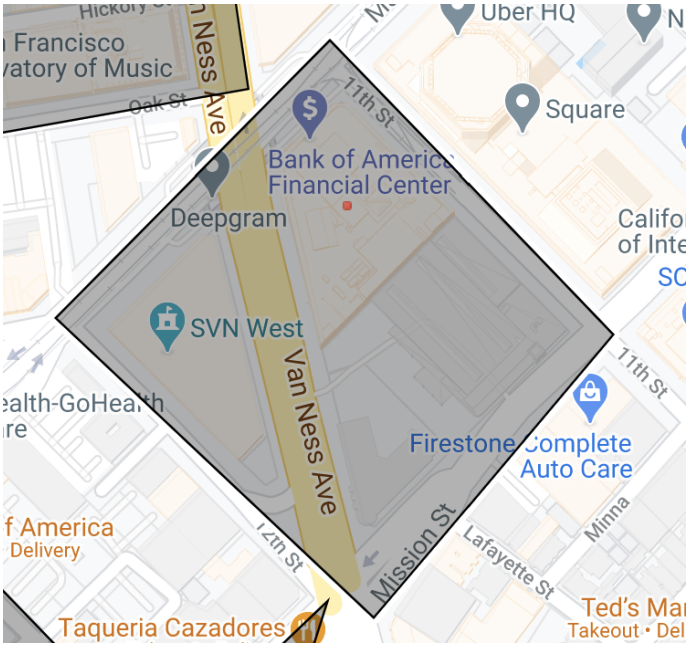


[Image description: The image shows a screenshot of the Medical Examiner building.]

Incident Category	Number of SFPD Incidents	Percent
Assault	2	0.060606
Burglary	2	0.060606
Fire Report	1	0.030303
Forgery And Counterfeiting	1	0.030303
Larceny Theft	7	0.212121
Lost Property	1	0.030303
Malicious Mischief	2	0.060606
Missing Person	2	0.060606
Motor Vehicle Theft	7	0.212121
Non-Criminal	2	0.060606
Other Miscellaneous	2	0.060606
Robbery	1	0.030303
Stolen Property	1	0.030303

Suspicious Occ	2	0.060606

- 1 South Van Ness Avenue, San Francisco, CA 94103

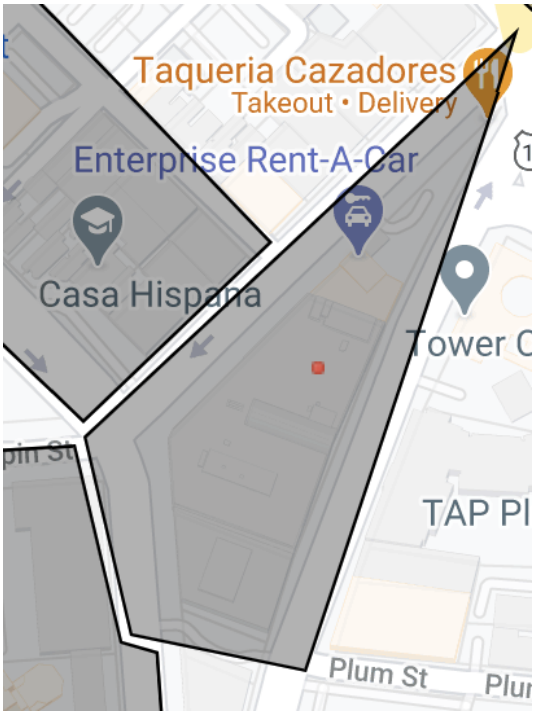


[Image description: The image shows a screenshot of a mapped area around the 1 South Van Ness Avenue building.]

Incident Category	Number of SFPD Incidents	Percent
Arson	2	0.011561
Assault	23	0.132948
Burglary	15	0.086705
Disorderly Conduct	7	0.040462
Drug Offense	2	0.011561
Family Offense	1	0.00578
Fire Report	2	0.011561
Forgery And Counterfeiting	1	0.00578
Fraud	4	0.023121
Larceny Theft	22	0.127168
Lost Property	4	0.023121
Malicious Mischief	11	0.063584
Missing Person	1	0.00578
Motor Vehicle Theft	3	0.017341
Non-Criminal	31	0.179191
Offences Against The Family And Children	4	0.023121
Other	2	0.011561
Other Miscellaneous	13	0.075145

Other Offenses	2	0.011561
Rape	1	0.00578
Robbery	2	0.011561
Stolen Property	1	0.00578
Suspicious Occ	7	0.040462
Traffic Violation Arrest	4	0.023121
Warrant	7	0.040462
Weapons Offense	1	0.00578

- 1650 Mission Street, San Francisco, CA 94103

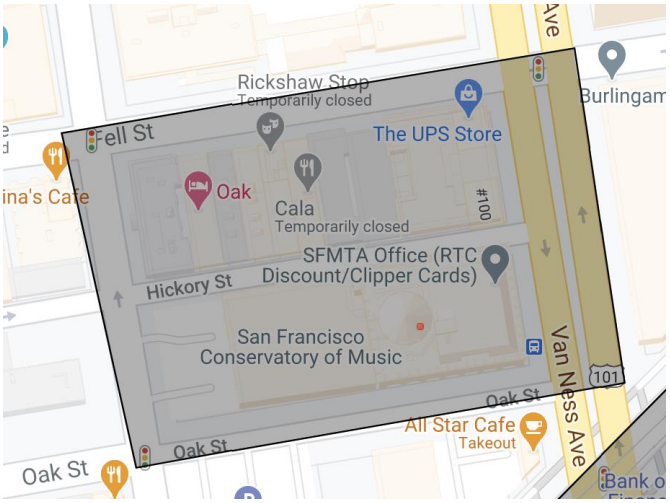


[Image description: The image shows a screenshot of a mapped area around the 1650 Mission Street building.]

Incident Category	Number of SFPD Incidents	Percent
Assault	11	0.099099
Burglary	7	0.063063
Courtesy Report	1	0.009009
Disorderly Conduct	7	0.063063
Fraud	5	0.045045
Larceny Theft	22	0.198198
Malicious Mischief	12	0.108108
Miscellaneous Investigation	4	0.036036
Missing Person	3	0.027027
Motor Vehicle Theft	2	0.018018
Non-Criminal	11	0.099099

Offences Against The Family And Children	5	0.045045
Other	2	0.018018
Other Miscellaneous	7	0.063063
Prostitution	1	0.009009
Robbery	1	0.009009
Suspicious Occ	4	0.036036
Traffic Violation Arrest	2	0.018018
Warrant	4	0.036036

- 25 Van Ness Avenue, San Francisco, CA 94102



[Image description: The image shows a screenshot of a mapped area around the 25 Van Ness Avenue building.]

Incident Category	Number of SFPD Incidents	Percent
Arson	1	0.006098
Assault	7	0.042683
Burglary	10	0.060976
Disorderly Conduct	1	0.006098
Drug Offense	1	0.006098
Embezzlement	1	0.006098
Fraud	7	0.042683
Larceny Theft	91	0.554878
Lost Property	1	0.006098
Malicious Mischief	12	0.073171
Missing Person	2	0.012195
Motor Vehicle Theft	5	0.030488
Non-Criminal	4	0.02439
Offences Against The Family And Children	4	0.02439
Other Miscellaneous	6	0.036585

Recovered Vehicle	2	0.012195
Robbery	2	0.012195
Suspicious Occ	3	0.018293
Traffic Violation Arrest	2	0.012195
Warrant	2	0.012195

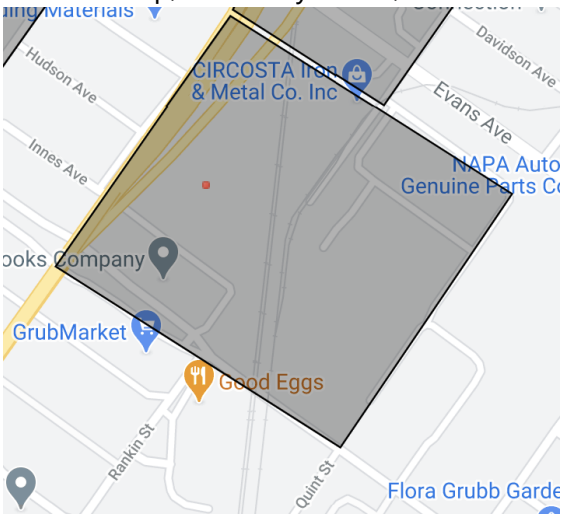
- Central Shop, 450 Toland Street, San Francisco, CA 94124

[Image description: The image shows a screenshot of a mapped area around the Central Shops building at 450 Toland Street.]

Incident Category	Number of SFPD Incidents	Percent
	4	0.033333
Arson	1	0.008333
Assault	5	0.041667
Burglary	5	0.041667
Disorderly Conduct	4	0.033333
Fire Report	1	0.008333
Fraud	3	0.025
Larceny Theft	52	0.433333
Malicious Mischief	5	0.041667
Miscellaneous Investigation	2	0.016667
Missing Person	1	0.008333
Motor Vehicle Theft	9	0.075
Non-Criminal	2	0.016667
Other Miscellaneous	9	0.075
Other Offenses	1	0.008333
Recovered Vehicle	2	0.016667

Robbery	3	0.025
Stolen Property	1	0.008333
Suspicious Occ	3	0.025
Traffic Violation Arrest	1	0.008333
Vandalism	1	0.008333
Warrant	1	0.008333
Weapons Offense	4	0.033333

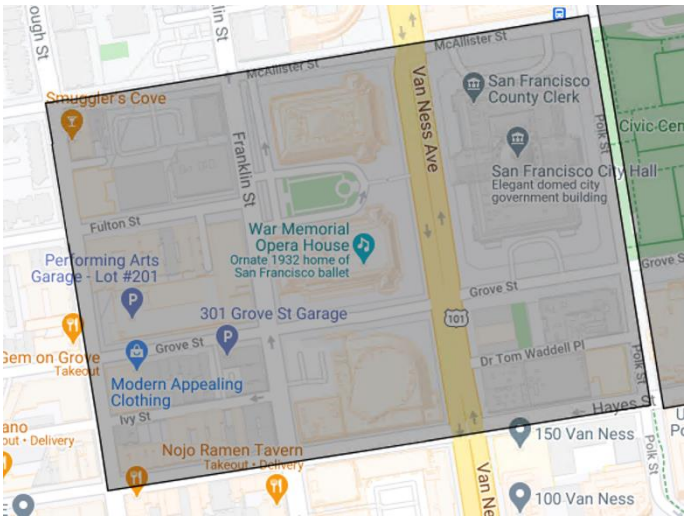
- Central Shop, 555 Selby Street, San Francisco, CA 94124



[Image description: The image shows a screenshot of a mapped area around the Central Shops building at 555 Selby.]

Incident Category	Number of SFPD Incidents	Percent
Arson	2	0.060606
Assault	3	0.090909
Burglary	2	0.060606
Fire Report	1	0.030303
Larceny Theft	7	0.212121
Malicious Mischief	2	0.060606
Miscellaneous Investigation	1	0.030303
Missing Person	1	0.030303
Motor Vehicle Theft	3	0.090909
Non-Criminal	3	0.090909
Other Miscellaneous	4	0.121212
Other Offenses	1	0.030303
Recovered Vehicle	1	0.030303
Stolen Property	1	0.030303
Weapons Offense	1	0.030303

- City Hall, 1 Dr Carlton B Goodlett Pl, San Francisco, CA 94102

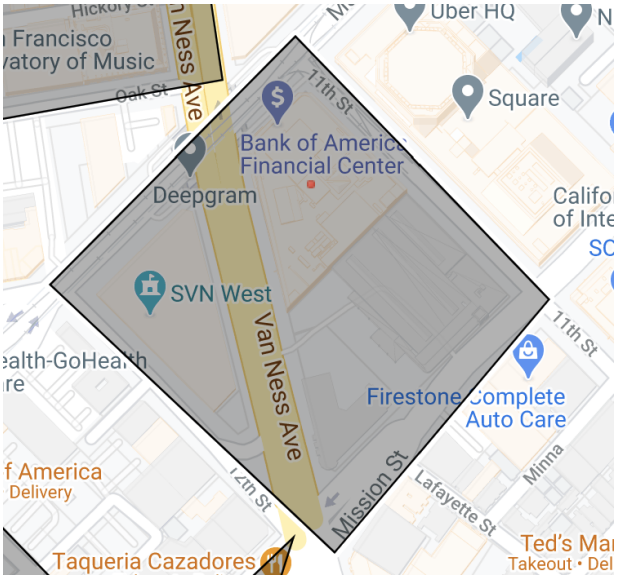


[Image description: The image shows a screenshot of a mapped area around the San Francisco City Hall building.]

Incident Category	Number of SFPD Incidents	Percent
Arson	1	0.001701
Assault	29	0.04932
Burglary	65	0.110544
Courtesy Report	1	0.001701
Disorderly Conduct	2	0.003401
Drug Offense	5	0.008503
Embezzlement	1	0.001701
Fire Report	1	0.001701
Forgery And Counterfeiting	1	0.001701
Fraud	10	0.017007
Larceny Theft	250	0.42517
Liquor Laws	1	0.001701
Lost Property	15	0.02551
Malicious Mischief	67	0.113946
Miscellaneous Investigation	3	0.005102
Missing Person	3	0.005102
Motor Vehicle Theft	30	0.05102
Non-Criminal	15	0.02551
Offences Against The Family And Children	7	0.011905
Other	8	0.013605
Other Miscellaneous	32	0.054422
Other Offenses	2	0.003401
Recovered Vehicle	1	0.001701
Robbery	5	0.008503
Stolen Property	3	0.005102

Suspicious Occ	4	0.006803
Traffic Violation Arrest	5	0.008503
Vandalism	2	0.003401
Vehicle Impounded	1	0.001701
Warrant	10	0.017007
Weapons Offense	7	0.011905

- 49 South Van Ness Avenue, San Francisco, CA 94103

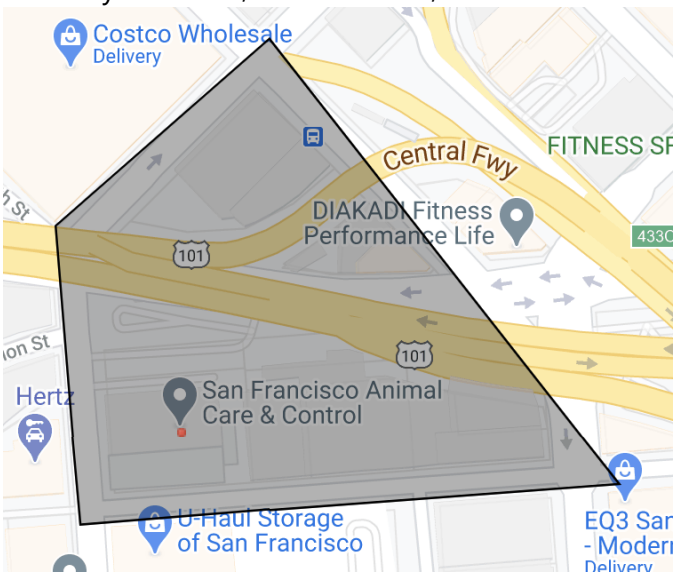


[Image description: The image shows a screenshot of a mapped area around the 49 Van Ness Avenue building.]

Incident Category	Number of SFPD Incidents	Percent
Arson	2	0.011561
Assault	23	0.132948
Burglary	15	0.086705
Disorderly Conduct	7	0.040462
Drug Offense	2	0.011561
Family Offense	1	0.00578
Fire Report	2	0.011561
Forgery And Counterfeiting	1	0.00578
Fraud	4	0.023121
Larceny Theft	22	0.127168
Lost Property	4	0.023121
Malicious Mischief	11	0.063584
Missing Person	1	0.00578
Motor Vehicle Theft	3	0.017341
Non-Criminal	31	0.179191

Offences Against The Family And Children	4	0.023121
Other	2	0.011561
Other Miscellaneous	13	0.075145
Other Offenses	2	0.011561
Rape	1	0.00578
Robbery	2	0.011561
Stolen Property	1	0.00578
Suspicious Occ	7	0.040462
Traffic Violation Arrest	4	0.023121
Warrant	7	0.040462
Weapons Offense	1	0.00578

- 1419 Bryant Street, San Francisco, CA 94103

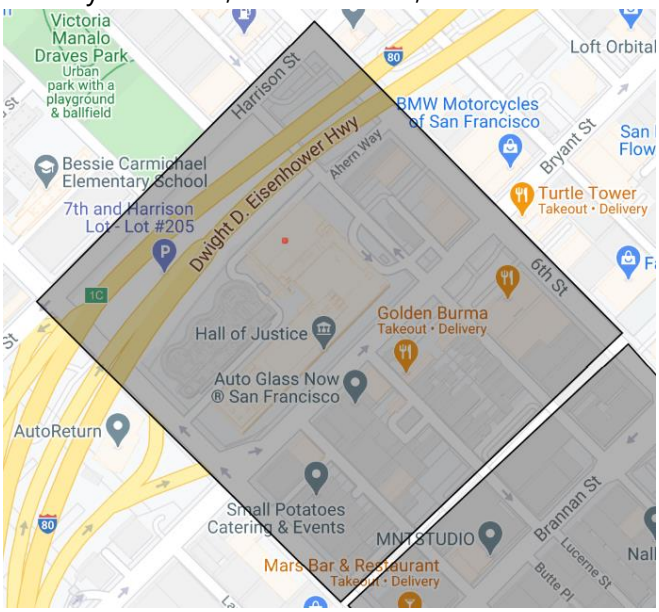


[Image description: The image shows a screenshot of a mapped area around the 1419 Bryant Street building, currently under construction.]

Incident Category	Number of SFPD Incidents	Percent
Assault	5	0.036765
Burglary	6	0.044118
Courtesy Report	1	0.007353
Disorderly Conduct	1	0.007353
Drug Offense	6	0.044118
Embezzlement	14	0.102941
Fire Report	2	0.014706
Forgery And Counterfeiting	2	0.014706
Fraud	3	0.022059
Larceny Theft	19	0.139706

Malicious Mischief	6	0.044118
Miscellaneous Investigation	2	0.014706
Missing Person	1	0.007353
Motor Vehicle Theft	28	0.205882
Non-Criminal	2	0.014706
Other Miscellaneous	24	0.176471
Other Offenses	2	0.014706
Recovered Vehicle	1	0.007353
Robbery	1	0.007353
Sex Offense	1	0.007353
Suspicious Occ	1	0.007353
Traffic Violation Arrest	2	0.014706
Vandalism	1	0.007353
Warrant	5	0.036765

- 850 Bryant Street, San Francisco, CA 94103



[Image description: The image shows a screenshot of a mapped area around the 850 Bryant Street building.]

Incident Category	Number of SFPD Incidents	Percent
Assault	8	0.019093
Burglary	4	0.009547
Case Closure	15	0.0358
Courtesy Report	5	0.011933
Disorderly Conduct	6	0.01432
Drug Offense	4	0.009547
Embezzlement	2	0.004773

Fire Report	1	0.002387
Forgery And Counterfeiting	7	0.016706
Fraud	11	0.026253
Human Trafficking, Commercial Sex Acts	1	0.002387
Larceny Theft	36	0.085919
Lost Property	7	0.016706
Malicious Mischief	23	0.054893
Miscellaneous Investigation	10	0.023866
Missing Person	8	0.019093
Motor Vehicle Theft	9	0.02148
Non-Criminal	14	0.033413
Offences Against The Family And Children	8	0.019093
Other Miscellaneous	16	0.038186
Robbery	2	0.004773
Sex Offense	135	0.322196
Suspicious	2	0.004773
Suspicious Occ	18	0.042959
Traffic Violation Arrest	2	0.004773
Vandalism	1	0.002387
Warrant	59	0.140811
Weapons Carrying Etc	3	0.00716
Weapons Offense	2	0.004773

Information on crime statistics in 2020 is provided by the San Francisco Police Department. Statistics are taken from a 1-block radius around the location of cameras. All information obtained through the San Francisco Open Data Portal: https://datasf.org/opendata/

In addition, the department maintains an internal incident log, which is available on request.

Surveillance Impact Report

Department of Technology
Security Cameras

As required by San Francisco Administrative Code, Section 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 surveillance cameras.

DESCRIPTION OF THE TECHNOLOGY

The Department of Technology's mission is "to provide innovative, reliable, and secure business solutions that support and empower City agencies and departments in their delivery of high-quality government services for the public."

In line with its mission, the Department shall use security cameras only for the following authorized purposes:

Authorized Use(s):

1. Live monitoring.
2. Recording of video and images in the event of an incident.
3. Reviewing camera footage.
4. Providing video footage/images to law enforcement or other authorized persons following an incident.

Prohibited use cases include any uses not stated in the Authorized Use Case section.

Further, processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, gender, gender identity, disability status, or an individual person's sex life or sexual orientation, and the processing of genetic data and/or biometric data for the purpose of uniquely identifying an individual person shall be prohibited.

Department technology may be deployed in the following locations, based on use case:

The Department of Technology's "Critical Infrastructure Cameras" or "CICs" are located at the City's public safety radio sites and DT's Public Safety offices at 200 Paul St.

Surveillance Oversight Review Dates

COIT Review: March 18, 2021
Board of Supervisors Review: TBD

Technology Details

The following is a product description:

Avigilon Control Center software is video management software that optimizes the way security professionals manage and interact with high-definition video. It captures and stores HD video, while managing bandwidth and storage using the vendor's High Definition Stream Management (HDSM) technology.

A. How It Works

The CICs are used to monitor public safety radio sites for suspected theft or vandalism of a system upon which San Francisco residents depend for emergency service delivery.].

Data collected or processed by security cameras will not be handled or stored by an outside provider or third-party vendor on an ongoing basis. The Department will remain the sole Custodian of Record.

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 security cameras has the following benefits for the residents of the City and County of San Francisco:

▪	Education	
▪	Community Development	
X	Health	Protect safety of staff, patrons, and facilities while promoting an open and welcoming environment.
▪	Environment	
X	Criminal Justice	Review video footage after a security incident; provide video evidence to law enforcement or the public upon request by formal process, order, or subpoena.
▪	Jobs	

- Housing
- Other

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:

The use of CICs may result in dignity loss, discrimination or loss of liberty. The quality of the video captured through the CICs may vary in quality due to lighting, motion or other factors. Poor quality video may lead to mis-identification. Conversely, the video may not correctly convey intent and viewers may interpret actions captured as threatening or menacing which may have a more benign interpretation. For example, the CICs may capture a person approaching a facility with a brick and assume they intend to cause physical damage to the property when there may be an alternative explanation. That person may be correctly identified as an employee or member of the public, but subsequently subjected to investigation and possibly arrest.

The Department of Technology strives to mitigate all potential civil rights impacts through responsible technology and associated data use policies and procedures, and intends to use CICs and their associated data exclusively for aforementioned authorized uses cases. All other uses, including surveillance of San Francisco residents or groups, are expressly prohibited.

Specifically, DT applies the following safeguards:

- Administrative: the video can only be accessed by Data can only be accessed by 7362 and 7368 Technicians.
- Technical: the CIC video is on a closed system not connected to other City data networks.
- Physical: stored CIC video can only be accessed at DT's offices at 200 Paul Ave or 1011 Turk Street.
- The CICs cannot be used to monitor anything other than City property.
- Stored video is only accessed if DT staff identify an incident, typically a break-in resulting in vandalism or loss of property.
- The CIC system records video of the City's public safety radio sites. Currently, the video is stored for 7 days prior to deletion. In the event of an incident of theft of vandalism, DT staff will review the recorded video to determine if it has captured the incident. (DT understands that it may have to store recorded video for a longer period, we will seek to store video for the minimum possible duration.)
- DT intends to continue using operating the CIC system as severely limited, closed nature of system.

To protect camera from potential breach, misuse or abuse that may result in civil rights impacts, data is maintained on secure, department-owned servers. Only persons authorized to utilize the raw data may access the information and are required to maintain records of access by completing the community security cameras data access log described in section 3.23. Only data that has been edited to remove PII will be shared and stored on servers, and sharing will only occur with partner CCSF

agencies for whom the Department of Technology has been contracted to purchase, install and maintain the cameras.

C. Fiscal Analysis of Costs and Benefits

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

Benefit		Description
X	Financial Savings	Department Security Camera Systems will save on building or patrol officers.
X	Time Savings	Department Security Camera Systems will run 24/7, thus eliminating building or patrol officer supervision
X	Staff Safety	Security cameras help identify violations of Department Patron Code of Conduct and provide assurance that staff safety is emphasized and will be protected at their place of employment.
X	Data Quality	Security cameras run 24/7/365 so full-time staffing is not required to subsequently review footage of security incidents. Data resolution can be set by level and is currently set to high resolution.

Number of FTE (new & existing)	0.5	
Classification	7362 Communications System Technician 7368 Senior Communications System Technician 8234 Fire Alarm Dispatchers 8236 Chief Fire Alarm Dispatchers	
	Annual Cost	***One-Time Cost***
Software		$23,000
Hardware/Equipment		$400,000
Professional Services		
Training		
Other		
Total Cost		*$423,000*

DT funds its use and maintenance of the CICs through its annual operating budget. The one-time costs for hardware and software represent historic costs, not costs incurred in the recent past or anticipated in the current budget cycle. Individual items, such as cameras, are replaced when they fail through annual operating budget.

COMPARISON TO OTHER JURISDICTIONS

Camera systems similar to those used by the CICs are currently utilized by other governmental entities for similar purposes.

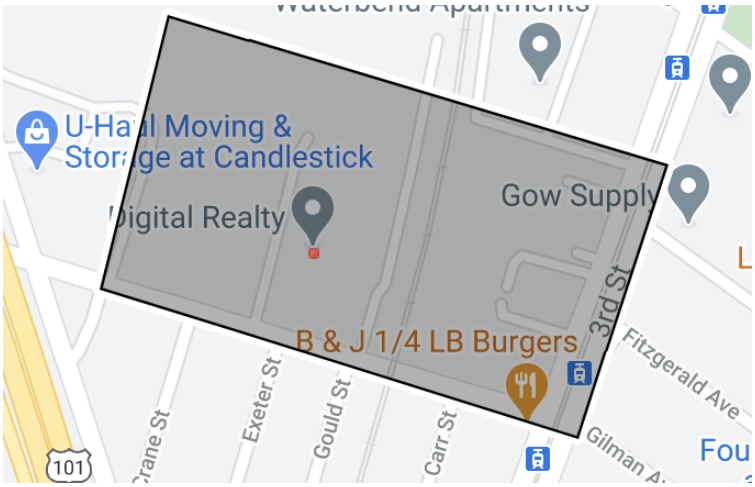
Appendix A: Crime Statistics

Department: Technology Department

Section 19B requires each department in their Surveillance Impact Report to respond to the following question if applicable, "the general location(s) [of the surveillance technology] may be deployed and crime statistics for any location(s)."

The Technology Department operates a total of 87 Security Cameras at the following locations:

- 200 Paul Avenue, San Francisco, CA 94124

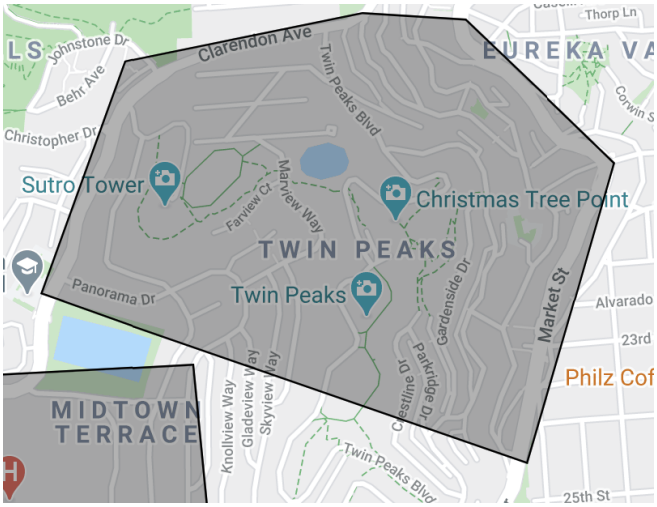


[Image description: The image shows a screenshot of a mapped area around the 200 Paul Avenue building.]

Incident Category	Number of SFPD Incidents	Percent
Assault	14	0.117647
Burglary	5	0.042017
Disorderly Conduct	3	0.02521
Embezzlement	3	0.02521
Fire Report	1	0.008403
Fraud	2	0.016807
Larceny Theft	11	0.092437
Lost Property	2	0.016807
Malicious Mischief	6	0.05042
Miscellaneous Investigation	2	0.016807
Missing Person	2	0.016807
Motor Vehicle Theft	28	0.235294
Non-Criminal	6	0.05042
Other Miscellaneous	10	0.084034
Recovered Vehicle	3	0.02521

Robbery	4	0.033613
Suspicious Occ	4	0.033613
Traffic Collision	1	0.008403
Traffic Violation Arrest	2	0.016807
Warrant	3	0.02521
Weapons Carrying Etc	4	0.033613
Weapons Offense	3	0.02521

- Twin Peaks Radio Tower



[Image description: The image shows a screenshot of a mapped area around the Twin Peaks Radio Tower site.]

Incident Category	Number of SFPD Incidents	Percent
Assault	6	0.010204
Burglary	41	0.069728
Disorderly Conduct	1	0.001701
Drug Offense	3	0.005102
Forgery And Counterfeiting	5	0.008503
Fraud	13	0.022109
Larceny Theft	354	0.602041
Lost Property	2	0.003401
Malicious Mischief	43	0.073129
Miscellaneous Investigation	2	0.003401
Missing Person	3	0.005102
Motor Vehicle Theft	30	0.05102
Non-Criminal	16	0.027211
Offences Against The Family And Children	5	0.008503
Other	5	0.008503
Other Miscellaneous	25	0.042517

Other Offenses	1	0.001701
Recovered Vehicle	1	0.001701
Stolen Property	2	0.003401
Suspicious Occ	8	0.013605
Traffic Violation Arrest	8	0.013605
Vandalism	3	0.005102
Warrant	7	0.011905
Weapons Carrying Etc	3	0.005102
Weapons Offense	1	0.001701

Information on crime statistics in 2020 in this area is provided by the San Francisco Police Department. Statistics are taken from a 1-block radius around the location of cameras. All information is obtained through the San Francisco Open Data Portal: https://datasf.org/opendata/

In addition, the department maintains an internal incident log which is available on request.

Surveillance Impact Report

Department of Emergency Management
Security Cameras

As required by San Francisco Administrative Code, Section 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 surveillance cameras.

DESCRIPTION OF THE TECHNOLOGY

The San Francisco Department of Emergency Management (DEM) leads the City in planning, preparedness, communication, response, and recovery for daily emergencies, large scale citywide events, and major disasters. DEM is the vital link in emergency communication between the public and first responders, and provides key coordination and leadership to City departments, stakeholders, residents, and visitors.

In line with its mission, the Department shall use security cameras only for the following authorized purposes:

Authorized Use(s):

1. Live monitoring.
2. Recording of video and images in the event of an incident.
3. Reviewing camera footage.
4. Providing video footage/images to law enforcement or other authorized persons following an incident.

Prohibited use cases include any uses not stated in the Authorized Use Case section.

Further, processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, gender, gender identity, disability status, or an individual person's sex life or sexual orientation, and the processing of genetic data and/or biometric data for the purpose of uniquely identifying an individual person shall be prohibited.

Department technology may be deployed in the following locations, based on use case:

- 1011 Turk St – Department of Emergency Management Headquarters

Surveillance Oversight Review Dates

COIT Review: March 18, 2021
Board of Supervisors Review: TBD

Technology Details

The following is a product description:

DEM Camera system provides building perimeter visual security for the Combined Emergency Communications Center (CECC) building at 1011 Turk St. The CECC is a critical building for the City's public safety operations, housing both the 9-1-1 Center for the City and County, as well as the Citywide Emergency Operations Center and the Watch Center. The building has 24-hour security, offered by the Sheriff's Department, and it is surrounded on all 4 sides by public parks. There is currently a total of 28 cameras which most of them are fix point focus and 6 pan-tilt-zoom (PTZ) cameras. The video is recorded across two on-premise video servers converting the analog video to digital file format utilizing video management software from Exacqvision. The system current has a retention period of about 21 days to a month. The approximate age of the camera system is at least 7 years old.

The system is primarily used by Sheriff staffed at CECC to monitor for surrounding safety for the occupants of this building and overall perimeter security. There many times the footage of the security camera system is used as evidence to apprehend suspects on criminal event within the view of the cameras within our system. DEM maintains a policy for requesting access to the video camera footage.

Data collected or processed by security cameras will not be handled or stored by an outside provider or third-party vendor on an ongoing basis. The Department will remain the sole Custodian of Record.

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 security cameras has the following benefits for the residents of the City and County of San Francisco:

- Education
- Community Development

X	Health	Protect safety of staff, patrons, and facilities while promoting an open and welcoming environment.

- Environment

X	Criminal Justice	Review video footage after a security incident; provide video evidence to law enforcement or the public upon request by formal process, order, or subpoena. Deter Crime

- Jobs
- Housing
- Other

B. *Civil Rights Impacts and Safeguards*

The Department has considered the potential impacts on civil liberties and has identified the technical, administrative, and physical protections as mitigating measures. The 2 potential impacts that were identified are Dignity Loss and Loss of Liberty.

An individual could suffer dignity loss and experience emotional distress if cameras capture behaviors, appearances, or circumstances by which they might feel humiliated. Examples include individuals ridiculing appearance or behavior, and unlawfully sharing this with other individuals. Risks for loss of dignity are reduced by restricting access to live views and limiting access of trained Security staff. Further, DEM has developed a Security Video Access Policy that is posted on the Intranet, and available to all staff. It covers how to request video footage from the garage, lobby, and exterior cameras. Additionally, the recorded footage has limited retention period, of less than 1 month. Audio is not recorded or enabled.

Loss of liberty could potentially occur if a person were to be misidentified as the perpetrator of a crime or other incident, making them subject to wrongful arrest. An innocent person might be similar in appearance to someone who committed an offense. Surveillance images could reinforce other circumstantial evidence tying the wrong person to a criminal incident. As an example, someone might be wearing clothing like clothing worn by someone seen leaving an office where a theft had just occurred. Loss of liberty risks due to misidentification of a subject in surveillance video is mitigated by restricting access to live views and recorded footage to a limited number of trained personnel.

DEM believes that the following items (Dignity Loss, Discrimination, Economic Loss, Autonomy Loss, Physical or Loss of Trust) are not a potential impact on civil liberties and rights due to the nature of the surveillance system.

C. Fiscal Analysis of Costs and Benefits

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

Benefit		Description
X	Financial Savings	Department Security Camera Systems will save on building or patrol officers.
X	Time Savings	Department Security Camera Systems will run 24/7, thus eliminating building or patrol officer supervision
X	Staff Safety	Security cameras help identify violations of Department Patron Code of Conduct and provide assurance that staff safety is emphasized and will be protected at their place of employment.
X	Data Quality	Security cameras run 24/7/365 so full-time staffing is not required to subsequently review footage of security incidents. Data resolution can be set by level and is currently set to high resolution.

Number of FTE (new & existing)	Estimated at .1 FTE	
Classification	Existing FTE: 1042, 1094	
	Annual Cost	***One-Time Cost***
Software		
Hardware/Equipment		
Professional Services		
Training		
Other		
Total Cost	*$15,000 (est. based on current system)*	*$200-$800K*

The Department funds its use and maintenance of the surveillance technology through

- City General Fund

COMPARISON TO OTHER JURISDICTIONS

Video Cameras are currently utilized by other City Department and other governmental entities for similar purposes.

Appendix A: Crime Statistics

Department: Emergency Management

Section 19B requires each department in their Surveillance Impact Report to respond to the following question if applicable, "the general location(s) [of the surveillance technology] may be deployed and crime statistics for any location(s)."

The Emergency Management Department operates a total of 26 Security Cameras at the following location:

- 1011 Turk Street, San Francisco, CA 94102

[Image description: The image shows a screenshot of a mapped area around the Emergency Management building.]

Incident Category	Number of SFPD Incidents	Percent
Arson	2	0.008511
Assault	14	0.059574
Burglary	11	0.046809
Disorderly Conduct	5	0.021277
Drug Offense	9	0.038298
Family Offense	2	0.008511
Fraud	4	0.017021
Larceny Theft	52	0.221277
Lost Property	3	0.012766
Malicious Mischief	17	0.07234
Miscellaneous Investigation	2	0.008511
Missing Person	2	0.008511

Motor Vehicle Theft	17	0.07234
Non-Criminal	16	0.068085
Offences Against The Family And Children	14	0.059574
Other	8	0.034043
Other Miscellaneous	24	0.102128
Other Offenses	1	0.004255
Recovered Vehicle	1	0.004255
Robbery	4	0.017021
Stolen Property	1	0.004255
Suspicious Occ	5	0.021277
Traffic Collision	1	0.004255
Traffic Violation Arrest	5	0.021277
Warrant	13	0.055319
Weapons Carrying Etc	1	0.004255
Weapons Offense	1	0.004255

Information on crime statistics in 2020 in this area is provided by the San Francisco Police Department. Statistics are taken from a 1-block radius around the location of cameras. All information is obtained through the San Francisco Open Data Portal: https://datasf.org/opendata/

In addition, the department maintains an internal incident log which is available on request.

Surveillance Impact Report

Fire Department
Security Cameras

As required by San Francisco Administrative Code, Section 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 surveillance cameras.

DESCRIPTION OF THE TECHNOLOGY

The Mission of the Fire Department is to protect the lives and property of the people of San Francisco from fires, natural disasters, and hazardous materials incidents; to save lives by providing emergency medical services; to prevent fires through prevention and education programs; and to provide a work environment that values health, wellness and cultural diversity and is free of harassment and discrimination.

In line with its mission, the Department shall use security cameras only for the following authorized purposes:

Authorized Use(s):

1. Live monitoring.
2. Recording of video and images in the event of an incident.
3. Reviewing camera footage.
4. Providing video footage/images to law enforcement or other authorized persons following an incident.

Prohibited use cases include any uses not stated in the Authorized Use Case section.

Further, processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, gender, gender identity, disability status, or an individual person's sex life or sexual orientation, and the processing of genetic data and/or biometric data for the purpose of uniquely identifying an individual person shall be prohibited.

Department technology may be deployed in the following locations, based on use case:

- Fire Department Bureau of Equipment/Ambulance Deployment Facility
- Fire Department Division of Training

Surveillance Oversight Review Dates

COIT Review: March 18, 2021
Board of Supervisors Review: TBD

Technology Details

The following is a product description:

Security Cameras are installed at Department facilities. The surveillance cameras are used to protect against theft or vandalism of the Department's property at a number of locations. They are necessary to ensure that critical functions are secure and operational at all times. Currently the Department has installed Illustra Pro Series 2MP mini-dome outdoor camera.

A. How It Works

To function, the camera system has been installed and fences and walls of the Department's property, The camera system records video of some of the Department's critical facilities. The video is stored, and in the event of an incident of theft of vandalism, staff will review the recorded video to determine if it has captured the incident.

Data collected or processed by security cameras will not be handled or stored by an outside provider or third-party vendor on an ongoing basis. The Department will remain the sole Custodian of Record.

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 security cameras has the following benefits for the residents of the City and County of San Francisco:

▪	Education	
▪	Community Development	
X	Health	Protect safety of staff, patrons, and facilities while promoting an open and welcoming environment.
▪	Environment	

X	Criminal Justice	Review video footage after a security incident; provide video evidence to law enforcement or the public upon request by formal process, order, or subpoena.

- Jobs
- Housing
- Other

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:

The San Francisco Fire Department strives to mitigate all potential civil rights impacts through responsible technology and associated data use policies and procedures. All other uses, including surveillance of San Francisco residents or groups, are expressly prohibited.

To protect data from potential breach, misuse or abuse that may result in civil rights impacts, data is maintained on secure, department-owned servers as well as secure cloud environments. Only persons authorized to utilize the raw data may access the information.

Data will not be collected, disseminated or retained solely for the purpose of monitoring activities protected by the U.S. Constitution, such as the First Amendment's protections of religion, speech, press, assembly, and redress of grievances (e.g., protests, demonstrations).

Collection, use, dissemination, or retention of data should not be based solely on individual characteristics (e.g., race, ethnicity, national origin, sexual orientation, gender identity, religion, age, or gender), which is a violation of the law.

C. Fiscal Analysis of Costs and Benefits

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

Benefit		**Description**
X	Financial Savings	Department Security Camera Systems will save on building or patrol officers.
X	Time Savings	Department Security Camera Systems will run 24/7, thus eliminating building or patrol officer supervision
X	Staff Safety	Security cameras help identify violations of Department Patron Code of Conduct and provide assurance that staff safety is emphasized and will be protected at their place of employment.

X	Data Quality	Security cameras run 24/7/365 so full-time staffing is not required to subsequently review footage of security incidents. Data resolution can be set by level and is currently set to high resolution.

Number of FTE (new & existing)	No FTEs	
Classification	N/A	
	Annual Cost	***One-Time Cost***
Software	***$0***	$0
Hardware/Equipment	*$0*	$5,198.17
Professional Services	*$0*	$0
Training	*$0*	*$0*
Other (installation)	$0	$12,763.00
Total Cost	***$0***	***$17,961.17***

The Department funds its use and maintenance of the surveillance technology through its general fund operating budget.

COMPARISON TO OTHER JURISDICTIONS

Security cameras are currently utilized by other governmental entities for similar purposes.

APPENDIX A: Crime Statistics

Department: Fire Department

Section 19B requires each department in their Surveillance Impact Report to respond to the following question if applicable, "the general location(s) [of the surveillance technology] may be deployed and crime statistics for any location(s)."

The Fire Department operates a total of 5 Security Cameras at the following locations:

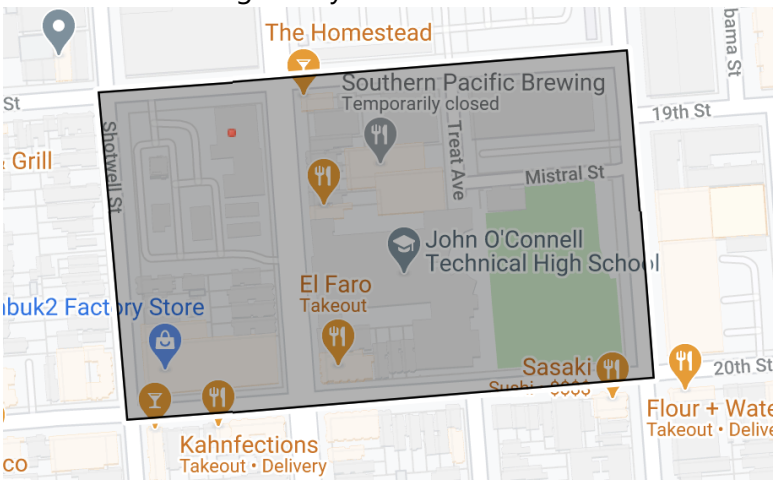
- 1415 Evans Avenue, San Francisco, CA

[Image description: The image shows a screenshot of the Fire Department Station 49 building.]

Incident Category	Number of SFPD Incidents	Percent
Assault	1	0.027027
Burglary	5	0.135135
Courtesy Report	1	0.027027
Disorderly Conduct	1	0.027027
Forgery And Counterfeiting	1	0.027027
Fraud	1	0.027027
Larceny Theft	6	0.162162
Lost Property	4	0.108108
Malicious Mischief	2	0.054054
Motor Vehicle Theft	3	0.081081
Non-Criminal	2	0.054054
Other Miscellaneous	3	0.081081
Recovered Vehicle	1	0.027027
Suspicious Occ	1	0.027027
Traffic Violation Arrest	1	0.027027

Warrant	2	0.054054
Weapons Offense	2	0.054054

- Division of Training facility at 19th Street and Folsom Street



[Image description: The image shows a screenshot of a mapped area around the Fire Department Division of Training building.]

Incident Category	Number of SFPD Incidents	Percent
	1	0.005236
Assault	6	0.031414
Burglary	14	0.073298
Disorderly Conduct	4	0.020942
Drug Offense	4	0.020942
Fraud	4	0.020942
Larceny Theft	41	0.21466
Lost Property	2	0.010471
Malicious Mischief	12	0.062827
Miscellaneous Investigation	1	0.005236
Missing Person	1	0.005236
Motor Vehicle Theft	16	0.08377
Non-Criminal	7	0.036649
Other	1	0.005236
Other Miscellaneous	28	0.146597
Other Offenses	2	0.010471
Prostitution	9	0.04712
Recovered Vehicle	1	0.005236
Robbery	2	0.010471
Suspicious Occ	6	0.031414
Traffic Violation Arrest	10	0.052356

Vandalism	2	0.010471
Vehicle Impounded	2	0.010471
Warrant	11	0.057592
Weapons Carrying Etc	3	0.015707
Weapons Offense	1	0.005236

Information on crime statistics in this are is provided by the San Francisco Police Department. All information obtained through the San Francisco Open Data Portal: https://datasf.org/opendata/

In addition, the department maintains an internal incident log which is available upon request.

Surveillance Impact Report

Homelessness and Supportive Housing
Surveillance Cameras

As required by San Francisco Administrative Code, Section 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 surveillance cameras.

DESCRIPTION OF THE TECHNOLOGY

The Department's mission is through the provision of coordinated, compassionate, and high-quality services, the Department of Homelessness and Supportive Housing strives to make homelessness in San Francisco rare, brief, and one time.

In line with its mission, the Department uses surveillance cameras to:

1. provide for shelter & navigation center site staff to cover the vulnerable access points and common areas for the safety and security of site staff and our clients;
2. augment security staff by providing additional camera monitoring in the common area for the safety and security of our staff at 440 Turk Street location;

Homelessness and Supportive Housing shall use surveillance cameras only for the following authorized purposes:

1. Live monitoring.
2. Recording of video and images.
3. Reviewing camera footage in the event of an incident.
4. Providing video footage/images to law enforcement or other authorized persons following an incident or upon request.

Prohibited use cases include any uses not stated in the Authorized Use Case section.

Further, processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data 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.

Surveillance Oversight Review Dates
COIT Review: March 18, 2021
Board of Supervisors Review: TBD

Technology Details

Homelessness and Supportive Housing surveillance cameras are located in public areas of all floors at 440 Turk Street Headquarters building.

The following is a product description of the 440 Turk Street Surveillance Camera System:

Cameras: 2x Samsung PNM-7000VD, 18x Samsung XNV-6080R

Server: exacqVision

A. How It Works
The technology's primary functions are to provide live views and record video footage to a dedicated, secure server. The system is comprised of multiple cameras connected by data cables and infrastructure to the server. The footage is recorded on the server and stored for a limited amount of time.

Data collected or processed by the 440 Turk Street Surveillance Camera System will not be handled or stored by an outside provider or third-party vendor on an ongoing basis. The Department will remain the sole Custodian of Record.

Below technology are being used at shelter:

Different site might have different type of DVR equipment but a typical DVR equipment would be Honeywell – HRDP16D1T0-R connected to various security cameras

A. How It Works
The technology's primary functions are to provide live views and record video footage to a dedicated, secure server. The system is comprised of multiple cameras connected by data cables and infrastructure to the server. The footage is recorded on the server and stored for a limited amount of time.

As it is necessary for their operations, data collected or processed by the shelter & navigation center Surveillance Camera System will be accessible to our shelter and navigation center contractors on a limited basis. The Department will remain the sole Custodian of Record.

Security camera system is programmed to overwrite oldest images once the hard drive reaches 90% capacity. Depending on the size of the DVR hard drive, video images data are held between 1 week to 1 month.

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 [Technology name] has the following benefits for the residents of the City and County of San Francisco:

☐	Education	
☐	Community Development	
☐	Health	
☐	Environment	
☑	Criminal Justice	May provide evidence for law enforcement criminal investigations.
☐	Jobs	
☐	Housing	
☑	Other	Public Safety - Assists security officers investigating Code of Conduct violations and/or criminal acts at 440 Turk HQ building and/or shelters - Provides a mechanism to augment foot patrols, prevent criminal acts, and assist anyone requiring emergency help.

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:

Department of Homelessness and Supportive Housing believes the Surveillance Camera System poses potential risks to civil liberties in respect to dignity loss and loss of liberty.

An individual could be embarrassed or experience emotional distress if cameras capture behaviors, appearances, or circumstances by which they might feel humiliated. Examples include views of someone exhibiting an emotional outburst, a person's clothing or hair being disheveled, or someone having their physique ridiculed or leered at. Risks for loss of dignity are reduced by restricting access to live views, as well as recorded footage, to a limited number of Facilities staff. For cameras at our shelter and navigation center, access is limited to a small number of shelter and navigation center staff on an as needed basis. In addition, the cameras do not pan, tilt or zoom, thus removing possible temptation for system operators to use those features to follow or enhance views of individuals. Audio is also not recorded or enabled.

Loss of liberty could potentially occur if a person were to be misidentified as the perpetrator of a crime or other incident, making them subject to wrongful arrest. An innocent person might be similar in appearance to someone who committed an offense. Surveillance images could reinforce other circumstantial evidence tying the wrong person to a criminal incident. As an example, someone might be wearing clothing like clothing worn by someone seen leaving an office where a theft had just occurred. Loss of liberty risks due to misidentification of a subject in surveillance video is mitigated by restricting access to live views and recorded footage to a limited number of trained personnel.

C. Fiscal Analysis of Costs and Benefits

The Department's use of Surveillance Camera system yields the following business and operations benefits:

- Financial savings: with security camera system, site staff is able to manage the main entry and still be able to effectively cover the vulnerable access points. Essentially, minimize the need to hire 50 security officers (see response to question 1.4).
- Time savings: deploying a security camera system can provide time saving over the additional scope of work for security contract, hiring and managing additional security officers
- Staff safety: security camera system allows staff to be proactive rather than reactive in term of conflict de-escalation

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

Number of FTE (new & existing)	4 existing employees Total expected staff hours (all): 15 hrs/mo
Classification	(7334) - Stationary Engineers
Total Salary & Fringe	*60 hrs x 12 months x $155/hr:* ***$111,600/yr***
Software	Included
Hardware/Equipment	$60,000 one-time cost ($5,000 x 12 site)
Professional Services	0
Training	*Internal staff training – no additional cost*
Other	
Total Cost	***$171,600 per year***

The Department funds its use and maintenance of the surveillance technology through Annual Operating Budget. Staff time used to inspect security camera systems will be charged as any other labor costs, to overhead or General Fund.

Equipment: This is a one-time cost as equipment had been purchased and deployed. Any future replacement equipment will be part of the department's ongoing equipment budget request.

COMPARISON TO OTHER JURISDICTIONS

Surveillance Camera Technologies like the Veterans Building Surveillance Camera System are currently utilized by other governmental entities for similar purposes.

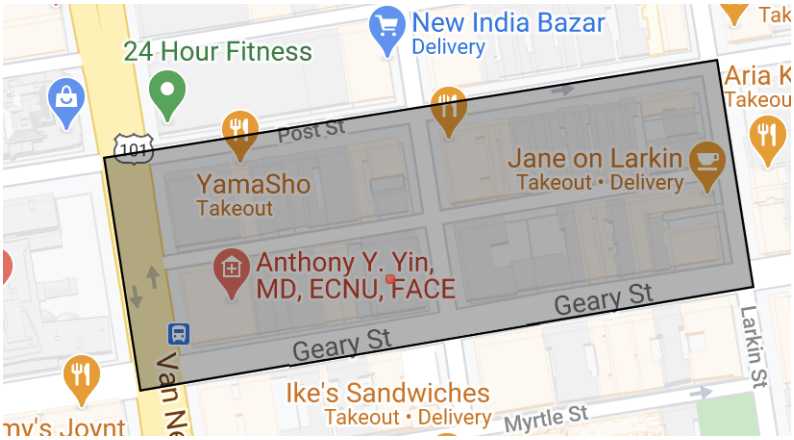
Appendix A: Surveillance Impact Report: Crime Statistics

Department: Homelessness and Supportive Housing

Section 19B requires each department in their Surveillance Impact Report to respond to the following question if applicable, "the general location(s) [of the surveillance technology] may be deployed and crime statistics for any location(s)."

The Homelessness and Supportive Housing Department operates a total of 244 Security Cameras at the following locations:

- Next Door Shelter, 1001 Polk Street, San Francisco, CA 94109



[Image description: The image shows a screenshot of a mapped area around the Next Door Shelter.]

Incident Category	Number of SFPD Incidents	Percent
	5	0.008913
Assault	72	0.128342
Burglary	20	0.035651
Courtesy Report	2	0.003565
Disorderly Conduct	8	0.01426
Drug Offense	26	0.046346
Embezzlement	1	0.001783
Family Offense	1	0.001783
Forgery And Counterfeiting	1	0.001783
Fraud	13	0.023173
Human Trafficking (A), Commercial Sex Acts	1	0.001783
Larceny Theft	93	0.165775
Lost Property	12	0.02139
Malicious Mischief	36	0.064171
Miscellaneous Investigation	13	0.023173
Missing Person	15	0.026738

Motor Vehicle Theft	27	0.048128
Non-Criminal	47	0.083779
Offences Against The Family And Children	25	0.044563
Other	8	0.01426
Other Miscellaneous	44	0.078431
Other Offenses	6	0.010695
Recovered Vehicle	1	0.001783
Robbery	13	0.023173
Sex Offense	1	0.001783
Stolen Property	2	0.003565
Suicide	1	0.001783
Suspicious Occ	23	0.040998
Traffic Collision	1	0.001783
Traffic Violation Arrest	10	0.017825
Vandalism	2	0.003565
Warrant	22	0.039216
Weapons Carrying Etc	5	0.008913
Weapons Offense	4	0.00713

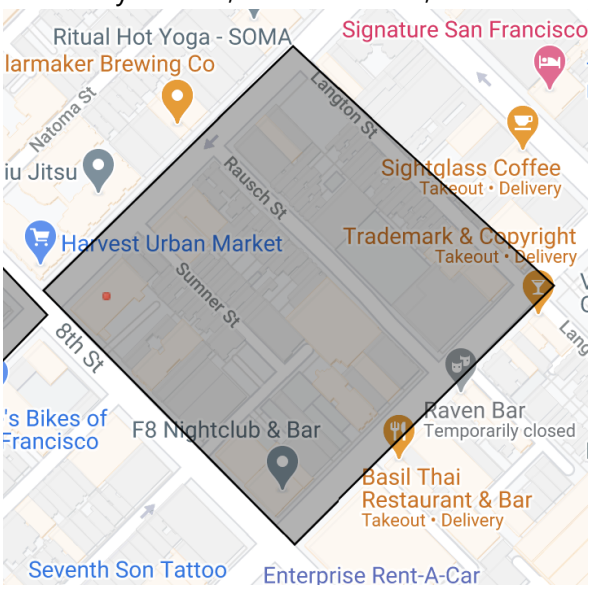
- MSC South Shelter, 525 5th Street, San Francisco, CA 94107

[Image description: The image shows a screenshot of a mapped area around the MSC South Shelter.]

Incident Category	Number of SFPD Incidents	Percent
Arson	1	0.005348
Assault	24	0.128342
Burglary	9	0.048128

Disorderly Conduct	6	0.032086
Drug Offense	3	0.016043
Family Offense	1	0.005348
Fraud	6	0.032086
Larceny Theft	32	0.171123
Lost Property	4	0.02139
Malicious Mischief	17	0.090909
Miscellaneous Investigation	2	0.010695
Missing Person	1	0.005348
Motor Vehicle Theft	9	0.048128
Non-Criminal	26	0.139037
Offences Against The Family And Children	1	0.005348
Other	3	0.016043
Other Miscellaneous	13	0.069519
Other Offenses	1	0.005348
Recovered Vehicle	1	0.005348
Robbery	7	0.037433
Suspicious Occ	3	0.016043
Traffic Violation Arrest	4	0.02139
Warrant	11	0.058824
Weapons Offense	2	0.010695

- Sanctuary Shelter, 201 8th Street, San Francisco, CA 94103

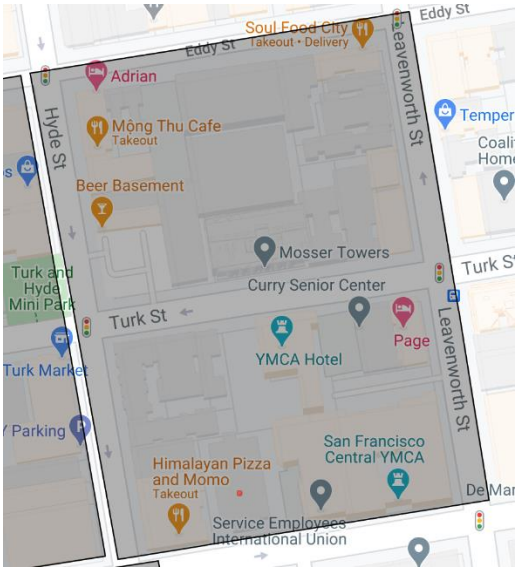


[Image description: The image shows a screenshot of a mapped area around the Sanctuary Shelter.]

Incident Category	Number of SFPD Incidents	Percent
Assault	12	0.065934

Burglary	22	0.120879
Disorderly Conduct	1	0.005495
Drug Offense	1	0.005495
Forgery And Counterfeiting	1	0.005495
Fraud	3	0.016484
Larceny Theft	55	0.302198
Malicious Mischief	21	0.115385
Miscellaneous Investigation	2	0.010989
Missing Person	3	0.016484
Motor Vehicle Theft	10	0.054945
Non-Criminal	12	0.065934
Offences Against The Family And Children	4	0.021978
Other	2	0.010989
Other Miscellaneous	12	0.065934
Robbery	3	0.016484
Stolen Property	1	0.005495
Suspicious Occ	8	0.043956
Traffic Violation Arrest	1	0.005495
Warrant	6	0.032967
Weapons Carrying Etc	1	0.005495
Weapons Offense	1	0.005495

- Hamilton Families, 260 Golden Gate Avenue, San Francisco, CA 94102

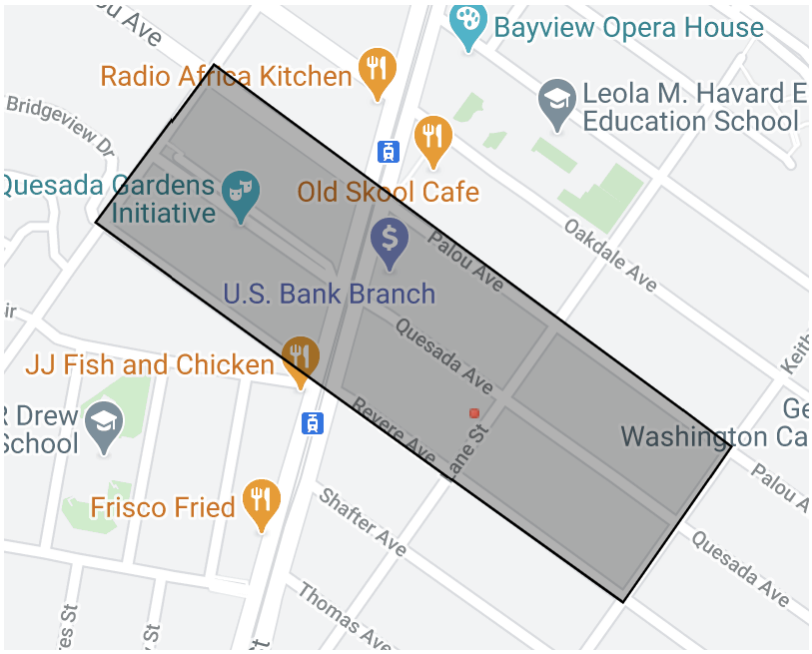


[Image description: The image shows a screenshot of a mapped area around the Hamilton Families Shelter.]

Incident Category	Number of SFPD Incidents	Percent

Arson	4	0.003439
Assault	138	0.118659
Burglary	31	0.026655
Courtesy Report	2	0.00172
Disorderly Conduct	18	0.015477
Drug Offense	282	0.242476
Family Offense	1	0.00086
Fire Report	2	0.00172
Forgery And Counterfeiting	3	0.00258
Fraud	8	0.006879
Larceny Theft	102	0.087704
Lost Property	23	0.019776
Malicious Mischief	45	0.038693
Miscellaneous Investigation	12	0.010318
Missing Person	25	0.021496
Motor Vehicle Theft	26	0.022356
Non-Criminal	109	0.093723
Offences Against The Family And Children	27	0.023216
Other	48	0.041273
Other Miscellaneous	88	0.075666
Other Offenses	3	0.00258
Recovered Vehicle	3	0.00258
Robbery	44	0.037833
Sex Offense	1	0.00086
Stolen Property	1	0.00086
Suspicious Occ	26	0.022356
Traffic Collision	1	0.00086
Traffic Violation Arrest	15	0.012898
Vandalism	1	0.00086
Warrant	60	0.051591
Weapons Carrying Etc	5	0.004299
Weapons Offense	9	0.007739

- Jelani Shelter, 1601 Quesada Avenue, San Francisco, CA 94124

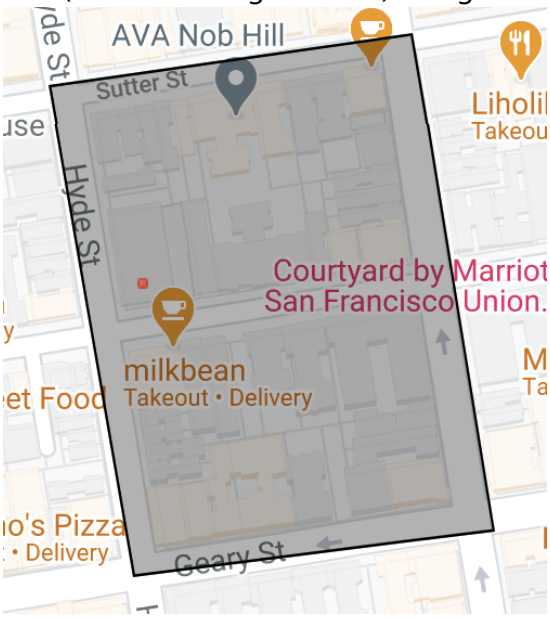


[Image description: The image shows a screenshot of a mapped area around the Jelani Shelter.]

Incident Category	Number of SFPD Incidents	Percent
Assault	38	0.149606
Burglary	6	0.023622
Courtesy Report	1	0.003937
Disorderly Conduct	9	0.035433
Drug Offense	4	0.015748
Forgery And Counterfeiting	1	0.003937
Fraud	7	0.027559
Larceny Theft	34	0.133858
Lost Property	5	0.019685
Malicious Mischief	18	0.070866
Miscellaneous Investigation	5	0.019685
Missing Person	5	0.019685
Motor Vehicle Theft	27	0.106299
Non-Criminal	6	0.023622
Offences Against The Family And Children	7	0.027559
Other Miscellaneous	27	0.106299
Other Offenses	6	0.023622
Robbery	8	0.031496
Suspicious Occ	7	0.027559
Traffic Collision	3	0.011811
Traffic Violation Arrest	7	0.027559
Warrant	13	0.051181

Weapons Carrying Etc	5	0.019685
Weapons Offense	5	0.019685

- TAY (Transitional Aged Youth) Navigation Center, 888 Post Street, San Francisco, CA 94109

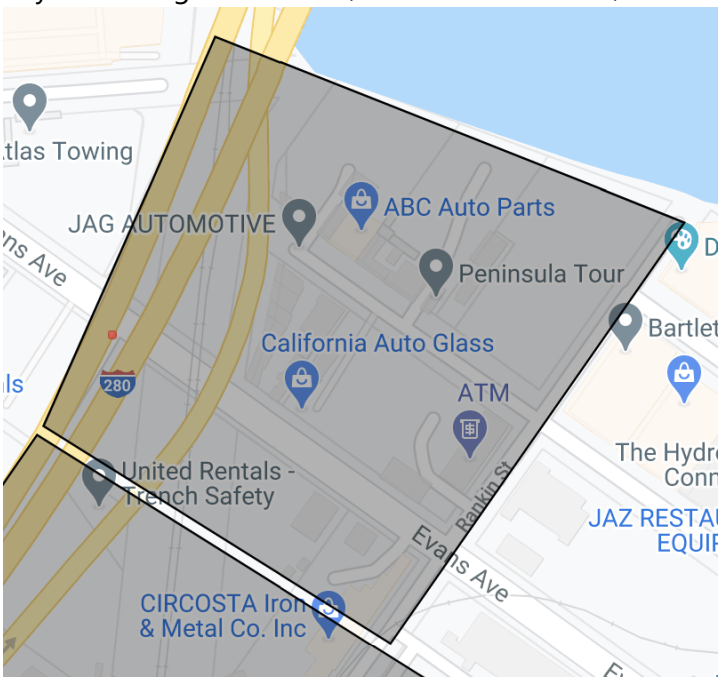


[Image description: The image shows a screenshot of a mapped area around the TAY (Transitional Aged Youth) Navigation Center.]

Incident Category	Number of SFPD Incidents	Percent
Arson	2	0.004474
Assault	18	0.040268
Burglary	59	0.131991
Disorderly Conduct	8	0.017897
Drug Offense	5	0.011186
Fraud	15	0.033557
Larceny Theft	96	0.214765
Liquor Laws	1	0.002237
Lost Property	15	0.033557
Malicious Mischief	41	0.091723
Miscellaneous Investigation	5	0.011186
Missing Person	9	0.020134
Motor Vehicle Theft	28	0.06264
Non-Criminal	31	0.069351
Offences Against The Family And Children	9	0.020134
Other	13	0.029083
Other Miscellaneous	35	0.0783
Other Offenses	1	0.002237

Prostitution	1	0.002237
Rape	1	0.002237
Recovered Vehicle	2	0.004474
Robbery	12	0.026846
Sex Offense	2	0.004474
Stolen Property	6	0.013423
Suspicious Occ	14	0.03132
Traffic Violation Arrest	5	0.011186
Vandalism	3	0.006711
Warrant	6	0.013423
Weapons Carrying Etc	1	0.002237
Weapons Offense	3	0.006711

- Bayview Navigation Center, 1925 Evans Avenue, San Francisco, CA 94124

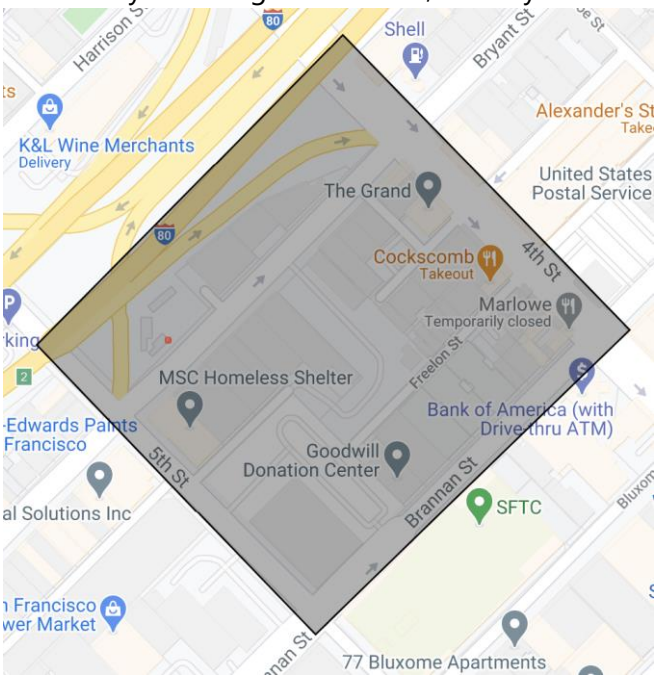


[Image description: The image shows a screenshot of a mapped area around the Bayview Navigation Center.]

Incident Category	Number of SFPD Incidents	Percent
Arson	2	0.066667
Assault	3	0.1
Fire Report	3	0.1
Larceny Theft	6	0.2
Malicious Mischief	3	0.1
Miscellaneous Investigation	3	0.1
Motor Vehicle Theft	4	0.133333

Other Miscellaneous	1	0.033333
Robbery	1	0.033333
Warrant	1	0.033333
Weapons Offense	3	0.1

- 5th and Bryant Navigation Center, 680 Bryant Street, San Francisco, CA 94107

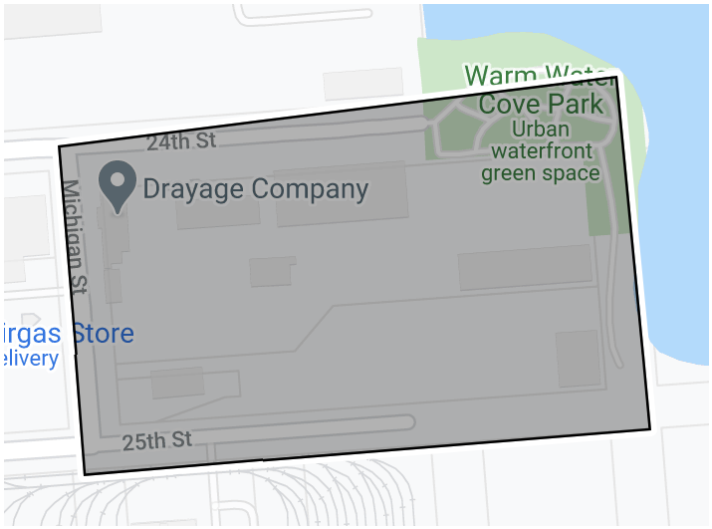


[Image description: The image shows a screenshot of a mapped area around 5th and Bryant Navigation Center.]

Incident Category	Number of SFPD Incidents	Percent
Arson	1	0.005348
Assault	24	0.128342
Burglary	9	0.048128
Disorderly Conduct	6	0.032086
Drug Offense	3	0.016043
Family Offense	1	0.005348
Fraud	6	0.032086
Larceny Theft	32	0.171123
Lost Property	4	0.02139
Malicious Mischief	17	0.090909
Miscellaneous Investigation	2	0.010695
Missing Person	1	0.005348
Motor Vehicle Theft	9	0.048128
Non-Criminal	26	0.139037
Offences Against The Family And Children	1	0.005348

Other	3	0.016043
Other Miscellaneous	13	0.069519
Other Offenses	1	0.005348
Recovered Vehicle	1	0.005348
Robbery	7	0.037433
Suspicious Occ	3	0.016043
Traffic Violation Arrest	4	0.02139
Warrant	11	0.058824
Weapons Offense	2	0.010695

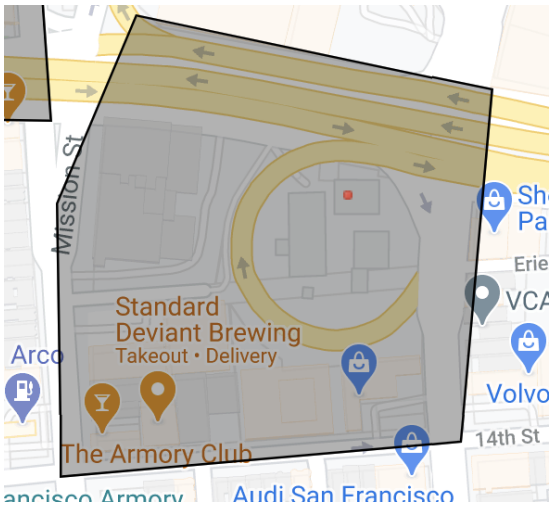
- Central Waterfront Navigation Center, 25th Street, San Francisco, CA 94107



[Image description: The image shows a screenshot of a mapped area around the Central Waterfront Navigation Center.]

No SFPD Incident Data exists or was available for the Central Waterfront Navigation Center site in 2020.

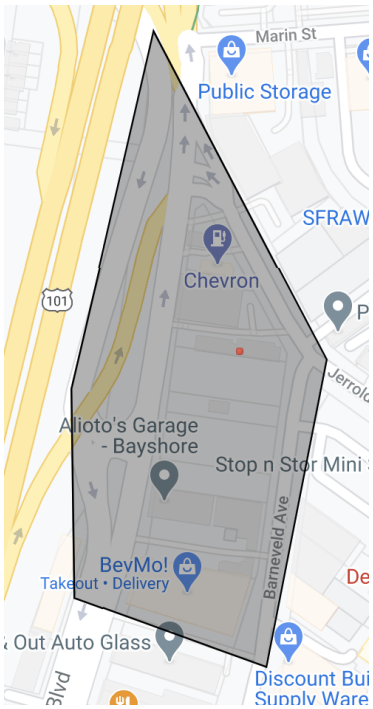
- Division Circle Navigation Center, 224 S Van Ness Avenue, San Francisco, CA 94103



[Image description: The image shows a screenshot of a mapped area around the Division Circle Navigation Center.]

Incident Category	Number of SFPD Incidents	Percent
	2	0.01105
Arson	2	0.01105
Assault	20	0.110497
Burglary	7	0.038674
Courtesy Report	1	0.005525
Disorderly Conduct	1	0.005525
Drug Offense	4	0.022099
Drug Violation	1	0.005525
Embezzlement	1	0.005525
Fraud	1	0.005525
Larceny Theft	38	0.209945
Lost Property	6	0.033149
Malicious Mischief	9	0.049724
Miscellaneous Investigation	1	0.005525
Missing Person	5	0.027624
Motor Vehicle Theft	13	0.071823
Non-Criminal	15	0.082873
Offences Against The Family And Children	2	0.01105
Other	2	0.01105
Other Miscellaneous	27	0.149171
Robbery	4	0.022099
Suspicious Occ	5	0.027624
Traffic Violation Arrest	2	0.01105
Vandalism	1	0.005525
Warrant	7	0.038674
Weapons Carrying Etc	4	0.022099

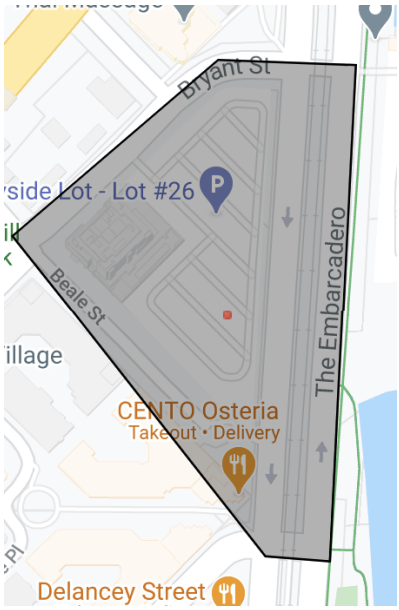
- Bayshore Navigation Center, 125 Bayshore Boulevard, San Francisco, CA 94124



[Image description: The image shows a screenshot of a mapped area around the Bayshore Navigation Center.]

No SFPD Incident Data exists or was available for the Bayshore Navigation Center site in 2020.

- Embarcadero Navigation Center, 555 Beale Street, San Francisco, CA 94107

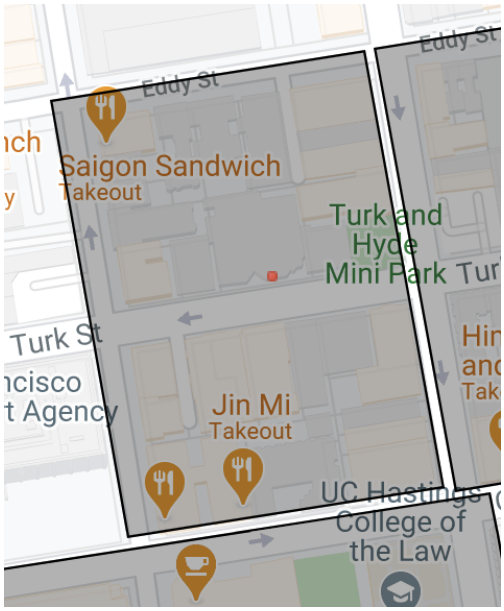


[Image description: The image shows a screenshot of a mapped area around the Embarcadero Navigation Center.]

Incident Category	Number of SFPD Incidents	Percent

Assault	6	0.064516
Burglary	7	0.075269
Courtesy Report	1	0.010753
Drug Offense	2	0.021505
Fraud	2	0.021505
Larceny Theft	28	0.301075
Lost Property	3	0.032258
Malicious Mischief	11	0.11828
Missing Person	1	0.010753
Motor Vehicle Theft	6	0.064516
Non-Criminal	9	0.096774
Other	1	0.010753
Other Miscellaneous	6	0.064516
Other Offenses	1	0.010753
Robbery	2	0.021505
Stolen Property	2	0.021505
Suspicious Occ	3	0.032258
Warrant	2	0.021505

- Homelessness and Supportive Housing Department Home Office, 440 Turk Street, San Francisco, CA 94102



[Image description: The image shows a screenshot of a mapped area around the Homelessness and Supportive House Department Home Office building.]

Incident Category	Number of SFPD Incidents	Percent
	2	0.00627
Assault	21	0.065831

Burglary	10	0.031348
Courtesy Report	1	0.003135
Disorderly Conduct	5	0.015674
Drug Offense	70	0.219436
Fraud	3	0.009404
Larceny Theft	38	0.119122
Lost Property	7	0.021944
Malicious Mischief	11	0.034483
Miscellaneous Investigation	1	0.003135
Missing Person	3	0.009404
Motor Vehicle Theft	16	0.050157
Non-Criminal	36	0.112853
Offences Against The Family And Children	3	0.009404
Other	13	0.040752
Other Miscellaneous	28	0.087774
Other Offenses	1	0.003135
Recovered Vehicle	5	0.015674
Robbery	9	0.028213
Sex Offense	1	0.003135
Stolen Property	2	0.00627
Suspicious Occ	5	0.015674
Traffic Collision	1	0.003135
Traffic Violation Arrest	3	0.009404
Warrant	20	0.062696
Weapons Carrying Etc	1	0.003135
Weapons Offense	3	0.009404

Information on crime statistics in 2020 in this area is provided by the San Francisco Police Department. Statistics are taken from a 1-block radius around the location of cameras. All information is obtained through the San Francisco Open Data Portal: https://datasf.org/opendata/

In addition, the department maintains an internal incident log. No incidents were recorded for 2020.

Surveillance Impact Report

Department of Human Resources
Security Cameras

As required by San Francisco Administrative Code, Section 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 surveillance cameras.

DESCRIPTION OF THE TECHNOLOGY

DHR's Mission is to use fair and equitable practices to hire, develop, support, and retain a highly-qualified workforce.

In line with its mission, the Department shall use security cameras only for the following authorized purposes:

Authorized Use(s):

1. Live monitoring.
2. Recording of video and images in the event of an incident.
3. Reviewing camera footage.
4. Providing video footage/images to law enforcement or other authorized persons following an incident.

Prohibited use cases include any uses not stated in the Authorized Use Case section.

Further, processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, gender, gender identity, disability status, or an individual person's sex life or sexual orientation, and the processing of genetic data and/or biometric data for the purpose of uniquely identifying an individual person shall be prohibited.

Department technology may be deployed in the following locations, based on use case:

Certain areas of the 4th floor of 1 South Van Ness that constitute path-of-travel for DHR employees and guests but, due to nature of building design, may be considered public (i.e., pre-security space near elevators and escalators). .

Surveillance Oversight Review Dates
COIT Review: March 18, 2021
Board of Supervisors Review: TBD

Technology Details

The following is a product description:

The cameras and OpenEye software are more than 10 years old. Product descriptions are not currently available.

A. How It Works

To function, Non-zoom, fixed surveillance camera and OpenEye video recording system. The security camera provides a feed that, at request and in the case of a suspected wrongdoing, may be reviewed by the Department's Chief Engineer. The system records on a continuous loop.

Data collected or processed by security cameras will not be handled or stored by an outside provider or third-party vendor on an ongoing basis. The Department will remain the sole Custodian of Record.

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 security cameras has the following benefits for the residents of the City and County of San Francisco:

▪	Education	
▪	Community Development	
X	Health	Protect safety of staff, patrons, and facilities while promoting an open and welcoming environment.
▪	Environment	
X	Criminal Justice	Review video footage after a security incident; provide video evidence to law enforcement or the public upon request by formal process, order, or subpoena.
▪	Jobs	
▪	Housing	

- Other

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:

DHR addresses potential civil rights/liberties impacts by using extreme discretion with regard to the cameras. DHR does not actively monitor the camera feed. The cameras are in the limited portion of the fourth floor that may be considered public space. Only one employee has access to the cameras, the data is local and not saved into perpetuity, and the camera feeds are only pulled in the event of suspected wrongdoing, and only at the request of only one of three senior managers (Human Resources Director, Managing Deputy Director, or Department Personnel Officer). DHR has never provided recordings to other City departments or outside entities, and would never do so without first consulting with the City Attorney.

C. Fiscal Analysis of Costs and Benefits

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

Benefit		**Description**
X	Financial Savings	Department Security Camera Systems will save on building or patrol officers.
X	Time Savings	Department Security Camera Systems will run 24/7, thus eliminating building or patrol officer supervision
X	Staff Safety	Security cameras help identify violations of Department Patron Code of Conduct and provide assurance that staff safety is emphasized and will be protected at their place of employment.
X	Data Quality	Security cameras run 24/7/365 so full-time staffing is not required to subsequently review footage of security incidents. Data resolution can be set by level and is currently set to high resolution.

Number of FTE (new & existing)	Cameras and system are more than 10 years old. DHR could not locate cost records. The system is accessed and maintained by our IS Engineer, but is accessed with little frequency – approximately one to five hours per year.	
Classification	1042 IS Engineer-Journey	
	Annual Cost	***One-Time Cost***
Software	***0***	0

Hardware/Equipment	*0*	0
Professional Services	*0*	0
Training	*0*	*0*
Other	0	0
Total Cost	*0*	*0*

The Department funds its use and maintenance of the surveillance technology through its General Fund allocation.

COMPARISON TO OTHER JURISDICTIONS

Non-zoom, fixed surveillance cameras and the OpenEye video recording system are currently utilized by other governmental entities for similar purposes.

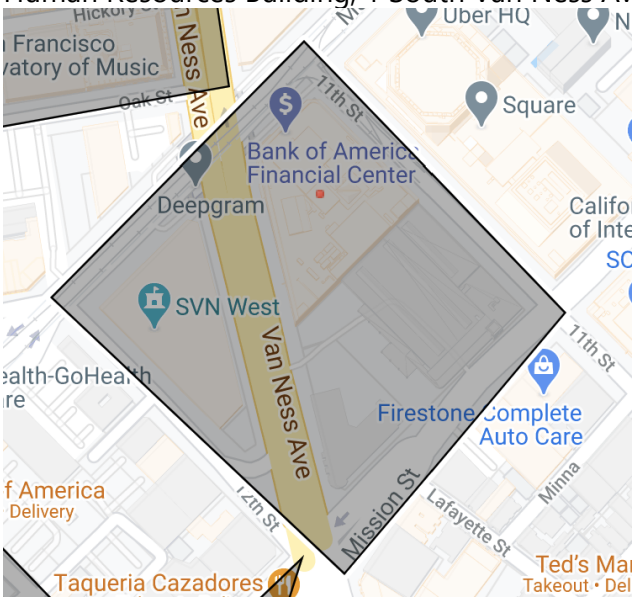
Appendix A: Crime Statistics

Department: Human Resources

Section 19B requires each department in their Surveillance Impact Report to respond to the following question if applicable, "the general location(s) [of the surveillance technology] may be deployed and crime statistics for any location(s)."

The Department of Human Resources operates a total of 3 Security Cameras at the following locations:

- Human Resources Building, 1 South Van Ness Avenue, 4th Floor, San Francisco, CA, 94103



[Image description: The image shows a screenshot of a mapped area around 1 South Van Ness building.]

Incident Category	Number of SFPD Incidents	Percent
Arson	2	0.011561
Assault	23	0.132948
Burglary	15	0.086705
Disorderly Conduct	7	0.040462
Drug Offense	2	0.011561
Family Offense	1	0.00578
Fire Report	2	0.011561
Forgery And Counterfeiting	1	0.00578
Fraud	4	0.023121
Larceny Theft	22	0.127168
Lost Property	4	0.023121
Malicious Mischief	11	0.063584

Missing Person	1	0.00578
Motor Vehicle Theft	3	0.017341
Non-Criminal	31	0.179191
Offences Against The Family And Children	4	0.023121
Other	2	0.011561
Other Miscellaneous	13	0.075145
Other Offenses	2	0.011561
Rape	1	0.00578
Robbery	2	0.011561
Stolen Property	1	0.00578
Suspicious Occ	7	0.040462
Traffic Violation Arrest	4	0.023121
Warrant	7	0.040462
Weapons Offense	1	0.00578

Information on crime statistics in this are is provided by the San Francisco Police Department. All information obtained through the San Francisco Open Data Portal: https://datasf.org/opendata/

In addition, the department maintains an internal incident log. No incidents were recorded in 2020.

Surveillance Impact Report

Human Services Agency
Security Cameras

As required by San Francisco Administrative Code, Section 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 surveillance cameras.

DESCRIPTION OF THE TECHNOLOGY

The Human Services Agency promotes well-being and self-sufficiency among individuals, families and communities in San Francisco. Security Cameras are used to identify potential threats to persons and property, and to investigate complaints and criminal activity occurring at HSA sites.

In line with its mission, the Human Services Agency (HSA) shall use security cameras only for the following authorized purposes:

Authorized Use(s):

1. Live monitoring.
2. Recording of video and images.
3. Reviewing camera footage in the event of an incident.
4. Providing video footage/images to law enforcement or other authorized persons following an incident or upon request.

Prohibited use cases include any uses not stated in the Authorized Use Case section.

Further, processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, gender, gender identity, disability status, or an individual person's sex life or sexual orientation, and the processing of genetic data and/or biometric data for the purpose of uniquely identifying an individual person shall be prohibited.

Department technology may be deployed in the following locations, based on use case:

Cameras are located at the following locations:

- 1235 Mission
- 1440 Harrison
- 170 Otis
- 2 Gough
- 3120 Mission

Surveillance Oversight Review Dates
COIT Review: March 18, 2021
Board of Supervisors Review: TBD

Technology Details

The following is a product inventory and manufacturer's description:

- 1235 Mission:
    - HONEYWELL MAXPRO – RECORDER
    - PELCO DX8100 – RECORDER
    - ANALOG CAMERAS (25)
    - IP CAMERAS (16) – HONEYWELL IP AND 2 AXIS P3708-PVE
- 1440 Harrison:
    - SALIENT – RECORDER
    - IP CAMERAS (12) – HONEYWELL IP
- 170 Otis:
    - HONEYWELL – RECORDER
    - ANALOG CAMERAS (31) – SONY
    - NAS (VM) – RECORDER
    - WIN SERVER 2019 / VAST VIDEO MANAGEMENT SOFTWARE (VMS)
    - DIGITAL IP CAMERAS (6) – VIVOTEK
- 2 Gough:
    - NAS (VM) – RECORDER
    - WIN SERVER 2019 / VAST VIDEO MANAGEMENT SOFTWARE (VMS)
    - DIGITAL IP CAMERAS (2) - VIVOTEK
- 3120 Mission:
    - HONEYWELL – RECORDER
    - ANALOG CAMERAS (4)

- Manufacturers' Product Descriptions:
    - VIVOTEK - VIVOTEK Inc. was founded in February 2000. The Company markets VIVOTEK solutions worldwide, and has become a leading brand in global security surveillance. To fulfill its global strategic footprint, VIVOTEK is committed to building an ecosystem for the IP surveillance industry, and looks forward to long term collaboration and growth with all partners in our shared pursuit of a safe and secure society.
    - PELCO DX8100 - The DX8100 Series digital video recorders (DVRs) are professional security-level DVRs based on a new and innovative hardware platform that is powered by unparalleled and unique high-performance software. As the security requirements of your business expand into multiple sites and become more diversified, you need a professional DVR that you can quickly and effortlessly increase the channel and recording capacity. •The DX8100 is interoperable with your existing DX8000 DVRs, allowing you to build upon your existing security system. A DX8100 client can operate and administer both the DX8100 and DX8000 within the same network.•When you need to quickly and easily add more security cameras, the new DX8100-EXP 16-channel expansion unit extends the 8- or 16-channel

DX8100 to 24 or 32 channels. With or without the channel expansion unit, all of the cameras can now take advantage of the increased frame rate of 2CIF and 4CIF recording. The DX8100 records video up to 480 images per second ips at a maximum CIF image size. •If your security project requirements increase storage capacity, you can extend internal storage up to 3 TB. With the optional DX9200 HDDI, you can further increase the DX8100 storage capacity. Alternately, you can use the DX9200 HDDI as a redundant RAID solution. •As your audio security needs grow, use the DX8108-AUD or DX8116-AUD audio option to add a total of 8 or 16 audio inputs. •Sophisticated video security applications require a network of DVRs to monitor multiple locations. The 10/100/1000 megabit Ethernet port supports today's high-speed networks. You can network your DX8100 and DX8000 systems and remotely operate the DVRs for continuous, motion detection, alarm, ATM/POS, normal scheduled recording, and administer and view live and playback video. For time-critical security applications, you must ensure that all video recordings are synchronized to an accurate time source. The DX8100 supports the network time protocol (NTP), which allows you to synchronize all networked DX8100s to one NTP time server.

- HONEYWELL MAXPRO VMS is an enterprise-class video management and hybrid solution. It enables you to operate the traditional analog, network and IP based video equipment in the same surveillance network. You can deploy thousands of cameras in number of locations, and add many video devices such as recorders and monitors.
- NAS VIRTUAL MACHINE (VM) – The VM is powered by Intel® Xeon® dual core CPU E5-2670 0 @ 2.60GHz x-64 processor, 64-bit Operating System, 4.00 GB of RAM, 75 GB of hard drive space.
- SALIENT NVR SERVER – Salient's hybrid NVRs are industry-leading, value-oriented digital video surveillance systems. Power-built for the rigors of continuous duty operation using advanced components, the 1U rack-mountable PowerPro hybrid NVR delivers the reliability and processing power required for mission critical video surveillance. PowerPro offers a Single Intel Xeon processor with 16GB of memory and up to 48TB of video storage delivering high reliability and processing power. Providing up to 32 analog direct connect channels, this hybrid NVR supports IP and analog cameras in a 1U rack mount unit.
- VIVOTEK's FD8169A is an easy-to-use fixed dome network camera specifically designed for indoor security applications, with a 2MP sensor enabling a viewing resolution of 1920x1080 at a smooth 30 fps. Dynamic and highly adaptable. The FD8169A is an all-in-one camera capable of capturing high quality video at high resolutions of up to 2 Megapixels. It also features POE, Real-time H.264, MJPEG Compression (Dual Codec), Removable IR-cut Filter for Day & Night Function, Built-in IR Illuminators effective up to 20 Meters, SNV (Supreme Night Visibility) for Low Light Conditions, Smart Stream II to Optimize Bandwidth Efficiency, Smart IR Technology to Avoid Overexposure, Supports ONVIF Standard to Simplify Integration and Enhance Interoperability, Support Installation with AM-712 Indoor Conduit Box, VIVOCloud App & Portal for 24/7 Surveillance, and Trend Micro IoT Security

- VIVOTEK's FD8182-F2 is an economic professional indoor fixed dome network cameras in VIVTOTEK's 5MP V-Pro Lite series. Design to provide higher resolution and sharper image with more detail, the FD8182-F2 offers up to 15 fps at 5-Megapixel or 30 fps at 1080p resolution. With powerful 3D Noise Reduction technology and Smart Stream technology, the FD8182-F2 can also optimize resolution for a desired object or area to maximize efficiency of bandwidth usage. Other features include POE, Built-in IR Illuminator Effective up to 30 Meters, WDR Enhancement for Unparalleled Visibility in Bright and Dark Environments, Smart Stream to Optimize Bandwidth Efficiency, 3D Noise Reduction for Low-light Conditions, Two-way Audio, PIR motion sensors, Video Rotation for Corridor View, Support Installation with AM-712 Indoor Conduit Box, VIVOCloud App & Portal for 24/7 Surveillance, and Trend Micro IoT Security
- VIVOTEK's IB8360-W (wireless) is a stylish 2-megapixel mini outdoor bullet network camera, specifically designed for boutique retail applications. Delivering a resolution of 1920x1080 at 30 fps, having IR illuminators effective up to 12 meters, and including SNV technology for low light environments, the remarkable cameras provide users with superior image quality around the clock. It also provide built-in IR Illuminators up to 12 meters, Smart IR Technology to Avoid Overexposure, SNV (Supreme Night Visibility) for Low Light Conditions, Smart Stream II to Optimize Bandwidth Efficiency, Weather-proof IP66-rated Housing, Built-in 802.11 b/g/n WLAN, Compact Size, VIVOCloud App & Portal for 24/7 Surveillance, and Trend Micro IoT Security
- HANWHA PNM SERIES MULTI-SENSOR 360 – Network vandal outdoor Multi-sensor Multi-Directional dome camera, (5MP X 4 sensors) 20MP @ 30fps WDR off/on, motorized vari-focal Lens 2.6x (3.6 ~ 9.4mm) (102.5˚ ~ 38.7˚), triple Codec H.265/H.264/MJPEG with WiseStream II technology, 120dB WDR, Defocus detection, built in analytics, true D/N, 4x SD card, hallway view, HLC, Defog detection, DIS(Gyro sensor), 12VAC/HPoE (power adaptor is included), IP66/IK10, -40°C ~ +55°C (-40°F ~ +131°F)
- HANWHA X SERIES DOME – WiseNet X powered by WiseNet 5 network IR indoor dome camera, 5MP @30fps WDR off/on, 3.7mm fixed focal lens (97.5°), H.265/H.264/MJPEG, WiseStream II compression technology, 120dB WDR, USB port for easy installation, advanced video analytics and sound classification, High powered IR LEDs range of 98', True D/N, dual SD card, hallway view, HLC, defog detection with simple focus, DIS , 12VDC/24VAC/PoE, IK08 rated
- AXIS P3708-PVE - is a fixed dome network camera with three sensors. It gives you a 180º panoramic overview of large areas using a single camera. And it's perfect for use in challenging light conditions, both during the day and at night.
- HONEYWELL – HD4DIRH - 700TVL VFAI WDR TDN IR Mini Dome – Honeywell 960H System Series of cameras provides a wide range of high-quality, feature rich video surveillance options for indoor, outdoor, and low-light applications. 1/3" 960H CCD image sensor, ultra-high resolution image (700TVL), 3D digital noise reduction, digital wide dynamic range, backlight compensation and highlight masking, smart IR technology for

even distribution of the IR, 2.8-12 mm varifocal auto iris (VFAI) lens, true day/night function for vivid color pictures by day and clear black and white pictures at night, excellent low-light performance (0.19 lux color, 0 lux with IR LEDs on), 18 IR LEDs provide up to 50 ft of illumination, depending on scene reflectance, weatherproof, impact-resistant housing (IP66), built-in heater for cold weather operation down to -40 F, breather vent prevents condensation buildup.

- HONEYWELL – HD4D2 – 650 TVL DOME CAMERA – PRODUCT DESCRIPTION NOT FOUND/UNAVAILABLE.
- HONEYWELL – H4L2GR1V – 2 MEGAPIXEL DOME IP CAMERA - Full HD 1080p 50/60 fps image with a ½.8"2 MP sensor, WDR up to 120 dB ensures glare-free images, true day/night provides colour images by day and clear black-and-white images at night with ICR, excellent low-light performance with 3D noise reduction, saving storage and bandwidth together with H.265 High Profile codec, low light technology is able to capture high quality colour images in low light environments, 2.7-13.5 mm, F1.6, motorized focus/zoom lens, H.265 plus, H265, H.264 and MJPEG codec, triple stream support, IR LEDs provide up to 50m (150') of illumination in dimly lit or night time scenes (depending on scene reflectance), smart IR technology provides even distribution of IR, waterproof (IP67) and IK10 vandal resistant camera housing, -40C to 60C working temperature, ONVIF Profile S, G & Q compliant, security features include individual signed certificates and data encryption, cameras can be retrofitted on many existing DVR/NVR installations without requiring additional storage, built-in PoE eliminates separate power supply and associated wiring; 24 V AC/12 V DC inputs where PoE is unavailable, 12 VDC/2W output, supports up to 128 GB micro SDHC (Class 10) card for local video storage when network is interrupted.
- ARECONT – AV2256PM – 2 MEGAPIXLE DOME IP CAMERA - The AV2256PM MegaDome® 2 series network camera is part of Arecont Vision's Wide Dynamic Range line of H.264 MegaDome® 2 series cameras. This fully compliant implementation of H.264 (MPEG 4, Part 10) provides full 1920 x 1080 megapixel resolution at full video frame rates of 32fps. The AV2255AM camera line provides an all-in-one solution with integrated 1080p resolution camera, remote focus, remote zoom, motorized P-iris lens, and IP66 and vandal resistant dome enclosure. With the features of Casino mode, ONVIF Profile S, PSIA conformance, privacy masking, extended motion detection and flexible cropping, the AV2256PM is a high sensitivity, PoE (IEEE 802.3af) compliant camera. Built with Arecont Vision's massively-parallel MegaVideo® technology, this camera offers over six times the resolution of standard resolution IP cameras with the ability to output full real-time frame rates and deliver the high quality megapixel imaging for both indoor and outdoor applications.
- AXIS – P3707-PE – 8 MEGAPIXEL MULTI-SENSOR 360-DEGREE IP CAMERA - AXIS P3707-PE comprises four camera heads that can be repositioned along a circular track to point in the desired viewing direction. Each camera head can be individually tilted and adjusted to provide a 108° to 54° horizontal field of view for either wide or zoomed-in views. The camera heads can be rotated to support Axis' Corridor Format for optimal coverage of

vertically oriented scenes. A specially designed clear cover, with no sharp edges, allows for undistorted views in all directions. AXIS P3707-PE supports individually configurable video streams for each camera head, as well as quad-view streaming, enabling 1080p resolution videos at 12.5/15 frames per second and 720p videos at full frame rate.

- SONY – EX543 – ANALOG CAMERA – PRODUCT DESCRIPTION NOT FOUND/UNAVAILABLE
- TRIVIEW – TFD-CVSH312A1241IR – DOME ANALOG CAMERA – PRODUCT DESCRIPTION NOT FOUND/UNAVAILABLE

A. How It Works

IP, digital and analog cameras record images from public and non-public areas to digital recording devices.

Data collected or processed by security cameras will not be handled or stored by an outside provider or third-party vendor on an ongoing basis. The Department will remain the sole Custodian of Record.

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 security cameras has the following benefits for the residents of the City and County of San Francisco:

	▪ Education	
	▪ Community Development	
X	Health	Protect safety of staff, patrons, and facilities while promoting an open and welcoming environment.
	▪ Environment	
X	Criminal Justice	Safeguards and protects public property. Review video footage after a security incident; provide video evidence to law

	enforcement or the public upon request by formal process, order, or subpoena.

- Jobs
- Housing
- Other

In addition, the Department's sworn investigative staff are charged with monitoring the multi-million dollar security officer contract to ensure services are provided in accordance with that contract. The assigned Department Liaison Officer (DLO) uses the surveillance system to review incidents involving security as needed for conformity with the contract provisions.

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:

Since its initial installation in the 1980's, the video surveillance technology employed by HSA at its various facilities has been used solely to identify threats to persons and property, investigate complaints and criminal activity that occurs at these locations. In keeping with these policies and practices, there has been no negative impact on HSA staff, public, or others through the use of this technology.

The technology has been successfully used in both criminal prosecutions and the investigation and resolution of administrative complaints lodged against HSA staff persons and members of the public. To date, no complaints have been lodged against the Department relative to its use. Moreover, the Department's practice of limiting access to the system to its sworn investigators via a secure internal network minimizes the likelihood of its misuse or employment for unauthorized purposes.

In sum, this technology as it is employed by the Department poses no significant risk to the public and/or HSA employees for the aforementioned categories: dignitary loss, discrimination, economic loss, loss of autonomy, loss of liberty physical harm, or loss of trust.

C. Fiscal Analysis of Costs and Benefits

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

Benefit		Description
X	Financial Savings	The camera system's live feeds are monitored by on site contract security officers, enabling them to identify potential threats to staff and public in real time. The cameras augment the security officers' ability to respond quickly and efficiently with fewer officers required to manage specific building floor areas.

X	Time Savings	Department Security Camera Systems will run 24/7, thus eliminating building or patrol officer supervision
X	Staff Safety	Security cameras help identify violations of Department Patron Code of Conduct and provide assurance that staff safety is emphasized and will be protected at their place of employment.
X	Data Quality	Security cameras run 24/7/365 so full-time staffing is not required to subsequently review footage of security incidents. Data resolution can be set by level and is currently set to high resolution.

Number of FTE (new & existing)	No FTE assigned	
Classification	n/a	
	Annual Cost	***One-Time Cost***
Software	**-**	-
Hardware/Equipment	-	-
Professional Services	*$100,000 for ongoing maintenance*	-
Training	-	-
Other	-	-
Total Cost	*Varies between $50,000 - $100,000*	

The Department funds its use and maintenance of the surveillance technology through

- Support through the City's General Fund.

COMPARISON TO OTHER JURISDICTIONS

Security Cameras are currently utilized by other governmental entities for similar purposes.

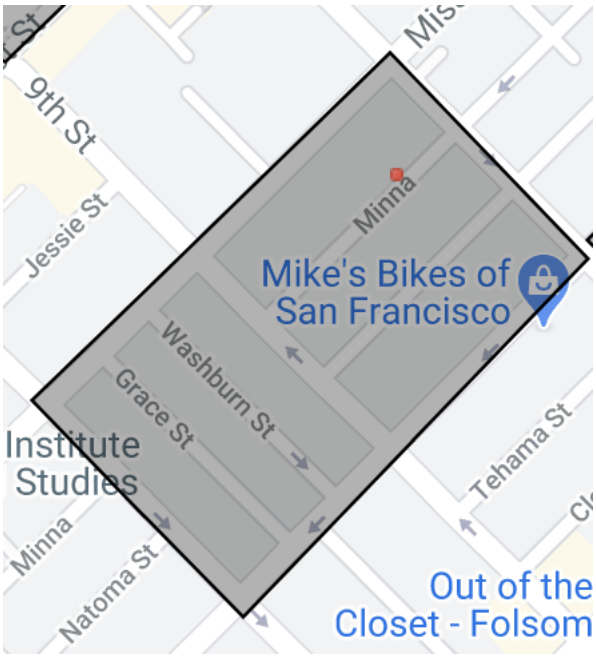
Appendix A: Surveillance Impact Report: Crime Statistics

Department: Human Services Agency

Section 19B requires each department in their Surveillance Impact Report to respond to the following question if applicable, "the general location(s) [of the surveillance technology] may be deployed and crime statistics for any location(s)."

The Human Services Agency operates a total of 102 Security Cameras at the following locations:

- 1235 Mission Street, San Francisco, CA 94103

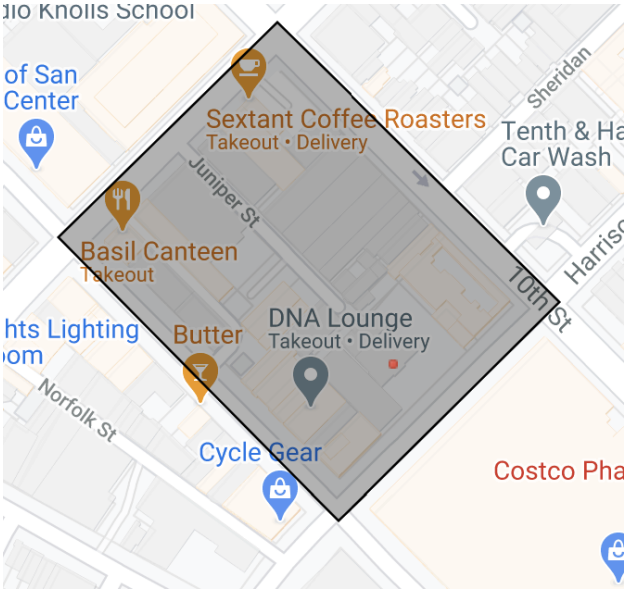


[Image description: The image shows a screenshot of a mapped area around the 1235 Mission Street building.]

Incident Category	Number of SFPD Incidents	Percent
	7	0.007865
Arson	1	0.001124
Assault	72	0.080899
Burglary	54	0.060674
Disorderly Conduct	16	0.017978
Drug Offense	119	0.133708
Forgery And Counterfeiting	1	0.001124
Fraud	16	0.017978
Larceny Theft	137	0.153933
Lost Property	8	0.008989
Malicious Mischief	76	0.085393

Miscellaneous Investigation	12	0.013483
Missing Person	10	0.011236
Motor Vehicle Theft	28	0.031461
Non-Criminal	84	0.094382
Offences Against The Family And Children	18	0.020225
Other	20	0.022472
Other Miscellaneous	74	0.083146
Other Offenses	6	0.006742
Rape	1	0.001124
Recovered Vehicle	3	0.003371
Robbery	17	0.019101
Sex Offense	3	0.003371
Stolen Property	4	0.004494
Suspicious Occ	19	0.021348
Traffic Collision	2	0.002247
Traffic Violation Arrest	16	0.017978
Vandalism	4	0.004494
Warrant	48	0.053933
Weapons Carrying Etc	6	0.006742
Weapons Offense	8	0.008989

- 1440 Harrison Street, San Francisco, CA 94103

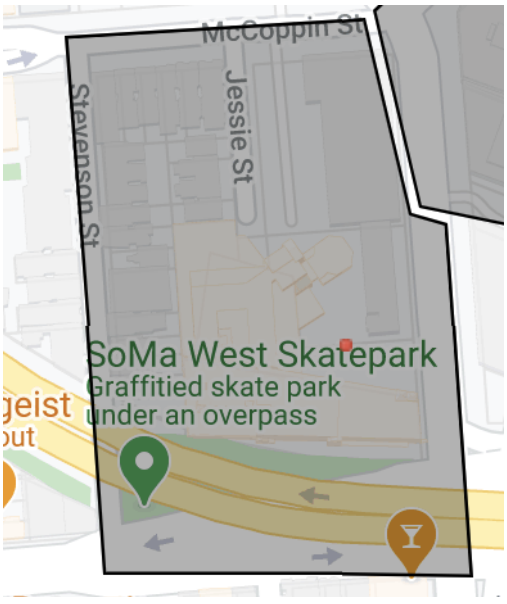


[Image description: The image shows a screenshot of a mapped area around the 1440 Harrison Street building.]

Incident Category	Number of SFPD Incidents	Percent
	1	0.005618

Arson	1	0.005618
Assault	13	0.073034
Burglary	19	0.106742
Disorderly Conduct	4	0.022472
Drug Offense	1	0.005618
Embezzlement	1	0.005618
Fraud	1	0.005618
Larceny Theft	28	0.157303
Lost Property	3	0.016854
Malicious Mischief	22	0.123596
Miscellaneous Investigation	1	0.005618
Missing Person	2	0.011236
Motor Vehicle Theft	20	0.11236
Non-Criminal	11	0.061798
Offences Against The Family And Children	4	0.022472
Other	3	0.016854
Other Miscellaneous	16	0.089888
Other Offenses	1	0.005618
Robbery	5	0.02809
Stolen Property	2	0.011236
Suspicious Occ	5	0.02809
Traffic Collision	1	0.005618
Traffic Violation Arrest	3	0.016854
Vandalism	2	0.011236
Warrant	6	0.033708
Weapons Offense	2	0.011236

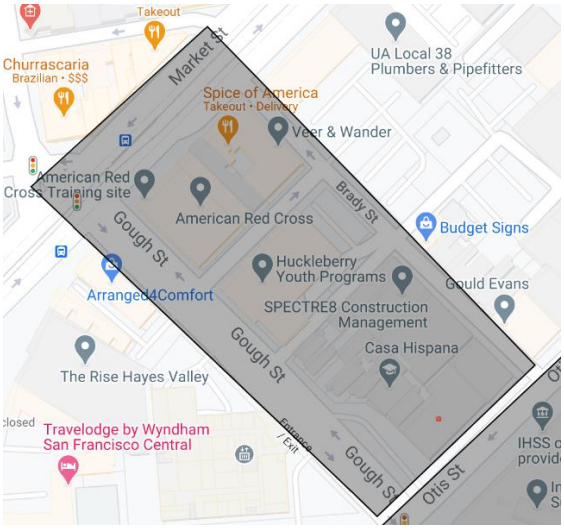
- 170 Otis Street, San Francisco, CA 94103



[Image description: The image shows a screenshot of a mapped area around the 170 Otis Street building.]

Incident Category	Number of SFPD Incidents	Percent
Assault	7	0.089744
Burglary	3	0.038462
Fire Report	1	0.012821
Fraud	1	0.012821
Larceny Theft	17	0.217949
Malicious Mischief	6	0.076923
Missing Person	1	0.012821
Motor Vehicle Theft	8	0.102564
Non-Criminal	9	0.115385
Offences Against The Family And Children	4	0.051282
Other Miscellaneous	7	0.089744
Other Offenses	2	0.025641
Robbery	3	0.038462
Suspicious Occ	2	0.025641
Traffic Violation Arrest	2	0.025641
Warrant	4	0.051282
Weapons Carrying Etc	1	0.012821

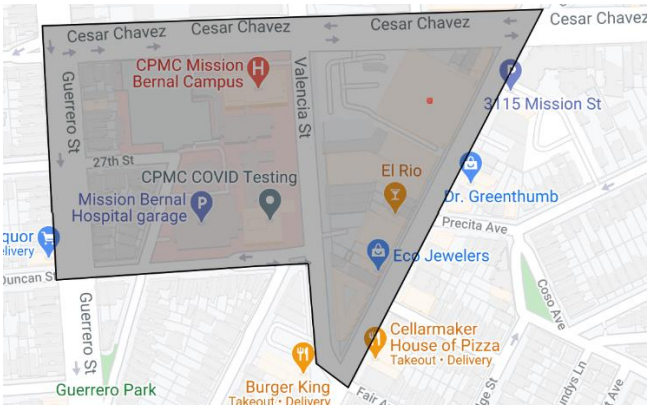
- 2 Gough Street, San Francisco, CA 94103



[Image description: The image shows a screenshot of a mapped area around the 2 Gough Street building.]

Incident Category	Number of SFPD Incidents	Percent
Arson	2	0.020408
Assault	5	0.05102
Burglary	10	0.102041
Civil Sidewalks	1	0.010204
Drug Offense	1	0.010204
Larceny Theft	24	0.244898
Lost Property	3	0.030612
Malicious Mischief	17	0.173469
Motor Vehicle Theft	6	0.061224
Non-Criminal	3	0.030612
Offences Against The Family And Children	2	0.020408
Other	3	0.030612
Other Miscellaneous	6	0.061224
Other Offenses	1	0.010204
Recovered Vehicle	1	0.010204
Robbery	4	0.040816
Stolen Property	1	0.010204
Vandalism	1	0.010204
Warrant	7	0.071429

- 3120 Mission Street, San Francisco, CA 94110



[Image description: The image shows a screenshot of a mapped area around the 3120 Mission Street building.]

Incident Category	Number of SFPD Incidents	Percent
	4	0.018692
Assault	18	0.084112
Burglary	24	0.11215

Courtesy Report	1	0.004673
Disorderly Conduct	3	0.014019
Drug Offense	4	0.018692
Fire Report	1	0.004673
Fraud	12	0.056075
Larceny Theft	41	0.191589
Lost Property	1	0.004673
Malicious Mischief	23	0.107477
Miscellaneous Investigation	5	0.023364
Missing Person	2	0.009346
Motor Vehicle Theft	7	0.03271
Non-Criminal	8	0.037383
Offences Against The Family And Children	5	0.023364
Other	2	0.009346
Other Miscellaneous	24	0.11215
Other Offenses	1	0.004673
Recovered Vehicle	1	0.004673
Robbery	9	0.042056
Stolen Property	1	0.004673
Suspicious Occ	4	0.018692
Traffic Violation Arrest	5	0.023364
Warrant	4	0.018692
Weapons Carrying Etc	3	0.014019
Weapons Offense	1	0.004673

Information on crime statistics in 2020 in this area is provided by the San Francisco Police Department. Statistics are taken from a 1-block radius around the location of cameras. All information is obtained through the San Francisco Open Data Portal: https://datasf.org/opendata/

In addition, the department maintains an internal incident log which cannot be shared publicly.

Surveillance Impact Report

Port of San Francisco
Security Cameras

As required by San Francisco Administrative Code, Section 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 surveillance cameras.

DESCRIPTION OF THE TECHNOLOGY

The Port of San Francisco manages the waterfront as the gateway to a world-class city and advances environmentally and financially sustainable maritime, recreational, and economic opportunities to serve the City, Bay Area region, and California.

In line with its mission, the Department shall use security cameras only for the following authorized purposes:

Authorized Use(s):

1. Live monitoring.
2. Recording of video and images in the event of an incident.
3. Reviewing camera footage.
4. Providing video footage/images to law enforcement or other authorized persons following an incident.

Prohibited use cases include any uses not stated in the Authorized Use Case section.

Further, processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, gender, gender identity, disability status, or an individual person's sex life or sexual orientation, and the processing of genetic data and/or biometric data for the purpose of uniquely identifying an individual person shall be prohibited.

Department technology may be deployed in the following locations, based on use case:

Port Security Camera technology is installed on Port property along the 7.5 miles of San Francisco waterfront. This technology includes CCTV cameras installed on exterior of Pier Bulkhead buildings, Pier Sheds, and Small Craft Harbors. Port Security Camera technology provides layered security protection to multiple MTSA regulated facilities throughout the Port.

Surveillance Oversight Review Dates
COIT Review: March 18, 2021
Board of Supervisors Review: TBD

Technology Details

The following is a product description:

Enterprise Video Management System (VMS) exacqVision Enterprise VMS software records surveillance video from thousands of IP camera models and displays video on Windows, Linux or OSX client software. exacqVision Enterprise VMS software can be licensed for up to 128 IP cameras per server. Building upon the enhanced functionality of Professional Edition VMS, exacqVision Enterprise provides large organizations with features that provide a high level of situational awareness, both of events and system health monitoring

A. How It Works

The technology's primary functions are to provide live views and record video footage to a dedicated, secure server. The system is comprised of multiple cameras connected by data cables and infrastructure to the server. The footage is recorded on the server and stored for a limited amount of time. Data collected or processed Port Security Surveillance Camera System will not be handled or stored by an outside provider or third-party vendor on an ongoing basis. The Department will remain the sole Custodian of Record.

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 security cameras has the following benefits for the residents of the City and County of San Francisco:

- Education
- Community Development

X	Health	Protect safety of staff, patrons, and facilities while promoting an open and welcoming environment.

- Environment

X	Criminal Justice	Review video footage after a security incident; provide video evidence to law enforcement or the public upon request by formal process, order, or subpoena.

- Jobs
- Housing
- Other

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:

The Port of San Francisco believes the Veterans Building Surveillance Camera System poses potential risks to civil liberties in respect to dignity loss and loss of liberty.

An individual could be embarrassed or experience emotional distress if cameras capture behaviors, appearances, or circumstances by which they might feel humiliated. Examples include views of someone exhibiting an emotional outburst, a person's clothing or hair being disheveled, or someone having their physique ridiculed or leered at. Risks for loss of dignity are reduced by restricting access to live views, as well as recorded footage, to a limited number of trained Port staff. Audio is not recorded or enabled.

Loss of liberty could potentially occur if a person were to be misidentified as the perpetrator of a crime or other incident, making them subject to wrongful arrest. An innocent person might be similar in appearance to someone who committed an offense. Surveillance images could reinforce other circumstantial evidence tying the wrong person to a criminal incident. As an example, someone might be wearing clothing like clothing worn by someone seen leaving an office where a theft had just occurred. Loss of liberty risks due to misidentification of a subject in surveillance video is mitigated by restricting access to live views and recorded footage to a limited number of trained personnel.

Fiscal Analysis of Costs and Benefits

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

Benefit		**Description**
X	Financial Savings	Department Security Camera Systems will save on building or patrol officers.
X	Time Savings	Department Security Camera Systems will run 24/7, thus eliminating building or patrol officer supervision

X	Staff Safety	Security cameras help identify violations of Department Patron Code of Conduct and provide assurance that staff safety is emphasized and will be protected at their place of employment.
X	Data Quality	Security cameras run 24/7/365 so full-time staffing is not required to subsequently review footage of security incidents. Data resolution can be set by level and is currently set to high resolution.

Number of FTE (new & existing)	.5	
Classification	5502 Project Manager	
	Annual Cost	***One-Time Cost***
Software		
Hardware/Equipment	*$85,000*	$1,114,319
Professional Services		
Training		
Other		
Total Cost	***$85,000***	*$1,114,319*

The Department funds its use and maintenance of the surveillance technology through

Annual Operating budget and the FEMA Port Security Grant Program.

COMPARISON TO OTHER JURISDICTIONS

Security Cameras similar to the Port Security CCTV System are currently utilized by other governmental entities for similar purposes.

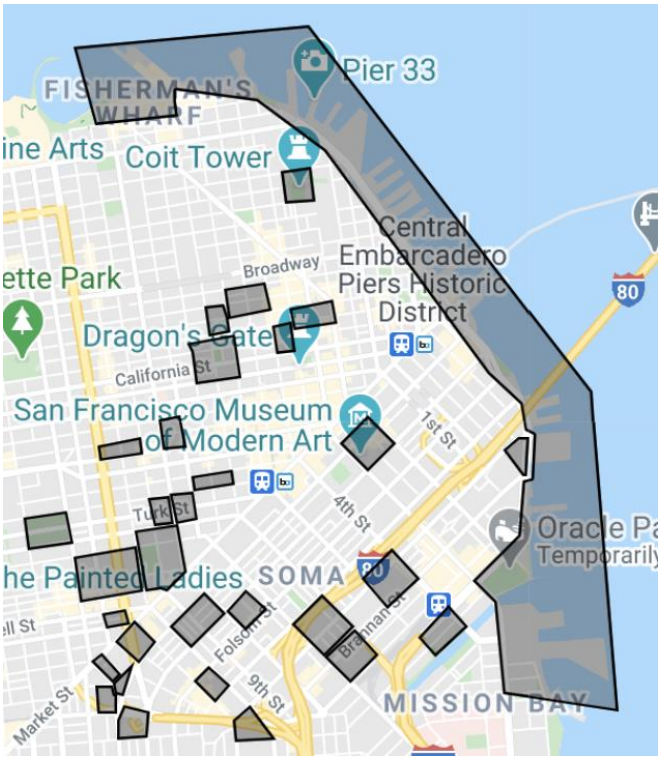
Appendix A: Crime Statistics

Department: Port Department

Section 19B requires each department in their Surveillance Impact Report to respond to the following question if applicable, "the general location(s) [of the surveillance technology] may be deployed and crime statistics for any location(s)."

The Port Department operates a total of 142 Security Cameras over 7.5 miles of waterfront and 13 facilities:

- Hyde St Pier -JOS-Marine Unit
- Pier 22.5 Fireboat – Temporarily out of Service
- Pier 26
- Pier 28
- Pier 29
- Pier 38
- Pier 48
- Pier 50
- Roundhouse
- Pier 23
- Pier 40
- Pier 45
- South Beach Harbor



[Image description: The image shows a screenshot of a mapped area around the San Francisco Ports.]

Incident Category	Number of SFPD Incidents	Percent
	10	0.01292
Arson	2	0.002584
Assault	30	0.03876
Burglary	42	0.054264
Courtesy Report	1	0.001292
Disorderly Conduct	9	0.011628
Drug Offense	4	0.005168
Fire Report	2	0.002584
Forgery And Counterfeiting	2	0.002584
Fraud	10	0.01292
Larceny Theft	333	0.430233
Lost Property	21	0.027132
Malicious Mischief	66	0.085271
Miscellaneous Investigation	6	0.007752
Missing Person	11	0.014212
Motor Vehicle Theft	24	0.031008
Non-Criminal	66	0.085271
Offences Against The Family And Children	10	0.01292
Other	3	0.003876
Other Miscellaneous	73	0.094315
Other Offenses	5	0.00646
Robbery	5	0.00646
Sex Offense	1	0.001292
Stolen Property	5	0.00646
Suicide	1	0.001292
Suspicious Occ	9	0.011628
Traffic Violation Arrest	4	0.005168
Vandalism	2	0.002584
Warrant	10	0.01292
Weapons Carrying Etc	1	0.001292
Weapons Offense	6	0.007752

Information on crime statistics in 2020 in this area is provided by the San Francisco Police Department. Statistics are taken from a 1-block radius around the location of cameras. All information is obtained through the San Francisco Open Data Portal: https://datasf.org/opendata/

In addition, the department maintains an internal incident log which is not publicly available.

Surveillance Impact Report

Department of Public Health
Security Cameras

As required by San Francisco Administrative Code, Section 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 surveillance cameras.

DESCRIPTION OF THE TECHNOLOGY

To protect and promote the health of all San Franciscans. **SFDPH** strives to achieve its **mission** through the work of two main Divisions – the San Francisco Health Network and Population Health In line with its mission, the Department shall use security cameras only for the following authorized purposes:

Authorized Use(s):

1. Live monitoring.
2. Recording of video and images in the event of an incident.
3. Reviewing camera footage.
4. Providing video footage/images to law enforcement or other authorized persons following an incident.

Prohibited use cases include any uses not stated in the Authorized Use Case section.

Further, processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, gender, gender identity, disability status, or an individual person's sex life or sexual orientation, and the processing of genetic data and/or biometric data for the purpose of uniquely identifying an individual person shall be prohibited.

Department technology may be deployed in the following locations, based on use case:

The Critical Infrastructure Camera system records video of the private and sensitive entry ways and exits for City and County's public buildings

Surveillance Oversight Review Dates
COIT Review: March 18, 2021
Board of Supervisors Review: TBD

Technology Details

The following is a product description:

The Lenel CIC solution provides video surveillance of CCSF medical facilities' private and secure areas.

A. How It Works

To function, healthcare industry standard video surveillance and capture technology.

Data collected or processed by security cameras will not be handled or stored by an outside provider or third-party vendor on an ongoing basis. The Department will remain the sole Custodian of Record.

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 be applied as a security safeguard for managing vulnerabilities, a psychological deterrence against criminal activity, and 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 security cameras has the following benefits for the residents of the City and County of San Francisco:

X	Health	Protect safety of staff, patrons, and facilities while promoting an open and welcoming environment.
X	Criminal Justice	Review video footage after a security incident; provide video evidence to law enforcement or the public upon request by formal process, order, or subpoena.

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:

DPH believes Tenant/Contractor security cameras pose potential risks to civil liberties in respect to dignity loss and loss of liberty.

An individual could be embarrassed or experience emotional distress if cameras capture behaviors, appearances, or circumstances by which they might feel humiliated. Examples include views of someone exhibiting an emotional outburst, a person's clothing or hair being disheveled, or someone having their physique ridiculed or leered at. Risks for loss of dignity are reduced by restricting access to live views, as well as any recorded footage shared with Department by Tenant/Contractor, to a limited number of trained Security staff. In addition, live camera views provided to Department staff do not pan, tilt or zoom, thus removing possible temptation for system operators to use those features to follow or enhance views of individuals. Audio is also not recorded or enabled.

Loss of liberty could potentially occur if a person were to be misidentified as the perpetrator of a crime or other incident, making them subject to wrongful arrest. An innocent person might be similar in appearance to someone who committed an offense. Surveillance images could reinforce other circumstantial evidence tying the wrong person to a criminal incident. As an example, someone might be wearing clothing like clothing worn by someone seen leaving an office where a theft had just occurred. Loss of liberty risks due to misidentification of a subject in surveillance video is mitigated by restricting access to live views and any recorded footage shared with Department by Tenant/Contractor to a limited number of trained personnel.

DPH IT defers to the City Attorney's Office on all legal matters.

C. Fiscal Analysis of Costs and Benefits

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

Benefit		Description
X	Financial Savings	Department Security Camera Systems will save on building or patrol officers.
X	Time Savings	Department Security Camera Systems will run 24/7, to augment building and patrol officers
X	Staff Safety	Security cameras help to gather facts in an investigation, and when integrated into the protection system, alerts the operator when the monitor must be viewed, which provides assurance that staff safety is emphasized and will be protected at their place of employment.
X	Data Quality	Security cameras run 24/7/365 so full-time staffing is not required to subsequently review footage of security incidents. Data resolution can be set by level and is currently set to high resolution.

Number of FTE (new & existing)	ZSFG = 7.2 FTE LHH = 5.2 FTE 12.4 FTE total	
Classification	**ZSFG:** 1705 8300 8304 7262	**LHH:** 8300 7262
	Annual Cost	***One-Time Cost***
Total Salary & Fringe	*$1,946,563*	-
Software	-	-
Hardware/Equipment	-	$3,690,575
Professional Services	-	$354,950
Training	-	-
Other	-	-
Total Cost		***$5,992,088***

The Department funds its use and maintenance of the surveillance technology through

- City and County, DPH General Funds

COMPARISON TO OTHER JURISDICTIONS

CIC are currently utilized by other governmental entities for similar purposes.

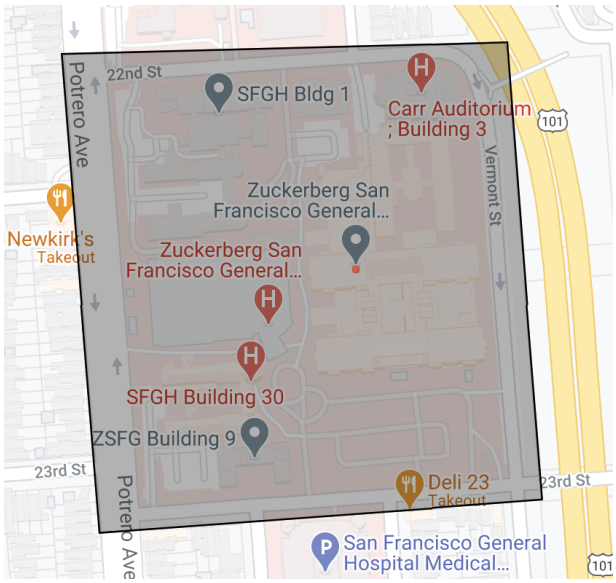
Appendix A: Crime Statistics

Department: Department of Public Health

Section 19B requires each department in their Surveillance Impact Report to respond to the following question if applicable, "the general location(s) [of the surveillance technology] may be deployed and crime statistics for any location(s)."

The Public Health Department operates a total of 509 Security Cameras at the following locations:

- 1001 Potrero Avenue, San Francisco, CA 94110

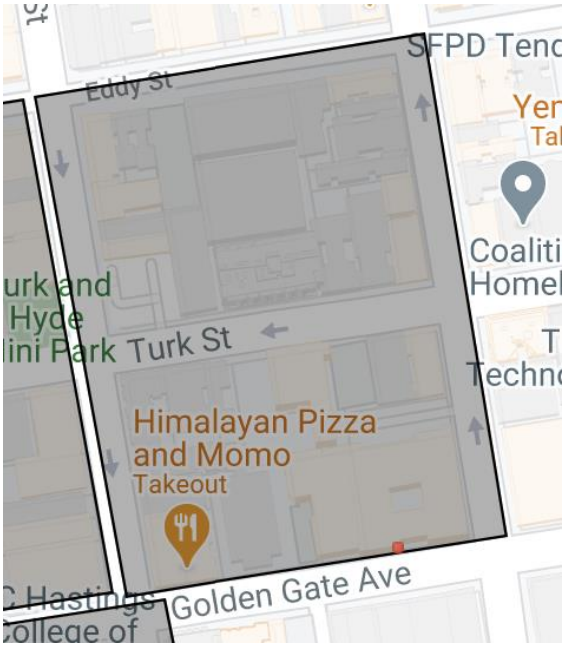


[Image description: The image shows a screenshot of a mapped area around the 1001 Potrero Avenue building.]

Incident Category	Number of SFPD Incidents	Percent
Assault	8	0.0625
Burglary	5	0.039063
Courtesy Report	1	0.007813
Disorderly Conduct	1	0.007813
Fraud	2	0.015625
Larceny Theft	32	0.25
Lost Property	8	0.0625
Malicious Mischief	9	0.070313
Miscellaneous Investigation	3	0.023438
Missing Person	16	0.125
Motor Vehicle Theft	9	0.070313
Non-Criminal	9	0.070313

Offences Against The Family And Children	4	0.03125
Other	1	0.007813
Other Miscellaneous	9	0.070313
Robbery	1	0.007813
Stolen Property	1	0.007813
Suspicious Occ	3	0.023438
Traffic Violation Arrest	3	0.023438
Weapons Carrying Etc	3	0.023438

- 230 Golden Gate Avenue, San Francisco, CA 94102

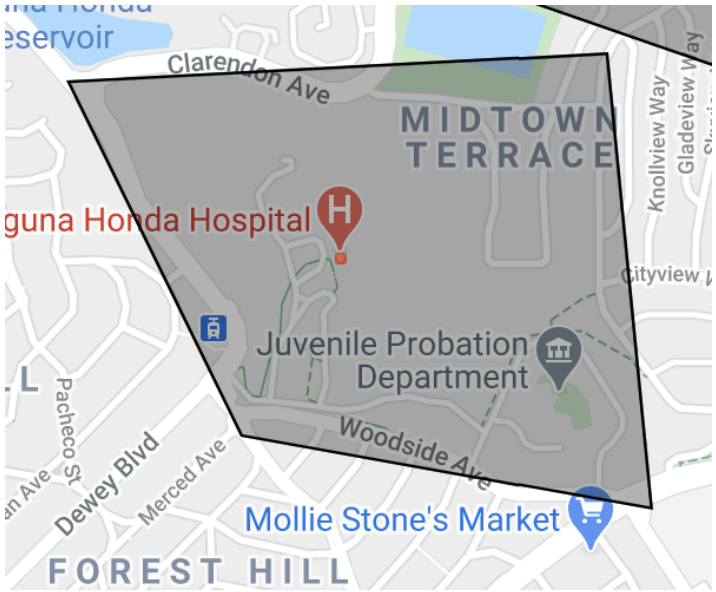


[Image description: The image shows a screenshot of a mapped area around the 230 Golden Gate Avenue building.]

Incident Category	Number of SFPD Incidents	Percent
Arson	4	0.003439
Assault	138	0.118659
Burglary	31	0.026655
Courtesy Report	2	0.00172
Disorderly Conduct	18	0.015477
Drug Offense	282	0.242476
Family Offense	1	0.00086
Fire Report	2	0.00172
Forgery And Counterfeiting	3	0.00258
Fraud	8	0.006879
Larceny Theft	102	0.087704

Lost Property	23	0.019776
Malicious Mischief	45	0.038693
Miscellaneous Investigation	12	0.010318
Missing Person	25	0.021496
Motor Vehicle Theft	26	0.022356
Non-Criminal	109	0.093723
Offences Against The Family And Children	27	0.023216
Other	48	0.041273
Other Miscellaneous	88	0.075666
Other Offenses	3	0.00258
Recovered Vehicle	3	0.00258
Robbery	44	0.037833
Sex Offense	1	0.00086
Stolen Property	1	0.00086
Suspicious Occ	26	0.022356
Traffic Collision	1	0.00086
Traffic Violation Arrest	15	0.012898
Vandalism	1	0.00086
Warrant	60	0.051591
Weapons Carrying Etc	5	0.004299
Weapons Offense	9	0.007739

- 375 Laguna Honda Boulevard, San Francisco, CA 94116



[Image description: The image shows a screenshot of a mapped area around the 375 Laguna Honda Boulevard building.]

Incident Category	Number of SFPD Incidents	Percent
Assault	7	0.081395
Burglary	6	0.069767
Disorderly Conduct	8	0.093023
Drug Offense	1	0.011628
Embezzlement	1	0.011628
Forgery And Counterfeiting	2	0.023256
Fraud	2	0.023256
Larceny Theft	17	0.197674
Lost Property	1	0.011628
Malicious Mischief	8	0.093023
Miscellaneous Investigation	2	0.023256
Missing Person	1	0.011628
Motor Vehicle Theft	4	0.046512
Non-Criminal	11	0.127907
Offences Against The Family And Children	3	0.034884
Other	4	0.046512
Other Miscellaneous	3	0.034884
Suspicious Occ	3	0.034884
Warrant	2	0.023256

Information on crime statistics in 2020 in this area is provided by the San Francisco Police Department. Statistics are taken from a 1-block radius around the location of cameras. All information is obtained through the San Francisco Open Data Portal: https://datasf.org/opendata/

In addition, the department maintains an internal incident log which is available on request.

Surveillance Impact Report

San Francisco Recreation and Parks
Security Cameras

As required by San Francisco Administrative Code, Section 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 surveillance cameras.

DESCRIPTION OF THE TECHNOLOGY

The Department's mission is to provide enriching recreational activities, maintain beautiful parks and preserve the environment for the well-being of our diverse community.

In line with its mission, the Department uses security cameras to protect the public and our staff in our parks, playgrounds and at special events. Security cameras are also used to protect our critical infrastructure sites. The Department has additional cameras that provide educational content to the public, as well promote community development.

In line with its mission, the Department shall use cameras only for the following authorized purposes:

Authorized Use(s):

1. Live monitoring.
2. Recording of video and images in the event of an incident.
3. Reviewing camera footage.
4. Providing video footage/images to law enforcement or other authorized persons following an incident.

Prohibited use cases include any uses not stated in the Authorized Use Case section.

Further, processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, gender, gender identity, disability status, or an individual person's sex life or sexual orientation, and the processing of genetic data and/or biometric data for the purpose of uniquely identifying an individual person shall be prohibited.

Department technology may be deployed in the following locations, based on use case:

All cameras will be located on poles or building facades.

Surveillance Oversight Review Dates
COIT Review: March 18, 2021
Board of Supervisors Review: TBD

Technology Details

The following is a product description:

1. Security Cameras:
   These are network security cameras ranging from 2 to 5 megapixels. Most have pan-tilt-zoom capabilities. Camera vendors are as follows:
   - Arecont Vision
   - Samsung
   - Vivotek
   - AXIS

A. How It Works

To function:

1. Security Cameras
   The video feeds are recorded and retained on a server at each site. If the server is connected to RPD's network, the feed can be streamed to a RPD's Park Ranger Headquarters where they can be monitored for public safety purposes.

Data collected or processed by security cameras will not be handled or stored by an outside provider or third-party vendor on an ongoing basis. The Department will remain the sole Custodian of Record.

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 security cameras has the following benefits for the residents of the City and County of San Francisco:

- Education
- Community Development

X	Health	Protect safety of staff, patrons, and facilities while promoting an open and welcoming environment.
▪	Environment	
X	Criminal Justice	Review video footage after a security incident; provide video evidence to law enforcement or the public upon request by formal process, order, or subpoena.
▪	Jobs	
▪	Housing	
▪	Other	

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:

1. Security Cameras

   The Department has considered the potential impacts of security cameras and has identified technical, administrative, and physical protections as mitigating measures. Through operationalization of the Camera Surveillance Policy, the following will be implemented:

   1. Administrative Safeguards - All security camera data will be captured in a request management software solution. Data will include information about camera procurement, camera attributes, approved requestors of surveillance data, and all requests for Surveillance data. In addition, there will be knowledge articles describing step by step instructions on how to collect and send the data to the requestor.

   2. Technical Safeguards – Security camera data cannot be accessed unless by an approved requestor, and only for approved requests. Violation of the policy will be subject to standard RecPark departmental policies, which may include disciplinary action up to and including termination.

   3. Physical Safeguards - Hardware is secured in the server room, where there is limited physical access. Additionally, there is limited access to the software that stores and retrieves the security camera data.

C. Fiscal Analysis of Costs and Benefits

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

Benefit		Description
X	Financial Savings	Department Security Camera Systems will save on building or patrol officers.
X	Time Savings	Department Security Camera Systems will run 24/7, thus eliminating building or patrol officer supervision
X	Staff Safety	Security cameras help identify violations of Department Patron Code of Conduct and provide assurance that staff safety is emphasized and will be protected at their place of employment.
X	Data Quality	Security cameras run 24/7/365 so full-time staffing is not required to subsequently review footage of security incidents. Data resolution can be set by level and is currently set to high resolution.

SECURITY CAMERAS

Number of FTE (new & existing)	6.75 FTE	
Classification	• Park Rangers (8208-8210, 1704) [6 FTE/ year] • IT analysts (1823) [.5 FTE/year] • 1050 series, 1090 series) [.25 FTE/ year]	
	Annual Cost	***One-Time Cost***
Personnel	$1,210,255	$0.00
Software	$0.00	$0.00
Hardware/Equipment		$180,000
Professional Services	$15,000	$30,000
Training	$2,000	$0.00
Other	0.00	$0.00
Total Cost	*$1,227,255*	*$210,000*
2.1 Please disclose any current or potential sources of funding (e.g. potential sources = prospective grant recipients, etc.). SIR, ASR		
Operational Funds, Capital Funds		

COMPARISON TO OTHER JURISDICTIONS

Security Cameras – similar to other City departments for security and surveillance purposes.

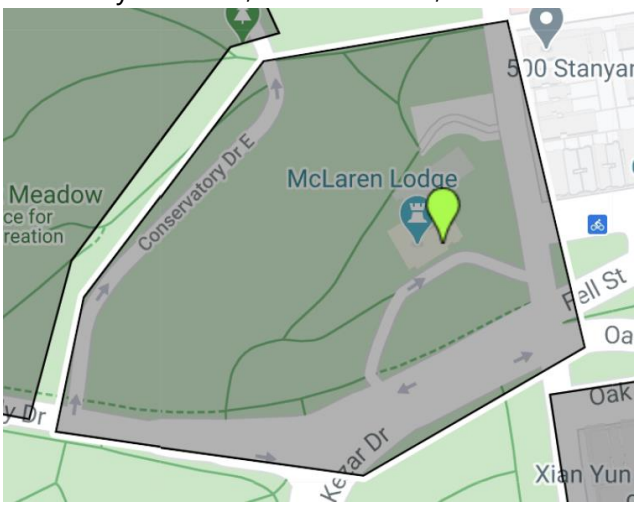
Appendix A: Crime Statistics

Department: Recreation and Parks

Section 19B requires each department in their Surveillance Impact Report to respond to the following question if applicable, "the general location(s) [of the surveillance technology] may be deployed and crime statistics for any location(s)."

The Recreation and Parks Department operates approximately 300 Security Cameras at the following locations:

- 501 Stanyan Street, San Francisco, CA 94117

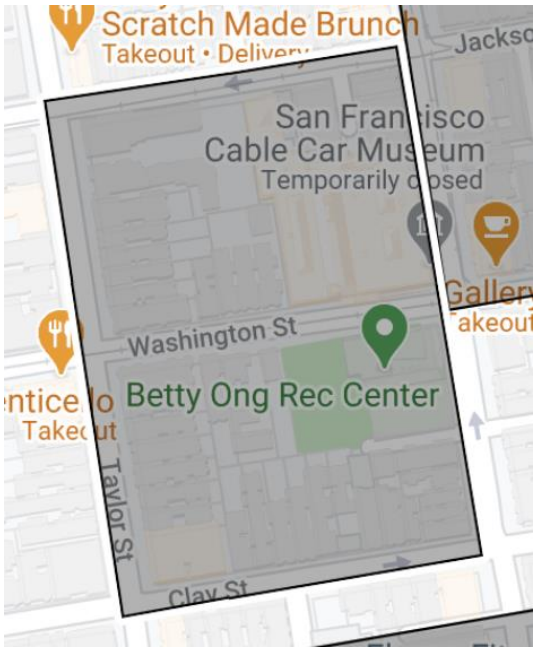


[Image description: The image shows a screenshot of a mapped area around the 501 Stanyan Street address.]

Incident Category	Number of SFPD Incidents	Percent
Assault	6	0.069767
Burglary	1	0.011628
Drug Offense	1	0.011628
Larceny Theft	27	0.313953
Lost Property	1	0.011628
Malicious Mischief	4	0.046512
Miscellaneous Investigation	2	0.023256
Missing Person	11	0.127907
Motor Vehicle Theft	1	0.011628
Non-Criminal	13	0.151163
Offences Against The Family And Children	1	0.011628
Other	1	0.011628
Other Miscellaneous	5	0.05814

Other Offenses	1	0.011628
Robbery	2	0.023256
Suspicious Occ	1	0.011628
Traffic Violation Arrest	2	0.023256
Warrant	3	0.034884
Weapons Carrying Etc	2	0.023256
Weapons Offense	1	0.011628

- Betty Ann Ong Recreation Center, 1199 Mason Street, San Francisco, CA 94108

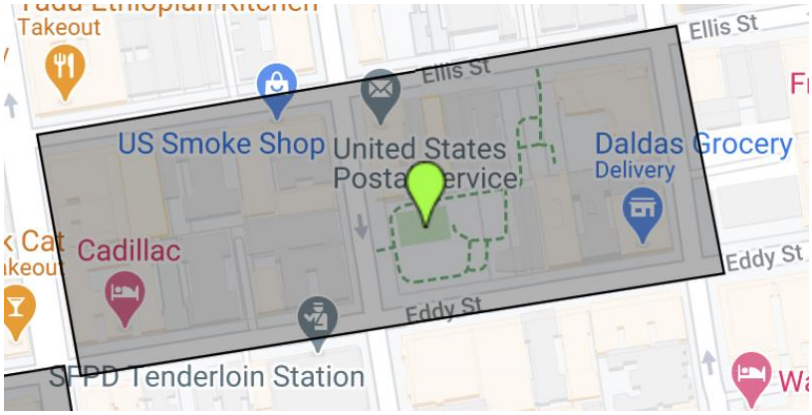


[Image description: The image shows a screenshot of a mapped area around the Betty Ann Ong Recreation Center.]

Incident Category	Number of SFPD Incidents	Percent
Assault	1	0.016949
Burglary	10	0.169492
Disorderly Conduct	1	0.016949
Forgery And Counterfeiting	1	0.016949
Fraud	1	0.016949
Larceny Theft	19	0.322034
Lost Property	1	0.016949
Malicious Mischief	9	0.152542
Missing Person	1	0.016949
Motor Vehicle Theft	5	0.084746
Non-Criminal	1	0.016949
Other	1	0.016949

Other Miscellaneous	5	0.084746
Other Offenses	1	0.016949
Vandalism	1	0.016949
Warrant	1	0.016949

- Boeddeker Park, 246 Eddy Street, San Francisco, CA 94102

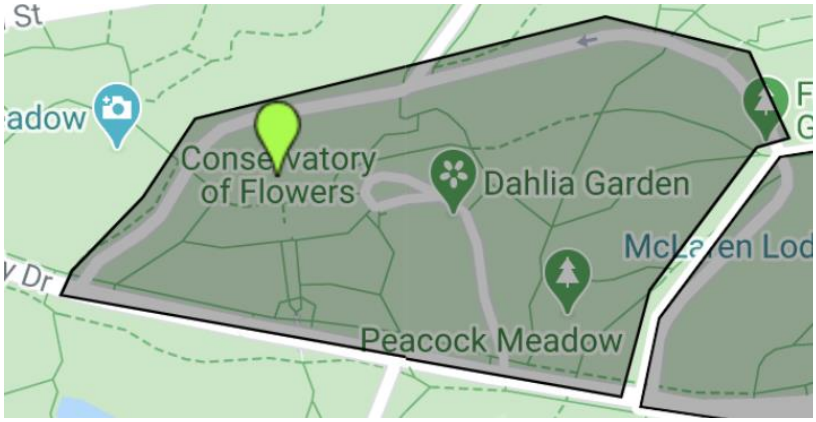


[Image description: The image shows a screenshot of a mapped area around Boeddeker Park.]

Incident Category	Number of SFPD Incidents	Percent
	2	0.002242
Arson	1	0.001121
Assault	111	0.124439
Burglary	10	0.011211
Courtesy Report	14	0.015695
Disorderly Conduct	15	0.016816
Drug Offense	10	0.011211
Embezzlement	3	0.003363
Forgery And Counterfeiting	3	0.003363
Fraud	20	0.022422
Larceny Theft	76	0.085202
Lost Property	28	0.03139
Malicious Mischief	70	0.078475
Miscellaneous Investigation	22	0.024664
Missing Person	66	0.073991
Motor Vehicle Theft	22	0.024664
Non-Criminal	147	0.164798
Offences Against The Family And Children	22	0.024664
Other	32	0.035874
Other Miscellaneous	105	0.117713
Other Offenses	1	0.001121

Recovered Vehicle	1	0.001121
Robbery	14	0.015695
Stolen Property	2	0.002242
Suspicious Occ	55	0.061659
Traffic Collision	1	0.001121
Traffic Violation Arrest	6	0.006726
Vandalism	1	0.001121
Warrant	17	0.019058
Weapons Carrying Etc	5	0.005605
Weapons Offense	10	0.011211

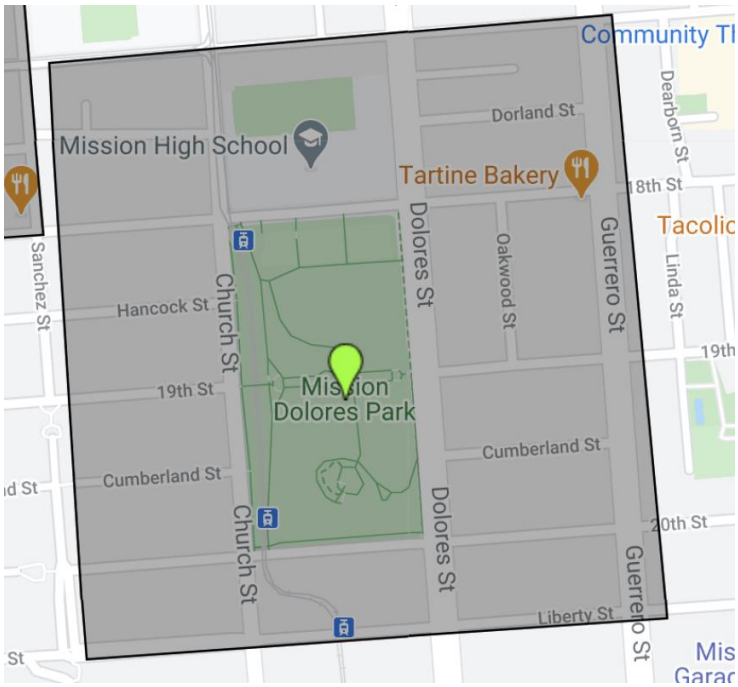
- Conservatory of Flowers, 100 John F Kennedy Drive, San Francisco, CA 94118



[Image description: The image shows a screenshot of a mapped area around Conservatory of Flowers Building.]

Incident Category	Number of SFPD Incidents	Percent
Assault	1	0.05
Drug Offense	1	0.05
Larceny Theft	10	0.5
Malicious Mischief	1	0.05
Motor Vehicle Theft	1	0.05
Non-Criminal	2	0.1
Offences Against The Family And Children	1	0.05
Other Miscellaneous	1	0.05
Robbery	1	0.05
Suspicious Occ	1	0.05

- Dolores Park, Dolores Street and 19th Street, San Francisco, CA 94114

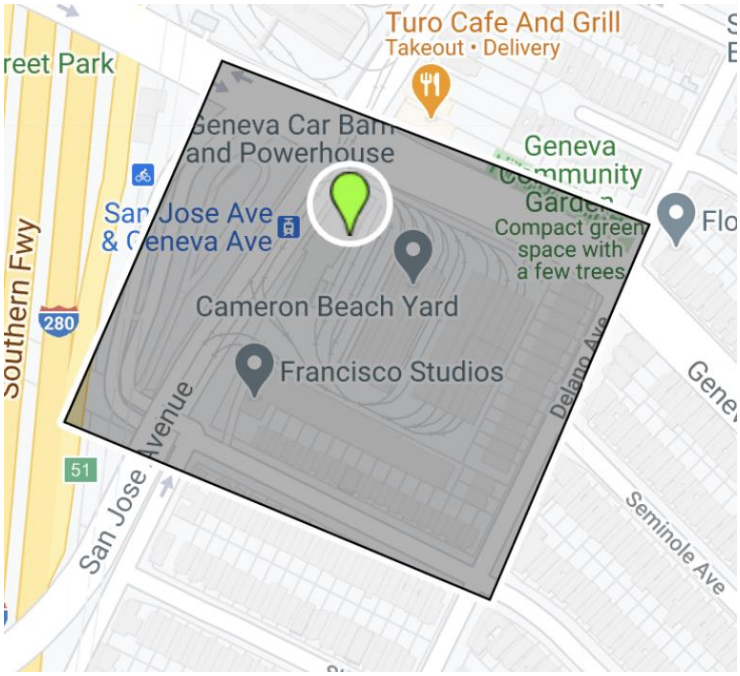


[Image description: The image shows a screenshot of a mapped area around Dolores Park.]

Incident Category	Number of SFPD Incidents	Percent
	1	0.001745
Arson	3	0.005236
Assault	37	0.064572
Burglary	50	0.08726
Courtesy Report	2	0.00349
Disorderly Conduct	10	0.017452
Drug Offense	5	0.008726
Family Offense	1	0.001745
Fire Report	1	0.001745
Forgery And Counterfeiting	1	0.001745
Fraud	15	0.026178
Larceny Theft	171	0.298429
Lost Property	18	0.031414
Malicious Mischief	43	0.075044
Miscellaneous Investigation	7	0.012216
Missing Person	8	0.013962
Motor Vehicle Theft	37	0.064572
Non-Criminal	53	0.092496
Offences Against The Family And Children	11	0.019197
Other	5	0.008726
Other Miscellaneous	36	0.062827

Recovered Vehicle	2	0.00349
Robbery	12	0.020942
Sex Offense	3	0.005236
Stolen Property	1	0.001745
Suspicious Occ	16	0.027923
Traffic Collision	1	0.001745
Traffic Violation Arrest	1	0.001745
Vandalism	3	0.005236
Warrant	15	0.026178
Weapons Carrying Etc	2	0.00349
Weapons Offense	2	0.00349

- Geneva Powerhouse, 2301 San Jose Avenue, San Francisco, CA 94112

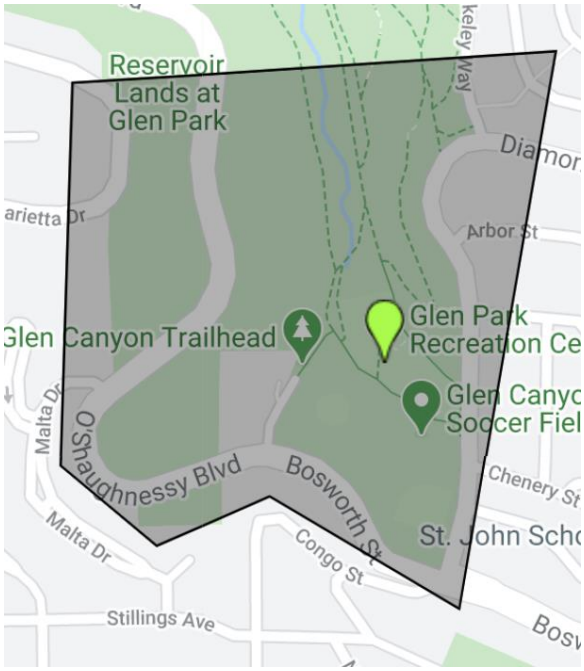


[Image description: The image shows a screenshot of a mapped area around the Geneva Powerhouse building.]

Incident Category	Number of SFPD Incidents	Percent
Assault	8	0.150943
Disorderly Conduct	2	0.037736
Fraud	3	0.056604
Larceny Theft	15	0.283019
Malicious Mischief	4	0.075472
Miscellaneous Investigation	1	0.018868
Missing Person	1	0.018868
Motor Vehicle Theft	6	0.113208

Non-Criminal	3	0.056604
Other Miscellaneous	5	0.09434
Robbery	3	0.056604
Traffic Violation Arrest	1	0.018868
Weapons Offense	1	0.018868

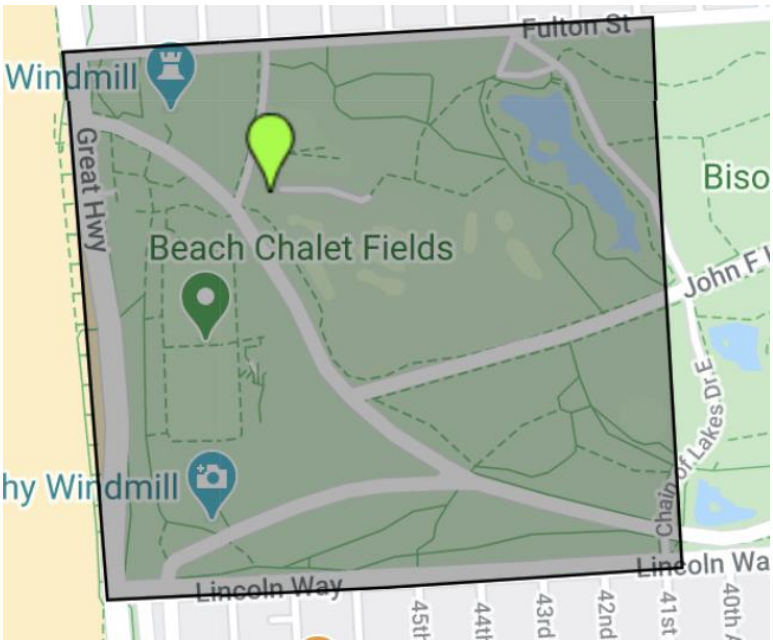
- Glen Park Recreation Center, 70 Elk Street, San Francisco, CA 94131



[Image description: The image shows a screenshot of a mapped area around the Glen Park Recreation Center.]

Incident Category	Number of SFPD Incidents	Percent
Assault	1	0.052632
Fraud	3	0.157895
Larceny Theft	2	0.105263
Malicious Mischief	4	0.210526
Motor Vehicle Theft	4	0.210526
Non-Criminal	1	0.052632
Other Miscellaneous	1	0.052632
Suspicious Occ	1	0.052632
Traffic Violation Arrest	1	0.052632
Warrant	1	0.052632

- Golden Gate Park Golf Course, 970 47th Avenue, San Francisco, CA 94121



[Image description: The image shows a screenshot of a mapped area around the Golden Gate Park Golf Course.]

Incident Category	Number of SFPD Incidents	Percent
	1	0.003058
Arson	1	0.003058
Assault	17	0.051988
Burglary	14	0.042813
Disorderly Conduct	6	0.018349
Drug Offense	4	0.012232
Embezzlement	1	0.003058
Fraud	10	0.030581
Larceny Theft	134	0.409786
Lost Property	4	0.012232
Malicious Mischief	16	0.04893
Miscellaneous Investigation	2	0.006116
Missing Person	3	0.009174
Motor Vehicle Theft	39	0.119266
Non-Criminal	30	0.091743
Offences Against The Family And Children	7	0.021407
Other	1	0.003058
Other Miscellaneous	18	0.055046
Other Offenses	1	0.003058
Robbery	4	0.012232
Suspicious Occ	6	0.018349

Traffic Collision	1	0.003058
Vandalism	1	0.003058
Warrant	3	0.009174
Weapons Carrying Etc	1	0.003058
Weapons Offense	2	0.006116

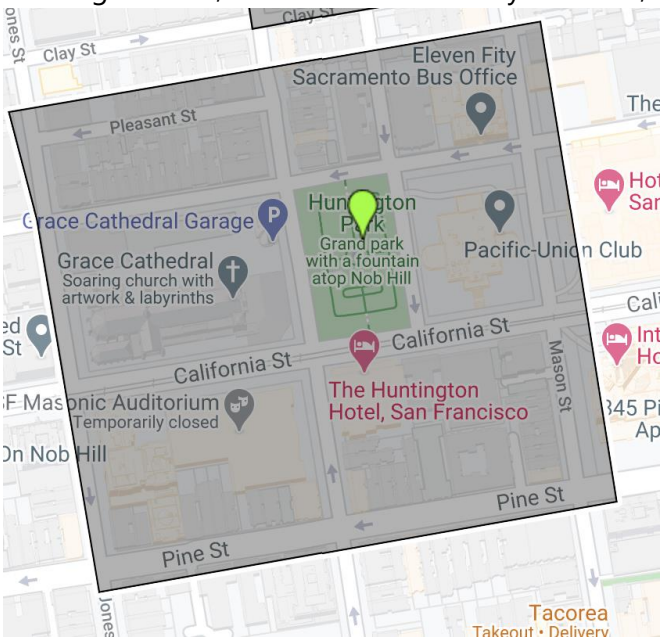
- Herz Park Playground, 1701 Visitacion Avenue, San Francisco, CA 94134

[Image description: The image shows a screenshot of a mapped area around the Herz Park Playground.]

Incident Category	Number of SFPD Incidents	Percent
Arson	1	0.008621
Assault	18	0.155172
Burglary	2	0.017241
Courtesy Report	1	0.008621
Disorderly Conduct	6	0.051724
Family Offense	1	0.008621
Fraud	7	0.060345
Gambling	1	0.008621
Larceny Theft	19	0.163793
Lost Property	2	0.017241
Malicious Mischief	5	0.043103
Motor Vehicle Theft	10	0.086207
Non-Criminal	6	0.051724
Offences Against The Family And Children	6	0.051724
Other	1	0.008621

Other Miscellaneous	10	0.086207
Recovered Vehicle	1	0.008621
Robbery	6	0.051724
Suspicious Occ	3	0.025862
Traffic Violation Arrest	1	0.008621
Warrant	2	0.017241
Weapons Carrying Etc	3	0.025862
Weapons Offense	4	0.034483

- Huntington Park, California Street & Taylor Street, San Francisco, CA 94108

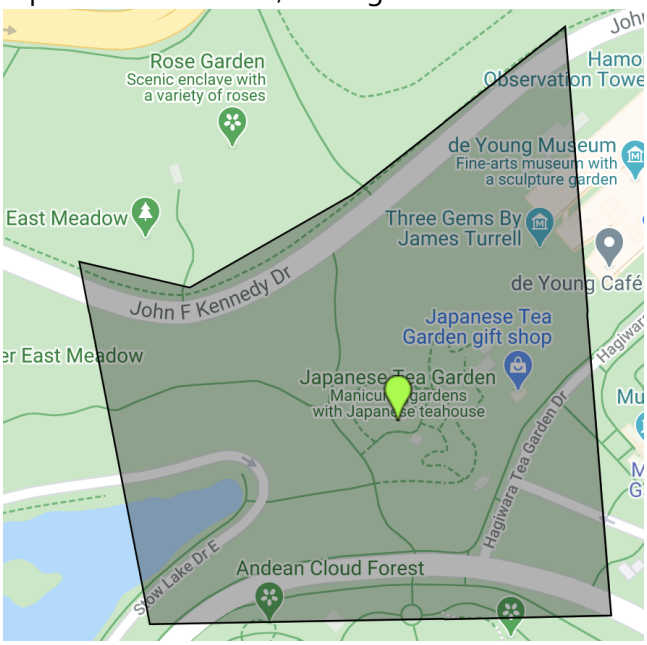


[Image description: The image shows a screenshot of a mapped area around Huntington Park.]

Incident Category	Number of SFPD Incidents	Percent
Arson	1	0.004184
Assault	12	0.050209
Burglary	12	0.050209
Disorderly Conduct	5	0.020921
Drug Offense	2	0.008368
Fraud	10	0.041841
Larceny Theft	63	0.263598
Lost Property	3	0.012552
Malicious Mischief	26	0.108787
Miscellaneous Investigation	6	0.025105
Missing Person	1	0.004184
Motor Vehicle Theft	29	0.121339
Non-Criminal	19	0.079498

Offences Against The Family And Children	3	0.012552
Other	7	0.029289
Other Miscellaneous	18	0.075314
Other Offenses	2	0.008368
Robbery	3	0.012552
Stolen Property	2	0.008368
Suspicious Occ	6	0.025105
Traffic Violation Arrest	3	0.012552
Vandalism	3	0.012552
Warrant	3	0.012552

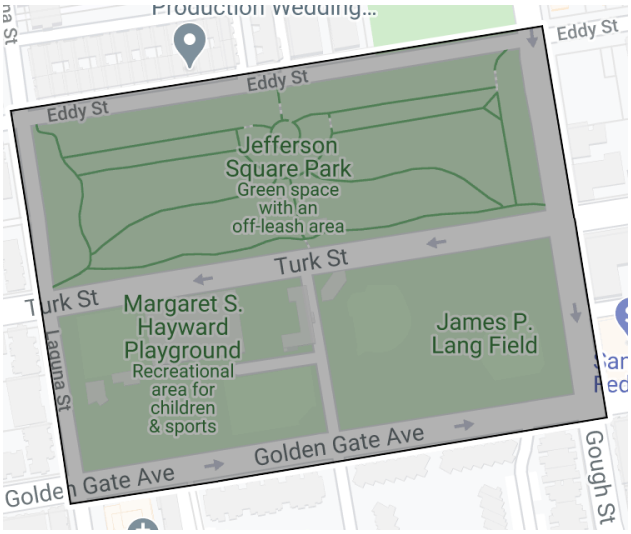
- Japanese Tea Garden, 75 Hagiwara Tea Garden Drive, San Francisco, CA 94118



[Image description: The image shows a screenshot of a mapped area around the Japanese Tea Garden.]

No SFPD Incident Data exists or was available for the Japanese Tea Garden in 2020.

- Margaret Hayward Complex, 1016 Laguna Street, San Francisco, CA 94102

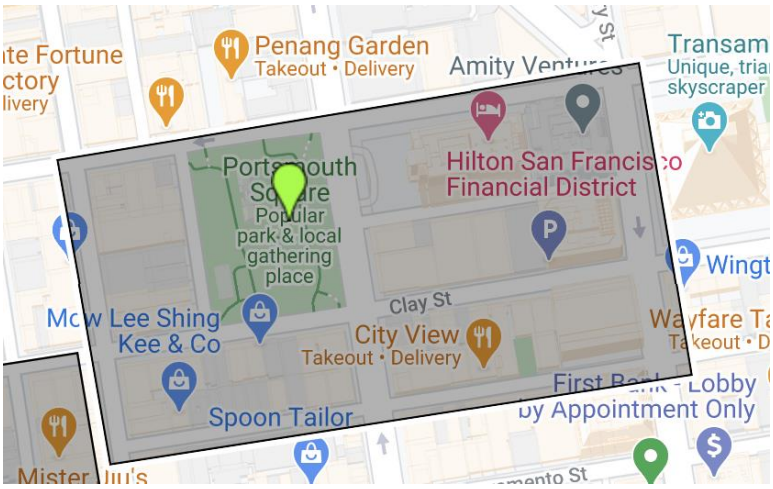


[Image description: The image shows a screenshot of a mapped area around the Margaret Hayward Complex.]

Incident Category	Number of SFPD Incidents	Percent
Arson	2	0.008511
Assault	14	0.059574
Burglary	11	0.046809
Disorderly Conduct	5	0.021277
Drug Offense	9	0.038298
Family Offense	2	0.008511
Fraud	4	0.017021
Larceny Theft	52	0.221277
Lost Property	3	0.012766
Malicious Mischief	17	0.07234
Miscellaneous Investigation	2	0.008511
Missing Person	2	0.008511
Motor Vehicle Theft	17	0.07234
Non-Criminal	16	0.068085
Offences Against The Family And Children	14	0.059574
Other	8	0.034043
Other Miscellaneous	24	0.102128
Other Offenses	1	0.004255
Recovered Vehicle	1	0.004255
Robbery	4	0.017021
Stolen Property	1	0.004255
Suspicious Occ	5	0.021277
Traffic Collision	1	0.004255
Traffic Violation Arrest	5	0.021277

Warrant	13	0.055319
Weapons Carrying Etc	1	0.004255
Weapons Offense	1	0.004255

- Portsmouth Square, 745 Kearny Street between Clay Street and, Washington Street, San Francisco, CA 94108

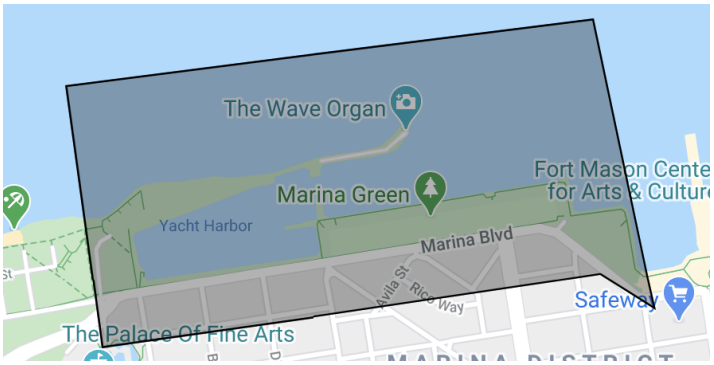


[Image description: The image shows a screenshot of a mapped area around Portsmouth Square.]

Incident Category	Number of SFPD Incidents	Percent
Arson	2	0.008163
Assault	20	0.081633
Burglary	13	0.053061
Courtesy Report	2	0.008163
Disorderly Conduct	1	0.004082
Drug Offense	2	0.008163
Fire Report	1	0.004082
Forgery And Counterfeiting	1	0.004082
Fraud	15	0.061224
Larceny Theft	59	0.240816
Lost Property	7	0.028571
Malicious Mischief	20	0.081633
Miscellaneous Investigation	1	0.004082
Missing Person	9	0.036735
Motor Vehicle Theft	11	0.044898
Non-Criminal	24	0.097959
Offences Against The Family And Children	4	0.016327
Other	6	0.02449
Other Miscellaneous	22	0.089796
Other Offenses	4	0.016327

Robbery	5	0.020408
Suspicious Occ	5	0.020408
Traffic Collision	1	0.004082
Traffic Violation Arrest	2	0.008163
Vandalism	2	0.008163
Warrant	4	0.016327
Weapons Carrying Etc	1	0.004082
Weapons Offense	1	0.004082

- San Francisco Marina, San Francisco, CA

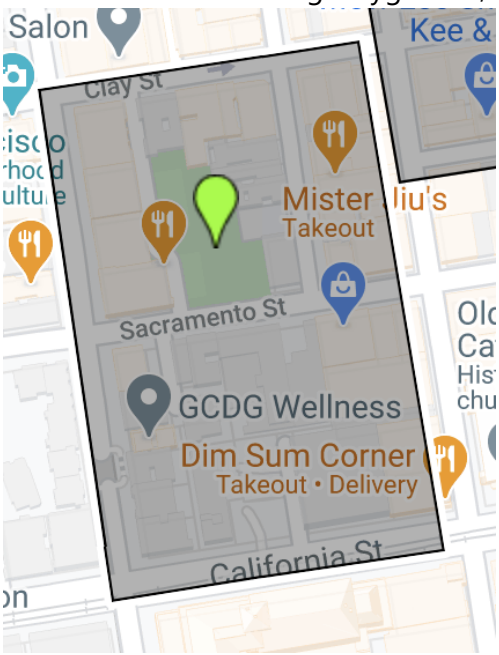


[Image description: The image shows a screenshot of a mapped area around the San Francisco Marina.]

Incident Category	Number of SFPD Incidents	Percent
	1	0.002801
Arson	1	0.002801
Assault	7	0.019608
Burglary	10	0.028011
Disorderly Conduct	3	0.008403
Drug Offense	2	0.005602
Family Offense	1	0.002801
Fraud	6	0.016807
Larceny Theft	212	0.593838
Lost Property	9	0.02521
Malicious Mischief	16	0.044818
Miscellaneous Investigation	1	0.002801
Missing Person	1	0.002801
Motor Vehicle Theft	12	0.033613
Non-Criminal	25	0.070028
Offences Against The Family And Children	5	0.014006
Other	1	0.002801
Other Miscellaneous	19	0.053221

Other Offenses	2	0.005602
Recovered Vehicle	1	0.002801
Robbery	6	0.016807
Stolen Property	3	0.008403
Suspicious Occ	5	0.014006
Traffic Violation Arrest	1	0.002801
Warrant	3	0.008403
Weapons Carrying Etc	1	0.002801
Weapons Offense	3	0.008403

- Willie "Woo Woo" Wong Playground, 830 Sacramento Street, San Francisco, CA 94108

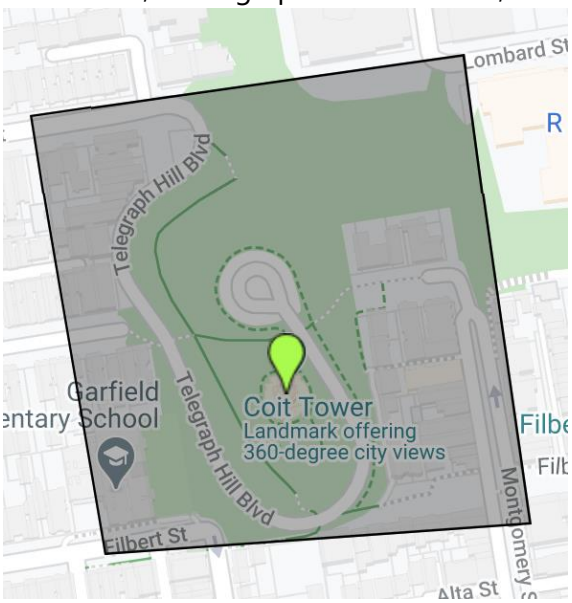


[Image description: The image shows a screenshot of a mapped area around the Willie “Woo Woo” Wong Playground.]

Incident Category	Number of SFPD Incidents	Percent
Assault	6	0.050847
Burglary	11	0.09322
Disorderly Conduct	1	0.008475
Fraud	4	0.033898
Larceny Theft	28	0.237288
Lost Property	1	0.008475
Malicious Mischief	10	0.084746
Miscellaneous Investigation	5	0.042373
Missing Person	1	0.008475
Motor Vehicle Theft	3	0.025424
Non-Criminal	7	0.059322

Offences Against The Family And Children	3	0.025424
Other	5	0.042373
Other Miscellaneous	8	0.067797
Other Offenses	1	0.008475
Robbery	6	0.050847
Suspicious	1	0.008475
Suspicious Occ	10	0.084746
Traffic Violation Arrest	2	0.016949
Warrant	5	0.042373

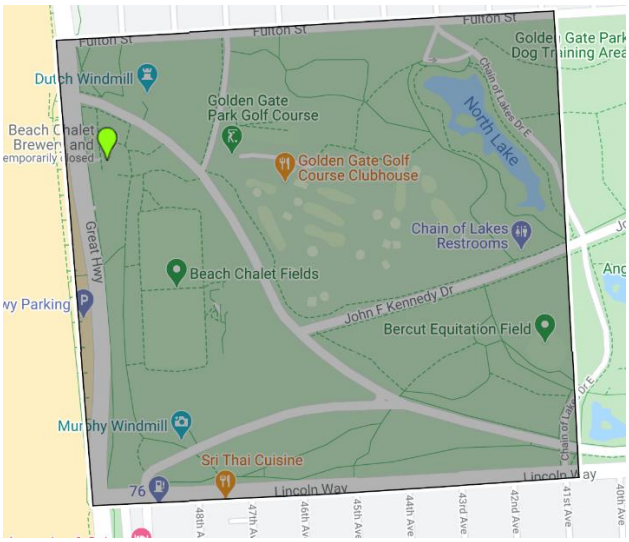
- Coit Tower, 1 Telegraph Hill Boulevard, San Francisco, CA 94133



[Image description: The image shows a screenshot of a mapped area around Coit Tower.]

Incident Category	Number of SFPD Incidents	Percent
Arson	1	0.032258
Assault	1	0.032258
Burglary	5	0.16129
Disorderly Conduct	1	0.032258
Larceny Theft	9	0.290323
Malicious Mischief	1	0.032258
Motor Vehicle Theft	5	0.16129
Non-Criminal	2	0.064516
Other Miscellaneous	5	0.16129
Robbery	1	0.032258

- Beach Chalet Soccer Field, 1400-1598 John F Kennedy Dr, San Francisco, CA 94121

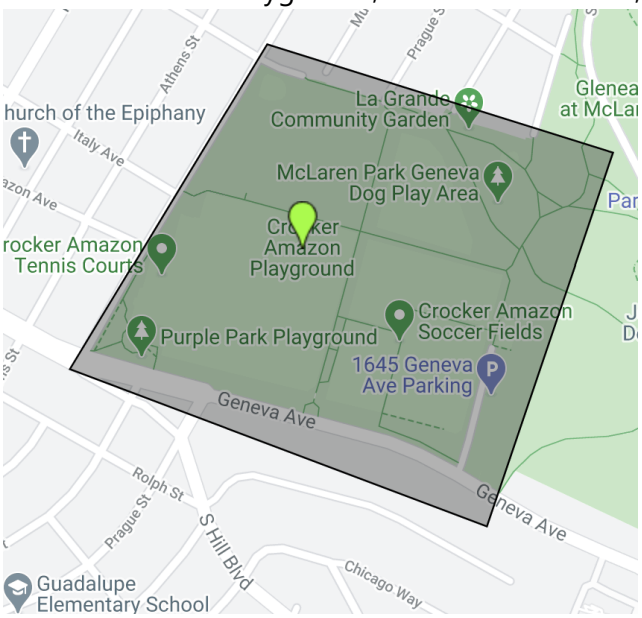


[Image description: The image shows a screenshot of a mapped area around the Beach Chalet Soccer Field.]

Incident Category	Number of SFPD Incidents	Percent
	1	0.003058
Arson	1	0.003058
Assault	17	0.051988
Burglary	14	0.042813
Disorderly Conduct	6	0.018349
Drug Offense	4	0.012232
Embezzlement	1	0.003058
Fraud	10	0.030581
Larceny Theft	134	0.409786
Lost Property	4	0.012232
Malicious Mischief	16	0.04893
Miscellaneous Investigation	2	0.006116
Missing Person	3	0.009174
Motor Vehicle Theft	39	0.119266
Non-Criminal	30	0.091743
Offences Against The Family And Children	7	0.021407
Other	1	0.003058
Other Miscellaneous	18	0.055046
Other Offenses	1	0.003058
Robbery	4	0.012232
Suspicious Occ	6	0.018349
Traffic Collision	1	0.003058
Vandalism	1	0.003058
Warrant	3	0.009174

Weapons Carrying Etc	1	0.003058
Weapons Offense	2	0.006116

- Crocker Amazon Playground, 799 Moscow Street, San Francisco, CA 94112



[Image description: The image shows a screenshot of a mapped area around the Crocker Amazon Playground.]

Incident Category	Number of SFPD Incidents	Percent
	1	0.013333
Assault	7	0.093333
Burglary	2	0.026667
Disorderly Conduct	4	0.053333
Fraud	1	0.013333
Larceny Theft	9	0.12
Lost Property	1	0.013333
Malicious Mischief	4	0.053333
Miscellaneous Investigation	2	0.026667
Missing Person	1	0.013333
Motor Vehicle Theft	7	0.093333
Non-Criminal	8	0.106667
Other	1	0.013333
Other Miscellaneous	7	0.093333
Other Offenses	1	0.013333
Robbery	8	0.106667
Stolen Property	1	0.013333
Suspicious Occ	2	0.026667

Warrant	5	0.066667
Weapons Carrying Etc	1	0.013333
Weapons Offense	2	0.026667

- Golden Gate Park Maintenance Yard, San Francisco, CA
  No location information could be found for this site.

Information on crime statistics in 2020 in this area is provided by the San Francisco Police Department. Statistics are taken from a 1-block radius around the location of cameras. All information is obtained through the San Francisco Open Data Portal: https://datasf.org/opendata/

In addition, the department maintains an internal incident log which is available on request.

Surveillance Impact Report

Residential Rent Stabilization and Arbitration Board
Security Cameras

As required by San Francisco Administrative Code, Section 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 surveillance cameras.

DESCRIPTION OF THE TECHNOLOGY

The Residential Rent Stabilization and Arbitration Board's (RNT) mission is to protect tenants from excessive rent increases and unjust evictions, while assuring landlords fair and adequate rents; to provide fair and even-handed treatment for both tenants and landlords through efficient and consistent administration of the rent law; to promote the preservation of sound, affordable housing; and to maintain the ethnic and cultural diversity that is unique to San Francisco

In line with its mission, the Department shall use security cameras only for the following authorized purposes:

Authorized Use(s):

1. Live monitoring.
2. Recording of video and images in the event of an incident.
3. Reviewing camera footage.
4. Providing video footage/images to law enforcement or other authorized persons following an incident.

Prohibited use cases include any uses not stated in the Authorized Use Case section.

Further, processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, gender, gender identity, disability status, or an individual person's sex life or sexual orientation, and the processing of genetic data and/or biometric data for the purpose of uniquely identifying an individual person shall be prohibited.

Department technology may be deployed in the following locations, based on use case:

- The Lobby Cameras are used to protect against harassment, theft, safety or vandalism of the Rent Board's lobby area, which includes publicly accessible computers and other City owned assets.

Surveillance Oversight Review Dates
COIT Review: March 18, 2021
Board of Supervisors Review: TBD

Technology Details

The following is a product description:

Q-See QT454 - This DVR uses high-performance video processing chips and an embedded Linux operating system for quality image recording and ease of use. It utilizes numerous advanced technologies including the industry-standard H.264 codec to deliver high-quality, smooth videos and dual stream capability for remote viewing. A SATA hard-drive interface offers upgradability and VGA output allows users to connect to any standard TV or monitor for viewing.

A. How It Works

To function, Lobby Cameras record video of the Rent Board's lobby and entrance. The video is stored for 7 days prior to deletion. In the event of an incident of harassment, staff safety, theft or vandalism, RNT staff will review the recorded video to determine if it has captured the incident.

Data collected or processed by security cameras will not be handled or stored by an outside provider or third-party vendor on an ongoing basis. The Department will remain the sole Custodian of Record.

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 security cameras has the following benefits for the residents of the City and County of San Francisco:

▪	Education	
▪	Community Development	
X	Health	Protect safety of staff, patrons, and facilities while promoting an open and welcoming environment.
▪	Environment	

X	Criminal Justice	Review video footage after a security incident; provide video evidence to law enforcement or the public upon request by formal process, order, or subpoena.

- Jobs
- Housing
- Other

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:

Administrative Safeguards: The data can only be accessed by 0961 Department Head and a vendor in case of assistance in fixing/troubleshooting or to retrieve at the direction of the Department Head.

Technical Safeguards: The Lobby Camera data is on a closed system not connected to other City data networks.

Physical Safeguards: Data can only be accessed at the Rent Board's Office at 25 Van Ness Ave., Ste. 320, SF, CA

The Rent Arbitration Board strives to mitigate all potential civil rights impacts through responsible technology and associated data use policies and procedures, and intends to use Lobby Cameras and their associated data exclusively for aforementioned authorized uses cases. All other uses, including surveillance of San Francisco residents or groups, are expressly prohibited. The Lobby Cameras are used at the department's offices to monitor entrance and exit points and the lobby in case of a break in, for staff safety, and to monitor in case there is an allegation of any other illegal activity. They capture footage of the interior of the site, and do regularly capture members of the public who come into the department's offices. The use of Lobby Cameras may result in dignity loss, discrimination or loss of liberty. The quality of the video captured through the CICs may vary in quality due to lighting, motion or other factors. Poor quality video may lead to mis-identification. Conversely, the video may not correctly convey intent and viewers may interpret actions captured as threatening or menacing which may have a more benign interpretation. For example, the Lobby Cameras may capture a person approaching a facility with a brick and assume they intend to cause physical damage to the property when there may be an alternative explanation. That person may be correctly identified as an employee or member of the public, but subsequently subjected to investigation and possibly arrest. To protect camera data from potential breach, misuse or abuse that may result in civil rights impacts, data is maintained on secure, department-owned DVR. Only persons authorized to utilize the raw data may access the information and are required to maintain records of access by completing the community security cameras data access log described in section 3. Data stored on the DVR is deleted every seven

days, and sharing with building management or law enforcement pursuant to policy. Vendor has limited access to data only to install and maintain the cameras.

C. Fiscal Analysis of Costs and Benefits

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

Benefit		Description
X	Financial Savings	Department Security Camera Systems will save on building or patrol officers.
X	Time Savings	Department Security Camera Systems will run 24/7, thus eliminating building or patrol officer supervision
X	Staff Safety	Security cameras help identify violations of Department Patron Code of Conduct and provide assurance that staff safety is emphasized and will be protected at their place of employment.
X	Data Quality	Security cameras run 24/7/365 so full-time staffing is not required to subsequently review footage of security incidents. Data resolution can be set by level and is currently set to high resolution.

Number of FTE (new & existing)	0.05 FTE	
Classification	NA - Outside vendor if needed.	
	Annual Cost	***One-Time Cost***
Software		
Hardware/Equipment		$700
Professional Services		
Training		
Other		
Total Cost		***$700***

The Department funds its use and maintenance of the surveillance technology through

- The Board is an enterprise department funded by the Rent Board fee, and receives no general fund support. The DVR system costs a minimal amount.

COMPARISON TO OTHER JURISDICTIONS

Security Cameras are currently utilized by other governmental entities for similar purposes.

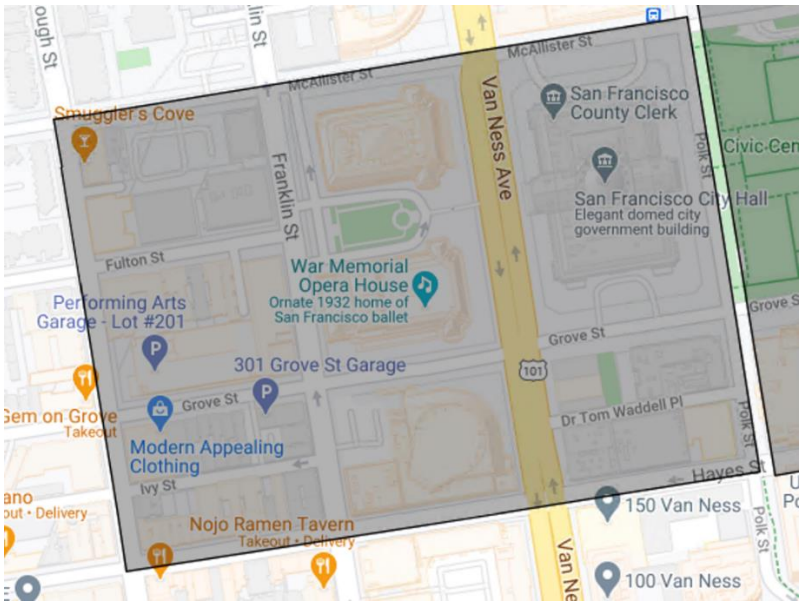
Appendix A: Crime Statistics

Department: Rent Board

Section 19B requires each department in their Surveillance Impact Report to respond to the following question if applicable, "the general location(s) [of the surveillance technology] may be deployed and crime statistics for any location(s)."

The Rent Board operates a total of 3 Security Cameras at the following locations:

- 25 Van Ness Avenue, Suite 320, San Francisco, CA



[Image description: The image shows a screenshot of a mapped area around the 25 Van Ness Avenue building.]

Incident Category	Number of SFPD Incidents	Percent
Arson	1	0.006098
Assault	7	0.042683
Burglary	10	0.060976
Disorderly Conduct	1	0.006098
Drug Offense	1	0.006098
Embezzlement	1	0.006098
Fraud	7	0.042683
Larceny Theft	91	0.554878
Lost Property	1	0.006098
Malicious Mischief	12	0.073171
Missing Person	2	0.012195
Motor Vehicle Theft	5	0.030488

Non-Criminal	4	0.02439
Offences Against The Family And Children	4	0.02439
Other Miscellaneous	6	0.036585
Recovered Vehicle	2	0.012195
Robbery	2	0.012195
Suspicious Occ	3	0.018293
Traffic Violation Arrest	2	0.012195
Warrant	2	0.012195

Information on crime statistics in 2020 in this area is provided by the San Francisco Police Department. Statistics are taken from a 1-block radius around the location of cameras. All information is obtained through the San Francisco Open Data Portal: https://datasf.org/opendata/

In addition, the department maintains an internal incident log which is available on request.

Surveillance Impact Report

War Memorial
Security Cameras

As required by San Francisco Administrative Code, Section 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 the Veterans Building Surveillance Camera System.

DESCRIPTION OF THE TECHNOLOGY

The San Francisco War Memorial & Performing Arts Center manages, maintains and operates safe, accessible, world-class venues to promote cultural, educational, and entertainment opportunities in a cost-effective manner for enjoyment by the public, while best serving the purposes and beneficiaries of the War Memorial Trust.

In line with its mission, the War Memorial Security Division utilizes the Veterans Building Surveillance Camera System to increase security officer capacity directly related to public safety. The technology enhances the Department's ability to provide a safe and welcoming environment to patrons, visitors and staff.

War Memorial shall use the Veterans Building Surveillance Camera System only for the following authorized purposes:

Authorized Use(s):

1. Live monitoring.
2. Recording of video and images in the event of an incident.
3. Reviewing camera footage.
4. Providing video footage/images to law enforcement or other authorized persons following an incident.

Prohibited use cases include any uses not stated in the Authorized Use Case section.

Further, processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, gender, gender identity, disability status, or an individual person's sex life or sexual orientation, and the processing of genetic data and/or biometric data for the purpose of uniquely identifying an individual person shall be prohibited.

Surveillance Oversight Review Dates
COIT Review: March 18, 2021
Board of Supervisors Review: TBD

Technology Details

War Memorial surveillance cameras are located in public areas of all floors in the Veterans Building. Additional cameras are planned for public interior and exterior areas of the Veterans Building.

The following is a product description of the Veterans Building Surveillance Camera System:

Cameras: Mobotix S15D FlexMount Dual Camera

Server: Rasilient ApplianceStor90

Software: Avigilon Control Center Server v6.8.6.4.

A. How It Works

The technology's primary functions are to provide live views and record video footage to a dedicated, secure server. The system is comprised of multiple cameras connected by data cables and infrastructure to the server. The footage is recorded on the server and stored for a limited amount of time.

Data collected or processed by the Veterans Building Surveillance Camera System will not be handled or stored by an outside provider or third-party vendor on an ongoing basis. The Department will remain the sole Custodian of Record.

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 security cameras has the following benefits for the residents of the City and County of San Francisco:

- Education
- Community Development

X	Health	Protect safety of staff, patrons, and facilities while promoting an open and welcoming environment.

- Environment

X	Criminal Justice	Review video footage after a security incident; provide video evidence to law enforcement or the public upon request by formal process, order, or subpoena.

- Jobs
- Housing
- Other

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:

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

War Memorial believes the Veterans Building Surveillance Camera System poses potential risks to civil liberties in respect to dignity loss and loss of liberty.

An individual could be embarrassed or experience emotional distress if cameras capture behaviors, appearances, or circumstances by which they might feel humiliated. Examples include views of someone exhibiting an emotional outburst, a person's clothing or hair being disheveled, or someone having their physique ridiculed or leered at. Risks for loss of dignity are reduced by restricting access to live views, as well as recorded footage, to a limited number of trained Security staff. In addition, the cameras do not pan, tilt or zoom, thus removing possible temptation for system operators to use those features to follow or enhance views of individuals. Audio is also not recorded or enabled.

Loss of liberty could potentially occur if a person were to be misidentified as the perpetrator of a crime or other incident, making them subject to wrongful arrest. An innocent person might be similar in appearance to someone who committed an offense. Surveillance images could reinforce other circumstantial evidence tying the wrong person to a criminal incident. As an example, someone might be wearing clothing like clothing worn by someone seen leaving an office where a theft had just occurred. Loss of liberty risks due to misidentification of a subject in surveillance video is mitigated by restricting access to live views and recorded footage to a limited number of trained personnel.

C. Fiscal Analysis of Costs and Benefits

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

Benefit		**Description**
X	Financial Savings	Department Security Camera Systems will save on building or patrol officers.
X	Time Savings	Department Security Camera Systems will run 24/7, thus eliminating building or patrol officer supervision

X	Staff Safety	Security cameras help identify violations of Department Patron Code of Conduct and provide assurance that staff safety is emphasized and will be protected at their place of employment.
X	Data Quality	Security cameras run 24/7/365 so full-time staffing is not required to subsequently review footage of security incidents. Data resolution can be set by level and is currently set to high resolution.

Number of FTE (new & existing)	.25 of 1 8207's time 2.5% of 1 1093's time (est. 1 hour per week)	
Classification	8207 and 1093	
	Annual Cost	***One-Time Cost***
Total Salary & Fringe	*$32,697*	
Software		$4,260
Hardware/Equipment		$14,730
Professional Services		$5,520
Training		*$570*
Other		$140,000
Total Cost		***$197,777***

The Department funds its use and maintenance of the surveillance technology through

The Veterans Building Surveillance Camera System is an existing system that was installed during the Veterans Building Seismic Retrofit and Renovation Project completed in 2015. A subsequent project to upgrade the Surveillance Camera server and software was completed in 2018. Of the Total Cost of $197,777, $165,080 has already been expended. Salary & Fringe costs of $32,697 are ongoing annual costs. The War Memorial funds the ongoing costs associated with this system through its Annual Operating Budget.

COMPARISON TO OTHER JURISDICTIONS

Surveillance Cameras are currently utilized by other governmental entities for similar purposes.

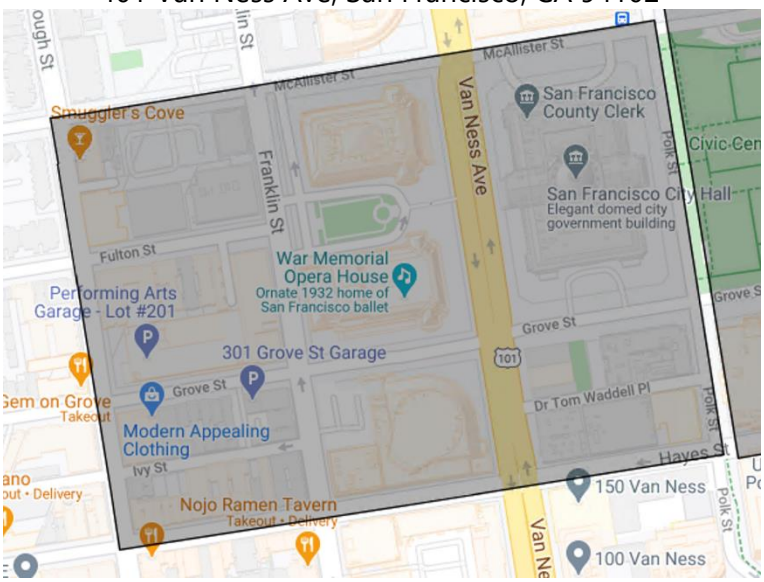
Appendix A: Crime Statistics

Department: War Memorial

Section 19B requires each department in their Surveillance Impact Report to respond to the following question if applicable, "the general location(s) [of the surveillance technology] may be deployed and crime statistics for any location(s)."

The War Memorial Department operates a total of 27 Security Cameras at the following location:

- 401 Van Ness Ave, San Francisco, CA 94102



[Image description: The image shows a screenshot of a mapped area around the War Memorial building.]

Incident Category	Number of SFPD Incidents	Percent
	1	0.001701
Arson	1	0.001701
Assault	29	0.04932
Burglary	65	0.110544
Courtesy Report	1	0.001701
Disorderly Conduct	2	0.003401
Drug Offense	5	0.008503
Embezzlement	1	0.001701
Fire Report	1	0.001701
Forgery And Counterfeiting	1	0.001701
Fraud	10	0.017007
Larceny Theft	250	0.42517
Liquor Laws	1	0.001701
Lost Property	15	0.02551

Malicious Mischief	67	0.113946
Miscellaneous Investigation	3	0.005102
Missing Person	3	0.005102
Motor Vehicle Theft	30	0.05102
Non-Criminal	15	0.02551
Offences Against The Family And Children	7	0.011905
Other	8	0.013605
Other Miscellaneous	32	0.054422
Other Offenses	2	0.003401
Recovered Vehicle	1	0.001701
Robbery	5	0.008503
Stolen Property	3	0.005102
Suspicious Occ	4	0.006803
Traffic Violation Arrest	5	0.008503
Vandalism	2	0.003401
Vehicle Impounded	1	0.001701
Warrant	10	0.017007
Weapons Offense	7	0.011905

Information on crime statistics in this are is provided by the San Francisco Police Department. All information obtained through the San Francisco Open Data Portal: https://datasf.org/opendata/

In addition, the department maintains an internal incident log which is available on request.

Surveillance Technology Policy

Department of Technology
Security Cameras

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 Department's Security Camera System 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

The Surveillance Technology Policy ("Policy") defines the manner in which the Security Camera System (fixed or mobile) will be used to support department operations.

This Policy applies to all department personnel that use, plan to use, or plan to secure Security Camera Systems, 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

City departments using this policy will limit their use of Security Camera to the following authorized use cases and requirements listed in this Policy.

Authorized Use(s):

1. Live monitoring.
2. Recording of video and images.
3. Reviewing camera footage in the event of an incident.
4. Providing video footage/images to law enforcement or other authorized persons following an incident or upon request.

Prohibited use cases include any uses not stated in the Authorized Use Case section.

Departments may use information collected from security cameras only for legally authorized purposes, and may not use that information to unlawfully discriminate against people based on race, ethnicity, political opinions, religious or philosophical beliefs, trade union membership, gender, gender identity, disability status, sexual orientation or activity, or genetic and/or biometric data. Additionally, departments may not use automated systems to scan footage and identify individuals based on any of the categories listed in the preceding sentence.

All data collected by surveillance cameras is the exclusive property of the City and County of San Francisco. Under no circumstance shall collected data be sold to another entity.

Surveillance Oversight Review Dates
COIT Review: March 18, 2021
Board of Supervisors Review: TBD

BUSINESS JUSTIFICATION

In support of Department operations, Security Cameras promise to help with:

	▪ Education	
	▪ Community Development	
X	Health	Protect safety of staff, patrons, and facilities while promoting an open and welcoming environment.
	▪ Environment	
X	Criminal Justice	Review video footage after a security incident; provide video evidence to law enforcement or the public upon request by formal process, order, or subpoena.
	▪ Jobs	
	▪ Housing	
X	Other	Better management of city assets by leveraging remote condition assessment. Improvement of overall situational awareness.

In addition, the following benefits are obtained:

Benefit		Description
X	Financial Savings	Department Security Camera Systems will save on building or patrol officers.
X	Time Savings	Department Security Camera Systems will run 24/7, thus decreasing or eliminating building or patrol officer supervision
X	Staff Safety	Security cameras help identify violations of City Employee's Code of Conduct, Building Rules and Regulations, and City, State and Federal law and provide assurance that staff safety is emphasized and will be protected at their place of employment.
X	Data Quality	Security cameras run 24/7/365 so full-time staffing is not required to subsequently review footage of security incidents. Data resolution can be set by level and is currently set to high resolution.
X	Service Levels	Security cameras will enhance effectiveness of incident response and result in improved level of service.

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 security cameras must be kept up-to-date and maintained.

Data Collection: Department shall only collect data required to execute the authorized use case. 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 types:

Data Type(s)	*Format(s)*	*Classification*
Video and Images	MP4, AVI, MPEG	Level 3
Date and Time	MP4 or other format	Level 3
Geolocation data	TXT, CSV, DOCX	Level 3

Notification: Departments shall notify the public of intended 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. Department notifications shall identify the type of technology being used and the purpose for such collection.

The Department's public notice will include the following items:

X Information on the surveillance technology

X Description of the authorized use

- Type of data collected
- Will persons be individually identified
- Data retention

X Department identification

X Contact information

Access:	Prior to accessing or using data, authorized individuals receive training in system access and operation, and instruction regarding authorized and prohibited uses. Access to live views and recorded footage is restricted to specific trained personnel. Recorded footage is accessed only in response to an incident. Details on department staff and specific access are available in Appendix A.
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. Departments shall, at minimum, apply the following safeguards to protect surveillance technology information from unauthorized access and control, including misuse: - Encryption: Data retained by the Department will be encrypted. Raw data may be retained by the Department only for the authorized use case of sharing with law enforcement or the public. - Storage: Any use of a third-party service provider must meet City's cyber security requirements. - Audits: A data access log will be maintained by the Department for all Security Camera data that is processed and utilized. This log will include but is not limited to the following: date/time data was originally obtained/collected, reasons/intended use for data, department requesting data, date/time of access of raw data, outcome of data processing, as well as date processed data was delivered to users.
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 will endeavor to ensure that other agencies or departments that may receive data collected by their own Security Camera Systems will act in conformity with this Surveillance Technology 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. Each department that believes another agency or department receives or may receive data collected from its use of Security Cameras should consult with its assigned Deputy City Attorney regarding their response.

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

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

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.

The Department may share Security Camera footage with the following entities:

A. Internal Data Sharing:

In the event of an incident, Security Camera images may be live-streamed or shared by alternative methods to the following agencies:

- Within the operating Department
- Police
- City Attorney
- District Attorney
- Sheriff
- On request following an incident.

Data sharing occurs at the following frequency:

- As needed.

B. External Data Sharing:

- Other local law enforcement agencies

Data sharing occurs at the following frequency:

- As needed.

Data Retention:	Department may store and retain raw PII data only as long as necessary to accomplish a lawful and authorized purpose. Department data retention standards should align with how the department prepares its financial records and should be consistent with any relevant Federal Emergency Management Agency (FEMA) or California Office of Emergency Services (Cal OES) sections. The Department's data retention period and justification are as follows: - Security Camera data will be stored for one (1) year to be available to authorized staff for operational necessity and ready reference. If data is associated with an incident, it may be kept for longer than the standard retention period. - Justification: This retention period conforms with the available server system storage space and allows for ample time for security staff to review footage related to security incidents and/or external requests for records. 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.) X Department of Technology Data Center X Software as a Service Product X Cloud Storage Provider
Data Disposal:	Upon completion of the data retention period, Department shall dispose of data in the following manner: - Automatic overwrite of all existing files when standard data retention period ends. This may take the form of a delete/reformat, wipe, overwrite of existing data, or degaussing.
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 must receive training on data security policies and procedures. - Annual cybersecurity training (COIT Policy Link)

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.

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.

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.
Sensitive Data:	Data intended for release on a need-to-know basis. Data regulated by privacy laws or regulations or restricted by a regulatory agency or contract, grant, or other agreement terms and conditions.

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."

Appendix A: Department Specific Responses
Department: Asian Art Museum

1. A description of the product, including vendor and general location of technology.
    - CCTV product is Exacqvision, vendor for support is Pacific Technology CCTV, located in Santa Rosa. Cameras are located in both public facing and staff only areas both inside the museum and covering exterior areas.
2. The specific categories and titles of individuals who are authorized by the Department to access or use the collected information
    - Security Director (0922) – full access
    - Security Supervisors (8228) – full access
    - Security staff (8226 and 8202) – view access with access to recording in the event of an incident when supervisors are not present
3. What procedures will be put in place by which members of the public can register complaints or concerns, or submit questions about the deployment or use of a specific Surveillance Technology, and how the Department will ensure each question and complaint is responded to in a timely manner.
    - Information will be posted on the Asian Art Museum website. The Security Director or designee will respond to questions, complaints, and concerns in a timely manner.
        - securitymanagers@asianart.org
4. Specific details on where data will be stored (local, DT, SaaS, Cloud Storage) including name of vendor and retention period.
    - Data is stored on servers within the museum main server room. Retention period is variable based on motion recording and space on each server. Approximately 6 months retention for each server.
5. Is a subpoena required before sharing with law enforcement?
    - No

Appendix A: Department Specific Responses

Department: City Adminstrator's Office - Real Estate Division

1. A description of the product, including vendor and general location of technology.

   All RED systems are self-contained and do not share information or data with any other departments or agencies.

Building	**Video Surveillance System**	**Number of Cameras**
1 Newhall (Medical Examiner)	Avigilon	51
1 South Van Ness	Avigilon	34
1650 Mission	Avigilon	31
25 Van Ness	Avigilon	20
450 Toland (Central Shop)	Avigilon	6
555 Selby (Central Shop)	Avigilon	15
City Hall	Avigilon	163
49 South Van Ness	Avigilon	128
ACC 1419 Bryant	Avigilon	57
850 Bryant	Avigilon	6

2. The specific categories and titles of individuals who are authorized by the Department to access or use the collected information.

   - Monitoring (Viewing Live Feed) –

- HOJ – Limited to Basement Door, Freight Hallway, Outside Basement Area – Campus Superintendent, Boiler Watch Engineering, Engineering staff (24/7)

- ACC – Security Guard

- City Hall: Deputy Sheriff

- Other RED Facilities: Deputy Sheriff, Security Guard, Building Manager

- Review of Recorded Video –

    - City Hall: Sheriff, Media Services staff upon approval by Sheriff's legal counsel for City Hall

    - OCME: Deputy City Administrator

    - ACC – RED Media Services upon approval by Department head

    - Other RED Facilities: Security, District General Manager, Campus Superintendent, Building Manager, RED Department head upon approval by Department head

- Export recorded video—

    - City Hall: Media Services staff upon approval by Sheriff's legal counsel for City Hall

    - OCME: Deputy City Administrator

    - Other RED Facilities: Media Services staff, District General Manager, Campus Superintendent, Building Manager - - Upon approval of Director, or designee, after consultation with City Attorney's Office

3. What procedures will be put in place by which members of the public can register complaints or concerns, or submit questions about the deployment or use of a specific Surveillance Technology, and how the Department will ensure each question and complaint is responded to in a timely manner.

Any complaints, questions, and concerns by members of the public regarding or relating RED's surveillance equipment, deployment and use of Surveillance Technology will be forwarded to the applicable Building Manager and copied to the applicable District General Manager. Responses to same will be drafted by the Building Manager with review by the District General Manager, and by the Director, or their designee, if warranted.

4. Specific details on where data will be stored (local, DT, SaaS, Cloud Storage) including name of vendor and retention period.
    - City Hall – Avigilon local server/recorder in AV server room
    - Medical Examiner – Avigilon local server/recorder in MPOE at 1 New Hall
    - One South Van Ness – Avigilon local server/recorder in server room at 1 South Van Ness
    - 1650 Mission – Avigilon local Server/Recorder – MPOE at 1650 Mission
    - Central Shop #1- Avigilon local server/recorder in server room at 555 Selby
    - Central Shop #2 - Avigilon local server/recorder in server room at 450 Toland
    - 25 Van Ness – Avigilon local server/recorder in room 400 at 25 Van Ness
    - 49 South Van Ness – Avigilon local server/recorder in server room at 49 South Van Ness
    - 850 Bryant (HOJ) – Microbiz local server/recorder in server room at HOJ

5. Is a subpoena required before sharing with law enforcement?
    - No.

Appendix A: Department Specific Responses
Department: San Francisco International Airport

1. A description of the product, including vendor and general location of technology.
   The Airport uses Verint Video Management Software (VMS) and, primarily, Pelco Analog and Digital Pan-Tilt-Zoom (PTZ) and fixed cameras. The cameras are installed in public areas of the Airport. Specific to this submission, the cameras are located pre-security.

   The Verint system is a closed system, running on a security local area network that is not exposed to the internet.

2. The specific categories and titles of individuals who are authorized by the Department to access or use the collected information

   - *9202 911 Dispatcher*
   - *9203 911 Dispatch Supervisor*
   - *9212 Security Operations Center (SOC) Analyst*
   - *9213 Airfield Safety Officer*
   - *9220 SOC Supervisor*
   - *9221 Airport Operations Supervisor*
   - *Air Train Staff and Contractors*
   - *Aviation Security System MX Contractors*
   - *Ground Transportation Unit*
   - *Parking Management*
   - *SFPD-AB*

3. What procedures will be put in place by which members of the public can register complaints or concerns, or submit questions about the deployment or use of a specific Surveillance Technology, and how the Department will ensure each question and complaint is responded to in a timely manner.

   Public question and complaint can be submitted via the:

   - *Airport Guest Services (Contact SFO)*
   - *Airport public email, phone, or website ((Contact SFO), or*
   - *Airport Commission meetings (How to Address the Commission)*

4. Specific details on where data will be stored (local, DT, SaaS, Cloud Storage) including name of vendor and retention period.

   Data is in local server for 45 days then video files are transferred to Amazon Web Services for up to 1 year and files are deleted after 320 days based on lifecycle policy in AWS.

5. Is a subpoena required before sharing with law enforcement?

   - No

6. Questions & Concerns

- *In Authorized Use(s) - #3 "incident" should be defined*
- *In Notification – Admin Code Section 19.5 does not apply to Airport. Airport does not intend to post signage at location of each camera. However, Airport will publish public notice on its external website at www.flysfo.com.*
- *In Audits – "processed and utilized" is unclear. Alternate language suggested-- "shared with a 3rd party."*
- *In Audits –departments should not ask public record act requestors to provide their "reasons/intended use for data." "Intended use" is not a consideration when determining whether video footage is discloseable pursuant to a PRA request.*
- *In Data Sharing – 3rd procedure lists "Redact names, scrub faces…" The video is unalterable and names are not contained in the system. In addition, if video footage is subject to disclosure under PRA, scrubbing faces may be inappropriate unless privacy interests are implicated.*
- *In External Data Sharing – data collected can be requested under Public Records Request.*
- *In Data Retention – 1st paragraph states "…department prepares its financial records…" Not sure how this aligns with use of technology.*

Appendix A: Department Specific Responses
Department: Arts Commission

1. A description of the product, including vendor and general location of technology.

   Exacqvision servers. Axis, Hanwha and Samsung Cameras.

   - Main Gallery: 401 Van Ness Avenue, Suite 126 (6 cameras)
   - African American Art & Culture Complex: 762 Fulton Street (9 cameras)
   - Bayview Opera House: 4705 3rd Street (12 cameras – Exacqvision)
   - Mission Cultural Center for Latino Arts: 2868 Mission Street (28 cameras)
   - SOMArts: 934 Brannan Street (15 cameras – Exacqvision)

2. The specific categories and titles of individuals who are authorized by the Department to access or use the collected information
   - Arts Commission Staff:
     - Deputy Director of Programs (0923)
     - Director of Community Investments (1824)
     - Commission Secretary (1452)
     - Office Manager (1840)
   - Law enforcement

3. What procedures will be put in place by which members of the public can register complaints or concerns, or submit questions about the deployment or use of a specific Surveillance Technology, and how the Department will ensure each question and complaint is responded to in a timely manner.

   Public can inquire by contacting the Department directly (listed below) or through the City's Public Records Request process.

   401 Van Ness Avenue, Suite 325

   San Francisco, CA 94102

   (415)252-2255

   ART-Info@sfgov.org

4. Specific details on where data will be stored (local, DT, SaaS, Cloud Storage) including name of vendor and retention period.

   Local servers installed by Microbiz Security Company.

5. Is a subpoena required before sharing with law enforcement?

   - No

Appendix A: Department Specific Responses
Department: Child Support Services

1. A description of the product, including vendor and general location of technology.

Sonitrol is used to protect against unauthorized access to confidential customer data, and for customer and employee safety. Sonitrol monitors physical access to the facility where customer information resides to detect and respond to physical security incidents. Sonitrol surveillance cameras are installed at points of entry, public lobby, and Intake/Interview areas.

Sonitrol's verified alarms are sound-based – not motion-based – so when an alarm is triggered, our monitoring professionals can actually listen to determine whether a break-in is in progress, or whether a false alarm has occurred. If it is a break-in, we immediately dispatch police and relay real-time information to the responding officers. If it is a false alarm, we simply reset the system without bothering you or the police. Because of this ability to verify alarms, Sonitrol has the highest apprehension rate and the lowest false alarm rate in the industry.

2. The specific categories and titles of individuals who are authorized by the Department to access or use the collected information:

CCSF employees:

- *1094- IT Operations Support Admin IV*
- *1093 - IT Operations Support Admin III*
- *0922 – Manager I*
- *1244 - Sr. HR Analyst*
- *0952 - Deputy Director II*
- *0963 - Director III*
- *Contractors – Allied Security Guards*

SFPD – Southern Station:

- *Police Officers*

Departmental access is restricted to SFDCSS IT, SFDCSS Executive Management, SFDCSSHR and Allied Security Guards. Upon request, SFDCSS IT will provide access to

video footage to the above mentioned, as well as SFPD personnel. Executive Management, IT Manager/Security Officer or HR will request IT to review and provide video footage clip(s) of access point records in the event of a security or personnel incident. All staff and contractors are required to sign confidentiality forms annually, complete annual training and submit to Live Scan background checks to meet minimum employment requirements

3. What procedures will be put in place by which members of the public can register complaints or concerns, or submit questions about the deployment or use of a specific Surveillance Technology, and how the Department will ensure each question and complaint is responded to in a timely manner.

Customers can submit inquiries by telephone, letter, e-mail, facsimile, in person by visiting the office, or through the customer self-service website.

1. *Department of Child Support Services website: https://sfgov.org/dcss*
2. *Email to: sfdcss@sfgov.org*
3. *Phone: Call 311 or 1-866-901-3212*

Incoming communications from the public are reviewed by a supervisor for immediate handling or assigned for specialized review and resolution. Response time 24-48 hours. Communication information is captured and reported out in monthly management reports.

4. Specific details on where data will be stored (local, DT, SaaS, Cloud Storage) including name of vendor and retention period.

Technical Safeguards: SFDCSS follows restricted access protocols. Only IT Manager and IT Administrators have access to stored video footage and access point records. To protect data from potential breach, misuse or abuse that may result in impacts to the public, data is maintained on secure, department-owned servers. Server backup transmission is secured in accordance with Federal, State and local regulations. Only persons authorized to utilize the data may access the information and are required to maintain records of access. Data is provided to Executive Management, HR and SFPD upon request. Lobby Security Guard personnel have view-only access and monitor live footage during business hours.

Physical Safeguards: Data can only be accessed onsite at SFDCSS – 617 Mission Street or, in the event of a disaster, our secondary backup appliance is stored at SFO The data and data systems are secured during transmission and during rest in accordance with Federal, State and Local regulations.

5. Is a subpoena required before sharing with law enforcement?

    - No

Appendix A: Department Specific Responses
Department: Emergency Management

1. A description of the product, including vendor and general location of technology.

Cameras are deployed at all entry/exit points for the Combined Emergency Communications Center Building at 1011 Turk St. These include entry points and drive paths to underground parking garage, balcony space to the east face of the building, along the walkway of the west face of the building that is along Turk St, and side space area in the buffer protection zone adjacent to the REC facilities.

2. The specific categories and titles of individuals who are authorized by the Department to access or use the collected information

8300 SFSD, Cadet

8304 or 8504, SFSD Deputies

8306 SFSD Sr. Deputy

8308 SFSD, Sergeant

1842 DEM, Facility Manager

1093 DEM IT Administrator

Access to the system is through designated PC workstations with the appropriate manufacturer proprietary client software. The software requires an assigned User ID and Credential/password before accessing the video. Permissions to export the video are provided on individual account settings.

3. What procedures will be put in place by which members of the public can register complaints or concerns, or submit questions about the deployment or use of a specific Surveillance Technology, and how the Department will ensure each question and complaint is responded to in a timely manner.

DEM has the Custodian of Records function that allows the public to seek access to the cameras, or to register complaints or concerns. DEM's external affairs divisions handles public questions or concerns, including Sunshine Requests.

4. Specific details on where data will be stored (local, DT, SaaS, Cloud Storage) including name of vendor and retention period.

   There is currently a total of 28 cameras which most of them are fix point focus and 6 pan-tilt-zoom (PTZ) cameras. The video is recorded across two on-premise video servers

converting the analog video to digital file format utilizing video management software from Exacqvision.

5. Is a subpoena required before sharing with law enforcement?
    - No

Appendix A: Department Specific Responses
Department: Human Resources

1. A description of the product, including vendor and general location of technology.

   DHR's security cameras are non-zoom, fixed surveillance cameras connected to an OpenEye video recording system. The equipment was purchased more than ten years ago, and DHR was unable to locate purchase details.

2. The specific categories and titles of individuals who are authorized by the Department to access or use the collected information

   Video may only be accessed by DHR's 1042 IS Engineer, and only at the request of (a) the Human Resources Director; (b) the DHR Managing Deputy Director; or (c) the Department Personnel Officer.

3. What procedures will be put in place by which members of the public can register complaints or concerns, or submit questions about the deployment or use of a specific Surveillance Technology, and how the Department will ensure each question and complaint is responded to in a timely manner.

   Members of the public can register complaints/concerns or submit questions via calls or emails at 311.org. DHR's Director of Finance and Administration will work with the 311 Team to ensure that responses meet or exceed 311's standards.

4. Specific details on where data will be stored (local, DT, SaaS, Cloud Storage) including name of vendor and retention period.

   Data is only available to the IS Engineer, and is only accessible within the DHR Network. Access requires Local Area Network access, software installed, system configuration, software log-in, and passwords. The cameras record on a time loop that eventually overwrites itself. The recording system is not designed for permanent storage.

5. Is a subpoena required before sharing with law enforcement?

- No

Appendix A: Department Specific Responses
Department: Public Health

1. A description of the product, including vendor and general location of technology.

Lenel On-Guard/Prism and Johnson Control, Inc. P2000 System, Vendors: Comtel and Johnson Control, Inc.

Locations and Number of Cameras:

- Zuckerberg General Hospital: 381 Lenel On-Guard/Prism cameras
- Laguna Honda Hospital: 128 Johnson Control, Inc. cameras

2. The specific categories and titles of individuals who are authorized by the Department to access or use the collected information

- Comtel Service Technicians - Technical support (integrators/maintenance/repairs)
- San Francisco Sheriff Department - SOC
- 7262 Maintenance Planner
- 8300 Sheriff's Cadet
- 0953 Deputy Director III
- 8304 Deputy Sheriff
- 8306 Senior Deputy Sheriff
- 8308 Sheriff's Sergeant
- 8310 Sheriff's Lieutenant
- 8238 Public Safety Communications Dispatcher

3. What procedures will be put in place by which members of the public can register complaints or concerns, or submit questions about the deployment or use of a specific Surveillance Technology, and how the Department will ensure each question and complaint is responded to in a timely manner.

Complaints can be sent to Director of Security, Department of Public Health in accordance to the 2020 – SOP – SFDPH Records and Disclosure Policy. Contact information for complaints or concerns:

City and County of San Francisco
1001 Potrero Avenue
San Francisco, CA 94110
Office: 415-206-2577
Cell: 415 926-3669
basil.price@sfdph.org

4. Specific details on where data will be stored (local, DT, SaaS, Cloud Storage) including name of vendor and retention period.

The files at rest are stored on the on premises Lenel system with proprietary encryption.

Appendix A: Department Specific Responses
Department: Technology

1. A description of the product, including vendor and general location of technology.

   DT Critical Infrastructure Camera system (CIC) use Avigilon Control Center video management software to mange and interact with high-definition video. It captures and stores HD video, while intelligently managing bandwidth and storage using High Definition Stream Management (HDSM) technology.

   The CICs are located at the eight Public Safety Radio sites, as well as the DT Public Safety Division headquarters at 200 Paul Ave.

2. The specific categories and titles of individuals who are authorized by the Department to access or use the collected information.

   7362 Communications System Technician
   7368 Senior Communications System Technician
   8234 Fire Alarm Dispatcher
   8236 Chief Fire Alarm Dispatcher

3. What procedures will be put in place by which members of the public can register complaints or concerns, or submit questions about the deployment or use of a specific Surveillance Technology, and how the Department will ensure each question and complaint is responded to in a timely manner.

   Members of the public can register complaints or concerns through the following mechanisms:

   - Via a form on the Department of Technology website https://tech.sfgov.org/
   - Send an email to dtis.helpdesk@sfgov.org
   - Call the Citywide Service Desk at (628) 652-5000, or
   - Send a letter via post to 1 S. Van Ness Ave, 2nd floor, San Francisco, CA, 94103

   Regardless of which communication channel a member of the public uses, their inquiry is recorded into ServiceNow, a work management tool in use by the Department of Technology and assigned to a staff member. ServiceNow creates a ticket for each entry, and staff receive an email when assigned to work the ticket. Each ticket has a tracking number, date received and expected due date.

4. Specific details on where data will be stored (local, DT, SaaS, Cloud Storage) including name of vendor and retention period.

   The video recorded by the CIC system is stored locally. DT understands that it may have to store recorded video for a minimum of one year, we will seek to store video for the minimum possible duration.

5. Is a subpoena required before sharing with law enforcement?
   - No

Appendix A: Department Specific Responses
Department: Fire

1. A description of the product, including vendor and general location of technology.

The Fire Department has installed security cameras at its current Station 49 Ambulance/Bureau of Equipment facility as well as its Division of Training. Cameras are mounted on fences and walls for security purposes. In addition, security cameras are part of the plans of two current facilities under construction for the Department.

2. The specific categories and titles of individuals who are authorized by the Department to access or use the collected information

Access to the cameras are limited to a select few members in the Department's Administrative Division. Video is only accessed after a security incident has been identified and is not actively monitored.

3. What procedures will be put in place by which members of the public can register complaints or concerns, or submit questions about the deployment or use of a specific Surveillance Technology, and how the Department will ensure each question and complaint is responded to in a timely manner.

Members of the public can register complaints / concerns or submit questions through the Fire Department website and complaint process, or through the Chief's Office. (https://sf-fire.org/how-file-complaint). Constituent calls and complaints to the Fire Department are routed to the appropriate division The appropriate division designee will discuss concerns or complaints with constituent and record details regarding nature of conversation. If additional action is required or requested by caller, the Fire Department commits to a follow-up (by email or telephone) in a timely manner.

4. Specific details on where data will be stored (local, DT, SaaS, Cloud Storage) including name of vendor and retention period.

Data is stored on a secured cloud storage solution for a period of six months. The Department is working with COIT and the City Attorney on any data retention requirement changes.

5. Is a subpoena required before sharing with law enforcement?

- No

Appendix A: Department Specific Responses
Department: Homelessness and Supportive Housing

1. A description of the product, including vendor and general location of technology.

    1) 440 Turk Street Headquarters
    Cameras: 2x Samsung PNM-7000VD, 18x Samsung XNV-6080R
    Server: exacqVision
    Locations: devices are deployed mostly inside the building. Two cameras are deployed at the gate facing the front gate entrance area and street.

    2) Below technology are being used at shelter:
    Different site might have different type of DVR equipment but a typical DVR equipment would be Honeywell – HRDP16D1T0-R connected to various security cameras.

    Cameras will be mounted on ceiling in vulnerable areas at the shelters & navigation centers. It should be noted that cameras are not mounted in the bathroom or sleeping areas. Same applies for 440 Turk building.

2. The specific categories and titles of individuals who are authorized by the Department to access or use the collected information

    Sr. IS Engineer (1043) and Facilities Manager (7203) are authorized by the Department to access or use the collected information as requested by law enforcement or department HR.

3. What procedures will be put in place by which members of the public can register complaints or concerns, or submit questions about the deployment or use of a specific Surveillance Technology, and how the Department will ensure each question and complaint is responded to in a timely manner.

    Constituent calls and complaints to the Department of Homelessness & Supportive housing (HSH) are received by counter personnel and routed to the Shelter & Navigation Center Program manager. Program manager will discuss concerns or complaints with constituent, enter details regarding nature of conversation on excel spreadsheet stored in the department shared drive, referred to as the Security Camera System Constituent Feedback Log ("CFL"). If additional action is required or requested by caller, HSH commits to a follow-up (by email or telephone) within 48 hours. Department shall be prepared to host a viewing of edited imagery if caller is insistent, to demonstrate that no PII was collected. Depending upon the urgency or sensitivity of call, Program manager shall notify department IT of details and discuss resolution before follow-up with caller. Final outcome and action(s) taken shall be logged onto CFL.

Constituent can also file direct complaint to the Shelter Monitoring Committee and the Shelter Advocates. These organizations work directly with the HSH to address comments or concerns.

4. Specific details on where data will be stored (local, DT, SaaS, Cloud Storage) including name of vendor and retention period.

   The surveillance camera system at 440 Turk Street provides live views and record video footage to a dedicated, secure server. The footage is recorded on the server and stored for a limited amount of time. Data collected or processed by the 440 Turk Street Surveillance Camera System will not be handled or stored by an outside provider or third-party vendor on an ongoing basis. The Department will remain the sole Custodian of Record.

5. Is a subpoena required before sharing with law enforcement?

   - Yes

Appendix A: Department Specific Responses
Department: Human Services Agency

1. A description of the product, including vendor and general location of technology.

The following is a product inventory and manufacturer's description:

- 1235 Mission:
  - HONEYWELL MAXPRO – RECORDER
  - PELCO DX8100 – RECORDER
  - ANALOG CAMERAS (25)
  - IP CAMERAS (16) – HONEYWELL IP AND 2 AXIS P3708-PVE
- 1440 Harrison:
  - SALIENT – RECORDER
  - IP CAMERAS (12) – HONEYWELL IP
- 170 Otis:
  - HONEYWELL – RECORDER
  - ANALOG CAMERAS (31) – SONY
  - NAS (VM) – RECORDER
  - WIN SERVER 2019 / VAST VIDEO MANAGEMENT SOFTWARE (VMS)
  - DIGITAL IP CAMERAS (6) – VIVOTEK
- 2 Gough:
  - NAS (VM) – RECORDER
  - WIN SERVER 2019 / VAST VIDEO MANAGEMENT SOFTWARE (VMS)
  - DIGITAL IP CAMERAS (2) - VIVOTEK
- 3120 Mission:
  - HONEYWELL – RECORDER
  - ANALOG CAMERAS (4)

- Manufacturers' Product Descriptions:
  - VIVOTEK - VIVOTEK Inc. was founded in February 2000. The Company markets VIVOTEK solutions worldwide, and has become a leading brand in global security surveillance. To fulfill its global strategic footprint, VIVOTEK is committed to building an ecosystem for the IP surveillance industry, and looks forward to long term collaboration and growth with all partners in our shared pursuit of a safe and secure society.
  - PELCO DX8100 - The DX8100 Series digital video recorders (DVRs) are professional security-level DVRs based on a new and innovative hardware platform that is powered by unparalleled and unique high-performance

software. As the security requirements of your business expand into multiple sites and become more diversified, you need a professional DVR that you can quickly and effortlessly increase the channel and recording capacity. •The DX8100 is interoperable with your existing DX8000 DVRs, allowing you to build upon your existing security system. A DX8100 client can operate and administer both the DX8100 and DX8000 within the same network.•When you need to quickly and easily add more security cameras, the new DX8100-EXP 16-channel expansion unit extends the 8- or 16-channel DX8100 to 24 or 32 channels. With or without the channel expansion unit, all of the cameras can now take advantage of the increased frame rate of 2CIF and 4CIF recording. The DX8100 records video up to 480 images per second ips at a maximum CIF image size. •If your security project requirements increase storage capacity, you can extend internal storage up to 3 TB. With the optional DX9200 HDDI, you can further increase the DX8100 storage capacity. Alternately, you can use the DX9200 HDDI as a redundant RAID solution. •As your audio security needs grow, use the DX8108-AUD or DX8116-AUD audio option to add a total of 8 or 16 audio inputs. •Sophisticated video security applications require a network of DVRs to monitor multiple locations. The 10/100/1000 megabit Ethernet port supports today's high-speed networks. You can network your DX8100 and DX8000 systems and remotely operate the DVRs for continuous, motion detection, alarm, ATM/POS, normal scheduled recording, and administer and view live and playback video. For time-critical security applications, you must ensure that all video recordings are synchronized to an accurate time source. The DX8100 supports the network time protocol (NTP), which allows you to synchronize all networked DX8100s to one NTP time server.

- HONEYWELL MAXPRO VMS is an enterprise-class video management and hybrid solution. It enables you to operate the traditional analog, network and IP based video equipment in the same surveillance network. You can deploy thousands of cameras in number of locations, and add many video devices such as recorders and monitors.
- NAS VIRTUAL MACHINE (VM) – The VM is powered by Intel® Xeon® dual core CPU E5-2670 0 @ 2.60GHz x-64 processor, 64-bit Operating System, 4.00 GB of RAM, 75 GB of hard drive space.

- SALIENT NVR SERVER – Salient's hybrid NVRs are industry-leading, value-oriented digital video surveillance systems. Power-built for the rigors of continuous duty operation using advanced components, the 1U rack-mountable PowerPro hybrid NVR delivers the reliability and processing power required for mission critical video surveillance. PowerPro offers a Single Intel Xeon processor with 16GB of memory and up to 48TB of video storage delivering high reliability and processing power. Providing up to 32 analog direct connect channels, this hybrid NVR supports IP and analog cameras in a 1U rack mount unit.
- VIVOTEK's FD8169A is an easy-to-use fixed dome network camera specifically designed for indoor security applications, with a 2MP sensor enabling a viewing resolution of 1920x1080 at a smooth 30 fps. Dynamic and highly adaptable. The FD8169A is an all-in-one camera capable of capturing high quality video at high resolutions of up to 2 Megapixels. It also features POE, Real-time H.264, MJPEG Compression (Dual Codec), Removable IR-cut Filter for Day & Night Function, Built-in IR Illuminators effective up to 20 Meters, SNV (Supreme Night Visibility) for Low Light Conditions, Smart Stream II to Optimize Bandwidth Efficiency, Smart IR Technology to Avoid Overexposure, Supports ONVIF Standard to Simplify Integration and Enhance Interoperability, Support Installation with AM-712 Indoor Conduit Box, VIVOCloud App & Portal for 24/7 Surveillance, and Trend Micro IoT Security
- VIVOTEK's FD8182-F2 is an economic professional indoor fixed dome network cameras in VIVTOTEK's 5MP V-Pro Lite series. Design to provide higher resolution and sharper image with more detail, the FD8182-F2 offers up to 15 fps at 5-Megapixel or 30 fps at 1080p resolution. With powerful 3D Noise Reduction technology and Smart Stream technology, the FD8182-F2 can also optimize resolution for a desired object or area to maximize efficiency of bandwidth usage. Other features include POE, Built-in IR Illuminator Effective up to 30 Meters, WDR Enhancement for Unparalleled Visibility in Bright and Dark Environments, Smart Stream to Optimize Bandwidth Efficiency, 3D Noise Reduction for Low-light Conditions, Two-way Audio, PIR motion sensors, Video Rotation for Corridor View, Support Installation with AM-712 Indoor Conduit Box, VIVOCloud App & Portal for 24/7 Surveillance, and Trend Micro IoT Security

- VIVOTEK's IB8360-W (wireless) is a stylish 2-megapixel mini outdoor bullet network camera, specifically designed for boutique retail applications. Delivering a resolution of 1920x1080 at 30 fps, having IR illuminators effective up to 12 meters, and including SNV technology for low light environments, the remarkable cameras provide users with superior image quality around the clock. It also provide built-in IR Illuminators up to 12 meters, Smart IR Technology to Avoid Overexposure, SNV (Supreme Night Visibility) for Low Light Conditions, Smart Stream II to Optimize Bandwidth Efficiency, Weather-proof IP66-rated Housing, Built-in 802.11 b/g/n WLAN, Compact Size, VIVOCloud App & Portal for 24/7 Surveillance, and Trend Micro IoT Security
- HANWHA PNM SERIES MULTI-SENSOR 360 – Network vandal outdoor Multi-sensor Multi-Directional dome camera, (5MP X 4 sensors) 20MP @ 30fps WDR off/on, motorized vari-focal Lens 2.6x (3.6 ~ 9.4mm) (102.5˚ ~ 38.7˚), triple Codec H.265/H.264/MJPEG with WiseStream II technology, 120dB WDR, Defocus detection, built in analytics, true D/N, 4x SD card, hallway view, HLC, Defog detection, DIS(Gyro sensor), 12VAC/HPoE (power adaptor is included), IP66/IK10, -40°C ~ +55°C (-40°F ~ +131°F)
- HANWHA X SERIES DOME – WiseNet X powered by WiseNet 5 network IR indoor dome camera, 5MP @30fps WDR off/on, 3.7mm fixed focal lens (97.5°), H.265/H.264/MJPEG, WiseStream II compression technology, 120dB WDR, USB port for easy installation, advanced video analytics and sound classification, High powered IR LEDs range of 98', True D/N, dual SD card, hallway view, HLC, defog detection with simple focus, DIS , 12VDC/24VAC/PoE, IK08 rated
- AXIS P3708-PVE - is a fixed dome network camera with three sensors. It gives you a 180º panoramic overview of large areas using a single camera. And it's perfect for use in challenging light conditions, both during the day and at night.
- HONEYWELL – HD4DIRH - 700TVL VFAI WDR TDN IR Mini Dome – Honeywell 960H System Series of cameras provides a wide range of high-quality, feature rich video surveillance options for indoor, outdoor, and low-light applications. 1/3" 960H CCD image sensor, ultra-high resolution image (700TVL), 3D digital noise reduction, digital wide dynamic range, backlight compensation and highlight masking, smart IR technology for even distribution of the IR, 2.8-12 mm varifocal auto iris (VFAI) lens, true day/night

function for vivid color pictures by day and clear black and white pictures at night, excellent low-light performance (0.19 lux color, 0 lux with IR LEDs on), 18 IR LEDs provide up to 50 ft of illumination, depending on scene reflectance, weatherproof, impact-resistant housing (IP66), built-in heater for cold weather operation down to -40 F, breather vent prevents condensation buildup.

- HONEYWELL – HD4D2 – 650 TVL DOME CAMERA – PRODUCT DESCRIPTION NOT FOUND/UNAVAILABLE.
- HONEYWELL – H4L2GR1V – 2 MEGAPIXEL DOME IP CAMERA - Full HD 1080p 50/60 fps image with a ½.8"2 MP sensor, WDR up to 120 dB ensures glare-free images, true day/night provides colour images by day and clear black-and-white images at night with ICR, excellent low-light performance with 3D noise reduction, saving storage and bandwidth together with H.265 High Profile codec, low light technology is able to capture high quality colour images in low light environments, 2.7-13.5 mm, F1.6, motorized focus/zoom lens, H.265 plus, H265, H.264 and MJPEG codec, triple stream support, IR LEDs provide up to 50m (150') of illumination in dimly lit or night time scenes (depending on scene reflectance), smart IR technology provides even distribution of IR, waterproof (IP67) and IK10 vandal resistant camera housing, -40C to 60C working temperature, ONVIF Profile S, G & Q compliant, security features include individual signed certificates and data encryption, cameras can be retrofitted on many existing DVR/NVR installations without requiring additional storage, built-in PoE eliminates separate power supply and associated wiring; 24 V AC/12 V DC inputs where PoE is unavailable, 12 VDC/2W output, supports up to 128 GB micro SDHC (Class 10) card for local video storage when network is interrupted.
- ARECONT – AV2256PM – 2 MEGAPIXLE DOME IP CAMERA - The AV2256PM MegaDome® 2 series network camera is part of Arecont Vision's Wide Dynamic Range line of H.264 MegaDome® 2 series cameras. This fully compliant implementation of H.264 (MPEG 4, Part 10) provides full 1920 x 1080 megapixel resolution at full video frame rates of 32fps. The AV2255AM camera line provides an all-in-one solution with integrated 1080p resolution camera, remote focus, remote zoom, motorized P-iris lens, and IP66 and vandal resistant dome enclosure. With the features of Casino mode, ONVIF Profile S, PSIA conformance, privacy masking, extended motion detection and

flexible cropping, the AV2256PM is a high sensitivity, PoE (IEEE 802.3af) compliant camera. Built with Arecont Vision's massively-parallel MegaVideo® technology, this camera offers over six times the resolution of standard resolution IP cameras with the ability to output full real-time frame rates and deliver the high quality megapixel imaging for both indoor and outdoor applications.

- AXIS – P3707-PE – 8 MEGAPIXEL MULTI-SENSOR 360-DEGREE IP CAMERA - AXIS P3707-PE comprises four camera heads that can be repositioned along a circular track to point in the desired viewing direction. Each camera head can be individually tilted and adjusted to provide a 108° to 54° horizontal field of view for either wide or zoomed-in views. The camera heads can be rotated to support Axis' Corridor Format for optimal coverage of vertically oriented scenes. A specially designed clear cover, with no sharp edges, allows for undistorted views in all directions. AXIS P3707-PE supports individually configurable video streams for each camera head, as well as quad-view streaming, enabling 1080p resolution videos at 12.5/15 frames per second and 720p videos at full frame rate.
- SONY – EX543 – ANALOG CAMERA – PRODUCT DESCRIPTION NOT FOUND/UNAVAILABLE
- TRIVIEW – TFD-CVSH312A1241IR – DOME ANALOG CAMERA – PRODUCT DESCRIPTION NOT FOUND/UNAVAILABLE

2. The specific categories and titles of individuals who are authorized by the Department to access or use the collected information
   - 2966 WELFARE FRAUD INVESTIGATOR
3. What procedures will be put in place by which members of the public can register complaints or concerns, or submit questions about the deployment or use of a specific Surveillance Technology, and how the Department will ensure each question and complaint is responded to in a timely manner.

Public:

General compliant and comment forms are available in public areas of all HSA buildings. All complaints are processed on a flow basis.

City and County of San Francisco Employees:

All questions regarding this policy should be directed to the employee's supervisor or to the director. Similarly, questions about other applicable laws governing the use of the surveillance technology or the issues related to privacy should be directed to the employee's supervisor or the director.

4. Specific details on where data will be stored (local, DT, SaaS, Cloud Storage) including name of vendor and retention period.

See question #1 for specific storage details. When an incident occurs, images may be recovered from the recorder and preserved on DVD diskettes pursuant to the requirements of a given investigation and evidence retention guidelines. Data is stored with case documents in locked file cabinet and/or evidence vault in secure agency office facility.

5. Is a subpoena required before sharing with law enforcement?
    - Yes

Appendix A: Department Specific Responses
Department: Port

1. A description of the product, including vendor and general location of technology.

The Port Security CCTV System consists of the following components.

- Arcenot - Omni Directional Day/Night Camera
- Arcenot – Fixed IR Camera
- Arcenot- Day / Night Camera
- Axis – Camera
- Illuminar – Infrared Illuminator
- Raytec- 180 Degree Illuminator
- Vario- Infrared Illuminator
- Exacq- Server
- Exacq- NVR

Port Security Security Camera technology is installed on Port property along the 7.5 miles of San Francisco waterfront. This technology includes CCTV cameras installed on exterior of Pier Bulkhead buildings, Pier Sheds, and Small Craft Harbors. Port Security Camera technology provides layered security protection to multiple MTSA regulated facilities throughout the Port.

2. The specific categories and titles of individuals who are authorized by the Department to access or use the collected information

- Security and Emergency Planning Manager (0922)
- Homeland Security Project Manager (9978)

3. What procedures will be put in place by which members of the public can register complaints or concerns, or submit questions about the deployment or use of a specific Surveillance Technology, and how the Department will ensure each question and complaint is responded to in a timely manner.

Members of the public may contact the Port's Custodian of Records or by calling the Port's 24/hr. contact number 415-274-0400

4. Specific details on where data will be stored (local, DT, SaaS, Cloud Storage) including name of vendor and retention period.

The data is stored on servers maintained by the Department of Technology.

5. Is a subpoena required before sharing with law enforcement?

- No

Appendix A: Department Specific Responses
Department: Rent Board

1. A description of the product, including vendor and general location of technology.

The CIC system records video of the Rent Board's lobby and entrance. In the event of an incident of theft of vandalism, RNT staff will review the recorded video to determine if it has captured the incident.

Q-See QT454-This DVR uses high-performance video processing chips and an embedded Linux operating system for quality image recording and ease of use. It utilizes numerous advanced technologies including the industry-standard H.264 codec to deliver high-quality, smooth videos and dual stream capability for remote viewing. A SATA hard-drive interface offers upgradability and VGA output allows users to connect to any standard TV or monitor for viewing.

The Lobby Cameras are used to protect against harassment, theft, safety or vandalism of the Rent Board's lobby area, which includes publicly accessible computers and other City owned assets.

2. The specific categories and titles of individuals who are authorized by the Department to access or use the collected information

0961 – Department Head

3. What procedures will be put in place by which members of the public can register complaints or concerns, or submit questions about the deployment or use of a specific Surveillance Technology, and how the Department will ensure each question and complaint is responded to in a timely manner.

The Department of Human Resources Employee Handbook addresses Employee Use of City Resources and City Computers and Data Information Systems. The Department of Technology defines CIC as a City resource.

4. Specific details on where data will be stored (local, DT, SaaS, Cloud Storage) including name of vendor and retention period.

All data is stored locally.

5. Is a subpoena required before sharing with law enforcement?
    - No

Appendix A: Department Specific Responses
Department: Recreation and Parks

1. A description of the product, including vendor and general location of technology.

Approximately 300 security cameras are located on poles or building facades. Cameras range from 2 to 5 megapixels and most have pan-tilt-zoom capabilities. The video feeds are recorded and retained on a server at each site. If the server is connected to RPD's network, the feed can be streamed to a RPD's Park Ranger Headquarters where they can be monitored for public safety purposes. In some instances, cameras are streamed to the operators on site who are managing the facility and services on RPD's behalf.

As of March 2021, below are the sites with security cameras:

Location	Type
501 Stanyan NVR	Arecont Vision
Betty Ann Ong	Arecont Vision
	Samsung
	Vivotek
Boeddeker Park	Arecont Vision
	Samsung
Conservatory of Flowers GGP	Arecont Vision
	Samsung
Dolores Park	Arecont Vision
Geneva Powerhouse	Samsung
Glen Park Rec	Samsung
Golf Course GGP	Samsung
Herz Park Playground	Arecont Vision
Huntington Park	Arecont Vision
Japanese Tea Garden	AXIS
Maintenance Yard GGP	Samsung
Margret Hayward Complex	Samsung
Portsmouth Square	Samsung
SF Marina	Arecont Vision
Willie Woo Woo Wong	Samsung
COIT Tower	Samsung
Beach Chalet Soccer Field	Samsung
Crocker Amazon	Samsung

RPD is continuously adding cameras to new capital sites and existing facilities (budget permitting).

2. The specific categories and titles of individuals who are authorized by the Department to access or use the collected information

The following individuals may access or use the collected information:

- Park Rangers (8208-8210)
- IT analysts and technical staff (1820 series, 1050 series, 1090 series)

3. ***What procedures will be put in place by which members of the public can register complaints or concerns, or submit questions about the deployment or use of a specific Surveillance Technology, and how the Department will ensure each question and complaint is responded to in a timely manner.***

Members of the public can register complaints/concerns or submit questions to San Francisco Recreation and Parks through several ways:

- Send written correspondence to McLaren Lodge in Golden Gate Park, 501 Stanyan Street, San Francisco, CA 94117
- Call to the RPD Front Desk 415-831-2700
- Send an email to rpdinfo@sfgov.org
- Contact 311.

All calls/complaints from the public received via mail or via call to the RPD Front Desk are routed to the RPD IT HelpDesk and logged in our department's request management system. Any requests from 311 are received in our department's dispatch system and routed to the RPD IT HelpDesk which then is logged in the request management system.
Once the request is tracked in the request management system, IT will work with all relevant parties to ensure completion.

Review of open / closed requests occur with the CIO on a weekly basis.

4. ***Specific details on where data will be stored (local, DT, SaaS, Cloud Storage) including name of vendor and retention period.***

Footage is retained on Exacqvision servers hosted on RPD's network.

Appendix A: Department Specific Responses
Department: War Memorial

1. A description of the product, including vendor and general location of technology.
   Product Description:
   Cameras: Mobotix S15D FlexMount Dual Camera
   Server: Rasilient ApplianceStor90
   Software: Avigilon Control Center Server v6.8.6.4.
   Vendor: N/A
   Location: War Memorial surveillance cameras are located in public areas of all floors in the Veterans Building. Additional cameras are planned for public interior and exterior areas of the Veterans Building.
2. The specific categories and titles of individuals who are authorized by the Department to access or use the collected information
   8207 - Building and Grounds Patrol Officers,
   8211 - Supervisor Building and Grounds Patrol Officer,
   0922 - Director of Security,
   1093 - IT Manager,
   1844 - Facilities Administrator
3. What procedures will be put in place by which members of the public can register complaints or concerns, or submit questions about the deployment or use of a specific Surveillance Technology, and how the Department will ensure each question and complaint is responded to in a timely manner.

   Complaints or concerns can be submitted to the Department by sending an email to WarMemorialinfo@sfgov.org.

   Department shall acknowledge and respond to complaints and concerns in a timely and organized response. To do so, Department shall monitor the War Memorial information email box throughout the day during standard business hours. Any communications to that email address are responded to directly or brought to the attention of responsible staff.
4. Specific details on where data will be stored (local, DT, SaaS, Cloud Storage) including name of vendor and retention period.
   Storage Locations:
   Local storage
   Department of Technology Data Center
   Vendor: None
   Retention Period: One (1) year at minimum.
5. Is a subpoena required before sharing with law enforcement?
   - No

Surveillance Impact Report

San Francisco Municipal Transportation Agency - SFMTA
Security Cameras

As required by San Francisco Administrative Code, Section 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 surveillance cameras.

DESCRIPTION OF THE TECHNOLOGY

The San Francisco Municipal Transportation Agency (SFMTA) is a multi-modal transportation organization responsible for operating buses, rail, world-famous cable cars and an historic fleet of streetcars, as well as developing and implementing innovative transportation solutions to benefit auto drivers, transit riders, taxicab users, bicyclists and pedestrians. The SFMTA's programs and services promote safe, efficient and convenient mobility alternatives for San Francisco residents, commuters, businesses and visitors.

In line with its mission, the Department shall use security cameras only for the following authorized purposes:

Authorized Use(s):

1. Live monitoring.
2. Recording of video and images in the event of an incident.
3. Reviewing camera footage.
4. Providing video footage/images to law enforcement or other authorized persons following an incident.
5. Enforcing parking and driving violations.

Prohibited use cases include any uses not stated in the Authorized Use Case section.

Further, processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, gender, gender identity, disability status, or an individual person's sex life or sexual orientation, and the processing of genetic data and/or biometric data for the purpose of uniquely identifying an individual person shall be prohibited.

Surveillance Oversight Review Dates
COIT Review: March 18, 2021
Board of Supervisors Review: TBD

Department technology may be deployed in the following locations, based on use case:

System	Description
SFGO	Cameras installed on signal poles
Facilities	Locations where employees work
Transit platforms and subway	Locations where the public wait to access our vehicles
Vehicles	Cameras in Buses, LRV's Cable Cars, Taxis, trucks, etc.
PARCS (Parking Access and Revenue Control System)	Cameras in our parking garages

Technology Details

The following are product descriptions:

- The department maintains varies surveillance cameras throughout San Francisco. Although there are various legacy systems that are still in operation, the department has been working to standardize surveillance systems. The legacy systems use the same technology but may not be from the standard vendors.
- The departments typical security cameras are IP based cameras that are supplied by Hanwha or Axis. These cameras stream video footage across the network to the datacenter where video management solution (VMS) stores the footage. Genetec is the manufacturer of our VMS platform.
- Mobile video recorders from DTI (a third-party vendor) are used in buses and trains to record footage from inside and outside of the vehicle. This digital video recording (DVR) technology captures digital, color images and allow easier transmission, storage, and portability of those images.
- DriveCam is a G-Force triggered digital event recorder that saves triggered events and forwards them via the Internet. Each video is scanned for behavior-based actions and then analyzed by DriveCam safety experts and commented on accordingly. These analyzed events and data are then sent back to the client (SFMTA) for review and follow up to identify and address behavior-based actions that triggered the recording.

How It Works

To function, SFMTA has installed surveillance cameras to monitor critical aspects of our business so we can monitor the safety and quality of services we provide to the citizens of San Francisco. These cameras also stream the video across our network to the SFMTA datacenter where the footage is stored for later review in the event of an incident.

Data collected or processed by security cameras will not be handled or stored by an outside provider or third-party vendor on an ongoing basis. The Department will remain the sole Custodian of Record.

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 security cameras has the following benefits for the residents of the City and County of San Francisco:

▪	Education	
▪	Community Development	
X	Health	Protect safety of staff, patrons, and facilities while promoting an open and welcoming environment.
▪	Environment	
X	Criminal Justice	Review video footage after a security incident; provide video evidence to law enforcement or the public upon request by formal process, order, or subpoena.
▪	Jobs	
▪	Housing	
X	Other	Job Training and Safety – Review video footage from on-board cameras to train transit operators and improve on-board conditions and safety for customers.

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:

SFMTA strives to mitigate any potential civil rights impacts by ensuring the responsible usage of surveillance cameras. SFMTA restricts access to video footage. Only authorized trained staff has access to the cameras that pertain to their job roll. Additionally, the ability to export or save video footage is blocked by default for all users and only specific individuals are allowed this type of access. SFTMA Video Management System has extensive auditing capabilities so that all access requests are

logged, including date, time and requestor. Furthermore, where practical, watermarks are added to the footage to show the requester on the footage. SFMTA staff consider privacy and civil rights impacts when they choose camera locations and to try to minimize the potential compromising footage.

C. Fiscal Analysis of Costs and Benefits

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

Benefit		Description
X	Financial Savings	Department Security Camera Systems will save on building or patrol officers.
X	Time Savings	Department Security Camera Systems will run 24/7, thus eliminating building or patrol officer supervision
X	Staff Safety	Security cameras help identify violations of Department Patron Code of Conduct and provide assurance that staff safety is emphasized and will be protected at their place of employment.
X	Data Quality	Security cameras run 24/7/365 so full-time staffing is not required to subsequently review footage of security incidents. Data resolution can be set by level and is currently set to high resolution.

The total fiscal cost, including initial purchase, personnel and other ongoing costs	SFMTA maintains numerous systems that were purchased at different times; therefore, it would be very difficult if not impossible to provide specific numbers. These numbers are approximations.	
Number of FTE (new & existing) and Classification	10 – 7318 Electronic Maintenance Tech 1 – 1044 IS Engineer-Principal 3 – 14xx Surveillance Clerks	
	Annual Cost	***One-Time Cost***
Software	*~$100,000*	~$3,000,000
Hardware/Equipment	*$50,000-$100,000*	~$1,000,000
Storage (excluding mobile vehicle video)	*~$200,000*	~$1,000,000
Professional Services	*$50,000-$100,000*	~$500,000
Training	*$5,000*	*$20,000*

Other		
Total Cost	***$205,000***	*~$4,520,000*

Cost on Public Requests and Crime

SFPD request in 2018 accounted for 12% of SFMTA video pulls requiring 238 staff hours per month. In this same time frame, 34% of SFMTA video pulls and approximately 673 staff hours were public request which encompassed 311, Sunshine and TOLE.

The Department funds its use and maintenance of the surveillance technology through general operations budget and occasional grants

COMPARISON TO OTHER JURISDICTIONS

Surveillance cameras are currently utilized by other governmental entities for similar purposes.

Appendix A: Crime Statistics

Department: Municipal Transportation Authority

Section 19B requires each department in their Surveillance Impact Report to respond to the following question if applicable, "the general location(s) [of the surveillance technology] may be deployed and crime statistics for any location(s)."

The Municipal Transportation Authority operates approximately 15,000 Security Cameras throughout its transit system and associated properties.

The department maintained an internal incident log for 2020:

Category	Number of Incidents	% of Incidents
Assault & Battery	283	3.17%
Burglary	69	0.77%
Criminal Activity	135	1.51%
Fatality	2	0.02%
Fire	19	0.21%
Homicide	117	1.31%
Ill Passenger	264	2.96%
Inattentiveness	140	1.57%
Injured Passenger	30	0.34%
Intoxicated passenger	146	1.64%
Accidents	1,010	11.32%
Non-Muni Incidents/Collisions	169	1.89%
Operator assault	34	0.38%
Operator Conduct	895	10.03%
Operator Injury	39	0.44%
Passenger Altercation	1,620	18.15%
Pick pocket	66	0.74%
Red Light Violation	68	0.76%
Rendering Aid	298	3.34%
Robbery	321	3.60%
Sexual Battery	10	0.11%
Shooting	105	1.18%
Slip & Fall	502	5.62%
Sleeper on Board	325	3.64%
Sunshine Requests	39	0.44%
Suspicious Behavior/Person	17	0.19%
Theft/ Stolen Cellphone	237	2.66%
Title VI Complaint/Harassment	113	1.27%
Transit-Only Lane Enforcement (TOLE)	694	7.78%
Tunnel Intruder	21	0.24%
Vandalism	1,062	11.90%

Violation	75	0.84%
Total	**8,925**	

Surveillance Technology Policy

San Francisco Municipal Transportation Agency
Security Cameras

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 San Francisco Municipal and Transportation Agency (Department) aims to ensure the responsible use of department's Security Camera System, 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

This Surveillance Technology Policy ("Policy") defines the manner in which the Security Camera System (fixed or mobile) will be used to support Department's operations.

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

POLICY STATEMENT

Department will limit its use of Security Camera Systems to the following authorized use cases and requirements listed in this Policy.

Authorized Use(s):

1. Live monitoring.
2. Recording of video, images and review in the event of an incident.
3. Reviewing camera footage and/or images.
4. Providing video footage/images to law enforcement or other authorized persons following an incident.
5. Enforcing parking and driving violations.

Prohibited use cases include any uses not stated in the Authorized Use Case section.

Further, processing of data from Department' Surveillance Technologies to identify the racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, gender, gender identity, disability status, or sex life or sexual orientation of an individual or group of individuals shall be prohibited. The processing of genetic data and/or biometric data for the purpose of uniquely identifying an individual person shall be prohibited.

BUSINESS JUSTIFICATION

In support of Department operations, Security Cameras help with:

	▪ Education	
	▪ Community Development	
X	Health	Protect safety of staff, patrons, and facilities while promoting an open and welcoming environment.
	▪ Environment	
X	Criminal Justice	Review video footage after a security incident; provide video evidence to law enforcement or the public upon request by formal process, order, or subpoena.
	▪ Jobs	
	▪ Housing	
X	Other	Job Training and Safety – Review video footage from on-board cameras to train transit operators and improve on-board conditions and safety for customers.

In addition, the following benefits are obtained:

Benefit		Description
X	Financial Savings	Department's Security Camera Systems saves on building or patrol officers.
X	Time Savings	Department's Security Camera Systems run 24/7, thus eliminating building or patrol officer supervision
X	Staff Safety	Security cameras help identify violations of Department Patron Code of Conduct and provide assurance that staff safety is emphasized and will be protected at their place of employment.
X	Data Quality	Security cameras run 24/7/365 so full-time staffing is not required to subsequently review footage of security incidents. Data resolution can be set by level and is currently set to high resolution.
X	Other	Travel Time Savings -- Security cameras at key intersections help ensure clear and safe paths of travel for all surface modes. Security cameras in subway tunnels help ensure clear and safe paths of travel for sub-surface modes.

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 security cameras must be kept up-to-date and maintained.

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

The surveillance technology collects the following data types:

Data Type(s)	*Format(s)*	*Classification*
Video and Images	MP4, AVI, MPEG	Level 3
Date and Time	MP4 or other format	Level 3
Geolocation data	TXT, CSV, DOCX	Level 3

Notification: Departments shall notify the public of intended surveillance technology operation at publicly accessible sites through signage in readily viewable public areas at those site. Department notifications shall identify the type and purpose of technology being used.

Department includes the following items in its public notice:

- X Information on the surveillance technology
- X Description of the authorized use
  - Type of data collected
  - Will persons be individually identified
  - Data retention
  - Department identification
- X Contact information

Access: Prior to accessing or using data from Department's Security Camera System, authorized individuals receive training in system access and operation, and instruction regarding authorized and prohibited uses.

	Access to live views and recorded footage is restricted to specific trained Security and IT personnel. Recorded footage is accessed only in response to an incident. Details on Department staff and specific access are available in Appendix A.
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. Departments shall, at minimum, apply the following safeguards to protect surveillance technology information from unauthorized access and control, including misuse: - Encryption: Data retained by the Department will be encrypted. Raw data may be retained by the Department only for the authorized use case of sharing with law enforcement or the public. - Audits: A data access log will be maintained by the Department for all Security Camera data that is processed and utilized. This log will include but is not limited to the following: date/time data was originally obtained/collected, reasons/intended use for data, Department requesting data, date/time of access of raw data, outcome of data processing, as well as date processed data was delivered to users.
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 will endeavor to ensure that other agencies or departments that may receive data collected by Department's Security Camera Systems will act in conformity with this Surveillance Technology 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. Each department that believes another agency or department receives or may receive data collected from its use of Security Cameras should consult with its assigned deputy city attorney regarding their response. Before sharing data with any recipients, the Department will use the following procedure to ensure appropriate data protections are in place: X Confirm the purpose of the data sharing aligns with the department's mission.

X	Consider alternative methods other than sharing data that can accomplish the same purpose.
X	Redact names, scrub faces, and ensure all PII is removed in accordance with the department's data policies.
X	Review of all existing safeguards to ensure shared data does not increase the risk of potential civil rights and liberties impacts on residents.
X	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.
X	Ensure shared data will be done in a cost-efficient manner and exported in a clean, machine-readable format.

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.

The Department may share Security Camera footage with the following entities:

A. Internal Data Sharing:

In the event of an incident, Security Camera images may be live-streamed or shared by alternative methods to the following agencies:

- Within the operating Department
- Police
- City Attorney
- District Attorney
- Sheriff

Data sharing occurs at the following frequency:

- As needed.

B. External Data Sharing:

- Other local police departments

Data sharing occurs at the following frequency:

- As needed.

Data Retention:	Department may store and retain raw PII data only as long as necessary to accomplish a lawful and authorized purpose. Department data retention standards should be aligned with how the department prepares its financial records and should be consistent with any relevant Federal Emergency

Management Agency (FEMA) or California Office of Emergency Services (Cal OES) sections.

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

- In accordance with California Government Code section 34090.8(b), Department's Security Camera data will be stored for a minimum of one month or as long as the installed technology allows to be available to authorized staff for operational necessity and ready reference.

  If data is associated with an incident, it may be kept for longer than the standard retention period.

- Justification: This retention period conforms with the available server system storage space and allows for ample time for security staff to review footage related to security incidents and/or external requests for records.

Data will be stored in the following location:

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

X SFMTA Data Center

X Software as a Service Product

▪ Cloud Storage Provider

Data Disposal:	Upon completion of the data retention period, Department shall dispose of data in the following manner: - Automatic overwrite of all existing files when standard data retention period ends. This may take the form of a delete/reformat, wipe, overwrite of existing data, or degaussing.
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 must receive training on data security policies and procedures. - Annual cybersecurity training (COIT Policy Link) or specific Department training tailored to their specific role.

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.

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.

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.
Exigent Circumstances	An emergency involving imminent danger of death or serious physical injury to any person that requires the immediate use of Surveillance Technology or the information it provides.

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."

Appendix A: Department Specific Responses

1. **Products and Vendors the department uses:**

    a. The department maintains varies surveillance cameras throughout San Francisco. Although there are various legacy systems that are still in operation, the department has been working to standardize surveillance systems. The legacy systems use the same technology but may not be from the standard vendors.

    b. The departments typical security cameras are IP based cameras that are supplied by Hanwa or Axis. These cameras stream video footage across the network to the datacenter where video management solution (VMS) stores the footage. Genetec is the manufacturer of our VMS platform.

    c. Mobile video recorders from DTI (a third-party vendor) are used in buses and trains to record footage from inside and outside of the vehicle. This digital video recording (DVR) technology captures digital, color images and allow easier transmission, storage, and portability of those images.

    d. DriveCam is a G-Force triggered digital event recorder that saves triggered events and forwards them via the Internet. Each video is scanned for behavior-based actions and then analyzed by DriveCam safety experts and commented on accordingly. These analyzed events and data are then sent back to the client (SFMTA) for review and follow up in order to identify and address behavior-based actions that triggered the recording.

2. **General locations of cameras installed to help monitor the safety of patrons and staff.**

System	Description
SFGO	Cameras installed on signal poles
Facilities	Locations where employees work
Transit platforms and subway	Locations where the public wait to access our vehicles
PARCS (Parking Access and Revenue Control System)	Cameras in our parking garages
Transit Vehicles	Cameras installed in Buses, LRV's Cable Cars, etc.

3. Titles of Individuals authorized to access, or use collected information

SFMTA has staff that reviews video as part of their normal job responsibilities. They do this for varies operational reasons such as but not limited to; monitoring security events, reviewing operational efficiencies, customer service, and safety monitoring. This access is granted to select staff if their job role justifies access and that such access is restricted to specific area that is appropriate based on their needs.

Security Officers

Contract Security Officers, located in the Revenue Basement at One South Van Ness, monitor the Revenue Processing facility, and Customer Service Center at 11 South Van Ness on 24 hour/7 days a week (24/7) basis. Officers are also stationed and monitor Muni Metro East at 601 25th Street.

Remote sites are monitored after normal business hours and on weekends by Security Operations Center (SOC) Supervisors.

Parking Staff

It is the responsibility of the Parking Division (or their garage management contractor) to monitor their site(s). All requests for video shall be directed to or coordinated with the Video Surveillance Program Manager, following all SFMTA procedures and applicable laws in handling requests from law enforcement agencies and/or public records request. Internal request for video shall be directed to Parking Division Management who shall notify the Video Surveillance Program Manager.

Parking Staff Job Classification Details:

2 - 1824 Pr. Administrative Analyst
3 - 91xx Managers

Garage Operators

The Parking Division delegates the day to day operational activities to contracted companies to ensure our parking garages are well maintained. The local contractors will have at least view access to the local cameras to ensure they can monitor the facility in real time. The Parking staff may delegate additional work and access to the garage operators as they see fit.

Transit Division Staff

The Transit Division includes the following units: *Operations, Planning & Schedules*; *Transit Administration; Transit Services; Transit Management; and Bus and Rail Maintenance Units*. All requests for video data must follow the procedure(s) outlined in this document. While all of Transit can utilize and benefit from the various video cameras deployed by SFMTA, the following Units use or have need of use of SFMTA's Video Surveillance System on a regular or day-to-day basis:

a. Transit Services

Transit Services is a primary user of surveillance data and has authorized personnel who have specific need to view/review both live and recorded video data. Use of such data or recordings shall be done in a manner that protects the privacy of the public in accordance with this SFMTA policy.

Transit Services shall use video in response to a specific need and where a review of such data would contribute to the following:

- Review of a traffic operations or safety problem(s);
- Provision of a training review for future operator training;
- Research activities that will improve future technology or operations;
- Post-incident review of a particularly complex incident and/or emergency for the purposes of improving operations procedures and response;
- Demonstrating, testing equipment or system functions;
- Collection of data for transportation planning management purposes

Transit Staff Job Classifications Details:

5 - 91xx– Managers
1 - 9160 –Transit Operations Specialist

b. Transportation Management Center (TMC) Staff

Transportation Management Center (TMC) is responsible for management and administration of the operations workforce for all transit modes: bus, rail and cable car, staff scheduling, dispatching, workforce planning and day-to-day contract administration. The TMC monitors roadway

conditions, provides support to SFMTA drivers/operators and field personnel responding to rail or roadway incidents, which enhances effectiveness of transit operations and enables the active management of traffic flow.

Except as provided for in this document, SFMTA surveillance video shall not be disseminated by TMC staff. The TMC shall receive surveillance video in a real-time or a limited-time-delay data feed. Furthermore, the TMC shall use and/or review the data for transit operations, maintaining and improving safety.

TMC Staff Job Classifications Details:

2 - 91xx – Managers
1 - 9160 – Transit Operations Specialist
2 - 915x – Transportation Controllers
1 - 9139 – Transit Supervisor

4. Public Record Requests for Video

The Video Surveillance Program Manager is responsible for ensuring that Video Surveillance Program staff respond to Public Records Requests for video in accordance with SFMTA's Public Records Policy and Procedure guidance document.

Video recordings are public records and disclosure is governed by the California Public Records Act (Government Code Section 6252) and the City's Sunshine Ordinance, Chapter 67 of the San Francisco Administrative Code. Sec **Error! Reference source not found.**.

In compliance with state and local law, video recordings are generally released in response to a public records request unless there is an applicable exemption, such as a pending law enforcement investigation, provided for under state or local law.

Surveillance Impact Report

San Francisco Public Library
Security Cameras

As required by San Francisco Administrative Code, Section 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 surveillance cameras.

DESCRIPTION OF THE TECHNOLOGY

The San Francisco Public Library (SFPL) system is dedicated to free and equal access to information, knowledge, independent learning and the joys of reading for our diverse community.

In line with its mission, the Department shall use security cameras only for the following authorized purposes:

Authorized Use(s):

1. Live monitoring to protect safety of SFPL staff, patrons and facilities.
2. Recording of video and images.
3. Reviewing camera footage in the event of an incident.
4. Providing video footage/images to law enforcement or other authorized persons following an incident or upon request.

Prohibited use cases include any uses not stated in the Authorized Use Case section.

Further, processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, gender, gender identity, disability status, or an individual person's sex life or sexual orientation, and the processing of genetic data and/or biometric data for the purpose of uniquely identifying an individual person shall be prohibited.

Department technology may be deployed in the following locations, based on use case:

- Bayview Branch Library
- CARS Building at 750 Brannan Street
- Chinatown Branch Library
- Eureka Valley Branch Library
- Main Library
- Marina Branch Library
- Mission Bay Branch Library
- Ortega Branch Library
- Park Branch Library
- Presidio Branch Library
- Richmond Branch Library

Surveillance Oversight Review Dates

COIT Review: March 18, 2021
Board of Supervisors Review: TBD

• Support Services building at 190 9th Street
• Visitation Valley Branch Library
• Western Addition Branch Library
• Ocean View Branch Library

Technology Details

The following is a product description:

The P2000 security management system helps buildings achieve maximum security while increasing efficiencies and lowering costs. Built on open standards and compatible with virtually any third party program, the P2000 can integrate multiple businesses, buildings and security systems to achieve interactive, real-time security management. The P2000's built-in web browser allows users to access the platform from a central location — or remotely, through web-connected devices.

A. How It Works

To function, security cameras record and retain video footage of public and non-public spaces within and on the exterior of the facilities of the San Francisco Public Library. That video footage is stored on a server system that lives on the 6th Floor of the Main Library. Video footage is then accessible for review by authorized users.

Data collected or processed from the security cameras will not be handled or stored by an outside provider or third-party vendor on an ongoing basis. The Department will remain the sole Custodian of Record.

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 security cameras has the following benefits for the residents of the City and County of San Francisco:

- Education
- Community Development

X	Health	Protect safety of SFPL staff, patrons, and facilities while promoting an open and welcoming environment.
☐	Environment	
X	Criminal Justice	Review video footage after a security incident; provide video evidence to law enforcement or other authorized persons following an incident or upon request.
☐	Jobs	
☐	Housing	
☐	Other	

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:

The San Francisco Public Library strives to mitigate all potential civil rights impacts through responsible technology and associated data use policies and procedures and intends to use security cameras and their associated data exclusively for authorized use cases. All other uses, including active surveillance of San Francisco residents or groups, are expressly prohibited.

The security cameras are used within library facilities and adjoining perimeter to protect SFPL staff, patrons and facilities. Without proper safeguards in place, the use of these security cameras could result in dignity loss, discrimination, loss of liberty and/or loss of trust. The quality of the video captured through the security cameras may vary in quality due to lighting, motion or other factors, which may lead to mis-identification and other subsequent impacts such as loss of liberty. Correspondingly, the video may not correctly convey intent and viewers may interpret actions captured as threatening or menacing which may have a more benign interpretation, leading to possible issues of discrimination and loss of dignity. Incidents such as these collectively could lead to a loss of trust in the institution of the San Francisco Public Library and municipal government in general.

To protect security camera data from potential breach, misuse or abuse that may result in civil rights impacts, data is maintained on secure servers located on the premises of the 6th Floor of the Main Library, staff are trained on proper usage of the technology and protocols for documenting requests and safeguarding information are followed. Only persons authorized to utilize the data may access this information.

C. Fiscal Analysis of Costs and Benefits

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

Benefit		Description
X	Financial Savings	Department Security Camera Systems will save on building or patrol officers.
X	Time Savings	Department Security Camera Systems will run 24/7, thus eliminating building or patrol officer supervision
X	Staff Safety	Security cameras help identify violations of Department Patron Code of Conduct and provide assurance that staff safety is emphasized and will be protected at their place of employment.
X	Data Quality	Security cameras run 24/7/365 so full-time staffing is not required to subsequently review footage of security incidents. Data resolution can be set by level and is currently set to high resolution.
X	Service Levels	Security cameras will enhance effectiveness of incident response and result in improved level of service.

The total annual fiscal cost, including initial purchase, personnel and other ongoing costs is: Number of FTE (new & existing)	0.10 FTE	
Classification	1822 Administrative Analyst; 9976 ILS Administrator.	
	Annual Cost	***One-Time Cost***
Software	*$16,128*	
Hardware/Equipment	*$15,170*	
Professional Services	*$23,611*	
Training	*$0*	
Other (Salary/Fringe)	*$33,557*	
Total Cost	***$88,466***	

2.1 Please disclose any current or potential sources of funding (e.g. potential sources = prospective grant recipients, etc.). SIR, ASR
Library Preservation Fund.

The Department funds its use and maintenance of the surveillance technology through the Library Preservation Fund.

COMPARISON TO OTHER JURISDICTIONS

Johnson Controls P2000 Security Management System - Video System is currently utilized by other governmental entities for similar purposes.

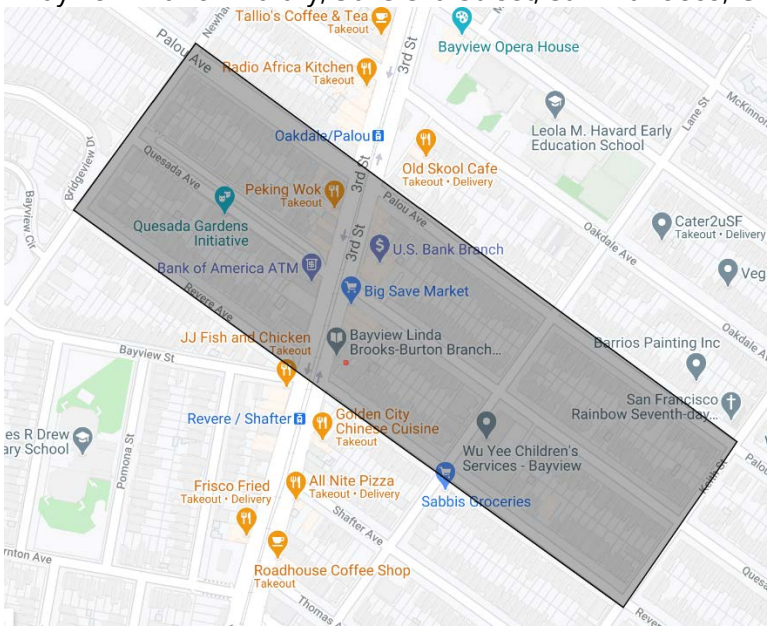
Appendix A: Crime Statistics

Department: San Francisco Public Library

Section 19B requires each department in their Surveillance Impact Report to respond to the following question if applicable, "the general location(s) [of the surveillance technology] may be deployed and crime statistics for any location(s)."

The San Francisco Public Library operates a total of 155 Security Cameras at the following locations:

- Bayview Branch Library, 5075 3rd Street, San Francisco, CA 94124

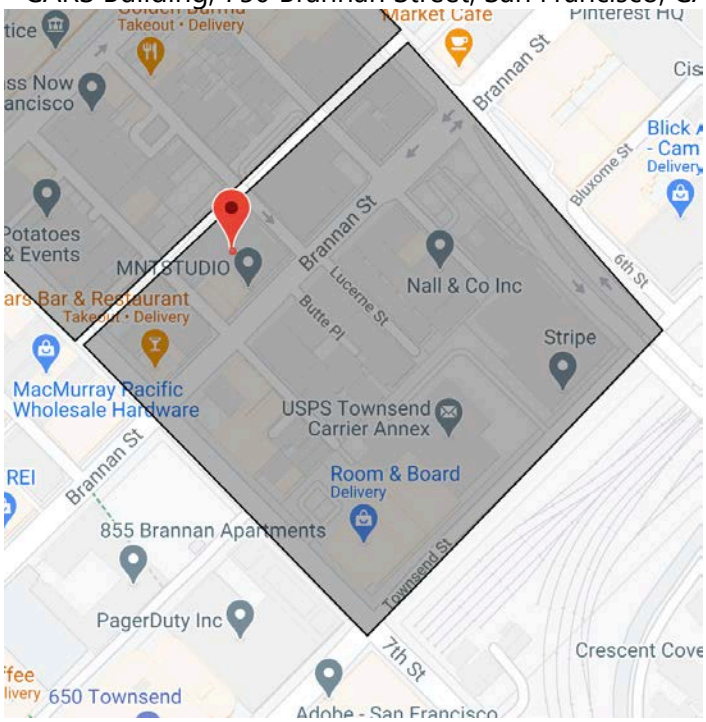


[Image description: The image shows a screenshot of a mapped area around Bayview Branch Library.]

Incident Category	Number of SFPD Incidents	Percent
Assault	38	0.149606
Burglary	6	0.023622
Courtesy Report	1	0.003937
Disorderly Conduct	9	0.035433
Drug Offense	4	0.015748
Forgery And Counterfeiting	1	0.003937
Fraud	7	0.027559
Larceny Theft	34	0.133858
Lost Property	5	0.019685
Malicious Mischief	18	0.070866
Miscellaneous Investigation	5	0.019685
Missing Person	5	0.019685
Motor Vehicle Theft	27	0.106299

Non-Criminal	6	0.023622
Offences Against The Family And Children	7	0.027559
Other Miscellaneous	27	0.106299
Other Offenses	6	0.023622
Robbery	8	0.031496
Suspicious Occ	7	0.027559
Traffic Collision	3	0.011811
Traffic Violation Arrest	7	0.027559
Warrant	13	0.051181
Weapons Carrying Etc	5	0.019685
Weapons Offense	5	0.019685

• CARS Building, 750 Brannan Street, San Francisco, CA 94103

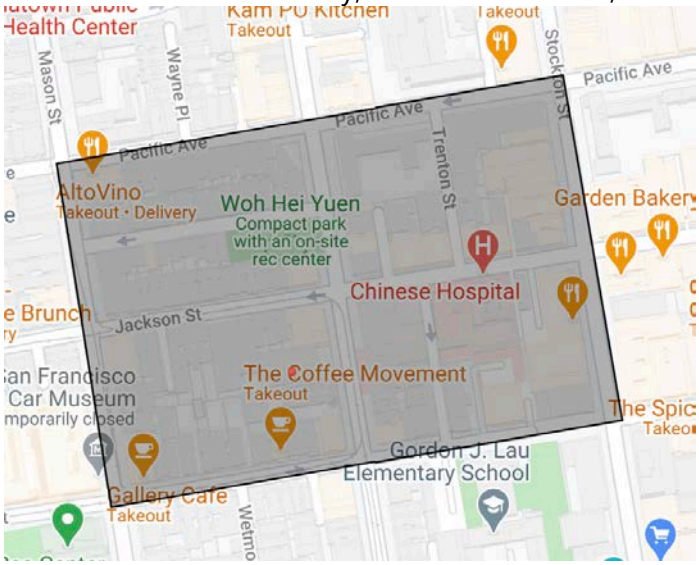


[Image description: The image shows a screenshot of a mapped area around the CARS Building at 750 Brannan Street.]

Incident Category	Number of SFPD Incidents	Percent
Arson	2	0.021505
Assault	4	0.043011
Burglary	11	0.11828
Disorderly Conduct	1	0.010753
Drug Offense	1	0.010753
Forgery And Counterfeiting	1	0.010753
Fraud	1	0.010753
Larceny Theft	23	0.247312

Malicious Mischief	14	0.150538
Missing Person	4	0.043011
Motor Vehicle Theft	4	0.043011
Non-Criminal	6	0.064516
Other Miscellaneous	10	0.107527
Robbery	1	0.010753
Stolen Property	1	0.010753
Suicide	2	0.021505
Suspicious Occ	1	0.010753
Warrant	5	0.053763
Weapons Offense	1	0.010753

• Chinatown Branch Library, 1135 Powell Street, San Francisco, CA 94108

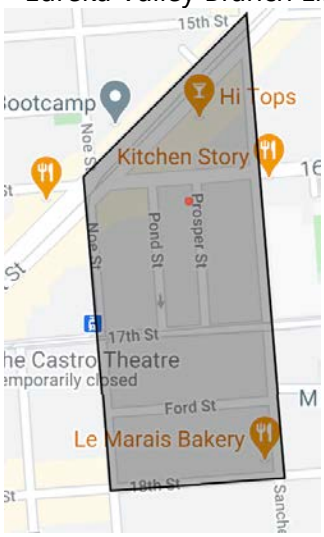


[Image description: The image shows a screenshot of a mapped area around Chinatown Branch Library.]

Incident Category	Number of SFPD Incidents	Percent
Arson	1	0.004098
Assault	13	0.053279
Burglary	14	0.057377
Disorderly Conduct	8	0.032787
Drug Offense	2	0.008197
Forgery And Counterfeiting	3	0.012295
Fraud	12	0.04918
Larceny Theft	54	0.221311
Lost Property	11	0.045082
Malicious Mischief	20	0.081967
Miscellaneous Investigation	4	0.016393

Missing Person	6	0.02459
Motor Vehicle Theft	17	0.069672
Non-Criminal	17	0.069672
Offences Against The Family And Children	7	0.028689
Other	4	0.016393
Other Miscellaneous	19	0.077869
Robbery	5	0.020492
Sex Offense	2	0.008197
Stolen Property	4	0.016393
Suspicious Occ	11	0.045082
Traffic Violation Arrest	1	0.004098
Warrant	4	0.016393
Weapons Carrying Etc	3	0.012295
Weapons Offense	2	0.008197

• Eureka Valley Branch Library, 1 Jose Sarria Court, San Francisco, CA 94114

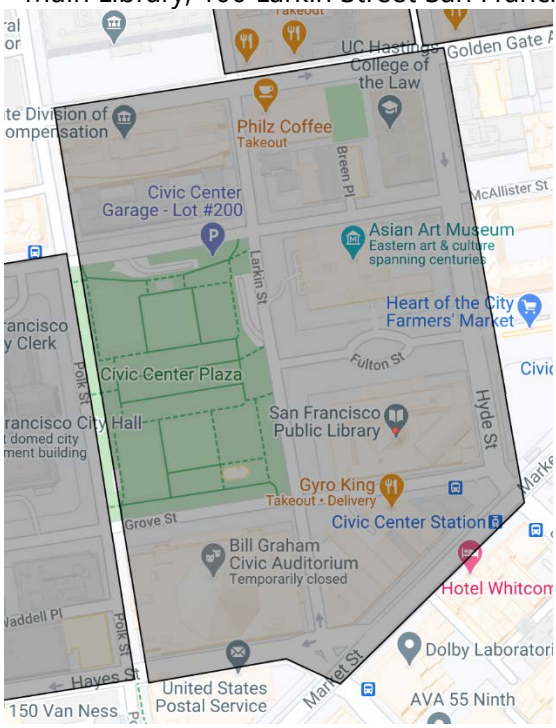


[Image description: The image shows a screenshot of a mapped area around Eureka Valley Branch Library.]

Incident Category	Number of SFPD Incidents	Percent
	2	0.004357
Arson	3	0.006536
Assault	26	0.056645
Burglary	43	0.093682
Civil Sidewalks	1	0.002179
Disorderly Conduct	1	0.002179
Drug Offense	8	0.017429
Forgery And Counterfeiting	4	0.008715

Fraud	20	0.043573
Larceny Theft	86	0.187364
Lost Property	5	0.010893
Malicious Mischief	47	0.102397
Miscellaneous Investigation	5	0.010893
Missing Person	4	0.008715
Motor Vehicle Theft	28	0.061002
Non-Criminal	28	0.061002
Offences Against The Family And Children	20	0.043573
Other	3	0.006536
Other Miscellaneous	57	0.124183
Other Offenses	1	0.002179
Recovered Vehicle	1	0.002179
Robbery	7	0.015251
Sex Offense	7	0.015251
Stolen Property	3	0.006536
Suspicious Occ	15	0.03268
Traffic Violation Arrest	6	0.013072
Vandalism	1	0.002179
Warrant	25	0.054466
Weapons Carrying Etc	2	0.004357

- Main Library, 100 Larkin Street San Francisco, CA 94102



[Image description: The image shows a screenshot of a mapped area around Main Library.]

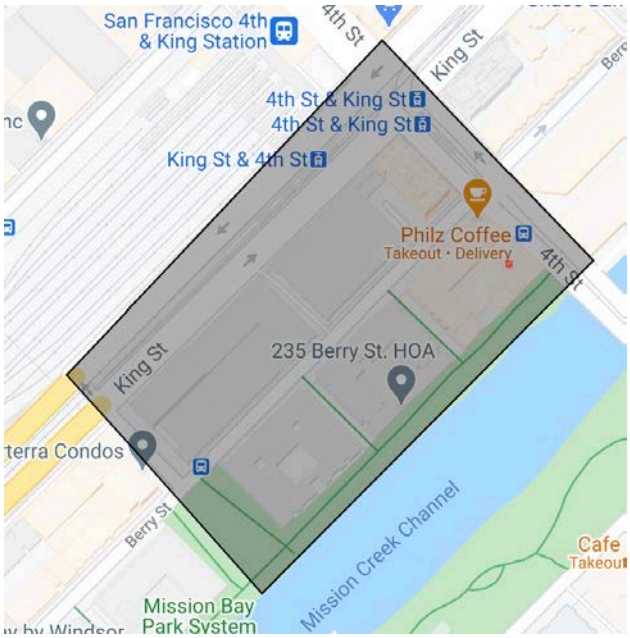
Incident Category	Number of SFPD Incidents	Percent
	5	0.002798
Arson	1	0.00056
Assault	123	0.06883
Burglary	23	0.012871
Courtesy Report	5	0.002798
Disorderly Conduct	16	0.008954
Drug Offense	640	0.358142
Drug Violation	1	0.00056
Fire Report	1	0.00056
Forgery And Counterfeiting	7	0.003917
Fraud	25	0.01399
Larceny Theft	159	0.088976
Lost Property	26	0.01455
Malicious Mischief	63	0.035255
Miscellaneous Investigation	9	0.005036
Missing Person	19	0.010632
Motor Vehicle Theft	33	0.018467
Non-Criminal	137	0.076665
Offences Against The Family And Children	29	0.016228
Other	31	0.017348
Other Miscellaneous	148	0.08282
Other Offenses	15	0.008394
Prostitution	1	0.00056
Recovered Vehicle	13	0.007275
Robbery	43	0.024063
Sex Offense	3	0.001679
Stolen Property	2	0.001119
Suspicious Occ	37	0.020705
Traffic Collision	4	0.002238
Traffic Violation Arrest	34	0.019026
Vandalism	3	0.001679
Vehicle Impounded	1	0.00056
Warrant	104	0.058198
Weapons Carrying Etc	13	0.007275
Weapons Offense	13	0.007275

- Marina Branch Library, 1890 Chestnut Street San Francisco, CA 94123

[Image description: The image shows a screenshot of a mapped area around Marina Branch Library.]

Incident Category	Number of SFPD Incidents	Percent
Assault	9	0.069231
Burglary	23	0.176923
Disorderly Conduct	3	0.023077
Fraud	3	0.023077
Larceny Theft	51	0.392308
Lost Property	6	0.046154
Malicious Mischief	6	0.046154
Miscellaneous Investigation	1	0.007692
Motor Vehicle Theft	6	0.046154
Non-Criminal	6	0.046154
Offences Against The Family And Children	2	0.015385
Other Miscellaneous	7	0.053846
Robbery	3	0.023077
Suspicious Occ	2	0.015385
Traffic Violation Arrest	1	0.007692
Warrant	1	0.007692

- Mission Bay Branch Library, 960 4th Street San Francisco, CA 94158

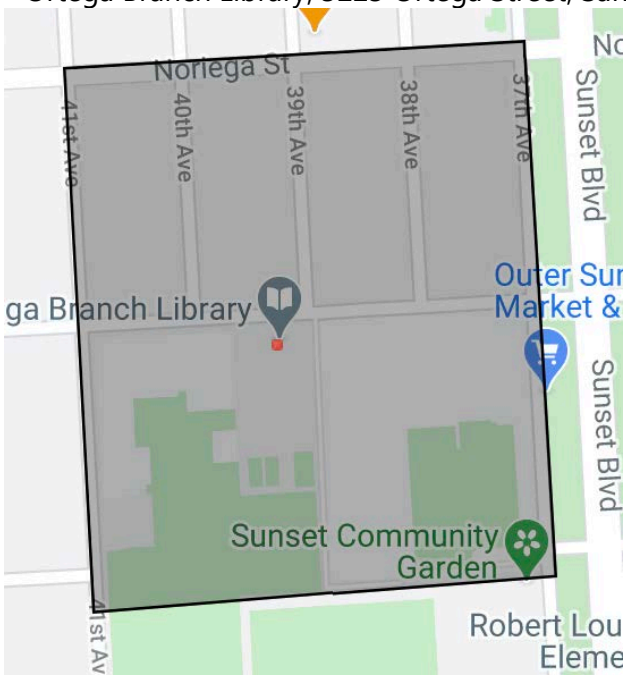


[Image description: The image shows a screenshot of a mapped area around Mission Bay Branch Library.]

Incident Category	Number of SFPD Incidents	Percent
Arson	2	0.007874
Assault	26	0.102362
Burglary	26	0.102362
Disorderly Conduct	5	0.019685
Drug Offense	2	0.007874
Fraud	10	0.03937
Larceny Theft	57	0.224409
Lost Property	12	0.047244
Malicious Mischief	14	0.055118
Missing Person	9	0.035433
Motor Vehicle Theft	8	0.031496
Non-Criminal	31	0.122047
Offences Against The Family And Children	3	0.011811
Other	5	0.019685
Other Miscellaneous	18	0.070866
Robbery	7	0.027559
Stolen Property	2	0.007874
Suspicious	1	0.003937
Suspicious Occ	7	0.027559
Traffic Violation Arrest	2	0.007874
Vandalism	1	0.003937
Warrant	2	0.007874

Weapons Carrying Etc	1	0.003937
Weapons Offense	3	0.011811

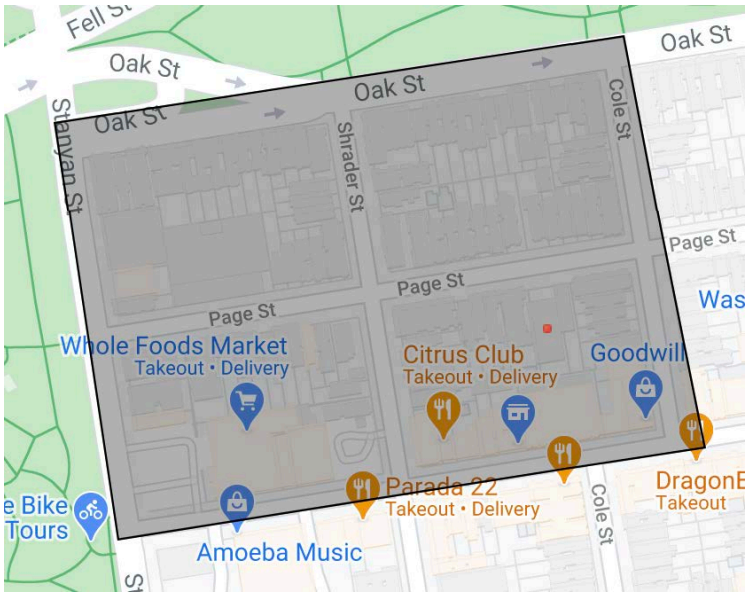
• Ortega Branch Library, 3223 Ortega Street, San Francisco CA, CA 94122



[Image description: The image shows a screenshot of a mapped area around Ortega Branch Library.]

Incident Category	Number of SFPD Incidents	Percent
Arson	1	0.022727
Assault	1	0.022727
Burglary	6	0.136364
Courtesy Report	1	0.022727
Disorderly Conduct	3	0.068182
Family Offense	1	0.022727
Fraud	3	0.068182
Larceny Theft	12	0.272727
Malicious Mischief	2	0.045455
Miscellaneous Investigation	1	0.022727
Missing Person	1	0.022727
Motor Vehicle Theft	3	0.068182
Non-Criminal	4	0.090909
Other Miscellaneous	2	0.045455
Robbery	2	0.045455
Vandalism	1	0.022727

• Park Branch Library, 1833 Page Street San Francisco, CA 94117

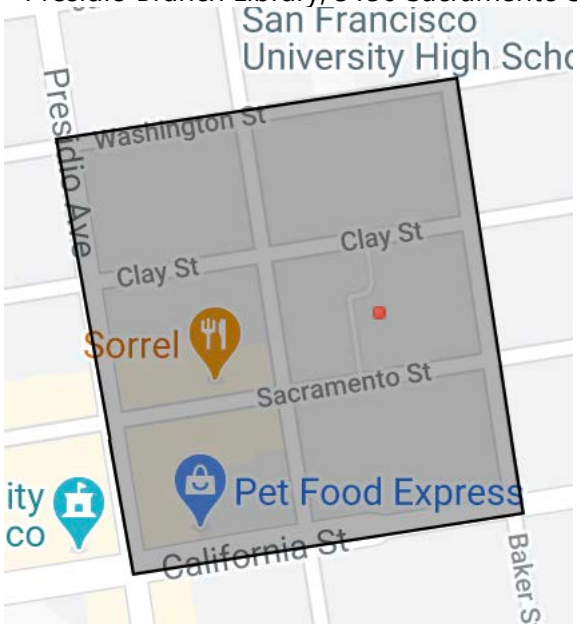


[Image description: The image shows a screenshot of a mapped area around Park Branch Library.]

Incident Category	Number of SFPD Incidents	Percent
Arson	1	0.004878
Assault	8	0.039024
Burglary	14	0.068293
Civil Sidewalks	4	0.019512
Disorderly Conduct	4	0.019512
Drug Offense	4	0.019512
Forgery And Counterfeiting	3	0.014634
Fraud	4	0.019512
Larceny Theft	78	0.380488
Lost Property	10	0.04878
Malicious Mischief	14	0.068293
Miscellaneous Investigation	1	0.004878
Missing Person	2	0.009756
Motor Vehicle Theft	9	0.043902
Non-Criminal	13	0.063415
Offences Against The Family And Children	2	0.009756
Other	1	0.004878
Other Miscellaneous	7	0.034146
Other Offenses	2	0.009756
Robbery	3	0.014634
Suspicious	1	0.004878
Suspicious Occ	8	0.039024
Traffic Violation Arrest	1	0.004878
Vandalism	1	0.004878

Warrant	7	0.034146
Weapons Carrying Etc	1	0.004878
Weapons Offense	2	0.009756

• Presidio Branch Library, 3150 Sacramento Street San Francisco, CA 94115

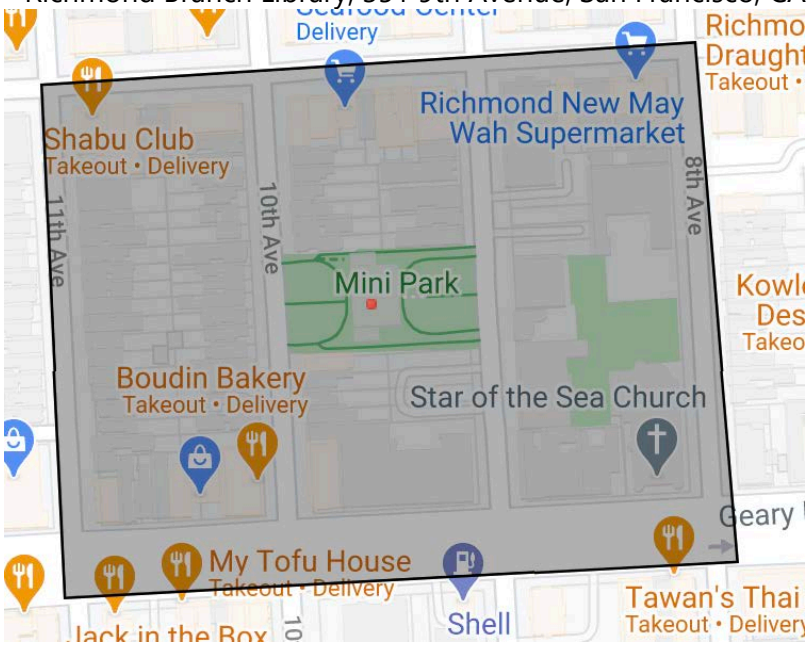


[Image description: The image shows a screenshot of a mapped area around Presidio Branch Library.]

Incident Category	Number of SFPD Incidents	Percent
	1	0.007692
Assault	4	0.030769
Burglary	25	0.192308
Disorderly Conduct	1	0.007692
Forgery And Counterfeiting	1	0.007692
Fraud	4	0.030769
Larceny Theft	40	0.307692
Lost Property	3	0.023077
Malicious Mischief	14	0.107692
Miscellaneous Investigation	4	0.030769
Missing Person	2	0.015385
Motor Vehicle Theft	10	0.076923
Non-Criminal	7	0.053846
Other Miscellaneous	6	0.046154
Other Offenses	1	0.007692
Robbery	1	0.007692
Suspicious Occ	2	0.015385

Traffic Collision	1	0.007692
Vandalism	1	0.007692
Weapons Carrying Etc	1	0.007692
Weapons Offense	1	0.007692

• Richmond Branch Library, 351 9th Avenue, San Francisco, CA 94118

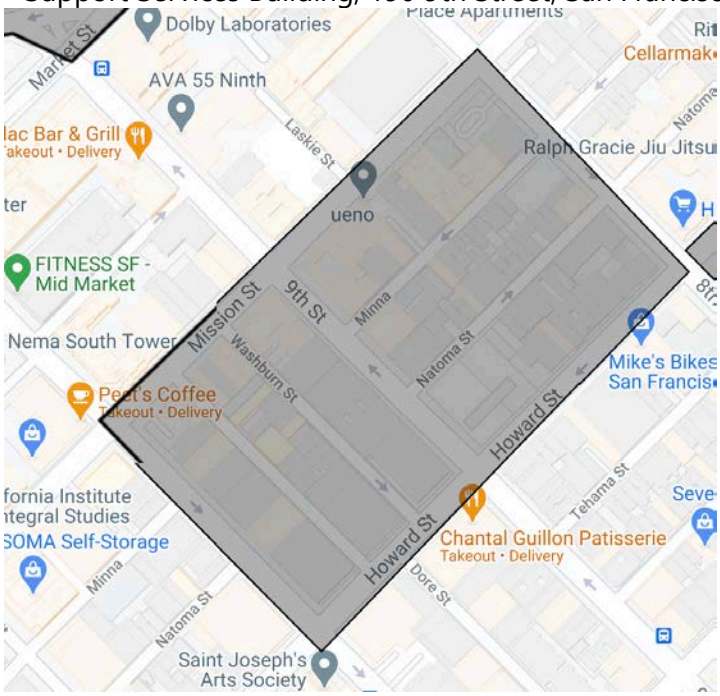


[Image description: The image shows a screenshot of a mapped area around Richmond Branch Library.]

Incident Category	Number of SFPD Incidents	Percent
Assault	13	0.057522
Burglary	21	0.09292
Disorderly Conduct	2	0.00885
Family Offense	1	0.004425
Human Trafficking (A), Commercial Sex Acts	1	0.004425
Larceny Theft	89	0.393805
Lost Property	11	0.048673
Malicious Mischief	26	0.115044
Miscellaneous Investigation	2	0.00885
Missing Person	1	0.004425
Motor Vehicle Theft	7	0.030973
Non-Criminal	7	0.030973
Offences Against The Family And Children	2	0.00885
Other	1	0.004425
Other Miscellaneous	18	0.079646

Other Offenses	1	0.004425
Recovered Vehicle	1	0.004425
Robbery	8	0.035398
Suspicious Occ	4	0.017699
Traffic Violation Arrest	2	0.00885
Warrant	5	0.022124
Weapons Offense	3	0.013274

• Support Services Building, 190 9th Street, San Francisco, CA 94103

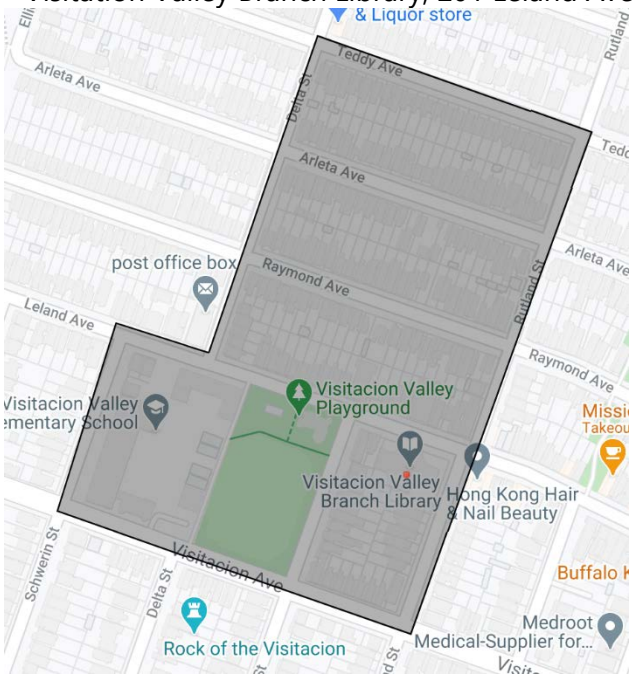


[Image description: The image shows a screenshot of a mapped area around Support Services Building at 190 9th Street.]

Incident Category	Number of SFPD Incidents	Percent
	7	0.007865
Arson	1	0.001124
Assault	72	0.080899
Burglary	54	0.060674
Disorderly Conduct	16	0.017978
Drug Offense	119	0.133708
Forgery And Counterfeiting	1	0.001124
Fraud	16	0.017978
Larceny Theft	137	0.153933
Lost Property	8	0.008989
Malicious Mischief	76	0.085393
Miscellaneous Investigation	12	0.013483

Missing Person	10	0.011236
Motor Vehicle Theft	28	0.031461
Non-Criminal	84	0.094382
Offences Against The Family And Children	18	0.020225
Other	20	0.022472
Other Miscellaneous	74	0.083146
Other Offenses	6	0.006742
Rape	1	0.001124
Recovered Vehicle	3	0.003371
Robbery	17	0.019101
Sex Offense	3	0.003371
Stolen Property	4	0.004494
Suspicious Occ	19	0.021348
Traffic Collision	2	0.002247
Traffic Violation Arrest	16	0.017978
Vandalism	4	0.004494
Warrant	48	0.053933
Weapons Carrying Etc	6	0.006742
Weapons Offense	8	0.008989

• Visitation Valley Branch Library, 201 Leland Avenue San Francisco, CA 94134

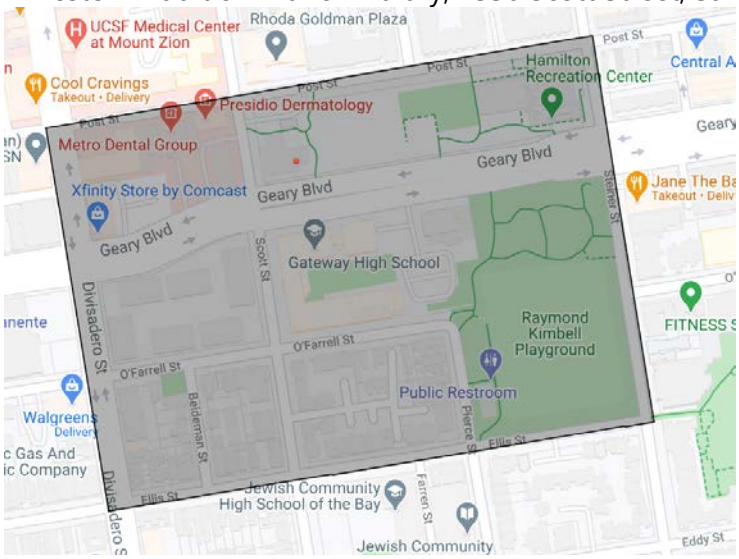


[Image description: The image shows a screenshot of a mapped area around the Visitation Valley Branch.]

Incident Category	Number of SFPD Incidents	Percent

Arson	1	0.012821
Assault	7	0.089744
Burglary	4	0.051282
Family Offense	1	0.012821
Fire Report	1	0.012821
Fraud	8	0.102564
Larceny Theft	19	0.24359
Malicious Mischief	5	0.064103
Motor Vehicle Theft	10	0.128205
Non-Criminal	2	0.025641
Offences Against The Family And Children	3	0.038462
Other Miscellaneous	7	0.089744
Recovered Vehicle	1	0.012821
Robbery	3	0.038462
Suspicious Occ	3	0.038462
Vandalism	1	0.012821
Vehicle Impounded	1	0.012821
Weapons Carrying Etc	1	0.012821

• Western Addition Branch Library, 1550 Scott Street, San Francisco, CA 94115

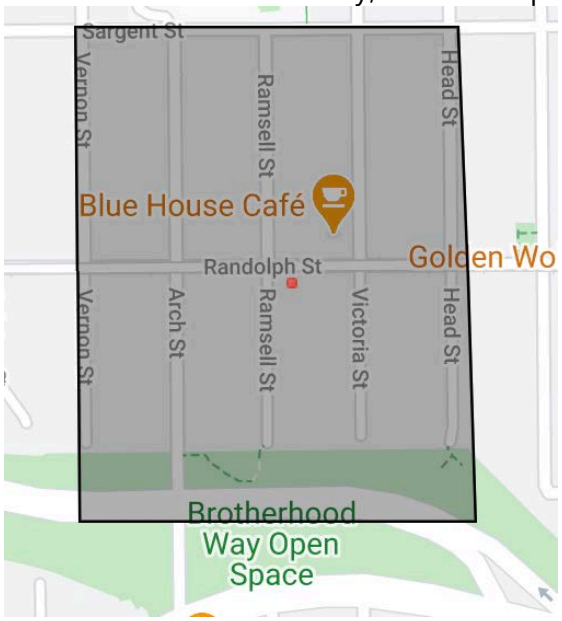


[Image description: The image shows a screenshot of a mapped area around the Western Addition Branch.]

Incident Category	Number of SFPD Incidents	Percent
Assault	17	0.050445
Burglary	23	0.068249
Courtesy Report	1	0.002967
Disorderly Conduct	5	0.014837

Drug Offense	1	0.002967
Embezzlement	1	0.002967
Fraud	15	0.04451
Larceny Theft	124	0.367953
Lost Property	5	0.014837
Malicious Mischief	31	0.091988
Missing Person	2	0.005935
Motor Vehicle Theft	10	0.029674
Non-Criminal	22	0.065282
Offences Against The Family And Children	10	0.029674
Other	2	0.005935
Other Miscellaneous	20	0.059347
Other Offenses	3	0.008902
Robbery	12	0.035608
Sex Offense	1	0.002967
Stolen Property	3	0.008902
Suspicious Occ	9	0.026706
Traffic Violation Arrest	1	0.002967
Vandalism	1	0.002967
Vehicle Misplaced	1	0.002967
Warrant	12	0.035608
Weapons Carrying Etc	1	0.002967
Weapons Offense	4	0.011869

• Ocean View Branch Library, 345 Randolph Street, San Francisco, CA 94132



[Image description: The image shows a screenshot of a mapped area around the Ocean View Branch.]

Incident Category	Number of SFPD Incidents	Percent
	1	0.017241
Assault	3	0.051724
Burglary	1	0.017241
Disorderly Conduct	2	0.034483
Forgery And Counterfeiting	1	0.017241
Fraud	5	0.086207
Larceny Theft	6	0.103448
Lost Property	1	0.017241
Malicious Mischief	4	0.068966
Miscellaneous Investigation	2	0.034483
Missing Person	3	0.051724
Motor Vehicle Theft	10	0.172414
Non-Criminal	4	0.068966
Offences Against The Family And Children	1	0.017241
Other	2	0.034483
Other Miscellaneous	3	0.051724
Other Offenses	1	0.017241
Robbery	2	0.034483
Suspicious Occ	4	0.068966
Warrant	1	0.017241
Weapons Offense	1	0.017241

Information on crime statistics in 2020 in this area is provided by the San Francisco Police Department. Statistics are taken from a 1-block radius around the location of cameras. All information is obtained through the San Francisco Open Data Portal: https://datasf.org/opendata/

In addition, the department maintains an internal incident log which is available on request.

Surveillance Technology Policy

San Francisco Public Library
Security Cameras

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 Department's Security Camera System 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

The San Francisco Public Library (SFPL) system is dedicated to free and equal access to information, knowledge, independent learning and the joys of reading for our diverse community.

The Surveillance Technology Policy ("Policy") defines the manner in which the Johnson Controls P2000 Security Management System - Video System will be used to support department operations.

This Policy applies to all Department personnel that use, plan to use, or plan to secure the Johnson Controls P2000 Security Management System - Video System, including employees, contractors, and volunteers. Employees, consultants, volunteers, and vendors while working on behalf of the City with SFPL are required to comply with this Policy.

POLICY STATEMENT

The use of Johnson Controls P2000 Security Management System - Video System technology for the San Francisco Public Library is limited to the following authorized use cases and requirements listed in this Policy.

Authorized Use(s):

1. Live monitoring to protect safety of SFPL staff, patrons and facilities.
2. Recording of video and images.
3. Reviewing camera footage in the event of an incident.
4. Providing video footage/images to law enforcement or other authorized persons following an incident or upon request.

Prohibited use cases include any uses not stated in the Authorized Use Case section.

Departments may use information collected from security cameras only for legally authorized purposes, and may not use that information to unlawfully discriminate against people based on race, ethnicity, political opinions, religious or philosophical beliefs, trade union membership, gender, gender identity, disability status, sexual orientation or activity, or genetic and/or

biometric data. Additionally, departments may not use automated systems to scan footage and identify individuals based on any of the categories listed in the preceding sentence.

BUSINESS JUSTIFICATION

In support of SFPL operations, the Johnson Controls P2000 Security Management System - Video System promises to help with:

	▪ Education	
	▪ Community Development	
X	Health	Protect safety of SFPL staff, patrons and facilities while promoting an open and welcoming environment.
	▪ Environment	
X	Criminal Justice	Review video footage after a security incident; provide video evidence to law enforcement or other authorized persons following an incident or upon request.
	▪ Jobs	
	▪ Housing	
X	Other	Better management of city assets by leveraging remote condition assessment. Improvement of overall situational awareness.

In addition, the following benefits are obtained:

Benefit		Description
X	Financial Savings	Security cameras will save on need for building or patrol officers.
X	Time Savings	Security cameras will run 24/7/365, thus decreasing need for building or patrol officer supervision.
X	Staff Safety	Security cameras help identify violations of City Employee's Code of Conduct, SFPL Patron Code of Conduct, and City, State and Federal law and provide assurance that staff safety is emphasized and will be protected at their place of employment.
X	Data Quality	Security cameras run 24/7/365 so full-time staffing is not required to subsequently review footage of security incidents. Data resolution can be set by level and is currently set to high resolution.
X	Service Levels	Security cameras will enhance effectiveness of incident response and result in improved level of service.

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 Johnson Controls P2000 Security Management System - Video System must be kept up-to-date and maintained.

Data Collection: Department shall only collect data required to execute the authorized use case. 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 types:

Data Type(s)	*Format(s)*	*Classification*
Video and Images	MP4, AVI, MPEG	Level 3
Date and Time	MP4 or other format	Level 3
Geolocation data	TXT, CSV, DOCX	Level 3

Notification: Departments shall notify the public of intended 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. Department notifications shall identify the type of technology being used and the purpose for such collection.

The Department's public notice will include the following items:

X Information on the surveillance technology

X Description of the authorized use

- Type of data collected
- Will persons be individually identified
- Data retention

	X Department identification X Contact information
Access:	Prior to accessing or using data, authorized individuals receive training in system access and operation, and instruction regarding authorized and prohibited uses. Access to live views and recorded footage is restricted to specific trained personnel. Recorded footage is accessed only in response to an incident. Details on department staff and specific access are available in Appendix A.
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. Departments shall, at minimum, apply the following safeguards to protect surveillance technology information from unauthorized access and control, including misuse: - Encryption: Data retained by the Department will be encrypted. Raw data may be retained by the Department only for the authorized use case of sharing with law enforcement or the public. - Storage: Any use of a third-party service provider must meet City's cyber security requirements. - Audits: A data access log will be maintained by the Department for all the Johnson Controls P2000 Security Management System - Video System data that is processed and utilized. This log will include but is not limited to the following: date/time data was originally obtained/collected, reasons/intended use for data, department requesting data, date/time of access of raw data, outcome of data processing, as well as date processed data was delivered to users.
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 will endeavor to ensure that other agencies or departments that may receive data collected by the Johnson Controls P2000 Security Management System - Video System will act in conformity with this Surveillance Technology 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.

Each department that believes another agency or department receives or may receive data collected from its use of Johnson Controls P2000 Security Management System - Video System should consult with its assigned Deputy City Attorney regarding their response.

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

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

SFPL 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.

The Department may share Johnson Controls P2000 Security Management System - Video System footage with the following entities:

A. Internal Data Sharing:

In the event of an incident, Johnson Controls P2000 Security Management System - Video System images may be live-streamed or shared by alternative methods to the following agencies:

- Within the San Francisco Public Library
- Police
- City Attorney
- District Attorney

- Sheriff
- On request following an incident.

Data sharing occurs at the following frequency:

- As needed.

B. External Data Sharing:

- Other local law enforcement agencies, via formal process, order or subpoena, per the San Francisco Public Library Privacy Policy.

Data sharing occurs at the following frequency:

- As needed.

Data Retention:

Department may store and retain raw PII data only as long as necessary to accomplish a lawful and authorized purpose. Department data retention standards should align with how the department prepares its financial records and should be consistent with any relevant Federal Emergency Management Agency (FEMA) or California Office of Emergency Services (Cal OES) sections.

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

- Johnson Controls P2000 Security Management System - Video System data currently will be stored for a minimum of four (4) months as SFPL seeks to expand server capacity to meet State requirements of a minimum of one (1) year to authorized staff for operational necessity and ready reference, subject to technical limitations.

  If data is associated with an incident, it may be kept for longer than the standard retention period.

- Justification: This retention period conforms with the available server system storage space and allows for ample time for security staff to review footage related to security incidents and/or external requests for records.

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.)

X Department of Technology Data Center

X Software as a Service Product

X Cloud Storage Provider

Data Disposal:	Upon completion of the data retention period, Department shall dispose of data in the following manner: - Automatic overwrite of all existing files when standard data retention period ends. This may take the form of a delete/reformat, wipe, overwrite of existing data, or degaussing.
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 must receive training on data security policies and procedures. - Annual cybersecurity training (COIT Policy Link)

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.

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.

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.

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."

Appendix A: Department Specific Responses

1. A description of the product, including vendor and general location of technology.

The Johnson Controls P2000 security management system (https://author.johnsoncontrols.com/en_gb/buildings/security-and-fire-safety/access-controls) helps organizations achieve maximum security while increasing efficiencies and lowering costs. Built on open standards and compatible with virtually any third party program, the P2000 can integrate multiple businesses, buildings and security systems to achieve interactive, real-time security management. The P2000's built-in web browser allows users to access the platform from a central location — or remotely, through web-connected devices.

Security cameras record and retain video footage of public and non-public spaces within and on the exterior of 15 facilities of the San Francisco Public Library. That video footage is stored on a server system that lives on the 6th Floor of the Main Library. Video footage is then accessible for review by authorized users within the organization, local law enforcement, including the Sheriff's Department (per existing MOU), or, can be shared externally, upon request, given policy constraints enumerated herein.

2. The specific categories and titles of individuals who are authorized by the Department to access or use the collected information

Access to SFPL security camera data is restricted to staff with specific needs related to protecting the safety of SFPL staff, patrons and facilities while in or around library locations. Training and user access restrictions will prevent unauthorized access and use of the security camera software, including misuse.

Access to the information includes 23 8207 Grounds and Patrol Officers, 3 8211 Ground and Patrol Supervisors, the 0923 Manager of Security Operations and Emergency Planning, the 0923 Manager of Buildings and Engineering, the 0932 Director of Facilities, the 0953 Chief Operating Officer and the 0964 City Librarian. The Sheriff's Department also has access to security camera footage, per existing MOU for onsite support at the Main Library.

All other staff requesting access to this data must make a formal written request to the Facilities Division, pending approval by the Chief Operating Officer or the City Librarian. These protocols ensure limited access to security camera footage among SFPL staff.

3. What procedures will be put in place by which members of the public can register complaints or concerns, or submit questions about the deployment or use of a specific Surveillance Technology, and how the Department will ensure each question and complaint is responded to in a timely manner.

Public: Members of the public can register complaints/concerns or submit questions in writing via the library's chat service, or "Comments and Suggestions" page online, or in person at the City Librarian's Office, Main Library, 100 Larkin Street, San Francisco 94102. They can also contact the library through telephone at 415-557-4400 or email at info@sfpl.org. All questions and complaints are forwarded to the proper SFPL division for appropriate and timely responses.

City and County of San Francisco Employees: All questions regarding this policy should be directed to the employee's supervisor or to the division chief. Similarly, questions about other applicable laws governing the use of the surveillance technology or the issues related to privacy should be directed to the employee's supervisor or division chief.

4. Specific details on where data will be stored (local, DT, SaaS, Cloud Storage) including name of vendor and retention period.

Security camera data is stored on a local server at the Main Library and is maintained remotely by Johnson Controls, Inc. The retention period for this data is related to server capacity, and it is currently holding approximately 4 months of footage before being overwritten. SFPL recognizes that there is a 1-year storage requirement per the California Public Records Act, and is working toward increasing capacity to comply with state law.

5. Questions & Concerns

Public: Members of the public can register complaints/concerns or submit questions in writing via the library's chat service, or "Comments and Suggestions" page online, or in person at the City Librarian's Office, Main Library. They can also contact the library through telephone at 415-557-4400 or email at info@sfpl.org. All questions and complaints are forwarded to the proper SFPL division for appropriate and timely responses.

City and County of San Francisco Employees: All questions regarding this policy should be directed to the employee's supervisor or to the division chief. Similarly, questions about other applicable laws governing the use of the surveillance technology or the issues related to privacy should be directed to the employee's supervisor or division chief.

Surveillance Impact Report

San Francisco Public Utilities Commission (SFPUC)
Security Cameras

As required by San Francisco Administrative Code, Section 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 surveillance cameras.

DESCRIPTION OF THE TECHNOLOGY

The San Francisco Public Utilities Commission (SFPUC) aims to provide our customers with high quality, efficient and reliable water, power, and sewer services in a manner that is inclusive of environmental and community interests, and that sustains the resources entrusted to our care.

Security Cameras are used to deter malicious behavior, capture potential or actual malicious behavior by or against SFPUC facilities, employees, or personnel working on behalf of SFPUC. Provide evidence to support incident investigations. Provide real-time monitoring of operations and critical equipment at SFPUC facilities. Support SFPUC health and safety requirements and objectives. Monitor wildlife/game, vegetation, and water flow management.

In line with its mission, the Department shall use security cameras only for the following authorized purposes:

Authorized Use(s):

1. Live monitoring.
2. Recording of video and images in the event of an incident.
3. Reviewing camera footage.
4. Providing video footage/images to law enforcement or other authorized persons following an incident.

Prohibited use cases include any uses not stated in the Authorized Use Case section.

Further, processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, gender, gender identity, disability status, or an individual person's sex life or sexual orientation, and the processing of genetic data and/or biometric data for the purpose of uniquely identifying an individual person shall be prohibited.

Department technology may be deployed in the following locations, based on use case:

SFPUC surveillance cameras are located in public areas of SFPUC facilities. Additional cameras are used to monitor wildlife/game, vegetation, and water flow management in exterior areas of SFPUC facilities.

Surveillance Oversight Review Dates
COIT Review: March 18, 2021
Board of Supervisors Review: TBD

Technology Details

The following is a product description:

Axis offers a wide portfolio of IP-based products and solutions for security and video surveillance. Our security cameras, video encoders, accessories and access control products are based on open industry standards. The products integrate easily with Axis' video management software, or with a partner product, to build a complete security or surveillance solution.

A. How It Works

The technology's primary functions are to provide live views and record video footage to a dedicated, secure server. The system is comprised of multiple cameras connected by data cables and infrastructure to the server. The footage is recorded on the server and stored for a maximum of 30 days.

Data collected or processed by security cameras will not be handled or stored by an outside provider or third-party vendor on an ongoing basis. The Department will remain the sole Custodian of Record.

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 security cameras has the following benefits for the residents of the City and County of San Francisco:

- Education
- Community Development

X	Health	*The technology helps ensure that the City's critical infrastructure can effectively carry out its mission, which would have underlying health consequences for the general public if non-operational.*
X	Environment	*Natural Resources (NRD) utilize the technology to monitor wildlife and vegetation located within SFPUC sites.*

X	Criminal Justice	*The technology is used to capture an event that may or may not include the SFPUC or its facilities, assets, or employees that necessitates action from law enforcement and requires video surveillance for a supporting law enforcement investigation.*
▪	Jobs	
▪	Housing	
X	Other	*The technology helps ensure that the City's critical infrastructure is in continuous operation, these operations are used to provide high quality, efficient and reliable water, power, and sewer services.*

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:

The San Francisco Public Utilities Commission (SFPUC) is committed to addressing potential civil rights/liberties impacts associated with surveillance technology, including but not limited to Critical Infrastructure Cameras (CICs). We implement administrative safeguards such as POL-EPS-001, Security Video Footage Release and Playback Policy that details the purpose of SFPUC security system cameras and video surveillance equipment. This Policy also outlines the circumstances under which this security footage may be accessed. Specifically, the Emergency Planning and Security (EPS) director shall only permit the viewing of supervised security footage playback according to (1) local, state or federal law enforcement involvement or request, (2) SFPUC incident investigation, (3) SFPUC Human Resource Services or Department of Human Resources investigation. EPS shall not entertain or fulfill requests for playback viewing from employees, consultants, contractors, vendors, others acting at the direction of the SFPUC, or members of the public. As such, the CICs cannot be used to monitor anything other than for its intended purpose explained below. This technology is utilized to record a visual representation of events occurring at or around SFPUC facilities, assets, and project sites. Footage is stored for thirty (30) days prior to deletion when it can no longer be recovered. In the event of an incident, Emergency Planning & Security (EPS) maintains the authority to operate, manage, monitor and archive all footage from any SFPUC facility. Playback requests are only permitted according the four (4) use cases previously noted or at the discretion of the SFPUC General Manager, Deputy General Manager, or EPS Director.

All SFPUC Enterprises, Bureaus and staff will adhere to this Policy. The only instance where this policy does not apply is for wildlife/game and go-pro cameras that are rotated at various locations on SFPUC watershed land that is generally accessible to the public and which are used for vegetation and water flow management purposes.

C. Fiscal Analysis of Costs and Benefits

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

Benefit		Description
X	Financial Savings	*Department Security Camera Systems will save on building or patrol officers. The system is also used to prevent loss through theft or vandalism.*
X	Time Savings	*Department Security Camera Systems will run 24/7, thus eliminating building or patrol officer supervision. The system can also ensure that operational issues are resolved in a timely manner.*
X	Staff Safety	*Security cameras help identify violations of policy and provide assurance that staff safety is emphasized and will be protected at their place of employment. The system is also used to prevent personal injury to staff and ensure compliance with SFPUC health and safety requirements/objectives.*
X	Data Quality	*Security cameras run 24/7/365 so full-time staffing is not required to subsequently review footage of security incidents.*

The total fiscal cost, including initial purchase, personnel and other ongoing costs is Number of FTE (new & existing)	.25 FTE	
Classification	0931 – Director of Security & Asset Protection 1054 – Principal IS Business Analyst 1044 – Principal IS Engineer Total expected staff hours: 10 hrs/week $42,000 total per year for all employees	
	Annual Cost	***One-Time Cost***
Software	Milestone: $3,182 Lenel: $5,000	
Hardware/Equipment	One Camera: $2,517.00	
Professional Services	$100,000/yr	
Training	*Milestone: $1,995* *Lenel: $6,000*	
Other		
Total Cost	***$160,695 per year***	

Below is a breakdown of the cost for SFPUC to retain video data for one year (vs the current policy of 30 days).

- Cloud storage on GCP (committed allocation egress/overages included) – estimate = $86,365 / month (assumes 2.5PB of storage… yes petabytes…)
- Cloud compute resources on GCP for video archive post-processing (down-sampling, compression, AI+ML computer vision analytics) = $36,052 / month
- Local storage gateways (x5) to support "drip feed" and staging/tiering of video archive = $47,083 / month (lease cost)
- Added DIA bandwidth charges to support constant video archive tiering or direct peering with cloud storage provider = $15,500 / month
- Assume expansion/growth in the costs of these services annually at 15% (additional cameras, higher resolution cameras, new sites, etc.)

Educated guess (and this is a very high level estimate) for SFPUC to retain 12 months of video surveillance data ~ $2,553,000 (annually)

The Department funds its use and maintenance of the surveillance technology through an Annual Operating Budget.

COMPARISON TO OTHER JURISDICTIONS

Surveillance Camera Technologies like the San Francisco Public Utilities Commission (SFPUC) Surveillance Camera System are currently utilized by other governmental entities for similar purposes.

APPENDIX A: Crime Statistics

Department: Public Utilities Commission

Section 19B requires each department in their Surveillance Impact Report to respond to the following question if applicable, "the general location(s) [of the surveillance technology] may be deployed and crime statistics for any location(s)."

The Public Utilities Commission operates a total of 37 Security Cameras in public areas. Public Utilities Commission locations include public wastewater facilities over seven counties.

The department maintained an internal incident log for 2020:

Category	**Number of Incidents**	**% of Incidents**
Assault	2	0.81%
Fire	17	6.88%
Other	73	29.55%
Robbery/theft (or attempted)	18	7.29%
Threat	4	1.62%
Trespassing	67	27.13%
Vandalism	35	14.17%
Vehicle Accident	31	12.55%
Grand Total	**247**	**100%**

Title:	**Security Video Footage Release and Playback Policy**	Effective Date: February 9, 2021
Business Owner:	Emergency Planning and Security	Supersedes: N/A
Applicable To:	All SFPUC	Review Cycle: Minimum 2 years
Document No:	POL-EPS-001	
Page **1** of **5**		

1. PURPOSE

The San Francisco Public Utilities Commission (SFPUC) has a robust security system that includes hundreds of operating and planned project cameras. These cameras are distributed across the Water, Wastewater and Power Enterprises, and have the capacity to record video footage 24 hours per day, 7 days per week, and store security footage for up to thirty (30) days as is permitted by network capabilities.

The purpose of SFPUC security system cameras and video surveillance equipment is to:

1. Deter malicious behavior to SFPUC facilities, employees, or personnel working on behalf of the SFPUC;
2. Capture potential or actual malicious behavior by or against SFPUC facilities, employees, or personnel working on behalf of the SFPUC;
3. Provide evidence to support incident investigations;
4. Provide real-time monitoring of operations and critical equipment at SFPUC facilities; and
5. Support SFPUC health and safety requirements and objectives.

This Policy will outline the circumstances under which this security footage may be accessed by law enforcement, SFPUC personnel and the public.

2. SCOPE

This Policy applies to all video footage that is captured by SFPUC security cameras. This Policy applies to all SFPUC employees, consultants, contractors, vendors, and others who are otherwise acting at the direction of the SFPUC.

This Policy applies to all video footage and camera equipment that is currently installed or will be installed in future SFPUC projects.

Surveillance Oversight Review Dates
COIT Review: March 18, 2021
Board of Supervisors Review: TBD

Exceptions to this Policy will only be granted by written authorization by the SFPUC General Manager, Deputy General Manager, or Emergency Planning and Security (EPS) Director. Any granted exceptions will be documented and kept recorded in accordance with the SFPUC Records Retention Policy.

3. RESPONSIBILITY

3.1. All employees, consultants, contractors, vendors, and others referenced above are to familiarize themselves with this policy.

3.2. The SFPUC General Manager will understand and enforce this Policy.

3.3. All SFPUC Enterprises, Bureaus and staff will adhere to this Policy. All contracted staff performing work under the direction of SFPUC Enterprises, Bureaus and staff will adhere to this Policy.

3.4. When appropriate, Attorneys for the Department are asked to review, provide strategic direction to, and approve this policy.

3.5. The SFPUC Emergency Planning and Security (EPS) Director and staff will implement this Policy. EPS will maintain the authority to operate, manage, monitor and archive all video footage from any SFPUC facility. The following EPS employees are authorized by the Department to access or use the collected information:

Classification & Job Title	Employee Name
0931 – Director of Security	Jeff Harp
0932 –Emergency Planning Director	Josh Gale
1844 – Senior Management Assistant	Oscar Miron
1822 – EPS Administrative Analyst	N/A
1820 – EPS Junior Administrative Analyst	Stephanie Marquez
1054 – Principal IS Business Analyst	Marcus Coleman
5291 – Training & Exercise Planner III	Stephanie Murti

3.6. EPS shall ensure compliance with the Policy by holding an initial and periodic meeting with involved parties regarding the appropriate and inappropriate use of the security video technology. EPS will also send SFPUC staff important updates, deadlines, and reminders on a regular basis.

3.7. The SFPUC will adhere to security industry standards in order to ensure that all video security and applications are within best practices and compliant with local, state and federal regulations. All video surveillance footage recording, and monitoring shall be conducted in a professional, legal and ethical manner.

3.8. Members of the public are not required to be familiar with this Policy. The purpose of SFPUC security cameras and subsequent captured footage is not to gather information about the public. However, if a member of the public requests footage for personal use, this Policy may be provided to better inform the requesting party of SFPUC's standard operating procedure.

3.9. SFPUC EPS has various communication channels available to ensure that members of the public can register complaints, concerns or submit questions. By emailing info@sfwater.org, calling our General Inquiries phone number (415) 554-3289, or sending a letter to 525 Golden Gate Avenue, 10th floor, San Francisco, CA 94102 EPS shall ensure that all concerns are addressed.

4. DEFINITIONS

Camera: Refers to any device installed, operated and maintained by the SFPUC or its designees to capture video surveillance footage for any of the reasons outlined in Section 1.

Emergency Planning and Security (EPS): Any staff member of the Emergency Planning and Security Division of the SFPUC.

Video Footage: Any digital representation of events that are captured and recorded by SFPUC security camera equipment. Stored in digital formats on network video recorders.

Playback: The process of reviewing recorded, stored or archived footage.

5. POLICY

5.1. Security Footage Capture

All fully functioning SFPUC cameras should capture and record visual representation of events occurring at or around SFPUC facilities, assets and project sites. Footage is recorded and stored at the relevant security system server for thirty (30) days. Footage is automatically deleted after thirty (30) days and cannot be retrieved.

Due to the placement of the cameras and 24/7 video monitoring capabilities, events such as traffic accidents, malicious behavior not associated with the SFPUC or

SFPUC facilities, and the actions of the general public may be captured. However, this footage will not be released to SFPUC employees or the public for personal use.

Collected information cannot be accessed or used by members of the public, governmental agencies, departments, bureaus, divisions, or units not detailed below.

5.2. Playback Requests

Only designated personnel and security staff from ITS and EPS have access to live streaming video and/or footage playback. Depending on designated job duties, viewing access and playback access may be limited. Authorized employees receive briefing on policy and respective playback capabilities.

Designated personnel with access to video playback shall not entertain or fulfill requests for playback viewing from employees, consultants, contractors, vendors, others acting at the direction of the SFPUC, or members of the public. All requests to view playback of footage must be made directly to the Emergency Planning Director and Director of Security.

The Director of Security or designee will permit the viewing of supervised security footage playback in the following circumstances:

5.2.1 Local, state or federal law enforcement involvement or request – An event that may or may not include the SFPUC or its facilities, assets, or employees that necessitates action from law enforcement and requires video evidence for a supporting law enforcement investigation

5.2.2 SFPUC incident investigation – An event that includes SFPUC facilities or personnel and includes potential or actual malicious behavior by or against the SFPUC, or an event that includes SFPUC facilities or personnel and includes evidence of critical operations and/or equipment functions including health and safety considerations

5.2.3 SFPUC Human Resource Services or Department of Human Resources investigation – An event that may or may not include an SFPUC employee, consultant, contractor, vendor, or other person acting at the direction of the SFPUC who is under investigation by human resources personnel associated with the City and County of San Francisco

5.3. Archive Footage and Distribution

Requests to obtain copies of footage on disk, flash drive, email file, or by other means or media shall only be granted with approval of the EPS Director and shall be the direct result of one of the circumstances outlined in Section 5.2.

Recorded and archived footage shall not be cut, edited or otherwise altered for any reason. Any provided footage must include the uncut, unedited footage in its complete form.

Footage will be distributed by EPS to the applicable party. The means by which the footage will be distributed will depend on file size. Distributed footage is proprietary information and shall not be duplicated, saved, further distributed, or otherwise used for anything other than the intended purpose.

EPS shall maintain a formal record of exported and distributed footage that conforms to the SFPUC Records Retention Policy.

6. ADDITIONAL REFERENCES

None.

7. HISTORY OF REVISIONS

Effective Date	Revision	Author	Description of Changes
05/04/2018	New	Mary Ellen Carroll	New Policy for SFPUC video surveillance, playback, export and distribution.
2/8/2021	Revision	Jeffrey Harp	Reflects updates in accordance with "Surveillance Technology Ordinance."

Joshua Gale, Emergency Planning Director (jgale@sfwater.org)
Jeffrey Harp, Director of Security (jharp@sfwater.org)

8. APPROVAL SIGNATURES

Approved by: _____ Date: _____
Michael Carlin
Acting General Manager

Approved by: _____ Date: _____
Jeffrey Harp
Director of Security

Surveillance Impact Report

Bibliotheca RFID circulation and security gate system
San Francisco Public Library

As required by San Francisco Administrative Code, Section 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 the Bibliotheca RFID circulation and security gate system.

DESCRIPTION OF THE TECHNOLOGY

The San Francisco Public Library system is dedicated to free and equal access to information, knowledge, independent learning and the joys of reading for our diverse community.

In line with its mission, the Department uses the Bibliotheca RFID circulation and security gate system to improves the customer service experience at the library.

It is the Library's opinion that the use of passive low frequency RFID technology as an inventory control mechanism does not constitute the implementation of Surveillance Technology. No patron information is collected, retained, processed or shared through the use of RFID in the process of circulating and securing materials. Patron's library cards will continue to use eye readable barcode labels which will only be readable by barcode scanners. The Library is including this technology in its response because RFID is specifically cited as a possible surveillance technology in the relevant ordinance.

The use of passive low frequency RFID tags on the library's collection in conjunction with Bibliotheca staff workstations and self-service equipment improves the customer service experience at the library. Self-check machines are significantly quicker and easier to use than those based on tattle-tape technology. Staff RFID workstations speed up the circulation tasks significantly, freeing up staff time to better serve the public. Both patrons and staff will be able to check in or out approximately 8 items at a time (piles up to 12 inches high), since RFID eliminates the existing need to scan and desensitize each item. The overall improved inventory control ensures patrons find the items they are looking for and reduces the time that books are unavailable to the patrons by streamlining circulation cycle from check-in to on-shelf.

RFID security gate technology will improve security, while improving service through improved communication. If the alarms sounds, staff will be able to quickly identify which item was not checked out or if it is a false alarm, eliminating the need to go through bags and check every item the patron may have against the printed check-out slip or pull up their record in the Sierra ILS database.

The Department shall use the Bibliotheca RFID circulation and security gate system only for the following authorized purposes:

- Passive RFID tags applied to library material – For use in inventory management and circulation functions.
- Staff workstation RFID pads – For use by staff to check in and out material and trigger holds.

Surveillance Oversight Review Dates

COIT Review: February 20, 2020
Board of Supervisors Review: TBD

- Self-check machines – For use by patrons to check out material.
- Inventory wand – For use by staff to confirm the current inventory on the library's shelves.
- Sorting machine – For use in checking in material and sorting the items into carts and bins for delivery to other floors and branches.

The following use cases are expressly prohibited:

The Library will not use RFID tags on patron library cards. To ensure patron privacy, the library will continue to use eye readable barcodes on library cards. The Library's revised Privacy Policy specifically references the library's use of passive low frequency RFID technology and excludes the use of RFID tags on patron cards.

Department technology is located at all 28 public library locations and 4 bookmobiles which travel to all neighborhoods in the City visiting senior centers, early education schools and playgrounds will have the technology deployed. RFID will also be used for inventory purposes at 190 9th Street and 950 Brannan Street.

Technology Details

A. The following a is product description of the Bibliotheca RFID circulation and security gate system.

Staff Workstation RFID Pad Specification: Reader connects to PC via USB; it is supplied with a localized plug-in supply (110V ac/60Hz or 240V ac/50Hz). The RF power output is 1.2 Watt and the workstation™ shielded conforms to CE and FCC. Our staffConnect™ circ software will need to be installed on your existing PC, running MicrosoftTM Windows (XP SP3 or W7 32/64). Connection to the LMS/ILS is only required for some of the functionalities.

Self-Check Specification: Operating frequency: 13,56MHz, Max. Transmitting power: 1.2W Supported tag types: ISO 15693, ISO 18000-3-A (NXP SLI, SLIx, SLIx2) RFID Item capacity: Approximately 5 items at any one time. Software: selfCheck™ components uses our quickConnect™ self-service software, which provides the customer with the full range of borrow, return and account functions. The software is configured for connection to the library ILS/LMS through SIP2. Access to the library's network via Ethernet is required.

Inventory Wand: Scan rate: Up to 20 items per second. Operating frequency: 13.56 MHz. RF Transmitting power: Standard Mode 1.5 W / Boost Mode 4.0 W. The mobile inventory device comes with our staffConnect™ inventory software which provides the user with the full range of search, inventory and shelf order functionality. The software does not require a connection to the LMS/ILS, but it can be configured to communicate directly via SIP2/NCIP. Access is required via a Wi-Fi access point. The software can be used on tablets and mobile devices that are able to run Java version 6.

Sorting Machine: SPECIFICATIONS LYNGSOE LIBRARY MATE™ 1200 SELF-RETURN KIOSK

Dimensions Large front: 708 mm H x 506 mm W / 28" H x 20" W Tunnel2000: 800 mm L; Max. angle: 7 degrees

Power 100-240 V AC 50-60 Hz

Network connection Wired Ethernet

Capacity Up to 1,100 materials/hour

Touch screen 19″ color touch screen

Standard colors Front plate: Green (RAL 6025/Brilliance 70); Shelf: Storm (RAL 7015)

Suitable for receiving Library materials (books, magazines, CD/DVDs etc.)

Item restrictions Item size: Min: 100 mm L x 100 mm W x 2 mm H / 4″ L x 4″ W x .1″ H Max: 400 mm L x 300 mm W x 100 mm H / 15.8″ L x 11.8″ W x 4″ H Item weight: Min: 30 g / 1 oz Max: 5 kg / 11 lbs

For use with LMS/ILS using SIP standard interface protocols Sorters: Sort Mate 1000 and 2000 sorter series Software: Library Mate software communicating with the ILS/LMS Software: IMMS for control of floating collections and reservations RFID: Danish Data Model

LYNGSOE SORT MATE™ 2000 MODULESPECIFICATIONS

Dimensions Module: 600 mm L x 420 mm W x 860/950 mm H / 23.6″ L x 16.5″ W x 34/37.5″ H Chute: Depending on choice of chute

Weight 44 kg / 88 lbs

Power 100-240 V AC 50-60 Hz

Network connection Wired Ethernet to master module containing the PLC

Capacity Up to 2,400 materials per hour

Materials Steel chassis

Chute Standard chute for trolley

Standard colors Chassis: Black (RAL 9005) Corner and end plates: Green (RAL 6025) Standard chute covers: Green (RAL 6025)

Suitable for receiving Library materials (books, magazines, CD/DVDs etc.) Material restrictions Material size: Min: 100mm L x 100mm W x 2mm H / 4″ L x 4″ W x .1″ H Max: 400mm L x 300mm W x 100mm H / 15.8″ L x 11.8″ W x 4″ H Item weight: Min: 30 g/1 oz Max: 5 kg/11 lbs

For use with Hardware: Library Mate™ inductions Hardware: Lyngsoe Ergo Staff™ inductions Hardware: Lyngsoe Turn Mate™ Hardware: Lyngsoe Ergo Chutes™ Hardware: Standard chutes Software: Lyngsoe PLC software 1.0 and newer Software: Library Mate™ software communicating with the ILS/LMS Software: IMMS for control of floating collections and reservations RFID: Danish data model Bar code: Dependent on Library Mate™ and Ergo Staff™ induction configuration

B. How It Works

Passive RFID tags applied to library material: RFID tags have adhesive on the back and are applied primarily to the inside back cover of a library book or directly on to DVDs or CDs. The tag is used to store the 14-digit barcode number that is assigned to the item for use of inventory tracking within our Sierra ILS database. There is also a security component stored on the RFID tag, which tells an RFID reader whether the item is checked out or not. The tags are passive and only transmit data when a Bibliotheca reader comes into range.

Staff workstation RFID pads: The pads can simultaneously read multiple RFID tags in piles of material that are placed on top of the pad. The number of items may vary, since the read range is 12 inches

from the pad. USB RFID pads have a smaller read range of only 6 inches, so they are mainly used for single-item transactions.

Self-check machines: The touch-screen devices allow patrons to check out their own library material. They allow multiple items to be stacked on the reader for instant and simultaneous check-out. The number of items may vary, since the read range is 12 inches from the pad.

Inventory wand: These portable wands include a RFID reader and allow staff to upload a shelf list of items that should currently be on the shelf. Items on a shelf can be inventoried by moving the handheld wand along the spine of each item. The read range is 8 inches from the front of the wand.

Sorting machine: RFID scanners track the item as it moves along the conveyer belt to be sorted. The read range is limited within the equipment to ensure the sorting process is not interrupted. The equipment also communicates using SIP2 communication to the Sierra ILS system, so that the library material is checked in.

Data collected or processed by the Bibliotheca RFID circulation and security gate system will not be handled or stored by an outside provider or third-party vendor on an ongoing basis. The Department will remain the sole Custodian of Record.

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 Bibliotheca RFID circulation and security gate system has the following benefits for the residents of the City and County of San Francisco:

- Time savings and improved customer interaction

Additional benefits include:

- Improved Customer Service at security gates. Security gates that use tattle-tape technology can only notify staff that an item may not be checked out. This requires staff to ask patrons to go through their items and check item by item to see if any material is not checked out. RFID gates do not read RFID tags from other libraries, book stores or other sources, so false hits will be eliminated. If an SFPL item is not checked out, the specific title will be listed in the StaffConnect software, allowing staff to provide that title to the patron and ask them to check the item out.

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:

The Library is following the 2012 RFID privacy guidelines recommended by the American Library Association and the National Information Standards Organization (NISO). These standards were developed to safeguard patron privacy. For library material, the Library uses low frequency 13.56 MHz passive tags that are compliant with ISO 18000-3 mode 1 and ISO15693 air interface protocols and the SLi-1 and SLi-2 chips are capable of storing data in the industry standard ISO 28560 format. The RFID readers on staff desks and self-check machines only detect the tags within 6 to 12 inches. The RFID Security gates have a read range of up to 30 inches. By limiting the read range, the library is limiting the chances that a tag will accidently be read by staff equipment. The use of shielded RFID work pads at circulation desks ensures that the equipment only reads 12 inches directly above the pad and not to the sides, ensuring better control at our busy service desks. Even if a non-staff person was able to obtain a Bibliotheca reader, they would need to stand in very close proximity to a patron to read the tag. If they did succeed in reading the tag, the only information they would retrieve is the 14-digit barcode number of the item. Without access to the Sierra database, this barcode cannot be used to pull up bibliographic information about the item. Since the library cards will use barcode labels for patron library card numbers (not RFID tags), it will not be possible to use a RFID reader to gather patron barcodes.

By following the 2012 RFID privacy guidelines recommended by the American Library Association and NISO, the library is able to safeguard patrons' civil rights and liberties by minimizing risk through the implementation of appropriate safeguards. Even after the RFID reader's read range limitations, personal information cannot be obtained through a RFID reader. RFID readers read only RFID tags. Notably, SFPL's RFID tags contain 14-digit barcode numbers that are linked just to SFPL items (i.e. books, magazines, DVDs, etc.). If an RFID tag is read, only library item data will appear; no personal patron information will be viewable. Notably, Patron library cards do not contain RFID tags, but rather utilize separate barcode labels. Access of patron information by RFID reader is therefore impossible.

As no personal information is transmitted or collected by RFID readers and only SFPL item data is viewable (i.e. item title, author, etc.), patrons remain completely anonymous when engaging with RFID readers. The risks of dignity loss, discrimination, loss of liberty, or loss of autonomy that might ensue if RFID readers were able to identify personal patron information if within RFID reading range are therefore negligible to nonexistent.

As patron data remains secure and untouched by RFID readers, other risks such as economic loss from financial information breach, physical harm from location tracking, or loss of trust resulting from tracked personal trends or appropriated personal data are also negligible to nonexistent.

C. Fiscal Analysis of Costs and Benefits

The Department's use of the Bibliotheca RFID circulation and security gate system yields the following business and operations benefits:

- Time savings during the check in and check out process of handling the library material. See attached Radio Frequency Identification (RFID) Costs/Return on Investment report. During staff tests, it was found that an average savings of 5.16 seconds will be saved for each item checked

in (CKI) and 7.83 seconds will be saved for each item checked out (CKO). While some staff time will be saved as we tag each branch's collection, the complete conversion will not be finished until the end of FY20. For the report we opted to only track a full year of savings, estimating approximately $626,185.40 in organizational time savings in FY21.

- Improved Collection Inventory - Improved accuracy during circulation transactions and the ability to perform collection inventories will greatly reduce the number of missing items that are repurchased. SFPL replaces missing items on a regular basis, and the average cost of replacing such material is $25.00 per item.

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

Number of FTE	550 (est.) Note: number of staff versus FTE are not the same.
Classification	36xx, 99xx, 18xx
Total Salary & Fringe – (one time cost of tagging the collection initially)	$577,476
Software (one-time cost)	$64,633
Hardware (one-time cost)	$1,887,182
Professional Services (ongoing costs)	First year of maintenance is covered in the cost of the equipment purchase. It is too early to predict the cost of future equipment maintenance, but there will be an annual charge.
Other (Tags, one-time cost)	$848,465
Other (Tags, ongoing costs)	$20,000
Total Cost	One-time cost: $3,377,756 Ongoing cost: $20,000 plus cost of technical support contract. First year coverage for equipment is free.

The Department funds its use and maintenance of the surveillance technology through

Capital project budget funded by the Library Preservation Fund, City Charter Section 16.109.

COMPARISON TO OTHER JURISDICTIONS

RFIDs are currently utilized by other governmental entities for similar purposes.

APPENDIX A: Surveillance Impact Report Requirements

The following section shows all Surveillance Impact Report requirements in order as defined by the San Francisco Administrative Code, Section 19B.

1. Information describing the Surveillance Technology and how it works, including product descriptions from manufacturers.
Passive RFID tags applied to library material: RFID tags have adhesive on the back and are applied primarily to the inside back cover of a library book or directly on to DVDs or CDs. The tag is used to store the 14-digit barcode number that is assigned to the item for use of inventory tracking within our Sierra ILS database. There is also a security component stored on the RFID tag, which tells an RFID reader whether the item is checked out or not. The tags are passive and only transmit data when a Bibliotheca reader comes into range. Staff workstation RFID pads: The pads can simultaneously read multiple RFID tags in piles of material that are placed on top of the pad. The number of items may vary, since the read range is 12 inches from the pad. USB RFID pads have a smaller read range of only 6 inches, so they are mainly used for single-item transactions. Self-check machines: The touch-screen devices allow patrons to check out their own library material. They allow multiple items to be stacked on the reader for instant and simultaneous check-out. The number of items may vary, since the read range is 12 inches from the pad. Inventory wand: These portable wands include a RFID reader and allow staff to upload a shelf list of items that should currently be on the shelf. Items on a shelf can be inventoried by moving the handheld wand along the spine of each item. The read range is 8 inches from the front of the wand. Sorting machine: RFID scanners track the item as it moves along the conveyer belt to be sorted. The read range is limited within the equipment to ensure the sorting process is not interrupted. The equipment also communicates using SIP2 communication to the Sierra ILS system, so that the library material is checked in. Passive RFID Tags: Staff Workstation RFID Pad Specification: Reader connects to PC via USB; it is supplied with a localized plug-in supply (110V ac/60Hz or 240V ac/50Hz). The RF power output is 1.2 Watt and the workstation™ shielded conforms to CE and FCC. Our staffConnect™ circ software will need to be installed on your existing PC, running MicrosoftTM Windows (XP SP3 or W7 32/64). Connection to the LMS/ILS is only required for some of the functionalities. Self-Check Specification: Operating frequency: 13,56MHz, Max. Transmitting power: 1.2W Supported tag types: ISO 15693, ISO 18000-3-A (NXP SLI, SLIx, SLIx2) RFID Item capacity: Approximately 5 items at any one time. Software: selfCheck™ components uses our quickConnect™ self-service software, which provides the customer with the full range of borrow, return and account functions. The software is configured for connection to the library ILS/LMS through SIP2. Access to the library's network via Ethernet is required.

Inventory Wand: Scan rate: Up to 20 items per second. Operating frequency: 13.56 MHz. RF Transmitting power: Standard Mode 1.5 W / Boost Mode 4.0 W. The mobile inventory device comes with our staffConnect™ inventory software which provides the user with the full range of search, inventory and shelf order functionality. The software does not require a connection to the LMS/ILS, but it can be configured to communicate directly via SIP2/NCIP. Access is required via a Wi-Fi access point. The software can be used on tablets and mobile devices that are able to run Java version 6.

Sorting Machine: SPECIFICATIONS LYNGSOE LIBRARY MATE™ 1200 SELF-RETURN KIOSK

Dimensions Large front: 708 mm H x 506 mm W / 28″ H x 20″ W Tunnel2000: 800 mm L; Max. angle: 7 degrees

Power 100-240 V AC 50-60 Hz

Network connection Wired Ethernet

Capacity Up to 1,100 materials/hour

Touch screen 19″ color touch screen

Standard colors Front plate: Green (RAL 6025/Brilliance 70); Shelf: Storm (RAL 7015)

Suitable for receiving Library materials (books, magazines, CD/DVDs etc.)

Item restrictions Item size: Min: 100 mm L x 100 mm W x 2 mm H / 4″ L x 4″ W x .1″ H Max: 400 mm L x 300 mm W x 100 mm H / 15.8″ L x 11.8″ W x 4″ H Item weight: Min: 30 g / 1 oz Max: 5 kg / 11 lbs

For use with LMS/ILS using SIP standard interface protocols Sorters: Sort Mate 1000 and 2000 sorter series Software: Library Mate software communicating with the ILS/LMS Software: IMMS for control of floating collections and reservations RFID: Danish Data Model

LYNGSOE SORT MATE™ 2000 MODULESPECIFICATIONS

Dimensions Module: 600 mm L x 420 mm W x 860/950 mm H / 23.6″ L x 16.5″ W x 34/37.5″ H Chute: Depending on choice of chute

Weight 44 kg / 88 lbs

Power 100-240 V AC 50-60 Hz

Network connection Wired Ethernet to master module containing the PLC

Capacity Up to 2,400 materials per hour

Materials Steel chassis

Chute Standard chute for trolley

Standard colors Chassis: Black (RAL 9005) Corner and end plates: Green (RAL 6025) Standard chute covers: Green (RAL 6025)

Suitable for receiving Library materials (books, magazines, CD/DVDs etc.) Material restrictions Material size: Min: 100mm L x 100mm W x 2mm H / 4″ L x 4″ W x .1″ H Max: 400mm L x 300mm W x 100mm H / 15.8″ L x 11.8″ W x 4″ H Item weight: Min: 30 g/1 oz Max: 5 kg/11 lbs

For use with Hardware: Library Mate™ inductions Hardware: Lyngsoe Ergo Staff™ inductions Hardware: Lyngsoe Turn Mate™ Hardware: Lyngsoe Ergo Chutes™ Hardware: Standard chutes Software: Lyngsoe PLC software 1.0 and newer Software: Library Mate™ software communicating with the ILS/LMS Software: IMMS for control of floating collections and reservations RFID: Danish data model Bar code: Dependent on Library Mate™ and Ergo Staff™ induction configuration

2. Information on the proposed purpose(s) for the Surveillance Technology.

It is the Library's opinion that the use of passive low frequency RFID technology as an inventory control mechanism does not constitute the implementation of Surveillance Technology. No patron information is collected, retained, processed or shared through the use of RFID in the process of circulating and securing materials. Patron's library cards will continue to use eye readable barcode labels which will only be readable by barcode scanners. The Library is including this technology in its response because RFID is specifically cited as a possible surveillance technology in the relevant ordinance.

The use of passive low frequency RFID tags on the library's collection in conjunction with Bibliotheca staff workstations and self-service equipment improves the customer service experience at the library. Self-check machines are significantly quicker and easier to use than those based on tattle-tape technology. Staff RFID workstations speed up the circulation tasks significantly, freeing up staff time to better serve the public. Both patrons and staff will be able to check in or out approximately 8 items at a time (piles up to 12 inches high), since RFID eliminates the existing need to scan and desensitize each item. The overall improved inventory control ensures patrons find the items they are looking for and reduces the time that books are unavailable to the patrons by streamlining circulation cycle from check-in to on-shelf.

RFID security gate technology will improve security, while improving service through improved communication. If the alarms sounds, staff will be able to quickly identify which item was not checked out or if it is a false alarm, eliminating the need to go through bags and check every item the patron may have against the printed check-out slip or pull up their record in the Sierra ILS database.

Use Case #1: Passive RFID tags applied to library material – For use in inventory management and circulation functions

Use Case #2: Staff workstation RFID pads – For use by staff to check in and out material and trigger holds.

Use Case #3: Self-check machines – For use by patrons to check out material.

Use Case #4: Inventory wand – For use by staff to confirm the current inventory on the library's shelves.

Use Case #5: Sorting machine – For use in checking in material and sorting the items into carts and bins for delivery to other floors and branches.

The Department's use of the Bibliotheca RFID circulation and security gate system has the following benefits for the residents of the City and County of San Francisco:

- Time savings and improved customer interaction

Additional benefits include:

- Improved Customer Service at security gates. Security gates that use tattle-tape technology can only notify staff that an item may not be checked out. This requires staff to ask patrons to go through their items and check item by item to see if any material is not checked out. RFID gates do not read RFID tags from other libraries, book stores or other sources, so false hits will be eliminated. If an SFPL item is not checked out, the specific title will be listed in the StaffConnect software, allowing staff to provide that title to the patron and ask them to check the item out.

The Department's use of the Bibliotheca RFID circulation and security gate system yields the following business and operations benefits:

- Time savings during the check in and check out process of handling the library material. See attached Radio Frequency Identification (RFID) Costs/Return on Investment report. During staff tests, it was found that an average savings of 5.16 seconds will be saved for each item checked in (CKI) and 7.83 seconds will be saved for each item checked out (CKO). While some staff time will be saved as we tag each branch's collection, the complete conversion will not be finished until the end of FY20. For the report we opted to only track a full year of savings, estimating approximately $626,185.40 in organizational time savings in FY21.
- Improved Collection Inventory - Improved accuracy during circulation transactions and the ability to perform collection inventories will greatly reduce the number of missing items that are repurchased. SFPL replaces missing items on a regular basis, and the average cost of replacing such material is $25.00 per item.

3. If applicable, the general location(s) it may be deployed and crime statistics for any location(s).

All 28 public library locations and 4 bookmobiles which travel to all neighborhoods in the City visiting senior centers, early education schools and playgrounds will have the technology deployed. RFID will also be used for inventory purposes at 190 9th Street and 950 Brannan Street.

4. An assessment identifying any potential impact on civil liberties and civil rights and discussing any plans to safeguard the rights of the public.

The Library is following the 2012 RFID privacy guidelines recommended by the American Library Association and the National Information Standards Organization (NISO). These standards were developed to safeguard patron privacy. For library material, the Library uses low frequency 13.56 MHz passive tags that are compliant with ISO 18000-3 mode 1 and ISO15693 air interface protocols and the SLi-1 and SLi-2 chips are capable of storing data in the industry standard ISO 28560 format. The RFID readers on staff desks and self-check machines only detect the tags within 6 to 12 inches. The RFID Security gates have a read range of up to 30 inches. By limiting the read range, the library is limiting the chances that a tag will accidently be read by staff

equipment. The use of shielded RFID work pads at circulation desks ensures that the equipment only reads 12 inches directly above the pad and not to the sides, ensuring better control at our busy service desks. Even if a non-staff person was able to obtain a Bibliotheca reader, they would need to stand in very close proximity to a patron to read the tag. If they did succeed in reading the tag, the only information they would retrieve is the 14-digit barcode number of the item. Without access to the Sierra database, this barcode cannot be used to pull up bibliographic information about the item. Since the library cards will use barcode labels for patron library card numbers (not RFID tags), it will not be possible to use a RFID reader to gather patron barcodes.

By following the 2012 RFID privacy guidelines recommended by the American Library Association and NISO, the library is able to safeguard patrons' civil rights and liberties by minimizing risk through the implementation of appropriate safeguards. Even after the RFID reader's read range limitations, personal information cannot be obtained through a RFID reader. RFID readers read only RFID tags. Notably, SFPL's RFID tags contain 14-digit barcode numbers that are linked just to SFPL items (i.e. books, magazines, DVDs, etc.). If an RFID tag is read, only library item data will appear; no personal patron information will be viewable. Notably, Patron library cards do not contain RFID tags, but rather utilize separate barcode labels. Access of patron information by RFID reader is therefore impossible.

As no personal information is transmitted or collected by RFID readers and only SFPL item data is viewable (i.e. item title, author, etc.), patrons remain completely anonymous when engaging with RFID readers. The risks of dignity loss, discrimination, loss of liberty, or loss of autonomy that might ensue if RFID readers were able to identify personal patron information if within RFID reading range are therefore negligible to nonexistent.

As patron data remains secure and untouched by RFID readers, other risks such as economic loss from financial information breach, physical harm from location tracking, or loss of trust resulting from tracked personal trends or appropriated personal data are also negligible to nonexistent.

5. The fiscal costs for the Surveillance Technology, including initial purchase, personnel and other ongoing costs, and any current or potential sources of funding.

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

Number of FTE	550 (est.) Note: number of staff versus FTE are not the same.
Classification	36xx, 99xx, 18xx
Total Salary & Fringe – (one time cost of tagging the collection initially)	$577,476
Software (one-time cost)	$64,633

Hardware (one-time cost)	$1,887,182
Professional Services (ongoing costs)	First year of maintenance is covered in the cost of the equipment purchase. It is too early to predict the cost of future equipment maintenance, but there will be an annual charge.
Other (Tags, one-time cost)	$848,465
Other (Tags, ongoing costs)	$20,000
Total Cost	One-time cost: $3,377,756 Ongoing cost: $20,000 plus cost of technical support contract. First year coverage for equipment is free.

The Department funds its use and maintenance of the surveillance technology through

Capital project budget funded by the Library Preservation Fund, City Charter Section 16.109.

6. Whether use or maintenance of the technology will require data gathered by the technology to be handled or stored by a third-party vendor on an ongoing basis.

Data collected or processed by the Bibliotheca RFID circulation and security gate system will not be handled or stored by an outside provider or third-party vendor on an ongoing basis. The Department will remain the sole Custodian of Record.

7. A summary of the experience, if any, other governmental entities have had with the proposed technology, including information about its effectiveness and any known adverse information about the technology such as anticipated costs, failures, or civil rights and civil liberties abuses.

APPENDIX B: Mapped Crime Statistics

Not applicable to this technology.

Surveillance Technology Policy

Bibliotheca RFID Circulation and Security Gate System
San Francisco Public Library

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 the Bibliotheca RFID circulation and security gate system 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

The San Francisco Public Library system is dedicated to free and equal access to information, knowledge, independent learning and the joys of reading for our diverse community.

The Surveillance Technology Policy ("Policy") defines the manner in which the Bibliotheca RFID circulation and security gate system will be used to support this mission, by describing the intended purpose, authorized and restricted uses, and requirements.

This Policy applies to all to department personnel that use, plan to use, or plan to secure the Bibliotheca RFID circulation and security gate system, 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 Bibliotheca RFID circulation and security gate system technology for the Department is limited to the following use cases and is subject to the requirements listed in this Policy.

Authorized Use(s):

- Passive RFID tags applied to library material – For use in inventory management and circulation functions.
- Staff workstation RFID pads – For use by staff to check in and out material and trigger holds.
- Self-check machines – For use by patrons to check out material.
- Inventory wand – For use by staff to confirm the current inventory on the library's shelves.
- Sorting machine – For use in checking in material and sorting the items into carts and bins for delivery to other floors and branches.

Prohibited use cases include any uses not stated in the Authorized Use Case section.

Surveillance Oversight Review Dates
COIT Review: February 20, 2020
Board of Supervisors Review: TBD

BUSINESS JUSTIFICATION

The Bibliotheca RFID circulation and security gate system supports the Department's mission and provides important operational value in the following ways:

It is the Library's opinion that the use of passive low frequency RFID technology as an inventory control mechanism does not constitute the implementation of Surveillance Technology. No patron information is collected, retained, processed or shared through the use of RFID in the process of circulating and securing materials. Patron's library cards will continue to use eye readable barcode labels which will only be readable by barcode scanners. The Library is including this technology in its response because RFID is specifically cited as a possible surveillance technology in the relevant ordinance.

The use of passive low frequency RFID tags on the library's collection in conjunction with Bibliotheca staff workstations and self-service equipment improves the customer service experience at the library. Self-check machines are significantly quicker and easier to use than those based on tattle-tape technology. Staff RFID workstations speed up the circulation tasks significantly, freeing up staff time to better serve the public. Both patrons and staff will be able to check in or out approximately 8 items at a time (piles up to 12 inches high), since RFID eliminates the existing need to scan and desensitize each item. The overall improved inventory control ensures patrons find the items they are looking for and reduces the time that books are unavailable to the patrons by streamlining circulation cycle from check-in to on-shelf.

RFID security gate technology will improve security, while improving service through improved communication. If the alarms sounds, staff will be able to quickly identify which item was not checked out or if it is a false alarm, eliminating the need to go through bags and check every item the patron may have against the printed check-out slip or pull up their record in the Sierra ILS database.

In addition, the Bibliotheca RFID circulation and security gate system promises to benefit residents in the following ways:

- Time savings and improved customer interaction

The Bibliotheca RFID circulation and security gate system will benefit the department in the following ways:

- Time savings during the check in and check out process of handling the library material. See attached Radio Frequency Identification (RFID) Costs/Return on Investment report. During staff tests, it was found that an average savings of 5.16 seconds will be saved for each item checked in (CKI) and 7.83 seconds will be saved for each item checked out (CKO). While some staff time will be saved as we tag each branch's collection, the complete conversion will not be finished until the end of FY20. For the report we opted to only track a full year of savings, estimating approximately $626,185.40 in organizational time savings in FY21.
- Improved Collection Inventory - Improved accuracy during circulation transactions and the ability to perform collection inventories will greatly reduce the number of missing items that are repurchased. SFPL replaces missing items on a regular basis, and the average cost of replacing such material is $25.00 per item.

Other benefits include Improved Customer Service at security gates. Security gates that use tattle-tape technology can only notify staff that an item may not be checked out. This requires staff to

ask patrons to go through their items and check item by item to see if any material is not checked out. RFID gates do not read RFID tags from other libraries, book stores or other sources, so false hits will be eliminated. If an SFPL item is not checked out, the specific title will be listed in the StaffConnect software, allowing staff to provide that title to the patron and ask them to check the item out.

To achieve its intended purpose, the Bibliotheca RFID circulation and security gate system (hereinafter referred to as "surveillance technology") works in the following ways:

Passive RFID tags applied to library material: RFID tags have adhesive on the back and are applied primarily to the inside back cover of a library book or directly on to DVDs or CDs. The tag is used to store the 14-digit barcode number that is assigned to the item for use of inventory tracking within our Sierra ILS database. There is also a security component stored on the RFID tag, which tells an RFID reader whether the item is checked out or not. The tags are passive and only transmit data when a Bibliotheca reader comes into range.

Staff workstation RFID pads: The pads can simultaneously read multiple RFID tags in piles of material that are placed on top of the pad. The number of items may vary, since the read range is 12 inches from the pad. USB RFID pads have a smaller read range of only 6 inches, so they are mainly used for single-item transactions.

Self-check machines: The touch-screen devices allow patrons to check out their own library material. They allow multiple items to be stacked on the reader for instant and simultaneous check-out. The number of items may vary, since the read range is 12 inches from the pad.

Inventory wand: These portable wands include a RFID reader and allow staff to upload a shelf list of items that should currently be on the shelf. Items on a shelf can be inventoried by moving the handheld wand along the spine of each item. The read range is 8 inches from the front of the wand.

Sorting machine: RFID scanners track the item as it moves along the conveyer belt to be sorted. The read range is limited within the equipment to ensure the sorting process is not interrupted. The equipment also communicates using SIP2 communication to the Sierra ILS system, so that the library material is checked in.

Department staff may use the technology for authorized use cases only, and is expressly prohibited from the following use cases:

The Library will not use RFID tags on patron library cards. To ensure patron privacy, the library will continue to use eye readable barcodes on library cards. The Library's revised Privacy Policy specifically references the library's use of passive low frequency RFID technology and excludes the use of RFID tags on patron cards.

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.

Safety: Surveillance technology must be operated in a safe manner. Surveillance technology should not be operated in a way that infringes on resident civil rights, including privacy, or causes personal injury or property damage.

Data Collection: Departments shall minimize the use, collection, and retention of Personally Identifiable Information (PII) to what is strictly necessary to accomplish the intended purpose of the surveillance technology.

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

Should information be incidentally collected that is not necessary to accomplish the intended purpose of the surveillance technology, including information that may be used to identify persons or private information, Department shall remove all incidental PII from raw data.

The surveillance technology collects the following data types:

Barcode for library material	The 14 digit number is transferred as temporary plain text and not stored.	Level 2

Notification: *No personally identifiable information (PII) is collected or tracked through this technology, so the Library does not post a notice.*

Access: All parties requesting access must adhere to the following rules and processes:

Data are not stored. RFID readers transfer the item barcode number to the Bibliotheca Staffconnect software, which temporarily stores it while it transfers the number to the Sierra ILS database. Once the RFID pad is used again or the software is closed, Bibliotheca Staffconnect software deletes the number. RFID gate logs will retain data for only titles not checked out and only for period designated by the library. Currently the time period is set for 5 minutes. Inventory wands will only use barcodes of material not checked out.

Access requirements vary by party:

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.

- 36xx, 99xx, 18xx

Department shall maintain access logs for surveillance technology and all data collected, processed, and/or stored by the surveillance technology. The name of the person making the log entry should be recorded, along with the date and time.

B. Members of the public, including criminal defendants

Data collected by surveillance technology is not stored and therefore will not be made available to members of the public, including criminal defendants.

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. Anyone, including criminal defendants, may access such data. 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, including by criminal defendants.

Members of the public, including criminal defendants, 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.

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).

To protect surveillance technology information from unauthorized access and control, including misuse, Departments shall, at minimum, apply the following safeguards:

Data used in circulation transaction are not stored.

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)

The Department currently participates in the following sharing practices:

A. Internal Data Sharing

The department does not share surveillance technology data with other departments or entities inside the City and County of San Francisco.

Data are not stored nor shared. Only assigned library staff will be allowed to use the technology. The Library has a Privacy Policy and Privacy Inventory that governs how circulation data will be handled by staff.

B. External Data Sharing

The department does not share surveillance technology data externally with entities outside the City and County of San Francisco.

Data Retention: While the Department does not collect PII through this technology, it adheres to the following data retention period and justification for the data it does collect.

Barcodes are stored in the passive RFID tags on each library item. Data are only stored by RFID readers long enough to pass the barcode number into the Sierra ILS database. Once another tag is read the barcode will be deleted. RFID gate logs will retain data only for titles not checked out and only for period designated by the library. Inventory wands will only use barcodes of material not currently checked out.	Barcodes collected during circulation transaction are not stored to ensure privacy. RFID gates and inventory wands only track items not connected with a patron account, so purging is less frequent. Security gate logs are retained to give staff the time to check the title provided and to interact with patron. RFID gate logs will retain data only for titles not checked out and only for period designated by the library. Currently the time period is set for 5 minutes. Inventory wands will only use barcodes of material not checked out. Barcodes collected during circulation transaction are not stored to ensure privacy. RFID gates and inventory wands only track items not connected with a patron account, so purging is less frequent. Security gate logs are

	retained to give staff the time to check the title provided and to interact with patron. RFID gate logs will retain data only for titles not checked out and only for period designated by the library. Currently the time period is set for 5 minutes. Inventory wands will only use barcodes of material not checked out.

PII data shall not be kept in a form which permits identification of data subjects for any longer than is necessary for the purposes for which the personal data are processed. PII data collected by the surveillance technology may be retained beyond the standard retention period only in the following circumstance(s):

Under no conditions would data be retained past the timeline described above.

Departments must establish appropriate safeguards for PII data stored for longer periods.

Data Disposal: Upon completion of the data retention period, Department shall dispose of data in the following manner:

Data are not stored.

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 must receive training on data security policies and procedures.

At the very least, 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. 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.

Staff need to be trained on how to launch the Bibliotheca Staff connect software, how to toggle between checking in material and checking out material, and how to ensure the cursor is in the Sierra ILS database input box to ensure the barcode number will be transferred.

COMPLIANCE

Department shall oversee and enforce compliance with this Policy using the following methods:

The Library will provide the Policy document and overview on internal intranet and on the public website.

Department shall assign the following personnel to oversee Policy compliance by the Department and third-parties.

Michael Liang, Chief Information Officer, San Francisco Public Library

Sanctions for violations of this Policy include the following:

The Library would work within existing City and departmental human resources guidelines to address and determine appropriate sanctions.

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.

EXCEPTIONS

Only in exigent circumstances or in circumstances where law enforcement requires surveillance technology data for investigatory or prosecutorial functions may data collected, retained or processed by the surveillance technology be shared with law enforcement.

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 a surveillance technology that has not been processed and cleaned of all personal identifiable information. The distribution and use of raw data is tightly restricted.
Exigent Circumstances	An emergency involving imminent danger of death or serious physical injury to any person that requires the immediate use of Surveillance Technology or the information it provides.

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

Public:

Complaints or concerns can be submitted to the Department in person, by phone, in writing that can be turned in by mail or in person, or electronically via the library's chat service, or "Comments and Suggestions" page.

Department shall acknowledge and respond to complaints and concerns in a timely and organized response. To do so, Department shall forward all questions and complaints to the proper internal department entities for timely response.

City and County of San Francisco Employees:

All questions regarding this policy should be directed to the employee's supervisor or to the director. Similarly, questions about other applicable laws governing the use of the surveillance technology or the issues related to privacy should be directed to the employee's supervisor or the director.

APPENDIX A: Surveillance Technology Policy Requirements

The following section shows all Surveillance Technology Policy requirements in order as defined by the San Francisco Administrative Code, Section 19B.

1. A description of the product and services addressed by the Surveillance Technology, including the identity of any provider(s) whose services are essential to the functioning or effectiveness of the Surveillance Technology equipment or services for the intended purpose.
Passive RFID tags applied to library material: RFID tags have adhesive on the back and are applied primarily to the inside back cover of a library book or directly on to DVDs or CDs. The tag is used to store the 14-digit barcode number that is assigned to the item for use of inventory tracking within our Sierra ILS database. There is also a security component stored on the RFID tag, which tells an RFID reader whether the item is checked out or not. The tags are passive and only transmit data when a Bibliotheca reader comes into range. Staff workstation RFID pads: The pads can simultaneously read multiple RFID tags in piles of material that are placed on top of the pad. The number of items may vary, since the read range is 12 inches from the pad. USB RFID pads have a smaller read range of only 6 inches, so they are mainly used for single-item transactions. Self-check machines: The touch-screen devices allow patrons to check out their own library material. They allow multiple items to be stacked on the reader for instant and simultaneous check-out. The number of items may vary, since the read range is 12 inches from the pad. Inventory wand: These portable wands include a RFID reader and allow staff to upload a shelf list of items that should currently be on the shelf. Items on a shelf can be inventoried by moving the handheld wand along the spine of each item. The read range is 8 inches from the front of the wand. Sorting machine: RFID scanners track the item as it moves along the conveyer belt to be sorted. The read range is limited within the equipment to ensure the sorting process is not interrupted. The equipment also communicates using SIP2 communication to the Sierra ILS system, so that the library material is checked in. Passive RFID Tags: Staff Workstation RFID Pad Specification: Reader connects to PC via USB; it is supplied with a localized plug-in supply (110V ac/60Hz or 240V ac/50Hz). The RF power output is 1.2 Watt and the workstation™ shielded conforms to CE and FCC. Our staffConnect™ circ software will need to be installed on your existing PC, running MicrosoftTM Windows (XP SP3 or W7 32/64). Connection to the LMS/ILS is only required for some of the functionalities. Self-Check Specification: Operating frequency: 13,56MHz, Max. Transmitting power: 1.2W Supported tag types: ISO 15693, ISO 18000-3-A (NXP SLI, SLIx, SLIx2) RFID Item capacity: Approximately 5 items at any one time. Software: selfCheck™ components uses our quickConnect™ self-service software, which provides the customer with the full range of borrow, return and account functions. The software is configured for connection to the library ILS/LMS through SIP2. Access to the library's network via Ethernet is required.

Inventory Wand: Scan rate: Up to 20 items per second. Operating frequency: 13.56 MHz. RF Transmitting power: Standard Mode 1.5 W / Boost Mode 4.0 W. The mobile inventory device comes with our staffConnect™ inventory software which provides the user with the full range of search, inventory and shelf order functionality. The software does not require a connection to the LMS/ILS, but it can be configured to communicate directly via SIP2/NCIP. Access is required via a Wi-Fi access point. The software can be used on tablets and mobile devices that are able to run Java version 6.

Sorting Machine: SPECIFICATIONS LYNGSOE LIBRARY MATE™ 1200 SELF-RETURN KIOSK

Dimensions Large front: 708 mm H x 506 mm W / 28″ H x 20″ W Tunnel2000: 800 mm L; Max. angle: 7 degrees

Power 100-240 V AC 50-60 Hz

Network connection Wired Ethernet

Capacity Up to 1,100 materials/hour

Touch screen 19″ color touch screen

Standard colors Front plate: Green (RAL 6025/Brilliance 70); Shelf: Storm (RAL 7015)

Suitable for receiving Library materials (books, magazines, CD/DVDs etc.)

Item restrictions Item size: Min: 100 mm L x 100 mm W x 2 mm H / 4″ L x 4″ W x .1″ H Max: 400 mm L x 300 mm W x 100 mm H / 15.8″ L x 11.8″ W x 4″ H Item weight: Min: 30 g / 1 oz Max: 5 kg / 11 lbs

For use with LMS/ILS using SIP standard interface protocols Sorters: Sort Mate 1000 and 2000 sorter series Software: Library Mate software communicating with the ILS/LMS Software: IMMS for control of floating collections and reservations RFID: Danish Data Model

LYNGSOE SORT MATE™ 2000 MODULESPECIFICATIONS

Dimensions Module: 600 mm L x 420 mm W x 860/950 mm H / 23.6″ L x 16.5″ W x 34/37.5″ H Chute: Depending on choice of chute

Weight 44 kg / 88 lbs

Power 100-240 V AC 50-60 Hz

Network connection Wired Ethernet to master module containing the PLC

Capacity Up to 2,400 materials per hour

Materials Steel chassis

Chute Standard chute for trolley

Standard colors Chassis: Black (RAL 9005) Corner and end plates: Green (RAL 6025) Standard chute covers: Green (RAL 6025)

Suitable for receiving Library materials (books, magazines, CD/DVDs etc.) Material restrictions Material size: Min: 100mm L x 100mm W x 2mm H / 4″ L x 4″ W x .1″ H Max: 400mm L x 300mm W x 100mm H / 15.8″ L x 11.8″ W x 4″ H Item weight: Min: 30 g/1 oz Max: 5 kg/11 lbs

For use with Hardware: Library Mate™ inductions Hardware: Lyngsoe Ergo Staff™ inductions Hardware: Lyngsoe Turn Mate™ Hardware: Lyngsoe Ergo Chutes™ Hardware: Standard chutes Software: Lyngsoe PLC software 1.0 and newer Software: Library Mate™ software communicating with the ILS/LMS Software: IMMS for control of floating collections and reservations RFID: Danish data model Bar code: Dependent on Library Mate™ and Ergo Staff™ induction configuration

Data collected or processed by the Bibliotheca RFID circulation and security gate system will not be handled or stored by an outside provider or third-party vendor on an ongoing basis. The Department will remain the sole Custodian of Record.

2. A description of the purpose(s) for which the Surveillance Technology equipment or services are proposed for acquisition, including the type of data that may be collected by the Surveillance Technology equipment or services.

It is the Library's opinion that the use of passive low frequency RFID technology as an inventory control mechanism does not constitute the implementation of Surveillance Technology. No patron information is collected, retained, processed or shared through the use of RFID in the process of circulating and securing materials. Patron's library cards will continue to use eye readable barcode labels which will only be readable by barcode scanners. The Library is including this technology in its response because RFID is specifically cited as a possible surveillance technology in the relevant ordinance.

The use of passive low frequency RFID tags on the library's collection in conjunction with Bibliotheca staff workstations and self-service equipment improves the customer service experience at the library. Self-check machines are significantly quicker and easier to use than those based on tattle-tape technology. Staff RFID workstations speed up the circulation tasks significantly, freeing up staff time to better serve the public. Both patrons and staff will be able to check in or out approximately 8 items at a time (piles up to 12 inches high), since RFID eliminates the existing need to scan and desensitize each item. The overall improved inventory control ensures patrons find the items they are looking for and reduces the time that books are unavailable to the patrons by streamlining circulation cycle from check-in to on-shelf.

RFID security gate technology will improve security, while improving service through improved communication. If the alarms sounds, staff will be able to quickly identify which item was not checked out or if it is a false alarm, eliminating the need to go through bags and check every item the patron may have against the printed check-out slip or pull up their record in the Sierra ILS database.

The surveillance technology collects the following data types:

Barcode for library material	The 14 digit number is transferred as temporary plain text and not stored.	Level 2

3. The uses that are authorized, the rules and processes required prior to such use, and uses of the Surveillance Technology that will be expressly prohibited.

[Toolkit 1.3, 1.5, & 3.16]

Use Case #1: Passive RFID tags applied to library material – For use in inventory management and circulation functions

Use Case #2: Staff workstation RFID pads – For use by staff to check in and out material and trigger holds.

Use Case #3: Self-check machines – For use by patrons to check out material.

Use Case #4: Inventory wand – For use by staff to confirm the current inventory on the library's shelves.

Use Case #5: Sorting machine – For use in checking in material and sorting the items into carts and bins for delivery to other floors and branches.

The Library will not use RFID tags on patron library cards. To ensure patron privacy, the library will continue to use eye readable barcodes on library cards. The Library's revised *Privacy Policy* specifically references the library's use of passive low frequency RFID technology and excludes the use of RFID tags on patron cards.

Data are not stored. RFID readers transfer the item barcode number to the Bibliotheca Staffconnect software, which temporarily stores it while it transfers the number to the Sierra ILS database. Once the tag is removed from the pad, Bibliotheca Staffconnect software deletes the number.

4. A description of the formats in which information collected by the Surveillance Technology is stored, copied, and/or accessed.

The surveillance technology collects the following data types:

Barcode for library material	The 14 digit number is transferred as temporary plain text and not stored.	Level 2

5. The specific categories and titles of individuals who are authorized by the Department to access or use the collected information, including restrictions on how and under what circumstances data collected with Surveillance Technology can be analyzed and reviewed, and the rules and processes required prior to access or use of the information.

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

- 36xx, 99xx, 18xx

Department shall maintain access logs for surveillance technology and all data collected, processed, and/or stored by the surveillance technology. The name of the person making the log entry should be recorded, along with the date and time. Data are not stored. RFID readers transfer the item barcode number to the Bibliotheca Staffconnect software, which temporarily stores it while it transfers the number to the Sierra ILS database. Once the RFID pad is used again or the software is closed, Bibliotheca Staffconnect software deletes the number. RFID gate logs will retain data for only titles not checked out and only for period designated by the library. Currently the time period is set for 5 minutes. Inventory wands will only use barcodes of material not checked out.
6. The general safeguards that protect information from unauthorized access, including encryption and access control mechanisms.
Data used in circulation transaction are not stored.
7. The limited time period, if any, that information collected by the Surveillance Technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s) enumerated in the Surveillance Technology Policy, the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond that period
Barcodes are stored in the passive RFID tags on each library item. Data are only stored by RFID readers long enough to pass the barcode number into the Sierra ILS database. Once another tag is read the barcode will be deleted. RFID gate logs will retain data only for titles not checked out and only for period designated by the library. Inventory wands will only use barcodes of material not currently checked out. Barcodes collected during circulation transaction are not stored to ensure privacy. RFID gates and inventory wands only track items not connected with a patron account, so purging is less frequent. Security gate logs are retained to give staff the time to check the title provided and to interact with patron. RFID gate logs will retain data only for titles not checked out and only for period designated by the library. Currently the time period is set for 5 minutes. Inventory wands will only use barcodes of material not checked out.
8. How collected information can be accessed or used by members of the public, including criminal defendants
Data are not stored.
9. Which governmental agencies, departments, bureaus, divisions, or units that may receive data collected by the Surveillance Technology operated by the Department, including any required justification or legal standard necessary to share that data and how it will ensure that any entity receiving such data complies with the Surveillance Technology Policy.

Data are not stored nor shared. Only assigned library staff will be allowed to use the technology. The Library has a Privacy Policy and Privacy Inventory that governs how circulation data will be handled by staff.

10. The training required for any individual authorized to use the Surveillance Technology or to access information collected by the Surveillance Technology

Every staff member likely to use the technology will be trained on using this technology. Staff need to be trained on how to launch the Bibliotheca Staff connect software, how to toggle between checking in material and checking out material, and how to ensure the cursor is in the Sierra ILS database input box to ensure the barcode number will be transferred.

11. The mechanisms to ensure that the Surveillance Technology Policy is followed, including internal personnel assigned to ensure compliance with the policy, internal recordkeeping of the use of the technology or access to information collected by the technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the sanctions for violations of the policy

Department shall oversee and enforce compliance with this Policy using the following methods:

The Library will provide the Policy document and overview on internal intranet and on the public website.

Department shall assign the following personnel to oversee Policy compliance by the Department and third-parties.

Michael Liang, Chief Information Officer, San Francisco Public Library

Sanctions for violations of this Policy include the following:

The Library would work within existing City and departmental human resources guidelines to address and determine appropriate sanctions.

12. What procedures will be put in place by which members of the public can register complaints or concerns, or submit questions about the deployment or use of a specific Surveillance Technology, and how the Department will ensure each question and complaint is responded to in a timely manner.

Complaints or concerns can be submitted to the Department in person, by phone, in writing that can be turned in by mail or in person, or electronically via the library's chat service, or "Comments and Suggestions" page.

Department shall acknowledge and respond to complaints and concerns in a timely and organized response. To do so, Department shall forward all questions and complaints to the proper internal department entities for timely response.

Committee on Information Technology

Office of the City Administrator

To: Members of the Board of Supervisors

From: Carmen Chu, City Administrator
Matthias Jaime, Director, Committee of Information Technology
Taraneh Moayed, Assistant Director, Office of Contract Administration, Chair of Privacy and Surveillance Advisory Board

Date: March 30, 2021

Subject: Legislation introduced for Acquisition of Surveillance Technology Approvals: Audio Recorder, Automatic License Plate Readers, Drones, Security Cameras, Radio Frequency Identification.

In compliance with Section 19B of the City and County of San Francisco's Administrative Code, the City Administrator's Office is pleased to submit the following Surveillance Technology Policies and Impact Reports for review by the Board of Supervisors.

- Audio Recorder (ShotSpotter)
- Automatic License Plate Readers (ALPR)
- Drones (a.k.a. Unmanned Aircraft Systems)
- Security Cameras
- Radio Frequency Identification (RFID)

In an effort to maintain the spirit of the legislation to engage the public discussion on the role of government surveillance, the Committee on Information Technology (COIT) and its subcommittee the Privacy and Surveillance Advisory Board (PSAB) held public meetings over the course of the last two years to review and approve the policies. All details of these discussions are available at sf.gov/coit.

The following sections provides more specific detail on the departments seeking Board of Supervisors approval for their Surveillance Technology Policy, and the COIT recommended course of action.

If you have questions on the review process, please direct all questions to Matthias Jaime, Director of the Committee on Information Technology (COIT).

Audio Recorder (ShotSpotter)

Department	Authorized Uses
Police Department	1. Gunshot detection: Record gunshot sounds and use sensors to locate the origin of the gunshots. Patrol Officers receive gunshot alerts to respond to crime scene. 2. Investigators use ShotSpotter Investigative Portal reports to find shell casing evidence on scene and to further analyze the incident.

ShotSpotter Public Meeting Dates:

Date	Meeting
August 28, 2020	Privacy and Surveillance Advisory Board (PSAB)
October 9, 2020	Privacy and Surveillance Advisory Board (PSAB)
October 23, 2020	Privacy and Surveillance Advisory Board (PSAB)
November 13, 2020	Privacy and Surveillance Advisory Board (PSAB)
January 21, 2021	Committee on Information Technology (COIT)

COIT recommends the following action be taken on the policies:

- Approve the ShotSpotter Surveillance Technology Policy for the Police Department for review by the Mayor, City Attorney, and Board of Supervisors.

Automatic License Plate Readers (ALPR)

Department	Authorized Uses
Airport	1. To track the activity of permitted commercial ground transportation at the Airport. Also used as a secondary method for collecting trip fees in the event an operator's transponder fails to read. 2. To support the Airport and local, state, federal, and regional public safety departments in the identification of vehicles associated with targets of investigations, including locating stolen, wanted, and or other vehicles that are the subject of investigation; and/or locating victims, witnesses, suspects, and others associated with a law enforcement investigation.
Police Department	1. Locate stolen, wanted, and or other vehicles that are the subject of investigation 2. To apprehend wanted persons subject to arrest warrants or who are otherwise lawfully sought by law enforcement. 3. To locate victims, witnesses, suspects, missing children, adults, and/or elderly individuals, including in response to Amber Alerts and Silver Alerts and others associated with a law enforcement investigation. 4. To assist with criminal investigations initiated by local, state and regional public safety departments by identifying vehicles associated with targets of criminal investigations. 5. Counter-terrorism: Identify potential threats to critical infrastructure sites. 6. For other law enforcement purposes as authorized by law: Investigations of major crimes.
Public Works	1. Discourage illegal dumping onto City Streets.
Recreation & Parks	1. To support local, state, federal, and regional public safety departments in the identification of vehicles associated with targets of criminal investigations, including investigations of serial crimes 2. To protect the public and our staff at special events from misconduct and/or violent confrontations. 3. To protect critical infrastructure sites from vandalism, theft and damage.

ALPR Public Meeting Dates:

Date	**Meeting**	**Departments**
July 24, 2020	PSAB	Public Works
August 14, 2020	PSAB	Police
August 28, 2020	PSAB	Recreation & Parks
September 11, 2020	PSAB	Police, Public Works
September 17, 2020	COIT	Police, Public Works
September 25, 2020	PSAB	Airport, Recreation & Parks
November 13, 2020	PSAB	Airport
January 21, 2021, 2020	COIT	Police
February 4, 2021, 2020	COIT	Airport, Recreation & Parks

COIT recommends the following action be taken on the policies:

Airport, Public Works, Recreation & Parks

- Approve the ALPR Surveillance Technology Policies for the Airport, Public Works, and Department of Recreation and Parks.

Police

- Approve the ALPR Surveillance Technology Policy for the Police Department with the additional recommendation to conduct a quantitative impact analysis on the use of ALPR for review by the Board of Supervisors.

Drones (Unmanned Aircraft Systems)

Department	Authorized Uses
Fire	1. Disaster Response: Assessment and District Surveys 2. Emergency Response: Building Fire Reconnaissance 3. Search & Rescue: Aerial or water borne drones. 4. Training: Assessment and evaluation of emergency response
Port	1. Disaster response and recovery: Provide DOC with high resolution images during response and recovery operations after a disaster. 2. Facility Inspections: Provide high resolution images during engineering and environmental surveys and assessments of Port properties. 3. Marketing: Capture Drone footage to be used in marketing materials for the promotion of activities and opportunities at the Port.
Public Works	1. Disaster preparedness and response 2. Environmental monitoring and documentation 3. Inspect/Survey properties & assets 4. Project inspection and documentation 5. Surveying/Mapping data collection
Public Utilities	1. Construction Management: Examples include inspection of project sites for contract and environmental compliance. 2. Environmental Monitoring & Documentation: Examples include monitoring of vegetation type and health, wildlife, and streams/reservoirs. 3. Inspections: Conducting surveys and assessments of SFPUC properties and assets. Examples include survey of bay and ocean outfalls, inspection of large wastewater collections and power line surveys. 4. Disaster Relief: Drones may be used in disaster relief to record footage of damage and assess the role PUC may play in responding to such disasters. 5. Marketing and Public Education: Drones may be used to capture footage of the watershed, as an example, to be used in public education and/or marketing materials.
Recreation & Parks	1. Disaster preparedness and response: In times of disaster preparedness or post-disaster mitigation, drones will provide critical emergency response functions such as logistical

	support for emergency routing, life safety, and cleanup efforts, not only assisting in protecting physical assets and public spaces but human life as well 2. Environmental monitoring and documentation 3. Inspect/Survey properties & assets 4. Project inspection and documentation 5. Surveying/Mapping data collection
Technology	1. Drone technology is authorized for use during Video production, specifically the capture of video stills and photographs as elements of SFGovTV's video productions. The completed videos will be broadcast on SFGovTV's cable channels and made available on the station's YouTube account. Marketing and promotional videos created for other City departments may also feature drone footage or photographs.

Drones Public Meeting Dates:

Date	**Meeting**	**Departments**
April 16, 2015	COIT	All
September 17, 2015	COIT	All
April 20, 2017	COIT	All
May 5, 2017	COIT	All
March 21, 2019	COIT	All
September 19, 2019	COIT	All
February 28, 2020	PSAB	All
June 12, 2020	PSAB	Public Works
June 26, 2020	PSAB	Fire, Public Utilities, Tech
July 10, 2020	PSAB	Port, Recreation & Parks
July 17, 2020	COIT	All

COIT recommends the following action be taken on the policies:

- Approve the Drone Surveillance Technology Policies for the Fire, Port, Public Works, Public Utilities, Recreation and Parks, and Technology Departments.

Security Cameras

Departments Using Consolidated Policy	**Authorized Uses**
Airport Arts Commission Asian Art Museum Child Support Services City Administrator Emergency Management Fire Homelessness and Supportive Housing Human Resources Human Services Agency Port Public Health Recreation and Parks Rent Board Technology War Memorial	1. Live monitoring. 2. Recording of video and images. 3. Reviewing camera footage in the event of an incident. 4. Providing video footage/images to law enforcement or other authorized persons following an incident or upon request.
Department Specific Security Policies	**Authorized Uses**
Municipal Transportation Agency	1. Live monitoring. 2. Recording of video, images and review in the event of an incident. 3. Reviewing camera footage and/or images. 4. Providing video footage/images to law enforcement or other authorized persons following an incident. 5. Enforcing parking and driving violations.
Public Library	1. Live monitoring to protect safety of SFPL staff, patrons and facilities. 2. Recording of video and images.

	3. Reviewing camera footage in the event of an incident. 4. Providing video footage/images to law enforcement or other authorized persons following an incident or upon request.
Public Utilities Commission	1. Deter malicious behavior to SFPUC facilities, employees, or personnel working on behalf of the SFPUC; 2. Capture potential or actual malicious behavior by or against SFPUC facilities, employees, or personnel working on behalf of the SFPUC; 3. Provide evidence to support incident investigations; 4. Provide real-time monitoring of operations and critical equipment at SFPUC facilities; and 5. Support SFPUC health and safety requirements and objectives.

Security Cameras Public Meeting Dates:

Date	**Meeting**	**Departments**
November 13, 2020	PSAB	War Memorial
January 22, 2021	PSAB	ADM, DHR, FIR, MOHCD, REG, WAR
February 12, 2021	PSAB	AIR, AAM, DT, HSA, HSH, MTA, SFPL
February 26, 2021	PSAB	ART, CSS, DEM, OEWD, PRT, RNT, MOHCD, WAR, REG, PUC, REC
March 12, 2021	PSAB	DPH, PUC, REC
March 18, 2021	COIT	All

COIT recommends the following action be taken on the policies:

- Approve the Security Camera Technology Policies for the 19 departments,

In addition, COIT urges the Board to consider the following policy items in their review:

- Data Retention Standard: State Government Code section 34090.6 requires all local government camera footage to be stored for a minimum of 1 year. This presents significant privacy, security risks and also requires significant funds to comply. Current storage practices are typically 30 days or less. COIT recommends advocating to state law to reflect modern privacy and cybersecurity considerations.
- Sharing with Law Enforcement: Currently only the Homelessness and Supportive Housing, Human Services Agency, and Public Library require a subpoena before sharing camera footage with public safety. The Board of Supervisors should determine if a similar requirement should be on all departments.

Radio Frequency Identification (RFID)

Department	Authorized Uses
Public Library	1. Passive RFID tags applied to library material – For use in inventory management and circulation functions. 2. Staff workstation RFID pads – For use by staff to check in and out material and trigger holds. 3. Self-check machines – For use by patrons to check out material. 4. Inventory wand – For use by staff to confirm the current inventory on the library's shelves. 5. Sorting machine – For use in checking in material and sorting the items into carts and bins for delivery to other floors and branches.

RFID Public Meeting Dates:

Date	Meeting
January 24, 2020	Privacy and Surveillance Advisory Board (PSAB)
February 20, 2020	Committee on Information Technology (COIT)

COIT recommends the following action be taken on the policies:

- Approve the RFID Technology Policy for the Public Library.

BOARD of SUPERVISORS

City Hall
1 Dr. Carlton B. Goodlett Place, Room 244
San Francisco 94102-4689
Tel. No. 554-5184
Fax No. 554-5163
TDD/TTY No. 554-5227

M E M O R A N D U M

TO: Carmen Chu, City Administrator
Chief William Scott, Police Department
Airport Director Ivar C. Satero, Airport Department
Alaric Degrafinried, Interim Director, Public Works
Phil Ginsburg, General Manager, Recreation and Parks Department
Linda Gerull, Executive Director, Department of Technology
Mary Ellen Carroll, Executive Director, Dept. of Emergency Management
Chief Jeanine Nicholson, Fire Department
Elaine Forbes, Executive Director, SF Port Department
Michel Carlin, Acting General Manager, SFPUC
Michael Lambert, City Librarian
All City Department Heads via Sophia Kittler, Mayor's Office

FROM: Victor Young, Assistant Clerk

DATE: May 20, 2021

SUBJECT: LEGISLATION INTRODUCED

The Board of Supervisors' Rules Committee received the following proposed legisation:

File No. 210559

Ordinance approving Surveillance Technology Policies governing the use of 1) Audio Recorders (ShotSpotter) by the Police Department, 2) Automatic License Plate Readers by the Airport, Department of Public Works, Recreation and Parks Department, and Police Department, 3) Drones by the Fire Department, Port, Department of Public Works, Public Utilities Commission, Recreation and Parks Department, and Department of Technology, 4) Security Cameras by the Airport, Arts Commission, Asian Art Museum, Department of Child Support Services, City Administrator, Department of Technology, Department of Emergency Management, Fire Department, Department of Homelessness and Supportive Housing, Department of Human Resources, Human Services Agency, Library, Municipal Transportation Agency, Port, Public Utilities Commission, Department of Public Health, Recreation and Parks Department, Rent Board, and War Memorial, and 5) Radio Frequency Identification by the Library; making required findings in support of said approvals; and amending the Administrative Code to require departments to post each

Board-approved Surveillance Technology Policy on the department website.

If you have comments or reports to be included with the file, please forward them to me at the Board of Supervisors, City Hall, Room 244, 1 Dr. Carlton B. Goodlett Place, San Francisco, CA 94102 or by email at: victor.young@sfgov.org.

c. Tal Quetone, Office of the City Administrator
Rowena Carr, Police Department
Gamero, Police Department
Diana Oliva-Aroche, Police Department
Cathy Widener, Airport
David Steinberg, Public Works
Jeremy Spitz, Public Works
Lena Liu, Public Works
Sarah Madland, Recreation and Parks
Boris Delepine, Port Department
Karen Hong Yee, Department of Technology
Masood Ordikhani, SFPUC
Almer Castillo, Public Library
Andres Power, Mayor's Office
Victor Lim, Emergency Management

From: Hepner, Lee (BOS)
To: BOS Legislation, (BOS); Young, Victor (BOS)
Cc: Peskin, Aaron (BOS)
Subject: File 210559 - add Supe Peskin as co-sponsor
Date: Monday, July 19, 2021 11:36:57 AM

Dearest Clerks! Please kindly add Supervisor Peskin as co-sponsor of File 210559 – Surveillance Technology Policies.

Thanks,
Lee

Lee Hepner
Legislative Aide
Supervisor Aaron Peskin
(415) 554-7419 | *pronouns: he, him, his*

District 3 Website
Sign up for our newsletter here!