File No. 221043 **Committee Item No.** 7
Board Item No. _____

COMMITTEE/BOARD OF SUPERVISORS

AGENDA PACKET CONTENTS LIST

Committee: Rules Committee **Date** Oct. 17, 2022

Board of Supervisors Meeting **Date** _____

Cmte	Board	
☐	☐	**Motion**
☐	☐	**Resolution**
☒	☐	**Ordinance**
☒	☐	**Legislative Digest**
☐	☐	**Budget and Legislative Analyst Report**
☐	☐	**Youth Commission Report**
☐	☐	**Introduction Form**
☒	☐	**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**
☐	☐	**Information/Vacancies (Boards/Commissions)**
☐	☐	**Public Correspondence**

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

☐	☐	_____
☐	☐	_____
☐	☐	_____
☐	☐	_____
☐	☐	_____
☐	☐	_____
☐	☐	_____
☐	☐	_____
☐	☐	_____

Completed by: Victor Young **Date** Oct 12, 2022
Completed by: _____ **Date** _____

AMENDED IN COMMITTEE
10/3/2022

FILE NO. 221043 ORDINANCE NO.

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

Ordinance approving Surveillance Technology Policies governing the use of ~~1)~~ ~~Automatic License Plate Readers by the Municipal Transportation Agency, 2) Biometric Processing Software or System by the Juvenile Probation Department, 3~~1) **Body-Worn Cameras by the** ~~Fire Department and~~ **Recreation and Park Department,** ~~4) People-Counting Camera by the Library, 5~~2**) Security Cameras by the Department of Elections,** ~~6~~3**) Third-Party Security Cameras by the Airport,** and ~~Municipal Transportation Agency, Police Department, and War Memorial, 7~~4**) Location Management System**~~s~~ **by the** ~~Juvenile Probation Department and the~~ **Recreation and Park Department**~~,~~; ~~8) Computer Management System by the Library, and 9) Social Media Monitoring Software by the Library;~~ **and making required findings in support of said approvals.**

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) Terms used in this ordinance shall have the meaning set forth in Administrative Code Chapter 19B ("Chapter 19B").

(b) Chapter 19B regulates City Departments' acquisition and use of Surveillance Technology. Under Section 19B.5, City Departments that possessed or were using Surveillance Technology before Chapter 19B took effect in July 2019, must obtain Board of

Supervisors approval by ordinance of a Surveillance Policy for each type of existing Surveillance Technology. Under Section 19B.2, a Department must obtain Board of Supervisors approval by ordinance of a Surveillance Technology Policy before: (1) seeking funds for Surveillance Technology; (2) acquiring or borrowing new Surveillance Technology; (3) using new or existing Surveillance Technology for a purpose, in a manner, or in a location not specified in a Surveillance Technology Policy ordinance approved by the Board in accordance with Chapter 19B; (4) entering into agreement with a non-City entity to acquire, share, or otherwise use Surveillance Technology; or (5) entering into an oral or written agreement under which a non-City entity or individual regularly provides the Department with data or information acquired through the entity's use of Surveillance Technology.

(c) Beginning in August 2019, Departments submitted to the Committee on Information Technology ("COIT") inventories of their existing Surveillance Technology and submitted Surveillance Impact Reports for each type of Surveillance Technology on their inventory.

(d) After receiving the inventories and Surveillance Impact Reports, COIT and its Privacy and Surveillance Advisory Board ("PSAB") subcommittee, 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 ~~eight~~four categories of Surveillance Technology:

~~(1) Automatic License Plate Readers (ALPR)~~

~~(2) Biometric Processing Software or System~~

(~~3~~1) Body-Worn Cameras

~~(4) People-Counting Cameras~~

(~~5~~2) Security Cameras

(~~6~~3) Third-Party Security Cameras

(~~7~~4) Location Management System

~~(8) Computer Management System~~

(e) Additionally, ~~the Library submitted a Surveillance Impact Report for Social Media Monitoring Software and~~ the Recreation and Park Department submitted a Surveillance Impact Report for a Location Management System. Based on the Surveillance Impact Report~~s~~, COIT developed a Surveillance Technology Policy for ~~Social Media Monitoring Platforms used by the Library, and a Surveillance Technology Policy for~~ a Location Management System used by the Recreation and Park Department.

(f) The Surveillance Technology Policies that COIT developed for each Department are detailed in Sections 2 through ~~10~~5 of this ordinance. The Surveillance Technology Policies are available in Board File No. 220843, and are incorporated herein by reference. COIT recommends that the Board of Supervisors approve each Surveillance Technology Policy.

(g) This ordinance sets forth the Board's findings in support of each Surveillance Technology Policy and its approval of each policy.

~~Section 2. Automatic License Plate Readers ("ALPR"): Municipal Transportation Agency ("MTA").~~

~~(a) Current Status. MTA currently possesses and uses ALPR.~~

~~(b) Purpose. MTA uses an ALPR ("MTA ALPR") to: (1) enforce parking restrictions and laws; (2) Transit Only Lane Enforcement; (3) link individual vehicles to their times of entry/exit into City-owned parking garages and lots to accurately calculate parking fees; (4) identify vehicles that are the subject of an active investigation by the Police Department; and (5) analyze and report on parking and curb usage.~~

~~(c) Surveillance Impact Report. MTA submitted a Surveillance Impact Report for MTA ALPR to COIT. A copy of the Surveillance Impact Report is in Board File No. 220843, and is incorporated herein by reference.~~

~~(d) Public Hearings. Between September 9, 2021 and October 21, 2021, 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 MTA ALPR ("MTA ALPR Policy"). A copy of the MTA ALPR Policy is in Board File No.220843, and is incorporated herein by reference.~~

~~(e) COIT Recommendation. On October 21, 2021, COIT voted to recommend the MTA ALPR Policy to the Board of Supervisors for approval.~~

~~(f) Findings. The Board of Supervisors hereby finds that the benefits that the MTA ALPR Policy authorizes outweigh the costs and risks; that the MTA ALPR Policy will safeguard civil liberties and civil rights; and that the uses and deployments of MTA ALPR, as set forth in the MTA ALPR 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 MTA ALPR Policy under which MTA may continue to possess and use the MTA ALPR.~~

~~Section 3. Biometric Processing Software or System (Continuous Alcohol Monitoring "CAM" technology): Juvenile Probation.~~

~~(a) Current Status. Juvenile Probation currently possesses and uses CAM technology.~~

~~(b) Purpose. Juvenile Probation uses CAM technology known as SCRAM CAM to monitor alcohol consumption among youth on court-ordered probation as a condition of their probation.~~

~~(c) Surveillance Impact Report. Juvenile Probation submitted a Surveillance Impact Report for SCRAM CAM to COIT. A copy of the Juvenile Probation Surveillance Impact Report for SCRAM CAM is in Board File No. 220843, and is incorporated herein by reference.~~

~~(d) Public Hearings. On January 14, 2022 and February 17, 2022, 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 Juvenile Probation's use of SCRAM CAM ("Juvenile Probation SCRAM CAM Policy"). A copy of the Juvenile Probation SCRAM CAM Policy is in Board File No. 220843, and is incorporated herein by reference.~~

~~(e) COIT Recommendation. On February 17, 2022, COIT voted to recommend the Juvenile Probation SCRAM CAM Policy to the Board of Supervisors for approval.~~

~~(f) Findings. The Board of Supervisors hereby finds that: the benefits authorized by the Juvenile Probation SCRAM CAM Policy outweigh its costs and risks; that the Juvenile Probation SCRAM CAM Policy will safeguard civil liberties and civil rights, and that the uses and deployments of SCRAM CAM, as set forth in the Juvenile Probation SCRAM CAM 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 Juvenile Probation SCRAM CAM Policy under which Juvenile Probation may continue to possess and use SCRAM CAM.~~

Section ~~4~~2. Body-Worn Cameras: ~~Fire Department and~~ Recreation and Park Department.

(a) Current Status. The following Department~~s~~ currently possesse~~s~~ and use~~s~~ Body-Worn Cameras: ~~the Fire Department; and~~ the Recreation and Park Department.

~~(b) Fire Department.~~

~~(1) Purpose. The Fire Department's Public Information Officer (PIO) currently uses a Body-Worn Camera when on-scene at large incidents to capture video of surroundings and the totality of the incident.~~

~~(2) Surveillance Impact Report. The Fire Department submitted to COIT a Surveillance Impact Report for Fire Department Body-Worn Cameras. A copy of the Surveillance Impact Report is in Board File No. 220843, and is incorporated herein by reference.~~

~~(3) Public Hearings. On September 10, 2021, and October 21, 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 Fire Department Body-Worn Cameras ("Fire Department Body-Worn Cameras Policy"). A copy of the Fire Department Body-Worn Cameras Policy is in Board File No. 220843, and is incorporated herein by reference.~~

~~(4) COIT Recommendation. On October 21, 2021, COIT voted to recommend the Fire Department Body-Worn Cameras Policy to the Board of Supervisors for approval.~~

~~(5) Findings. The Board of Supervisors hereby finds that the benefits that the Fire Department Body-Worn Cameras Policy authorizes outweigh the costs and risks; that the Fire Department Body-Worn Cameras Policy will safeguard civil liberties and civil rights; and that the uses and deployments of Body-Worn Cameras, as set forth in the Fire Department Body-Worn Cameras 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 Department Body-Worn Cameras Policy under which the Fire Department may continue to possess and use the Body-Worn Cameras.~~

(~~c~~b) Recreation and Park Department.

(1) Purpose. The Recreation and Park Department uses Body-Worn Cameras to record video and audio footage in the event of an incident, including actual or potential criminal conduct; in situations where a Park Ranger reasonably believes recordings of evidentiary value may be requested; and calls for service involving a crime where the recording may aid in the apprehension/prosecution of a suspect. The Recreation and Park Department also provides Body-Worn Camera recordings to law enforcement or other authorized persons upon request.

(2) Surveillance Impact Report. The Recreation and Park Department submitted a Surveillance Impact Report for Body-Worn Cameras to COIT. A copy of the Surveillance Impact Report is in Board File No. 220843, and is incorporated herein by reference.

(3) Public Hearings. On September 24, 2021 and October 21, 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 Recreation and Park Department Body-Worn Cameras ("Recreation and Parks Department Body-Worn Cameras Policy"). A copy of the Recreation and Parks Department's Body-Worn Cameras Policy is in Board File No. 220843, and is incorporated herein by reference.

(4) COIT Recommendation. On October 21, 2021, COIT voted to recommend the Recreation and Parks Department Body-Worn Cameras Policy to the Board of Supervisors for approval.

(5) Findings. The Board of Supervisors hereby finds that the benefits that the Recreation and Parks Department's Body-Worn Cameras Policy authorizes outweighs its costs and risks; that the Recreation and Parks Department Body-Worn Cameras Policy will safeguard civil liberties and civil rights; and that the uses and deployments of the Body-Worn Cameras, as set forth in the Recreation and Parks Department Body-Worn Cameras 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 Recreation and Parks Department Body-Worn Cameras Policy under which the Recreation and Park Department may continue to possess and use the Body-Worn Cameras.

~~Section 5. People-Counting Camera: Library.~~

~~(a) Current Status. The Library currently possesses and uses People-Counting Cameras.~~

~~(b) Purpose. Library uses People-Counting Cameras to: (A) tally the entry and exit of Library visitors at all 28 public facilities; and (B) track usage of meeting rooms, elevators, and restrooms for purposes of resource allocation.~~

~~(c) Surveillance Impact Report. The Library submitted a Surveillance Impact Report for Library People-Counting Cameras to COIT. A copy of the Library Surveillance Impact Report for Library People-Counting Cameras is in Board File No. 220843, and is incorporated herein by reference.~~

~~(d) Public Hearings. On January 28, 2022, March 11, 2022, and April 21, 2022, 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 Library People-Counting Cameras. A copy of the Surveillance Technology Policy for the Library's use of the Library People-Counting Cameras ("Library People-Counting Cameras Policy") is in Board File No. 220843, and is incorporated herein by reference.~~

~~(e) COIT Recommendation. On April 21, 2022, COIT voted to recommend the Library People-Counting Cameras Policy to the Board of Supervisors for approval.~~

~~(f) Findings. The Board of Supervisors hereby finds that: the benefits that the Library People-Counting Cameras Policy authorizes outweigh its costs and risks; that the Library People-Counting Cameras Policy will safeguard civil liberties and civil rights; and that the uses and deployments of Library People-Counting Cameras, as set forth in the Library People-Counting Cameras 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 People-Counting Cameras Policy under which the Library may continue to possess and use the Library People-Counting Cameras.~~

Section ~~6~~3. Security Cameras: Department of Elections.

(a) Current Status. The Department of Elections currently possesses and uses Security Cameras.

(b) Purpose. The Department of Elections uses the Security Cameras to: (A) conduct live monitoring of voting center lines; (B) conduct live monitoring of Department staff during elections operations; (C) record video and images of Department staff during elections operations; (D) review camera footage of Department staff in the event of an incident; and (E) share camera footage of Department staff with the public to promote transparency into elections operations.

(c) Surveillance Impact Report. The Department of Elections submitted a Surveillance Impact Report for the Security Cameras. A copy of the Surveillance Impact Report is in Board File No. 220843, and is incorporated herein by reference.

(d) Public Hearings. On January 22, 2021, October 21, 2021, and November 18, 2021, 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 Security

Cameras. A copy of the Department of Elections Cameras Policy is in Board File No. 220843, and is incorporated herein by reference.

(e) COIT Recommendation. On November 18, 2021, COIT voted to recommend the Department of Elections Cameras Policy to the Board of Supervisors for approval.

(f) Findings. The Board of Supervisors hereby finds that: the benefits authorized by the Department of Elections Cameras Policy outweigh the costs and risks; that the Department of Elections Cameras Policy will safeguard civil liberties and civil rights, and that the uses and deployments of Cameras, as set forth in the Department of Elections Cameras 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 Department of Elections Cameras Policy under which the Department of Elections may continue to possess and use the Security Cameras.

Section ~~7~~4. Third-Party Security Cameras: San Francisco International Airport ("SFO")~~, MTA, War Memorial and Performing Arts Center ("War Memorial")~~.

(a) Current Status. The following Department~~s~~ currently possesses and uses data from Third-Party Security Cameras: SFO~~, MTA, and War Memorial~~.

(b) SFO.

(1) Purpose. SFO uses data from security cameras owned and operated by SFO tenants, including airlines, concessionaries, food and beverage operators, and rental car agencies ("Tenant Security Cameras"), to (A) review camera footage in the event of an incident; and (B) approve Airport tenants' disclosure of digital recordings and other data from its security camera.

(2) Surveillance Impact Report. SFO submitted a Surveillance Impact Report for Tenant Security Cameras. A copy of the Surveillance Impact Report is in Board File No. 220843, and is incorporated herein by reference.

(3) Public Hearings. Between January 14, 2022 and February 17, 2022, 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 SFO Tenant Security Cameras ("SFO Tenant Security Cameras Policy"). A copy of the SFO Tenant Security Cameras Policy is in Board File No. 220843, and is incorporated herein by reference.

(4) COIT Recommendation. On February 17, 2022, COIT voted to recommend the SFO Tenant Security Cameras Policy to the Board of Supervisors for approval.

(5) Findings. The Board of Supervisors hereby finds that the benefits authorized by the SFO Tenant Security Cameras Policy outweigh the costs and risks; that the SFO Tenant Security Cameras Policy will safeguard civil liberties and civil rights; and that the uses and deployments of Tenant Security Cameras, as set forth in the SFO Tenant Security Cameras 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 SFO Tenant Security Cameras Policy under which SFO may continue to possess and use the Tenant Security Cameras.

~~(c) MTA.~~

~~(1) Purpose. MTA uses Third-Party Security Cameras owned and operated by taxi drivers that are located inside taxi cabs ("Taxi Dashboard Cameras") to: (A) review recordings of on-board incidents based upon complaints received from the public, and use at appeals hearings in response to a fine, suspension, or response to fine revocation; (B) review~~

~~video data in response to complaints from the public to ensure compliance by taxi cab companies and other taxi permittees with requirements and conditions under Article 1100 (Regulation of Motor Vehicles for Hire) of Division II of the Transportation Code; (C) review video data to confirm taxi cab companies and other taxi permittees complete rides paid for with public funds before paying the companies for those rides; (D) review video to investigate criminal acts involving taxi drivers or riders; and (E) review video data to investigate accidents involving a taxi cab.~~

~~(2) Surveillance Impact Report. MTA submitted a Surveillance Impact Report for MTA Taxi Dashboard Cameras to COIT. A copy of the Surveillance Impact Report is in Board File No. 220843, and is incorporated herein by reference.~~

~~(3) Public Hearings. On March 11, 2022, and April 21, 2022, 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 MTA Taxi Dashboard Cameras ("MTA Taxi Dashboard Camera Policy"). A copy of the MTA Taxi Dashboard Camera Policy is in Board File No. 220843, and is incorporated herein by reference.~~

~~(4) COIT Recommendation. On April 21, 2022, COIT voted to recommend the MTA Taxi Dashboard Camera Policy to the Board of Supervisors for approval.~~

~~(5) Findings. The Board of Supervisors hereby finds that the benefits authorized by the MTA Taxi Dashboard Camera Policy outweigh the costs and risks; that the MTA Taxi Dashboard Camera Policy will safeguard civil liberties and civil rights, and that the uses and deployments of the MTA Taxi Dashboard Cameras, as set forth in the MTA Taxi Dashboard 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 Taxi Dashboard Camera Policy under which MTA may continue to possess and use the MTA Taxi Dashboard Cameras.~~

~~(d) War Memorial.~~

~~(1) Purpose. War Memorial uses data from security cameras owned and operated by the San Francisco Symphony located at War Memorial venues ("Tenant Security Cameras") to: (A) live monitor Davies Symphony Hall internal and public areas; and (B) review camera footage in the event of an incident.~~

~~(2) Surveillance Impact Report. War Memorial submitted a Surveillance Impact Report for Tenant Security Cameras. A copy of the Surveillance Impact Report is in Board File No. 220843, and is incorporated herein by reference.~~

~~(3) Public Hearings. Between August 27, 2021, and April 21, 2022, 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 Tenant Security Cameras ("War Memorial Tenant Security Cameras Policy"). A copy of the War Memorial Tenant Security Cameras Policy is in Board File No. 220843, and is incorporated herein by reference.~~

~~(4) COIT Recommendation. On April 21, 2022, COIT voted to recommend the War Memorial Tenant Security Cameras Policy to the Board of Supervisors for approval.~~

~~(5) Findings. The Board of Supervisors hereby finds that benefits authorized by the War Memorial Tenant Security Cameras Policy outweigh the costs and risks; that the War Memorial Tenant Security Cameras Policy will safeguard civil liberties and civil rights; and that the uses and deployments of Tenant Security Cameras, as set forth in the War Memorial Tenant Security Cameras 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 War Memorial Tenant Security Cameras Policy under which War Memorial may continue to possess and use the Tenant Security Cameras.~~

Section ~~8~~5. Location Management System: ~~Juvenile Probation and~~ Recreation and Park Department.

(a) Current Status. ~~Juvenile Probation currently possesses and uses a Location Management System.~~ The Recreation and Park Department seeks to acquire and use a Location Management System.

~~(b) Juvenile Probation~~

~~(1) Purpose. Juvenile Probation uses a Location Management System known as SCRAM Global Positioning System ("SCRAM GPS") to enforce court-ordered supervision of youth placed on electronic monitoring as a condition of their probation or as an alternative to detention.~~

~~(2) Surveillance Impact Report. Juvenile Probation submitted a Surveillance Impact Report for SCRAM GPS. A copy of the Surveillance Impact Report is in Board File No. 220843, and is incorporated herein by reference.~~

~~(3) Public Hearings. On October 22, 2021 and November 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 SCRAM GPS ("Juvenile Probation SCRAM GPS Policy"). A copy of the Juvenile Probation SCRAM GPS Policy is in Board File No. 220843, and is incorporated herein by reference.~~

~~(4) COIT Recommendation. On November 18, 2021, COIT voted to recommend the Juvenile Probation SCRAM GPS Policy to the Board of Supervisors for approval.~~

~~(5) Findings. The Board of Supervisors hereby finds that the benefits authorized in the Juvenile Probation SCRAM GPS Policy outweigh the costs and risks; that the SCRAM GPS will safeguard civil liberties and civil rights; and that the uses and deployments of SCRAM GPS, as set forth in the Juvenile Probation SCRAM GPS 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 Juvenile Probation SCRAM GPS Policy under which Juvenile Probation may continue to possess and use SCRAM GPS.~~

(~~c~~b) Recreation and Park Department

(1) Purpose. The Recreation and Park Department would like to use a Location Management System to manage reservations for tennis facilities and determine if reservation holders are present at the tennis facility at the time of their reservation.

(2) Surveillance Impact Report. The Recreation and Park Department submitted a Surveillance Impact Report for a Location Management System to COIT. A copy of the Surveillance Impact Report is in Board File No. 220843, and is incorporated herein by reference.

(3) Public Hearings. On March 11, 2022, May 27, 2022, and June 16, 2022, 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 Location Management System ("Tennis Reservations Application Policy"). A copy of the Recreation and Park Department Tennis Reservations Application Policy is in Board File No. 220843, and is incorporated herein by reference.

(4) COIT Recommendation. On June 16, 2021, COIT voted to recommend the Recreation and Park Department Tennis Reservations Application Policy to the Board of Supervisors for approval.

(5) Findings. The Board of Supervisors hereby finds that the benefits authorized by the Recreation and Park Department Tennis Reservations Application Policy outweigh the costs and risks; that the Location Management System will safeguard civil liberties and civil rights; and that the uses and deployments of the Location Management System, as set forth in the Recreation and Park Department Tennis Reservations Application 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 Recreation and Park Department Tennis Reservations Application Policy under which the Recreation and Park Department may acquire and use the Location Management System.

~~Section 9. Computer Management System: Library.~~

~~(a) Current Status. The Library currently possesses and uses a Computer Management System.~~

~~(b) Purpose. The Library uses a Computer Management System to provide time-delimited public access to library computers and allow the public to print, copy, scan, and fax documents, as well as to track usage of computers and print resources throughout Library facilities for purposes of resource allocation and management.~~

~~(c) Surveillance Impact Report. The Library submitted a Surveillance Impact Report for their Computer Management System to COIT. A copy of the Library Surveillance Impact Report for their Computer Management System is in Board File No. 220843, and is incorporated herein by reference.~~

~~(d) Public Hearings. On May 27, 2022, and June 16, 2022, 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 Computer Management System. A copy of the Surveillance Technology Policy for the Library's use of the Library Computer Management System ("Library Computer Management System Policy") is in Board File No. 220843, and is incorporated herein by reference.~~

~~(e) COIT Recommendation. On June 16, 2022, COIT voted to recommend the Library Computer Management System Policy to the Board of Supervisors for approval.~~

~~(f) Findings. The Board of Supervisors hereby finds that the benefits that the Library Computer Management System Policy authorizes outweigh its costs and risks; that the Library Computer Management System Policy will safeguard civil liberties and civil rights; and that the uses and deployments of the Library Computer Management System, as set forth in the Library Computer Management System 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 Computer Management System Policy under which the Library may continue to possess and use the Library Computer Management System.~~

~~Section 10. Social Media Monitoring Software: Library.~~

~~(a) Current Status. The Library seeks to acquire and use Social Media Monitoring Software.~~

~~(b) Purpose. The Library would like to use Social Media Monitoring Software to plan, execute, and analyze trends in communication campaigns across social media platforms.~~

~~(c) Surveillance Impact Report. The Library submitted a Surveillance Impact Report for Social Media Monitoring Software to COIT. A copy of the Library Surveillance Impact Report is in Board File No. 220843, and is incorporated herein by reference.~~

~~(d) Public Hearings. On August 27, 2021 and October 21, 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 Social Media Monitoring Software ("Library Social Media Monitoring Software Policy"). A copy of the Library Social Media Monitoring Software Policy is in Board File No. 220843, and is incorporated herein by reference.~~

~~(e) COIT Recommendation. On October 21, 2021, COIT voted to recommend the Library Social Media Monitoring Software Policy to the Board of Supervisors for approval.~~

~~(f) Findings. The Board of Supervisors hereby finds that the benefits authorized by the Library Social Media Monitoring Software Policy outweigh the costs and risks; that the Social Media Monitoring Software will safeguard civil liberties and civil rights; and that the uses and deployments of Social Media Monitoring Software, as set forth in the Library Social Media Monitoring Software 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 Social Media Monitoring Software Policy under which the Library may acquire and use the Social Media Monitoring Software.~~

Section ~~11~~6. 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:
DAVID CHIU, City Attorney

By: /s/ Zachary Porianda
ZACHARY PORIANDA
Deputy City Attorney

n:\govern\as2022\1900636\01632431.docx

FILE NO. 221043

LEGISLATIVE DIGEST

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

Ordinance approving Surveillance Technology Policies governing the use of 1) Body-Worn Cameras by the Recreation and Park Department, 2) Security Cameras by the Department of Elections, 3) Third-Party Security Cameras by the Airport, and 4) Location Management Systems by the Recreation and Park Department; and making required findings in support of said approvals.

Background Information

Chapter 19B regulates City Departments' acquisition and use of Surveillance Technology.

Under 19B.5, City Departments that possessed or were using Surveillance Technology before Chapter 19B took effect in July 2019 must obtain Board of Supervisors approval by ordinance of a Surveillance Policy for each type of existing Surveillance Technology.

Under Chapter 19B.2, a Department must obtain Board of Supervisors approval by ordinance of a Surveillance Technology Policy before: (1) seeking funds for Surveillance Technology; (2) acquiring or borrowing new Surveillance Technology; (3) using new or existing Surveillance Technology for a purpose, in a manner, or in a location not specified in a Surveillance Technology Policy ordinance approved by the Board in accordance with Chapter 19B; (4) entering into agreement with a non-City entity to acquire, share, or otherwise use Surveillance Technology; or (5) entering into an oral or written agreement under which a non-City entity or individual regularly provides the Department with data or information acquired through the entity's use of Surveillance Technology.

Beginning in August 2019, Departments submitted to the Committee on Information Technology ("COIT") inventories of their existing Surveillance Technology and submitted Surveillance Impact Reports for each type of Surveillance Technology on their inventory. After receiving the inventories and Surveillance Impact Reports, COIT and its Privacy and Surveillance Advisory Board ("PSAB") subcommittee, 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 three categories of Surveillance Technology:

(1) Body-Worn Cameras

(2) Security Cameras; and
(3) Third-Party Security Cameras.

Additionally, the Recreation and Park Department submitted a Surveillance Impact Report for a Location Management System. Based on the Surveillance Impact Report, COIT developed a Surveillance Technology Policy for Location Management Systems used by the Recreation and Park Department.

The Surveillance Technology Policies that COIT developed for each Department are detailed in Sections 2 through 5 of the proposed ordinance. The Surveillance Technology Policies are available in Board File No. 220843. COIT recommends that the Board of Supervisors approve each Surveillance Technology Policy.

n:\govern\as2022\1900636\01632427.docx

City & County of San Francisco
London N. Breed, Mayor

Office of the City Administrator
Carmen Chu, City Administrator
Jillian Johnson, Director
Committee on Information Technology

To: Angela Calvillo
Clerk of Board of Supervisors

From: Carmen Chu, City Administrator
Jillian Johnson, Director, Committee of Information Technology

Date: July 18, 2022

Subject: Legislation introduced for Approval of Surveillance Technology Policies for Multiple City Departments

---

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 Surveillance Technology Policies and Impact Reports for the following technologies to the Board of Supervisors for their review:

- Automatic License Plate Readers (ALPR)
- Biometric Processing Software and/or System
- Body-Worn Cameras
- People-Counting Camera
- Security Cameras
- Third-Party Security Cameras
- Location Management System
- Computer Management System
- Social Media Monitoring Software

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 year to engage the public in developing these Surveillance Technology policies. All details of these discussions are available at sf.gov/COIT.

The following sections provide more detail on the departments seeking Board of Supervisors approval for their surveillance technology policies, and the COIT recommended course of action.

If you have questions on the review process, please direct questions to Jillian Johnson, Director of the Committee on Information Technology (COIT).

Automatic License Plate Readers (ALPR)

Department	Authorized Uses
Municipal Transportation Agency (MTA)	1. Enforce parking restrictions and laws. 2. Transit Only Lane Enforcement (TOLE). 3. Link individual vehicles to their times of entry/exit into City-owned parking garages and lots to accurately calculate parking fees. 4. Identify vehicles that are the subject of an active investigation by the SFPD (e.g., vehicles included on "hot lists" generated by the SFPD –see Appendix B & C of MTA policy, and page 8 of SFPD ALPR Policy). 5. Analysis of and reporting on parking and curb usage.

ALPR Public Meeting Dates:

Date	Meeting
August 27, 2021	Privacy and Surveillance Advisory Board (PSAB)
September 24, 2021	Privacy and Surveillance Advisory Board (PSAB)
October 21, 2021	Committee on Information Technology (COIT)

COIT Recommendation:

COIT recommends the Board of Supervisors adopt the ALPR Surveillance Technology Policy for the MTA.

Biometric Processing Software or System

Department	Authorized Uses
Juvenile Probation	- Youth are only placed on continuous alcohol monitoring (CAM) in San Francisco with a court order. The Court may order a youth to be placed on CAM as a condition of probation, if the Court determines that is in the interest of public safety and the youth's wellbeing. CAM data is analyzed on a daily basis by probation officers to ensure compliance with the Court's order.

Biometric Processing Software/System Public Meeting Dates:

Date	Meeting
January 14, 2022	Privacy and Surveillance Advisory Board (PSAB)
February 17, 2022	Committee on Information Technology (COIT)

COIT Recommendation:

COIT recommends the Board of Supervisors adopt the Biometric Processing System Surveillance Technology Policy for Juvenile Probation.

Body-Worn Cameras

Departments	Authorized Uses
Fire	- Use by Public Information Officer (PIO) at large incidents to capture video of surroundings and the totality of the incident
Recreation and Parks	- Recording video and audio footage in the event of an incident. Incidents can be: o Actual or potential criminal conduct o Situation when a Park Ranger reasonably believes recordings of evidentiary value may be obtained o Calls for service involving a crime where the recording may aid in the apprehension/ prosecution of a suspect - Providing recording to law enforcement or other authorized persons upon request.

Body-Worn Cameras Public Meeting Dates:

Date	Meeting	Departments
September 10, 2021	PSAB	Fire
September 24, 2021	PSAB	Recreation and Parks
October 21, 2021	COIT	Fire, Recreation and Parks

COIT Recommendation:

COIT recommends the Board of Supervisors adopt the Body-Worn Camera Surveillance Technology Policies for the Fire Department and the Recreation and Parks Department.

People-Counting Cameras

Departments	Authorized Uses
Library	- To tally the entry and exit of Library visitors at all 28 public facilities. - To track usage of meeting rooms, elevators and restrooms for purposes of resource allocation.

People-Counting Cameras Public Meeting Dates:

Date	Meeting
January 28, 2022	Privacy and Surveillance Advisory Board (PSAB)
March 11, 2022	Privacy and Surveillance Advisory Board (PSAB)
April 21, 2022	Committee on Information Technology (COIT)

COIT Recommendation:

COIT recommends the Board of Supervisors adopt the People-Counting Camera Surveillance Technology policy for the Library.

Security Cameras

Departments	Authorized Uses
Elections	- Live monitoring of voting center lines. - Live monitoring of Department staff during elections operations. - Recording of video and images of Department staff during elections operations. - Reviewing camera footage of Department staff in the event of an incident. - Sharing camera footage of Department staff with the public to promote transparency into elections operations.

Security Cameras Public Meeting Dates:

Date	Meeting
October 22, 2021	Privacy and Surveillance Advisory Board (PSAB)
November 18, 2021	Committee on Information Technology (COIT)

COIT Recommendation:

COIT recommends the Board of Supervisors adopt the Security Camera Surveillance Technology Policy for the Department of Elections.

Third-Party Security Cameras

Departments	Authorized Uses
Airport (AIR)	- Reviewing camera footage in the event of an incident. - Approving Tenant's disclosure of digital recordings and other data from its security camera system.
Municipal Transportation Agency (MTA)	- Review recording of on-board incidents based upon complaints received from the public and at appeals hearing in response to a fine, suspension or response to fine revocation. - Review video data in response to complaints from the public to ensure compliance by taxi cab companies and other taxi permittees with requirements and conditions under Article 1100 (Regulation of Motor Vehicles for Hire) of Division II of the SF Transportation Code. - Review video data to confirm taxi cab companies and other taxi permittees complete rides paid for with public funds before paying the companies for those rides. For example, under its wheelchair program taxi incentive, the Department reviews video data from the technology to confirm that taxi cab drivers pick up individuals with certain disabilities before paying drivers for those rides, which are funded under various paratransit programs. - Review video to investigate criminal acts involving taxi drivers or riders. - Review video data to investigate accidents involving a taxi cab.
War Memorial (WAR)	- Live monitoring internal office space and public area of Davies Symphony Hall. - Reviewing camera footage provided by Tenant/Contractor upon request in the event of an incident.

Third-Party Security Cameras Public Meeting Dates:

Date	Meeting	Departments
October 22, 2021	PSAB	WAR
January 14, 2022	PSAB	WAR, AIR
January 28, 2022	PSAB	AIR
February 17, 2022	COIT	AIR
March 11, 2022	PSAB	MTA
April 21, 2022	COIT	WAR, MTA

COIT Recommendation:

COIT recommends the Board of Supervisors adopt the Third-Party Security Camera Surveillance Technology Policies for the Airport, Municipal Transportation Agency, and War Memorial.

Location Management System

Department	Authorized Uses
Juvenile Probation	- Youth are only placed on electronic monitoring in San Francisco with a court order. The Court may order a youth to be placed on electronic monitoring as an alternative to detention. - Electronic monitoring (EM) may also be added as a condition of probation if additional supervision is warranted. EM data is analyzed on a daily basis by probation officers to ensure compliance with: - Court ordered curfews o Inclusion zones: addresses/areas where the minor has approval to be present, for example their home, school, work. o Exclusion zones: addresses/areas where the minor should not be present, including Stay Away orders o Schedules: To monitor school attendance, program participation, work.
Recreation and Parks	- Confirm that the person who reserved the booking for a tennis court is at the location at the reserved time. - Utilize data to determine if there are any reservation holders who are violating booking policies because they are not showing up at the reserved time.

Location Management System Public Meeting Dates:

Date	Meeting	Department
October 22, 2021	PSAB	Juvenile Probation
November 18, 2021	COIT	Juvenile Probation
March 11, 2022	PSAB	Recreation and Parks
May 27, 2022	PSAB	Recreation and Parks
June 16, 2022	COIT	Recreation and Parks

COIT Recommendation:

COIT recommends the Board of Supervisors adopt the Location Management Surveillance Technology Policies for Juvenile Probation and the Recreation and Parks Department.

Social Media Monitoring Software

Department	Authorized Uses
Library	- Plan and execute more effective and strategic campaigns across social media platforms. - Schedule multiple social media posts in advance. - Create and monitor multiple streams of content across various platforms. - Maintain active social media presence that is automated, specifically on weekends when staff is off. - Ensure consistency of messaging across all social media platforms. - Track post performance and analyze trends to improve content and strategy. - Create reports.

Social Media Monitoring Software Public Meeting Dates:

Date	Meeting
August 27, 2021	Privacy and Surveillance Advisory Board (PSAB)
October 21, 2021	Committee on Information Technology (COIT)

COIT Recommendation:

COIT recommends the Board of Supervisors adopt the Social Media Monitoring Software Surveillance Technology Policy for the Library.

Computer Management System

Departments	Authorized Uses
Library	- The authorized use case for the TBS Computer Time and Print Management tool is to provide time-delimited public access to library computers and allow the public to print, copy, scan and fax documents, as well as track usage of computers and print resources throughout the library's 28 facilities for purposes of resource allocation and management.The five specific components within TBS Computer Time and Print Management are as follows: • MyPC: Manages patron access to library computers and regulates amount of time each patron can use computers • EZ Booking: Allows patrons to manage their reservations in MyPC, schedule public computer use, etc. • Papercut/EPrintIt: Manages public print jobs sent from library computers and patrons' personal devices, allowing them to print their documents on library printers. Also allows select library staff members, in the interest of customer service and support, to retrieve and print jobs submitted to the system by users during the 24-hour period in which documents are retrievable. This allows staff to print jobs when printers fail, when print jobs do not meet user expectations, to intermediate when users are struggling with technology, etc. • Allows library patrons to scan, manipulate, manage, print, email, fax and save documents using either the library's flat-bed or document feeder scanners. • Payment Kiosk: Allows patrons to pay for print and copy jobs processed through Papercut/EPrintIt and/or ScanEZ.

Security Cameras Public Meeting Dates:

Date	Meeting
May 27, 2022	Privacy and Surveillance Advisory Board (PSAB)

June 16, 2022	Committee on Information Technology (COIT)

COIT Recommendation:

COIT recommends the Board of Supervisors adopt the Computer Management System Surveillance Technology Policy for the Library.

Surveillance Impact Report

San Francisco International Airport ("Airport" or "Department")
Tenant 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 San Francisco International Airport ("Airport" or "Department") use of digital recordings and data from third party security cameras.

DESCRIPTION OF THE TECHNOLOGY

This impact assessment applies to the Airport's access to and use of digital recordings and other data from and the security cameras of the following entities:

- Airport airlines, concessionaires, food and beverage operators, and rental car agency tenants. ("Tenants")

In line with its mission, the Department shall use security cameras only for the following authorized purposes:

Authorized Use(s):

1. Reviewing camera footage in the event of an incident.
2. Approving Tenant's disclosure of digital recordings and other data from its security camera system.

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.

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

Tenants' proprietary lease space.

Surveillance Oversight Review Dates
COIT Review: TBD
Board of Supervisors Review: TBD

Technology Details

The following a is product description:

There are various types of camera technology used by the Tenants. During the application process Tenants are required to provide the Airport with camera make, model, and technical specifications as well as their security plan. Tenants are responsible for their hardware and the Airport does not maintain an inventory except as noted on the Tenants application form. Tenants are required to update the Airport on their inventory as change occurs.

A. How It Works

Subject to the Airport Rules and Regulations, Tenants are allowed to install their own security cameras in their proprietary lease space. Tenants use these cameras to record live video within their proprietary lease space.

Handling or storage of data collected from or processed by Tenant's security camera system is solely the responsibility of Tenant.

Data Retention:	Department may store and retain PII data shared by Tenant/Contractor 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: - One year, consistent with the Department's Data Retention Policy and state law; longer if necessary for an ongoing investigation or in anticipation of litigation. 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): - If necessary for an ongoing investigation or in anticipation of litigation. Data may be stored in the following location: x Local storage (e.g., local server, storage area network (SAN), network-attached storage (NAS), backup tapes, etc.) ▪ Department of Technology Data Center ▪ 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:

- 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.

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 Tenant'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 Tenants 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:

Airport's use of recordings and data from third party security cameras is restricted to the identified Authorized Use Cases. Tenant's disclosure of recordings and data from its own cameras is subject to the Airport Rules and Regulations and policies that restrict use of CCTV to the approved use in the Tenant Application. Tenants are required to report to the Airport any changes or modifications to video monitoring and/or recording device use prior to executing the changes or modifications.

Tenants are required to obtain Airport's written authorization prior to the release of any video monitoring and/or recording device footage from Tenants cameras/devices. In appropriate cases, Airport may also request review and a determination of whether the footage may be disclosed from the Transportation Security Administration (TSA).

Further, Tenants approved camera use are audited as part of the Airport weekly and monthly audit of Tenants space. Airlines are also audited on an annual basis.

C. Fiscal Analysis of Costs and Benefits

The Department's use of surveillance cameras yields the following business and operations benefits [Please customize chart below according to department circumstances]:

Benefit		**Description**
X	Financial Savings	Tenants security Camera Systems will save on building or patrol officers.
X	Time Savings	Tenants security Camera Systems will run 24/7/365, thus decreasing or eliminating building or patrol officer supervision.
X	Staff Safety	Tenants security cameras help identify violations 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 recommended to be set to high resolution.

Number of FTE (new & existing)	Tenants cost to implement and support security cameras are not reported to Airport. Cost noted in this table reflect the Airport's cost for the approval and audit of Tenants use of the technology. .45	
Classification	1. 9212 – Aviation Security Analyst – 10% 2. 9220 – Aviation Security Supervisor – 10% 3. 0931 – Manager Aviation Security & Regulatory Compliance – 10% 4. 0933 - Director, Security, Emergency Management & Communications – 10% 5. 0943 - Managing Director, Safety, Security and Airside Services – 5% 6. 0955 – Chief Operating Officer – 5%	
	Annual Cost	***One-Time Cost***
Software		
Hardware/Equipment		
Professional Services		
Training		
Other – Salaries & Benefits	$ 108,000	
Total Cost	**$ 108,000**	

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

Annual Operating funds. Tenants fund their use and maintenance of the surveillance technology.

COMPARISON TO OTHER JURISDICTIONS

Third Party Security Cameras 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):

Tenants proprietary space across the Airport property.

City & County of San Francisco
London N. Breed, Mayor

Office of the City Administrator
Carmen Chu, City Administrator
Jillian Johnson, Director
Committee on Information Technology

To: Angela Calvillo
Clerk of Board of Supervisors

From: Carmen Chu, City Administrator
Jillian Johnson, Director, Committee of Information Technology

Date: July 18, 2022

Subject: Legislation introduced for Approval of Surveillance Technology Policies for Multiple City Departments

---

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 Surveillance Technology Policies and Impact Reports for the following technologies to the Board of Supervisors for their review:

- Automatic License Plate Readers (ALPR)
- Biometric Processing Software and/or System
- Body-Worn Cameras
- People-Counting Camera
- Security Cameras
- Third-Party Security Cameras
- Location Management System
- Computer Management System
- Social Media Monitoring Software

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 year to engage the public in developing these Surveillance Technology policies. All details of these discussions are available at sf.gov/COIT.

The following sections provide more detail on the departments seeking Board of Supervisors approval for their surveillance technology policies, and the COIT recommended course of action.

If you have questions on the review process, please direct questions to Jillian Johnson, Director of the Committee on Information Technology (COIT).

Automatic License Plate Readers (ALPR)

Department	Authorized Uses
Municipal Transportation Agency (MTA)	1. Enforce parking restrictions and laws. 2. Transit Only Lane Enforcement (TOLE). 3. Link individual vehicles to their times of entry/exit into City-owned parking garages and lots to accurately calculate parking fees. 4. Identify vehicles that are the subject of an active investigation by the SFPD (e.g., vehicles included on "hot lists" generated by the SFPD –see Appendix B & C of MTA policy, and page 8 of SFPD ALPR Policy). 5. Analysis of and reporting on parking and curb usage.

ALPR Public Meeting Dates:

Date	Meeting
August 27, 2021	Privacy and Surveillance Advisory Board (PSAB)
September 24, 2021	Privacy and Surveillance Advisory Board (PSAB)
October 21, 2021	Committee on Information Technology (COIT)

COIT Recommendation:

COIT recommends the Board of Supervisors adopt the ALPR Surveillance Technology Policy for the MTA.

Biometric Processing Software or System

Department	Authorized Uses
Juvenile Probation	- Youth are only placed on continuous alcohol monitoring (CAM) in San Francisco with a court order. The Court may order a youth to be placed on CAM as a condition of probation, if the Court determines that is in the interest of public safety and the youth's wellbeing. CAM data is analyzed on a daily basis by probation officers to ensure compliance with the Court's order.

Biometric Processing Software/System Public Meeting Dates:

Date	Meeting
January 14, 2022	Privacy and Surveillance Advisory Board (PSAB)
February 17, 2022	Committee on Information Technology (COIT)

COIT Recommendation:

COIT recommends the Board of Supervisors adopt the Biometric Processing System Surveillance Technology Policy for Juvenile Probation.

Body-Worn Cameras

Departments	Authorized Uses
Fire	- Use by Public Information Officer (PIO) at large incidents to capture video of surroundings and the totality of the incident
Recreation and Parks	- Recording video and audio footage in the event of an incident. Incidents can be: o Actual or potential criminal conduct o Situation when a Park Ranger reasonably believes recordings of evidentiary value may be obtained o Calls for service involving a crime where the recording may aid in the apprehension/ prosecution of a suspect - Providing recording to law enforcement or other authorized persons upon request.

Body-Worn Cameras Public Meeting Dates:

Date	Meeting	Departments
September 10, 2021	PSAB	Fire
September 24, 2021	PSAB	Recreation and Parks
October 21, 2021	COIT	Fire, Recreation and Parks

COIT Recommendation:

COIT recommends the Board of Supervisors adopt the Body-Worn Camera Surveillance Technology Policies for the Fire Department and the Recreation and Parks Department.

People-Counting Cameras

Departments	Authorized Uses
Library	- To tally the entry and exit of Library visitors at all 28 public facilities. - To track usage of meeting rooms, elevators and restrooms for purposes of resource allocation.

People-Counting Cameras Public Meeting Dates:

Date	Meeting
January 28, 2022	Privacy and Surveillance Advisory Board (PSAB)
March 11, 2022	Privacy and Surveillance Advisory Board (PSAB)
April 21, 2022	Committee on Information Technology (COIT)

COIT Recommendation:

COIT recommends the Board of Supervisors adopt the People-Counting Camera Surveillance Technology policy for the Library.

Security Cameras

Departments	Authorized Uses
Elections	- Live monitoring of voting center lines. - Live monitoring of Department staff during elections operations. - Recording of video and images of Department staff during elections operations. - Reviewing camera footage of Department staff in the event of an incident. - Sharing camera footage of Department staff with the public to promote transparency into elections operations.

Security Cameras Public Meeting Dates:

Date	Meeting
October 22, 2021	Privacy and Surveillance Advisory Board (PSAB)
November 18, 2021	Committee on Information Technology (COIT)

COIT Recommendation:

COIT recommends the Board of Supervisors adopt the Security Camera Surveillance Technology Policy for the Department of Elections.

Third-Party Security Cameras

Departments	Authorized Uses
Airport (AIR)	- Reviewing camera footage in the event of an incident. - Approving Tenant's disclosure of digital recordings and other data from its security camera system.
Municipal Transportation Agency (MTA)	- Review recording of on-board incidents based upon complaints received from the public and at appeals hearing in response to a fine, suspension or response to fine revocation. - Review video data in response to complaints from the public to ensure compliance by taxi cab companies and other taxi permittees with requirements and conditions under Article 1100 (Regulation of Motor Vehicles for Hire) of Division II of the SF Transportation Code. - Review video data to confirm taxi cab companies and other taxi permittees complete rides paid for with public funds before paying the companies for those rides. For example, under its wheelchair program taxi incentive, the Department reviews video data from the technology to confirm that taxi cab drivers pick up individuals with certain disabilities before paying drivers for those rides, which are funded under various paratransit programs. - Review video to investigate criminal acts involving taxi drivers or riders. - Review video data to investigate accidents involving a taxi cab.
War Memorial (WAR)	- Live monitoring internal office space and public area of Davies Symphony Hall. - Reviewing camera footage provided by Tenant/Contractor upon request in the event of an incident.

Third-Party Security Cameras Public Meeting Dates:

Date	Meeting	Departments
October 22, 2021	PSAB	WAR
January 14, 2022	PSAB	WAR, AIR
January 28, 2022	PSAB	AIR
February 17, 2022	COIT	AIR
March 11, 2022	PSAB	MTA
April 21, 2022	COIT	WAR, MTA

COIT Recommendation:

COIT recommends the Board of Supervisors adopt the Third-Party Security Camera Surveillance Technology Policies for the Airport, Municipal Transportation Agency, and War Memorial.

Location Management System

Department	Authorized Uses
Juvenile Probation	- Youth are only placed on electronic monitoring in San Francisco with a court order. The Court may order a youth to be placed on electronic monitoring as an alternative to detention. - Electronic monitoring (EM) may also be added as a condition of probation if additional supervision is warranted. EM data is analyzed on a daily basis by probation officers to ensure compliance with: - Court ordered curfews o Inclusion zones: addresses/areas where the minor has approval to be present, for example their home, school, work. o Exclusion zones: addresses/areas where the minor should not be present, including Stay Away orders o Schedules: To monitor school attendance, program participation, work.
Recreation and Parks	- Confirm that the person who reserved the booking for a tennis court is at the location at the reserved time. - Utilize data to determine if there are any reservation holders who are violating booking policies because they are not showing up at the reserved time.

Location Management System Public Meeting Dates:

Date	Meeting	Department
October 22, 2021	PSAB	Juvenile Probation
November 18, 2021	COIT	Juvenile Probation
March 11, 2022	PSAB	Recreation and Parks
May 27, 2022	PSAB	Recreation and Parks
June 16, 2022	COIT	Recreation and Parks

COIT Recommendation:

COIT recommends the Board of Supervisors adopt the Location Management Surveillance Technology Policies for Juvenile Probation and the Recreation and Parks Department.

Social Media Monitoring Software

Department	Authorized Uses
Library	- Plan and execute more effective and strategic campaigns across social media platforms. - Schedule multiple social media posts in advance. - Create and monitor multiple streams of content across various platforms. - Maintain active social media presence that is automated, specifically on weekends when staff is off. - Ensure consistency of messaging across all social media platforms. - Track post performance and analyze trends to improve content and strategy. - Create reports.

Social Media Monitoring Software Public Meeting Dates:

Date	Meeting
August 27, 2021	Privacy and Surveillance Advisory Board (PSAB)
October 21, 2021	Committee on Information Technology (COIT)

COIT Recommendation:

COIT recommends the Board of Supervisors adopt the Social Media Monitoring Software Surveillance Technology Policy for the Library.

Computer Management System

Departments	Authorized Uses
Library	- The authorized use case for the TBS Computer Time and Print Management tool is to provide time-delimited public access to library computers and allow the public to print, copy, scan and fax documents, as well as track usage of computers and print resources throughout the library's 28 facilities for purposes of resource allocation and management.The five specific components within TBS Computer Time and Print Management are as follows: • MyPC: Manages patron access to library computers and regulates amount of time each patron can use computers • EZ Booking: Allows patrons to manage their reservations in MyPC, schedule public computer use, etc. • Papercut/EPrintIt: Manages public print jobs sent from library computers and patrons' personal devices, allowing them to print their documents on library printers. Also allows select library staff members, in the interest of customer service and support, to retrieve and print jobs submitted to the system by users during the 24-hour period in which documents are retrievable. This allows staff to print jobs when printers fail, when print jobs do not meet user expectations, to intermediate when users are struggling with technology, etc. • Allows library patrons to scan, manipulate, manage, print, email, fax and save documents using either the library's flat-bed or document feeder scanners. • Payment Kiosk: Allows patrons to pay for print and copy jobs processed through Papercut/EPrintIt and/or ScanEZ.

Security Cameras Public Meeting Dates:

Date	Meeting
May 27, 2022	Privacy and Surveillance Advisory Board (PSAB)

June 16, 2022	Committee on Information Technology (COIT)

COIT Recommendation:

COIT recommends the Board of Supervisors adopt the Computer Management System Surveillance Technology Policy for the Library.

Surveillance Impact Report

Department of Elections
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 San Francisco Department of Elections is to provide access to election-related services and voting and to conduct elections that are free, fair, and functional.

In line with its mission, the Department shall use cameras only for the following authorized purposes:

Authorized Use(s):

1. Live monitoring of voting center lines.
2. Live monitoring of Department staff during elections operations.
3. Recording of video and images of Department staff during elections operations.
4. Reviewing camera footage of Department staff in the event of an incident.
5. Sharing camera footage of Department staff with the public to promote transparency into elections operations.

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:

1. Department of Elections in City Hall
2. Department's Warehouse at Pier 31

Surveillance Oversight Review Dates

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

Technology Details

The following is product description:

The Nest Cam Security Camera lets you keep an eye on what matters most to you, even when you're far from home. Take advantage of 24/7 live video streaming to your mobile device or tablet. Get alerts if something happens and watch footage live in 1080p HD.

A. How It Works

To function, streaming cameras capture video at Department of Elections office in City Hall and Warehouse locations. Stream from the City Hall Voting Center is private and is monitored only from inside the Elections office. Streams of ballot processing are streamed publicly on the internet and can be found on the Department's website. Video from streams is stored for 10 days prior to automatic deletion.

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:

X	Education	Allows the public to watch and learn about the election process in San Francisco.
☐	Community Development	
X	Health	Protect safety of staff, patrons, and facilities while promoting an open and welcoming environment.
☐	Environment	
☐	Criminal Justice	
☐	Jobs	

☐	Housing	
X	Other	Transparency is a key component of free, fair, and functional elections. To that end, the Department of Elections welcomes members of the public to observe its operations and offer feedback.

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: Recordings can only be accessed by 1092-1095 IS Administrator Series, 1840-1844 Management Assistant series, 1115 Director, 0951-0955 Deputy Director series. Internal streams of voting line are not posted publicly.

Technical Safeguards: Access to recordings is password protected. Recordings are automatically deleted from Google servers after 10 days.

Physical Safeguards: Cameras are located only at secured Department of Elections offices at City Hall and Pier 31.

The Department of Elections strives to mitigate all potential civil rights impacts through responsible technology and associated data use policies and procedures, and intends to use Streaming Cameras and their associated data exclusively for aforementioned authorized use cases. All other uses, including surveillance of San Francisco residents or groups, are expressly prohibited.

Streaming Cameras are used to monitor line of voters to determine if additional personnel are needed at the City Hall Voting Center to ensure efficient service. Live streams of ballot processing activities provide the public with transparent and accessible opportunities to observe election processes.

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	Streaming cameras allow us to provide election observation activities while minimizing deployment of personnel to staff each observation area.
X	Time Savings	Streaming cameras enable monitoring of election processes happening in different areas of the city at the same time from a central location.
X	Staff Safety	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	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 is Number of FTE (new & existing)	2 existing employees, Total expected staff hours (all): 10 hrs/election *8 hrs x 1 election x $61/hr:* ***$488/election*** *2 hrs x 1 election x $51/hr:* ***$102/election*** ***Total: $590/election***	
Classification	IS Admin (1092) & Elections Clerk (1403)	
	Annual Cost	***One-Time Cost***
Software		
Hardware/Equipment		21 cameras x $200: **$4,200**/one-time cost
Professional Services		
Training		
Other	Subscription plan for 10 day recording retention: **$2,100**	
Total Cost	***$2,690/yr (1 election), $3,280/yr (2 elections).***	***$4,200***
2.1 Please disclose any current or potential sources of funding (e.g. potential sources = prospective grant recipients, etc.). SIR, ASR		

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

Annual Operating Budget.

COMPARISON TO OTHER JURISDICTIONS

The Nest Cam Security Cameras 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).

Surveillance Technology Policy

Security Cameras
Department of Elections

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 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 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 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 Cameras to the following authorized use cases and requirements listed in this Policy.

Authorized Use(s):

1. Live monitoring of voting center lines.
2. Live monitoring of Department staff during elections operations.
3. Recording of video and images of Department staff during elections operations.
4. Reviewing camera footage of Department staff in the event of an incident.
5. Sharing camera footage of Department staff with the public to promote transparency into elections operations.

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.

Surveillance Oversight Review Dates
COIT Review: November 21, 2021
Board of Supervisors Review: Upcoming

BUSINESS JUSTIFICATION

In support of Department operations, Security Cameras promise to help with:

X	Education	Allows the public to watch and learn about the election process in San Francisco.
▪	Community Development	
X	Health	Protect safety of staff, patrons, and facilities while promoting an open and welcoming environment.
▪	Environment	
▪	Criminal Justice	
▪	Jobs	
▪	Housing	
X	Other	Transparency is a key component of free, fair, and functional elections. To that end, the Department of Elections welcomes members of the public to observe its operations and offer feedback.

In addition, the following benefits are obtained:

Benefit		Description
X	Financial Savings	Streaming cameras allow us to provide election observation activities while minimizing deployment of personnel to staff each observation area.
X	Time Savings	Streaming cameras enable monitoring of election processes happening in different areas of the city at the same time from a central location.
X	Staff Safety	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	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	Cameras will enhance transparency of elections operations to the public.

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 are available to the public via a live-stream video feed, for the duration of the election activities which include voting and vote tallying. Live video footage is made available to the public to provide transparency surrounding city and county elections. Recorded footage is restricted to specific trained personnel. Recorded footage is accessed only in response to an incident and is automatically deleted 10 days after the recording is made. 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 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. Because this footage is streamed live

to the public, it is possible that viewers of the footage will retain, share, or and use the footage in ways that do not comply with this policy.

Each department that believes another agency or department receives or may receive data collected from its use of 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 Camera footage with the following entities:

A. Internal Data Sharing:

In the event of an incident, 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:

- On request following an incident.

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:

- Camera data will be stored for a minimum of one (1) year to be available 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.
    - Google Nest Cam Indoor security cameras. Deployed during Election cycle at Department of Elections in City Hall and Department's Warehouse at Pier 31.
2. The specific categories and titles of individuals who are authorized by the Department to access or use the collected information
    - Streams of Election processes are available to the public.
    - Streams used for line management at City Hall Vote Center is accessible by all Department of Elections staff.
    - Recordings are accessible to the following authorized staff of the Department:
        - 1092-1095 IS Administrator Series
        - 1840-1844 Management Assistant series
        - 1115 Director
        - 0951-0955 Deputy Director 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 at San Francisco Department of Elections City Hall 1 Dr. Carlton B. Goodlett Place, Room 48 San Francisco, CA 94102 415-554-4375, SFVote@sfgov.org, Contact form: https://sfelections.org/sfvote/
    - The Department responds to all inquiries within 10 days of receipt, regardless of method of submission. During the election cycle, all inquiries are logged in a Public Inquiry Tracking Application, assigned to a division or staff member, and tracked to completion.
4. Specific details on where data will be stored (local, DT, SaaS, Cloud Storage) including name of vendor and retention period.
    - Recordings are automatically saved to Google's Cloud for a period of 10 days as part of the Nest Cam subscription plan. After 10 days, the recordings are deleted.
5. Questions & Concerns

Surveillance Impact Report

Spotery - web application used for tennis reservations
Recreation and Parks 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 Spotery - web application used for tennis reservations.

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 Spotery to allow for equitable access to our recreational sites.

The Department shall use Spotery only for the following authorized purposes:

- To confirm that the person who reserved the booking for a tennis court is at the location at the reserved time
- To utilize data to determine if there are any reservation holders who are violating booking policies because they are not showing up at the reserved time. Data can be accessed on the web application or as a report delivered by Spotery.

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

Department technology is located as an app through Spotery. The reservation holder can use the check in button (sent by the reservation system) within 15 minutes before or after the reservation time. Spotery checks the location of the reservation holder to ensure that they are within 0.1 miles of the tennis court reserved. If not, the check in process cannot be completed.

Technology Details

The following is a product description of Spotery:

Spotery's core business is a marketplace for facility rentals. San Francisco Recreation & Park Department (SFRPD) Permits & Reservations worked with Spotery to custom build a reservation platform for tennis courts so that these could be fairly allocated (please see: https://www.spotery.com/).

A. How It Works

To function, Spotery works as reservation holder to allow a person to book a tennis court up to seven days in advance.

Surveillance Oversight Review Dates
COIT Review: June 16, 2022
Board of Supervisors Review: TBD

24 hours prior to the reservation, a reminder email is sent to the reservation holder. The reminder email contains a check-in button. The reservation holder can use the check in button within 15 minutes before or after the reservation time.

Spotery checks the location of the reservation holder to ensure that they are within .1 miles of the tennis court. Spotery needs access to the reservation holder's location so "Enable Location Services" must be turned on.

All data processed by Spotery will be handled by an outside provider or third-party vendor on an ongoing basis. Specifically, data will be handled by Social Solutions 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:

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 Spotery has the following benefits for the residents of the City and County of San Francisco:

X Health - Residents are able to book reservations for tennis courts which allow for recreational and physical activity.

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 Recreation and Park Department strives to mitigate all potential civil rights impacts through responsible technology and associated data use policies and procedures. The Department intends to use the Spotery GPS check in and associated data exclusively for the authorized uses cases. All other uses, including surveillance of San Francisco residents or groups, are expressly prohibited.

  The administrative, technical and physical safeguards are described below.

- Administrative Safeguards: Only the Chief Information Officer (0941) and the Director of Property, Permits and Reservation (0953) or designee - Administrative Analysts (1820 series) will have logins to the Spotery web app to access the data.
- Technical Safeguards: Only the Chief Information Officer (0941) and the Director of Property, Permits and Reservation (0953) or designee - Administrative Analysts (1820 series) will have logins to the Spotery web app to access the data. Data is encrypted and sent via SSL.
- Physical Safeguards: Data is securely stored by Spotery in the cloud.

C. Fiscal Analysis of Costs and Benefits

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

X Time Savings, Staff do not need to review and research anecdotal evidence about reservation holders not utilizing the court for the reserved time.

The fiscal cost, such as initial purchase, personnel and other ongoing costs, include:

- Number of FTE (new & existing): 1 FTE - Senior Administrative Analyst (1823) - 25%
- The annual costs are:
    - Total Salary & Fringe: $42k Based on: 1823 Salary (127k) * Fringe (.33) * % Time Spent (.25)
    - Software: $15k for all functionality offered by Spotery (include the GPS Check in feature)
    - Hardware/ Equipment: 0
    - Professional Services: 0
    - Training: 0
    - Other: 0

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

COMPARISON TO OTHER JURISDICTIONS

Spotery is currently utilized by other governmental entities for similar purposes.

Surveillance Technology Policy

Body-Worn Cameras
Recreation and Parks

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 Body-Worn Cameras 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 Body-Worn Cameras 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 Body-Worn Cameras, 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 Body-Worn Cameras technology for the Department is limited to the following use cases and is subject to the requirements listed in this Policy.

Authorized Use(s):

- Recording video and audio footage in the event of an incident. Incidents can be:
  - Actual or potential criminal conduct
  - Situation when a Park Ranger reasonably believes recordings of evidentiary value may be requested
  - Calls for service involving a crime where the recording may aid in the apprehension/ prosecution of a suspect
- Providing recording to law enforcement or other authorized persons upon request.

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

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

In line with its mission, the Department uses body worn cameras to protect the public and our staff in our parks, playgrounds and at special events. The Department can review footage for improvements in response or for training opportunities.

In addition, Body-Worn Cameras promises to benefit residents in the following ways:

- Public safety - Protect safety of residents while promoting an open, safe and welcoming environment
- Criminal justice - Providing recording to law enforcement or other authorized persons upon request.

Body-Worn Cameras will benefit the department in the following ways:

- Staff Safety - Ensure more accountability of actions of staff
- Financial and Time Savings - Recording available so no need to do individual assessment for any incidents

To achieve its intended purpose, a Body-Worn Camera (hereinafter referred to as "surveillance technology") is a device worn by a law enforcement officer that makes an electronic audio and video recording of activities that take place during any law enforcement action. In order to function, the Park Ranger turns the body worn camera on and off. Once a Park Rangers activates the body worn camera, he/she must make every reasonable effort to have the device remain on until the incident has concluded. Park Rangers download the recordings which are saved on Evidence.com.

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:

Data Type	Data Format	Data Classification
- Facial images, - voice audio - location - vehicle license plate number - Additionally, Park Rangers may request personal information (e.g. name) post the incident.	MOV, AVI	Level 2

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):

- Prior to accessing or using data, authorized individuals receive training in system access and operation, and instruction regarding authorized and prohibited uses.
- Access to recorded footage is restricted to the Chief Park Ranger or designee. Recorded footage is accessed only in response to an incident.

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:

- Chief Park Rangers (0951)
- Lieutenant Park Ranger (8210 - Lead)

B. Members of the public, including criminal defendants

The Recreation and Parks 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:

- Access limited only to Chief Park Ranger or designee. Without training or appropriate security levels in software, recordings cannot be accessed.

Data Sharing: The Recreation and Parks Department will endeavor to ensure that other agencies or departments that may receive data collected by Recreation and Parks's Body-Worn Cameras 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.

The Recreation and Parks 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 Recreation and Parks 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.

The Recreation and Parks 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:

Data Type	Data Recipient
Recordings from body worn cameras	Police, Sheriff, City Attorney, District Attorney, and Public Defender

Data sharing occurs at the following frequency:

- When requested, pursuant to a subpoena.

B. External Data Sharing

Department shares the following data with the recipients:

Data Type	Data Recipient
Recordings from body worn cameras	Outside law enforcement

Data sharing occurs at the following frequency:

- When requested.

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

- The Chief Park Ranger will be responsible for enforcing the Surveillance Technology policy through its incorporation into the overall Department Policy for Body Worn Cameras.

Before data sharing with any recipient, 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.
- Ensure shared data will be done in a cost-efficient manner and exported in a clean, machine-readable format.
- Redact names, scrub faces, and ensure all PII is removed in accordance with the department's data policies.

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:

Data Retention Period	Data Retention Justification
Body worn camera recordings will be stored for a minimum of one (1) year.	This retention period allows for ample time for security staff to review footage related to security incidents and/or external requests for records.

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):

- If data is associated with an incident, it may be kept for longer than the standard retention period:
  - Use of force - not deleted
  - Investigations - until case closure

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

Data will be stored in the following location:

- Local Storage
- Software as a Service Product

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

Practices:

- Evidence.com auto-deletes after 1 year.

Processes and Applications:

- Evidence.com has a feature that allows for redaction/ de-identification. This will be performed by the Lieutenant 8210 -Lead.

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 on Evidence.com on how to view and download recordings is required.
- Evidence.com is the storage location for footage captured by Axon Body Worn Cameras.

COMPLIANCE

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

- The Chief Park Ranger or designee will be responsible for enforcing the Surveillance Technology policy through its incorporation into the overall Department Policy for Body Worn Cameras.

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

- Chief Park Ranger (0951) or designee - Lieutenant (8210 - Lead).

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.
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

For the Public:

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

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

- 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.

For 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 Technology Policy

Tenant Security Cameras
SAN FRANCISCO INTERNATIONAL AIRPORT ("SFO", "Airport", OR "Department")

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, this Surveillance Technology Policy aims to ensure the responsible use of Security Camera Systems by airlines, concessionaires, food and beverage operators, rental car agency tenants (hereinafter Tenants) at the San Francisco Internal Airport ("SFO", "Airport", OR "Department") as well as any associated data to which Department is privy, and the protection of City and County of San Francisco residents' civil rights and liberties.

PURPOSE AND SCOPE

The Department's mission is to provide an exceptional airport in service to our communities.

The Surveillance Technology Policy ("Policy") defines the manner in which the Tenant Security Camera System (fixed or mobile) will be used to support Department operations.

This Policy applies to all Department personnel, and other agents acting on the Department's behalf that access or use digital recordings or other data from Tenants Security Camera Systems, including employees, contractors, and volunteers.

POLICY STATEMENT

This policy applies to the Airport's access to and use of digital recordings and other data from the security cameras of the following entities:

- Airport Tenants

The Airport limits its use of recordings and other data from Tenant security cameras to the following authorized use cases and requirements listed in this Policy only.

Authorized Use(s):

1. Reviewing camera footage in the event of an incident.
2. Approving Tenant's disclosure of digital recordings and other data from its security camera system.

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

Department's processing of personal data revealing legally protected categories, including 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: February 17, 2022
Board of Supervisors Review: Upcoming

BUSINESS JUSTIFICATION

Access to and use of digital recordings and other data from Tenant Security cameras will benefit the Department in the following ways.:

	▪ 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.
	▪ Jobs	
	▪ Housing	

In addition, the following benefits are obtained:

Benefit		Description
X	Financial Savings	Equipment is owned and operated by non-city entity.
X	Time Savings	Tenant/Contractor Security Camera Systems operate 24/7/365, thus decreasing or eliminating building or patrol officer supervision. Additionally, full-time staffing is not required to subsequently review footage of security incidents.
X	Staff Safety	Tenant/Contractor Security cameras help identify violations of 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.

- 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.

Data Collection:

Department shall only collect the data that is necessary to execute the authorized use cases. All surveillance technology data shared with Department by a Tenant/Contractor, 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

Access:

The Airport does not have direct system access to, or control over, the operation of Tenant's technology. Recorded footage is accessed only in response to an incident.

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:

- 9212 – Aviation Security Analyst
- 9220 – Aviation Security Supervisor
- 0931 – Manager Aviation Security & Regulatory Compliance.
- 0933 - Director, Security, Emergency Management & Communications
- 0943 - Managing Director, Safety, Security and Airside Services
- 0955 – Chief Operating Officer

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

- Tenants/Vendors are responsible for the maintenance of the surveillance technology systems.

B. Members of the public

	Data collected by surveillance technology will not be made generally available to members of the public. Collected data that is classified as Level 1-Public data may be made available for public access or release via DataSF's Open Data portal. Open Data has a Public Domain Dedication and License, and makes no warranties on the information provided. Once public on Open Data, data can be freely shared, modified, and used for any purpose without any restrictions. Any damages resulting from use of public data are disclaimed Members of the public may also request access by submission of a request pursuant to San Francisco's Sunshine Ordinance. No record shall be withheld from disclosure in its entirety, unless all information contained in it is exempt from disclosure under express provisions of the California Public Records Act or some other statute.
Data Security:	Department shall secure any PII received from Tenant (or shared by Tenant) against unauthorized or unlawful processing or disclosure; unwarranted access, manipulation or misuse; and accidental loss, destruction, or damage. Surveillance technology data collected and retained by the Department shall be protected by the safeguards appropriate for its classification level(s) as defined by the National Institute of Standards and Technology (NIST) security framework 800-53, or equivalent requirements from other major cybersecurity framework selected by the Department. Departments shall, at minimum, apply the following safeguards to protect surveillance technology information received from Tenant 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:	Tenant/Contractor is the sole owner and custodian of its Surveillance Technology data. Tenant/Contractor may share such data with the Department, but pursuant

to Airport Rule & Regulation 7.5, must seek prior authorization from Department for release to other third parties.

The Department will endeavor to ensure that other agencies or departments that may receive data collected by Tenant's security cameras will act in conformity with this Surveillance Technology Policy.

In the event of a substantive amendment to Rule 7.5, the Department must resubmit this Policy for approval in accordance with Chapter 19B.

Data is shared by Tenant/Contractor with the Department as needed.

A. Internal Data Sharing

In the event of an incident, Security Camera images may be shared with the following agencies:

- Within the Department on a need-to-know basis
- Police
- City Attorney
- District Attorney
- Sheriff

Data sharing occurs at the following frequency:

- As needed.

B. External Data Sharing:

- Other law enforcement agencies
- Member(s) of the public, if required under the California Public Records Act or the Sunshine Ordinance

Data sharing occurs at the following frequency:

- As needed.

Data Retention:	Department may store and retain PII data shared by Tenant/Contractor 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: - One year, consistent with the Department's Data Retention Policy and state law; longer if necessary for an ongoing investigation or in anticipation of litigation. 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): - If necessary for an ongoing investigation or in anticipation of litigation. Data may be stored in the following location: x Local storage (e.g., local server, storage area network (SAN), network-attached storage (NAS), backup tapes, etc.) ▪ Department of Technology Data Center ▪ 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 on behalf of Department 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 memoranda of understanding with the labor organization representing employees of the City and County of San Francisco.

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.

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

- 9212 – Aviation Security Analyst
- 9220 – Aviation Security Supervisor
- 0931 – Manager Aviation Security & Regulatory Compliance.

- 0933 - Director, Security, Emergency Management & Communications
- 0943 - Managing Director, Safety, Security and Airside Services
- 0955 – Chief Operating Officer

DEFINITIONS	
Tenant/Contractor	Non-City Entity that owns and operates security cameras and shares security camera footage with a City department.
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."

QUESTIONS & CONCERNS

Public:

Complaints, concerns or questions can be submitted to:

- *Airport Guest Services - https://www.flysfo.com/contact-sfo(Contact SFO)*
- *Airport public email, phone, or website --https://www.flysfo.com/contact-sfo or*
- *Airport Commission meetings -- https://www.flysfo.com/about-sfo/airport-commission/addressing-the-commission*

Department shall acknowledge and respond to complaints and concerns in a timely and organized response. To do so, Department shall follow its process where questions and complaints are tracked by Airport Guest Services and response are promptly responded to by the Director of Guest Experience and/or his staff.

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.

Attachment 1: Appendix A: Rules and Regulations, Rule 7.5 (2022 edition)

RULE 7.0

AIRPORT SECURITY

7.5 VIDEO MONITORING AND RECORDING DEVICES / ACCESS TO AIRPORT CLOSED CIRCUIT TELEVISION (CCTV) SYSTEM

(A) Installation or Removal of Video Monitoring and Other Recording Devices

No video monitoring or other recording devices may be installed or removed by any Airport tenant or contractor in or around the Airport premises without prior written authorization from the Aviation Security unit. To obtain authorization for CCTV camera installation or removal, tenants and contractors must submit an application, specifying the following:

- Field-of View (FOV) screenshots
- Video monitoring/recording device model and specifications
- Recording system and retention time
- Camera layout drawing
- Security infrastructure and plan to prevent unauthorized access

The use of Pan-Tilt-Zoom (PTZ) security cameras by tenants and contractors in any Restricted area is strictly prohibited and no video monitoring and/or recording device may be installed or focused in a manner that depicts/records security checkpoints, or doors that provide access to any area on Airport premises that, in the sole and exclusive discretion of the Director or his designee, is deemed to present a potential risk to Airport security. All subsequent changes or modifications to tenant and contractor video monitoring and/or recording device use must be submitted to Aviation Security in writing and approved prior to executing modifications.

(B) Remote Viewing and Authorization Access

No video monitoring and/or recording device data may be streamed or otherwise transmitted on a wireless network unless the wireless network is equipped with WPA2 security. Real-time access to all footage must be available to the Aviation Security unit at all times. No tenant or contractor shall release any video monitoring and/or recording device footage from cameras/devices without prior written authorization from the Aviation Security unit and, if deemed appropriate, the TSA. Remote access to video monitoring and/or recording devices in secure areas will not be permitted unless explicitly authorized by the Director.

All forms of video footage, whether real-time or stored, must be password protected. Passwords must comply with the Airport's Password policy.

(C) Inventory of Video Monitoring and Other Recording Devices

All tenants and contractors shall provide Aviation Security with an inventory of existing video monitoring and/or recording devices and security plans, including all of the following:

- Device manufacturer, model and specifications
- Field-of-view
- Data retention time
- Placement of video monitoring and/or recording devices

- Remote access usage
- Written security plan detailing how unauthorized access will be prevented

(C) Airport Closed-Circuit Television (CCTV) Access Policy

The Airport owns and operates the CCTV system. This system contains information that is confidential, which may be sensitive secure, affect personal privacy, or both. A tenant or contractor may access Airport CCTV feeds only through Airport equipment upon request to Airport Aviation Security (AVSEC). If access is granted, the tenant or contractor shall designate individual employees to view CCTV feeds for the performance of official job duties, on a need-to-know basis only. Any such individual must hold an Airport ID badge and execute a Non-Disclosure Acknowledgement as a condition of authorized access. (ASB 20-02, ASB 20-06)