File No. 240469 **Committee Item No.** 7
Board Item No. 22

COMMITTEE/BOARD OF SUPERVISORS

AGENDA PACKET CONTENTS LIST

Committee: Rules Committee **Date** June 17, 2024

Board of Supervisors Meeting **Date** June 25, 2024

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

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

X	☐	Airport Resolution No. 23-0103
☐	☐	
☐	☐	
☐	☐	
☐	☐	
☐	☐	
☐	☐	
☐	☐	
☐	☐	

Completed by: Victor Young **Date** June 14, 2024
Completed by: _____ **Date** _____

[Administrative Code - Amended Airport Surveillance Technology Policy]

Ordinance approving the amended Airport Surveillance Technology Policy governing the use of pre-security cameras.

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 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) Under Administrative Code Section 19B.2(b), the Board of Supervisors may approve a Surveillance Technology Policy ordinance under Section 19B.2(a) if: (1) the department seeking Board approval first submits to the Committee on Information Technology (COIT) a Surveillance Impact Report for the Surveillance Technology to be acquired or used; (2) based on the Surveillance Impact Report, COIT develops a Surveillance Technology Policy for the Surveillance Technology to be acquired or used; and (3) at a public meeting at which COIT considers the Surveillance Technology Policy, COIT recommends that the Board adopt, adopt with modification, or decline to adopt the Surveillance Technology Policy for the Surveillance Technology to be acquired or used.

(d) The Airport submitted an Amended Surveillance Technology Policy for the Airport Pre-Security Cameras to COIT. Between January 25, 2024 and February 15, 2024, COIT and its Privacy and Surveillance Advisory Board (PSAB) conducted two public hearings at which they considered Airport Surveillance Impact Reports and the Amended Surveillance Technology Policy for the Airport Pre-Security Cameras.

(e) On February 15, 2024, COIT voted to recommend the Amended Airport Pre-Security Cameras Policy to the Board for approval.

(f) The Amended Surveillance Technology Policy is available in Board File No. 240469. COIT recommended that the Board approve the Amended Surveillance Technology Policy.

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

Section 2. Pre-Security Camera Usage.

(a) The Airport currently possesses and uses Pre-Security Cameras.

(b) The Airport uses the Pre-Security Cameras for: (1) live monitoring; (2) recording of video and images; (3) reviewing camera footage in the event of an incident; and (4) providing video footage/images to law enforcement or other authorized persons following an incident or upon request.

Section 3. Findings and Approval of the Policy.

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

(b) The Board of Supervisors hereby approves the Amended Airport Pre-Security Cameras Policy.

Section 4. 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/ Andrew A. Angeles*
ANDREW A. ANGELES
Deputy City Attorney

n:\legana\as2024\2400376\01751779.docx

FILE NO. 240469

LEGISLATIVE DIGEST

[Administrative Code - Amended Airport Surveillance Technology Policy]

Ordinance approving the amended Airport Surveillance Technology Policy governing the use of pre-security cameras.

Background Information

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

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

Under Chapter 19B.2, a department seeking to use or acquire Surveillance Technology 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 January 2024, the Committee on Information Technology ("COIT") and its Privacy and Surveillance Advisory Board ("PSAB") subcommittee conducted multiple public hearings, at which COIT and its PSAB considered Airport Surveillance Impact Reports and the Amended Surveillance Technology Policy for Pre-Security Cameras.

Following those hearings, COIT approved the final draft of the Amended Surveillance Technology Policy for Pre-Security Cameras. The Amended Surveillance Technology Policy that COIT developed are detailed in Sections 2 and 3 of the proposed ordinance. The Surveillance Technology Policy is available in Board File No. _____. COIT recommended that the Board of Supervisors approve the Amended Surveillance Technology Policy in the proposed ordinance.

Committee on Information Technology

Office of the City Administrator

To: Members of the Board of Supervisors

From: Carmen Chu, City Administrator
Katharine Petrucione, Deputy City Administrator

Date: April 23, 2024

Subject: Legislation introduced to approve the amended Surveillance Technology Policy for the Airport's Security Cameras (including BART Video Streaming, Airport Shuttle Bus and AirTrain).

In compliance with Section 19B of the City and County of San Francisco's Administrative Code, the City Administrator's Office is pleased to submit the amended Surveillance Technology Policy for the Airport's Security Cameras (including BART Video Streaming, Airport Shuttle Bus and AirTrain).

To engage the public in discussion on the role of government surveillance, the Committee on Information Technology (COIT) and its subcommittee the Privacy and Surveillance Advisory Board (PSAB) held two public meetings for Airport's Security Cameras between January and February 2024 to review and approve the amended Policy. All details of these discussions are available at sf.gov/coit.

The following page provides greater detail on the review process for the Surveillance Technology Policy, and COIT's recommended course of action.

If you have questions on the review process please direct them to Jane Gong, Acting Director of the Committee on Information Technology (COIT).

Security Cameras

Department	**Authorized Uses**
Airport	1. Live monitoring. 2. Recording of video and images. 3. Reviewing camera footage in the event of an incident. 4. Providing video footage/images to law enforcement or other authorized persons following an incident or upon request.

Security Cameras Public Meeting Dates

Pre-Security Cameras	
Date	**Meeting**
January 25, 2024	Privacy and Surveillance Advisory Board (PSAB)
February 15, 2024	Committee on Information Technology (COIT)

COIT recommends the following action be taken on the policy:

- Approve the amended Security Cameras Surveillance Technology Policy for the Airport.

AIRPORT COMMISSION

CITY AND COUNTY OF SAN FRANCISCO

RESOLUTION NO. 23-0103

RESOLUTION AUTHORIZING THE AIRPORT TO SEEK BOARD OF SUPERVISORS' APPROVAL OF AIRPORT SURVEILLANCE TECHNOLOGY POLICIES AND ANNUAL SURVEILLANCE REPORT PURSUANT TO CHAPTER 19B OF THE SAN FRANCISCO ADMINISTRATIVE CODE GOING FORWARD

WHEREAS, based on the City's Surveillance Technology Ordinance, San Francisco Administrative Code Chapter 19B (Ordinance or Chapter 19B), adopted by the Board of Supervisors (Board) in 2019, the Airport must obtain Board approval for its Surveillance Technology Policies and Annual Surveillance Report (Policies); and

WHEREAS, Chapter 19B, which has been in effect since July 2019, regulates City departments' acquisition and use of Surveillance Technology, as defined in the Ordinance, and requires that departments adopt Board-approved Policies for each item of Surveillance Technology they currently use or plan to acquire; and

WHEREAS, until recently, the City's Committee on Information Technology (COIT) took the responsibility of obtaining that approval for all City departments, including the Airport, but recently revised procedures now require departments, rather than COIT, to seek such approval from the Board; and

WHEREAS, as a result, Staff requests authorization for the Airport to seek Board approval for these Policies going forward; now, therefore, be it

RESOLVED, that this Commission authorizes the Airport to seek approval for the Airport Surveillance Technology Policies and its Annual Surveillance Report from the Board of Supervisors pursuant to Chapter 19B of the San Francisco Administrative Code going forward.

I hereby certify that the foregoing resolution was adopted by the Airport Commission

at its meeting of APR 18 2023

Secretary

San Francisco International Airport

MEMORANDUM

April 18, 2023

TO: AIRPORT COMMISSION
Hon. Malcolm Yeung, President
Hon. Everett A. Hewlett, Jr.
Hon. Jane Natoli
Hon. Jose F. Almanza

23-0103

APR 18 2023

FROM: Airport Director

SUBJECT: Authorization for the Airport to Seek Board of Supervisors' Approval of Airport Surveillance Technology Policies and Annual Surveillance Report Pursuant to Chapter 19B of the San Francisco Administrative Code Going Forward

DIRECTOR'S RECOMMENDATION: ADOPT RESOLUTION AUTHORIZING THE AIRPORT TO SEEK BOARD OF SUPERVISORS' APPROVAL OF AIRPORT SURVEILLANCE TECHNOLOGY POLICIES AND ANNUAL SURVEILLANCE REPORT PURSUANT TO CHAPTER 19B OF THE SAN FRANCISCO ADMINISTRATIVE CODE GOING FORWARD.

Executive Summary

In June of 2019, the San Francisco Board of Supervisors (Board) passed an amendment to the City's Administrative Code – Acquisition of Surveillance Technology ordinance to monitor, regulate and require reporting for City department's acquisition and use of Surveillance Technology, as defined in the ordinance, which is codified at Administrative Code Chapter 19B (Ordinance or Chapter 19B).

Under the Ordinance, City departments are required to obtain Board approval of Surveillance Technology Policies and an Annual Surveillance Report (Policies). Until recently, as described below, the City's Committee on Information Technology (COIT) took responsibility for obtaining that approval. But, recently revised procedures now require City departments, rather than COIT, to seek it. As a result, Staff requests that the Commission authorize the Airport to seek such approval by the Board going forward. The three policies that the Airport plans to submit to the Board in the near future are: Application Based Commercial Transport (ABCT), Electronic Toll Readers (ETR) and Gunshot Detection Solution (GDS) technologies.

THIS PRINT COVERS CALENDAR ITEM NO. 9

Background

Chapter 19B, which has been in effect since July 2019, regulates City departments' acquisition and use of Surveillance Technology, defined below, and requires that departments adopt Board-approved Policies for each item of Surveillance Technology they currently use or plan to acquire. The Ordinance's definition of Surveillance Technology is very broad as follows,

> "Surveillance Technology" means any software, electronic device, system utilizing an electronic device, or similar device used, designed, or primarily intended to collect, retain, process, or share audio, electronic, visual, location, thermal, biometric, olfactory or similar information specifically associated with, or capable of being associated with, any individual or group.
>
> "Surveillance Technology" includes but is not limited to the following: international mobile subscriber identity (IMSI) catchers and other cell site simulators; automatic license plate readers; electric toll readers; closed-circuit television cameras; gunshot detection hardware and services; video and audio monitoring and/or recording technology, such as surveillance cameras, wide-angle cameras, and wearable body cameras; mobile DNA capture technology; biometric software or technology, including facial, voice, iris, and gait-recognition software and databases; software designed to monitor social media services; x-ray vans; software designed to forecast criminal activity or criminality; radio-frequency I.D. (RFID) scanners; and tools, including software and hardware, used to gain unauthorized access to a computer, computer service, or computer network.

Admin Code §19B.1. Since the Ordinance became effective, COIT has taken responsibility for introducing all department Policies to the Board for approval, including the Airport. Beginning in August 2019, as required under the Ordinance, departments provided COIT with inventories of their existing Surveillance Technology. Soon after, departments began submitting to COIT Surveillance Impact Reports (SIRs), and draft policies generated using COIT's toolbox.

COIT and its Privacy and Surveillance Advisory Board (PSAB) held public hearings to consider the policies and ultimately vote on whether to recommend them to the Board. To date, the Board has approved three Airport Polices for: (1) Airport Security Cameras (Pre-Security Closed-Circuit Television); (2) Third Party Security Cameras, and (3) Automated License Plate Readers. See attached summary of Policies.

Recently, COIT notified City departments that it will no longer be introducing individual department policies, nor their Annual Surveillance Reports to the Board on departments' behalf. Instead, departments will now have that responsibility. COIT will still provide a recommendation letter for the Board file, and present its recommendation on the department's Policy at the Board hearing. In addition, COIT will continue to handle the introduction of citywide Policies to the Board. As a result, Staff recommends that the Commission authorize the Airport to seek Board approval of the Policies going forward.

Recommendation

I recommend the Commission authorize the Airport to seek Board of Supervisors' approval of Airport Surveillance Technology Policies and its Annual Surveillance Report pursuant to Chapter 19B of the San Francisco Administrative Code ~~going~~ forward.

Ivar C. Satero
Airport Director

Prepared by: Ray Ricardo
Acting Chief Information Officer

Attachment - Surveillance Technology Policies Summary

Summary of the Airport's Surveillance Technology (ST) Policies

Surveillance Technology (ST)	ST Description	ST Authorized Use Cases – The Airport shall use the ST only for the following authorized purposes:	Benefits of the ST
BOS Approved Policies (STPs):			
Pre-Security Closed-Circuit Television (CCTV) Cameras	Airport owns and operates CCTV cameras which monitor pre-security checkpoint areas that are open and accessible to all members of the public. **STATUS:** POLICY APPROVED 7/27/21 – Board passed 8/4/21 – Mayor approved	1. Live Monitoring 2. Recording of video and images in the event of an incident. 3. Reviewing camera footage. 4. Providing video footage/ images to law enforcement or other authorized persons following an incident or upon request, when footage is subject to disclosure pursuant to a Public Records Act Request.	**For Residents:** - Health: Protect Safety of Staff, patrons, and facilities while promoting an open and welcoming environment. - 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. **Civil Rights Impacts and Safeguards:** - The Airport's use of CCTV is restricted to those identified Authorized Use Cases. - The Airport retains CCTV footage for one year, consistent with State law. - Video files are only released through subpoena, a public records act request, to assist law enforcement with an investigation and to assist Airport personnel in the investigation of claims. **Fiscal Analysis of Costs and Benefits:** - Financial Savings: Airport CCTV saves on salary cost for Airport staff and SFPD-AB patrol officers.

Summary of the Airport's Surveillance Technology (ST) Policies

Surveillance Technology (ST)	**ST Description**	**ST Authorized Use Cases –** The Airport shall use the ST only for the following authorized purposes:	**Benefits of the ST**
			- Time Savings: Airport CCTV provides real-time feeds that run 24/7, thus eliminating lengthy physical surveillance of Airport facilities. - Staff Security: Security cameras provide advance view of an incident to better prepare those responding to an incident. - Data Quality: Security cameras operate 24/365 which maximizes the Airport's ability to capture video of incidents. Video can be used to verify the accuracy of written reports regarding the incident.
License Plate Recognition System: Automated License Plate Readers (ALPR) – Ground Transportation Management System (GTMS)	Airport uses license plate recognition cameras on Airport roadways to monitor commercial ground transportation operators and for revenue collection. **STATUS:** POLICY APPROVED 7/27/21 – Board passed 8/4/21 – Mayor approved	1. To track the activity of permitted commercial ground transportation at the Airport. Also used as a secondary method for collecting trip fees in the event of an operator's transponder fails to read. 2. To support the Airport and local, state, federal, and regional public safety departments in the identification of vehicles that are the subject of investigation; and/or locating victims, witnesses, suspects, and other associated with a law enforcement investigation.	**For Residents:** - Environment: Traffic congestion studies – ALPR-GTMS can be used to conduct studies on traffic volumes and patterns, with the potential to mitigate environmental impacts of traffic congestion on residents. - Criminal Justice: ALPR-GTMS can be used to support identification of vehicles as a part of law enforcement investigations. - Public Safety: ALPR-GTMS can be used to locate stolen, wanted, and or other vehicles that are subjects of investigation, and can improve overall roadway safety for residents using Airport roadways.

Summary of the Airport's Surveillance Technology (ST) Policies

Surveillance Technology (ST)	ST Description	ST Authorized Use Cases – The Airport shall use the ST only for the following authorized purposes:	Benefits of the ST
			Civil Rights Impacts and Safeguards: - Commercial ground transportation operators acknowledge notice of GTMS Policies and Procedures, which include the Airport's use of ALPR and Electronic Toll Readers, by signing the Airport Permit. - In compliance with California Civil Code 1798.90.5, the Airport shall notify the public of ALPR-GTMS surveillance technology operation by posting the ALPR-GTMS Privacy and Usage Policy on the FlySFO.com website. **Fiscal Analysis of Costs and Benefits:** - Time Savings: Without the ALPR-GTMS technology, the Airport would need to deploy a manually staffed ground transportation operation. Team members would have to conduct manual verification of registration via visual observation of permits and decals, and conduct traffic counts. The ALPR-GTMS technology removes the necessity of staffing for these purposes. - Data Quality: The ALPR-GTMS technology is verified against the AVI technology to confirm all permitted vehicles' trips have been documented for tracking and fee assessment purposes

Summary of the Airport's Surveillance Technology (ST) Policies

Surveillance Technology (ST)	ST Description	ST Authorized Use Cases – The Airport shall use the ST only for the following authorized purposes:	Benefits of the ST
			(in case the AVI malfunctions and fails to read the Airport transfixed transponder). - Financial: The ALPR-GTMS technology enables the Airport to assess trip fees on permitted Commercial ground transportation operators. For example, in 2019, the Airport collected $64.8M+ in trip fees from ground transportation operators.
Tenant ("Third-Party") Security Cameras	Airport Tenants own and operate security cameras in their physical locations within the Airport. **STATUS:** POLICY APPROVED 11/15/22 – Board passed 11/17/22 – Mayor approved	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.	**For Residents:** - Health: Protect Safety of staff, patrons, and facilities while promoting an open and welcoming environment. - 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. - Financial Savings: Equipment is owned and operated by a non-city entity. - 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.

Summary of the Airport's Surveillance Technology (ST) Policies

Surveillance Technology (ST)	ST Description	ST Authorized Use Cases – The Airport shall use the ST only for the following authorized purposes:	Benefits of the ST
			Civil Rights Impacts and Safeguards: - 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 & 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). **Fiscal Analysis of Costs and Benefits:** - Financial Savings: Tenants' Security Camera Systems will save on building or patrol officers.

Summary of the Airport's Surveillance Technology (ST) Policies

Surveillance Technology (ST)	**ST Description**	**ST Authorized Use Cases –** The Airport shall use the ST only for the following authorized purposes:	**Benefits of the ST**
			- Time Savings: Tenants' Security Camera Systems will run 24/365, thus decreasing or eliminating building or patrol officer supervision. - Staff Safety: Tenant/Contractor Security cameras help identify violations of the Patron Code of Conduct and provide assurance that staff safety is emphasized and will be protected at their place of employment. - Data Quality: Security cameras run 24/365, 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.

Summary of the Airport's Surveillance Technology (ST) Policies

Surveillance Technology (ST)	ST Description	ST Authorized Use Cases – The Airport shall use the ST only for the following authorized purposes:	Benefits of the ST
COIT Approved Policies (STPs) - Next Step: Seek BOS Approval			
Application Based Commercial Transport (ABCT)	The primary functions for the Application Based Commercial Transport (ABCT) technology are to use location data to help Airport personnel enforce operating agreements for Transportation Network Companies (TNCs), administer and regulate these programs, and for general transportation planning. • ABCT reconciles the monthly self-reported invoices from the TNC's (Transportation Network Companies) against its collected data to ensure the Airport is properly compensated for the correct amount of traffic and receives accurate payments each month.	1. To invoice Transportation Network Companies (TNCs) for trip fees based on their passenger pick-ups and drop-offs at the Airport and perform invoice reconciliation. 2. To monitor and enforce TNCs' compliance with the conditions of their operating permit and the Airport's Rules & Regulations (R&Rs). 3. To provide support for the issuance of citations for traffic violations by the SFPD Airport Bureau. 4. To support Public Safety by ensuring only authorized and approved drivers and vehicles are allowed to service passengers at SFO.	**For Residents:** Community Development: Equitable distribution of and access to transportation. Environment: Traffic patterns and congestion within SFO. Jobs: TNC companies and driver's; Ground Transportation Unit (GTU) resources. Public Safety: Reduces the risk of fraud and unethical business practices. **Civil Rights Impacts and Safeguards:** SFO strictly prohibits the use of location data to identify or track individual users or customers of the City's Airport transportation system.

Summary of the Airport's Surveillance Technology (ST) Policies

Surveillance Technology (ST)	**ST Description**	**ST Authorized Use Cases –** The Airport shall use the ST only for the following authorized purposes:	**Benefits of the ST**
			To avoid resident loss of trust, public notice regarding SFO's receipt and use of data regarding TNC drivers' activity at the Airport is provided on the SFOConnect web-site (sfoconnect.com). - To avoid discrimination and other potential civil rights impacts, data access is granted only to authorized users for authorized uses. - To protect the individual identities, travel preferences, and trip patterns and behaviors of individuals, any data released to the public through Sunshine requests or Public Records do not contain personal identifying information. - Collected data is stored on a secure network in a restricted, password-protected system that can only be accessed by authorized personnel for authorized uses. **Fiscal Analysis of Costs and Benefits:** Financial Savings: Not having to hire additional staff to manually monitor and manage the TNC's activities.

Summary of the Airport's Surveillance Technology (ST) Policies

Surveillance Technology (ST)	**ST Description**	**ST Authorized Use Cases –** The Airport shall use the ST only for the following authorized purposes:	**Benefits of the ST**
			Time Savings: Staff can reconcile monthly invoices quickly with the use of aggregated data, saving dozens of hours per month of accounting time. Data Quality: Human error is reduced; information is legible and can be easily sorted and summarized by computers; can be paired with analytical analysis; likely reduction in fraudulent handwritten records; increase in the number of records, since they are automatically created and sent. Enforcement of Non-Compliant Drivers: Improved enforcement for non-compliance: drivers exceeding curbside staging times, drop-off and pick-ups at non-designated areas can be subject to fines and/or citations by the Airport (GTU and SFPD-AB), based upon the contracts with the TNC's.
Electronic Toll Readers (ETR)	Use of FasTrak Toll Readers provides the ability to accept an alternate payment method that efficiently processes parking fees.	1. Process Parking Transactions. 2. Investigation of Parking Transaction Disputes.	**For Residents:** Public Safety: More efficient payment systems for customers reduce traffic congestion and bottlenecks,

Summary of the Airport's Surveillance Technology (ST) Policies

Surveillance Technology (ST)	ST Description	ST Authorized Use Cases – The Airport shall use the ST only for the following authorized purposes:	Benefits of the ST
	Parking efficiency minimizes traffic on SFO's roadways. More efficient payment systems for customers reduce traffic congestion and bottlenecks, decreasing the likelihood of collisions and improving customer safety. Provides a uniform methodology for SFO parking fee collection and more effectively quantifies parking demand, which supports future SFO planning.		decreasing the likelihood of collisions and improving customer safety. Convenience: Limits parking congestion through more efficient payment processes. **Civil Rights Impacts and Safeguards:** The Airport strives to mitigate all potential civil rights impacts through responsible technology and data use policies and procedures, and intends to use electronic toll readers and their associated data exclusively for the aforementioned authorized use cases. All other uses, including surveillance of San Francisco residents or groups, are expressly prohibited. Access to personal information collected by the FasTrak Toll Readers is limited only to certain operations and technical employees for limited, approved purposes based on their specific work responsibilities.

Summary of the Airport's Surveillance Technology (ST) Policies

Surveillance Technology (ST)	ST Description	ST Authorized Use Cases – The Airport shall use the ST only for the following authorized purposes:	Benefits of the ST
			Authorized personnel must submit a request to the Data Steward to access the limited dataset identified. Requesting personnel must specify the reason for their request. Privacy and security training is required for employees with access to Personally Identifiable Information (PII), upon hire or assignment to projects involving toll readers. A breach of the toll reader system is also not likely to compromise personal information, as all data collected by the toll readers is seamlessly transmitted to an Airport database. No data is retained on the toll reader itself. To further avoid breach and misuse of personal information collected by toll readers, storage of PII on databases is encrypted and protected by software, hardware and physical security measures to prevent unauthorized access.

Summary of the Airport's Surveillance Technology (ST) Policies

Surveillance Technology (ST)	**ST Description**	**ST Authorized Use Cases –** The Airport shall use the ST only for the following authorized purposes:	**Benefits of the ST**
			Third parties with whom the Airport shares PII are also required to implement adequate security measures to maintain the confidentiality of such information. **Fiscal Analysis of Costs and Benefits:** Financial Savings: Low maintenance and operating costs in addition to minimal training of personnel on the use of the technology. Time Savings: Parking fee collections are much more efficient. Staff Safety: Staff no longer need to sit in parking booths that are near fast moving vehicles. Data Quality: Provides a uniform methodology for SFO parking fee collection, and more effectively quantifies parking demand, which supports future SFO planning.
Gunshot Detection Solution (GDS)	The primary function for the Gunshot Detection Solution (GDS) is a detection and response system designed to protect lives in incidents involving an indoor active	1. Detect the sound of gun shots, aggressive voices, glass breaking, and unusual disturbances (based upon	**For Residents:** Health: Protect safety of staff, patrons, and facilities while promoting an open and welcoming environment.

Summary of the Airport's Surveillance Technology (ST) Policies

Surveillance Technology (ST)	ST Description	ST Authorized Use Cases – The Airport shall use the ST only for the following authorized purposes:	Benefits of the ST
	shooter, aggressive behavior, glass breaking or unusual disturbances. • By automating the emergency notification process and removing the human element, first responders arrive on scene faster, equipped with the vital information needed to contain threats and mitigate casualties. The GDS provides immediate and accurate response information, including specific location and type of sound, for Airport Commission staff and law enforcement teams. • The gunshot detection system will use existing Wi-Fi access points owned and deployed by the Airport. • All analysis is conducted at the sensor (detector), with no real-time audio transmitted or recorded, ensuring privacy.	machine learned decibel level) and use of device sensors to locate the origin of the sounds. 2. Provide the date and time stamp, the type of gun used or sound detected and the geographical location (i.e., which sensor detected the sound) to law enforcement or other authorized persons in connection with the investigation of an incident, or to members of the public when the information is subject to disclosure pursuant to a Public Records Act request. 3. Upon a GDS alarm, 9-1-1 Dispatch and the Security Operations Center (SOC) can immediately view CCTV feeds of the location identified in the alarm to provide Airport First Responders situational awareness (i.e., location) of an incident.	Criminal Justice: SFPD-AB can be quickly alerted and respond, when needed, to the sound of gunshots, aggressive voices, glass shattering, or other high decibel level sound disturbances such as blasts, with improved geographic precision. In conjunction with the video images from the Airport's CCTV system, Law Enforcement can be provided situational awareness or information to assist in its investigation of an incident. Public Safety: Improved protection of the public and City assets by leveraging remote condition assessment technology, which improves overall situational awareness. The technology helps ensure the safety of the 49,000+ people who work at the Airport and the 58 million people who fly to and from SFO every year.

Summary of the Airport's Surveillance Technology (ST) Policies

Surveillance Technology (ST)	ST Description	ST Authorized Use Cases – The Airport shall use the ST only for the following authorized purposes:	Benefits of the ST
			Civil Rights Impacts and Safeguards: The Airport's use of the AmberBox solution is restricted to those identified Authorized Use Cases. Data is housed in servers located in secured areas that are only accessible by approved and badged employees. Cloud access to data is administered by Airport badged employees with access to cloud services that enable continuous monitoring of the Airport account activity. **Fiscal Analysis of Costs and Benefits:** Financial Savings: The gunshot detection solution (GDS), in conjunction with the Airport Security Camera Systems, will run 24/7, thus decreasing or eliminating the need for additional building or SFPD-AB patrol officer supervision and saving on salary expense.

Summary of the Airport's Surveillance Technology (ST) Policies

Surveillance Technology (ST)	ST Description	ST Authorized Use Cases – The Airport shall use the ST only for the following authorized purposes:	Benefits of the ST
			Time Savings: The gunshot detection solution's automated notification removes the human element of notification which allows first responders to arrive more promptly to the scene to de-escalate any potentially violent situations. Use of the solution provides instant alerts, so that real-time 24/7 CCTV feeds can be viewed, to provide pinpoint location accuracy, thus eliminating lengthy physical surveillance of Airport facilities. Staff Safety: The gunshot detection solution will provide immediate information about the location of potential threats to staff safety. The gunshot detection solution will alert Law Enforcement to the location of the incident. This will prompt them to view the camera feeds for an immediate view as the event is occurring, to better prepare those responding to the incident.

Summary of the Airport's Surveillance Technology (ST) Policies

Surveillance Technology (ST)	**ST Description**	**ST Authorized Use Cases –** The Airport shall use the ST only for the following authorized purposes:	**Benefits of the ST**
			Data Quality: The identification of ambient noise from GDS coupled with CCTV cameras use, provides Law Enforcement complete situational awareness.

AIRPORT COMMISSION

CITY AND COUNTY OF SAN FRANCISCO

RESOLUTION NO._____

RESOLUTION AUTHORIZING THE AIRPORT TO SEEK BOARD OF SUPERVISORS' APPROVAL OF AIRPORT SURVEILLANCE TECHNOLOGY POLICIES AND ANNUAL SURVEILLANCE REPORT PURSUANT TO CHAPTER 19B OF THE SAN FRANCISCO ADMINISTRATIVE CODE GOING FORWARD

WHEREAS, based on the City's Surveillance Technology Ordinance, San Francisco Administrative Code Chapter 19B (Ordinance or Chapter 19B), adopted by the Board of Supervisors (Board) in 2019, the Airport must obtain Board approval for its Surveillance Technology Policies and Annual Surveillance Report (Policies); and

WHEREAS, Chapter 19B, which has been in effect since July 2019, regulates City departments' acquisition and use of Surveillance Technology, as defined in the Ordinance, and requires that departments adopt Board-approved Policies for each item of Surveillance Technology they currently use or plan to acquire; and

WHEREAS, until recently, the City's Committee on Information Technology (COIT) took the responsibility of obtaining that approval for all City departments, including the Airport, but recently revised procedures now require departments, rather than COIT, to seek such approval from the Board; and

WHEREAS, as a result, Staff requests authorization for the Airport to seek Board approval for these Policies going forward; now, therefore, be it

RESOLVED, that this Commission authorizes the Airport to seek approval for the Airport Surveillance Technology Policies and its Annual Surveillance Report from the Board of Supervisors pursuant to Chapter 19B of the San Francisco Administrative Code going forward.

I hereby certify that the foregoing resolution was adopted by the Airport Commission

*at its meeting of*_____

_____

Secretary

San Francisco International Airport

April 29, 2024

Ms. Angela Calvillo
Clerk of the Board
Board of Supervisors
City Hall
1 Dr. Carlton B. Goodlett Place, Room 244
San Francisco, CA 94102-4689

Subject: Chapter19B - Acquisition of Surveillance Technology Ordinance: Amended Surveillance Technology Policy being submitted pursuant to Administrative Code Section 19B.2(a).

Dear Ms. Calvillo:

Pursuant to Administrative Code Chapter 19B, Acquisition of Surveillance Technology Ordinance, I am forwarding to the Board of Supervisors the following COIT-approved Amended Surveillance Technology Policy, as that term is defined in Administrative Code Section 19B.1, for the San Francisco International Airport (Airport) for approval.

According to Administrative Code Section 19B.2(a), "a Department must obtain Board of Supervisors approval by ordinance of a Surveillance Technology Policy under which the Department will acquire and use Surveillance Technology…"

The following is a list of accompanying documents:

- This Letter;
- COIT Recommendation Memorandum;
- Ordinance Approving the Amended Airport Surveillance Technology Policy governing the use of Pre-Security Cameras.
- Legislative Digest
- Airport Commission Resolution No. 23-0103;
- Memorandum accompanying Airport Commission Resolution No. 23-0103; and
- COIT-Approved Amended Surveillance Technology Policy for Security Cameras

The following persons may be contacted regarding this matter:

Iyad Hindiyeh, Airport Chief Digital Transformation Officer
(650) 821-3350
iyad.hindiyeh@flysfo.com

Guy Clarke, IT Governance, Risk & Compliance, Airport ITT
(650) 821-3392
guy.clarke@flysfo.com

Very Truly Yours,

Ivar C. Satero
Airport Director

Surveillance Technology Policy

Security Cameras
San Francisco International Airport

The City and County of San Francisco values privacy and protection of San Francisco residents' civil rights and civil liberties. As required by San Francisco Administrative Code, Section 19B, the Surveillance Technology Policy aims to ensure the responsible use of the Department's Security Camera System (hereinafter referred to as "surveillance technology") itself as well as any associated data, and the protection of City and County of San Francisco residents' civil rights and liberties.

PURPOSE AND SCOPE

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

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

POLICY STATEMENT

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

Authorized Use(s):

1.	Live monitoring.
2.	Recording of video and images.
3.	Reviewing camera footage in the event of an incident.
4.	Providing video footage/images to law enforcement or other authorized persons following an incident or upon request.

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

Department 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.

All data collected by surveillance cameras is the exclusive property of the City and County of San Francisco. Under no circumstance shall collected data be sold to another entity.

Surveillance Oversight Review Dates
PSAB Review: January 25, 2024
COIT Review: February 15, 2024
Board of Supervisors Approval: TBD

BUSINESS JUSTIFICATION

Reason for Technology Use

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

See Appendix A Below.

Description of Technology

See Appendix A Below.

Resident Benefits

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

	Benefit	Description
☐	Education	
☐	Community Development	
X	Health	Protect safety of staff, patrons, and facilities while promoting an open and welcoming environment.
☐	Environment	
X	Criminal Justice	Review video footage after a security incident; provide video evidence to law enforcement or the public upon request by formal process, order, or subpoena.
☐	Jobs	
☐	Housing	
X	Other	Better management of city assets by leveraging remote condition assessment. Improvement of overall Situation Awareness.

Department Benefits

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

	Benefit	Description
X	Financial Savings	Department Security Camera Systems will save on building or patrol officers.
X	Time Savings	Department Security Camera Systems will run 24/7, thus decreasing or eliminating building or patrol officer supervision.

X	Staff Safety	Security cameras help identify violations of the City Employee's Code of Conduct, Building Rules and Regulations, and City, State and Federal law and provide assurance that staff safety is emphasized and will be protected at their place of employment.
X	Data Quality	Security cameras run 24/7/365 so full-time staffing is not required to subsequently review footage of security incidents. Data resolution can be set by level and is currently set to high resolution.
X	Other	Security cameras will enhance effectiveness of incident response and result in improved level of service.

POLICY REQUIREMENTS

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

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

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

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

Data Type(s)	*Format(s)*	*Classification*
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 with Section 19.5 of the Administrative Code. Department notifications shall identify the type of technology being used and the purpose for such collection.

Department includes the following items in its public notice:

X Information on the surveillance technology
X Description of the authorized use
☐ Type of data collected
☐ Data retention
X Department identification
X Contact information

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

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

Access to live views and recorded footage is restricted to specific trained personnel. Recorded footage is accessed only in response to an incident.

Details on department staff and specific access are available in Appendix A.

1. ***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:

See Appendix A Below.

2. ***Members of the public***

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

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

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

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.

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 dictated by this policy. 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.

More specifically, Department training will include:

Annual cybersecurity training (COIT Policy Link).

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.

Department shall ensure compliance with these security standards through the following:

- 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 the 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 Storage: Data will be stored in the following location:

X Local storage (e.g., local server, storage area network (SAN), network

attached storage (NAS), backup tapes, etc.)

X Department of Technology Data Center

X Software as a Service Product

X Cloud Storage Provider

Data Sharing: Department will endeavor to ensure that other agencies or departments that may receive data collected by the surveillance technology 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.

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

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

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

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

- Confirm the purpose of the data sharing aligns with the department's mission.
- Consider alternative methods other than sharing data that can accomplish the same purpose.
- Redact names and ensure all PII is removed in accordance with the department's data policies. NOTE: The Airport's camera software currently does not have the capability to "scrub faces" and Facial Recognition Technology is not used.
- Review of all existing safeguards to ensure shared data does not increase the risk of potential civil rights and liberties impacts on residents.
- Evaluation of what data can be permissibly shared with members of the public should a request be made in accordance with the San Francisco's Sunshine Ordinance.

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

The Department may share Security Camera footage with the following entities:

A. Internal Data Sharing:

In the event of an incident, Security Camera images may be live-streamed or shared by alternative methods to the following agencies within the City and County of San Francisco:

Data Type	Data Recipient
Video and Images Date and Time	- Within the operating Department - Police - City Attorney - District Attorney - Sheriff - On request following an incident.

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

B. External Data Sharing:

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

Data Type	Data Recipient
Video and Images Date and Time	Other local law enforcement agencies Airport Tenants, Contractors and Sub-Contractors

NOTE: Tenants, Contractors and Sub-Contractors are required to adhere to the Airport's requirements for protecting and maintaining video data via the contract Terms with the Airport.

Frequency - 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:

Retention Period	Retention Justification
1. Security Camera data will be stored for one (1) year to be available to authorized staff for operational necessity and ready reference.	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.

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.

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

If data is associated with an incident, it may be kept for longer than the standard retention period.

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

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

1. Automatic overwrite of all existing files when the standard data retention period ends.
2. This may take the form of a delete/reformat, wipe, overwrite of existing data, or degaussing.

COMPLIANCE

Department Compliance

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

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.

Interdepartmental, Intergovernmental & Non-Governmental Entity Compliance

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

See Appendix A Below.

Oversight Personnel

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

See Appendix A Below.

Sanctions for Violations

Sanctions for violations of this Policy include the following:

See Appendix A Below.

EXCEPTIONS

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

DEFINITIONS

Personally Identifiable Information:	Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.
Raw Data:	Information collected by a surveillance technology that has not been processed and cleaned of all personal identifiable information. The distribution and use of raw data is tightly restricted.
Exigent Circumstances	An emergency involving imminent danger of death or serious physical injury to any person that requires the immediate use of Surveillance Technology or the information it provides.

AUTHORIZATION

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

QUESTIONS & CONCERNS

Public Inquiries

See Appendix A Below.

Department shall acknowledge and respond to complaints and concerns in a timely and organized response, and in the following manner:

See Appendix A Below.

Inquiries from City and County of San Francisco Employees

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

Appendix A: Department Specific Responses

Department: San Francisco International Airport

1. **Reason for Technology Use**

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

The technology helps to protect and provide for the Safety and Security of our passengers, the public, and all Airport employees.

2. **Description of Technology**

A. Airport Cameras

The Airport uses Verint Video Management Software (VMS) and, primarily, Pelco Analog and Digital Pan-Tilt-Zoom (PTZ) and fixed cameras. The cameras are installed in public areas of the Airport. Specific to this submission, the cameras are located pre-security.

The Verint system is a closed system, running on a security local area network that is not exposed to the Internet.

B. AirTrain and SFO Shuttle Buses

The closed-circuit television (CCTV) system security cameras on the AirTrain vehicles and the SFO Shuttle Buses captures and records video images of passengers. The CCTV security cameras and the images/video they capture shall be used for business purposes only and not for personal use. The security cameras shall be used 24 hours a day, 365 days per year.

For the AirTrain vehicles, each vehicle has four Safe Fleet VMAX cameras mounted to the ceiling to provide video of the interior to an onboard Digital Video Recorder (DVR) which is also located inside the vehicle. The cameras record when the train is fully powered. The DVR has a microSD card that stores video recordings for two-weeks and automatically rewrites after that time. For viewing, the microSD card is removed with a key by AirTrain Administration personnel only and can be viewed on a password protected computer.

Each SFO Shuttle bus is equipped with multiple video cameras capturing multiple interior and exterior views. Interior cameras also capture sound. The footage is stored in an onboard DVR device located in a locked cabinet. The DVRs overwrite footage every 30 days. The only way to preserve footage is to remove the DVR, connect it to a

secured computer in the Administrative Office, and save the images to this password protected computer.

C. BART CCTV System and Video Streaming

The BART CCTV system will provide video streaming from 50 cameras deployed around the Airport BART Station to seven Airport workstations primarily at the Airport's Security Operations Center (SOC) using the VIDSYS Software Platform.

The VIDSYS Software Platform:

The Vidsys CSIM software platform continuously fuses, instantly correlates, and converts vast amounts of data into meaningful and actionable information gathered from virtually any type, brand, or generation of physical security system or sensor, and from many other networked management applications. The automated tools support safe, effective, and timely resolution of incidents and alarms. The tools also manage complex incidents that involve multiple simultaneous alarms at one or more locations.

The Vidsys CSIM platform has two primary components: Situation Awareness and Situation Management. The platform comes with software applications that integrate each category of devices with the single operating platform. As a secure web-based solution, the Vidsys platform allows operators to manage assets for a single facility or multiple locations.

3. **Access to the Technology and Department Compliance**

The specific categories and titles of individuals who are authorized by the Department to access or use the collected information:

- 9202 - 911 Dispatcher
- 9203 - 911 Dispatch Supervisor
- 9212 - Security Operations Center (SOC) Analyst
- 9213 - Airfield Safety Officer
- 9220 - SOC Supervisor
- 9221 - Airport Operations Supervisor

  5290 – Senior Transportation Planner
- Air Train Staff and Contractors
- Aviation Security System MX Contractors

- Ground Transportation Unit (GTU)
- Parking Management
- SFPD-AB
- San Mateo County Sheriff and District Attorney

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

Interdepartmental, Intergovernmental & Non-Governmental Entity Compliance

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

The Department will endeavor to ensure that other agencies or departments that may receive data collected by Airport cameras, AirTrain cameras, SFO Shuttle Bus cameras, and BART's security cameras will act in conformity with this Surveillance Technology Policy.

Oversight Personnel

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

- 9212 – Aviation Security Analyst
- 9220 – Aviation Security Supervisor
- 0923 – AirTrain Safety and Security Manager
- 0931 – Manager Aviation Security & Regulatory Compliance
- 0933 - Director, Security, Emergency Management & Communications and AirTrain Director
  0943 - Managing Director, Safety, Security and Airside Services
- 0955 – Chief Operating Officer

3. **Sanctions for Violations**

Sanctions for violations of this Policy include the following:

The discipline processes established in the various Memoranda of Understanding (MOUs) which apply to the different classifications of employees represented by the corresponding unions.

4. **Public Inquiries**

What procedures will be put in place by which members of the public can register complaints or concerns or submit questions about the deployment or use of a specific Surveillance

Technology, and how the Department will ensure each question and complaint is responded to in a timely manner.

Public question and complaint can be submitted via the:

- Airport Guest Services (Contact SFO – https://www.flysfo.com/contact-sfo)
- Airport public email, phone, or website (Contact SFO), or
- Airport Commission meetings (How to Address the Commission)

Specific details on where data will be stored (local, DT, SaaS, Cloud Storage) including name of vendor and retention period.

Data is stored on a local server for 45 days, then video files are transferred to Amazon Web Services for up to 1 year. Files are deleted after 320 days based on the lifecycle policy in AWS. BART is the custodian of their video footage, and as such, is solely responsible for the management, retention and destruction of that video footage.

For AirTrain, in accordance with the SFO Executive Directive (ED 18-05) Record Retention and Destruction Policy, video data will be stored in the vehicle for a two-week period before the data is overwritten. Any AirTrain saved images or videos will be retained for 4.5 years. As noted above, the SFO Shuttle Bus footage is stored in an onboard DVR device and is overwritten every 30 days. No Private Personal Information (PII) is stored on the drives. Additional information included with the images and video is the location, vehicle, and time/date.

Is a subpoena required before sharing with law enforcement?

- No

City and County of San Francisco

San Francisco International Airport

Airport Pre-Security Cameras

June 17, 2024

Joyce Mamiya, Derek Phipps, Guy Clarke – SFO

Technology Description – Pre-Security Cameras

Pre-Security Cameras support the Airport's mission and primary Objective:

Safety and Security.

- SFO is committed to the Safety and Security of the Airport in the following ways:
  - Live monitoring of the Airport's Pre-Security space for incident monitoring and claims investigations.
  - Safety and Security of the public within the Airport.
  - Reviewing camera footage in the event of an incident that occurs Pre-Security.
- The technology includes:
  - Video Management Software (VMS)
  - Various types of camera technology
- The primary function is to record live video feed of various areas of Pre-Security at the Airport.

Authorized Use Cases

Airport Specific Use Cases include:

1. *Live monitoring.*
2. *Recording of video and images.*
3. *Reviewing camera footage in the event of an incident.*
4. *Providing video footage/images to law enforcement or other authorized persons following an incident or upon request.*

Pre-Security Cameras ST Policy – Change Summary

- The Authorized Use Cases did not change.
- Updates were made as follows:
  - To the prior ST Policy in two areas:
    - <u>Data Sharing Section -Third Bullet Point:</u>
      - "Redact names and ensure all PII is removed in accordance with the department's data policies."
      - The following NOTE was added: "The Airport's camera software currently does not have the capability to "scrub faces."
  - By adding specific information regarding:
    - the use of Video Cameras on the AirTrain vehicles and the SFO Shuttle Buses for business purposes only.
    - "live" video streaming provided from the BART CCTV system's 50 cameras deployed around the Airport BART Station.

Thank You

Updates: ST Policy

Airport ST Policy change/update:

Data Sharing Section -Third Bullet Point:

"Redact names and ensure all PII is removed in accordance with the department's data policies."

- The following NOTE was added:

"The Airport's camera software currently does not have the capability to "scrub faces."

External Data Sharing Section – Data Recipient:

- The following text was added: "Airport Tenants, Contractors and Sub-Contractors

Updates: AirTrain & SFO Shuttle Buses

- The closed-circuit television (CCTV) system security cameras on the AirTrain vehicles and the SFO Shuttle Buses captures and records video images of passengers for Airport business purposes only.
    - The AirTrain cameras provide video of the interior to an onboard Digital Video Recorder (DVR) which has a microSD card that stores video recordings for two-weeks and automatically rewrites after that time.
        - For viewing, the microSD card is removed with a key by AirTrain Administration personnel only and can be viewed on a password protected computer.
    - The Shuttle Bus cameras capture multiple interior and exterior views.
        - The footage is stored in an onboard DVR device located in a locked cabinet.
        - The DVRs overwrite footage every 30 days.
        - The only way to preserve footage is to remove the DVR, connect it to a secured computer in the Administrative Office, and save the images to this password protected computer.

Updates: BART Video Streaming

1. The BART CCTV system will provide “live” video streaming from 50 cameras deployed around the Airport BART Station to seven Airport workstations primarily at the Airport's Security Operations Center (SOC) using the VIDSYS Software Platform.

2. The Airport does not have direct access to the recordings of the BART video footage.

   - As BART is the owner of the cameras and the software, as well as, the custodian of the video images, the Airport is required to submit a formal Request to BART (including date, time frame and specific camera views) should a copy of video footage be needed.

Data Lifecycle: Data Collected

Data captured is classified as Level 3, Sensitive.

This data includes:

- *Level 3 Classification:*
  - Video and Images
  - Date & Time
  - Vehicle

- All data will be retained for:
  - Resolution of an incident investigation and/or law enforcement matters.

- AirTrain and SFO Shuttle Bus data is retained for 4.5 years, as required by the Airport's Executive Directive 18-05 Record Retention and Destruction Policy and discarded/deleted afterwards.

Data Lifecycle: Data Access

1. Written approval from AVSEC and/or TSA is required prior to release of Pre-Security Camera data. Data is reviewed for Sensitive Security Information.

2. For investigative purposes, Department access to live views and recorded footage is restricted to specific trained personnel. Recorded footage is accessed only in response to an incident.

3. Personnel with access belong to the following groups:

- Security Ops Center
- TSA – SSI Assessment

SFO Law Enforcement Partners
Communications Center

Data Lifecycle: Data Security

1. Pre-Security Cameras are owned and controlled by the Airport.

2. Wireless networks are required to be equipped with WPA2 security.

3. All forms of video footage, whether real-time or stored, must be password protected.

4. Written authorization from AVSEC required prior to release of data.

Thank You