**File No.** 230895 **Committee Item No.** 1
**Board Item No.** 17

# COMMITTEE/BOARD OF SUPERVISORS

AGENDA PACKET CONTENTS LIST

**Committee:** Rules Committee **Date** Nov 6, 2023

**Board of Supervisors Meeting** **Date** November 28, 2023

## 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)**

| | | |
|---|---|---|
| ☒ | ☐ | Airport Commission Resolution 23-0103 |
| ☒ | ☐ | Surveillance Technology Policy (3) |
| ☐ | ☐ | |
| ☒ | ☐ | Surveillance Impact Report |
| ☐ | ☐ | |
| ☐ | ☐ | |
| ☐ | ☐ | |
| ☐ | ☐ | |
| ☐ | ☐ | |

**Completed by:** Victor Young **Date** November 2, 2023
**Completed by:** **Date**

[Administrative Code - Approval of Airport Surveillance Technology Policies]

**Ordinance approving Airport Surveillance Technology Policies governing the use of 1) application-based commercial transport technology, 2) electronic toll readers, and 3) detection systems for gunshots and other noises.**

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 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) Beginning in May 2022, 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 draft Surveillance Technology Policies for the following Surveillance Technology:

(1) Application-Based Commercial Transport Technology;

(2) Electronic Toll Readers; and

(3) Gunshot Detection Solution.

(e) The Surveillance Technology Policies developed for each of the above are detailed in Sections 2 through 4 of this ordinance. The Surveillance Technology Policies are available in Board File No. 230895. COIT recommended that the Board approve each Surveillance Technology Policy.

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

Section 2. Application-Based Commercial Transport (ABCT) Technology

(a) Current Status. The Airport currently possesses and uses ABCT Technology.

(b) Purpose. The Airport uses the ABCT Technology ("Airport ABCT Technology") to: (1) 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) monitor and enforce TNCs' compliance with the conditions of their operating permit and the Airport Rules & Regulations; (3) provide support for the issuance of citations for traffic violations by the Police Department-Airport Bureau; and (4) support public safety by ensuring only authorized and approved drivers and vehicles are allowed to service passengers at SFO.

(c) Surveillance Impact Report and Surveillance Technology Policy. The Airport submitted a Surveillance Impact Report and draft Surveillance Technology Policy for the Airport ABCT Technology to COIT. A copy of the Surveillance Impact Report is in Board File No. 230895.

(d) Public Hearings. Between July 8, 2022 and November 17, 2022, COIT and its PSAB conducted three public hearings at which they considered the Surveillance Impact Report and the draft Surveillance Technology Policy for the Airport ABCT Technology ("Airport ABCT Technology Policy").

(e) COIT Recommendation. On November 17, 2022, COIT voted to recommend the Airport ABCT Technology Policy to the Board for approval.

(f) Findings. The Board hereby finds that the benefits that the Airport ABCT Technology Policy authorizes outweigh the costs and risks; that the Airport ABCT Technology Policy will safeguard civil liberties and civil rights; and that the uses and deployments of

Airport ABCT Technology, as set forth in the Airport ABCT Technology 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 hereby approves the Airport ABCT Technology Policy.

Section 3. Electronic Toll Readers

(a) Current Status. The Airport currently possesses and uses Electronic Toll Readers.

(b) Purpose. The Airport uses Electronic Toll Readers ("Airport ETR") to: (1) Process parking transactions, and (2) Investigate parking transaction disputes.

(c) Surveillance Impact Report and Surveillance Technology Policy. The Airport submitted a Surveillance Impact Report and draft Surveillance Technology Policy for the Airport ETR to COIT. A copy of the Surveillance Impact Report is in Board File No. 230895.

(d) Public Hearings. Between January 27, 2023 and February 16, 2023, COIT and its PSAB conducted two public hearings at which they considered the Surveillance Impact Report and the draft Surveillance Technology Policy for the Airport ETR ("Airport ETR Policy").

(e) COIT Recommendation. On February 16, 2023, COIT voted to recommend the Airport ETR Policy to the Board for approval.

(f) Findings. The Board hereby finds that the benefits that the Airport ETR Policy authorizes outweigh the costs and risks; that the Airport ETR Policy will safeguard civil liberties and civil rights; and that the uses and deployments of Airport ETR, as set forth in the Airport ETR 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 hereby approves the Airport ETR Policy.

/ / / /

/ / / /

Section 4. Gunshot Detection Solution

(a) Current Status. The Airport seeks to acquire a Gunshot Detection Solution.

(b) Purpose. The Airport intends to use the Gunshot Detection Solution ("Airport GDS") to: (1) detect the sound of gun shots, aggressive voices, glass breaking, and unusual disturbances (based upon machine learned decibel level) and use device sensors to locate the origin of the sounds; (2) provide data to law enforcement or other authorized persons regarding date and time of the event, the sound detected, the type of gun used if applicable, and the geographical location in connection with the investigation of an incident; (3) use the Airport GDS alarm, and data provided by the Airport GDS, to allow 911 Dispatch and the Airport's Security Operations Center to immediately view video feeds of the location identified by the alarm; and (4) provide immediate and accurate response information for Airport Commission staff and law enforcement teams.

(c) Surveillance Impact Report and Surveillance Technology Policy. The Airport submitted a Surveillance Impact Report and draft Surveillance Technology Policy for the Airport GDS to COIT. A copy of the Surveillance Impact Report is in Board File No. 230895.

(d) Public Hearings. Between May 27, 2022 and October 20, 2022, COIT and its PSAB conducted three public hearings at which they considered the Surveillance Impact Report and the draft Surveillance Technology Policy for the Airport GDS ("Airport GDS Policy").

(e) COIT Recommendation. On October 20, 2022, COIT voted to recommend the Airport GDS Policy to the Board for approval.

(f) Findings. The Board hereby finds that the benefits that the Airport GDS Policy authorizes outweigh the costs and risks; that the Airport GDS Policy will safeguard civil liberties and civil rights; and that the uses and deployments of Airport GDS as set forth in the Airport GDS 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 hereby approves the Airport GDS Policy.

Section 5. 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/ Julie Veit
JULIE VEIT
Deputy City Attorney

n:\legana\as2023\2300401\01696860.docx

FILE NO. 230895

# LEGISLATIVE DIGEST

[Administrative Code - Approval of Airport Surveillance Technology Policies.]

**Ordinance approving Airport Surveillance Technology Policies governing the use of 1) Application Based Commercial Transport Technology, 2) Electronic Toll Readers, and 3) a Gunshot Detection Solution; and making required findings in support of said approvals.**

## 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 May 2022, 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 draft Surveillance Technology Policies for the following Surveillance Technology:

(1) Application-Based Commercial Transport Technology
(2) Electronic Toll Readers
(3) Gunshot Detection Solution

Following those hearings, COIT approved final drafts of the Surveillance Technology Policies for these Airport Surveillance Technologies. The Surveillance Technology Policies that COIT developed are detailed in Sections 2 through 5 of the proposed ordinance. The Surveillance Technology Policies are available in Board File No. _____. COIT recommends that the Board of Supervisors approve each 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
Jillian Johnson, Director, Committee of Information Technology

Date: May 2, 2023

Subject: Legislation introduced to approve Surveillance Technology Policy for the Airport's Application Based Commercial Transport, Electronic Toll Readers, and Gunshot Detection Solution

---

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 Surveillance Technology Policy for the Airport's Application Based Commercial Transport, Electronic Toll Readers, and Gunshot Detection Solution.

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 3 public meetings for Application Based Commercial Transport between July and November 2022, 2 public meetings for Electronic Toll Readers between January and February 2023, and 3 public meetings for Gunshot Detection Solution between May and October 2022 to review and approve the 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 Jillian Johnson, Director of the Committee on Information Technology (COIT).

## Application Based Commercial Transport

| Department | Authorized Uses |
|---|---|
| Airport | 1. Plan and execute more effective and strategic campaigns across social media platforms.<br>2. Invoice Transportation Network Companies (TNCs) for trip fees based on their passenger pick-ups and drop-offs at the Airport and perform invoice reconciliation.<br>3. Monitor and enforce TNCs' compliance with the conditions of their operating permit and the R&Rs.<br>4. Provide support for the issuance of citations for traffic violations by the SFPD Airport Bureau.<br>5. Support Public Safety by ensuring only authorized and approved drivers and vehicles are allowed to service passengers at SFO. |

## Electronic Toll Readers

| Department | Authorized Uses |
|---|---|
| Airport | 1. Process parking transactions.<br>2. Investigation of parking transaction disputes. |

## Gunshot Detection Solution

| Department | Authorized Uses |
|---|---|
| Airport | 1. Detect the sound of gun shots, aggressive voices, glass breaking, and unusual disturbances (based upon decibel level) and use of device sensors to locate the origin of the sounds.<br>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.<br>3. Upon a GSD 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. |

Application Based Commercial Transport Public Meeting Dates

| **Application Based Commercial Transport** | |
|---|---|
| **Date** | **Meeting** |
| July 8, 2022 | Privacy and Surveillance Advisory Board (PSAB) |
| August 26, 2022 | Privacy and Surveillance Advisory Board (PSAB) |
| November 17, 2022 | Committee on Information Technology (COIT) |

Electronic Toll Readers Public Meeting Dates

| **Electronic Toll Readers** | |
|---|---|
| **Date** | **Meeting** |
| January 27, 2023 | Privacy and Surveillance Advisory Board (PSAB) |
| February 16, 2023 | Committee on Information Technology (COIT) |

Gunshot Detection Solution Public Meeting Dates

| **Gunshot Detection Solution** | |
|---|---|
| **Date** | **Meeting** |
| May 27, 2022 | Privacy and Surveillance Advisory Board (PSAB) |
| July 8, 2022 | Privacy and Surveillance Advisory Board (PSAB) |
| October 20, 2022 | Committee on Information Technology (COIT) |

COIT recommends the following action be taken on the policy:

- Approve the Application Based Commercial Transport, Electronic Toll Readers, and Gunshot Detection Solution Surveillance Technology Policy for the Airport.

San Francisco International Airport

August 11, 2023

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: Surveillance Technology Policies are 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 Surveillance Technology Policies, 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:

- Board of Supervisors Resolution;
- COIT Recommendation Memorandum;
- Approved Airport Commission Resolution No. 23-0103;
- Memorandum accompanying Airport Commission Resolution No. 23-0103; and
- COIT-Approved Surveillance Technology Policies:
  - Application Based Commercial Transport (ABCT)
  - Electronic Toll Readers (ETR)
  - Gunshot Detection Solution (GDS)

Please contact Cathy Widener, Chief External Affairs Officer at (650) 821-5023 if you have any questions or concerns regarding this matter.

Very truly yours,

*Kantrice Ogletree/s/*

Kantrice Ogletree
Director of Commission Affairs & Commission Secretary



Post Office Box 8097 San Francisco, California 94128 Tel 650.821.5000 Fax 650.821.5005 www.flysfo.com

# Surveillance Technology Policy

Application Based Commercial Transport (ABCT)
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 Application Based Commercial Transport (ABCT) technology itself as well as any associated data, and the protection of City and County of San Francisco residents' civil rights and liberties.

**PURPOSE AND SCOPE**

The Department's mission is to

We provide an exceptional airport in service to our communities.

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

This Policy applies to all to department personnel that use, plan to use, or plan to secure Application Based Commercial Transport (ABCT) technology, including employees, contractors, and volunteers. Employees, consultants, volunteers, and vendors while working on behalf of the City with the Department are required to comply with this Policy.

**POLICY STATEMENT**

The authorized use of Application Based Commercial Transport (ABCT) technology for the Department is limited to the following use cases and is subject to the requirements listed in this Policy.

*Authorized Use(s):*

| |
|---|
| – *Invoice Transportation Network Companies (TNCs) for trip fees based on their passenger pick-ups and drop-offs at the Airport and perform invoice reconciliation.* |
| – *Monitor and enforce TNCs' compliance with the conditions of their operating permit and the R&Rs.* |
| - *Provide support for the issuance of citations for traffic violations by the SFPD Airport Bureau.* |
| – *Support Public Safety by ensuring only authorized and approved drivers and vehicles are allowed to service passengers at SFO.* |

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**

Application Based Commercial Transport (ABCT) technology supports the Department's mission and provides important operational value in the following ways:

The ABCT creates a system through which the Airport can receive data from Transportation Network Companies (Uber, Lyft, Wyngz) regarding their drivers' activity at the Airport, which the Airport uses to: (1) invoice TNCs for trip fees for passenger pickups and drop offs; (2) monitor and enforce TNCs' compliance with the conditions of their operating permits and the Airport Rules and Regulations (R&Rs); (3) support the issuance of citations for traffic violations issued by the SFPD Airport Bureau; and (4) for general transportation planning.

In addition, Application Based Commercial Transport (ABCT) technology promises to benefit residents in the following ways:

| | Benefit | Description |
|---|---|---|
| ☐ | Education | |
| X | Community Development | Equitable distribution of and access to transportation. |
| ☐ | Health | |
| X | Environment | Traffic patterns and congestion within SFO. |
| ☐ | Criminal Justice | |
| X | Jobs | TNC companies and driver's; Ground Transportation Unit (GTU) resources. |
| ☐ | Housing | |
| X | Public Safety | Reduces risk of fraud and unethical business practices. |
| ☐ | Other: | Passenger Preference for this type of ground transportation. |

Application Based Commercial Transport (ABCT) technology will benefit the department in the following ways:

| | Benefit | Description |
|---|---|---|
| X | Financial Savings | Not having to hire additional staff to manually monitor and manage the TNC's activities. |
| X | Time Savings | Staff can reconcile monthly invoices quickly with the use of aggregated data, saving dozens of hours per month of accounting time. |
| | Staff Safety | |
| X | 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. |
| X | Other: Enforcement of non-compliant drivers | Improved enforcement of 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. |

To achieve its intended purpose, Application Based Commercial Transport (ABCT) (hereinafter referred to as "surveillance technology") works in the following way: The ABCT technology works by defining a perimeter, or "geofence," around the Airport using geographic coordinates. Using these coordinates, TNCs, which collect data about the activity of their on-duty drivers through the TNC app on the drivers' mobile device, parse out certain data regarding driver activity within the geofence. The TNCs send this data, along with the license plate number they have on record for the driver's vehicle, to a third-party platform, which in turn relays it to SFO in real time. The selected data is of the TNC driver's commercial driving activity only after entering the Airport's geo-fence, not personal driving activity, and no passenger information is included. Through the ABCT mobile app, SFO staff members, including SFPD officers assigned to the Airport Bureau, can monitor TNC drivers' activity for compliance with Airport Rules and Regulations and the conditions of the TNC's operating permit. Fines can be levied against TNCs for driver activities such as exceeding curbside staging times, or for dropping off and picking up at non-designated areas. SFPD officers can also issue citations to the drivers based on violations of state and local law. The third-party platform that originally receives the data from the TNCs, the Airport Research and Development Foundation (ARDF), uses it to invoice and collect trip fees from the TNCs on the Airport's behalf.

**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 type(s):

| *Data Type(s)* | *Format(s)* | *Classification* |
|---|---|---|
| GPS Location Data | JSON, XML, Relational Database Management System (RDBMS), CSV | Level 2 |
| Data regarding entering and exiting of the SFO geofence | JSON, XML, Relational Database Management System (RDBMS), CSV | Level 2 |
| Vehicle license plate number | JSON, XML, Relational Database Management System (RDBMS), CSV | Level 2 |

Note: All the following Data Types are Classified Level 2 - Internal Use (based upon the City's Data Classification Standard.)

Data Types:

- UID (Unique ID created by the TNC through concatenation of its Driver ID and Trip ID. TNCs perform this concatenation to maintain the confidentiality of the driver's identity.
- TNC ID (a five-digit unique integer assigned to each TNC operating at SFO.)
- License Plate (Seven-character or less, numerical and alphabetic, that represents the vehicle license plate. Accepts an empty String value if there hasn't been a license plate assigned yet.)
- Timestamp (The current time of the event or "ping" expressed in ISO 8601 combined date and time in UTC using 24-hour clock.)
- Transaction Type (The four types of events or "pings" as defined in the national standard in the terms and conditions of the system: "DROP-OFF", "PICK-UP", ENTER", "EXIT".)
- Ride Count (Number of active TNC rides in the vehicle following the transaction event/ping.)
- Longitude (The longitude coordinate in WGS84 of the event or "ping" expressed as a positive or negative number. For locations in North America, this will always be a negative number. This value should have a minimum precision of six decimal places.)
- Latitude (The latitude coordinate in WGS84 of the event or "ping" expressed as a positive or negative number. For locations in North America this will always be a positive number. This value should have a minimum precision of six decimal places.)

Notification: Departments shall notify the public of intended surveillance technology operation at the site of operations through signage in readily viewable public areas. Department notifications shall identify the type of technology being used and the purpose for such collection. The ABCT Technology's collection of selected data from the TNC's is a requirement of the contractual Operating Permit between the Airport and the TNC's.

Department includes the following items in its public notice:

X Information on the surveillance technology

☐ Description of the authorized use

X Type of data collected

☐ Will persons be individually identified

☐ Data retention

☐ Department identification

☐ Contact information

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

- The requestor must submit a request to a data steward (within an SFO Business Unit) for the location data. The data steward obtains the user's requirements for data and its format for an authorized use. The data steward confirms end-user authorization and signals technical staff (SFO ITT) to retrieve and send data to the requestor through a secure channel if necessary.

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:

- Airport Planners (5200 series)
- Administrative Analysts (1840; 1842;1844)
- Information Systems Business Analysts (1052;1053;1054)
- Information Systems Engineers (1042;1043;1044)
- Information Systems Project Directors (1070)
- Sworn members of the SFPD assigned to the Airport Bureau:
  Police Officer (Q002/003/004)
  Sargent (Q50/51/52)

*B. Members of the public, including criminal defendants*

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

Collected data that is classified as Level 1-Public data may be made available for public access or release via DataSF's Open Data portal. 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:

- Technical Safeguards: Secure network, password-protected systems, encryption of data where necessary.
- Physical Safeguards: There are physical access restrictions for each server room containing database systems (i.e., badge access, locked door).

Data Sharing: The Department will endeavor to ensure that other agencies or departments that may receive data collected by the Application Based Commercial Transport (ABCT) 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 Department shall ensure proper administrative, technical, and physical safeguards are in place before sharing data with other CCSF departments, outside government entities, and third-party providers or vendors. (See Data Security)

The Department 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.

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

The Department currently participates in the following sharing practices:

A. Internal Data Sharing

Department shares the following data with the recipients:

| **Type** | **Recipient** |
|---|---|

| | |
|---|---|
| The limited data that is displayed in the ABCT mobile app listing TNC driver activity within the geofence. | SFPD Airport Bureau |
| Raw data for TNC operations at Airport. | City Attorney's Office |

Data sharing occurs at the following frequency:

The SFPD-AB Officers who have access to the ABCT app, can access the data daily, as needed to perform their job function.

For the City Attorney's Office, a limited dataset provided upon request. This has occurred less than 10 times in the past year.

B. External Data Sharing

Department shares the following data with the recipients:

| **Type** | **Recipient** |
|---|---|
| Raw data for TNC operations at Airport. | TNC's (e.g., Uber, Lyft, etc.) |

Data sharing occurs at the following frequency:

As needed for billing and administrative/operational compliance, including fines.

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

The Department does not share raw data unless they are employees, contractors or consultants under contract with a legitimate business need for such data. Data will not be shared externally or publicly, unless legally requested through the Sunshine Ordinance or the CA Public Records Act, or if requested by universities, consultants, or other transportation agencies. All shared information will be aggregated or redacted and only datasets limited to the requestor's request will be provided. As per the Public Domain Dedication and License (PDDL), public data is provided for on an "as is" basis and for informational purposes only. The Department and City make no warranty, representation, or guaranty of any type as to the completeness, accuracy, content, or fitness for any particular purpose or use of any public data set made available, nor shall any warranties be implied with respect to the data provided. The Department and City ask that recipients of publicly released data follow the Terms of Use published on DataSF's website.

Before data sharing with any recipient, 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 Evaluate 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.

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

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

| **Retention Period** | **Retention Justification** |
|---|---|
| SFO keeps data according to the retention policies established by the Department and approved by the Airport Commission (i.e.,Executive Directive 18-05) as well as, applicable legislation. When multiple retention standards apply, SFO utilizes the most restrictive legislation for each class of data. Permittees and vendors are required to retain data for the time period specified by legislation and permit conditions. Retention time periods vary by mobility program. ABCT data is currently maintained permanently in the Airport's AWS environment. | All data will be retained for transportation planning purposes, enforcement of operating agreements, regulation of mobility programs, and to ensure equitable distribution of transportation options throughout the Airport. |

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

- Location and license plate data that is used for prosecutorial or investigatory purposes will be retained beyond the stipulated retention period(s). Location data may also be retained for analytical purposes related to aforementioned authorized use cases, including but not limited to, the assessment of trends.

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

Data will be stored in the following location:

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

☐ Department of Technology Data Center

X Software as a Service Product

X Cloud Storage Provider

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

Practices:

- Local data stores are wiped when computers are turned in.

Processes and Applications:

- Not applicable.

Training: To reduce the possibility that surveillance technology or its associated data will be misused or used contrary to its authorized use, all individuals requiring access must receive training on data security policies and procedures.

At the very least, department shall require all elected officials, employees, consultants, volunteers, and vendors working with the technology on its behalf to read and formally acknowledge all authorized and prohibited uses. Department shall also require that all individuals requesting data or regularly requiring data access receive appropriate training before being granted access to systems containing PII.

Training is provided on an as-needed basis due to the low number of staff who have authorized access to such location data, the specialized software needed, the

specialized job skills needed to retrieve and analyze such data, and the business requirements for their roles.

**COMPLIANCE**

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

Currently any changes in these data sets or technical routines that manages this system are controlled through our Change Management Process and documented as such. All access is requested through a formal request and approved by the data stewards. Prior to accessing the data, all authorized staff shall be required to review and agree to Department's Surveillance Technology Policy. Access is role based controlled – access is only provided once approved. At any time, ITT can see who has / who had access to a specific dataset. .

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

- Chief Information Office (0951-54)
- ITT Business Services Manager (0941-43)
- SFO Business Unit Managers (0922-23; 0931-33 & 0941-43)

Sanctions for violations of this Policy include the following:

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

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 <u>not</u> been processed and cleaned of all personal identifiable information. The distribution and use of raw data is tightly restricted. |

| | |
|---|---|
| Exigent Circumstances | An emergency involving imminent danger of death or serious physical injury to any person that requires the immediate use of Surveillance Technology or the information it provides. |

**AUTHORIZATION**

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

**QUESTIONS & CONCERNS**

*Public:*

Complaints or concerns can be submitted to the Department by:

Members of the public can access www.flysfo.com to register complaints or concerns or submit questions via the "Contact Us" web page and form.

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

SFO uses ZenDesk to collect and route inquiries to the appropriate department at SFO.

*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

Electronic Toll Readers - FasTrak
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 FasTrak Electronic Toll Readers (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 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 surveillance technology will be used to support this mission, by describing the intended purpose, authorized and restricted uses, and requirements.

This Policy applies to all to department personnel that use, plan to use, or plan to secure 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):*

| |
|---|
| – Process parking transactions. |
| – Investigation of parking transaction disputes. |

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.

## BUSINESS JUSTIFICATION

**Reason for Technology Use**

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

SFO is committed to efficiently delivering world-class customer service while maximizing revenue opportunities. Use of FasTrak Toll Readers provides:

- The ability to accept an alternate payment method that efficiently processes parking fees.
- 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.
- A uniform methodology for SFO parking fee collection and more effectively quantifies parking demand, which supports future SFO planning.

NOTE: It is the parking customer's decision to sign-up for and use the FasTrak technology as a payment option. Use of FasTrak to pay for parking at the Airport is not required.

**Description of Technology**

- FasTrak transponders are activated by toll readers in designated FasTrak lanes. Individual account information is stored in the transponders. The toll readers identify the individual transponders and validate active accounts.
- During operational hours, the toll reader collects the transponder tag number, as well as the time, date, and location of tag. Customers can avoid having their transponder tag number collected by placing the transponder tag in the mylar bag in which the tag was first obtained by the customer.
- Upon exiting the parking facility, the parking fee amount is calculated and billed to the Bay Area Toll Authority (BATA) who in turn charges the FasTrak customer. Transponders are only read in designated FasTrak Entry and Exit lanes.
- The transponder information is transferred from the toll reader to the toll reader provider's central database.
- If the account is in good standing, the parking fee amount is billed to the Bay Area Toll Authority who in turn deducts from the customer's prepaid account.
- If the Entry and Exit lanes have gates, the gates open.
- The electronic system records each parking transaction, including the time, data, location, and parking charge of each vehicle.

**Resident Benefits**

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

| | Benefit | Description |
|---|---|---|
| ☐ | Education | |
| ☐ | Community Development | |

| | |
|---|---|
| ☐ | Health |
| ☐ | Environment |
| ☐ | Criminal Justice |
| ☐ | Jobs |
| ☐ | Housing |
| X | Other |

• Public Safety – More efficient payment systems for customers reduce traffic congestion and bottlenecks, decreasing the likelihood of collisions and improving customer safety.

• Other – Convenience; limits parking congestion through more efficient payment processes.

**Department Benefits**

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

| | Benefit | Description |
|---|---|---|
| X | Financial Savings | Low maintenance and operating costs, in addition to minimal training of personnel on the use of the technology. |
| X | Time Savings | Parking fee collections are much more efficient. |
| X | Staff Safety | Staff no longer need to sit in parking booths that are near fast-moving vehicles. |
| X | Data Quality | Provides a uniform methodology for SFO parking fee collection and more effectively quantifies parking demand, which supports future SFO planning. |
| ☐ | Other | |

## POLICY REQUIREMENTS

This Policy defines the responsible data management processes and legally enforceable safeguards required by the Department to ensure transparency, oversight, and accountability measures. Department use of surveillance technology and information collected, retained, processed or shared

by surveillance technology must be consistent with this Policy; must comply with all City, State, and Federal laws and regulations; and must protect all state and federal Constitutional guarantees.

**Specifications:** The software and/or firmware used to operate the surveillance technology must be 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 Images | MOV | Level 3 |
| Still Images | Downloaded as PDFs | Level 3 |
| Transaction Details (time and date stamp, location, toll charge) | Plain Text | Level 2 |
| Toll Tag Number | Plain Text | Level 3 |

**Notification:** Airport shall notify the public of surveillance technology operation by posting the technology policy on the external agency website, FLYSFO.com. Department notifications shall identify the type of technology being used and the purpose for such collection.

Department includes the following items in its public notice:

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

There is also signage in the Airport's parking facilities designated exit lanes where FasTrak is accepted as a payment option.

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

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. The data steward will review the reason to ensure it aligns with the authorized use and the requesting personnel's work function. The requesting personnel must have completed the required privacy and security training prior to access.

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.

***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:

- 1657 Accountant IV
- 0922 Manager I
- 0923 Manager II
- 0932 Manager IV

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

- FasTrak
- New South Parking
- Scheidt & Bachmann

***B. 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:

Privacy and security training are required for employees with access to PII, upon hire or assignment to projects involving electronic toll readers. In addition, regular periodic refresher training is required for those employees.

**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:

Data can only be accessed through the Parking Access and Revenue Control System (PARCS) application. Users must provide unique computer login credentials such as username and password to access the data. Passwords must comply with the City and County of San Francisco cyber security requirements.

Administrative:
• Access to Personally Identifiable Information ("PII") and Payment Card Industry ("PCI") Information is limited only to certain operations and technical employees for limited, approved purposes based on their specific work responsibilities.
• Privacy and security training is required for employees with access to PII, upon hire or assignment to projects involving toll readers. In addition, regular periodic refresher training is required for those employees.

Technical:
• Servers and network perimeters are protected with firewalls and are continuously monitored.

• Databases are implemented to ensure PII is segregated from aggregate information. Data is aggregated into a non-identifiable format before sharing.
• Internal and external audits of perimeter and software code security are conducted.

Physical:
• All network equipment and servers containing sensitive data are maintained in a secured location accessible only to Airport badged, authorized personnel.

**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.)
- ☐ Department of Technology Data Center
- ☐ 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, scrub faces, and ensure all PII is removed in accordance with the department's data policies.
- Review of all existing safeguards to ensure shared data does not increase the risk of potential civil rights and liberties impacts on residents.
- Evaluation of what data can be permissibly shared with members of the public should a request be made in accordance with the San Francisco's Sunshine Ordinance.
- Ensure data will be shared in a cost-efficient manner and exported in a clean, machine-readable format.

***A. Internal Data Sharing:***

The department shares surveillance technology data with other departments or entities inside the City and County of San Francisco, as follows:

- City Attorney's Office
- Law Enforcement: SFPD – AB

***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 |
|---|---|
| - Transaction details (time and date stamp, location, toll charge)<br>- Toll Tag Number | - FasTrak CSC contractor (Third-party service provider)<br>- San Mateo County Sheriff |

**Frequency -** Data sharing occurs at the following frequency:

The third-party service provider is provided with relevant data in order to verify FasTrak transactions in processing customer disputes. The department requires the third-party to maintain the confidentiality of the information and to use it only as necessary to perform their duties in connection to the toll readers.

PII will not be disclosed to any other third party, except as required to comply with laws or legal processes served on the department.

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

The Airport has strict contractor agreements with all third-party providers that clearly state the conditions for data disclosure to the third-party, including acceptable and prohibited uses by the third-party, required protections and safeguards, and reporting procedures requiring third-party providers to disclose their compliance with established contractor agreements.

**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 |
|---|---|
| FasTrak data retention = 4.5 years | Required by the Bay Area Toll Authority |

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):

PII required to comply with laws or legal processes served on the Airport will be retained longer than the stated 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:

- Practices: Through its contractor, the department shall discard all PII no more than four years and 6 months after the date the PII is collected.
- Processes and Applications: PII is converted to a non-identifiable format and aggregated. Aggregated data does not contain information that could be used to contact or identify individual customers.

## COMPLIANCE

### Department Compliance

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

Staff from parking operator New South Parking and parking equipment provider Scheidt & Bachmann will be assigned to maintain updates and perform required maintenance. Compliance with the Surveillance Technology Policy will be self-assessed and reported on regularly by SFO Parking Management via the department's Annual Surveillance Report. The department will also positively respond and amend appropriate recommendations detailed in the annual Audit prepared by the Controller's Office of the City Service Auditor.

### 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:

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

### Oversight Personnel

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

- 1823 Senior Administrative Analyst
- 0922 Parking Operations Manager
- 0932 Airport Parking Manager

### Sanctions for Violations

Sanctions for violations of this Policy include the following:

- First offence: Violator shall be verbally notified by Airport management of nature of violation.
- Second offence: Violator shall be notified in writing of second offence and privileges to access toll readers and associated data shall be suspended for 60 days.
- Third offence (following reinstatement of operator privileges): Violator shall be permanently banned from Toll Reader operations and disciplinary action may be taken depending upon the severity of second/third offences.

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

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

## EXCEPTIONS

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

## DEFINITIONS

| | |
|---|---|
| Personally Identifiable Information: | Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. |
| 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**

Members of the public may submit complaints or concerns via phone, mail or online submission through the Contact SFO portal (https://www.flysfo.com/contact-sfo). Submissions are reviewed by Airport Guest Services team regularly and forwarded to the Airport stakeholder responsible for handling, as necessary. Additionally, Airport Commission holds bi-monthly public meetings where the public may register complaints or concerns during the Public Comment section of the calendared agenda.

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

The Airport will review and respond to constituent calls and complaints within 3 business days. Airport management shall review complaints received on a quarterly basis to discuss best practices, evaluate for lessons learned and opportunities to improve and refine the toll reader program based on caller complaints, concerns, and other community feedback.

**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.

# Surveillance Technology Policy

San Francisco International Airport
Gunshot Detection Solution

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 the Department's gunshot detection solution itself, as well as any associated data, and the protection of members of the public who visit the Airport and all those who work at the Airport.

## PURPOSE AND SCOPE

The Surveillance Technology Policy ("Policy") defines the manner in which the gunshot detection solution will be used to support department operations.

This Policy applies to all department personnel that use, plan to use, or plan to secure the gunshot detection solution, 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 Airport will limit its use of the gunshot detection solution (GSD) to the following authorized use cases and requirements listed in this Policy.

*Authorized Use(s):*

1. Detect the sound of gun shots, aggressive voices, glass breaking, and unusual disturbances (based upon 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 GSD 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.

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

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.

## BUSINESS JUSTIFICATION

The gunshot detection solution supports the Airport's Core Value of "Safety and Security is our first priority" and provides important operational value in the following ways:

The gunshot detection solution is an alert system designed to provide real-time notification and information regarding incidents that potentially threaten the public safety, such as an indoor active shooter incident, aggression, glass break or unusual disturbances. As a result, first responders arrive on scene faster, equipped with the vital information needed to contain threats and mitigate casualties. The gunshot detection solution provides immediate and accurate response for Airport Commission staff and law enforcement teams.

In support of Department operations, the gunshot detection solution promises to help with:

| | | |
|---|---|---|
| ☐ | Education | |
| ☐ | Community Development | |
| X | Health | Protect safety of staff, patrons, and facilities while promoting an open and welcoming environment. |
| ☐ | Environment | |
| X | Criminal Justice | 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. |
| ☐ | Jobs | |
| ☐ | Housing | |
| X | Other | Improved protection of the public and city assets by leveraging remote condition assessment technology, which improves the 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. |

In addition, the following benefits are obtained:

| Benefit | | Description |
|---|---|---|
| | Financial Savings | The gunshot detection solution (GSD), 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. |
| X | 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. |
| X | 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. |
| X | Data Quality | The identification of ambient noise from GSD coupled with CCTV cameras use, provides Law Enforcement complete situational awareness. |
| X | Service Levels | The gunshot detection solution will enhance effectiveness of incident response by allowing First Responders to arrive more promptly to the scene, resulting in an 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 be consistent with all state and federal Constitutional guarantees.

Specifications: The software and/or firmware used to operate the gunshot detection solution surveillance technology must be kept 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 types:

| *Data Type(s)* | *Format(s)* | *Classification* |
|---|---|---|

| | | |
|---|---|---|
| Alarm<br>• Date<br>• Time<br>• Geolocation<br>• Noise level | MP4 or other format | Level 2 |
| Geolocation data | TXT, CSV, DOCX | Level 2 |

| | | |
|---|---|---|
| **Data Class:**<br>**Level 2 =** Internal Use | **Description:**<br>Data intended for release on a need-to-know basis. Data regulated by privacy laws or regulations or restricted by a regulatory agency or contract, grant, or other agreement terms and conditions. | **Potential Adverse Impact:**<br>Low |

Notification: The notice requirements in Administrative Code Section 19.5 do not apply to the Airport.

However, the Airport will publish a public notice on its external website at www.flysfo.com regarding the use of this surveillance technology.

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 (who must have a current Airport ID Badge)

receive training in system access and operation, and instruction regarding authorized and prohibited uses.

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 shared with a third party. This log will include, but is not limited to, the following: date/time data was originally obtained/collected, department requesting data, date/time of access of raw data, outcome of data processing, as well as, the date processed data was delivered to users.

Data Sharing:

The Department will endeavor to ensure that other City agencies or departments that may receive data collected by their own Security Camera Systems will act in conformity with this Surveillance Technology Policy.

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

Before sharing data with any recipients, the Department will use the following procedure to ensure doing so is consistent with the policy:

| | |
|---|---|
| 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 | 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 members of the public. |
| 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, the California Public Records Act, and the various federal, state and local laws protecting privacy. |
| 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 the federal, state, and local laws protecting an individual's right to privacy.

The Department may share data from the Gunshot Detection System with the following entities:

*A. Internal Data Sharing:*

In the event of an incident, data from the Gunshot Detection System and views from the Airport's CCTV may be shared by alternative methods to the following agencies:

-Within the Department on a need-to-know basis
- SFPD
- SF City Attorney

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

*B. External Data Sharing:*

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

- Other law enforcement agencies:
  - San Mateo County District Attorney
  - San Mateo County Sheriff's Office
  - DHS/TSA
  - FBI
  - other local, state and federal law enforcement agencies if required by law
  - 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 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 manages its records and should be consistent with any relevant Federal Emergency Management Agency (FEMA) or California Office of Emergency Services (Cal OES) sections.

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

- Security Camera data will be stored for a minimum of one (1) year per State law 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: Per the Airport's Record Retention and Data Destruction Policy (ED 18-05) and the statutes referenced within, which are in

compliance with State law, requiring security camera footage be retained for one year. 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:

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:<br>- 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.<br>- Annual cybersecurity training (COIT Policy Link) |

**COMPLIANCE**

Department shall oversee and enforce employee compliance with this Policy in accordance with the Memoranda of Understanding of the labor organization representing employee.

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

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

**DEFINITIONS**

| | |
|---|---|
| Personally Identifiable Information: | Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. |

**AUTHORIZATION**

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

**Appendix A: Department Specific Responses**

1. A description of the product, including vendor and general location of technology.

   The AmberBox gunshot detection solution is a detection and response system designed to protect lives in an indoor active shooter, aggressive behavior, glass break and unusual disturbance incidents (based upon artificial intelligence employing machine learned decibel level). Specifically, the GDS listens for the ambient (normal) noise within the Airport buildings (i.e., terminals, Commission office buildings) and sets a baseline decibel level for the buildings to eliminate false alarms by only detecting and notifying when the baseline decibel level is exceeded and detected by multiple device sensors.

   By automating the notification process, First Responders arrive on scene faster, equipped with the vital information needed to contain threats and mitigate casualties. The AmberBox gunshot detection solution provides immediate and accurate response for internal and law enforcement teams.

   The AmberBox gunshot detection solution offers an advanced sensing system, ensuring maximum protection from threats. Shots are detected through percussion and infrared sensors, that analyze the binodal signature of a gunshot. Combined with AmberBox's gunshot detection solution's algorithm, false alarm sources are virtually eradicated. All analysis is conducted at the sensor (detector), with no real-time audio transmitted or recorded, ensuring privacy.

   The Proof of Concept, Phase I, will require the deployment of 25 sensors in the Consolidated Airport Campus Building 674. The sensors will be connected to the Aruba Wi-Fi system on the 1st floor (lobby area), as well as, throughout the 4th floor. In Phase II, the sensors will be deployed both pre- and post-security throughout the terminals, as well as the Airport buildings throughout the campus.

   The Airport uses Verint Video Management Software (VMS), and primarily, Pelco Analog/Digital Pan-Tilt-Zoom (PTZ) and fixed cameras. The cameras are installed in public areas of the Airport.

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

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

   - *9202 911 Dispatcher*
   - *9203 911 Dispatch Supervisor*
   - *9212 Security Operations Center (SOC) Analyst*

- *9213 Airfield Safety Officer*
- *9220 SOC Supervisor*
- *9221 Airport Operations Supervisor*

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

   *Public questions and complaints can be submitted via the:*

   - *Airport Guest Services (Contact SFO)*
   - *Airport public email, phone, or website ((Contact SFO), or*
   - *Airport Commission meetings (How to Address the Commission)*

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

   *CCTV data is in a local server for 45 days; then video files are transferred to Amazon Web Services (AWS) for minimum one year. Files are deleted after 320 days based on the lifecycle policy in AWS.*

5. Is a subpoena required before sharing with law enforcement?

   - No

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.<br><br>**STATUS:** POLICY APPROVED<br>7/27/21 – Board passed<br>8/4/21 – Mayor approved | 1. Live Monitoring<br>2. Recording of video and images in the event of an incident.<br>3. Reviewing camera footage.<br>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:**<br>- Health: Protect Safety of Staff, patrons, and facilities while promoting an open and welcoming environment.<br>- 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.<br><br>**Civil Rights Impacts and Safeguards:**<br>- The Airport's use of CCTV is restricted to those identified Authorized Use Cases.<br>- The Airport retains CCTV footage for one year, consistent with State law.<br>- 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.<br><br>**Fiscal Analysis of Costs and Benefits:**<br>- 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.<br>- Staff Security: Security cameras provide advance view of an incident to better prepare those responding to an incident.<br>- 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.<br><br>**STATUS:** POLICY APPROVED<br>7/27/21 – Board passed<br>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.<br>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:**<br>- 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.<br>- Criminal Justice: ALPR-GTMS can be used to support identification of vehicles as a part of law enforcement investigations.<br>- 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:**<br>- 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.<br>- 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.<br><br>**Fiscal Analysis of Costs and Benefits:**<br>- 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.<br>- 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).<br>- 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.<br><br>**STATUS:** POLICY APPROVED<br>11/15/22 – Board passed<br>11/17/22 – Mayor approved | 1. Reviewing camera footage in the event of an incident.<br>2. Approving Tenant's disclosure of digital recordings and other data from its security camera system. | **For Residents:**<br>- Health: Protect Safety of staff, patrons, and facilities while promoting an open and welcoming environment.<br>- 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.<br>- Financial Savings: Equipment is owned and operated by a non-city entity.<br>- 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:**<br>- Airport's use of recordings and data from third-party security cameras is restricted to the identified Authorized Use Cases.<br>- 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.<br>- 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.<br>- 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).<br><br>**Fiscal Analysis of Costs and Benefits:**<br>- 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.<br>- 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.<br>- 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.<br><br>• 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.<br><br>2. To monitor and enforce TNCs' compliance with the conditions of their operating permit and the Airport's Rules & Regulations (R&Rs).<br><br>3. To provide support for the issuance of citations for traffic violations by the SFPD Airport Bureau.<br><br>4. To support Public Safety by ensuring only authorized and approved drivers and vehicles are allowed to service passengers at SFO. | **For Residents:**<br><br>Community Development: Equitable distribution of and access to transportation.<br><br>Environment: Traffic patterns and congestion within SFO.<br><br>Jobs: TNC companies and driver's; Ground Transportation Unit (GTU) resources.<br><br>Public Safety: Reduces the risk of fraud and unethical business practices.<br><br>**Civil Rights Impacts and Safeguards:**<br>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).<br>- To avoid discrimination and other potential civil rights impacts, data access is granted only to authorized users for authorized uses.<br>- 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.<br>- 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.<br><br>**Fiscal Analysis of Costs and Benefits:**<br>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.<br><br>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.<br><br>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.<br><br>2. Investigation of Parking Transaction Disputes. | **For Residents:**<br>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.<br><br>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.<br><br>Convenience: Limits parking congestion through more efficient payment processes.<br><br>**Civil Rights Impacts and Safeguards:**<br>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.<br><br>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.<br><br>Privacy and security training is required for employees with access to Personally Identifiable Information (PII), upon hire or assignment to projects involving toll readers.<br><br>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.<br><br>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.<br><br>**Fiscal Analysis of Costs and Benefits:**<br><br>Financial Savings: Low maintenance and operating costs in addition to minimal training of personnel on the use of the technology.<br><br>Time Savings: Parking fee collections are much more efficient.<br><br>Staff Safety: Staff no longer need to sit in parking booths that are near fast moving vehicles.<br><br>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:**<br>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.<br><br>• 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.<br>• The gunshot detection system will use existing Wi-Fi access points owned and deployed by the Airport.<br>• 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.<br>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.<br>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.<br><br>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:**<br><br>The Airport's use of the AmberBox solution is restricted to those identified Authorized Use Cases.<br><br>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.<br><br>**Fiscal Analysis of Costs and Benefits:**<br><br>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.<br><br>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*

# Surveillance Impact Report

Application Based Commercial Transport (ABCT)
Airport

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 Application Based Commercial Transport (ABCT) technology.

## DESCRIPTION OF THE TECHNOLOGY

The Department's mission is the following:

We provide an exceptional airport in service to our communities.

In line with its mission, the Department uses Application Based Commercial Transport (ABCT) technology to receive data from Transportation Network Companies (TNCs) regarding their drivers' activity at the Airport, which the Airport uses to: (1) invoice TNCs for trip fees for passenger pickups and drop offs; (2) monitor and enforce TNCs' compliance with the conditions of their operating permits and the Airport Rules and Regulations (R&Rs); (3) support the issuance of citations for traffic violations issued by the SFPD Airport Bureau; and (4) for general transportation planning.

The Department shall use Application Based Commercial Transport (ABCT) technology only for the following authorized purposes:

*Authorized Use(s):*

- *Invoice TNCs for trip fees based on their passenger pick-ups and drop-offs at the Airport and perform invoice reconciliation.*
- *Monitor and enforce TNCs' compliance with the conditions of their operating permit and the R&Rs.*
- *Provide support for the issuance of citations for traffic violations by the SFPD Airport Bureau.*
- *Support Public Safety by ensuring only authorized and approved drivers and vehicles are allowed to service passengers at SFO.*

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

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

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

ABCT is located on the  cloud of the third party platform that initially receives the data from the TNCs, Airport Research and Development Foundation (ARDF is a wholly owned subsidiary of AAAE).,and on premises at the Airport. The Airport's on-premises systems are comprised of a private cloud and on-premises hardware.

**Technology Details**
The following is a product description:

The ABCT app provides a real-time look into TNC traffic at an airport.  This eliminates guessing how many rides happen daily or where the activity is occurring.

The ABCT service provides more than just reporting activity stats.  The ABCT technology reconciles an airport's totals against the self-reported documents to ensure an airport is properly compensated for the amount of traffic and processes payments each month, helping make the process smoother for the  many airport departments involved.

The ABCT mobile app gives airport curbside personnel the ability to check activity happening at the airport right from their phone or tablet.

Since each airport is unique with distinctive ground transportation challenges, the ABCT technology supports custom reporting features to fulfill each airport's unique need.

A. How It Works

To function, Application Based Commercial Transport (ABCT) works in the following way:  The ABCT technology works by defining a perimeter, or "geofence," around the Airport using geographic coordinates.  Using these coordinates, TNCs, which collect data about the activity of their on-duty drivers through the TNC app on the drivers' mobile device, parse out certain data regarding driver activity within the geofence.  The TNCs send this data, along with the license plate number they have on record for the driver's vehicle, to a third-party platform, which in turn relays it to SFO in real time. The selected data is of the TNC driver's commercial activity, not personal driving activity, and includes no passenger information.  Through the ABCT mobile app, SFO staff members, including SFPD officers assigned to the Airport Bureau, can monitor TNC drivers' activity for compliance with Airport Rules and Regulations and the conditions of the TNC's operating permit.  Fines can be levied against TNCs for driver activities such exceeding curbside staging times, or for dropping off and picking up at non-designated areas.  SFPD officers can also issue citations to the drivers based on violations of state and local law.

The third-party platform that originally receives the data from the TNCs, ARDF, uses it to invoice and collect trip fees from the TNCs on the Airport's behalf.

SFO keeps all the data for historical analysis.

All data collected or processed by Application Based Commercial Transport (ABCT) will be handled or stored by an outside provider or third-party vendor on an ongoing basis.  Specifically, data will be

handled by ARDF (the vendor who licenses the technology) and Amazon Web Services 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 Application Based Commercial Transport (ABCT) has the following benefits for the residents of the City and County of San Francisco:

| | Benefit | Description |
|---|---|---|
| ☐ | Education | |
| X | Community Development | Equitable distribution of and access to transportation. |
| ☐ | Health | |
| X | Environment | Traffic patterns and congestion within SFO. |
| ☐ | Criminal Justice | |
| X | Jobs | TNC companies and driver's; Ground Transportation Unit (GTU) resources. |
| ☐ | Housing | |
| X | Public Safety | Reduces risk of fraud and unethical business practices. |
| ☐ | Other: | Passenger Preference for this type of ground transportation. |

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 International Airport (SFO) strives to mitigate all potential civil rights impacts through responsible technology and associated data use policies and procedures, and intends to use aforementioned data exclusively for aforementioned authorized use cases. All other uses are expressly prohibited.

Specifically, SFO strives to support the civil liberties and freedoms of all persons and strictly prohibits the use of location data to identify or track individual users or customers of the City's Airport transportation system.

To set San Francisco residents' expectation of privacy and 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 SFO Connect web-site (sfoconnect.com).

The SFO implements technical, physical, and administrative safeguards to mitigate potential misuse, abuse, or breach of collected data. 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. Further, server rooms containing database systems are protected by physical access restrictions (i.e. badge access, locked door). The Department also follows data aggregation policies to ensure individuals' data is adequately protected.

To avoid discrimination and other potential civil rights impacts, data access is granted only to authorized users for authorized uses. Any Department personnel requesting access to the data must first submit a request to the Data Steward, specifically for the location data. The Data Steward obtains the user's requirements for data and its format for an authorized use. The Data Steward confirms end user authorization and signals technical staff to retrieve and send data to the requestor through a secure channel if necessary.

The administrative safeguards are the following: 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. Released datasets are limited to the requestor's specific request.

The technical safeguards are the following: 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. The Department also follows data aggregation policies to ensure individuals' data is adequately protected.

The physical safeguards are the following: Specifically, server rooms containing database systems are protected by physical access restrictions (i.e. badge access, locked door).

C. Fiscal Analysis of Costs and Benefits

The Department's use of Application Based Commercial Transport (ABCT) yields the following business and operations benefits:

| | Benefit | Description |
|---|---|---|
| X | Financial Savings | Not having to hire additional staff to manually monitor and manage the TNC's activities. |
| X | Time Savings | Staff can reconcile monthly invoices quickly with the use of aggregated data, saving dozens of hours per month of accounting time.· |
| | Staff Safety | |
| X | 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. |
| X | Other: 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. |

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

| | | |
|---|---|---|
| Number of FTE (new & existing) | *0.5 (IT staff maintaining API and data warehouse)* | |
| Classification | *Principal Information Systems Engineer (1044) / IS Project Director (1070)* | |
| | ***Annual Cost*** | ***One-Time Cost*** |
| Total Salary & Fringe | *$115,000 per* | |
| Software | | |
| Hardware/Equipment | *$25,000* | |
| Professional Services | | |
| Training | | |
| Other | | |
| Total Cost | ***$140,000.00*** | ***None*** |

The Department funds its use and maintenance of the surveillance technology through operating funds and cost recovery through Permit Fees.

## COMPARISON TO OTHER JURISDICTIONS

Application Based Commercial Transport (ABCT) technologies are currently utilized by other governmental entities for similar purposes.

# Surveillance Impact Report

Electronic Toll Readers - FasTrak
San Francisco International Airport

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 FasTrak Electronic Toll Readers, (hereinafter referred to as "surveillance technology").

## PURPOSE OF THE TECHNOLOGY

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

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

In line with its mission, the Department uses FasTrak Electronic Toll Readers to efficiently deliver world-class customer service while maximizing revenue opportunities. Use of Toll Readers provides the ability to accept an alternate payment method that efficiently processes parking fees. Parking efficiency minimizes traffic on SFO's roadways.

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

***Authorized Use(s):***

- Process parking transactions
- Investigation of parking transaction disputes

Any use cases not stated in the Authorized Use Case section are expressly prohibited.

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

Toll readers are located at all public parking garages at SFO.

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

Participating vehicles (i.e., vehicles that have elected the electronic toll payment system), contain a transponder approximately the size of a deck of cards, which is placed on the inside of the car's windshield behind the rearview mirror. Transponders are battery-operated, radio frequency identification (RFID) units that transmit radio signals. The transponder is a two-way radio with a microprocessor, operating in the 900-MHz band. Basic account information, such as an identification number is stored in this RFID transponder.

Electronic toll readers are positioned above each FasTrak entry and exit lane. These toll readers emit radio frequencies that communicate with the transponder. The detection zone of a toll reader is typically 6 to 10 feet (2 to 3 meters) wide and about 10 feet long. These two devices, the transponder and the toll reader, interact to complete the parking transaction.

The transponder information is transferred from the toll reader to the toll reader provider's central database. If the account is in good standing, the parking fee amount is billed to the Bay Area Toll Authority (BATA) who in turn deducts from the customer's prepaid account. If the entry and exit lanes have gates, the gates open. The electronic system records each parking transaction, including the time, date, location, and parking charge for each vehicle.

This is a description of how the technology works:

To function, Electronic Toll Readers FasTrak transponders are activated by toll readers in designated FasTrak lanes. Individual account information is stored in the transponders. The toll readers identify the individual transponders and validate active accounts. Upon exit, the parking fee amount is calculated and billed to the Bay Area Toll Authority (BATA) who in turn charges the FasTrak customer. Transponders are only read in designated FasTrak entry and exit lanes. During operational hours, the toll reader collects the transponder tag number, as well as the time, date, and location of tag. Customers can avoid having their transponder tag number collected by placing the transponder tag in the mylar bag in which the tag was first obtained by the customer.

**Third-Party Vendor Access to Data**

All data collected or processed by the surveillance technology will be handled or stored by an outside provider or third-party vendor on an ongoing basis. Specifically, data will be handled by FasTrak, New South Parking, and Scheidt & Bachmann 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 the surveillance technology has the following benefits for the residents of the City and County of San Francisco:

| | Benefit | Description |
|---|---|---|
| ☐ | Education | |
| ☐ | Community Development | |
| ☐ | Health | |
| ☐ | Environment | |
| ☐ | Criminal Justice | |
| ☐ | Jobs | |
| ☐ | Housing | |
| X | Other: | Public Safety – More efficient payment systems for customers reduce traffic congestion and bottlenecks, decreasing the likelihood of collisions and improving customer safety.<br><br>Other – Convenience; limits parking congestion through more efficient payment processes. |

**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 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.

The limitations of the technology and the safeguards established by the department mitigate the privacy and civil rights concerns associated with it. First, the read range and fixed nature of the toll readers eliminates the risk that they can be used to track an individual's location on an ongoing basis. Data is only collectable from a range of three meters, meaning persons and vehicles cannot be tracked outside of the toll booth or garage area. Further, only information loaded to the toll transponder by the customer will be available for reading by the toll reader. The likelihood that information from other electronic tags inside the vehicle will be picked up is slim to none. Toll readers are adjusted to a unique frequency designed to pick up only the frequency associated with the provider's transponders.

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. Personal information collected by the toll reader and transmitted to the database cannot be accessed without access to the department database. Authorized personnel who conduct regular technical maintenance ensure toll readers remain dialed into the appropriate frequency and transmitting to the appropriate databases. Server network perimeters are protected with firewalls and internal and external audits of perimeter and software code security are conducted. 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. Moreover, physical access to internal servers with data is restricted to authorized technical personnel via photo passcode authentication, and other security protocols.

Third parties with whom the Airport shares PII are also required to implement adequate security measures to maintain the confidentiality of such information. Additionally, as part of the FasTrak dispute process, encrypted emails are utilized to transmit PII to authorized third parties.

To ensure that airport staff are equipped with the skills and awareness necessary to access and utilize toll readers responsibly, privacy and security training is required for employees with access to PII, upon hire or assignment to projects involving toll readers. In addition, regular periodic refresher training is required for those employees. Training is designed to educate employees on responsible data management practices and to inform them of policies expectations on use, as well as on prohibited actions.

While parking booths and FasTrak lanes present unique safety challenges, the Airport has also taken measures to mitigate potential physical harm to customers and staff. The potential for physical harm, such as being struck by a vehicle, is greatest when staff are required to cross or close a lane. Risk of physical harm may be greater in mixed-payment situations (i.e., cash and electronic collection) as some lanes stop while other lanes maintain a constant speed. A solution to mitigate this risk is to position all FasTrak lanes to the left of the facility (i.e., toward the middle of the roadway), and to prohibit employees from crossing these lanes. Additional safety precautions include requiring all staff to wear safety vests when inside and/or outside the booths, the issuance of a stop paddle to each employee, and the strategic installment of crosswalks. These safeguards have been implemented to mitigate the risk of physical harm.

### C. Fiscal Analysis of Costs and Benefits

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

| | Benefit | Description |
|---|---|---|
| X | Financial Savings | Low maintenance and operating costs in addition to minimal training of personnel on the use of the technology. |
| X | Time Savings | Parking fee collections are much more efficient. |
| X | Staff Safety | Staff no longer need to sit in parking booths that are near fast moving vehicles. |
| X | Data Quality | Provides a uniform methodology for SFO parking fee collection, and more effectively quantifies parking demand, which supports future SFO planning. |
| ☐ | Other | |

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

| | | |
|---|---|---|
| Number of Budgeted FTE (new & existing) & Classification | 5; 1842 Management Assistant, 7318 Electronic Maintenance Technician (Support) | |
| | ***Annual Cost***<br>[If Toolkit 3.9 = yes, include all onetime costs, Toolkit answers 3.10-3.15] | ***One-Time Cost***<br>[If Toolkit 3.2 = yes, include all one-time costs, Toolkit answers 3.3-3.8] |
| Total Salary & Fringe | *$600,000* | $0 |
| Software | *$0* | $50,000 |
| Hardware/Equipment | *$0* | $800,000 |
| Professional Services | *$20,000* | $0 |
| Training | *$0* | $0 |
| Other | *$0* | $0 |
| Total Cost | $1,470,000 | |

The Department funds its use and maintenance of the surveillance technology through Airport Operating Funds.

## COMPARISON TO OTHER JURISDICTIONS

No other CCSF Department employs the FasTrak Toll Reader technology for parking fees.

# Surveillance Impact Report

San Francisco International Airport
Gunshot Detection Solution

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

This Surveillance Impact Report details the benefits, costs, and potential impacts associated with the Airport's use of a gunshot detection solution (from AmberBox, Inc.) integrated with the Department's Closed Circuit Security Camera System .

**DESCRIPTION OF THE TECHNOLOGY**

The Airport's mission is to provide an exceptional airport in service to our communities. In line with its mission, the Airport will use a gunshot detection system in the terminals and employee buildings throughout the Airport. The system will enable the San Francisco Police Department – Airport Bureau (SFPD-AB), the Airport Communication Center and Security Operations Center (SOC) to be aware of gunshots, aggressive voices, glass breaking, and unusual disturbances in the buildings on the Airport campus. The system will notify the respective department of verified gunshot events, which allows SFPD-AB to quickly respond to gunshots, aggression, glass breaking and incidents involving unusual disturbances.

It shall be the policy of the Airport to properly utilize the gunshot detection system to enhance law enforcement's ability to respond to and investigate incidents involving gunfire, aggressive voices, glass breaking, and unusual disturbances. The location information provided by the gunshot detection solution will expedite police and ambulance response to incidents involving gunfire, aggressive voices, glass breaking, and unusual disturbances which will accelerate the identification of the location of victims, witnesses and suspects.

In line with its mission, the Airport shall implement the gunshot detection system, only for the following authorized purposes:

*Authorized Use(s):*

1. Detect the sound of gun shots, aggressive voices, glass breaking, and unusual disturbances (based upon 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 GSD alarm, 9-1-1 Dispatch and the Security Operations Center (SOC) can immediately view CCTV feeds of the location identified in the GSD alarm to provide Airport First Responders situational awareness (i.e., location) of an incident.

**Surveillance Oversight Review Dates**

COIT Review: TBD
Board of Supervisors Review: TBD

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

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

Airport technology may be deployed in the following locations, based on Use Case:

The gunshot detection system will use existing Wi-Fi access points owned and deployed by the Airport.

As part of Phase I of this project to implement the gunshot detection solution, the Airport plans to conduct a Proof of Concept (POC) inside the Consolidated Airport Campus Building 674 (Commission Business office). If successful, Phase II (approximately two months effort) will include the deployment of the system throughout the Airport buildings, including the pre- and post-security at all terminals.

**Technology Details**

The following is a product description:

AmberBox is a detection and response system designed to protect lives in an indoor active shooter incident, aggression, glass break, and unusual disturbances (based upon artificial intelligence employing machine learned decibel level). Specifically, the GDS listens for the ambient (normal) noise within the Airport terminals (i.e., passenger/worker and restaurant/bar decibel levels) and sets a baseline decibel level for the Terminals to eliminate false alarms by only detecting and notifying when the baseline decibel level is exceeded and detected by multiple device sensors.

By automating the emergency notification process, first responders arrive on scene faster, equipped with the vital information needed to contain threats and mitigate casualties. AmberBox provides for immediate and accurate response from internal security and law enforcement teams.

AmberBox offers the most advanced sensing system available, ensuring maximum protection from an active shooter threat, aggressive voices, glass breaking, and unusual disturbances. Specific sounds are detected through percussion and infrared sensors, that analyze the bi-nodal signature, especially those of a gunshot. Combined with AmberBox's sound learning algorithm, false alarm sources are virtually eradicated. All analysis is conducted at the sensor (detector), with no real-time audio transmitted or recorded, guaranteeing privacy.

How AmberBox works:

1. AmberBox utilizes a patented gunshot detection algorithm to provide immediate notifications and alerts to allow immediate response following a firearm discharge, aggressive voices, glass breaking, and unusual disturbances.
2. AmberBox detectors use acoustic and infrared data to determine the firearm signature instantly with a near-zero false alarm rate.

3. AmberBox detectors send an alert signal through a wireless MESH network to the building gateway.
4. An automatic call is made to 911 and to the Airport's 24/7 Security Operations Center (SOC) who connect via the CAD (Computer Aided Dispatch) System to share real-time incident information with first responders.
5. AmberBox can immediately activate building security systems, such as access control, and alert personnel with SMS, email, and other notification methods. Real-time shooter or suspect location and data tracking can be viewed through the web or mobile platform.

The system consists of a number of distinct elements:

- Gunshot Detectors
- Gateway – network devices that connect to the AmberBox Response Platform servers via a VPN and HTTPS connection.
- AmberBox Cloud Server

The detectors sense for the presence of a gunshot, aggressive voices, glass breaking, and unusual disturbances, conducting full analysis on the device (no real-time audio is sent back or recorded). In the event of an activation, the alert message is sent over the Airport's proprietary wireless mesh (potentially hopping over multiple detectors) back to the gateway. The gateway connects to the AmberBox Response Platform servers via a VPN and HTTPS connection. The AmberBox Response Platform servers are hosted by their cloud provider, Google Cloud.

**SYSTEM INTEGRATION**

The Gunshot Detection System (GDS) is expected to integrate with the following Airport systems:

- Computer Aided Dispatch (CAD)
- Mass Notification System

**IMPACT ASSESSMENT**

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

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

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

A. Benefits

The Airport's use of the AmberBox solution with the Closed-Circuit Television (CCTV) has the following benefits for residents:

| | | |
|---|---|---|
| ☐ | Education | |
| ☐ | Community Development | |
| X | Health | Protect safety of staff, patrons, and facilities while promoting an open and welcoming environment. |
| ☐ | Environment | |
| X | Criminal Justice | 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. |
| ☐ | Jobs | |
| ☐ | Housing | |
| ☐ | Other – Public Safety | Improved protection of the public and city assets by leveraging remote condition assessment technology, which improves the 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. |

B. Civil Rights Impacts and Safeguards

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

The Airport's use of the AmberBox solution is restricted to those identified Authorized Use Cases.

NOTE:

Data is housed in servers located in secured areas that are only accessible by approved and badged employees. Cloud access to data is administered by Airport badged employees with access to cloud services that enables continuous monitoring of the Airport account activity.

C. Fiscal Analysis of Costs and Benefits

The Airport's use of the AmberBox solution with the surveillance cameras yields the following business and operations benefits:

| Benefit | | Description |
|---|---|---|
| X | Financial Savings | The gunshot detection solution (GSD), 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. |
| X | 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. |
| X | 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. |
| X | Data Quality | The identification of ambient noise from GSD coupled with CCTV cameras use, provides Law Enforcement complete situational awareness. |

| | | |
|---|---|---|
| Number of FTE (new & existing) | $579,168 | |
| Classification | *1070, IS Project Director* 5%<br>*1042, System Engineer - Journey* 25%<br>*1043, System Engineer - Senior* 10%<br>*1044, System Engineer - Principal* 25%<br>*1041, Network Engineer - Asst.* 20%<br>*1042, Network Engineer - Journey* 20%<br>*1043, Network Engineer - Senior* 20%<br>*1044, Network Engineer - Principal* 15%<br>*1044, Network Engineer - Principal* 20%<br>*7308, Cable Splicer* 20%<br>*7318, Electronic Maint Tech* 100%<br>*7318, Electronic Maint Tech* 15% | |
| | ***Annual Cost*** | ***One-Time Cost*** |
| Software | | Combined in the hardware cost |

| | | |
|---|---|---|
| Hardware/Equipment | | $665,900 |
| Professional Services | | |
| Training | | |
| Other - Installation | | $285,000 |
| Total Cost | ***$TBD*** | ***$950,900*** |

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

Airport Operating Funds, Capital Funds, and Federal Grants.

**COMPARISON TO OTHER JURISDICTIONS**

Gunshot detection solutions are used by other governmental entities, including Airports, for similar purposes.

**APPENDIX A: Mapped Crime Statistics**

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

Gunshot detection solution sensors will be deployed in ceilings and walls inside Airport buildings.