File No. 260107 **Committee Item No.** 3
Board Item No. 15

COMMITTEE/BOARD OF SUPERVISORS

AGENDA PACKET CONTENTS LIST

Committee: Government Audit and Oversight **Date:** March 19, 2026
Board of Supervisors Meeting: **Date:** April 21, 2026

Cmte	Board	
☐	☐	**Motion**
☐	☐	**Resolution**
☒	☒	**Ordinance**
☒	☒	**Legislative Digest**
☐	☐	**Budget and Legislative Analyst Report**
☐	☐	**Youth Commission Report**
☐	☐	**Introduction Form**
☐	☐	**Department/Agency Cover Letter and/or Report**
☐	☐	**MOU - FY2022-2024 - Clean**
☐	☐	**MOU - FY2022-2024 - Redline**
☐	☐	**Grant Information Form**
☐	☐	**Grant Budget**
☐	☐	**Subcontract Budget**
☐	☐	**Contract / DRAFT Mills Act Agreement**
☐	☐	**Form 126 – Ethics Commission**
☐	☐	**Award Letter**
☐	☐	**Application**
☐	☐	**Public Correspondence**

OTHER

☒	☒	STP - Virtual Vehicle Queuing System
☒	☒	AIR Comm Reso No 23-0103 041823
☒	☒	SFO Cover Ltr 011626
☐	☒	Airport Presentation 031926
☐	☒	PAM Temp Membership 031826
☐	X	Letter from Lyft 4/13/26
☐	☐	

Prepared by: Monique Crayton **Date:** April 3, 2026
Prepared by: Monique Crayton **Date:** March 13, 2026
Prepared by: **Date:**

[Administrative Code - Airport Surveillance Technology Policy]

Ordinance approving the Airport Surveillance Technology Policy governing the use of the Transportation Network Company Virtual Queue technology.

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

(c) Under Administrative Code Section 19B.2(b), the Board of Supervisors may approve a Surveillance Technology Policy ordinance under Section 19B.2(a) if: (1) the Department seeking Board approval under subsection (a) creates a Surveillance Technology Policy and Surveillance Impact Report for the Surveillance Technology to be acquired or used; and (2) at a public hearing at which Committee on Information Technology ("COIT") considers the Surveillance Technology Policy, COIT recommends that the Board of Supervisors adopt, adopt with modifications, or decline to adopt the Surveillance Technology Policy for the Surveillance Technology to be acquired or used.

(d) The Airport submitted a Surveillance Technology Policy for the Transportation Network Company Virtual Queue technology to COIT. On December 4, 2025, COIT and its Privacy and Surveillance Advisory Board ("PSAB") conducted one public hearing at which they considered Airport Surveillance Impact Reports and the Surveillance Technology Policy for the Transportation Network Company Virtual Queue technology.

(e) On December 4, 2025, COIT voted to recommend the Transportation Network Company Virtual Queue Policy to the Board for approval.

(f) The Surveillance Technology Policy is available in Board File No. 260107. COIT recommended that the Board approve the Surveillance Technology Policy.

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

Section 2. Transportation Network Company Virtual Queue Technology.

(a) The Airport is seeking to obtain and develop software to implement the Airport's Transportation Network Company Virtual Queue technology ("TNCvq").

(b) The Airport will use TNCvq for: (1) providing a text message based virtual queue system to manage the Transportation Network Company staging lot supply; (2) assisting with

overall ground transportation planning; (3) monitoring driver compliance with their respective operating permit and the Airport's Rules and Regulations, including using the technology to issue citations, suspensions, and prohibitions from service; (4) verifying driver identity; and (5) ensuring that only authorized and approved drivers and vehicles are allowed to service the Airport.

(c) The Surveillance Technology Policy further describes the technology.

Section 3. Findings and Approval of the Policy.

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

(b) The Board of Supervisors hereby approves the TNCvq Policy.

Section 4. Effective Date.

This ordinance shall become effective at 12:00 a.m. on the 31st day after enactment. Enactment occurs when the Mayor signs the ordinance, the Mayor returns the ordinance unsigned or does not sign the ordinance within ten days of receiving it, or the Board of Supervisors overrides the Mayor's veto of the ordinance.

APPROVED AS TO FORM:
DAVID CHIU, City Attorney

By: */s/ Andrew A. Angeles*
ANDREW A. ANGELES
Deputy City Attorney

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

FILE NO. 260107

LEGISLATIVE DIGEST

[Administrative Code - Approval of Airport Surveillance Technology Policy]

Ordinance approving Airport Surveillance Technology Policy governing the use of the Transportation Network Company Virtual Queue technology; and making required findings in support of said approvals.

Background Information

Administrative Code Chapter 19B (Chapter 19B) regulates City Departments' acquisition and use of Surveillance Technology.

Under Chapter 19B.2(a), City Departments that acquire or use new Surveillance Technology must obtain the Board of Supervisors' approval by ordinance of a Surveillance Technology Policy under which the Department will acquire and use Surveillance Technology.

Under Administrative Code Section 19B.2(b), the Board of Supervisors may approve a Surveillance Technology Policy by ordinance under Section 19B.2(a) if: (1) the Department seeking Board approval under subsection (a) creates a Surveillance Technology Policy and Surveillance Impact Report for the Surveillance Technology to be acquired or used; and (2) at a public hearing at which the Committee on Information Technology ("COIT") considers the Surveillance Technology Policy, COIT recommends that the Board of Supervisors adopt, adopt with modifications, or decline to adopt the Surveillance Technology Policy for the Surveillance Technology to be acquired or used.

On December 4, 2025, COIT and its Privacy and Surveillance Advisory Board ("PSAB") subcommittee conducted one public hearings, at which COIT and its PSAB considered Airport Surveillance Impact Reports and the Surveillance Technology Policy for the Transportation Network Company Virtual Queue technology.

Following the hearing, COIT approved the final draft of the Surveillance Technology Policy for the Transportation Network Company Virtual Queue technology.

The Airport Commission (Airport) seeks approval for its Surveillance Technology Policy for the Transportation Network Company Virtual Queue technology (Surveillance Technology Policy). On December 4, 2025, the Airport submitted its Surveillance Technology Policy to COIT staff for review and questions. COIT provided approval for the Surveillance Technology Policy on December 4, 2025. The Surveillance Technology Policy is detailed in Sections 2 and 3 of the proposed ordinance. The Surveillance Technology Policy is available in Board File No. 260107.

Surveillance Technology Policy

Virtual Vehicle Queuing System
Airport

The City and County of San Francisco values privacy and protection of San Francisco residents' civil rights and civil liberties. As required by San Francisco Administrative Code, Section 19B, the Surveillance Technology Policy aims to ensure the responsible use of *the Virtual Vehicle Queuing system (specifically, the Transportation Network Company Virtual Queue (TNCvq))* 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: Delivering an airport experience where people and our planet come first.

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

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

Authorized Use(s):

– Use software (from QTrac and Airport developed) to provide the Airport with a text message–based virtual queue system to manage TNC driver staging lot supply.
– Assist with overall ground transportation planning at the Airport.
– Assist with monitoring Transportation Network Company (TNC) drivers' compliance with the conditions of their operating permit and the Airport's Rules and Regulations, including issuing citations, suspensions, and prohibitions from service.
- As part of the ground transportation management and reporting process, the TNCvq system will collect, process, and retain data, including Personally Identifying Information (PII) of the TNC drivers.

- Ensure that only authorized and approved drivers and vehicles are allowed to service passengers at SFO, including verifying drivers' identity.

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

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

San Francisco International Airport (SFO or Airport) seeks to implement TNCvq, a virtual queue system designed to manage the high demand for TNC staging lot access. This system enables drivers to request entry and receive real-time updates via SMS and a web browser, eliminating the need for a dedicated app. The primary objectives are to: reduce roadway congestion, enhance operational efficiency, and ensure equitable access to the Airport's limited staging lot capacity. With only 350 total staging spaces, 150 of which are revenue-generating at Lot DD, frequent lot closures due to oversupply have led to significant traffic congestion, safety concerns on South Airport Blvd and South McDonnell Road, and operational disruptions. TNCvq aims to eliminate unauthorized staging on nearby roadways, reduce driver conflicts and citations, and support the reclamation of Staging Lot 3 for public parking revenue. TNCvq is expected to streamline TNC operations, improve safety, and unlock valuable real estate for revenue-generating uses.

As part of the TNCvq, SFO seeks to acquire software (from QTrac), develop software, and implement the system, including a dedicated driver registration portal to ensure secure and efficient management of TNC operations. Drivers are required to submit key information, including: full legal name, selfie photo, license plate number, vehicle make, model, and color, TNC profile screenshot, TNC Placard information, phone number, and email address—through this portal. This data is used to verify each driver's identity and affiliation with an authorized TNC, match vehicles to registered users, and enable real-time communication via SMS. The registration portal is a critical component of the VQ system, supporting accurate queue management, reducing unauthorized access to staging lots, and enhancing enforcement and auditing capabilities. Additionally, the collected data allows SFO to monitor dwell time within the staging lots and issue citations for violations of TNC permit terms and Airport Rules and Regulations, helping to ensure fair access and efficient lot turnover.

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

	Benefit	Description
▪	Education	
X	Community Development	Promotes equitable distribution of and access to transportation by managing TNC flow and availability fairly across all drivers.
▪	Health	
X	Environment	Reduces traffic congestion and idling on SFO roadways, which helps lower vehicle emissions and improves air quality in surrounding communities.
▪	Criminal Justice	
X	Jobs	Supports employment opportunities for TNC drivers and enhances operational efficiency for TNC companies; also optimizes resource allocation for SFO's Ground Transportation Unit (GTU).
▪	Housing	
X	Public Safety	Minimizes the risk of fraud, unauthorized access, and unethical business practices by verifying driver credentials and enforcing compliance through the virtual queue system.
▪	Other:	Aligns with growing passenger demand for app-based, on-demand transportation services, improving the overall customer experience at SFO.

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

	Benefit	Description
X	Financial Savings	Eliminates the need to hire additional staff to manually monitor and manage TNC activities. Additionally, by reducing the size of TNC staging areas, the Airport can repurpose space for revenue-generating public parking.
	Time Savings	
X	Staff Safety	Staff safety is indirectly supported by reducing the need for physical monitoring in congested areas, thereby lowering exposure to traffic hazards.

X	Data Quality	Human error is reduced; information is legible and can be easily sorted and summarized by computers; information can be paired with analytical analysis; data will likely reduce handwritten records; and data will increase the number of records as they are automatically created and sent.
X	Other: Enforcement of non-compliant drivers	Enhances enforcement capabilities by enabling the Airport (GTU and SFPD-AB) to identify and enforce Rules and Regulations, and Permit terms against TNC drivers who exceed curbside staging times or operate outside designated areas.
X	Other: Public Safety	Improves public safety by eliminating unauthorized TNC staging on roadways and reducing vehicle oversupply on Airport property, leading to smoother traffic flow and fewer safety incidents.

To achieve its intended purpose, TNCvq (hereinafter referred to as "surveillance technology") works in the following way: The TNCvq technology works with the perimeter, or "geofence," around the Airport using geographic coordinates. The TNC driver's commercial driving activity data is collected after the driver enters the Airport's geo-fence for business purposes, not for personal driving activity. No passenger information is included. Fines can be levied against TNCs for driver activities, such as exceeding staging lot wait times.

The TNCvq application will use software (from QTrac and developed by the Airport) to provide the Airport with a text message–based virtual queue system to manage staging lot demand for TNC drivers. TNCvq will enable drivers to remotely request access to the Airport's staging lots and receive real-time updates on their queue status via SMS on their mobile devices. The system operates entirely via SMS, allowing drivers to join the queue, receive updates, and confirm entry using a smartphone.

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 within the latest three versions or whatever is defined in the service contract.

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
– Full legal name (as shown on driver's license) – Self-Photograph – Phone number – Screenshot of TNC (Transportation Network Company) profile screenshot	JSON, XML, Relational Database Management System (RDBMS), CSV	Level 3

- TNC Placard Information
- Email Address

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

Data Types:

- 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).
- 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).
- Vehicle make, model and color.

Note: The following Data Types are Classified Level 3 – Sensitive (based upon the City's Data Classification Standard.)

- Additional data required for the TNCvq system:
    - Full legal name (as shown on driver's license)
    - Digital self-photograph
    - Phone number
    - Screenshot of TNC (Transportation Network Company) profile
    - TNC Placard Information
    - Email Address

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 TNCvq Technology's collection of selected data from the TNC driver'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
- X Will persons be individually identified (TNC driver's)
- 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: Maintaining a secure network employing firewalls and segmentation, ensuring systems are password-protected, including MFA, and encryption of data at rest and in transit 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 TNCvq 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.

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 who must follow the City's Third-Party Risk Management (TPRM)/ Cybersecurity Risk Assessment (CRA) requirements. (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**
TNCvq registration data (driver name, selfie photo, license plate, phone number, vehicle details, TNC profile screenshot, TNC Placard Information and email address.)	City Attorney's Office, SFPD Airport Bureau

Data sharing occurs at the following frequency:

For the City Attorney's Office, a limited dataset (not the entire database) is provided upon request. The limited data provided is based upon the specifics (e.g., the time-frame – hours or days) of the event being addressed. 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**
TNCvq registration data (driver name, license plate, phone number, vehicle make, model, and color).	Authorized contractor for the TNCvq queuing software.

Data sharing occurs at the following frequency:

As needed for billing and administrative/operational compliance, including fines, suspensions, and prohibition of services for the TNC's and their driver's.

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.

The Airport shall ensure that digital self-photographs and other information collected through the TNCvq system are encrypted at rest and in transit. Access to this data shall be restricted to authorized personnel with a legitimate business need and subject to audit logging.

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. TNCvq data is currently maintained permanently in the Airport's AWS environment. However, the Driver Registration Portal data will be retained no longer than five years.	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. The Driver Registration Portal will provide an annual "Opt-In" recertification process for driver's to confirm their continued participation in the TNCvq program.

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) as required by state and federal law. 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:

- Drivers will have the ability to request the deletion of their PII when they no longer are providing TNC services at the Airport.

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 manage 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 managed via role-based access control (RBAC) – users are only provided access to perform their job role and nothing more. 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 Innovation & Technology 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.
Data Steward:	Individual responsible for: - day-to-day management responsibility of individual databases, datasets, or information systems. In general, a data steward has business knowledge of the data and can answer questions about the data itself. - determining the appropriate classification of the data generated by the department according to the City Data Classification Standard.

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 Customer Relationship Management (CRM) software 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.

AIRPORT COMMISSION

CITY AND COUNTY OF SAN FRANCISCO

RESOLUTION NO. 23-0103

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

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

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

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

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

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

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

at its meeting of APR 18 2023

Secretary

San Francisco International Airport

MEMORANDUM

April 18, 2023

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

23-0103

APR 18 2023

FROM: Airport Director

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

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

Executive Summary

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

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

THIS PRINT COVERS CALENDAR ITEM NO. 9

Background

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

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

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

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

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

Recommendation

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

Ivar C. Satero
Airport Director

Prepared by: Ray Ricardo
Acting Chief Information Officer

Attachment - Surveillance Technology Policies Summary

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

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

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

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

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

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

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

Surveillance Technology (ST)	ST Description	ST Authorized Use Cases – The Airport shall use the ST only for the following authorized purposes:	Benefits of the ST
			(in case the AVI malfunctions and fails to read the Airport transfixed transponder). - Financial: The ALPR-GTMS technology enables the Airport to assess trip fees on permitted Commercial ground transportation operators. For example, in 2019, the Airport collected $64.8M+ in trip fees from ground transportation operators.
Tenant ("Third-Party") Security Cameras	Airport Tenants own and operate security cameras in their physical locations within the Airport. **STATUS:** POLICY APPROVED 11/15/22 – Board passed 11/17/22 – Mayor approved	1. Reviewing camera footage in the event of an incident. 2. Approving Tenant's disclosure of digital recordings and other data from its security camera system.	**For Residents:** - Health: Protect Safety of staff, patrons, and facilities while promoting an open and welcoming environment. - Criminal Justice: Review video footage after a security incident; provide video evidence to law enforcement or the public upon request by formal process, order or subpoena. - Financial Savings: Equipment is owned and operated by a non-city entity. - Staff Safety: Tenant/Contractor Security cameras help identify violations of Building Rules and Regulations, and City, State and Federal law and provide assurance that staff safety is emphasized and will be protected at their place of employment.

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

Surveillance Technology (ST)	ST Description	ST Authorized Use Cases – The Airport shall use the ST only for the following authorized purposes:	Benefits of the ST
			Civil Rights Impacts and Safeguards: - Airport's use of recordings and data from third-party security cameras is restricted to the identified Authorized Use Cases. - Tenant's disclosure of recordings and data from its own cameras is subject to the Airport Rules & Regulations and policies that restrict use of CCTV to the approved use in the Tenant Application. - Tenants are required to report to the Airport any changes or modifications to video monitoring and/or recording device use prior to executing the changes or modifications. - Tenants are required to obtain Airport's written authorization prior to the release of any video monitoring and/or recording device footage from Tenants cameras/devices. In appropriate cases, Airport may also request review and a determination of whether the footage may be disclosed from the Transportation Security Administration (TSA). **Fiscal Analysis of Costs and Benefits:** - Financial Savings: Tenants' Security Camera Systems will save on building or patrol officers.

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

Surveillance Technology (ST)	ST Description	ST Authorized Use Cases – The Airport shall use the ST only for the following authorized purposes:	Benefits of the ST
			- Time Savings: Tenants' Security Camera Systems will run 24/365, thus decreasing or eliminating building or patrol officer supervision. - Staff Safety: Tenant/Contractor Security cameras help identify violations of the Patron Code of Conduct and provide assurance that staff safety is emphasized and will be protected at their place of employment. - Data Quality: Security cameras run 24/365, so full-time staffing is not required to subsequently review footage of security incidents. Data resolution can be set by level and is recommended to be set to high resolution.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

AIRPORT COMMISSION

CITY AND COUNTY OF SAN FRANCISCO

RESOLUTION NO. _____

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

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

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

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

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

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

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

at its meeting of _____

_____

Secretary

SAN FRANCISCO INTERNATIONAL AIRPORT

January 16, 2026

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

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

Dear Ms. Calvillo:

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

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

The following is a list of accompanying documents:

- This Letter;
- Ordinance Approving the Amended Airport Surveillance Technology Policy governing the use of Virtual Vehicle Queuing System (TNCvq) technology.
- Legislative Digest
- Airport Commission Resolution No. 23-0103;
- Memorandum accompanying Airport Commission Resolution No. 23-0103; and
- COIT-Approved Surveillance Technology Policy for Virtual Vehicle Queuing System (TNCvq).

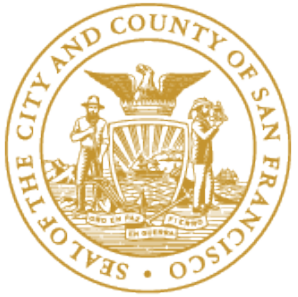
The following persons may be contacted regarding this matter:

Ralf Ruckelshausen, Airport Acting Chief Innovation & Technology Officer
(650) 821-5048
ralf.ruckelshausen@flysfo.com

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

Sincerely,

Mike Nakornkhet
Airport Director



City and County of San Francisco

San Francisco International Airport

Virtual Vehicle Queuing System Technology (TNCvq)

March 19, 2026

Annie Chung, Dushyant Singh & Guy Clarke

Technology Description - TNCvq

- The primary function for the *Virtual Vehicle Queuing system (specifically, the Transportation Network Company Virtual Queue (TNCvq))* technology is using software (from QTrac and Airport developed) to provide the Airport with a text message–based virtual queue system to manage TNC staging lot demand and ensure fair access to SFO's limited staging lot space.
- The system allows TNC drivers to request entry remotely via a web browser, eliminating the need to physically approach the staging lots to check for available space. When a spot opens, drivers receive an SMS notification and may proceed to the lot for verification.
- The primary objectives of the TNCvq technology are to:

    1. Reduce roadway congestion by eliminating unauthorized/illegal staging on nearby roadways, while minimizing violations and improving safety.

    2. Streamline TNC operations and improve operational efficiency, by aiming to reduce driver conflicts and citations.

    3. Free up valuable Airport real estate for revenue-generating uses. Specifically, supporting the reclamation of Staging Lot 3 space for revenue-generating public parking usage.

TNCvq Technology – How It Works

1. As part of the TNCvq, SFO seeks to acquire software (from QTrac) - a dedicated driver registration portal, to support secure and efficient management of TNC operations.
2. Drivers are required to submit key information, including: full legal name, selfie photo, license plate number, vehicle make, model, and color, TNC profile screenshot, TNC Placard information, phone number, and email address—through this portal.
3. This information is used to manually verify each driver's identity and affiliation with an authorized TNC, match vehicles to registered users, and enable real-time communication via SMS.
4. The collected data consists of the TNC driver's commercial driving activity while operating within the Airport's geo-fence. This does not include any personal driving activity. No passenger information is collected.

TNCvq Technology – How It Works (con't)

5. The registration portal is a critical component of the VQ system, supporting accurate queue management, reducing unauthorized access to staging lots, and strengthening SFO's enforcement and auditing capabilities.
6. All data collected or processed by the TNCvq technology is handled or stored by Amazon Web Services to host the application and its data which enables the Airport to access and receive the data at any time.
7. The collected data allows SFO to monitor dwell time within the staging lots and issue citations for violations of TNC permit terms and Airport Rules and Regulations, helping to ensure fair access and efficient lot turnover.
8. SFO maintains all the data for historical analysis.

NOTE: In the Fall of 2025, SFO received Patent approval from the U.S. Patents Office for the *Virtual Vehicle Queuing system.*

Authorized Use Cases

Airport Specific Use Cases include:

- The primary function of the Virtual Vehicle Queuing system (TNCvq) is to provide the Airport with an SMS- and web-based virtual queue, using QTrac software and Airport-developed tools, to manage demand for TNC staging lots.
- Improve safety and traffic flow on Airport roadways by reducing physical vehicle queues, illegal staging, and circulation near the staging areas.
- Monitor Transportation Network Company (TNC) driver compliance with their Operating Permit conditions and Airport Rules and Regulations, including identifying violations and enabling suspensions, prohibitions, and citations when necessary.
- Collect, process, and retain operational data, including TNC driver Personally Identifying Information (PII), as part of the ground transportation management, analytics, auditing, and reporting process.
- Ensure that only authorized and approved drivers and vehicles are permitted to operate at SFO by verifying identities, vehicle information, and valid TNC affiliations through a dedicated registration portal.

Data Lifecycle: Data Collected

Data captured is classified as Level 3, Sensitive.

This data includes:

- Full legal name (as shown on driver's license), Phone Number & Email Address
- Self-Photograph
- Screenshot of TNC (Transportation Network Company) profile screenshot & TNC Placard Information

- All data will be retained for:
  - Transportation Planning purposes
  - Enforcement of Operating Agreements
  - Regulation of Mobility Programs
  - Ensuring the Equitable Distribution of Transportation Options throughout the Airport.

Data Lifecycle: Data Deletion & Retention

1. All registered TNC drivers will have the option to request deletion of their driver profile and all associated personally identifiable information (PII) via the Driver Web Portal under the account management section.
    - Once a driver submits a deletion request, the profile will be scheduled for automatic deletion within seven (7) days. During this period, the driver may cancel the deletion request if it was submitted in error.

2. All registered and approved TNC drivers are required to accept the Terms and Conditions every twelve (12) months to remain opted in and continue operating under the TNCvq program. If a driver does not accept the Terms and Conditions within the required timeframe, their profile will be placed in inactive status, and they will not be permitted to operate at SFO.

3. The system will automatically delete all driver PII data after five (5) years if the driver profile status is anything other than active.
    - Driver trip-related data will be retained indefinitely for analytical purposes only. This data will be anonymized to ensure that no personally identifiable information (PII) is retained.

Thank You

Data Lifecycle: Data Access

1. Prior to accessing or using data, authorized individuals receive training in system access and operation, and instruction regarding authorized and prohibited uses.
2. For investigative purposes, Department access to data is restricted to specific and trained personnel. Location data that is used for prosecution or investigation purposes could be retained beyond the stipulated retention period(s).
3. For litigation purposes, the City Attorney's Office has been provided data upon request.
4. Personnel with access belong to the following groups:

- SFO Ground Transportation Unit (GTU)
- SFO IT (Ops Support)
- SFO Law Enforcement Partners
- SFO Landside Operations

Data Lifecycle: Data Security

1. Departments shall, at minimum, apply the following safeguards to protect surveillance technology information from unauthorized access, control, and misuse by using the following:
    - Password protected systems
    - Encrypted Storage
    - Physical Safeguards
    - Audits

2. Data is reviewed for Personally Identifiable Information (PII) and must always be scrubbed of PII as stated above prior to public use.

3. Access to systems utilizing wireless networks are required to be equipped with WPA2 security.

4. Written authorization from the Department is required prior to release of data.

Other Pertinent Information: TNCvq

Technology includes:

- The Technology is hosted on AWS cloud service – managed by SFO.
- All service provider systems are service-provider-owned.
- Service providers are required to provide data they manage and store to SFO in real-time.
- The Airport's on-premise systems are comprised of private cloud and on-premise hardware that ingest and store the data and process analytic reports.
- **NOTE:** SFO recently received Patent approval from the U.S. Patents Office for the *Virtual Vehicle Queuing system.*

President, District 8
BOARD of SUPERVISORS

City Hall
1 Dr. Carlton B. Goodlett Place, Room 244
San Francisco, CA 94102-4689
Tel. No. 554-6968
Fax No. 554-5163
TDD/TTY No. 544-5227

RAFAEL MANDELMAN

PRESIDENTIAL ACTION

Date: 03/18/2026

To: Angela Calvillo, Clerk of the Board of Supervisors

Madam Clerk,
Pursuant to Board Rules, I am hereby:

☐ Waiving 30-Day Rule (Board Rule No. 3.23)

File No. _____ _____
(Primary Sponsor)

Title. _____

☐ Transferring (Board Rule No 3.3)

File No. _____ _____
(Primary Sponsor)

Title. _____

From: _____ Committee

To: _____ Committee

☒ Assigning Temporary Committee Appointment (Board Rule No. 3.1)

Supervisor: Melgar Replacing Supervisor: Fielder

For: 03/19/2026 (Date) Government Audit & Oversight (Committee) Meeting

Start Time: 10:00AM End Time: 12:30PM

Temporary Assignment: ◉ Partial ○ Full Meeting

Rafael Mandelman, President
Board of Supervisors

185 Berry Street
Suite 400
San Francisco, CA 94107

April 13, 2026

Via Email (rafael.mandelman@sfgov.org)

Rafael Mandelman, President
San Francisco Board of Supervisors
_____
_____

Re Request for Short Continuance of Final Reading of Surveillance Technology Policy Virtual Vehicle Queuing System

Dear President Mandelman:

Lyft acknowledges that there are significant challenges in the staging lots at SFO Airport. It supports implementing measures to reduce congestion while ensuring adequate supply is available to serve the flying public's needs. Indeed, Lyft has already worked with SFO Airport to pilot certain products to help ease congestion issues.

We are respectfully requesting that the final reading of the Surveillance Technology Policy Virtual Vehicle Queuing System be continued for four weeks. Lyft will use this time to meet with airport staff to discuss its questions and concerns which include:

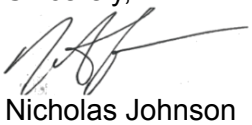
- PII privacy protections, specifically related to location data, law enforcement access, retention, and privacy and security terms with Qtrac.
- Due process protections related to citing drivers based on data not personal observation, including notification, validation, the right to contest and burdens of proof.
- Discussion on driver safety related to timing and interaction with SFO SMS messages
- Discussion of how invitations to the staging lots will be equitably distributed between available TNC platforms and that all TNC platforms are required to participate.
- Discussion on how the policy preserves drivers' ability to earn across multiple platforms simultaneously, ensuring no single platform can restrict a driver's access to other rideshare apps

- Discussion of how drivers' independent contractor rights to operate on multiple TNC platforms will be protected.
- Clearer identification of what data SFO airport will be gathering about drivers while not on airport property, does SFO expect Lyft to share additional real time location data?
- Confirmation that drivers who are inbound with an airport drop off are prioritized to be granted access to the staging lot (i.e., avoiding the need for drivers to deadhead (driving with no passengers) back to the city.
- Discussion of how the Virtual Vehicle Queue will impact environmentally friendly products like rematch and customer ETA products like tiered queuing.
- Seek a seat at the table for the Virtual Queuing System product finalization.

An underlying concern with all of the foregoing is that there is no reasonable transparency in how the use of this surveillance data will actually be used in implementing the Virtual Vehicle Queue product. It is presently impossible to discern the reasonableness of this proposed policy without understanding how the data's use will be done in a business neutral, objective, and consistent manner.

Lyft is looking to be supportive of SFO airport's efforts. This additional time will promote transparency and collaboration.

Sincerely,



Nicholas Johnson
Director Public Policy
Lyft, Inc.

cc: Sophie Marie (sophie.marie@sfgov.org)