File No. 250388 **Committee Item No.** 1
Board Item No. _____

COMMITTEE/BOARD OF SUPERVISORS

AGENDA PACKET CONTENTS LIST

Committee: Rules Committee **Date** June 16, 2025

Board of Supervisors Meeting **Date** _____

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

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

☒	☐	Surveillance Technology Policy
☒	☐	Surveillance Impact Report
☐	☐	
☐	☐	
☐	☐	
☐	☐	
☐	☐	
☐	☐	
☐	☐	

Completed by: Victor Young **Date** June 12, 2025
Completed by: _____ **Date** _____

[Administrative Code - Surveillance Technology Policy - Municipal Transportation Agency - Red Light and No Turn Enforcement Cameras]

Ordinance approving the Surveillance Technology Policy for the Municipal Transportation Agency's continued use of existing Automated Red Light and No Turn Enforcement Cameras.

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

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

Section 1. Background.

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

(b) Chapter 19B establishes requirements that City departments must follow before they may use or acquire new Surveillance Technology. Under Administrative Code Section 19B.2(a), a City department must obtain Board of Supervisors ("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 Board-approved Surveillance Technology Policy ordinance; (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 under Section 19B.2(a) only if: (1) the department seeking Board approval first 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 adopt or adopt with modifications the Surveillance Technology Policy for the Surveillance Technology to be acquired or used.

(d) Under Administrative Code Section 19B.4, it is the policy of the Board 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.

Section 2. Surveillance Technology Policy Ordinance for the Municipal Transportation Agency's Use of Automated Red Light and No Turn Enforcement Cameras.

(a) Purpose. The San Francisco Municipal Transportation Agency ("SFMTA") seeks Board approval under Administrative Code Section 19B.2(a)(3) to use existing Surveillance Technology— specifically, its Automated Red Light and No Turn Enforcement Cameras—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. The SFMTA wishes to continue using its existing Automated Red Light and No Turn Enforcement Cameras, in place since before the effective date of Chapter 19B, as follows: (1) to cite and prosecute red light

violations; (2) to cite and prosecute illegal turn violations; and (3) to perform engineering analysis from associated data such as vehicle counts, vehicle speeds, and violation numbers. The SFMTA currently uses these automated cameras, as part of its Automated Enforcement Program under California Vehicle Code section 21455.5, to reduce traffic collisions, injuries, and fatalities caused by red light running and illegal turns. The program, in place since 1996, uses automated cameras at high-collision intersections to detect violations, and capture photos and videos of offending vehicles and drivers. The program supports Vision Zero goals by enhancing traffic safety, reducing enforcement bias, and allowing police officers to focus on other priorities. It also provides valuable traffic data for engineering analysis.

(b) Surveillance Technology Policy and Surveillance Impact Report. In accordance with Administrative Code Section 19B.2(b)(1), the SFMTA first created a Surveillance Technology Policy and Surveillance Impact Report for Automated Red Light and No Turn Enforcement Cameras, copies of each are on file with the Clerk of the Board in File No. 250388, and are hereby incorporated herein by reference.

(c) Public Hearings. In accordance with Administrative Code Section 19B.2(b)(2), on November 7, 2024 and February 27, 2025, COIT, through its Privacy and Surveillance Advisory Board ("PSAB"), conducted two public hearings at which it considered the Surveillance Technology Policy and Surveillance Impact Report for the Automated Red Light and No Turn Enforcement Cameras.

(d) COIT Recommendation. In accordance with Administrative Code Section 19B.2(b)(2), on February 27, 2025, COIT's PSAB voted in the affirmative to recommend that the Board adopt the Surveillance Technology Policy for Automated Red Light and No Turn Enforcement Cameras.

(e) Findings. In accordance with Administrative Code Section 19B.4, the Board hereby finds, as follows: that the benefits of the SFMTA's use of Automated Red Light and No

Turn Enforcement Cameras, as stated in the Surveillance Technology Policy and Surveillance Impact Report for Automated Red Light and No Turn Enforcement Cameras, outweigh the costs and risks of using such Surveillance Technology; that the Surveillance Technology Policy for Automated Red Light and No Turn Enforcement Cameras will safeguard civil liberties and civil rights, as stated in the Surveillance Impact Report for Automated Red Light and No Turn Enforcement Cameras; and that the uses and deployments of Automated Red Light and No Turn Enforcement Cameras will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or a protected class, as set forth in the Surveillance Technology Policy and Surveillance Impact Report for Automated Red Light and No Turn Enforcement Cameras.

Section 3. Approval of Policy.

Based on the findings stated above and in accordance with Administrative Code Section 19B.4, the Board hereby approves the Surveillance Technology Policy for Automated Red Light and No Turn Enforcement Cameras.

Section 4. Effective Date. This ordinance shall become effective 30 days after enactment. Enactment occurs when the Mayor signs the ordinance, the Mayor returns the ordinance unsigned or does not sign the ordinance within 10 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/ Isidro A. Jiménez
Isidro A. Jiménez
Deputy City Attorney

n:\legana\as2025\2500290\01833716.docx

FILE NO. 250388

LEGISLATIVE DIGEST

[Administrative Code - Surveillance Technology Policy - Municipal Transportation Agency - Red Light and No Turn Enforcement Cameras]

Ordinance approving the Surveillance Technology Policy for the San Francisco Municipal Transportation Agency's continued use of existing Automated Red Light and No Turn Enforcement Cameras.

Existing Law

San Francisco Administrative Code Chapter 19B ("Chapter 19B") sets requirements for City departments before they may acquire or use "Surveillance Technology." Chapter 19B broadly defines Surveillance Technology as any system or device that collects, processes, or shares data linked to individuals or groups, including audio, visual, location, biometric, or other identifying information.

Before a City department may acquire or use Surveillance Technology, Chapter 19B requires Board of Supervisors approval, by ordinance, of a Surveillance Technology Policy governing that technology. This approval is required before the department: (1) seeks funds for Surveillance Technology; (2) acquires or borrows new Surveillance Technology; (3) uses new or existing Surveillance Technology for a purpose, in a manner, or in a location not specified in a Board-approved Surveillance Technology Policy ordinance; (4) enters into an agreement with a non-City entity to acquire, share, or otherwise use Surveillance Technology; or (5) enters 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.

Amendments to Current Law

Since 1996, the SFMTA has operated Automated Red Light and No Turn Enforcement Cameras—considered Surveillance Technology under Chapter 19B—as part of its Automated Enforcement Program to reduce traffic collisions, injuries, and fatalities caused by red light running and illegal turns. Although this program predates Chapter 19B, the SFMTA must now obtain Board approval of a Surveillance Technology Policy to continue using these enforcement cameras.

The proposed ordinance would authorize the SFMTA to continue using its Automated Red Light and No Turn Enforcement Cameras, as follows: (1) to cite and prosecute red light violations; (2) to cite and prosecute illegal turn violations; and (3) to perform engineering analysis using associated data such as vehicle counts, vehicle speeds, and violation numbers.

Background Information

On November 7, 2024 and February 27, 2025, the Committee on Information Technology's Privacy and Surveillance Advisory Board Subcommittee ("PSAB") held two public hearings to consider the SFMTA's Surveillance Technology Policy and Surveillance Impact Report for Automated Red Light and No Turn Enforcement Cameras. On February 27, 2025, PSAB voted to recommend that the Board adopt the policy.

Committee on Information Technology

Office of the City Administrator

To: Members of the Board of Supervisors

From: Carmen Chu, City Administrator
Edward McCaffrey, Director, Committee of Information Technology

Date: March 20, 2025

Subject: Legislation introduced to approve Surveillance Technology Policy for the Municipal Transportation Agency's Automated Red Light and No Turn Enforcement Cameras

---

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 amendments for the Municipal Transportation Agency's Automated Red Light and No Turn Enforcement Cameras.

To engage the public in discussion on the role of government surveillance, the Committee on Information Technology (COIT) and its subcommittee the Privacy and Surveillance Advisory Board (PSAB) held two public meetings for the Automated Red Light and No Turn Enforcement Cameras between November 2024 and February 2025 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 Edward McCaffrey, Director of the Committee on Information Technology (COIT).

Cameras, Non-Security

Department	Authorized Uses
Municipal Transportation Agency	1. To cite and prosecute red light violations. 2. To cite and prosecute illegal turn violations. 3. To perform engineering analysis from associated data such as vehicle counts, vehicle speeds and violation numbers.

Camera, Non-Security Public Meeting Dates

Date	Meeting
November 7, 2024	Privacy and Surveillance Advisory Board (PSAB)
February 27, 2025	Privacy and Surveillance Advisory Board (PSAB)

COIT recommends the following action be taken on the policy:

- Approve the Automated Red Light and No Turn Enforcement Camera Surveillance Technology Policy for the Municipal Transportation Agency.

Automated Red Light and No Turn Enforcement Cameras – Surveillance Technology Policy

San Francisco Administrative Code Chapter 19B ("Chapter 19B") sets requirements for City departments before they can acquire or use "Surveillance Technology." Before a City department can acquire or use Surveillance Technology, Chapter 19B requires Board of Supervisors approval, by ordinance, of a Surveillance Technology Policy governing that technology.

Since 1996, the SFMTA has operated automated red light and no turn enforcement cameras—considered Surveillance Technology under Chapter 19B—as part of its Automated Enforcement Program to reduce traffic collisions, injuries, and fatalities caused by red light running and illegal turns. While this program predates Chapter 19B, the SFMTA must now obtain Board approval of a Surveillance Technology Policy to continue using these enforcement cameras.

The proposed ordinance would authorize the SFMTA to continue using its automated red light and no turn enforcement cameras, as follows: (1) to cite and prosecute red light violations; (2) to cite and prosecute illegal turn violations; and (3) to perform engineering analysis from associated data such as vehicle counts, vehicle speeds, and violation numbers.

The approval of the proposed ordinance would not result in a direct or indirect physical change to the environment. Therefore, it is "Not a Project" under CEQA.

Not a "project" under CEQA pursuant to CEQA Guidelines Sections 15060(c) and 15378(b) because the action would not result in a direct or a reasonably foreseeable indirect physical change to the environment.

Marcus Barrango 3/31/2025

Marcus Barrango Date
San Francisco Municipal Transportation Agency

Jennifer McKellar 3/31/2025

Jennifer McKellar Date
San Francisco Planning Department

April 9, 2025

The Honorable Members of the Board of Supervisors
City and County of San Francisco
1 Dr. Carlton Goodlett Place, Room 244
San Francisco, CA 94102

Subject: Automated Red Light Cameras and No Turn Enforcement

Honorable Members of the Board of Supervisors:

The San Francisco Municipal Transportation Agency (SFMTA) requests that the San Francisco Board of Supervisors approve the Surveillance Technology Policy for the San Francisco Municipal Transportation Agency (SFMTA) use of Red Light Cameras and No Turn Enforcement. This fulfills the SF Administrative Code 19B requirements for new surveillance technologies.

BACKGROUND
Since 1996, the SFMTA has operated automated red light and no turn enforcement cameras—considered Surveillance Technology under Chapter 19B—as part of its Automated Enforcement Program to reduce traffic collisions, injuries, and fatalities caused by red light running and illegal turns. While this program predates Chapter 19B, the SFMTA must now obtain Board approval of a Surveillance Technology Policy to continue using these enforcement cameras.

The proposed ordinance would authorize the SFMTA to continue using its automated red light and no turn enforcement cameras, as follows: (1) to cite and prosecute red light violations; (2) to cite and prosecute illegal turn violations; and (3) to perform engineering analysis from associated data such as vehicle counts, vehicle speeds, and violation numbers.

The cameras support the SFMTA's mission for a safe, equitable, and sustainable transportation system, aiding in Vision Zero goals by reducing traffic-related fatalities and injuries. They advance equitable traffic enforcement. They ensure more predictable and effective traffic control and, when broadly implemented, help change driver behavior. Enforcing red lights and no turns is a reliable and cost-effective method to prevent further fatalities and injuries.

REQUEST FOR APPROVAL
The SFMTA respectfully requests that the Board of Supervisors approve the System Use Policy and System Impact Report.

Sincerely,

Julie Kirschbaum
Director of Transportation

OFFICE OF THE MAYOR
SAN FRANCISCO

DANIEL LURIE
MAYOR

TO: Angela Calvillo, Clerk of the Board of Supervisors
FROM: Adam Thongsavat, Liaison to the Board of Supervisors
RE: [Administrative Code - Surveillance Technology Policy - Municipal Transportation Agency - Red Light and No Turn Enforcement Cameras]
DATE: April 15, 2025

Ordinance approving the Surveillance Technology Policy for the San Francisco Municipal Transportation Agency's continued use of existing Automated Red Light and No Turn Enforcement Cameras

Should you have any questions, please contact Adam Thongsavat at adam.thongsavat@sfgov.org

1 DR. CARLTON B. GOODLETT PLACE, ROOM 200
SAN FRANCISCO, CALIFORNIA 94102-4681
TELEPHONE: (415) 554-6141

Surveillance Technology Policy

Automated Red Light and No Turn Enforcement Cameras Municipal Transportation Agency

The City and County of San Francisco values privacy and protection of San Francisco residents' civil rights and civil liberties. As required by San Francisco Administrative Code, Section 19B, the Surveillance Technology Policy aims to ensure the responsible use of Automated Red Light and No Turn Enforcement Cameras (hereinafter referred to as "surveillance technology" or "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 connect San Francisco through a safe, equitable, and sustainable transportation system.

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 department personnel that use, plan to use, or plan to secure the surveillance technology, including employees, contractors, vendors, and volunteers. Employees, contractors, vendors, and volunteers 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 Uses:

1. To cite and prosecute red light violations.
2. To cite and prosecute illegal turn violations.
3. To perform engineering analysis from associated data such as vehicle counts, vehicle speeds and violation numbers.

Examples of use case 3, engineering analysis, include:

- Confirm that yellow light durations are set appropriately to avoid BOTH rear end collisions and unjust red light camera violations. Key metrics in this analysis are the speed of the vehicle being cited, whether it's accelerating or decelerating through the intersection, and how long the signal has been red when cited.
- Confirm the appropriateness and effectiveness of traffic signal coordination at managing traffic speeds. For example, a properly coordinated signal will also reduce red light camera violations, while a poorly coordinated one could encourage some motorists to "race" toward a green light that's about to change.

Prohibited use cases include any uses not stated in the Authorized Uses section, unless it is to comply with a court-ordered search warrant or subpoena.

The Department may use information collected from the surveillance 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:

The Department's Automated Enforcement Program (Program) is authorized under California Vehicle Code section 21455.5. The Department began operation of the Program in 1996 to reduce the number of collisions, property damage, physical injuries, and deaths caused by red light running. San Francisco was one of the first cities in the United States to implement a program to enforce laws prohibiting red light running using automated cameras at street intersections. The Automated Enforcement Program is managed by the Department, with support from the San Francisco Police Department, the Superior Court of San Francisco, and the San Francisco City Attorney's Office. The Program uses a network of automated cameras to enforce illegal red light running and illegal turns and is part of the Department's Vision Zero commitment to eliminate traffic fatalities. Decisions for the placement of automated enforcement cameras are based on public safety with priority given to the intersections in the City with the highest collision totals. The Department tries to implement all other traffic safety measures first before considering an automated enforcement installation at an intersection. The Department's combined automated enforcement, engineering, and education efforts have resulted in a 66% citywide drop in injury collisions resulting from red light running between 1997 and 2022.

Description of Technology

The City's Automated Enforcement Program has been in operation since 1996. The Department installed Automated Enforcement systems at intersections with chronic red light running and illegal turn problems that endanger pedestrian, bicycle and vehicular traffic. These systems enforce traffic law by photographing the license plates and drivers of those vehicles that run red lights or make illegal turns and issuing citations to alleged violators by mail.

In 2019 the Department upgraded the Automated Enforcement System with state-of-the-art digital cameras and radar vehicle detection. The system equipment is owned, operated, and maintained by Verra Mobility (Contractor) and leased to the Department. The Contractor also provides program administration, violation review prior to SFPD approval, processing, citation printing and mailing, tree trimming, and construction design services.

Below is a description of how the technology works to detect and capture red light and illegal turn violations (events), followed by a description of how captured events are reviewed and approved to be issued and mailed as citations to alleged violators. (Note that the vehicle detection technology used to detect illegal turns is slightly different than the vehicle detection used for red light enforcement.)

The system captures photos of the license plate and the vehicle driver in accordance with state law. In California, red light running, and illegal turns are moving violations that result in points on a driver's DMV record. As such, a photo of the driver's face is necessary to identify the driver and establish responsibility for the moving violation.

Equipment and Photographs:

The camera control unit manages each component of the Automated Enforcement system. The system utilizes two or more high-speed digital cameras paired with illuminating strobes and a High Definition (HD) video camera to capture clear photos and video in all weather conditions. The camera control unit monitors a 3D traffic radar aimed at the roadway and tracks the position, speed, and direction of each vehicle passing through its field of view. Additionally, the camera control unit attaches to the traffic controller to monitor the color of each light phase as they change. To protect the system from tampering, a locked metal housing secures the complete system.

The system only activates into enforcement mode when the light phase cycles in sequence from yellow to red. Drivers who enter the intersection when the light phase is green or yellow and are in the intersection as the light turns yellow or red are not photographed. The design of this system only catches those violators who enter the intersection after the traffic signal phase has turned red.

When the traffic signal phase has turned red and the 3D traffic radar detects a vehicle entering the intersection, the system captures three digital photographs and a short video clip of the event. The system takes two photos of the rear and one photo of the front of the violating vehicle using two separate cameras. Placing one digital camera behind the violation point clearly shows the position of the vehicle relative to the violation point and the color of the traffic signal phase both before and after the vehicle enters the intersection. Placing an additional digital camera across the intersection photographs the front of the vehicle and captures a clear image of the driver. Each digital image appends the violation data, including date/time/lane/redlight time/etc., to that image. This violation data appears at the top of each image in the black data bar. Placing a high-resolution digital camera and HD video camera behind the violation point shows the vehicle and traffic signal phase prior to the vehicle entering and exiting the intersection.

To enforce illegal right turns made from Eastbound Market Street at Octavia Boulevard, the Department installed an Automated Enforcement System that operates similar to the red light system described above, although instead of using radar for detection, the system utilizes a video stream to detect and capture evidence of vehicles making a right-hand turn. Vehicles going straight through the intersection will not activate the system. When the system detects a vehicle entering the intersection

and making an illegal turn, the system captures three digital photographs and a short video clip of the event.

Violation Processing:

Once events are loaded into a Violation Processing System (VPS), the Contractor's trained technicians administratively review and categorize each event based on the Department's approved Business Rules Questionnaire (BRQ). For events meeting the requirements of a potential violation in the BRQ, the VPS obtains the name, address, and identifying information of the registered owner from the California Department of Motor Vehicles or the analogous agency of another state or country, based upon the license plate of the photographed vehicle. Once this information is obtained, a San Francisco Police Officer reviews, signs and issues the citation containing four images of the violation. The four images show: two full rear views of the violating vehicle, a close-up of the license plate, and a close-up of the driver. The close-up of the license plate and the close-up of the driver are cropped and enlarged versions of the other images. The system then sends the signed citation (Notice to Appear) to the alleged violator by mail.

Resident Benefits

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

	Benefit	Description
☐	Education	
☐	Community Development	
☒	Health	Decreases the risk of traffic collisions resulting in serious injuries/fatalities by reducing red light running and illegal turns.
☒	Environment	Improves street conditions for all users of the transportation network by enforcing traffic laws.
☒	Criminal Justice	Enforces red lights and illegal turns without bias and removes the potential of escalation during in-person traffic enforcement.
☐	Jobs	
☐	Housing	
☒	Public Safety	The reduction in red light running and illegal turns makes intersections safer for pedestrians, bicyclists, and other vehicles.

Department Benefits

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

Benefit	Description

☒	Financial Savings	Cameras are more cost-efficient than having police officers posted at intersections 24 hours a day, 7 days a week.
☒	Time Savings	Cameras save time that police officers can spend on other priorities.
☐	Staff Safety	
☒	Data Quality	Associated data collected by the system such as vehicle counts, vehicle speeds and violation counts can be used for engineering analysis by the Department to assess traffic patterns, traffic safety, and the effectiveness of automated cameras at reducing red light running and illegal turns.
☐	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. The 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

Data Type(s)	*Format(s)*	*Classification*
Photos of violation showing vehicle, license plate, and driver's face	**SBIF** (Verra Mobility Propriety encrypted image format) **and JPEG**	**Level 3**
Video of violation	**AVI video container H264**	**Level 3**

	Registered Owner	**DMV Information**	**All PII is stored as encrypted data at the table space level. So, all PII information is encrypted at rest. Level 3**

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

The Department includes the following items in its public notice:

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

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

a. For a Contractor user, receiving access to Axsis requires the submission of a ticket to the Contractor's IT Support. IT Support only provisions access once Contractor management approval has been received.
b. As part of the Contractor's access to National Law Enforcement Telecommunications System (NLETS) individuals with direct or incidental access to vehicle/registered owner information undergo Criminal Justice Information Services (CJIS) background checks.
c. Contractor's clients (SFMTA, SFPD, and Court) are typically provisioned a role for one or more of their selected users who can add/remove their staff to their instance.

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:

- 182x Administrative Analyst
- 9504 Permit and Permit Clerk
- 5207 Associate Engineer

B. Members of the public

In accordance with Vehicle Code section 21455.5(f), photographic records made by an automated traffic enforcement system shall be confidential, and shall be made available only to governmental agencies and law enforcement agencies and only for the purposes of this article. Confidential information obtained from the Department of Motor Vehicles for the administration or enforcement of an automated traffic enforcement system shall be held confidential, and shall not be used for any other purpose.

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

The Department shall require all 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. The 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.

Since the technology is owned by the Contractor and they are also responsible for the administration of the technology, Department does not provide any training. Contractor provides in-person hands-on training on how to use their software, how to review violations, approve/process citations, run reports, etc.

Data Security: The 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 frameworks selected by the department.

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

- The Contract Agreement lists the data security requirements the Contractor must follow, including the requirement to hold Technology Errors and Omissions Liability coverage and Cyber and Privacy Insurance. The contract includes Liquidated Damages for loss of Violation Data that results from

failure to secure System-generated data in accordance with the terms of the Contract Agreement.

- Authorized users require unique login credentials to access the technology, which is accessible on portable tablets and on workstations.

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

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

☒ Contractor's Data Center

☐ Software as a Service Product

☐ Cloud Storage Provider

Data Sharing: The 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.

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

A. Internal Data Sharing:

The Contractor shares the following data with recipients within the City and County of San Francisco:

Data Type	Data Recipient
Images, video, metadata, DMV information.	SFMTA, SFPD
XML and PDF, images, video, metadata, DMV information	Superior Court

Frequency - Data sharing occurs at the following frequency
Daily reports: On Monday- Friday, XML and PDF Reports are shared via SFTP (Secure File Transfer Protocol) folders created by the Superior Court. They contain the following information:

- Photos of the violation (in the PDF)
- Citation Number
- Vehicle State Vehicle Plate Number Make
- Violation Date Violation Time
- Citation (Section/Offense) Citing Officer (Badge Number)
- Location of Violation
- Driver information: Last Name First Name Middle Name Address City State Zip Code Driver's License State Height Weight Eye Color Hair Color Gender Date of Birth Commercial Vehicle File Name

On demand: Data available to the Department, Superior Court, SFPD and SFMTA on demand via online Axsis platform includes:

- All of the above data
- Short video clips of violations

B. External Data Sharing:

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

Data Type	Data Recipient
XML and PDF, images, metadata, DMV information	Print and mail subcontractor
Images, video, metadata, DMV information	Contractor's Call Center
PDF of Notice (court packages)	Contractor's Expert Witness

Frequency - Data sharing occurs at the following frequency:
PDF of notice shared with Contractor's expert witness daily Monday - Friday.
Contractor's print and mail subcontractor receives data daily Monday - Friday.
Contractor's call center access data on demand via online Axsis platform.

Data Retention: The 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
For Events that do not result in the issuance of a Citation (or Notice to Appear), pursuant to the signed Agreement, Contractor is required to destroy driver information, data, and Images within 15 Business Days of determining the Event does not meet the City's Business Rules, or the SFPD's rejection of the Event. For Violations that do result in the issuance of a Citation, Contractor is required to destroy all related information, including but not limited to all data, Images, and paper records within	The Contractor performs monthly audits for quality control, so they need sufficient time to be able to review rejected events and ensure that their processors are categorizing those events correctly. For Violations resulting in issuance of a Citation, the five-year retention period matches the five-year retention period of the Superior Court.

15 Business Days of final disposition. If notice of final disposition is not received from the Superior Court, Contractor shall destroy all related information, including but not limited to all data, Images, and paper records within 5 years of the Citation due date. This agreement is currently in the process of being documented in a Contract amendment. On-device data: Video cameras at the intersection record continuous video that is overwritten every 30 days. Only the brief video clips of potential violations are uploaded to the Contractor's system for processing by the Contractor.	

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):

Litigation holds, court orders, search warrants, subpoenas.

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

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

- Processes and Applications: The Contractor deletes data based on configurations which are defined by data type and retention period.
- Practices: When passengers are captured in violation photos, they are blurred.

COMPLIANCE

Department Compliance

The Department shall oversee and enforce compliance with this Policy using the following methods:
The Contract Agreement lists the data security requirements the Contractor must follow, including the requirement to hold Technology Errors and Omissions Liability coverage and Cyber and Privacy Insurance. The contract includes Liquidated Damages for loss of Violation Data that results from failure to secure System-generated data in accordance with the terms of the Contract Agreement.

For more details, see Appendix A.

Interdepartmental, Intergovernmental & Non-Governmental Entity Compliance

To ensure that entities receiving data collected by the surveillance technology comply with the Surveillance Technology Policy, the Department shall:
The Contract Agreement lists the data security requirements the Contractor must follow, including the requirement to hold Technology Errors and Omissions Liability coverage and Cyber and Privacy Insurance. The contract includes Liquidated Damages for loss of Violation Data that results from failure to secure System-generated data in accordance with the terms of the Contract Agreement. The technology has been in use since the 1990s, before 19B was enacted, and the current vendor has been under contract since 2018.

Oversight Personnel

The Department shall be assigned the following personnel to oversee Policy compliance by the Department and third parties.
• Automated Enforcement Program Manager (1824 Principal Administrative Analyst)

Sanctions for Violations

Sanctions for violations of this Policy include the following:
Violations of this Policy by department employees may result in disciplinary action commensurate with the severity of violation. Sanctions include written warning, suspension, and termination of employment. The Contract includes Liquidated Damages for loss of violation data that results from the contractor's failure to secure System-generated data in accordance with the terms of the Contract Agreement.

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

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

EXCEPTIONS

Outside the normal process of this policy, a search warrant or subpoena signed by a judge is required to share PII data.

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

Public complaints or concerns may be submitted to the Department by calling 311 or visiting 311.org.

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

Respond to 311 requests within required Service Level Agreement (SLA).

Inquiries from City and County of San Francisco Employees

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

APPENDIX A: EXCERPTS FROM CONTRACT WITH VERRA MOBILITY
Signed August 21, 2018 between Verra Mobility and the SFMTA.

Insurance Requirements from Article 5

(e) Technology Errors and Omissions Liability coverage, with limits of $1,000,000 each occurrence and each loss, and $2,000,000 general aggregate. The policy shall at a minimum cover professional misconduct or lack of the requisite skill required for the performance of services defined in the contract and shall also provide coverage for the following risks:

(i) Network security liability arising from the unauthorized access to, use of, or tampering with computers or computer systems, including hacker attacks; and

(ii) Liability arising from the introduction of any form of malicious software including computer viruses into, or otherwise causing damage to the City's or third person's computer, computer system, network, or similar computer related property and the data, software, and programs thereon.

(f) Contractor shall maintain in force during the full life of the agreement Cyber and Privacy Insurance with limits of not less than $5,000,000 per claim and $5,000,000 general aggregate. Such insurance shall include coverage for liability arising from theft, dissemination, and/or use of confidential information, including but not limited to, bank and credit card account information or personal information, such as name, address, social security numbers, protected health information or other personally identifying information, stored or transmitted in electronic form. Excess or umbrella coverage may be used to comply with this requirement.

Article 13: Data and Security

Article 13: Data and Security

13.1 Nondisclosure of Private, Proprietary or Confidential Information

13.1.1 Protection of Private Information. If this Agreement requires City to disclose "Private Information" to Contractor within the meaning of San Francisco Administrative Code Chapter 12M, Contractor and subcontractor shall use such information only in accordance with the restrictions stated in Chapter 12M and in this Agreement and only as necessary in performing the Services. Contractor is subject to the enforcement and penalty provisions in Chapter 12M.

13.1.2 City Data; Confidential Information. In the performance of Services, Contractor may have access to, or collect on City's behalf, City Data, which may include proprietary or Confidential Information that if disclosed to third parties may damage City. If City discloses proprietary or Confidential Information to Contractor, or Contractor collects such information on

City's behalf, such information must be held by Contractor in confidence and used only in performing the Agreement. Contractor shall exercise the same standard of care to protect such information as a reasonably prudent contractor would use to protect its own proprietary or Confidential Information.

Data Security Requirements from Appendix A Scope of Services

Data Security Requirements From Appendix A Scope of Services

K. Data Security

(i) Data Encryption. Contractor shall encrypt all System-generated data prior to electronic transmission via broadband communication. To encrypt such data, Contractor shall use a secure, tamperproof encryption system; Contractor shall encrypt data using, at minimum, the triple-DES encryption algorithm. The methods Contractor uses to encrypt and secure System-generated data shall, at all times, be subject to City's review and approval. The Department must approved Contractor's proposed substitutions of encryption algorithms before Contractor deploys substitutions.

(ii) Loss of Data. Contractor shall be solely responsible for loss of Violation Data that results from failure to secure System-generated data in accordance with the terms of this Agreement. Accordingly, Contractor shall be subject to liquidated damages in accordance with Section 4.7 of the Agreement.

Surveillance Impact Report

Automated Red Light and No Turn Enforcement Cameras Municipal Transportation Agency

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

The Surveillance Impact Report details the benefits, costs, and potential impacts associated with the Department's use of Automated Red Light and No Turn Enforcement Cameras (hereinafter referred to as "surveillance technology").

PURPOSE OF THE TECHNOLOGY

The Department's mission is to connect San Francisco through a safe, equitable, and sustainable transportation system.

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

The Department's Automated Enforcement Program (Program) is authorized under California Vehicle Code section 21455.5. The Department began operation of the Program in 1996 to reduce the number of collisions, property damage, physical injuries, and deaths caused by red light running. San Francisco was one of the first cities in the United States to implement a program to enforce laws prohibiting red light running using automated cameras at street intersections. The Automated Enforcement Program is managed by the Department, with support from the San Francisco Police Department, the Superior Court of San Francisco, and the San Francisco City Attorney's Office. The Program uses a network of automated cameras to enforce illegal red light running and illegal turns and is part of the department's Vision Zero commitment to eliminate traffic fatalities. Decisions for the placement of automated enforcement cameras are based on public safety with priority given to the intersections in the City with the highest collision totals. The Department tries to implement all other traffic safety measures first before considering an automated enforcement installation at an intersection. The Department's combined automated enforcement, engineering, and education efforts have resulted in a 66% citywide drop in injury collisions resulting from red light running between 1997 and 2022.

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

Authorized Use(s):

1. *To cite and prosecute red light violations.*
2. *To cite and prosecute illegal turn violations.*

Surveillance Oversight Review Dates
PSAB Review: 11/07/2024
COIT Review: TBD (list all dates at COIT, and write "Recommended: MM/DD/202X" for rec date)
Board of Supervisors Approval: TBD

3. *To perform engineering analysis from associated data such as vehicle counts, vehicle speeds and violation numbers.*

Examples of use case 3, engineering analysis, include:

- *Confirm that our yellow light durations are set appropriately to avoid BOTH rear end collisions and unjust red light camera violations. Key metrics in this analysis are the speed of the vehicle being cited, whether it's accelerating or decelerating through the intersection, and how long the signal has been re when cited.*
- *Confirm the appropriateness and effectiveness of traffic signal coordination at managing traffic speeds. For example, a properly coordinated signal will also reduce red light camera violations, while a poorly coordinated one could encourage some motorists to "race" toward a green light that's about to change.*

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

Cameras currently enforce 19 approaches at the 13 intersections listed below, all of which enforce red light violations, except for the intersection at Market Street and Octavia Boulevard, which enforces a posted NO RIGHT TURN regulation facing eastbound Market Street. The direction of traffic (approach) enforced at each intersection is indicated in parentheses. In 2022, the Department increased the scope of the contract by eight approaches (listed below), which are currently under design. Once construction is completed, cameras will enforce a total of 27 approaches at 21 intersections.

Currently enforced locations:

1. 6th St at Bryant St (eastbound, southbound)
2. 19th Ave at Sloat Blvd (northbound, southbound)
3. Fell St at Masonic Ave (westbound)
4. Hayes St at Polk St (southbound, westbound)
5. Market St at Octavia Blvd (eastbound illegal right turns)
6. Oak St at Octavia Blvd (eastbound, northbound, eastbound right turn lanes)
7. Park Presidio Blvd at Lake St (southbound)
8. So. Van Ness Ave at 14th St (northbound)
9. 4th St at Harrison St (southbound, westbound)
10. 6th St at Folsom St (southbound)
11. 8th St at Folsom St (southbound)
12. Divisadero St at Bush St (northbound)
13. Van Ness Ave at Broadway (southbound left turn lanes)

Future expansion locations (currently in design):

1. Divisadero St at Oak St (southbound)
2. Franklin St at Lombard St (northbound)
3. Geary Blvd at Gough St (eastbound)
4. Golden Gate Ave at Franklin St (eastbound)
5. Gough St at Oak St (southbound)
6. Harrison St at 6th St (westbound)
7. Masonic Ave at Fell St (northbound)
8. Presidio Ave at Pine St (northbound)

It is possible that additional intersections may be added in the future.

Description of Technology

The City's Automated Enforcement Program has been in operation since 1996. The Department installed Automated Enforcement systems at intersections with chronic red light running and illegal turn problems that endanger pedestrian, bicycle and vehicular traffic. These systems enforce traffic law by photographing the license plates and drivers of those vehicles that run red lights or make illegal turns and issuing citations to alleged violators by mail.

In 2019 the Department upgraded the Automated Enforcement System with state-of-the-art digital cameras and radar vehicle detection. The system equipment is owned, operated, and maintained by Verra Mobility (Contractor) and leased to the Department. The Contractor also provides program administration, violation review prior to SFPD approval, processing, citation printing and mailing, tree trimming, and construction design services.

Below is a description of how the technology works to detect and capture red light and illegal turn violations (events), followed by a description of how captured events are reviewed and approved to be issued and mailed as citations to alleged violators. (Note that the vehicle detection technology used to detect illegal turns is slightly different than the vehicle detection used for red light enforcement.)

The system captures photos of the license plate and the vehicle driver in accordance with state law. In California, red light running, and illegal turns are moving violations that result in points on a driver's DMV record. As such, a photo of the driver's face is necessary to identify the driver and establish responsibility for the moving violation.

Equipment and Photographs:

The camera control unit manages each component of the Automated Enforcement system. The system utilizes two or more high-speed digital cameras paired with illuminating strobes and a High Definition (HD) video camera to capture clear photos and video in all weather conditions. The camera control unit monitors a 3D traffic radar aimed at the roadway and tracks the position, speed, and direction of each vehicle passing through its field of view. Additionally, the camera control unit attaches to the

traffic controller to monitor the color of each light phase as they change. To protect the system from tampering, a locked metal housing secures the complete system.

The system only activates into enforcement mode when the light phase cycles in sequence from yellow to red. Drivers who enter the intersection when the light phase is green or yellow and are in the intersection as the light turns yellow or red are not photographed. The design of this system only catches those violators who enter the intersection after the traffic signal phase has turned red.

When the traffic signal phase has turned red and the 3D traffic radar detects a vehicle entering the intersection, the system captures three digital photographs and a short video clip of the event. The system takes two photos of the rear and one photo of the front of the violating vehicle using two separate cameras. Placing one digital camera behind the violation point clearly shows the position of the vehicle relative to the violation point and the color of the traffic signal phase both before and after the vehicle enters the intersection. Placing an additional digital camera across the intersection photographs the front of the vehicle and captures a clear image of the driver. Each digital image appends the violation data, including date/time/lane/redlight time/etc., to that image. This violation data appears at the top of each image in the black data bar. Placing a high-resolution digital camera and HD video camera behind the violation point shows the vehicle and traffic signal phase prior to the vehicle entering and exiting the intersection.

To enforce illegal right turns made from Eastbound Market Street at Octavia Boulevard, the Department installed an Automated Enforcement System that operates similar to the red light system described above, although instead of using radar for detection, the system utilizes a video stream to detect and capture evidence of vehicles making a right-hand turn. Vehicles going straight through the intersection will not activate the system. When the system detects a vehicle entering the intersection and making an illegal turn, the system captures three digital photographs and a short video clip of the event.

Violation Processing:

Once events are loaded into a Violation Processing System (VPS), the Contractor's trained technicians administratively review and categorize each event based on the Department's approved Business Rules Questionnaire (BRQ). For events meeting the requirements of a potential violation in the BRQ, the VPS obtains the name, address, and identifying information of the registered owner from the California Department of Motor Vehicles or the analogous agency of another state or country, based upon the license plate of the photographed vehicle. Once this information is obtained, a San Francisco Police Officer reviews, signs and issues the citation containing four images of the violation. The four images show: two full rear views of the violating vehicle, a close-up of the license plate, and a close-up of the driver. The close-up of the license plate and the close-up of the driver are cropped and enlarged versions of other images. The system then sends the signed citation (Notice to Appear) to the alleged violator by mail.

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 is currently handled by Verra Mobility, the Department's existing contractor.

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	Decreases the risk of traffic collisions resulting in serious injuries/fatalities by reducing red light running and illegal turns.
☒	Environment	Improves street conditions for all users of the transportation network by enforcing traffic laws.
☒	Criminal Justice	Enforces red lights and illegal turns without bias and removes the potential of escalation during in-person traffic enforcement.
☐	Jobs	

☐	Housing	
☒	Public Safety	The reduction in red light running and illegal turns makes intersections safer for pedestrians, bicyclists, and other vehicles.

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:

- **Dignity Loss**. Administrative safeguards make this impact (e.g., embarrassment and emotional distress) highly unlikely because the surveillance technology is used for the strictly limited purposes of identifying illegal red light running and illegal turns, and the resulting images and violation data are not disclosed to the public. If it is determined that a captured event is not a violation, the event is rejected, the images are destroyed, and no personal information is pulled from the DMV. In addition, for violations that do become issued citations, any images of passengers are cropped or blurred out of the violation photos to protect their privacy.
- **Discrimination**: Administrative safeguards make this impact (i.e., unfair or unethical differential treatment of individuals or denial of civil right) highly unlikely because the Program applies equally to all vehicles travelling through intersections where the technology is deployed. Additionally, technology was deployed at intersections with the highest rate of crashes due to red light running. This technology removes the possibility of bias when a police officer is required to stop and detain a driver who runs a red light.
- **Economic Loss:** Administrative safeguards make this impact (i.e., identity theft/ misidentification) minimal because the resulting images and violation data are not disclosed to the public. Additionally, each image is checked against a DMV-furnished photograph of the vehicle's registered owner to ensure there is a match. If a citation is issued, the person receiving a citation has the right to due process and to argue their case in Court. If the person receiving a citation was not the driver, there are administrative processes to dismiss or transfer liability.
- **Loss of Autonomy:** Administrative safeguards make this impact (i.e., loss of control over decisions on how personal information is used or processed) highly unlikely because the Program is used only to identify vehicles for purpose of illegal red light running and illegal turns on red. A subpoena or search warrant signed by a judge is required to release camera images and/or owner/driver information to law enforcement investigating an unrelated crime.
- **Loss of Liberty:** Technical safeguards make this impact (i.e., improper exposure to arrest or detainment due to incomplete or inaccurate data) highly unlikely because system equipment is tested for accuracy, inspected, and maintained on a regular schedule. Additionally, each image

is checked against a DMV-furnished photograph of the vehicle's registered owner to ensure there is a match.

- **Physical Harm**: Technical safeguards make this impact (e.g., physical harm or death) extremely unlikely because this technology removes the potential of escalation during an in-person police traffic stop that could lead to injury or death.
- **Loss of Trust:** Technical safeguards make this impact (e.g., breach of implicit or explicit expectations or agreements about the processing of data, or failure to meet subjects' expectation of privacy for information collected) extremely unlikely because Department limits access to the data to only authorized users. By State law, camera images and registered owner/driver information cannot be used for any other purpose other than citing and prosecuting red light and illegal turn violations. Camera images and registered owner/driver information cannot be disclosed to anyone other than the defendant receiving the citation, unless the department is served with a search warrant or subpoena signed by a judge.

The administrative safeguards are:

- Trained contractor staff administratively review and categorize each event based on the Department's approved Business Rules Questionnaire (BRQ). For events meeting the requirements of a potential violation in the BRQ, the registered owner's information is pulled from the DMV database based on the license plate of the photographed vehicle. Once this information is obtained, a San Francisco Police Officer reviews, signs and issues the citation.
- Images (photos and videos) of events captured by the cameras that do not result in citations are destroyed within 15 business days of determining the event does not meet the City's Business Rules, or the SFPD's rejection of the event.
- Per state law (CVC 21455.5), camera images and registered owner/driver information cannot be used for any other purpose other than citing and prosecuting red light and illegal turn violations. Camera images and registered owner/driver information cannot be disclosed to anyone other than the defendant receiving the citation, unless the department is served with a search warrant or subpoena signed by a judge.
- If the registered owner of a vehicle was not the driver at the time of the violation, there are processes in place to address that. There is a transfer of liability process for the registered owner to identify the actual driver and transfer the citation to that person. There is a secondary review process if the registered owner cannot identify who was driving. If the vehicle was stolen, the registered owner can provide a police report to have the citation dismissed.
- Anyone receiving a citation has the right to due process and to argue their case in Court.

The technical safeguards are:

- Per the Contract Agreement, Contractor is required to encrypt all System-generated data prior to electronic transmission via broadband communication. To encrypt such data, Contractor is

required to use a secure, tamperproof encryption system; and Contractor is required to encrypt data using, at minimum, the triple-DES encryption algorithm.

- A secure login/password is required to access Contractor's software. Only trained authorized staff have access.
- The system only enters enforcement mode when the light phase cycles in sequence from yellow to red. Drivers who enter the intersection when the light phase is green or yellow and are in the intersection as the light turns yellow or red are not photographed. The design of the system only catches those violators who enter the intersection after the traffic signal phase has turned red.
- A digital high-resolution front-facing camera is used to take a clear photograph of the driver to ensure proper identification of the person responsible for the moving violation.
- The rear-facing HD camera and HD video camera show the color of the traffic signal before and after the vehicle enters the intersection, which confirms if a violation did occur.
- The continuous video camera footage records over itself after 30 days and is not saved (apart from the short violation video clip that is saved as evidence with each citation).
- The system equipment is tested, inspected, and maintained on a regular schedule. Twice a day, the system runs an automated testing sequence. Once a week, technicians remotely inspect and test all system equipment and the functionality of the system as a whole. Once a month, a field technician physically inspects and cleans/maintains the system equipment in person at each intersection. The system alerts Contractor technical staff of any malfunctions, who have 24/7 remote access to assess and address any malfunctions.

The physical safeguards are:

- Equipment is placed high up on poles and secured in locked metal housing to protect them from tampering.
- Signs are posted at camera-enforced intersections to warn motorists.

C. Fiscal Analysis of Costs and Benefits

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

	Benefit	Description
☒	Financial Savings	Cameras are more cost-efficient than having police officers posted at intersections 24 hours a day, 7 days a week.
☒	Time Savings	Cameras save time that police officers can spend on other priorities.
☐	Staff Safety	

☒	Data Quality	Associated data collected by the system such as vehicle counts, vehicle speeds and violation numbers can be used for engineering analysis by the Department to assess traffic patterns, traffic safety, and the effectiveness of automated cameras at reducing red light running and illegal turns.
☐	Other	

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

Number of Budgeted FTE (new & existing) & Classification	1823 (0.2 FTE), 1824 (0.4 FTE), 5207 (0.1 FTE), 9504 (0.4 FTE) at MTA, 1.0 FTE Q004 Police Officer III at SFPD	
	Annual Cost	***One-Time Cost***
Total Salary & Fringe	$420,000.00	$0.00
Software	$0.00	$0.00
Hardware/Equipment	$0.00	$0.00
Professional Services	$800,000 to 1,100,000.00	$0.00
Training	$0.00	$0.00
Other	$0.00	$2,800,000.00
Total Cost	$1,220,000 to $1,520,000.00	$2,800,000.00

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

General Fund.

COMPARISON TO OTHER JURISDICTIONS

The surveillance technology is currently utilized by other governmental entities for similar purposes.

Other government entities have used the surveillance technology in the following way: The first red light camera program was implemented in 1992 in New York City. San Francisco installed its first red light cameras in 1996. Other major U.S. cities with red light safety cameras include Chicago, Denver, New Orleans, New York City, Philadelphia, Seattle and Washington, D.C. In 2023, 337 U.S. communities operated red light safety camera programs, including 33 in California. In the Bay Area, the following cities have red light camera programs: Daly City, Fremont, Millbrae, Napa, San Jose, and San Leandro (IIHS, 2024).

The effectiveness of the surveillance technology while used by government entities is determined to be the following: From the Insurance Institute for Highway Safety (IIHS) website (https://www.iihs.org/topics/red-light-running): Red light safety cameras have been shown to reduce both red light violations and crashes. A series of IIHS studies in different communities found that red light violations are reduced significantly with cameras. Institute studies in Oxnard, California, and Fairfax, Virginia, reported reductions in red light violation rates of about 40% after the introduction of red light safety cameras (Retting et al., 1999; Retting et al., 1999). In addition to the decrease in red light running at camera-equipped sites, the effect carried over to nearby signalized intersections not equipped with cameras. A more recent IIHS study in Arlington, Va., also found significant reductions in red light violations at camera intersections one year after ticketing began (McCartt & Hu, 2014). These reductions were greater the more time had passed since the light turned red, when violations are more likely to result in crashes. Violations occurring at least a half second after the light turned red were 39% less likely than would have been expected without cameras. Violations occurring at least 1 second after were 48% less likely, and the odds of a violation occurring at least 1.5 seconds into the red phase fell 86%. When it comes to crash reductions, an IIHS study comparing large cities with red light safety cameras to those without found the devices reduced the fatal red light running crash rate by 21% and the rate of all types of fatal crashes at signalized intersections by 14% (Hu & Cicchino, 2017). Previous research in Oxnard, California, found significant citywide crash reductions followed the introduction of red light safety cameras, and injury crashes at intersections with traffic signals were reduced by 29% (Retting & Kyrychenko, 2002). Front-into-side collisions -- the crash type most closely associated with red light running -- at these intersections declined by 32% overall, and front-into-side crashes involving injuries fell 68%. The Cochrane Collaboration, an international public health organization, reviewed 10 controlled before-after studies of red light safety camera effectiveness (Aeron-Thomas & Hess, 2005). Based on the most rigorous studies, there was an estimated 13%-29% reduction in all types of injury crashes and a 24% reduction in right-angle injury crashes. When camera programs are discontinued, crash rates go up. An IIHS study compared large cities that turned off red light safety cameras with those with continuous camera programs. In 14 cities that shut down their programs during 2010-14, the fatal red light running crash rate was 30% higher than would have been expected if they had left the cameras on. The rate of fatal crashes at signalized intersections was 16% higher (Hu & Cicchino, 2017). A study in Houston, which turned off red light

safety cameras in 2011, found that the camera deactivation was associated with a 23% increase in right-angle red light running crashes at the intersections that previously had cameras (Ko et al., 2017).

The adverse effects of the surveillance technology while it has been used by other government entities are:

	Effect	Description
☐	Unanticipated Costs	
☐	Failures	
☐	Civil Rights and/or Civil Liberties Abuses	
☒	Other	Some studies have reported that while red light safety cameras reduce front-into-side collisions and overall injury crashes, they can increase rear-end crashes. However, such crashes tend to be much less severe than front-into-side crashes, so the net effect is positive. A study sponsored by the Federal Highway Administration evaluated red light safety camera programs in seven cities (Council et al., 2005). It found that, overall, right-angle crashes decreased by 25% while rear-end collisions increased by 15%. Results showed a positive aggregate economic benefit of more than $18.5 million in the seven communities. The authors concluded that the economic costs from the increase in rear-end crashes were more than offset by the economic benefits from the decrease in right-angle crashes targeted by cameras. Not all studies have reported increases in rear-end crashes. The review by the Cochrane Collaboration did not find a statistically significant change in rear-end injury crashes (Aeron-Thomas & Hess, 2005).

SFMTA

SFMTA Automated Red Light and No Turn Enforcement Camera Technology

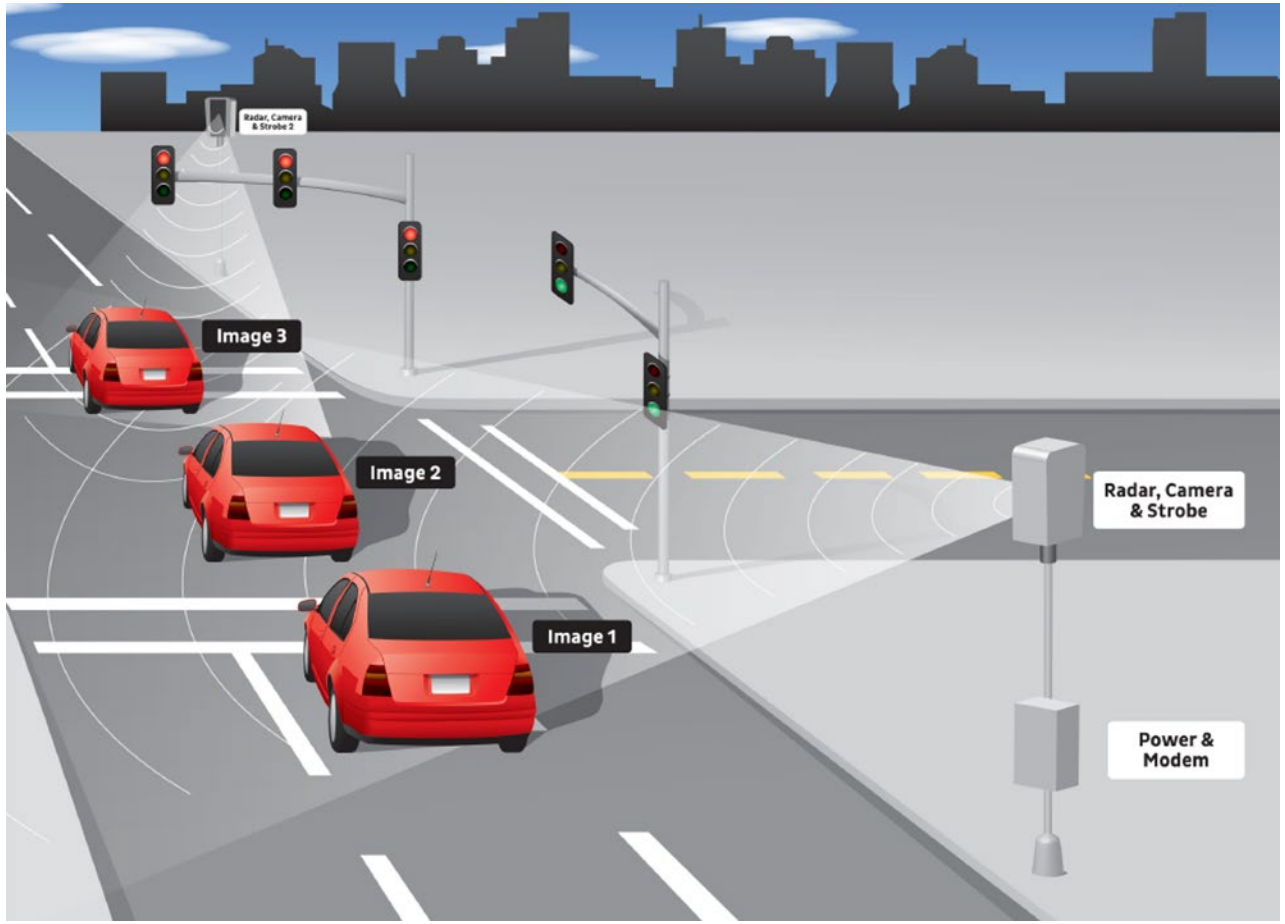
BOS Rules Committee Meeting: May 19, 2025

Technology Description

1) Automated Enforcement Program started in 1996 to reduce the number of collisions, property damage, physical injuries, and deaths caused by red-light running and illegal turns.
2) Authorized under California Vehicle Code section 21455.5 and part of Vision Zero.
3) Managed by MTA with support from SFPD, Superior Court, and the City Attorney's Office.
4) Automated cameras record traffic violations, photographing the license plates and drivers when vehicles run red lights or make illegal turns and mailing out citations.
5) Equipment is owned, operated, and maintained by Verra Mobility (Contractor) and leased to the Department.
6) Contractor also provides program administration, violation review prior to SFPD approval, processing, citation printing and mailing, tree trimming, and construction design services.

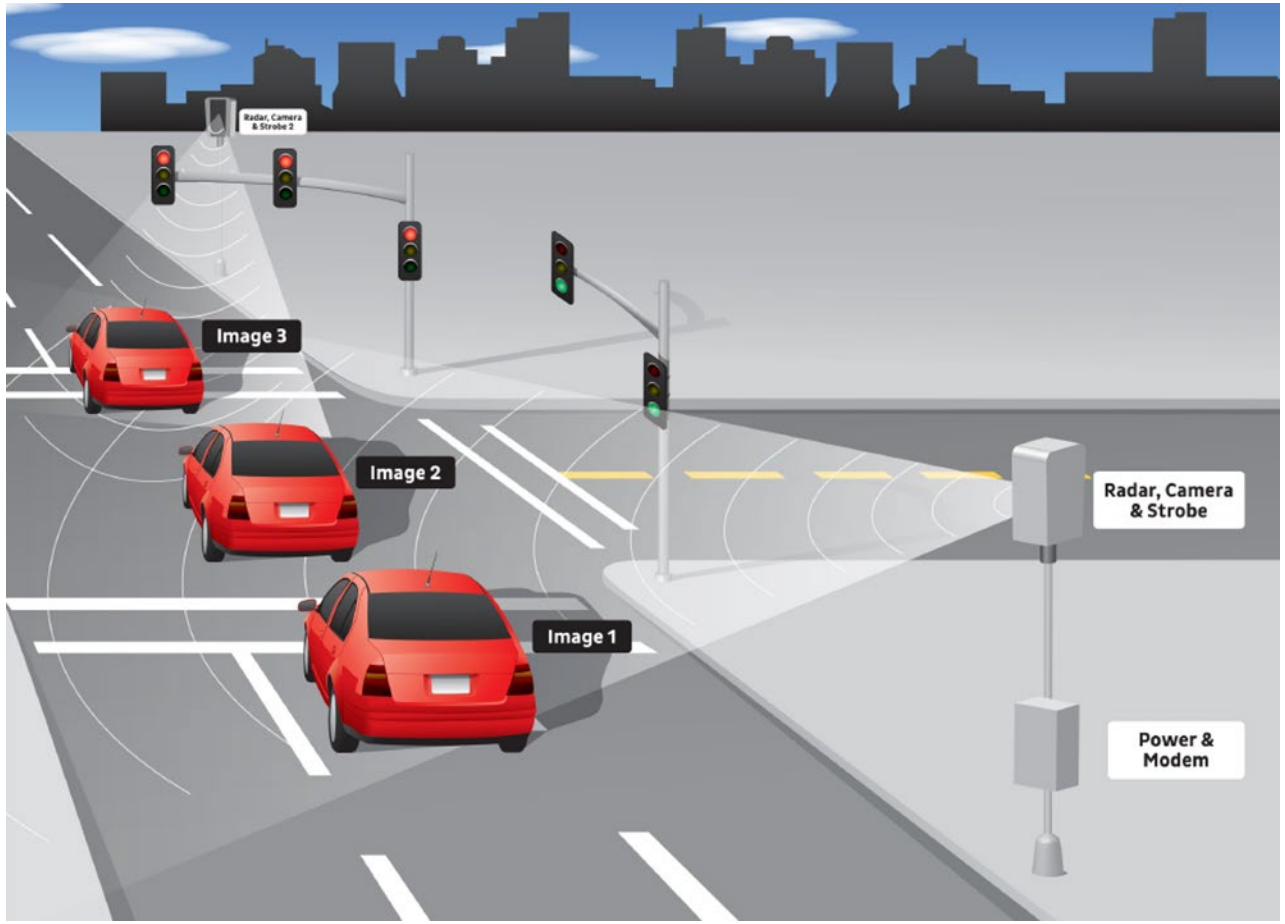
Technology Description

- How this Technology works: (Red Light Violation)
  - i. Camera control unit uses 3D traffic radar to track cars.
  - ii. Also monitors traffic light as it changes color.
  - iii. System enters enforcement mode when light changes from yellow to red.
  - iv. Does not photograph cars that enter intersection on a green or yellow light.
  - v. Once violation is detected, System captures photos of the license plate and driver and a short video clip.



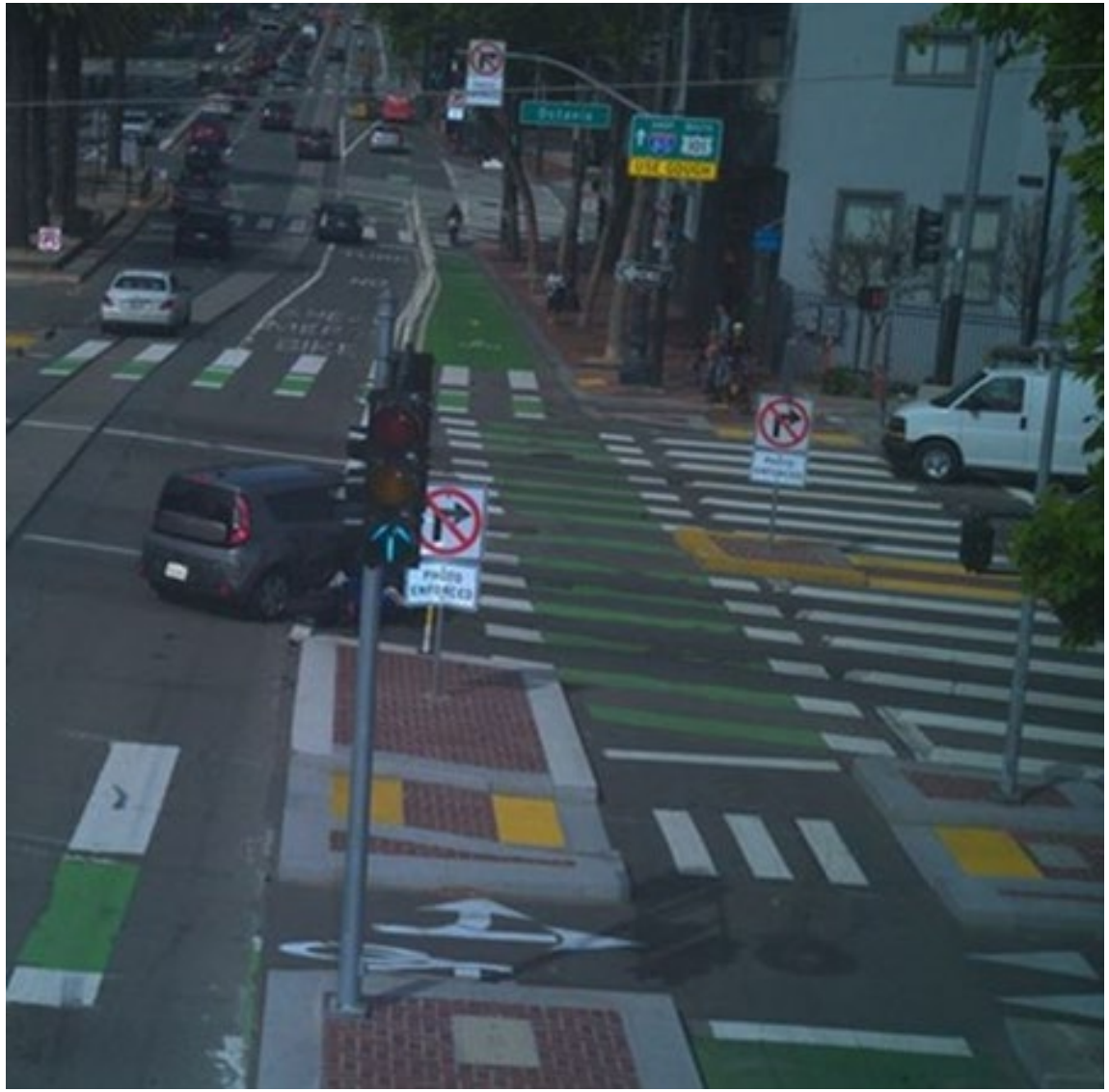
Technology Description (summary of system steps)

- Step 1: System activates when car enters intersection on a red light. Camera captures multiple images from rear and front of vehicle.
- Step 2: First image shows vehicle before entering intersection during red light.
- Step 3: Second image shows the vehicle proceeding through the intersection on a red light.
- Step 4: Third image, taken by camera two, identifies the driver of the vehicle.
- Step 5: Close-up image of the license plate is also captured.
- Step 6: Data, including the time, date, and duration of the yellow and red lights, is also recorded.
- Step 7: Cameras also record a 12-second digital video of the violation, including six seconds prior to and six seconds after running the red light.



Technology Description

- How this Technology works: (Illegal Turn Violation)
  i. Similar to Red Light violation.
  ii. Instead of radar, uses a video stream to capture vehicles making a turn.
  iii. Going straight through the intersection will not activate the system.
  iv. When the system detects a vehicle entering the intersection and making an illegal turn, the system captures three digital photographs and a short video clip (12 seconds long) of the event.



Authorized Use Cases

Department's use of the Automated Red Light and No Turn Enforcement Camera technology is limited to the following use cases:

1. To cite and prosecute red light violations.
2. To cite and prosecute illegal turn violations.
3. To perform engineering analysis from associated data such as vehicle counts, vehicle speeds and violation numbers.

Data Lifecycle Steps

- Collection
  - "Radar-system" continuously monitors for violations.
  - When one occurs, onsite camera captures a clear picture (.JPEG) of violating vehicle's rear license plate and driver's face and sends it to the vendor server.

- Processing & Use
  - Upon violation, data is captured and securely transfers to Contractor's Back Office
  - Contractor (Verra Mobility) reviews the violation. Once confirmed, collects DMV information and shares it with the Law Enforcement (SFPD)
  - SFPD reviews the violation, signs and issues the citation
  - Vendor mails the 'Notice of Violation/Citation' to the vehicle registered owner

Data Lifecycle Steps

- Sharing
  - **Department**: Data is available to only authorized department staff
    - Will not share technology data externally with entities outside the City and County of San Francisco unless a warrant/subpoena was issued
  - **Others**: SFPD, Superior Court
  - **External Data Sharing**: Verra Mobility (Contractor and Owner of the Technology) and their designated subcontractors.
- Retention
  - **Local Storage (On Device): 30 days**
  - **If no citation issued: 15 Business Days**
  - **If citation issued: 15 Business Days from the final disposition**
  - **If final disposition not received from the Superior Court: 5-Years from the Citation due date**
    - This agreement is currently in the process of being documented in a Contract amendment.

PSAB & COIT Meeting Dates

- COIT PSAB Meeting:
  - November 7, 2024
  - February 27, 2025

- COIT Recommendation Date:
  - Date COIT Recommended this policy for BOS Review: March 20, 2025

Questions

Team members available to Answer Questions:

Automated Enforcement Program:

– Monica Giese

Law Enforcement:

– SFPD (Not Present)

City Attorney's Office (CAO):

– Isidro Alarcon Jimenez (Not Present)

Information Technology:

– Sean Cunningham (Not Present)

Program Management Office (PMO)

– Sohail Warsi

– Nabil Arnaoot

BOARD of SUPERVISORS

City Hall
1 Dr. Carlton B. Goodlett Place, Room 244
San Francisco 94102-4689
Tel. No. (415) 554-5184
Fax No. (415) 554-5163
TDD/TTY No. (415) 554-5227

M E M O R A N D U M

TO: Julie Kirschbaum, Acting Director, Municipal Transportation Agency

FROM: Victor Young, Assistant Clerk

DATE: April 21, 2025

SUBJECT: LEGISLATION INTRODUCED

The Board of Supervisors' Rules Committee received the following proposed Ordinance:

File No. 250388

Ordinance approving the Surveillance Technology Policy for the Municipal Transportation Agency's continued use of existing Automated Red Light and No Turn Enforcement Cameras.

If you have comments or reports to be included with the file, please forward them to Victor Young at the Board of Supervisors, City Hall, Room 244, 1 Dr. Carlton B. Goodlett Place, San Francisco, CA 94102 or by email at: victor.young@sfgov.org.

c. Janet Martinsen, SFMTA
Joel Ramos, SFMTA
Christine Silva, SFMTA