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.