Surveillance Technology Toolkit

Purpose: The Surveillance Toolkit is a step-by-step guide to fill out the requirements in the Acquisition of Surveillance Technology Ordinance. This toolkit will help departments assess the following items for each surveillance technology:

A. Business Uses (i.e. Benefits)
B. Data Management Process & Lifecycle
C. Existing Civil Rights and Liberties Strategies
D. Identify Risks & Mitigations
E. Impact Assessment

The Surveillance Ordinance requires departments to assess the separate impact of every inventoried surveillance technology. By completing the toolkit, departments will have compiled the majority of information required by the Acquisition of Surveillance Technology Ordinance.

Tips: Please follow these tips as you complete the toolkit:

1. **Divide and conquer:** Some sections are better answered by certain department units. Please refer to "Best completed by" and forward appropriately.
2. **Do your best** and COIT will reach out if any further information is required.

Time required: The estimated time required for toolkit completion is 5 to 6 hours per technology.

Department:	*Municipal Transportation Agency*
Name of the Technology:	*ALPR*
Is this an existing technology already in use by your department, or a proposed new technology?	
Existing	
Custodian of Records:	*Kimberley Burrus* *Chief Security Officer* *Sustainable Streets Division – Security Investigations and Enforcement*

I. Business Uses (i.e. the benefits)

Best completed by: Business Owner
1.1 What is your Department's mission statement?
We connect San Francisco through a safe, equitable, and sustainable transportation system.

1.2 Describe how the surveillance technology is used to support your department's mission. SIR
The SFMTA uses ALPR technology to efficiently identify vehicles parked on city streets in violation of time-limited parking restrictions, and promote timely turnover of parking spaces. This use supports the SFMTA's mission because it helps ensure the sustainability of and more equitable access to the City's limited parking resources, which are part of its larger transportation system.

1.3 **Authorized Use Cases:** Please list all the distinct ways in which the department is authorized to use the surveillance technology. *Please be as specific as possible. This question will be referenced in future sections.*	
Authorized Use Case #1	*Identify vehicles parked on city streets in violation of time-limited parking restrictions.*
Authorized Use Case #2	*Identify vehicles parked on city streets that have five or more unpaid parking citations.*
Authorized Use Case #3	*Identify vehicles parked on city streets that are listed on SFPD's hotlist of stolen vehicles. (Hotlists contain license plate numbers and ~~make, model, and color information~~state of vehicles reported stolen ~~to the SFPD. SFPD emails~~.* *Hotlist is transmitted via Secure FTP;* *Hotlist is updated ~~hotlist to the SFMTA~~/overwritten on a daily basis.* *The SFMTA does not generate hotlists.)*
Authorized Use Case #4	*Future use – Pilot program to identify vehicles parked at metered spaces after paid parking session expires.*
Authorized Use Case #5	*Future use – Determine occupancy and turnover rates at public parking spaces throughout the city.*

1.4 For the Authorized Use cases described above, identify alternative methods to accomplish these tasks without the use of the surveillance technology.
ALPR automates the functions described for each authorized use; without ALPR those functions would be performed manually by PCOs. The function described for authorized use case #1 would be performed by manually chalking tires; the functions described for authorized use case #2 and #3 would require PCOs calling SFMTA Parking Enforcement Dispatch for individual vehicles; the function described for authorized use case #4 would require PCOs to manually check and confirm expiration of paid parking sessions at individual, metered parking spaces; and the function described for authorized use case #5 would require manual surveys of individual parking spots over extended time periods.

1.5 Please list any prohibited uses for the surveillance technology. [STP]
All uses not referenced above shall be prohibited, unless authorized under a separate SFMTA ALPR Surveillance Technology Policy. Examples of prohibited uses include: • *Use of ALPR technology or access to ALPR data by unauthorized users;* • *Unauthorized sharing of ALPR data;* • *Sale of ALPR data;* • *Retention of ALPR data in excess of applicable retention period; and* • *Personal use.*
1.6 Describe what the technology does and how it works. [SIR, STP]
An ALPR is a camera that captures color images of license plates within its field of view. Mobile cameras are mounted on moving objects, such as parking enforcement vehicles. *Software extracts the license plate numbers from the images and stores the images, plate numbers, and dates, times, and locations of the image captures in a searchable database.* *An ALPR system consists of the cameras, the software that reads and converts images of license plates into data, and the searchable database that stores the data.*
1.7 Provide the product description from the manufacturer. [SIR]
The system consists of the Genetec Auto Vu Sharp IP-based automatic license plate recognition cameras with onboard processing and the AutoVu Standard Software package. The cameras include Sharp V, AutoVu cameras mounted on the roof of the enforcement vehicle and wheel focused camera on the side of the vehicle. The roof top mounted cameras read the license plates and the side mounted cameras photograph the wheel/tire to compare on the second pass for time-limited enforcement. The system utilizes the Genetec Patroller software 6.5 to create the user interface and in-vehicle mapping. The system utilizes cellular communication to transmit reads to the backend software. The backend software consists of the Genetec Security Center software to manage access to all uploaded plate reads, hotlists, and user-level access credentials.
1.8 From the list below, select the areas where the surveillance technology's use or data might benefit residents, and describe how:
• *Education: N/A* • *Community Development: Informs planning, policy development, and pricing for public parking spaces (e.g., for specific commercial districts).* • *Health: N/A* • *Environment: Improves street conditions by ensuring timely turnover of parking spaces for use by city residents and visitors.*

- *Criminal Justice: Identifies vehicles reported to SFPD as stolen so they may be returned to their owners.*
- *Public Safety: Identifies vehicles reported to SFPD as stolen so they may be returned to their owners.*
- *Jobs: N/A*
- *Housing: N/A*
- *Other [Parking Enforcement]: Helps ensure timely turnover of parking spaces, giving city residents and visitors more equitable access to limited parking resources.*

1.9 From the list below, select the areas where the surveillance technology's use or data might benefit the department. **Please describe and quantify each benefit* selected.**

*Please specify units and time period quantified (i.e. dollars vs. hours, weekly vs. annually, department-wide vs. per staff member)

- *Financial savings: Minimizes physical chalking by PCOs; chalking can cause repetitive motion injuries, which result in workers compensation claims filed against the city.*
- *Time savings: Helps parking control officers cover larger geographic areas and improves effectiveness and efficiency in performing their duties.*
- *Staff safety: Minimizes repetitive motion injuries from physical chalking by automating the process for PCOs to mark vehicles.*
- *Improved data quality: Improves and simplifies information provided to PCOs, which makes parking enforcement more accurate and efficient. Provides higher volumes of data about parking utilization and turnover rates than currently available, which informs planning, policy development, and pricing for public parking spaces.*

1.10 Please list any other benefits not already captured above.

None.

Best completed by: Financial Staff

1.11 Please disclose the surveillance technology's cost of operations, making sure to include cost of initial purchase, number and cost of personnel providing support and maintenance, and other ongoing costs. SIR, ASR

Number of FTE	*33*
Classification	*8214*
Total Salary & Fringe	*$3,623,288*
Software	*$13,500*

Hardware/Equipment	*$420,000*
Professional Services	*$0*
Training	*$0*
Other	*$26,500*
Total Cost [Auto-calculate]	*$4,083,288*
1.12 Please disclose any current or potential sources of funding (e.g. potential sources = prospective grant recipients, etc.). SIR, ASR	
SFMTA Operating Budget.	

II. Data Management Process & Lifecycle

Best completed by: Business Owner
Purpose: The purpose of this section is to gather step-by-step information on department data management practices. Most questions in the following section are required by the Surveillance Technology Policy and Annual Surveillance Report. **Background:** Responsible data management practices minimize the risk for adverse impacts. Proper data management practices are important at each phase within a data lifecycle. **Lifecycle phases:** Collection – Processing & Use – Sharing – Retention – Disposal[1] Responses will primarily be used to populate the "Surveillance Technology Policy" which will be approved by COIT, Department leadership, and the Board of Supervisors.

Data Collection

Definition: The process of receiving or acquiring data from a user, device or entity including third party data providers.
3.1 Is Personally Identifiable Information (**PII**)* intentionally *or unintentionally* captured by the technology? *__PII__ is 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. PII includes, but is not limited to, the following: • *Personal information* (e.g. name, personal address/email, social security number, date of birth, age, end user IP address, GPS of an end user, IMSI numbers, marital status, health information, financial information, social services, personal utilities data) • *Individual and group characteristics* (e.g. race, ethnicity, religion, national origin, income level, sexual orientation, or political perspective) • *Biometric information* (e.g. facial, voice, gate, fingerprints, thermal, olfactory, etc.)
YES
3.2 Please identify all types of data collected by the surveillance technology. STP, ASR Please include the following data types that are collected, processed, retained, or shared by the surveillance technology:

[1] Privacy in Technology: Standards and Practices for Engineers and Security and IT Professionals. *An IAPP Publication* (2016).

- Non-sensitive data types

PII, intentionally *and* unintentionally captured

- *Digital images of vehicle license plates and their license plate numbers;*
- *Date and time stamps; and*
- *Geo-location.*

3.2 This is a three-part question:

a) Please identify all types of data collected by the surveillance technology. [STP, ASR]

Please list the non-sensitive data types and any personal information that is intentionally or unintentionally collected, processed, retained, or shared by the surveillance technology (e.g. barcode, aerial images of treetops, facial images, voice audio, pick up and drop off location, etc.).

b) Please indicate the data format in which the information is stored, copied, and/or processed. [STP] (e.g. XML, PDF, HTML, Plain Text, TIFF, JPEG, PNG, GIF, SHP, MOV, AVI, MP3, XMI, CSV, etc.)

c) Using the Data Classification Standard, please classify each type of data identified.

Data Type(s)	**Format(s)**	**Classification**
Digital images	*JPEG on device; proprietary format in server (g64m).*	*Level ~~2~~3*
Date & time stamps	*SQL on device; proprietary format in server (g64m).*	*Level 3*
Geo-location	*SQL on device; proprietary format in server (g64m).*	*Level 3*

3.3 Does the department have different access control, data sharing, data retention and/or data sharing requirements for each of the 5 classification levels listed above?

Yes

3.4 Is data stored in vendor proprietary format or an interoperable format? [ASR]

Data are stored in interoperable format on devices and in vendor proprietary format in server.

3.5 Identify the general location(s) where the surveillance technology may be deployed. [SIR]

Citywide on streets and off-street parking lots.

3.6 Where applicable, a general breakdown of what physical objects the Surveillance Technology hardware was installed upon. [ASR]

If not applicable because the technology is a software, please provide a general breakdown of what data sources the Surveillance Technology was applied to. [ASR]
SFMTA parking enforcement vehicles.
3.7 On average, how many hours per week does the surveillance technology operate?
96 hours
3.8 Was public notice given in the form of a physical sign on premises or through a terms of use agreement?
No
3.9 Please check all items that are included in the public notice.
None.
3.10 How can members of the public register complaints or concerns, or submit questions about the deployment of the Surveillance Technology? [STP]
Through 311.org or by directly contacting the SFMTA Parking Enforcement and Traffic Division.
3.11 How will the department ensure each question and complaint is responded to in a timely manner? [STP]
Questions and complaints received through 311.org are tracked through that system's tracking database; questions and complaints submitted directly to the SFMTA are tracked using Salesforce's case management software.
3.12 How will the department oversee and enforce compliance with the Surveillance Technology Policy (i.e. personnel responsible for oversight, compliance policies & procedures, internal recordkeeping, etc.)? [STP]
The Director of Parking Enforcement and Traffic will enforce and assign staff members under their direction to oversee compliance with the Surveillance Technology Policy. Principal Administrative Analyst from Finance and Information Technology Division will oversee pilots of ALPR technology.
3.13 Please provide the title(s) of personnel assigned to oversee Surveillance Technology Policy compliance. [STP]
Commander of Parking Enforcement and Traffic; IT Operations Support Admin; Principal Administrative Analyst from Finance and Information Technology Division.
3.14 Please describe the sanctions for violations of the Surveillance Technology Policy. [STP]

Violations of the Surveillance Technology Policy will result in disciplinary action commensurate with the violation. Sanctions include written warning, suspension, and termination of employment.

Data Processing & Use

Definition: The use or processing of information for any purpose beyond simple storage and deletion, including but not limited to use in analytics, reporting or in combination with other data.	
3.15 Who primarily accesses or uses data for authorized purposes? [STP]	
Employee Job Classification & Title: [STP]	*8214 – Parking Control Officer(s)* *1824 – Principal Administrative Analyst* *1823 – Sr. Administrative Analyst* *5277 – Planner I* *5288 – Transportation Planner II* *5289 – Transportation Planner III* *5290 – Transportation Planner IV*
Department:	*SFMTA - Sustainable Streets Division*
If applicable, contractor or vendor name:	*N/A*
3.16 Describe the rules and processes required prior to data access or use. [STP]	
Only authorized users may use ALPR or access ALPR data. Authorized user must complete mandatory training and obtain login credentials.	
3.17 Describe any restrictions on how and under what circumstances data can be accessed or used. [STP]	
Authorized users must have login credentials to access ALPR data.	
3.18 What safeguards and technical measures will be implemented to protect information from unauthorized access and use, including misuse? [STP]	
• *Users require unique login credentials to access the ALPR system; system is accessible on portable tablets (used in vehicles) and on desktop workstations;* • *Users approved to access ALPR devices and ALPR data under these guidelines are permitted access only for uses authorized under the Surveillance Technology Policy; and*	

• *All activity in the ALPR system is logged and can be audited.*
3.19 Is surveillance technology data secured during transmission and during rest?
Yes
3.20 Is training required for authorized individuals to use or access the information collected? [STP]
Yes
3.20a [If yes] Describe the required training. [STP]
The training for users to access the information collected in the field consists of classroom training provided by a Genetec authorized trainer. Training covers functionality of the system, use of the software; searching plates in the system, identifying hits and validation procedures and login and logoff procedures. *For backend users, training is also conducted by a Genetec authorized trainer and includes access and use of the software to generate reports, validate each systems status in real time, system settings including access rights. Access is restricted by the system administrator by user rights control settings.*
3.21 Will your department maintain audit logs for data access? [STP]
Yes
3.22 Is the Department's continued use of the surveillance technology reliant on services or equipment from any entity or individual? [STP, ASR]
Yes
3.22a [If Yes] Please identify the entity or individual that provides services or equipment essential to the functioning or effectiveness of the Surveillance Technology. [STP, ASR]
• *Conduent Technology – Citation-processing contractor* • *Genetec – ALPR vendor (subcontractor to Conduent Technology)*
3.23 Is data handled (i.e. used or processed) or stored by an outside provider or third-party vendor on an ongoing basis? [SIR]
Yes
3.23a [If Yes] Please identify the vendor.
Genetec

3.23b [If Yes] Is data handling or storage by a third-party vendor required for the department to use or maintain the surveillance technology? SIR
No

Data Sharing

Definition: The disclosure or sharing of information external to the department collecting it.
3.24 Is any data acquired by this technology been shared with entities outside the City and County of San Francisco? ASR
Yes
3.24a [If Yes] Name of recipient: STP, ASR
Genetec
3.24b [If Yes] How often will data be shared? ASR
Continuously.
3.24c [If Yes] What type of data will be disclosed? ASR
All data collected.
3.24d [If Yes] Under what legal standard was the data disclosed? ASR, STP
~~*N/A [I don't think this applies anymore.]*~~ *Under contract terms.*
3.24e [If Yes] Describe the justification for the disclosure? ASR
~~*They are the venfor of the ALPR technology.*~~*Vendor stores data under contract terms.*
3.25 Is any data acquired by this technology been shared with entities inside the City and County of San Francisco (e.g. other departments, divisions, or units)? STP
Yes
3.25a [If Yes] Name of recipient: STP, ASR
SFMTA Administrative Hearings
3.25b [If Yes] How often will data be shared? ASR
If requested. SFMTA Administrative Hearings infrequently requests data.

3.25c [If Yes] What type of data will be disclosed? ASR
Digital images, date and time stamps, and/or geo-location.
3.25e [If Yes] Describe the justification for the disclosure? ASR
SFMTA Administrative Hearings uses ALPR data to validate contested parking citations in public-parking spaces throughout the City.
3.26 How will the department ensure that any entity (internal and external) receiving data collected by the Surveillance Technology complies with the Surveillance Technology Policy? STP
The SFMTA will provide a copy of the Surveillance Technology Policy when it shares ALPR data.
3.27 Will the data be accessible or available for use by members of the public, including criminal defendants? STP
Yes
3.27a [If yes] Describe how data can be accessed by the public, including criminal defendants. STP
ALPR data will be provided to the public unless exempted under applicable law. For public requests for data, the SFMTA shall confer with the City Attorney's Office to determine whether the requested data are exempt from disclosure or are legally required to be disclosed.

Data Retention

Definition: The persistence or storage of data by a department after its collection.
3.28 What is the department data retention standard for data collected by the surveillance technology? STP
Data stored on ALPR devices are purged on every 24 hours. *ALPR data downloaded to the ALPR vendor's server are retained as follows:* • *Digital images not associated with parking citations are retained for seven days;* • *Digital images associated with parking citations are retained for 365 days;* • *Metadata (i.e., license plate numbers, time and date stamps, and geo-location) are retained for 365 days.* • *Anonymized ALPR data will be retained indefinitely for planning purposes.*
3.29 Describe the justification for the retention period. STP
Data on ALPR devices are stored for 24 hours to ensure uploading to ALPR vendor's server.

For ALPR downloaded to the ALPR vendor's server: • *Digital images not associated with a parking citation are retained for seven days to allow enforcement of 72-hour parking restrictions – the PCOs requires imaged taken at least 72 hours apart to enforce restrictions;* • *Digital images associated with parking citations are retained for 365 days to support validation of contested parking citations at SFMTA Administrative Hearings; and* • *Metadata (i.e., license plate numbers, time and date stamps, and geo-location) are retained for 365 days for use by SFMTA Parking and Curb Management to analyze and determine occupancy and turnover rates in public-parking spaces*
3.30 Under what condition(s) is data retained beyond this period? STP
Only if required by law.
3.31 Please identify where collected data is stored.
[check boxes for the below] - *Local storage - While data are in ALPR devices* - *Department of Technology Data Center – N/A* - *Software as a Service Product- N/A* - *Cloud Storage Provider – When downloaded from device.*

Data Disposal

Definition: The destruction of data at the end of its lifecycle, including the deletion of files, clearing of records from a database, or removal of data from a file.
3.32 Describe department practices to dispose data when the retention period ends. STP
Vender purges ALPR data at the end of applicable retention period.
3.33 Describe any processes or applications used to remove personal identifiable information or restricted data when needed (i.e. scrubbing or de-identification).
The SFMTA will use ALPR data to determine parking utilization and turnover rates at public parking spaces Citywide. The ALPR vendor will de-identify these data by replacing license plate numbers with unique identifiers before data are provided to the SFMTA.

III. Potential Impacts and Mitigation

Best completed by: Business Owner and Department Information Security Officer

As part of the Surveillance Impact Report, the Acquisition of Surveillance Technology Ordinance includes the following requirement:

> *"An assessment identifying any potential impact on civil liberties and civil rights and discussing any plans to safeguard the rights of the public;"*

The following section uses the draft National Institute of Standards and Technology (NIST) Privacy Framework to identify potential impacts that may result from the use of surveillance technologies. The 7 different impacts identified include:

- *Dignity Loss:* Includes embarrassment and emotional distress
- *Discrimination:* Unfair or unethical differential treatment of individuals or denial of civil rights
- *Economic Loss*: Direct financial losses as a result of identity theft or the failure to receive fair value in transaction due to misidentification, etc.
- *Loss of Autonomy*: Loss of control over decisions on how personal information is used or processed, or by whom it is used or processed
- *Loss of Liberty*: Improper exposure to arrest or detainment due to incomplete or inaccurate data
- *Physical Harm*: Physical harm or death
- *Loss of Trust*: Breach of implicit or explicit expectations or agreements about the processing of data, or failure to meet subjects' expectation of privacy for information collected.

In the following section, please provide a response to how your department's authorized use considers and mitigates adverse impacts.

Tool: Please refer to the *Surveillance Technology Impacts Defined* document for detailed definitions and impact examples.

Instructions: Your department's response should show that it has considered the above potential impacts and has thought through the technical, administrative, and physical* protections that mitigate these impacts. If an impact does not apply, please detail why not, being sure to mention the applicable safeguards or technology/data limitations that make impact negligible or nonexistent.

Helpful hint: Department responses to toolkit questions 1.3, 1.5, 1.6, 3.8-2.9, 3.12-3.13, 3.16-3.18, 3.19, and 3.20 may be helpful in describing department mitigation strategies and safeguards.

*Safeguards defined:

- *Administrative Safeguards*: Policies & procedures, such as documentation processes, roles and responsibilities, training requirements, data maintenance policies, and more.
- *Technical Safeguards*: Technical measures (i.e. encryption, pseudonymization, etc.) to properly secure data and systems from unauthorized access, whether at rest or in transit.

Physical Safeguards: Measures to ensure data and data systems are physically protected, such as security systems, video surveillance, door and window locks, secured server and computer locations, and policies about mobile devices and removing hardware/software from certain locations.

4.0 Using the instructions above, describe how your department addresses the potential civil rights/liberties impacts associated with the surveillance technology.

- *Dignity Loss: Administrative safeguards make this impact (e.g., embarrassment and emotional distress) negligible because the ALPR cameras take photos of vehicle tires and rears (including rear license plates) of parked vehicles, which are typically unattended; they do not capture images of vehicle occupants. Occasionally, images may include pedestrians, but these images are generally not available to the public and are purged from the ALPR system within seven days unless associated with a citation.*

- *Discrimination: ALPR is used to enforce time-limited parking regulations and identify scofflaw (i.e., five or more unpaid parking violations) and stolen vehicles. Time-limited parking enforcement - administrative safeguards make this impact (i.e., unfair or unethical differential treatment of individuals or denial of civil rights) negligible because ALPR technology is deployed equally in areas throughout the City where restrictions apply, and such restrictions are typically requested by the majority of residents in the corresponding communities. Scofflaw and stolen vehicles – administrative safeguards make this impact negligible because ALPR technology is deployed for this purpose throughout the SFMTA's jurisdiction.*

- *Economic Loss: Technical safeguards make this impact (e.g., identify theft/misidentification) negligible or non-existent because the ALPR system has no access to information identifying individuals, including vehicle owners or drivers; PCOs use separate technology to issue parking citations.*

- *Loss of Autonomy: Technical safeguards make this impact (e.g., loss of control over decisions on how personal information is used or processed) negligible or non-existent because the ALPR system has no access to information identifying individuals, including vehicle owners or drivers; PCOs use separate technology to issue parking citations.*

  The SFMTA's planned use of time, date, and geo-location data over time to determine parking occupancy and turnover rates may reveal information about personal travel patterns. However, administrative and technical safeguards make this impact negligible because the SFMTA does not share personal information it collects and will replace license plate numbers with a unique identifier that cannot be traced to a vehicle or person.

- *Loss of Liberty*: *Administrative safeguards make this impact (i.e., improper exposure to arrest or detainment due to incomplete or inaccurate data) negligible because PCOs validate data before taking any action. Before issuing citations for exceeding time-limited parking restrictions, PCOs visually compare images to confirm whether vehicles moved the minimum distance required to avoid citations; a similar validation process occurs when PCOs manually chalk vehicles. Before taking action on scofflaw or stolen vehicles, PCOs radio SFMTA Parking Enforcement Dispatch to verify vehicles have five or more outstanding parking citations or are reported stolen, as applicable.*

- *Physical Harm*: *Technical safeguards make this impact (e.g., physical harm or death) negligible or non-existent because the ALPR system has no access to information identifying individuals, including vehicle owners or drivers) negligible or non-existent; PCOs use separate technology to issue parking citations.*

  The SFMTA's planned use of time, date, and geo-location data over time to determine parking occupancy and turnover rates may reveal information about personal travel patterns and routine locations. However, administrative and technical safeguards make this impact negligible because the SFMTA does not share personal information it collects and will replace license plate numbers with a unique identifier that cannot be traced to a vehicle or person.

- *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) negligible or non-existent because license plate numbers are used only to identify vehicles for purposes of determining parking violations, scofflaws, and whether they are stolen.*

  The SFMTA's planned use of time, date, and geo-location data over time to determine parking occupancy and turnover rates may reveal information about personal travel patterns and routine locations. However, administrative and technical safeguards make this impact negligible because the SFMTA does not share personal information it collects and will replace license plate numbers with a unique identifier that cannot be traced to a vehicle or person.