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. Potential Impacts & Mitigation

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 2-3 hours per technology.

Department:	*Municipal Transportation Agency*
Technology Category:	*ALPR*
Name of the Technology:	*ALPR – City-Owned Parking Garages*
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*

A. 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 link parking tickets to vehicles parked in City-owned garages to calculate parking fees. This use supports the SFMTA's mission because it maximizes the integrity of parking revenues, which the SFMTA uses to fund elements of the larger transportation system, including transit.	
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. Click "Insert Item" for each additional use case.*	
Authorized Use Case #1	*Links individual vehicles to their times of entry into City-owned parking garages to accurately calculate parking fees.*
~~Authorized Use Case #2~~	~~*Identify vehicles parked in City-owned garages that are listed on SFPD's hotlist of stolen vehicles. (The SFMTA does not generate hotlists.)*~~
Authorized Use Case #~~3~~2	*Identify vehicles parked in City-owned garages that are the subject of an active investigation by the SFPD (e.g., stolen vehicles, amber alerts, arrest warrants), but only if requested by the SFPD.*
1.4 For the Authorized Use cases described above, identify alternative methods to accomplish these tasks without the use of the surveillance technology.	
There is no alternative to use case #1. At best, parking garage attendants would manually document vehicles parked overnight to estimate parking durations to assist in calculating fees when patrons lose tickets. *ALPR automates the functions described authorized use cases #2 and #3; without ALPR those functions would be performed manually by parking garage staff or contractors.*	
1.5 Please list any prohibited uses for the surveillance technology and data collected. 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. Fixed cameras are mounted on ceilings or poles inside City-owned parking garages. Cameras are triggered only when vehicles are moving over an arming loop, and cameras are positioned to focus only on license plates.

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.

1.6a Is the technology a physical piece of equipment (i.e. hardware or device)?

Yes

1.7 Provide the product description from the manufacturer. [SIR]

VRS-N60E vandal-proof 2MP IP imaging unit with customized illumination for optimum LPR performance in low light and under all weather conditions, for essential logistics and security performance VRS-N60E provides precision and efficiency in low-to-mid speed access control, parking and security/surveillance applications, including critical facilities – for all reflective and nonreflective license plate types.

The highly reliable, compact VRS-N60E Imaging unit features state-of-the-art hardware along with HTS's powerful, patented PC-based license plate recognition (LPR) and VRS-SeeControl management software. The hardware is optimized specifically for high performance with HTS software applications. With its built-in VRS Controller Application, the VRS-N60E provides maximum effectiveness as it's specifically engineered for optimal accuracy, confidence and vehicle recognition solutions.

HTS Imaging Units and value-added HTS solutions are field-proven in over 40 countries worldwide, including the United States. Sophisticated HTS algorithms identify both the state and country of any license plate.

The VRS-N60E's live IP video streaming extends functionality to real-time monitoring applications, providing both an image of the license plate and video stream of the event.

1.8 From the list below, select the areas where the surveillance technology's use or data might benefit residents, and describe how:

[below listed with check boxes in two columns, with description line if selected]

- *Education: N/A*
- *Community Development: N/A*

- *Health: N/A*
- *Environment: N/A*
- *Criminal Justice: Identifies vehicles reported to, and that are subject to an active investigation by, the SFPD.*
- *Public Safety: Identifies vehicles reported to, and that are subject to an active investigation by, the SFPD.*
- *Jobs: N/A*
- *Housing: N/A*

Other [Parking Enforcement]: None

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)

[below listed with check boxes in two columns, with description line if selected]

- *Financial savings: Reduces the need for attendants at City-owned parking garages; parking garage staff can be consolidated at command centers that serve all garages or reassigned to perform duties the SFMTA used to outsource (e.g., painting, janitorial, and maintenance).*
- *Time savings: Helps parking garage staff manage multiple parking garages simultaneously from a central location.*
- *Staff safety: Parking staff no longer required to work within confined areas in parking garages.*
- *Improved data quality: Improves data required to calculate parking fees, especially when patrons lose their tickets.*

1.10 Please list any other benefits not already captured above.

None

Best completed by: Financial Staff

2.0 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 (new & existing)	*None. Tool used by parking vendor's staff to assist with frictionless parking and exception transactions such as lost tickets. No separate staff used to opeate cameras.*

Classification	*N/A*
Total Salary & Fringe	*N/A*
Hardware/Equipment/Software	*$587,181*
Professional Services	*$17,500*
Training	*$850*
Other	
Total Cost [Auto-calculate]	
2.1 Please disclose any current or potential sources of funding (e.g. potential sources = prospective grant recipients, etc.). SIR, ASR	
SFMTA Capital Improvement Project (CIP) Budget for initial system; SFMTA Operating Budget for ongoing operations.	

B. 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.

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

3.1 Is Personal Information (**PI**)* intentionally or unintentionally captured by the technology?

*__PI__ 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.

PI includes, but is not limited to, the following:

Name, signature, social security number, physical characteristics or description, address, geolocation data, IP address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, genetic and biometric data, health insurance information, race, ethnicity, religion, national origin, income level, sexual orientation, or political perspective.

Yes

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*	*Level 2*
Date & time stamps	*SQL*	*Level ~~2~~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

Vendor proprietary format

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

City-owned parking garages.

3.6 Where applicable, a general breakdown of what physical objects the Surveillance Technology hardware is installed upon. [ASR] If not applicable because the technology is a software, please provide a general breakdown of what data sources the Surveillance Technology is applied to. [ASR]
Pole or celling mounted depending on location.
3.7 On average, how many hours per week does the surveillance technology operate?
24 hours a day, seven days a week.
3.8 Is public notice given in the form of a physical sign on premises or through a terms of use agreement?
Yes
3.9 Please check all items that are included in the public notice.
- *Information on the surveillance technology - Yes* - *Description of the authorized use - Yes* - *Type of data collected - Yes* - *Contact information - Yes*
3.10 How can members of the public register complaints or concerns, or submit questions about the deployment of the Surveillance Technology? [STP]
The public may register complaints or concerns, or submit questions about the ALPR through 311.org or email the SFMTA Parking Division parcs@sfmta.com.
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 by the Operations Manager, SFMTA Parking and Curb Management.
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 Operations Manager, SFMTA Parking and Curb Management will enforce and assign staff members under their direction to oversee compliance with the Surveillance Technology Policy.
3.13 Please provide the title(s) of personnel assigned to oversee Surveillance Technology Policy compliance. [STP]

Operations Manager, SFMTA Parking and Curb Management; Principal Analyst.
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	*SFMTA contractors primarily access/use ALPR data.*
Department:	*SFMTA contractors primarily access/use ALPR data.*
If applicable, contractor or vendor name:	*Reef Parking (d.b.a. Impark)* *LAZ*
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 users must complete mandatory training and obtain login credentials. Operations Manager, SFMTA Parking and Curb Management approves all authorized users.	
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 vendor work stations;* • *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
Training provided to third-party parking operators on how to look up license plate numbers in database to recreate lost tickets. Operators do not have access to personal information or other data that could be linked to license plate numbers.
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
Skidata (Parking Access and Revenue Control System (PARCS) vendor)
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
No (data are stored on SFMTA cloud network)
3.23a [If Yes] Please identify the vendor.
N/A
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
N/A

Data Sharing

Definition: The disclosure or sharing of information external to the department collecting it.

3.24 Is any data acquired by this technology shared with entities outside the City and County of San Francisco? ASR
No
3.24a [If Yes] Name of recipient: STP, ASR
N/A
3.24b [If Yes] How often is data shared? ASR
N/A
3.24c [If Yes] What type of data is disclosed? ASR
N/A
3.24d [If Yes] Under what legal standard is the data disclosed? ASR, STP
N/A
3.24e [If Yes] Describe the justification for the disclosure? ASR
N/A
3.25 Is any data acquired by this technology shared with entities inside the City and County of San Francisco (e.g. other departments, divisions, or units)? STP
3.25a [If Yes] Name of recipient: STP, ASR
No
3.25b [If Yes] How often is data shared? ASR
N/A
3.25c [If Yes] What type of data is disclosed? ASR
N/A
3.25d [If Yes] Under what legal standard is the data disclosed? ASR, STP
N/A
3.25e [If Yes] Describe the justification for the disclosure? ASR

N/A
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
N/A
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
Data not generally available to the public; data available through subpoena.

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
• *Digital images retained for 60 days after customer exits garage before being purged from database;* • *Data (image information converted) stored for archive reporting 2 years maximum;* • *If License plate is used as a credential for entry and exit (frictionless parking or reservation) license plate information stored for as long as individual is using that credential (like an access card)*
3.29 Describe the justification for the retention period. STP
Used maximum ALPR data retention allowed under law for CHP.
3.30 Under what condition(s) is data retained beyond this period? STP
Where ALPR data is used in pending criminal investigations.
3.31 Please identify where collected data is stored.
[check boxes for the below] - *Local storage - No*

- *Department of Technology Data Center – Yes. Plattech Database for 60 days (image), Report database 2 years for archive reporting purposes. SKIDATA database Access control indefinitely if the License plate is used as a credential for entering and exiting facility*
- *Software as a Service Product - No*
- *Cloud Storage Provider - No*

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
Automatic purging ALPR data at the end of applicable retention period for transient customers. License plate data for monthly parkers can still be kept if the data is used for credential purposes to enter and exit the garage (frictionless parking).
3.33 Describe any processes or applications used to remove personal identifiable information or restricted data when needed (i.e. scrubbing or de-identification).
None.

C. 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.

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.

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

- *Dignity Loss: Technical safeguards make this impact (e.g., embarrassment and emotional distress) negligible or nonexistent because the ALPR cameras take photos of vehicle license plates only; they do not capture images of vehicle occupants. Cameras are triggered only when vehicles are moving over an arming loop, and cameras are positioned to focus only on license plates. Cameras would capture images of a person only if they were in between the license plate and camera when the vehicle is driving over a loop, which is unlikely.*

- *Discrimination: Technical safeguards make this impact (i.e., unfair or unethical differential treatment of individuals or denial of civil rights) nonexistent because it does not distinguish among SFMTA parking garage customers who consent to its use.*

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

- *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.*

- *Loss of Liberty: Administrative safeguards make this impact (i.e., improper exposure to arrest or detainment due to incomplete or inaccurate data) non-existent because SFPD validate data (i.e., they confirm vehicle they seek are in parking garages associated with corresponding license plates) before taking any action.*

- *Physical Harm: Technical safeguards make this impact (e.g., physical harm or death) non-existent because the ALPR system has no access to information identifying individuals.*

- *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 to associate vehicles with their corresponding parking ticket so the SFMTA can accurately determine parking fees for lengths of stay.*