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. Potential Impacts & Mitigation
C. Data Management Process & Lifecycle

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:	
Technology Category:	
Name of the Technology:	
Is this an existing technology already in use by your department, or a proposed new technology?	
Custodian of Records:	

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

Best completed by: Business Owner
1.1 What is your Department's mission statement?
1.2 Describe how the surveillance technology is used to support your department's mission. [SIR]

Commented [CN1]: Renamed from "Risks"

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	
Authorized Use Case #2	
[Repeat as needed]	

1.4 For the Authorized Use cases described above, identify alternative methods to accomplish these tasks without the use of the surveillance technology.
1.5 Please list any prohibited uses for the surveillance technology and data collected. STP
1.6 Describe what the technology does and how it works. SIR, STP
1.6a Is the technology a physical piece of equipment (i.e. hardware or device)?
[Y/N]
1.7 Provide the product description from the manufacturer. SIR
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 • Community Development • Health • Environment • Criminal Justice • Public Safety • Jobs • Housing

Commented [CN2]: Added text for additional clarity in SharePoint form.

Commented [CN3]: Added text.

Commented [CN4]: New question added. Will be used to determine if public notice is necessary. Public notice only to be included in Surveillance Technology Policies for physical equipment/hardware.

• Other
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 • Time savings • Staff safety • Improved data quality • Other
1.10 Please list any other benefits not already captured above.
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 (new & existing)	
Classification	
Total Salary & Fringe	
Software	
Hardware/Equipment	
Professional Services	
Training	
Other	
Total Cost [Auto-calculate]	

1.12 Please disclose any current or potential sources of funding (e.g. potential sources = prospective grant recipients, etc.). SIR, ASR

II. Potential Impacts and Mitigation

Commented [CN5]: Renamed from "Risks"

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.

*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.

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

Commented [CN6]: Language and instructions updated for clarify.

Commented [CN7]: Slightly re-worded.

III. 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 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

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

biometric data, health insurance information, race, ethnicity, religion, national origin, income level, sexual orientation, or political perspective.

[Y/N]

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
[Multiple Lines of Text]	*[Multiple Lines of Text]*	*[Drop down list "Level 1- Level 5]*

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?

[Y/N]

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

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

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

Commented [CN8]: Language and definitions updated to more closely match language of SF Charter, CCPA, and GDPR.

Commented [CN9]: Revised to combine and replace previous questions 3.2, 3.3 & 3.6.

Commented [CN10]: Questions 3.3 – 3.33 renumbered to account for combined 3.2.

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]
3.7 On average, how many hours per week does the surveillance technology operate?
3.8 Is public notice given in the form of a physical sign on premises or through a terms of use agreement?
[Y/N]
3.9 Please check all items that are included in the public notice.
[check boxes for the below] - Information on the surveillance technology - Description of the authorized use - Type of data collected - Will persons will be individually identified - Data retention - Department identification - Contact information
3.10 How can members of the public register complaints or concerns, or submit questions about the deployment of the Surveillance Technology? [STP]
3.11 How will the department ensure each question and complaint is responded to in a timely manner? [STP]
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]
3.13 Please provide the title(s) of personnel assigned to oversee Surveillance Technology Policy compliance. [STP]

3.14 Please describe the sanctions for violations of the Surveillance Technology Policy. STP

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	
Department:	
If applicable, contractor or vendor name:	
3.16 Describe the rules and processes required prior to data access or use. STP	
3.17 Describe any restrictions on how and under what circumstances data can be accessed or used. STP	
3.18 What safeguards and technical measures will be implemented to protect information from unauthorized access and use, including misuse? STP	
3.19 Is surveillance technology data secured during transmission and during rest?	
[Y/N]	
3.20 Is training required for authorized individuals to use or access the information collected? STP	
3.20a [If yes] Describe the required training. STP	

3.21 Will your department maintain audit logs for data access? STP
[Y/N]
3.22 Is the Department's continued use of the surveillance technology reliant on services or equipment from any entity or individual? STP, ASR
[Y/N]
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
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
[Y/N]
3.23a [If Yes] Please identify the vendor.
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
[Y/N]

Commented [CN11]: Split into two questions (3.22 & 3.22a) and re-worded.

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
3.24a [If Yes] Name of recipient: STP, ASR
3.24b [If Yes] How often is data shared? ASR
3.24c [If Yes] What type of data is disclosed? ASR

3.24d [If Yes] Under what legal standard is the data disclosed? ASR, STP
3.24e [If Yes] Describe the justification for the disclosure? ASR
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
3.25b [If Yes] How often is data shared? ASR
3.25c [If Yes] What type of data is disclosed? ASR
3.25d [If Yes] Under what legal standard is the data disclosed? ASR, STP
3.25e [If Yes] Describe the justification for the disclosure? ASR
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
3.27 Will the data be accessible or available for use by members of the public, including criminal defendants? STP

3.27a [If yes] Describe how data can be accessed by the public, including criminal defendants. STP

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
3.29 Describe the justification for the retention period. STP
3.30 Under what condition(s) is data retained beyond this period? STP
3.31 Please identify where collected data is stored.
[check boxes for the below] - Local storage - Department of Technology Data Center - Software as a Service Product - Cloud Storage Provider

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
3.33 Describe any processes or applications used to remove personal identifiable information or restricted data when needed (i.e. scrubbing or de-identification).