# 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: | *Port of San Francisco* |
| Technology Category: | *Surveillance* |
| Name of the Technology: | *Unmanned aerial vehicles ("UAV" or "Drone" technology)* |
| Is this an existing technology already in use by your department, or a proposed new technology? | |
| *Technology is used by contractors. There are no UAV or Drones used by The Port* | |
| Custodian of Records: | *Randy Quezada* |

## A. Business Uses (i.e. the benefits)

| **Best completed by: Business Owner** |
|---|
| 1.1 What is your Department's mission statement? |
| *The Port of San Francisco manages the waterfront as the gateway to a world-class city and advances environmentally and financially sustainable maritime, recreational, and economic opportunities to serve the City, Bay Area region, and California* |

| 1.2 Describe how the surveillance technology is used to support your department's mission. [SIR] |
|---|
| *Drone technology will support our mission through the following:*<br>*1. Drones will provide the Port Department Operations Center (DOC) with high resolution images during response and recovery operations after a disaster.*<br>*2.*<br>*3. Drones will support the objective of maintaining city owned properties and landscapes by safely providing detailed photographic data and documentation to assist in the planning of corrective or new construction work by roofers, engineers, electricians, PMs, CMs and other personnel.* |

| 1.3 **Authorized Use Cases:** Please list all the distinct ways in which the department is authorized to use the surveillance technology.<br>*Please be as specific as possible. Click "Insert Item" for each additional use case.* | |
|---|---|
| Authorized Use Case #1 | *Disaster preparedness and response* |
| Authorized Use Case #2 | *Environmental monitoring and documentation* |
| Authorized Use Case #3 | *Inspect/Survey properties & assets* |
| Authorized Use Case #4 | *Project inspection and documentation* |
| Authorized Use Case #5 | *Surveying/Mapping data collection* |

| 1.4 For the Authorized Use cases described above, identify alternative methods to accomplish these tasks without the use of the surveillance technology. |
|---|
| *Use Case #1: Traditional methods during disaster response or major event response generally involve sending personnel into the field and communicating via two way or cellular phones and utilizing video cameras for live feeds to the DOC for logistics, planning, and execution of operations.*<br>*Use Case #2: Other than google satellite imagery, real time overhead/aerial data to determine canopy health is currently unavailable by any method other than BUF personnel physically ascending trees, a hazardous procedure. When evaluating trees that may require removal inspectors must visit the trees in person in order to make a thorough evaluation.*<br>*Use Case #3: In lieu of drones, inspections must be conducted by personnel and will often involve use of scaffolding, ladders, swing stage and other types of equipment to safely reach areas in need of inspection.*<br>*Use Case #4: Project inspection and documentation without drone technology is achieved by use of traditional camera photography and videography equipment.* |

| |
|---|
| *Use Case #5: Standard collection methods include use of surveying total stations and GNSS ("GPS"), as well as aerial photogrammetry and LiDAR data collection methods using airplanes.* |
| 1.5 Describe what the technology does and how it works. SIR, STP |
| *Drone technology incorporates unmanned, remotely operated aircraft with onboard visual recording equipment, for the purpose of capturing images from an aerial perspective.* |
| 1.5a Is the technology a physical piece of equipment (i.e. hardware or device)? |
| *Y* |
| 1.6 Provide the product description from the manufacturer. SIR |
| *Phantom 4 RTK is an aerial survey drone that combines centimeter-level navigation and positioning with a high-performance imaging system for use during surveying, mapping or inspection operations.* |
| 1.7 From the list below, select the areas where the surveillance technology's use or data might benefit residents, and describe how:<br><br>*[below listed with check boxes in two columns, with description line if selected]*<br><br>**Education:** *drone imagery to promote Public Works projects and demonstrate use of tax dollars on projects.*<br><br>Community Development<br><br>Health<br><br>**Environment:** *drone imagery to collect data on street-trees for maintenance and safety reasons.*<br><br>Criminal Justice<br><br>**Public Safety:** *to inspect tree canopies for damaged limbs (fall risks), to provide support when determining safety routes during emergencies, to collect data and information during emergencies (particularly in the event of loss of cellular communications) and during post-disaster cleanup operations.*<br><br>Jobs<br><br>Housing<br><br>Other |
| 1.8 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.**<br><br>~~*Please specify units and time period quantified (i.e. dollars vs. hours, weekly vs. annually, department-wide vs. per staff member)~~ |

Commented [EF1]: Did we change this format? If so, update instructions

| |
|---|
| *[below listed with check boxes in two columns, with description line if selected]*<br>**Financial savings:** *drones can be far more time efficient and cost effective when conducting asset inspections, by mitigating the need for traffic control, expensive scaffolding/swing stage or other equipment, and can provide more detailed photographs/videos of the assets or areas in need of maintenance or repairs than can be done manually, minimizing labor costs.*<br>**Time savings:** *deploying a drone can provide time savings over setting up and employing equipment such as scaffolds/swing stages/scissor-lift vehicles, etc.*<br>**Staff safety:** *drones can be deployed to dangerous locations instead of personnel, such as rooftops, at the sides of building/bridges, along cliff areas or areas prone to erosion.*<br>**Improved data quality:** *some locations which are difficult to access by personnel may be more easily photographed using drone technology, thereby achieving better data.*<br>Other |
| 1.9 Please list any other benefits not already captured above. |
| |

| **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) | | |
| Classification | | |
| | ***Annual Cost*** | ***One-Time Cost*** |
| Total Salary & Fringe<br>*(Fringe: Annual salary x .33)* | | |
| Software | | |
| Hardware/Equipment | | |
| Professional Services | | |
| Training | | |
| Other | | |

| | | |
|---|---|---|
| Total Cost [Auto-calculate] | | ***$233,800 per year*** |

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

**Personnel:** *Staff time devoted to use of drone for Inter-departmental work such as inspecting another agency's building can be charged to that agency as a line item cost. Time used to inspect Public Works assets will be charged as any other labor costs associated with project or inspection work.*

**Equipment:** *Funding to pay for cost of equipment purchase/lease and license for software to remove PII has been requested as part of the FY21 budget initiative process.*

## 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.

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:

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

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.

*[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]* |
| *Images/video of CCSF projects, assets, trees, etc.* | *JPGE, MOV, AVI* | *1 – Public* |
| *Images/video of CCSF projects, assets, trees, etc.* | *JPGE, MOV, AVI* | *2- Internal Use* |
| | | |
| | | |

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?

*N*

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

*Data will be stored in Public Works servers.*

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

***For city trees data collection:*** *Neighborhoods, parks, and other areas within San Francisco where City-owned street trees are located.*

***For asset/building data collection:*** *Islais Creek & Lefty O'Doul bridges, rooftops of City properties where solar panels or other equipment such as HVAC are located, or exterior walls of buildings, including schools, Police and Fire stations, public libraries, and other City owned buildings and facilities.*

***For Public Works project education/marketing/promotions:*** *various locations involving Public Works right-of-way or facility construction or repairs*

***For surveying/mapping activity:*** *survey site locations along streetscapes, landscape areas, steep hillsides and cliffs, at bridges and fixed structures such as piers, etc.*

***During disaster/emergency response operations:*** *Disaster areas, emergency evacuation routes, and other areas within San Francisco requiring Public Works safety response operations.*

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]

*Camera will be installed or built into aerial vehicle body*

3.7 On average, how many hours per week does the surveillance technology operate?

*Use is anticipated to be greatest for survey/mapping purposes; we estimate utilizing drone technology between 10-20 hours per week.*

3.8 Is public notice given in the form of a physical sign on premises or through a terms of use agreement?

*Y*

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 be individually identified** (*note: they will <u>not</u>* be)
- ✓ **Data retention** (any data that is retained beyond business use will be scrubbed of PII)
- ✓ **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 |
| *Members of the public can register complaints/concerns or submit questions via calls or emails at 311.org.*<br>~~*Members of the public can register complaints / concerns or submit questions at San Francisco Public Works Bureau of Street-Use and Mapping (BSM) 1155 Market Street, 3rd Floor San Francisco, CA 94103, 415-554-5810 or via calls/emails to 311.org.*~~ |
| 3.11 How will the department ensure each question and complaint is responded to in a timely manner? STP |
| *Constituent calls and complaints to the Bureau of Street-Use and Mapping (BSM) are received by counter personnel and routed to the bureau's Drone Program manager. Program manager will discuss concerns or complaints with constituent, enter details regarding nature of conversation on excel spreadsheet stored in Public Works shared drive, referred to as the drone Constituent Feedback Log ("CFL"). If additional action is required or requested by caller, Public Works commits to a follow-up (by email or telephone) within 48 hours. Department shall be prepared to host a viewing of edited imagery if caller is insistent, to demonstrate that no PII was collected. Depending upon the urgency or sensitivity of call, Drone Program manager shall notify bureau of details and discuss resolution before follow-up with caller. Final outcome and action(s) taken shall be logged onto CFL.*<br>***Public Works drone operators and Public Works management shall review log on a quarterly basis to discuss best practices, evaluate for learning lessons and opportunities to improve and refine the drone use program based on caller complaints, concerns and other community feedback.*** |
| 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 |
| *Two individuals will be assigned to maintain updates and perform required maintenance. A procedural pre-mobilization and post-mobilization safety check will be performed at each operation.* |
| 3.13 Please provide the title(s) of personnel assigned to oversee Surveillance Technology Policy compliance. STP |
| *Senior Administrative Analyst, BSM Deputy Bureau Manger* |
| 3.14 Please describe the sanctions for violations of the Surveillance Technology Policy. STP |

**Commented [EF2]:** Did we decide to provide a checklist of stock options here? I think we talked about including 311 as one of the options.

**Commented [13R2]:** I posted template language below

| |
|---|
| ***First offense**: violator shall be verbally notified by Public Works management of nature of violation.*<br>***Second offense**: violator shall notified in writing of second offence and privileges to operate drone hardware shall be suspended for 60 days.*<br>***Third offense**: (following reinstatement of operator privileges): violator shall be permanently banned from drone operations and disciplinary action may be taken depending upon the severity of second/third offences.* |

**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] | *7334 Stationary Engineer, 5310-13 Surveyor class series, 1823-27 Analyst class series; 0922-0954 Manager class series* |
| Department: | *San Francisco Public Works:*<br>*Bureau of Street Use & Mapping*<br>*Bureau of Urban Forestry*<br>*Bureau of Building Repair*<br>*Bureau of Engineering* |
| If applicable, contractor or vendor name: | |
| 3.16 Describe the rules and processes required prior to data access or use. [STP] | |
| *Distinctive personal features or license plate information collected inadvertently (if any) will be blurred using an approved editing software prior to use or storage of images (drone "data") for any business purposes. Once PII have been obscured or removed from images, data may be used by department based on use cases identified above and may be stored on servers for future use. RAW (unedited) data shall not be used or retained.* | |
| 3.17 Describe any restrictions on how and under what circumstances data can be accessed or used. [STP] | |
| *Data must always be scrubbed of PII as stated above prior to use.* | |

| |
|---|
| 3.18 What safeguards and technical measures will be implemented to protect information from unauthorized access and use, including misuse? [STP] |
| *Only authorized drone operators or PM may access unedited data.* |
| 3.19 Is surveillance technology data secured during transmission and during rest? |
| *Y* |
| 3.20 Is training required for authorized individuals to use or access the information collected? [STP] |
| Y |
| 3.20a [If yes] Describe the required training. [STP] |
| Data editors will be trained to properly utilize the editing software to ensure that all PII has been removed from still or video drone images before those images are released to other agencies or the public, or stored on servers for long term retention. |
| 3.21 Will your department maintain audit logs for data access? (Use the below template language and revise to fit department's plan) [STP] |
| A data access log will be maintained by the Department for all [insert technology] data that is processed and utilized. This log will include but is not limited to the following: date/time data was originally obtained/collected, reasons/intended use for data, Bureau/Section requesting data, name of data editor (ie, person accessing raw data for purpose of editing/scrubbing/blurring PII,) date/time of access of raw data, outcome of data processing and signed verification by data editor that all PII was removed, as well as date processed data was delivered to users. |
| 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, in the event we lease drones from a contractor, or utilize a contractor to obtain drone imagery.* |
| 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] |
| *At this point we are uncertain of specific contractors whose services may be required.* |
| 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] |
| *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]* |

**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 inside OR outside the City and County of San Francisco? (Include the below template language and add additional language as the department sees fit) ASR |
| • [Department] will endeavor to ensure that other agencies or departments that may receive data collected by [the ST that it operates] will act in conformity with this Surveillance Technology Policy.<br>• [Each department that believes another agency or department receives or may receive data collected from its use of STs should consult with its assigned deputy city attorney regarding their response.] |
| 3.24a [If Yes] Name of recipient: STP, ASR |
| |
| 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* |
| Before sharing data with any recipients, the Department will use the following procedure to ensure appropriate data protections are in place:<br>☐ Confirm the purpose of the data sharing aligns with the department's mission.<br>☐ Consider alternative methods other than sharing data by other means that can accomplish the same purpose.<br>☐ Redact names, scrub faces, and ensure all PII is removed in accordance with the department's data policies. |

**Formatted:** Indent: Left: 0"

**Formatted:** Indent: Left: 0.5"

| |
|---|
| ☐ Review of all existing safeguards to ensure shared data does not increase the risk of potential civil rights and liberties impacts on residents.<br>☐ Evaluation of what data can be permissibly shared with members of the public should a request be made in accordance with the San Francisco's Sunshine Ordinance.<br>☐ Ensure shared data will be done in a cost-efficient manner and exported in a clean, machine-readable format. |
| ~~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~~ |
| ~~*It is possible other department asset owners may review edited images (scrubbed of "PII") of assets Public Works is inspecting, maintaining/repairing or constructing on their behalf.*~~ |
| ~~3.25a [If Yes] Name of recipient: STP, ASR~~ |
| ~~*All SF Departments for which Public Works may provide services described in 3.27 response.*~~ |
| ~~3.25b [If Yes] How often is data shared? ASR~~ |
| ~~*Uncertain- will vary by case.*~~ |
| ~~3.25c [If Yes] What type of data is disclosed? ASR~~ |
| ~~*Images of assets (with PII removed or obscured)*~~ |
| 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 |
| *Public Works policy will prevent sharing data with any entities data that has not been edited to remove PII* |
| ~~3.27 Will the data be accessible or available for use by members of the public, including criminal defendants? (Include the below template language and add language as the department sees fit) STP~~ |

**Formatted:** Indent: Left: 0.5", Space Before: 0 pt, Line spacing: Multiple 1.15 li

**Formatted:** Font: Not Italic, Font color: Auto

- *[Department] will comply with the California Public Records Act, the San Francisco Sunshine Ordinance, the requirements of the federal and State Constitutions, and federal and State civil procedure laws and rules.*
- *[Each department should consult with their assigned deputy city attorney regarding their response.]*

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

~~*Members of the Public may request a release of edited images by contacting Rachel Gordon of Public Works in writing or by email.*~~

**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 Please list data retention schedules (i.e., x type of data will be retained for 1 year) based on the following categories:

- Permanent records (i.e., records that are essential): shall be retained and preserved indefinitely
- Current records (i.e., records for operational necessity, ready reference, convenience): record retention schedules may vary but generally less than 10 years
- Storage records (i.e., records retained offsite): record retentions may vary but generally less than 10 years

*Public Works will process raw data collected by drones as expeditiously as possible, removing or obscuring all PII. Only post-processed (i.e., "scrubbed") data will be maintained by Public Works per federal (FEMA) and state (OES) and local reimbursement and investigation requirements. Unedited data shall be deleted upon completion of processing.*

3.29 Describe the justification for the retention period. STP

*Scrubbed data will be maintained in Public Works servers for historical purposes.*

3.30 Under what condition(s) is data retained beyond this period? STP

*N/A*

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<br>✓ 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] |
| *Raw (unprocessed) data will be collected by the drone in the field, and stored on an onboard storage disc (i.e, "SD" card). Raw data (from the drone disc) will be downloaded from onboard storage disc onto secure Public Works servers by Drone Data Editor. Still or video frames will be identified for use by the appropriate Public Works data consumer (based upon pre-approved Public Works use cases.) Such data may include, as examples, images of buildings and structures, overhead images of topographic features, images of City tree canopy/limbs, and/or video images featuring Public Works project locations for use in Public Works TV episodes or other promotional materials. Once the subject image frames, still and/or video, have been identified for business needs, the Public Works Data editor will review all selected frames and identify each instance of PII (faces or license plates). All instances of PII will be blurred or obscured using editing software, such that no recognizable human features or license plate information remain. Once the subject image frames, still and/or video, have been identified for business needs, the Public Works Data editor will review all selected frames and identify each instance of PII (faces or license plates). All instances of PII will be blurred or obscured using editing software, such that no recognizable human features or license plate information remain. After processing and saving of edited data, all raw data will be permanently erased. Before replacing the SD storage cards into the drone, data editor will ensure the discs are completely free of all data.* |
| 3.33 Describe any processes or applications used to remove personal identifiable information or restricted data when needed (i.e. scrubbing or de-identification). |
| *All instances of PII will be blurred or obscured using editing software, such that no recognizable human features or license plate information remain.* |

## 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. |
| --- |
| *Public Works strives to mitigate all potential civil rights impacts through responsible technology and associated data use policies and procedures and intends to use drones and their associated data exclusively for authorized uses cases. All other uses, including surveillance of San Francisco residents or groups, are expressly prohibited.*<br><br>*Public Works drone operators/pilots will be prohibited from intentionally capturing data that can be used to identify individuals. Auto license plate information shall also not be deliberately captured. To mitigate the risk of potential embarrassment, emotional distress, self-censorship or diminished civic engagement by SF residents whose personal information may be unintentionally captured, Public Works requires the "scrubbing" or otherwise obscuring/blurring (through use of image editing software) of all collected data to remove facial images or other personally identifiable information unintentionally captured by aerial drones. All collected data, irrespective of the location of data capture or the identifying characteristics of captured persons, is subject to the same scrubbing processes and procedures. The image software scrubbing process obscures and blurs all data using either built-in AI recognition settings or through manual efforts by software operator.*<br><br>*To protect drone data from potential breach, misuse or abuse that may result in civil rights impacts, data is maintained on secure, department-owned servers. Only persons authorized to utilize the raw data may access the information and are required to maintain records of access using a drone data access log. Only data that has been edited to remove PII will be shared and stored on servers, and sharing will only occur with partner CCSF agencies for whom Public Works has been contracted to provide inspection, maintenance, repair, or construction services. To further protect data and any personal resident information captured by a drone, all raw data will be permanently erased after it has been processed and edited to blur or obscure human features and license plate information.*<br><br>*To mitigate any potential impacts to residents' physical safety or economic loss through property damage, all SFPW drone operators must have valid UAV pilot certifications.* |
| |