**File No.** 260334 **Committee Item No.** 1
**Board Item No.** _____

# COMMITTEE/BOARD OF SUPERVISORS

AGENDA PACKET CONTENTS LIST

**Committee:** Government Audit and Oversight **Date:** May 21, 2026
**Board of Supervisors Meeting:** **Date:** _____

## Cmte Board

| | | |
|---|---|---|
| ☐ | ☐ | **Motion** |
| ☐ | ☐ | **Resolution** |
| ☒ | ☐ | **Ordinance** |
| ☒ | ☐ | **Legislative Digest** |
| ☐ | ☐ | **Budget and Legislative Analyst Report** |
| ☐ | ☐ | **Youth Commission Report** |
| ☐ | ☐ | **Introduction Form** |
| ☐ | ☐ | **Department/Agency Cover Letter and/or Report** |
| ☐ | ☐ | **MOU - FY2022-2024 - Clean** |
| ☐ | ☐ | **MOU - FY2022-2024 - Redline** |
| ☐ | ☐ | **Grant Information Form** |
| ☐ | ☐ | **Grant Budget** |
| ☐ | ☐ | **Subcontract Budget** |
| ☐ | ☐ | **Contract / DRAFT Mills Act Agreement** |
| ☐ | ☐ | **Form 126 – Ethics Commission** |
| ☐ | ☐ | **Award Letter** |
| ☐ | ☐ | **Application** |
| ☐ | ☐ | **Public Correspondence** |

**OTHER**

| | | |
|---|---|---|
| ☒ | ☐ | Amended Drone Policy |
| ☒ | ☐ | Amended Illegal Dumping Camera System Policy |
| ☒ | ☐ | FYI Referral – April 15, 2026 |
| ☒ | ☐ | Public Works Introduction Memo – March 30, 2026 |
| ☐ | ☐ | |
| ☐ | ☐ | |
| ☐ | ☐ | |

**Prepared by:** John Carroll **Date:** May 14, 2026
**Prepared by:** _____ **Date:** _____
**Prepared by:** _____ **Date:** _____

[Administrative Code - Amendments to Public Works Surveillance Technology Policies]

**Ordinance approving amended Surveillance Technology Policies for the Department of Public Works' use of unmanned aerial vehicles ("Drones"), and the Department of Public Works' use of an illegal dumping camera system with automatic license plate reader technology and cameras; and making required findings in support of said approvals.**

NOTE: **Unchanged Code text and uncodified text** are in plain Arial font.
**Additions to Codes** are in *single-underline italics Times New Roman font*.
**Deletions to Codes** are in ~~*strikethrough italics Times New Roman font*~~.
**Board amendment additions** are in double-underlined Arial font.
**Board amendment deletions** are in ~~strikethrough Arial font~~.
**Asterisks (* * * *)** indicate the omission of unchanged Code subsections or parts of tables.

Be it ordained by the People of the City and County of San Francisco:

Section 1. Background.

(a) Terms used in this ordinance shall have the meaning set forth in Administrative Code Chapter 19B ("Chapter 19B").

(b) Chapter 19B regulates City departments' acquisition and use of Surveillance Technology, as defined in Chapter 19B. Under Section 19B.2(a), a department must obtain the approval of the Board of Supervisors ("Board") by ordinance of a Surveillance Technology Policy before: (1) seeking funds for Surveillance Technology; (2) acquiring or borrowing new Surveillance Technology; (3) using new or existing Surveillance Technology for a purpose, in a manner, or in a location not specified in a Surveillance Technology Policy ordinance approved by the Board in accordance with Chapter 19B; (4) entering into agreement with a non-City entity to acquire, share, or otherwise use Surveillance Technology; or (5) entering

into an oral or written agreement under which a non-City entity or individual regularly provides the department with data or information acquired through the entity's use of Surveillance Technology.

(c) Under Administrative Code Section 19B.2(b), the Board may approve a Surveillance Technology Policy ordinance under Section 19B.2(a) if: (1) the department seeking the Board's approval under Section 19B.2(a) creates a Surveillance Technology Policy and Surveillance Impact Report for the Surveillance Technology to be acquired or used; and (2) at a public hearing at which the Committee on Information Technology ("COIT") considers the Surveillance Technology Policy, COIT recommends that the Board adopt, adopt with modifications, or decline to adopt the Surveillance Technology Policy for the Surveillance Technology to be acquired or used.

(d) Under Administrative Code Section 19B.2(m), any amendment to an existing Surveillance Technology Policy shall be submitted directly to the Board and not to COIT.

(e) On July 27, 2021, the Board approved the Department of Public Works' (the "Department") Surveillance Technology Policy titled, "Unmanned Aerial Vehicles (Drones)" (Board File No. 210559), to be used for disaster preparedness and response, environmental monitoring and documentation, inspections and surveys of the Department's properties and assets, inspections and documentation of the Department's projects, and surveying and mapping data collection.

(f) On July 27, 2021, the Board of approved the Department's Surveillance Technology Policy titled, "OnSight Portable License Plate Reader" (Board File No. 210559), for Surveillance Technology used to discourage illegal dumping onto City streets.

(g) On August 1, 2025, the Department provided COIT with a courtesy copy of amendments to the Unmanned Aerial Vehicles (Drones) Surveillance Technology (the "Amended Drones Policy"), as well as a courtesy copy of amendments to the Department's

OnSight Portable License Plate Reader Surveillance Technology Policy, which has now been retitled, the "Illegal Dumping Camera System" Surveillance Technology Policy (the "Amended Illegal Dumping Camera Policy").

(h) The Amended Drones Policy and the Amended Illegal Dumping Camera Policy are on file and available for review in Board File No.260334.

(i) This ordinance sets forth the Board's findings in support of the Amended Drones Policy and the Amended Illegal Dumping Camera Policy and its approval of these policies.

Section 2. Usage of Unmanned Aerial Vehicles (Drones).

(a) The Department currently possesses and uses Unmanned Aerial Vehicles ("UAVs" or "Drones") pursuant to the Unmanned Aerial Vehicles (Drones) Surveillance Technology Policy. The Department currently uses drone technology for (1) disaster preparedness and response, (2) environmental monitoring and documentation, (3) inspections and surveys of the Department's properties and assets, (4) inspections and documentation of the Department's projects, and (5) surveying and mapping data collection.

(b) In addition to the preceding uses, the Department seeks to use Drones for the purposes of public education, the promotion of Department operations, and identifying illegal dumping refuse for garbage collection operations.

Section 3. Usage of the Illegal Dumping Camera System.

(a) The Department currently possesses and uses automated license plate reader ("ALPR") technology pursuant to the Onsight Portable License Plate Reader Surveillance Technology Policy. Specifically, for proof of concept, the Department has used two license plate readers mounted on poles at the Department's facilities and nine license plate readers

mounted on fixed locations in one supervisorial district as part of a pilot project to discourage illegal dumping.

(b) In addition to the preceding uses, the Department seeks to utilize ALPRs together with pan, tilt, and zoom ("PTZ") cameras as part of an "Illegal Dumping Camera System" comprised of the two technologies. The Illegal Dumping Camera System would be used to improve the identification of illegal dumping violators and enforcement actions directed at illegal dumping violators by capturing evidence of vehicle drivers' and passengers' illegal dumping activity along with the associated vehicles' license plate. In addition, the Department would use the Illegal Dumping Camera System for public education and to promote awareness of the Department's operations.

Section 4. Findings and Approval of Amended Surveillance Policies.

(a) The Board hereby finds that the benefits of the surveillance technology authorized by the Amended Drones Policy outweigh its costs and risks; that the Amended Drones Policy will safeguard civil liberties and civil rights; and that the uses and deployments of technology authorized under the Amended Drones Policy will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or Protected Class, as defined in Section 19B.1 of the Administrative Code.

(b) The Board hereby finds that the benefits of the surveillance technology authorized by the Amended Illegal Dumping Camera Policy outweigh its costs and risks; that the Amended Illegal Dumping Camera Policy will safeguard civil liberties and civil rights; and that the uses and deployments of technology authorized under the Amended Illegal Dumping Camera Policy will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or Protected Class, as defined in Section 19B.1 of the Administrative Code.

(c) The Board hereby approves the Amended Drones Policy and Amended Illegal Dumping Camera Policy.

Section 5. Effective Date. This ordinance shall become effective at 12:00 a.m. on the 31st day after enactment. Enactment occurs when the Mayor signs the ordinance, the Mayor returns the ordinance unsigned or does not sign the ordinance within ten days of receiving it, or the Board of Supervisors overrides the Mayor's veto of the ordinance.

APPROVED AS TO FORM:
DAVID CHIU, City Attorney

By: /s/
CHRISTOPHER T. TOM
Deputy City Attorney

4902-9798-2616, v. 1

FILE NO. 260334

# LEGISLATIVE DIGEST

[Administrative Code - Amendments to Public Works Surveillance Technology Policies]

**Ordinance approving amended Surveillance Technology Policies for the Department of Public Works' use of unmanned aerial vehicles ("Drones"), and the Department of Public Works' use of an illegal dumping camera system with automatic license plate reader technology and cameras; and making required findings in support of said approvals.**

## Existing Law

Currently, the Department of Public Works ("Department") uses Surveillance Technology, as defined in Administrative Code Chapter 19B, according to the Surveillance Technology Policy titled, "Unmanned Aerial Vehicles (Drones)" (Board File No. 210559), for the use of Drones for disaster preparedness and response, environmental monitoring and documentation, inspections and surveys of the Department's properties and assets, inspections and documentation of the Department's projects, and surveying and mapping data collection. In addition, the Department uses Surveillance Technology to discourage illegal dumping onto City streets according to the Surveillance Technology Policy titled, "OnSight Portable License Plate Reader" (Board File No. 210559).

Under Administrative Code Section 19B.2(m), any amendment to an existing Surveillance Technology Policy shall be submitted directly to the Board and not to the Committee on Information Technology ("COIT").

## Amendments to Current Law

On August 1, 2025, the Department provided COIT with a courtesy copy of amendments to the Unmanned Aerial Vehicles (Drones) Surveillance Technology (the "Amended Drones Policy"), as well as a courtesy copy of amendments to the Department's OnSight Portable License Plate Reader Surveillance Technology Policy, which has now been retitled, the "Illegal Dumping Camera System" Surveillance Technology Policy (the "Amended Illegal Dumping Camera Policy").

If approved by the Board of Supervisors, the Amended Drones Policy would authorize the Department to use Drones for the purposes of public education, the promotion of Department operations, and identifying illegal dumping refuse for garbage collection operations. Moreover, if approved, the Amended Illegal Dumping Camera Policy would authorize the Department to utilize automated license plate reader ("ALPR") technology together with pan, tilt, and zoom ("PTZ") cameras as part of an "Illegal Dumping Camera System" comprised of the two technologies. The Illegal Dumping Camera System would be used to improve the

identification of illegal dumping violators and enforcement actions directed at illegal dumping violators by capturing evidence of vehicle drivers' and passengers' illegal dumping activity along with the associated vehicles' license plate. In addition, the Department would use the Illegal Dumping Camera System for public education and to promote awareness of the Department's operations.

4935-6186-9210, v. 1

# Surveillance Technology Policy

Public Works
Unmanned Aircraft Systems (Drones)

The City and County of San Francisco values privacy and protection of San Francisco residents' civil rights and civil liberties. As required by San Francisco Administrative Code, Section 19B, the Department of Public Works' ("Department") Surveillance Technology Policy aims to ensure the responsible use of unmanned aerial vehicles ("UAV" or "Drone" technology) itself as well as any associated data, and the protection of City and County of San Francisco residents' civil rights and liberties.

## PURPOSE AND SCOPE

The Department's mission is to: enhance the quality of life in San Francisco as responsible stewards of the public's physical assets by providing outstanding service in partnership with the community. We design, build, manage, maintain, green, protect and improve the City's public spaces (infrastructure, public right of way and facilities) with skill, pride, innovation, and responsiveness.

The Surveillance Technology Policy ("Policy") defines the manner in which the Unmanned aerial vehicles or Drone technology will be used to support this mission, by describing the intended purpose, authorized and restricted uses, and requirements.

This Policy applies to all department personnel that use, plan to use, or plan to secure Unmanned aerial vehicles or Drone technology, including employees, suppliers, contractors, and volunteers while working on behalf of the City with the Department.

## POLICY STATEMENT

Unmanned Aerial Vehicles and Drone technology for the Department is limited to the following use cases and is subject to the requirements listed in this Policy.

*Authorized Use(s):*

1. Disaster preparedness and response
2. Environmental monitoring and documentation
3. Inspect/Survey properties & assets
4. Project inspection and documentation
5. Surveying/Mapping data collection
6. **Identifying illegally dumped refuse for garbage collection operations**
7. **Public Education and promotion of Public Works operations**

Prohibited use cases include any uses not stated in the Authorized Use Case section.

Surveillance Oversight Review Dates
COIT Review: July 17, 2020
Board of Supervisors Review: August 4, 2021

Departments may use information collected from technology only for legally authorized purposes, and may not use that information to unlawfully discriminate against people based on race, ethnicity, political opinions, religious or philosophical beliefs, trade union membership, gender, gender identity, disability status, sexual orientation or activity, or genetic and/or biometric data. Additionally, departments may not use automated systems to scan footage and identify individuals based on any of the categories listed in the preceding sentence.

## BUSINESS JUSTIFICATION

Unmanned aerial vehicles and Drone technology supports the Department's mission and provides important operational value in the following ways:

1. In times of disaster preparedness or post-disaster mitigation, drones will provide critical emergency response functions such as logistical support for emergency routing, life safety, and cleanup efforts, not only assisting in protecting physical assets and public spaces but human life as well;
2. Drones will support the maintenance efforts of City-owned streets and trees pursuant to our mission of greening and improving City public spaces;
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, architects, engineers, electricians, PMs, CMs and other personnel.
4. **Drone use will enable the Department to more effectively locate and document the imagery of illegally dumped refuse for clean up.**

In addition, unmanned aerial vehicles and Drone technology promises to benefit residents in the following ways:

| | | |
|---|---|---|
| X | Education | Drone imagery to promote Public Works projects and demonstrate use of tax dollars on projects. |
| □ | Community Development | |
| **X** | Health | **Drone imagery to aid in reporting and cleaning of illegally dumped refuse.** |
| X | Environment | Drone imagery to collect data on street-trees for maintenance and safety reasons. |
| □ | Criminal Justice | |
| □ | Jobs | |
| □ | Housing | |
| X | Other | 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. |

In addition, the following benefits are obtained:

| Benefit | | Description |
|---|---|---|
| X | 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. |
| X | Time Savings | Deploying a drone can provide time savings over setting up and employing equipment such as scaffolds/swing stages/scissor-lift vehicles, etc. |
| X | 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. |
| X | Data Quality | Some locations which are difficult to access by personnel may be more easily photographed using drone technology, thereby achieving better ~~data.~~**high-level digital imagery with precise location positioning data to integrate into the Department's operations.** |

## POLICY REQUIREMENTS

This Policy defines the responsible data management processes and legally enforceable safeguards required by the Department to ensure transparency, oversight, and accountability measures.

| | |
|---|---|
| Specifications: | The software and/or firmware used to operate the surveillance technology must be kept up to date and maintained. |
| Safety: | Surveillance technology must be operated in a safe manner. Surveillance technology should not be operated in a way that infringes on resident civil rights, including privacy, or causes personal injury or property damage. |

Data Collection:

Information collected, retained, processed or shared by surveillance technology must be consistent with this Policy; must comply with all City, State, and Federal laws and regulations; and must protect all state and federal Constitutional guarantees.

Departments shall minimize the use, collection, and retention of Personally Identifiable Information (PII) to what is strictly necessary to accomplish the intended purpose of the surveillance technology.

Department shall only collect data required to execute the authorized use case. All data collected by the surveillance technology, including PII, shall be classified according to the City's Data Classification Standard.

Should information be incidentally collected that is not necessary to accomplish the intended purpose of the surveillance technology, including information that may be used to identify persons or private information, Department shall remove all incidental PII from raw data.

The surveillance technology collects some or all of the following data types:

| ***Data Type(s)*** | ***Format(s)*** | ***Classification*** |
|---|---|---|
| Images/video of CCSF projects, assets, trees, **and refuse.** ~~etc.~~ | JPG~~E~~, MOV, AVI | Level 1 |
| Images/video of CCSF projects, assets, trees, **and refuse.** ~~etc.~~ | JPG~~E~~, MOV, AVI | Level 2 |

Notification: Departments shall notify the public of intended surveillance technology operation at the site of operations through signage in readily viewable public areas. Department notifications shall identify the type of technology being used and the purpose for such collection.

Department includes the following items in its public notice:

- X Information on the surveillance technology
- X Description of the authorized use
- X Type of data collected
- X Will persons be individually identified
- X Data retention
- X Department identification
- X Contact information

Access:

All parties requesting access must adhere to the following rules and processes (please refer to the data sharing section to ensure all information covered in that section is also included below): 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.

Data must always be scrubbed of PII as stated above prior to use.

*A. Department employees*

Employees: Once collected, the following roles and job titles are authorized to access and use data collected, retained, processed, or shared by the surveillance technology.

1. 7333-35 Stationary Engineer
2. 5310-13 Surveyor class series
3. 5201-~~18~~ **41** Engineers class series
4. 1823-27 Analyst class series
5. 0922-0954 Manager class series
6. 3435 BUF Inspectors
7. 5120 Architectural Administrator
8. 5260-74 Architect Class Series
9. 1312, 1314 Public Information Officer
10. 5408 Coordinator of Citizen Involvement
11. 3374 Outreach Coordinator
12. San Francisco Public Works: **Permits Division**, Bureau of Urban Forestry, Bureau of Building **and Street** Repair, Bureau of Engineering, Bureau of Architecture, Bureau of Street~~s and~~ Environmental Services. ~~Streets and Sewer Repair~~

Contractors: The following providers are required to support and maintain the surveillance technology and its associated data to ensure it remains functional:

- **ARUP (ARUP is an Engineering and Design Firm)**
- ~~At this point, Public Works does not anticipate using specific contractors whose services may be required~~

*B. Members of the public*

Public Works 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.

Collected data that is classified as Level 1-Public data may be made available for public access or release via DataSF's Open Data portal. Anyone, including criminal defendants, may access such data. Open Data has a Public Domain Dedication and License, and makes no warranties on the information provided. Once public on Open Data, data can be freely shared, modified, and used for any purpose without any restrictions. Any damages resulting from use of public data are disclaimed, including by criminal defendants.

Members of the public, including criminal defendants, may also request access by submission of a request pursuant to San Francisco's Sunshine Ordinance. No record shall be withheld from disclosure in its entirety unless all information contained in it is exempt from disclosure under express provisions of the California Public Records Act or some other statute.

Data Security:

Department shall secure PII against unauthorized or unlawful processing or disclosure; unwarranted access, manipulation or misuse; and accidental loss, destruction, or damage. Surveillance technology data collected and retained by the Department shall be protected by the safeguards appropriate for its classification level(s).

To protect surveillance technology information from unauthorized access and control, including misuse, Departments shall, at minimum, apply the following safeguards:

- Only authorized Drone operators ~~or PM~~ may access unedited data.
- **Access to captured data will be limited to approved employees.**
- **Data will be stored on local storage drive.**
- **Data will be secured with encryption or an Identity Access Management (IAM) function.**
- **Employees/Drone operators will be required to sign off on 1) a Drone Pre-Flight/Post-Flight Check List and 1) a Drone Data Privacy Integrity Log.**

Data Sharing:

Public Works will endeavor to ensure that other agencies or departments that may receive data collected by Department of Public Work's unmanned aerial vehicles policy will act in conformity with this Surveillance Technology Policy.

For internal and externally shared data, shared data shall not be accessed, used, or processed by the recipient in a manner incompatible with the authorized use cases stated in this Policy.

Public Works shall ensure proper administrative, technical, and physical safeguards are in place before sharing data with other CCSF departments, outside government entities, and third-party providers or vendors. (See Data Security)

Public Works shall ensure all PII and restricted data is de-identified or adequately protected to ensure the identities of individual subjects are effectively safeguarded.

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.

Before sharing data with any recipients, the Department will use the following procedure to ensure appropriate data protections are in place:

| | |
|---|---|
| X | Confirm the purpose of the data sharing aligns with the department's mission. |
| X | Consider alternative methods other than sharing data that can accomplish the same purpose. |
| X | Redact names, scrub faces, and ensure all PII is removed in accordance with the department's data policies. |
| X | Review of all existing safeguards to ensure shared data does not increase the risk of potential civil rights and liberties impacts on residents. |
| X | 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. |
| X | Ensure data will be shared in a cost-efficient manner and exported in a clean, machine-readable format. |

Public Works 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.

The Department currently participates in the following sharing practices:

*A. Internal Data Sharing:*

Department shares the following data with the recipients:

The department does not share surveillance technology data containing non-obscured ("raw" or unedited) PII with other departments or entities inside the City and County of San Francisco.

~~Data sharing occurs at the following frequency: N/A~~

- In emergency scenarios, Public Works may provide data to departments such as SFMTA, SFPUC, SF Port, SF Airport, SFDBI, and public access based on the Sunshine Ordinance. This data will be scrubbed and all PII will be removed, per Public Works' data processing protocols.

*B.* ***External Data Sharing:***

Data sharing occurs at the following frequency:

**Public Works does not share Surveillance Technology data with external entities.**

~~Data sharing will vary by case.~~

~~To ensure that entities receiving data collected by the surveillance technology comply with the Surveillance Technology Policy, Department shall~~:

- ~~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.~~

Data Retention: Department may store and retain raw PII data only as long as necessary to accomplish a lawful and authorized purpose.

The Department's data retention period and justification are as follows:

- Public Works will process raw data collected by drones as expeditiously as possible, and will commit to remove or obscure all PII within one year of collection. 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 **hard** deleted **permanently** upon completion of processing.
- Scrubbed data will be maintained in Public Works servers for historical purposes.

PII data shall not be kept in a form which permits identification of data subjects for any longer than is necessary for the purposes for which the personal data are processed. PII data collected by the surveillance technology may be retained beyond the standard retention period only in the following circumstance(s):
N/A

Departments must establish appropriate safeguards for PII data stored for longer periods.

Data will be stored in the following location:

**X Local storage (e.g., local server, storage area network (SAN), network- attached storage (NAS), backup tapes, etc.)**

☐ Department of Technology Data Center

☐ Software as a Service Product

☐ Cloud Storage Provider

| | |
|---|---|
| Data Disposal: | Upon completion of the data retention period, Department shall dispose of data in the following manner:<br><br>Practices:<br><br>1. Raw (unprocessed) data will be collected by the drone in the field, and stored on an onboard storage disc (i.e., "SD" card).<br>2. Raw data (from the drone disc) will be downloaded from onboard storage disc onto secure Public Works servers by Drone **Operator** ~~Data Editor~~.<br>3. Still or video frames will be identified for use by the appropriate Public Works **Operator to issue citations, or by Public Information Officer, Classification 1312 or 1314 if images are for public education and promotion of Public Works operations purpose.** ~~data consumer (based upon pre-approved Public Works use cases.)~~<br><br>Such data may include, as examples, **images of illegally dumped refuse**, 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.<br><br>Once the subject image frames, still and/or video, have been identified for business needs, the Public Works Drone **Operator or Public Information Officer** ~~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.<br><br>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.<br><br>Processes and Applications: All instances of PII will be blurred or obscured using editing software, such that no recognizable human features or distinctly identifying information remain. |
| Training: | To reduce the possibility that surveillance technology or its associated data will be misused or used contrary to its authorized use, all individuals requiring access to unedited data with PII present must receive training on data security policies and procedures.<br><br>At the very least, department shall require all elected officials, employees, consultants, volunteers, and vendors working with the technology on its behalf to read and formally acknowledge all authorized and prohibited uses. Department shall also require that all individuals requesting data or regularly requiring data access receive appropriate training before being granted access to systems containing PII.<br><br>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.

**COMPLIANCE**

Department shall oversee and enforce compliance with this Policy using the following methods:

1. 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.
2. Department shall assign one or more of the following personnel to oversee Policy compliance by the Department and third-parties.
    a. Senior Administrative Analyst,
    b. BSM Deputy Bureau Manger,
    c. BOE Deputy Bureau Manager,
    d. BOE structural section manager,
    e. BOA Deputy Bureau Manager,
    f. BUF Deputy Bureau Manager,
    g. Architectural Administrator,
    h. Architects and Engineers

Sanctions for violations of this Policy include the following:

1. First offense: violator shall be verbally notified by Public Works management of nature of violation.
2. Second offense: violator shall be notified in writing of second offence and privileges to operate drone hardware shall be suspended for 60 days.
3. 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.

If a Department is alleged to have violated the Ordinance under San Francisco Administrative Code Chapter 19B, Department shall post a notice on the Department's website that generally describes any corrective measure taken to address such allegation.

Department is subject to enforcement procedures, as outlined in San Francisco Administrative Code Section 19B.8.

**EXCEPTIONS**

Only in exigent circumstances or in circumstances where law enforcement requires surveillance technology data for investigatory or prosecutorial functions may data collected, retained, or

processed by the surveillance technology be shared with law enforcement.

| **DEFINITIONS** | |
|---|---|
| Personally Identifiable Information: | Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. |
| Sensitive Data: | Data intended for release on a need-to-know basis. Data regulated by privacy laws or regulations or restricted by a regulatory agency or contract, grant, or other agreement terms and conditions. |
| Exigent Circumstances | An emergency involving imminent danger of death or serious physical injury to any person that requires the immediate use of Surveillance Technology or the information it provides. |

**AUTHORIZATION**

Section 19B.4 of the City's Administrative Code states, "It is the policy of the Board of Supervisors that it will approve a Surveillance Technology Policy ordinance only if it determines that the benefits the Surveillance Technology ordinance authorizes outweigh its costs, that the Surveillance Technology Policy ordinance will safeguard civil liberties and civil rights, and that the uses and deployments of the Surveillance Technology under the ordinance will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or Protected Class."

**QUESTIONS & CONCERNS**

*Public:*

Complaints or concerns can be submitted to the Department by members of the public can register complaints / concerns or submit questions at San Francisco Public Works **Director's Office at 628-271-3160 or dpw@sfdpw.org**. ~~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~~. ~~As of July 15, Public Works will be located at 49 South Van Ness, Suite 300, San Francisco, CA 94102.~~

Department shall acknowledge and respond to complaints and concerns in a timely and organized response. To do so, Department shall:

**Respond to all comments or complaints ~~will be responded to~~ within 10 business days.**

~~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. The final outcome and action(s) taken shall be logged onto CFL.~~

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.

*City and County of San Francisco Employees:*

All questions regarding this policy should be directed to the employee's supervisor or to the **Public Works D**~~d~~irector. Similarly, questions about other applicable laws governing the use of the surveillance technology or the issues related to privacy should be directed to the employee's supervisor or the director.

# Surveillance Technology Policy

~~OnSight Portable License Plate Reader~~ **Illegal Dumping Camera System -** Public Works

The City and County of San Francisco values privacy and protection of San Francisco residents' civil rights and civil liberties. As required by San Francisco Administrative Code, Section 19B, the Surveillance Technology Policy aims to ensure the responsible use of ~~OnSight Portable License Plate Reader~~ **Illegal Dumping Camera Systems** as well as any associated data, and the protection of City and County of San Francisco residents' civil rights and liberties.

## PURPOSE AND SCOPE

The Department's mission is to care for and build the City's assets for the People of San Francisco

The Surveillance Technology Policy ("Policy") defines the manner in which the ~~OnSight Portable License Plate Reader~~ **Illegal Dumping Camera System, comprised of automated license plate reader ("ALPR") technology together with pan, tilt, and zoom ("PTZ") cameras** will be used to support this mission, by describing the intended purpose, authorized and restricted uses, and requirements.

This Policy applies to all ~~to~~ department personnel that use, plan to use, or plan to secure ~~OnSight Portable License Plate Reader~~ **the Illegal Dumping Camera System**, including employees, contractors, and volunteers. Employees, consultants, volunteers, and vendors while working on behalf of the City with the Department are required to comply with this Policy.

## POLICY STATEMENT

The authorized use of ~~OnSight Portable License Plate Reader~~ **the Illegal Dumping Camera System** technology for the Department is limited to the following use cases and is subject to the requirements listed in this Policy.

*Authorized Use(s):*

| |
|---|
| Discourage illegal dumping on City Streets.<br>**Identify and cite illegal dumping violators**.<br>**Public Education and promotion of Public Works operations.** |

Prohibited use cases include any uses not stated in the Authorized Use Case section.

Further, processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying an individual person, data concerning health or data concerning an individual person's sex life or sexual orientation shall be prohibited.

**Surveillance Oversight Review Dates**

COIT Review: September 17, 2020

Board of Supervisors Review: August 4, 2021

## BUSINESS JUSTIFICATION

~~OnSight Portable License Plate Reader~~ **The Illegal Dumping Camera System** supports the Department's mission and provides important operational value in the following ways:

Keeping the streets clean is a major challenge with ongoing illegal dumping. The ~~License plate reader~~ **Illegal Dumping Camera System** will allow us to capture **vehicle license plates and acts of** illegal dumping **to investigate, cite,** and discourage illegal dumping.

Public Works has two **Automated** License Plate Readers that are currently mounted on a pole on our facility for proof of concept. ~~Public Works' intention is to attach additional License Plate Readers to buildings in neighborhoods at the request of, or with permission from the property owner. The Supervisor's office is working on identifying participants.~~

**Public Works has nine Automated License Plate Readers mounted on fixed locations in a dumping hot spot neighborhood as a pilot project.**

**Public Works' intention is to procure and attach PTZ cameras on fixed locations alongside the ALPR cameras for a comprehensive 2-camera system capturing license plate data and video evidence of illegal dumping violations for investigation and enforcement.**

Hotspots of illegal dumping are identified through the following sources:

- 311
- Employee observations **during routine clean-up operations**
- ~~Email c~~Complaints from constituents

In addition, ~~OnSight Portable License Plate Reader~~ **the Illegal Dumping Camera System** promises to benefit residents in the following ways:

| | | |
|---|---|---|
| · | Education | |
| · | Community Development | |
| · | Health | |
| ☒ | Environment | Illegal dumping affects adjacent neighbors and businesses. This will allow us to catch and prevent future illegal dumping in these neighborhoods. |
| · | Criminal Justice | |
| · | Jobs | |
| · | Housing | |

- Other

~~OnSight Portable License Plate Reader~~ **The Illegal Dumping Camera System** will benefit the department in the following ways:

| Benefit | | Description |
|---|---|---|
| ☒ | **Financial Savings** | **It would be very costly to pay for humans to sit ~~at~~ all night and day to catch illegal dumpers** |
| - | Time Savings | |
| ☒ | Staff Safety | ~~We~~ **The Department** won't have to put staff in direct harm confronting illegal dumpers, won't have to have staff working at night in remote locations. |
| ☒ | Data Quality | The **ALPR** camera lens provides accurate license plate data. If **the Department** ~~we~~ were relying on a human they might misread the plate during low-light conditions. **The addition of PTZ cameras will capture evidence of illegal dumping activity; this data paired with license plate data will help substantiate enforcement efforts and citations issued to vehicle owners.** |
| - | Other | |

~~Other benefits include Easily deployed to any outdoor environment without need for trenching. Can be used on either A/C or solar power. Web based user interface for easy accessing of information.~~

## POLICY REQUIREMENTS

This Policy defines the responsible data management processes and legally enforceable safeguards required by the Department to ensure transparency, oversight, and accountability measures. Department use of surveillance technology and information collected, retained, processed or shared by surveillance technology must be consistent with this Policy; must comply with all City, State, and Federal laws and regulations; and must protect all state and federal Constitutional guarantees.

| | |
|---|---|
| Specifications: | The software and/or firmware used to operate the surveillance technology must be kept up to date and maintained. |
| Safety: | Surveillance technology must be operated in a safe manner. Surveillance technology should not be operated in a way that infringes on resident civil rights, including privacy, or causes personal injury or property damage. |

Data Collection:

Departments shall minimize the use, collection, and retention of Personally Identifiable Information (PII) to what is strictly necessary to accomplish the intended purpose of the surveillance technology.

Department shall only collect data required to execute the authorized use case. All data collected by the surveillance technology, including PII, shall be classified according to the City's Data Classification Standard.

Should information be incidentally collected that is not necessary to accomplish the intended purpose of the surveillance technology, including information that may be used to identify persons or private information, Department shall remove all incidental PII from raw data.

Data types can take the form video, audio, still images. Data formats can take the form of XML, PDF, HTML, Plain Text, JPEG, etc. ~~The surveillance technology collects the following data types and formats:~~

- ~~Video in MOV format~~
- ~~Still images from cameras in PDF format~~

The surveillance technology collects the following data types:

| *Data Type(s)* | *Format(s)* | *Classification* |
|---|---|---|
| License Plate **Numbers** | ~~AVI~~ **JPEG, PNG, MEG or compressed** | Level 3 |
| ~~Facial features~~ **Images of driver and passengers** | ~~AVI~~ **JPEG, PNG, MP4 or compressed** | Level **2,**3 |
| **Images/Videos of people and objects** | **JPEG, MOV, AVI, MP4** | **Level 2, 3** |

The technology does not use facial recognition **technology** but does take photos/videos that may capture **images of people** ~~facial features~~. This technology will only be used to pursue enforcement of illegal activity. **Images of people, drivers and passengers in the act of illegal dumping activity** ~~Facial features~~ and **vehicle** license plate information will only be shared with relevant law enforcement for enforcement purposes.

Notification:

Departments shall notify the public of intended surveillance technology operation at the site of operations through signage in readily viewable public areas. Department notifications shall identify the type of technology being used and the purpose for such collection.

Department includes the following items in its public notice:

☒ Information on the surveillance technology
☐ Description of the authorized use
☐ Type of data collected
☐ Will persons be individually identified
☐ Data retention
☒ Department identification
☐ Contact information

Access:

All parties requesting access must adhere to the following rules and processes (please refer to the ~~data~~ **Data** ~~sharing~~ **Sharing** section to ensure all information covered in that section is also included below): ~~evidence of illegal dumping~~

**Current Public Works employees must be approved to access the ALPR and PTZ data by the Deputy Director of Operations, Director of Communications, or Assistant Superintendent of Street Environmental Services.**

**The data use must be tied to the authorized use of this policy.**

**Authorized persons must sign an agreement to adhere to the Surveillance Technology Policy.**

*A. Department employees*

Once collected, the following roles and job titles are authorized to access and use data collected, retained, processed or shared by the surveillance technology.

- **7281 Street Environmental Services Operations Supervisors**
- **0942 Superintendent, Street Environmental Services, Operations**
- **0932 Asst. Superintendent, Street Environmental Services, Manager**
- **0923 Manager II**
- **0922 Manager, Street Environmental Services**
- **1840 Junior Management Assistant, SES Operations Admins.**
- **1312, 1314 Public Information Officer**
- **1310 Public Relations Assistant**
- **5408 Coordinator of Citizen Involvement**
- **3374 Outreach Coordinator**
- ~~7281 Operations Supervisor 2, Public Works~~

The following providers are required to support and maintains the surveillance technology and its associated data to ensure it remains functional:

- ~~V5 Systems~~

**Public Works has no current contract with ALPR or PTZ technology vendors.**

### *B. Members of the public*

Public Works 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.

Data collected by surveillance technology will not be made available to members of the public, including criminal defendants.

Collected data that is classified as Level 1-Public data may be made available for public access or release via DataSF's Open Data portal. Anyone, including criminal defendants, may access such data. Open Data has a Public Domain Dedication and License, and makes no warranties on the information provided. Once public on Open Data, data can be freely shared, modified, and used for any purpose without any restrictions. Any damages resulting from use of public data are disclaimed, including by criminal defendants.

Members of the public, including criminal defendants, may also request access by submission of a request pursuant to San Francisco's Sunshine Ordinance. No record shall be withheld from disclosure in its entirety unless all information contained in it is exempt from disclosure under express provisions of the California Public Records Act or some other statute.

Data Security: Department shall secure PII against unauthorized or unlawful processing or disclosure; unwarranted access, manipulation or misuse; and accidental loss, destruction, or damage. Surveillance technology data collected and retained by the Department shall be protected by the safeguards appropriate for its classification level(s).

To protect surveillance technology information from unauthorized access and control, including misuse, Departments shall, at minimum, apply the following safeguards:

**Access to captured data will be limited to approved employees.**

**Data will be stored on computer hard drive, not on shared drive or cloud drive**.

**ALPR and PTZ data files on hard drive will be secured with an encryption and- Identity Access Management (IAM) system.**

Only scrubbed still or video frames can be used by the appropriate Public Works **Operator to issue citations, or by Public Information Officer (Classification 1312 or 1314) if images are for public education and promotion of Public Works operations purpose.**

~~Supervisors will be monitored~~

Data Sharing: Public Works 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.

Public Works will endeavor to ensure that other agencies or departments that may receive data collected by ~~OnSight Portable License Plate Readers~~ **Illegal Dumping Camera System** will act in conformity with this Surveillance Technology Policy.

For internal and externally shared data, shared data shall not be accessed, used, or processed by the recipient in a manner incompatible with the authorized use cases stated in this Policy.

Public Works shall ensure proper administrative, technical, and physical safeguards are in place before sharing data with other CCSF departments, outside government entities, and third-party providers or vendors. (See Data Security)

Public Works shall ensure all PII and restricted data is de-identified or adequately protected to ensure the identities of individual subjects are effectively safeguarded.

Each department that believes another agency or department receives or may receive data collected from its use of **Surveillance Technologies** ~~STs~~ should consult with its assigned deputy city attorney regarding their response.

The Department currently participates in the following sharing practices:

### A. **Internal Data Sharing** ~~Internal and External Data Sharing~~

**Department shares the following data with the internal recipients:**

| **Type** | **Recipient** |
|---|---|
| **Redacted or scrubbed data per Data Collection and Data Security section of Surveillance Tech Policy** | **SFPD**<br><br>**City Attorney's Office**<br><br>**SF District Attorney's Office** |

**Data sharing occurs at the following frequency:**

- **On case use basis to pursue criminal charges for illegal dumping.**

### B. **External Data Sharing**

**Department shares the following data with the external recipients:**

| **Type** | **Recipient** |
|---|---|
| | The Department does not share surveillance technology data externally with entities outside the City and County of San Francisco. |

**Data sharing occurs at the following frequency:**

**Not applicable; see above.**

Before sharing data with any recipients, the Department will use the following procedure to ensure appropriate data protections are in place:

- ☑ Confirm the purpose of the data sharing aligns with the department's mission **by reviewing Surveillance Technology Policy before and after each use.**
- ☑ Consider alternative methods other than sharing data that can accomplish the same purpose.
- ☑ Redact names, scrub faces, and ensure all PII is removed in accordance with the department's data policies.
- ☑ Review of all existing safeguards to ensure shared data does not increase the risk of potential civil rights and liberties impacts on residents.
- ☑ Evaluation of what data can be permissibly shared with members of the public should a request be made in accordance with the San Francisco's Sunshine Ordinance.
- ☑ Ensure shared data will be done in a cost-efficient manner and exported in a clean, machine-readable format.

~~Department shares the following data with the recipients:~~

- ~~Public Works may share data with SFPD, CAT~~

~~Data sharing occurs at the following frequency:~~

- ~~As needed~~

~~Public Works may share data with SFPD and the District Attorney to pursue criminal charges.~~

| | |
|---|---|
| Data Retention: | Department may store and retain raw PII data only as long as necessary to accomplish a lawful and authorized purpose.<br><br>Please list data retention schedules (i.e., x type of data will be retained for 1 year) based on the following categories:<br><br>• 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

The Department's data retention period and justification are as follows:

| | |
|---|---|
| **Raw Data:** Maximum of 30 days | ~~Only need it long enough to confirm responsible parties~~ **Data is retained for only as long as it takes to issue a citation, if needed, to a party responsible for illegal dumping.** |

PII data shall not be kept in a form which permits identification of data subjects for any longer than is necessary for the purposes for which the personal data are processed. PII data collected by the surveillance technology may be retained beyond the standard retention period only in the following circumstance(s):

- **Data is not retained beyond the maximum stated retention period.** ~~n/a~~

Departments must establish appropriate safeguards for PII data stored for longer periods.

Data will be stored in the following location:

☑ **Local storage**
☑ **Vendor managed storage**
☐ Department of Technology Data Center
☑ **Software as a Service Product**
☑ Cloud Storage Provider

Data Disposal: Upon completion of the data retention period, Department shall dispose of data in the following manner:

Practices: **Raw Data is consolidated on the local hard drive and will be hard deleted after 30 days of captured data date by Department Internet Technology staff.**

**Department IT staff will use secure deletion method to overwrite file data.**

~~Automatic overwrite after 30 days~~

~~Processes and Applications: n/a~~

| | |
|---|---|
| Training: | To reduce the possibility that surveillance technology or its associated data will be misused or used contrary to its authorized use, all individuals requiring access must receive training on data security policies and procedures.<br><br>At the very least, department shall require all elected officials, employees, consultants, volunteers, and vendors working with the technology on its behalf to read and formally acknowledge all authorized and prohibited uses. Department shall also require that all individuals requesting data or regularly requiring data access receive appropriate training before being granted access to systems containing PII. |

## COMPLIANCE

Department shall oversee and enforce compliance with this Policy using the following methods:

Deputy Director for Operations, **Director of Communications, and Assistant Superintendent of Street Environmental Services are** responsible for monitoring compliance

Department shall assign the following personnel to oversee Policy compliance by the Department and third parties:

Deputy Director for Operations, **Director of Communications, and Assistant Superintendent of Street Environmental Services**

Sanctions for violations of this Policy include the following:

Removal or shutting down of technology **for investigation by compliance staff named above** until violations are resolved.

**Sanctions for violations of this Policy include the following:**

1. **First offense: violator shall be verbally notified by Public Works management of nature of violation.**
2. **Second offense: violator shall be notified in writing of second offence and privileges to operate ALPR and PTZ technology shall be suspended for 60 days.**
3. **Third offense: (following reinstatement of operator privileges) violator shall be permanently banned from surveillance technology operations and disciplinary action may be taken depending upon the severity of second/third offences.**

If a Department is alleged to have violated the Ordinance under San Francisco Administrative Code Chapter 19B, Department shall post a notice on the Department's website that generally describes any corrective measure taken to address such allegation.

Department is subject to enforcement procedures, as outlined in San Francisco Administrative Code Section 19B.8.

## EXCEPTIONS

Only in exigent circumstances or in circumstances where law enforcement requires surveillance technology data for investigatory or prosecutorial functions may data collected, retained or processed by the surveillance technology be shared with law enforcement.

## DEFINITIONS

| | |
|---|---|
| Personally Identifiable Information: | Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. |
| Raw Data: | Information collected by a surveillance technology that has not been processed and cleaned of all personal identifiable information. The distribution and use of raw data is tightly restricted. |
| Exigent Circumstances | An emergency involving imminent danger of death or serious physical injury to any person that requires the immediate use of Surveillance Technology or the information it provides. |

## AUTHORIZATION

Section 19B.4 of the City's Administrative Code states, "It is the policy of the Board of Supervisors that it will approve a Surveillance Technology Policy ordinance only if it determines that the benefits the Surveillance Technology ordinance authorizes outweigh its costs, that the Surveillance Technology Policy ordinance will safeguard civil liberties and civil rights, and that the uses and deployments of the Surveillance Technology under the ordinance will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or Protected Class."

## QUESTIONS & CONCERNS

*Public:*

Complaints or concerns can be submitted to the Department by:

All complaints or concerns should be routed **to the Public Works Director's Office at 628-271-3160 or dpw@sfdpw.org.** ~~through 311.org~~

Department shall acknowledge and respond to complaints and concerns in a timely and organized response. To do so, Department shall:

**Department will respond to all comments or complaints within 10 business days.**

~~Respond to 311 within required SLA~~

*City and County of San Francisco Employees:*

All questions regarding this policy should be directed to the employee's supervisor or to the **Public Works D**irector. Similarly, questions about other applicable laws governing the use of the surveillance technology or the issues related to privacy should be directed to the employee's supervisor or the director.

~~[APPENDIX A is an older template that covers the same material above. ]~~

***~~APPENDIX A: Surveillance Technology Policy Requirements~~***

~~The following section shows all Surveillance Technology Policy requirements in order as defined by the San Francisco Administrative Code, Section 19B.~~

~~1. A description of the product and services addressed by the Surveillance Technology, including the identity of any provider(s) whose services are essential to the functioning or effectiveness of the Surveillance Technology equipment or services for the intended purpose.~~

~~Powered by solar with a battery, it captures data from vehicles in day or night to read the license plate. -A 12 MM camera lens is paired with a LTE SIM Card to record the license plate information for a maximum of 30 days.~~

~~IR/Starlight Hybrid Camera Sensor. 21"lx15"Wx9"D Weight 25lbs~~

~~V5 Systems~~

~~2. A description of the purpose(s) for which the Surveillance Technology equipment or services are proposed for acquisition, including the type of data that may be collected by the Surveillance Technology equipment or services.~~

~~Technology Use:~~

Keeping the streets clean is a major challenge with ongoing illegal dumping. The License plate reader will allow us to capture illegal dumping and follow up with the bad actors.

PII:

True

3. The uses that are authorized, the rules and processes required prior to such use, and uses of the Surveillance Technology that will be expressly prohibited.

Authorized Uses:

Only to follow up on illegal dumping onto City Streets

Rules:

anything outside of illegal dumping cases

Prohibited Uses:

only where illegal dumping was confirmed

4. A description of the formats in which information collected by the Surveillance Technology is stored, copied, and/or accessed.

| Data Type | Formats STP |
|---|---|
| License Plate | AVI |
| Facial features | AVI |

5. The specific categories and titles of individuals who are authorized by the Department to access or use the collected information, including restrictions on how and under what circumstances data collected with Surveillance Technology can be analyzed and reviewed, and the rules and processes required prior to access or use of the information.

Employee Job Classification & Title:

only where illegal dumping was confirmed

Department:

Public Works

If applicable, contractor or vendor name:

V5 Systems

Rules and processes required prior to data access or use:

~~Supervisors will be monitored~~

~~6. The general safeguards that protect information from unauthorized access, including encryption and access control mechanisms.~~

~~only where illegal dumping was confirmed~~

~~7. The limited time period, if any, that information collected by the Surveillance Technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s) enumerated in the Surveillance Technology Policy, the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond that period~~

~~Retention:~~

~~only need it long enough to confirm responsible parties~~

~~Reason for retention:~~

~~n/a~~

~~Deletion process:~~

~~only need it long enough to confirm responsible parties~~

~~Retention exemption conditions:~~

~~n/a~~

~~8. How collected information can be accessed or used by members of the public, including criminal defendants~~

~~Will the data be accessible to the public:~~

~~Maximum of 30 days~~

~~How it can be accessed:~~

~~9. Which governmental agencies, departments, bureaus, divisions, or units that may receive data collected by the Surveillance Technology operated by the Department, including any required justification or legal standard necessary to share that data and how it will ensure that any entity receiving such data complies with the Surveillance Technology Policy.~~

~~Name of agency: Public Works may share data with SFPD, CAT~~

~~Justification:~~

~~10. The training required for any individual authorized to use the Surveillance Technology or to access information collected by the Surveillance Technology~~

~~Training required:~~

~~false~~

~~Description of training:~~

~~11. The mechanisms to ensure that the Surveillance Technology Policy is followed, including internal personnel assigned to ensure compliance with the policy, internal recordkeeping of the use of the technology or access to information collected by the technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the sanctions for violations of the policy~~

~~Training required:~~

~~false~~

~~Process for responding to complaints:~~

~~Deputy Director for Operations~~

~~Oversight process:~~

~~Removal or shutting down of technology until violations are resolved~~

~~Compliance personnel titles:~~

~~7281 Operations Supervisor 2, Public Works~~

~~Restrictions:~~

~~only where illegal dumping was confirmed~~

~~12. What procedures will be put in place by which members of the public can register complaints or concerns, or submit questions about the deployment or use of a specific Surveillance Technology, and how the Department will ensure each question and complaint is responded to in a timely manner.~~

~~Complaint procedures:~~

~~respond to 311 within required SLA~~

~~Departmental follow-up process:~~

~~Larry Stringer, Deputy Director for Operations is responsible for monitoring compliance~~

~~*Members of the public can register complaints/concerns or submit questions via calls or emails at 311.org.*~~

BOARD of SUPERVISORS

City Hall
1 Dr. Carlton B. Goodlett Place, Room 244
San Francisco, CA 94102-4689
Tel. No. (415) 554-5184
Fax No. (415) 554-5163
TDD/TTY No. (415) 554-5227

# M E M O R A N D U M

TO: Carla Short, Director, Public Works
Michael Makstman, Executive Director/CIO, Department of Technology

FROM: Monique Crayton, Assistant Clerk, Government Audit and Oversight Committee

DATE: April 15, 2026

SUBJECT: LEGISLATION INTRODUCED

---

The Board of Supervisors' Government Audit and Oversight Committee has received the following Ordinance request on April 7, 2026.

**File No. 260334**

**Administrative Code - Amendments to Public Works Surveillance Technology Policies**

**Ordinance approving amended Surveillance Technology Policies for the Department of Public Works' use of unmanned aerial vehicles ("Drones"), and the Department of Public Works' use of an illegal dumping camera system with automatic license plate reader technology and cameras; and making required findings in support of said approvals.**

If you have any comments or reports to be included with the file, please forward them to me at the Board of Supervisors, City Hall, Room 244, 1 Dr. Carlton B. Goodlett Place, San Francisco, CA 94102 or by email at: monique.crayton@sfgov.org.

cc:
David Steinberg, Public Works
Ian Schneider, Public Works
Karen Hong Yee, Department of Technology

**Carla Short, Director** | Director's Office
carla.short@sfdpw.org | T. 628.271.3078 | 49 South Van Ness Ave. Suite 1600, San Francisco, CA 94103

March 30, 2026

Angela Calvillo, Clerk of the Board of Supervisors
Board of Supervisors
1 Dr. Carlton B. Goodlet Place, Room 244
San Francisco, CA 94102

Dear Ms. Calvillo,

Pursuant to Administrative Code Chapter 19B, Acquisition of Surveillance Technology Ordinance, I am forwarding to the Board of Supervisors the following proposed amendment to the San Francisco Public Works Surveillance Technology Policy for approval.

According to Administrative Code Section 19B.2(m), any amendment to an existing Surveillance Technology Policy shall be submitted directly to the Board of Supervisors and not to COIT.

The following is a list of accompanying documents:

- Department Cover Letter
- Ordinance approving amended Public Works Surveillance Technology Policy for 1) Unmanned Aircraft Systems (Drones) and 2) Illegal Dumping Camera System
- Legislative Digest
- Proposed Amended Surveillance Technology Policy: Unmanned Aircraft Systems (Drones)
- Proposed Amended Surveillance Technology Policy: Illegal Dumping Camera System

The following people may be contacted regarding this matter:

Ian Schneider, Government Affairs Manager
628-271-3126
Ian.Schneider@sfdpw.org

Esther Lee, Government Affairs Liaison
628-271-3065
Esther.E.Lee@sfdpw.org

Sincerely,

Carla Short
Director