

BOARD of SUPERVISORS



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

MEMORANDUM

RULES COMMITTEE

SAN FRANCISCO BOARD OF SUPERVISORS

TO: Supervisor Matt Dorsey, Chair
Rules Committee

FROM: Victor Young, Assistant Clerk *Victor Young*

DATE: January 8, 2024

SUBJECT: **COMMITTEE REPORT, BOARD MEETING**
Tuesday, January 9, 2024

The following file should be presented as a **COMMITTEE REPORT** at the Board Meeting on Tuesday, January 9, 2024. This item was acted upon at the Rules Committee Meeting on Monday, January 8, 2024, at 10:00 a.m., by the votes indicated.

Item No. 25 File No. 231217

[Administrative Code - Surveillance Technology Policy - City Administrator - Security Camera Systems]

Ordinance approving a modified Surveillance Technology Policy for the City Administrator's Office's acquisition and use of security camera systems.

RECOMMENDED AS A COMMITTEE REPORT

Vote: Supervisor Shamann Walton - Aye
Supervisor Ahsha Safai - Aye
Supervisor Matt Dorsey - Aye

c: Board of Supervisors
Angela Calvillo, Clerk of the Board
Alisa Somera, Legislative Deputy Director
Anne Pearson, Deputy City Attorney

File No. 231217

Committee Item No. 4

Board Item No. _____

COMMITTEE/BOARD OF SUPERVISORS

AGENDA PACKET CONTENTS LIST

Committee: Rules Committee

Date Jan 8, 2024

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
- Memorandum of Understanding (MOU)
- Grant Information Form
- Grant Budget
- Subcontract Budget
- Contract/Agreement
- Form 126 - Ethics Commission
- Award Letter
- Application
- Form 700
- Information/Vacancies (Boards/Commissions)
- Public Correspondence

OTHER (Use back side if additional space is needed)

- Surveillance Tech Policy
- _____
- _____
- _____
- _____
- _____
- _____
- _____
- _____

Completed by: Victor Young

Date Jan 4, 2024

Completed by: _____

Date _____

1 [Administrative Code - Surveillance Technology Policy - City Administrator - Security Camera
2 Systems]

3 **Ordinance approving a modified Surveillance Technology Policy for the City**
4 **Administrator’s Office’s acquisition and use of security camera systems.**

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

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

13 Section 1. Background.

14 (a) Terms used in this ordinance have the meaning set forth in Administrative Code
15 Chapter 19B (“Chapter 19B”).

16 (b) Chapter 19B establishes requirements that City departments must follow before
17 they may use or acquire new Surveillance Technology. Under Administrative Code Section
18 19B.2(a), a City department must obtain Board of Supervisors (“Board”) approval by
19 ordinance of a Surveillance Technology Policy before: (1) seeking funds for Surveillance
20 Technology; (2) acquiring or borrowing new Surveillance Technology; (3) using new or
21 existing Surveillance Technology for a purpose, in a manner, or in a location not specified in a
22 Board-approved Surveillance Technology Policy; (4) entering into an agreement with a non-
23 City entity to acquire, share, or otherwise use Surveillance Technology; or (5) entering into an
24 oral or written agreement under which a non-City entity or individual regularly provides the
25 department with data or information acquired through the entity’s use of Surveillance
Technology.

1 (c) Under Administrative Code Section 19B.2(b), the Board may approve a
2 Surveillance Technology Policy if: (1) the department seeking Board approval first submits to
3 the Committee on Information Technology (“COIT”) a Surveillance Impact Report for the
4 Surveillance Technology to be acquired or used; (2) based on the Surveillance Impact Report,
5 COIT develops a Surveillance Technology Policy for the Surveillance Technology to be
6 acquired or used; and (3) at a public meeting at which COIT considers the Surveillance
7 Technology Policy, COIT recommends that the Board adopt, adopt with modification, or
8 decline to adopt the Surveillance Technology Policy for the Surveillance Technology to be
9 acquired or used.

10 (d) Under Administrative Code Section 19B.4, it is City policy that the Board of
11 Supervisors will approve a Surveillance Technology Policy only if it determines that the
12 benefits that the Surveillance Technology Policy authorizes outweigh its costs, that the
13 Surveillance Technology Policy will safeguard civil liberties and civil rights, and that the uses
14 and deployments of the Surveillance Technology under the Policy will not be based upon
15 discriminatory or viewpoint-based factors or have a disparate impact on any community or
16 Protected Class.

17
18 Section 2. Surveillance Technology Policy Ordinance for the Office of the City
19 Administrator’s Acquisition and Use of Security Cameras.

20 (a) Purpose. The Office of the City Administrator, including the divisions and
21 departments under the City Administrator’s control (collectively, “the City Administrator” or “the
22 Department”) seeks Board authorization under Section 19B.2(a) to acquire or use security
23 cameras owned, leased, managed, or operated by the City at specified locations as follows:
24 (1) live monitoring; (2) recording of video and images; (3) reviewing camera footage in the
25 event of an incident; and (4) providing video footage or images to law enforcement or other

1 authorized persons following an incident or upon request. Under the proposed Surveillance
2 Technology Policy (the “Policy”), the City Administrator may use information collected from
3 security cameras only for legally authorized purposes, and may not use that information to
4 unlawfully discriminate against people based on race, ethnicity, political opinions, religious or
5 philosophical beliefs, trade union membership, gender, gender identity, disability status,
6 sexual orientation or activity, or genetic and/or biometric data. Additionally, the City
7 Administrator may not use automated systems to scan footage and identify individuals based
8 on any of the categories listed in the preceding sentence.

9 The Policy revises and replaces the City Administrator’s current Surveillance
10 Technology Policy regarding security cameras, which the Board approved in Ordinance No.
11 116-21. That current policy applies only to cameras in and around properties under the
12 jurisdiction of the Real Estate Division, and requires the Director of Real Estate to approve
13 before security guards at the Department of Animal Care and Control monitor live feeds from
14 a camera. The new Policy that the Board approves in this ordinance applies to cameras in
15 and around properties under the jurisdiction of all divisions and departments under the City
16 Administrator; allows certain Animal Care and Control staff to monitor live and review
17 recorded footage without the approval from the Director of Real Estate; and expressly allows
18 the acquisition of additional cameras in the future.

19 (b) Surveillance Impact Report. The City Administrator and other departments
20 submitted to COIT Surveillance Impact Reports for their use of security cameras. A copy of
21 the Surveillance Impact Reports is in Board File No. 210559.

22 (c) Public Hearings and COIT Recommendation. On November 7, 2023, COIT’s
23 Privacy and Surveillance Advisory Board held a public hearing to consider the proposed
24 Policy, and on November 16, 2023, COIT held a public hearing to consider and approve the
25 proposed Policy. On November 16, 2023, COIT voted to recommend the Policy to the Board

1 for approval. A copy of the proposed Policy is in Board File No. 231217, and is incorporated
2 herein by reference.

3 (d) Findings. The Board hereby finds that the stated benefits of the City
4 Administrator’s acquisition and use of security cameras outweigh the costs and risks of use of
5 such Surveillance Technology; that the Policy will safeguard civil liberties and civil rights; and
6 that the uses and deployments of security cameras, as set forth in the Policy, will not be
7 based upon discriminatory or viewpoint-based factors or have a disparate impact on any
8 community or a protected class.

9
10 Section 3. Approval of Policy.

11 The Board of Supervisors hereby approves the City Administrator’s modified
12 Surveillance Technology Policy for security cameras, described in Section 2 of this ordinance
13 and referenced in Section 2(c).

14
15 Section 4. Effective Date. This ordinance shall become effective 30 days after
16 enactment. Enactment occurs when the Mayor signs the ordinance, the Mayor returns the
17 ordinance unsigned or does not sign the ordinance within ten days of receiving it, or the Board
18 of Supervisors overrides the Mayor’s veto of the ordinance.

19 APPROVED AS TO FORM:
20 DAVID CHIU, City Attorney

21 By: _____ /s/
22 JON GIVNER
23 Deputy City Attorney

24 n:\legana\as2023\2400220\01719806.docx

LEGISLATIVE DIGEST

[Administrative Code - Surveillance Technology Policy - City Administrator - Security Camera Systems]

Ordinance approving a modified Surveillance Technology Policy for the City Administrator's Office's acquisition and use of security camera systems.

Existing Law

Administrative Code Chapter 19B establishes requirements that City departments must follow before they may use or acquire new surveillance technology. A City department must obtain Board of Supervisors approval 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 Board-approved surveillance technology policy; (4) entering into an 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.

The Board approved the City Administrator's current surveillance technology policy regarding security cameras in Ordinance No. 116-21. The current policy applies only to cameras in and around properties under the jurisdiction of the Real Estate Division, and requires the Director of Real Estate to approve before security guards at the Department of Animal Care and Control monitor live feeds from a camera.

Amendments to Current Law

The proposed ordinance would approve a modified policy allowing the City Administrator to acquire or use security cameras owned, leased, managed, or operated by the City at specified locations as follows: (1) live monitoring; (2) recording of video and images; (3) reviewing camera footage in the event of an incident; and (4) providing video footage or images to law enforcement or other authorized persons following an incident or upon request.

The modified policy applies to cameras in and around properties under the jurisdiction of all divisions and departments under the City Administrator; allows certain Animal Care and Control staff to monitor live and review recorded footage without the approval from the Director of Real Estate; and expressly allows the acquisition of additional cameras in the future.

FILE NO. 231217



Committee on Information Technology

Office of the City Administrator

To: Members of the Board of Supervisors

From: Carmen Chu, City Administrator

Jillian Johnson, Director, Committee of Information Technology

Date: November 20, 2023

Subject: Legislation introduced to approve Surveillance Technology Policy Amendments for the City Administrator's Office's Security Cameras

In compliance with Section 19B of the City and County of San Francisco's Administrative Code, the City Administrator's Office is pleased to submit the Surveillance Technology Policy Amendments for the City Administrator's Office's Security Cameras.

To engage the public in discussion on the role of government surveillance, the Committee on Information Technology (COIT) and its subcommittee the Privacy and Surveillance Advisory Board (PSAB) held 2 public meetings for Security Cameras in November 2023 to review and approve the policy. All details of these discussions are available at sf.gov/coit.

The following page provides greater detail on the review process for the Surveillance Technology Policy, and COIT's recommended course of action.

If you have questions on the review process please direct them to Jillian Johnson, Director of the Committee on Information Technology (COIT).

Security Cameras

| Department | Authorized Uses |
|-----------------------------|--|
| City Administrator's Office | <ol style="list-style-type: none">1. Live monitoring.2. Recording of videos and images.3. Reviewing camera footage in the event of an incident.4. Providing footage or images to law enforcement or other authorized persons following an incident or upon request. |

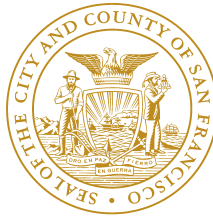
Security Cameras Public Meeting Dates

| Date | Meeting |
|-------------------|--|
| November 7, 2023 | Privacy and Surveillance Advisory Board (PSAB) |
| November 16, 2023 | Committee on Information Technology (COIT) |

COIT recommends the following action be taken on the policy:

- Approve the Security Cameras Surveillance Technology Policy Amendments for the City Administrator's Office.

City & County of San Francisco
London N. Breed, Mayor



Office of the City Administrator
Carmen Chu, City Administrator

November 27, 2023

SENT VIA EMAIL

To: Angela Calvillo, Clerk of the Board of Supervisors

From: Carmen Chu, City Administrator

Date: November 27, 2023

Subject: Ordinance approving a modified Surveillance Technology Policy for the City Administrator's Office's acquisition and use of security camera systems.

Enclosed please find a draft Ordinance for legislative introduction, along with a legislative digest, to approve a modified Surveillance Technology Policy for the City Administrator's Office. The amended policy would govern the use of security camera systems for divisions within the Office of the City Administrator.

By way of background, this legislation would amend an existing policy that currently governs security camera use and acquisition by the Department of Real Estate. The proposed amendments would do three things:

- Apply to cameras under the purview of the Treasure Island Development Authority (TIDA);
- Expand access to live and recorded video footage by certain Animal Care and Control staff in limited circumstances; and,
- Clarify that as new cameras are acquired, a policy amendment is not required, but all cameras will be included in the Annual Report submitted by the Office of the City Administrator.

Please feel free to contact Sophie Hayward, Director of Legislation and Public Affairs, at sophie.hayward@sfgov.org if you have any questions about the draft Ordinance or the legislative package itself.



Surveillance Technology Policy

City Administrator's Office

Security Cameras

The City and County of San Francisco values the 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 Department's Security Camera System 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 Surveillance Technology Policy ("Policy") defines the manner in which the Security Camera System (fixed or mobile) will be used to support operations of the Office of the City Administrator (CAO) and the divisions/departments (referred as CAO agencies) under its control.

This Policy applies to all department personnel that use, plan to use, or plan to secure Security Camera Systems, 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.

Additional locations and cameras acquired after approval of this policy will be reflected in subsequent Annual Surveillance Reports

POLICY STATEMENT

City departments using this policy will limit their use of Security Camera to the following authorized use cases and requirements listed in this Policy.

Authorized Use(s):

1. Live monitoring.
2. Recording of video and images.
3. Reviewing camera footage in the event of an incident.
4. Providing video footage/images to law enforcement or other authorized persons following an incident or upon request.

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

Departments may use information collected from security cameras 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

Surveillance Oversight Review Dates

PSAB Review: November 7, 2023

COIT Review:

Board of Supervisors Review:

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

In support of Department operations, Security Cameras promise to help with:

- Education
- Community Development

| | | |
|---|----------------------|---|
| X | Health | Protect safety of staff, patrons, and facilities while promoting an open and welcoming environment. |
| | • Environment | |
| X | Criminal Justice | Review video footage after a security incident such as break-ins, graffiti, accusations of behaviors that violate the law; provide video evidence to law enforcement or the public upon request by formal process, order, or subpoena. |
| | • Jobs | |
| | • Housing | |
| X | Other: Public Safety | Better management of city assets by leveraging remote condition assessment. Improvement of overall situational awareness; Assist the City's law/public safety agencies (SFPD/Sheriff's/SFFD) to identify the specific location of a security incident as they occur. Review footage afterwards to assist with related investigations, including violation of code of conduct. |

In addition, the following benefits are obtained:

| Benefit | | Description |
|---------|-------------------|---|
| X | Financial Savings | Department Security Camera Systems will save on building or patrol officers. |
| X | Time Savings | Department Security Camera Systems will run 24/7, thus decreasing or eliminating building or patrol officer supervision. |
| X | Staff Safety | Security cameras help identify violations of City Employee's Code of Conduct, Building Rules and Regulations, and City, State and Federal law and provide assurance that staff safety is emphasized and will be protected at their place of employment. |
| X | Data Quality | Security cameras run 24/7/365 so full-time staffing is not required to subsequently review footage of security incidents. Data resolution can be set by level and is currently set to high resolution. |

| | | |
|---|-----------------------|---|
| X | Service Levels | Security cameras will enhance effectiveness of incident response and result in improved level of service, by providing quicker and more informed responses. |
| X | Other: Animal Welfare | Reviewing footage afterwards to understand how an animal may have escaped its enclosure or made contact with other animals. |

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 security cameras must be kept up-to-date and maintained.

Data Collection: 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](#).
 The surveillance technology collects some or all of the following data types, as well as other data formats related to the data types listed below:

| Data Type(s) | Format(s) | Classification |
|---------------------|---------------------------|-----------------------|
| Video and Images | MP4, AVI, MPEG, AVE, JPEG | Level 1- 3 |
| Audio | .AVE | Level 1-2 |
| Date and Time | MP4 or other format, AVE | Level 3 |
| Geolocation data | TXT, CSV, DOCX | Level 3 |

Notification: Departments shall notify the public of intended surveillance technology operation at the site of operations through signage in readily viewable public areas in accordance to Section 19.5 of the Administrative Code. Department notifications shall identify the type of technology being used and the purpose for such collection.

The Department's public notice will include the following items:

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

Access: Prior to accessing or using data, authorized individuals receive training in system access and operation, and instruction regarding authorized and prohibited uses.

Access to live views and recorded footage is restricted to specific trained personnel. Recorded footage is accessed only in response to an incident.

Details on CAO agencies staff and specific access are available in Appendix A.

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) as defined by the National Institute of Standards and Technology (NIST) security framework 800-53, or equivalent requirements from other major cybersecurity framework selected by the department.

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

- Encryption: When accessing video or raw data through a browser or software client, an encrypted connection must be used to protect the information in transit between the two endpoints.
- Storage: Any use of a third-party service provider must meet City's cyber security requirements.
- Audits: A data access log will be maintained by the Department for all Security Camera 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,

department requesting data, date/time of access of raw data, outcome of data processing, as well as date processed data was delivered to users.

Data Sharing: 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. Department will endeavor to ensure that other agencies or departments that may receive data collected by their own Security Camera Systems will act in conformity with this Surveillance Technology Policy.

Department 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.

Each department that believes another agency or department receives or may receive data collected from its use of Security Cameras 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.

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.

The Department may share Security Camera footage with the following entities:

A. Internal Data Sharing:

In the event of an incident, Security Camera images may be live-streamed or shared by alternative methods upon request following an incident to the following agencies:

- Within the specific operating CAO agencies
- Police
- City Attorney
- District Attorney
- Sheriff
- Fire Department

Data sharing occurs at the following frequency:

- As needed and only as required for exigent circumstances.

B. External Data Sharing:

- Other law enforcement agencies

Data sharing occurs at the following frequency:

- As needed and only after a Deputy City Attorney consulting with the CAO agency has reviewed and approved export and release of video, upon receiving a written request with incident number.

Data Retention: Department may store and retain raw PII data only as long as necessary to accomplish a lawful and authorized purpose. Department data retention standards should align with how the department prepares its financial records and should be consistent with any relevant Federal Emergency Management Agency (FEMA) or California Office of Emergency Services (Cal OES) sections.

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

- Security Camera data will be stored for a minimum of three months to be available to authorized staff for operational necessity and ready reference, subject to technical limitations.
- If data is associated with an incident, it may be kept for longer than the standard retention period.

- Justification: This retention period conforms with the available server system storage space and allows for ample time for security staff to review footage related to security incidents and/or external requests for records.

Data may be stored in the following location:

- X Local storage (e.g., local server, storage area network (SAN), network-attached storage (NAS), backup tapes, etc.)
- X Department of Technology Data Center
- X Software as a Service Product
- X Cloud Storage Provider

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

- Automatic overwrite of all existing files when standard data retention period ends. This may take the form of a delete/reformat, wipe, overwrite of existing data, or degaussing.

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.

- Annual cybersecurity training (COIT Policy Link)

COMPLIANCE

Department shall oversee and enforce compliance with this Policy according to the respective memorandum of understanding of employees and their respective labor union agreement.

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.

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. |
|--------------------------------------|--|

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."

Appendix A: Department Specific Information

Department: City Administrator's Office

1. A description of the product, including vendor and general location of technology.

All systems below are self-contained and do not share information or data with any other departments or agencies, except as described elsewhere in this policy

| Building | Video Surveillance System | No. of Cameras | Additional notes |
|-------------------|---------------------------|----------------|---|
| 1 Newhall | Avigilon | 51 | Single tenant building (Office of the Chief Medical Examiner) with Sheriff operating all cameras |
| 1 South Van Ness | Avigilon | 34 | Multiple tenant building with RED operating cameras only in common areas (DT and MTA operate other cameras in the building) |
| 1650 Mission | Avigilon | 31 | Multiple tenant building with RED cameras only in common areas (HSA operates other cameras in the building) |
| 25 Van Ness | Avigilon | 20 | Multiple tenant building with RED operating all cameras |
| 450 Toland | Avigilon | 6 | Single tenant building (Central Shop) with RED operating all cameras |
| 555 Selby | Avigilon | 15 | Single tenant building (Central Shop) with RED operating all cameras |
| City Hall | Avigilon | 163 | Multiple tenant building with Sheriff operating all cameras |
| 49 South Van Ness | Avigilon | 128 | Multiple tenant building with RED operating all cameras |
| 1419 Bryant | Avigilon | 57 | Single tenant building (Animal Care and Control) with RED operating all cameras |
| 850 Bryant | Avigilon | 6 | Multiple tenant building (Hall of Justice) with RED operating cameras in Freight hallway and outside basement |

| | | | |
|------------------------------|----------|---|--|
| | | | area and doors (Sheriff and SF Court operate other cameras in the building) |
| 2 Avenue of the Palms Avenue | Avigilon | 5 | Single tenant building (Treasure Island Ferry Terminal) with TIDA Staff, TIDA lessees, or contracted operators operating all cameras |

2. The specific categories and titles of individuals who are authorized to access or use the collected information at the locations stated above.

- **Monitoring (Viewing Live Feed) ----**

| Building | Video Surveillance System | No. of Cameras | Authorized categories and titles of individuals |
|------------------|----------------------------------|-----------------------|--|
| 1 Newhall | Avigilon | 51 | Real Estate Division: Director, Deputy Director, Media/Security Systems and Facilities Manager OCME: Executive Director, Chief Medical Examiner, Chief Investigator Others: Deputy Sheriff, Building Manager, Chief Engineer |
| 1 South Van Ness | Avigilon | 34 | Real Estate Division: Director, Deputy Director, Media/Security Systems and Facilities Manager Others: Security Guard, Building Manager |
| 1650 Mission | Avigilon | 31 | Real Estate Division: Director, Deputy Director, Media/Security Systems and Facilities Manager Others: Security Guard, Building Manager |
| 25 Van Ness | Avigilon | 20 | Real Estate Division: Director, Deputy Director, Media/Security Systems and Facilities Manager Others: Security Guard, Building Manager |

| | | | |
|-------------------|----------|-----|---|
| 450 Toland | Avigilon | 6 | Real Estate Division: Director, Deputy Director, Media/Security Systems and Facilities Manager Others: Security Guard, Building Manager, Front Counter Staff |
| 555 Selby | Avigilon | 15 | Real Estate Division: Director, Deputy Director, Media/Security Systems and Facilities Manager Others: Security Guard, Building Manager, Front Counter Staff |
| City Hall | Avigilon | 163 | Real Estate Division: Director, Deputy Director, Media/Security Systems and Facilities Manager Others: Deputy Sheriff, SFPD officers assigned to City Hall, Mayor's Office security, City Hall Building Management engineers |
| 49 South Van Ness | Avigilon | 128 | Real Estate Division: Director, Deputy Director, Media/Security Systems and Facilities Manager Others: Security Guard, Building Manager |
| 1419 Bryant | Avigilon | 57 | Real Estate Division: Director, Deputy Director, Media/Security Systems and Facilities Manager ACC: Director, Deputy Director, Operations Manager, Animal Control Officer, Shelter Veterinarian, Principal Administrative Analyst, Front Counter Staff and other managers, supervisors and who work at the shelter |
| 850 Bryant | Avigilon | 6 | Real Estate Division: Director, Deputy Director, Media/Security Systems and Facilities Manager Others: Building engineers |

| | | | |
|------------------------------|----------|---|--|
| | | | |
| 2 Avenue of the Palms Avenue | Avigilon | 5 | TIDA: Director, Deputy Director, Principal Administrative Analyst Others: TIDA's lessees, contracted operator, and security |

- Review of Recorded Video**

| Building | Video Surveillance System | No. of Cameras | Authorized categories and titles of individuals |
|------------------|----------------------------------|-----------------------|--|
| 1 Newhall | Avigilon | 51 | Real Estate Division: Media Services staff upon approval by RED Director or Deputy Director Others: Building Managers |
| 1 South Van Ness | Avigilon | 34 | Real Estate Division: Media Services staff upon approval by RED Director or Deputy Director Others: Building Managers |
| 1650 Mission | Avigilon | 31 | Real Estate Division: Media Services staff upon approval by RED Director or Deputy Director Others: Building Managers |
| 25 Van Ness | Avigilon | 20 | Real Estate Division: Media Services staff upon approval by RED Director or Deputy Director Others: Building Managers |

| | | | |
|-------------------|----------|-----|--|
| 450 Toland | Avigilon | 6 | Real Estate Division: Media Services staff upon approval by RED Director or Deputy Director Others: Building Managers |
| 555 Selby | Avigilon | 15 | Real Estate Division: Media Services staff upon approval by RED Director or Deputy Director Others: Building Managers |
| City Hall | Avigilon | 163 | Real Estate Division: Media Services staff upon approval by RED Director or Deputy Director Others: Building Managers, Sheriff Department staff upon approval of Sheriff's Deputy City Attorney |
| 49 South Van Ness | Avigilon | 128 | Real Estate Division: Media Services staff upon approval by RED Director or Deputy Director Others: Building Managers |
| 1419 Bryant | Avigilon | 57 | Real Estate Division: Media Services staff upon approval by RED Director or Deputy Director ACC : Director, Deputy Director, Operations Manager, Principal Administrative Analyst, Animal Control Supervisor, Field Services Assistant Supervisors Others: Building Managers |
| 850 Bryant | Avigilon | 6 | Real Estate Division: Media Services staff upon approval by RED Director or Deputy Director |

| | | | |
|------------------------------|----------|---|--|
| | | | Others: Building Managers |
| 2 Avenue of the Palms Avenue | Avigilon | 5 | TIDA: Director, Deputy Director, Principal Administrative Analyst Others: TIDA's lessees and contracted operator upon approval of TIDA Director or Deputy Director or TIDA's Deputy City Attorney |

- Export recorded video

| Building | Video Surveillance System | No. of Cameras | Authorized categories and titles of individuals |
|------------------|---------------------------|----------------|---|
| 1 Newhall | Avigilon | 51 | Real Estate Division: Media Services staff upon approval by RED Director or Deputy Director |
| 1 South Van Ness | Avigilon | 34 | Real Estate Division: Media Services staff upon approval by RED Director or Deputy Director |
| 1650 Mission | Avigilon | 31 | Real Estate Division: Media Services staff upon approval by RED Director or Deputy Director |
| 25 Van Ness | Avigilon | 20 | Real Estate Division: Media Services staff upon approval by RED Director or Deputy Director |
| 450 Toland | Avigilon | 6 | Real Estate Division: Media Services staff upon approval by RED Director or Deputy Director |
| 555 Selby | Avigilon | 15 | Real Estate Division: Media Services staff upon approval by RED Director or Deputy Director |

| | | | |
|------------------------------|----------|-----|--|
| City Hall | Avigilon | 163 | Real Estate Division: Media Services staff upon approval by RED Director or Deputy Director |
| 49 South Van Ness | Avigilon | 128 | Real Estate Division: Media Services staff upon approval by RED Director or Deputy Director |
| 1419 Bryant | Avigilon | 57 | Real Estate Division: Media Services staff upon approval by RED Director or Deputy Director |
| 850 Bryant | Avigilon | 6 | Real Estate Division: Media Services staff upon approval by RED Director or Deputy Director |
| 2 Avenue of the Palms Avenue | Avigilon | 5 | TIDA lessees and contractors and TIDA Staff upon approval of TIDA Director or Deputy Director or TIDA's Deputy City Attorney |

3. 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.

For Treasure Island Development Authority (TIDA): Any complaints, questions, and concerns by members of the public regarding or relating TIDA's surveillance equipment, deployment and use of Surveillance Technology will be forwarded to TIDA's Principal Administrative Analyst. Responses will be drafted by Principal Administrative Analyst with review by the TIDA Director, or their designee, if warranted.

For all other CAO agencies: Any complaints, questions, and concerns by members of the public regarding or relating RED's surveillance equipment, deployment and use of Surveillance Technology will be forwarded to the applicable Building Manager and copied to the applicable District General Manager. Responses to same will be drafted by the Building Manager with review by the District General Manager, and by the Director, or their designee, if warranted.

4. Specific details on where data will be stored (local, DT, SaaS, Cloud Storage) including name of vendor and retention period.

| Building | Video Surveillance System | No. of Cameras | Storage site |
|------------------------------|----------------------------------|-----------------------|---|
| 1 Newhall | Avigilon | 51 | Avigilon local server/recorder in server room |
| 1 South Van Ness | Avigilon | 34 | Avigilon local server/recorder in server room |
| 1650 Mission | Avigilon | 31 | Avigilon local server/recorder in server room |
| 25 Van Ness | Avigilon | 20 | Avigilon local server/recorder in room 400 |
| 450 Toland | Avigilon | 6 | Avigilon local server/recorder in server room |
| 555 Selby | Avigilon | 15 | Avigilon local server/recorder in server room |
| City Hall | Avigilon | 163 | Avigilon local server/recorder in AV server room |
| 49 South Van Ness | Avigilon | 128 | Avigilon local server/recorder in server room |
| 1419 Bryant | Avigilon | 57 | Avigilon local server/recorder in server room |
| 850 Bryant | Avigilon | 6 | Local server in the Chief Engineer's office |
| 2 Avenue of the Palms Avenue | Avigilon | 5 | Local server on the Ferry Terminal |
| All the locations above | | | City Administrator and Deputy City Administrators |

5. Is a subpoena required before sharing with law enforcement?

- No.