Surveillance Technology Policy

Department of Technology
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 department operations.

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.

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 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.

All data collected by surveillance cameras is the exclusive property of the City and County of San Francisco. Under no circumstance shall collected data be sold to another entity.

Surveillance Oversight Review Dates
COIT Review: March 18, 2021
Board of Supervisors Review: TBD

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; provide video evidence to law enforcement or the public upon request by formal process, order, or subpoena.
	▪ Jobs	
	▪ Housing	
X	Other	Better management of city assets by leveraging remote condition assessment. Improvement of overall situational awareness.

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.

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:

Data Type(s)	*Format(s)*	*Classification*
Video and Images	MP4, AVI, MPEG	Level 3
Date and Time	MP4 or other format	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 department 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: Data retained by the Department will be encrypted. Raw data may be retained by the Department only for the authorized use case of sharing with law enforcement or the public. - 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 to the following agencies:

- Within the operating Department
- Police
- City Attorney
- District Attorney
- Sheriff
- On request following an incident.

Data sharing occurs at the following frequency:

- As needed.

B. External Data Sharing:

- Other local law enforcement agencies

Data sharing occurs at the following frequency:

- As needed.

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 one (1) year to be available to authorized staff for operational necessity and ready reference. 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.
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.

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 Responses
Department: Asian Art Museum

1. A description of the product, including vendor and general location of technology.
    - CCTV product is Exacqvision, vendor for support is Pacific Technology CCTV, located in Santa Rosa. Cameras are located in both public facing and staff only areas both inside the museum and covering exterior areas.
2. The specific categories and titles of individuals who are authorized by the Department to access or use the collected information
    - Security Director (0922) – full access
    - Security Supervisors (8228) – full access
    - Security staff (8226 and 8202) – view access with access to recording in the event of an incident when supervisors are not present
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.
    - Information will be posted on the Asian Art Museum website. The Security Director or designee will respond to questions, complaints, and concerns in a timely manner.
        - securitymanagers@asianart.org
4. Specific details on where data will be stored (local, DT, SaaS, Cloud Storage) including name of vendor and retention period.
    - Data is stored on servers within the museum main server room. Retention period is variable based on motion recording and space on each server. Approximately 6 months retention for each server.
5. Is a subpoena required before sharing with law enforcement?
    - No

Appendix A: Department Specific Responses

Department: City Adminstrator's Office - Real Estate Division

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

   All RED systems are self-contained and do not share information or data with any other departments or agencies.

Building	**Video Surveillance System**	**Number of Cameras**
1 Newhall (Medical Examiner)	Avigilon	51
1 South Van Ness	Avigilon	34
1650 Mission	Avigilon	31
25 Van Ness	Avigilon	20
450 Toland (Central Shop)	Avigilon	6
555 Selby (Central Shop)	Avigilon	15
City Hall	Avigilon	163
49 South Van Ness	Avigilon	128
ACC 1419 Bryant	Avigilon	57
850 Bryant	Avigilon	6

2. The specific categories and titles of individuals who are authorized by the Department to access or use the collected information.

   - Monitoring (Viewing Live Feed) –

- HOJ – Limited to Basement Door, Freight Hallway, Outside Basement Area – Campus Superintendent, Boiler Watch Engineering, Engineering staff (24/7)

- ACC – Security Guard

- City Hall: Deputy Sheriff

- Other RED Facilities: Deputy Sheriff, Security Guard, Building Manager

- Review of Recorded Video –

    - City Hall: Sheriff, Media Services staff upon approval by Sheriff's legal counsel for City Hall

    - OCME: Deputy City Administrator

    - ACC – RED Media Services upon approval by Department head

    - Other RED Facilities: Security, District General Manager, Campus Superintendent, Building Manager, RED Department head upon approval by Department head

- Export recorded video—

    - City Hall: Media Services staff upon approval by Sheriff's legal counsel for City Hall

    - OCME: Deputy City Administrator

    - Other RED Facilities: Media Services staff, District General Manager, Campus Superintendent, Building Manager - - Upon approval of Director, or designee, after consultation with City Attorney's Office

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.

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.
    - City Hall – Avigilon local server/recorder in AV server room
    - Medical Examiner – Avigilon local server/recorder in MPOE at 1 New Hall
    - One South Van Ness – Avigilon local server/recorder in server room at 1 South Van Ness
    - 1650 Mission – Avigilon local Server/Recorder – MPOE at 1650 Mission
    - Central Shop #1- Avigilon local server/recorder in server room at 555 Selby
    - Central Shop #2 - Avigilon local server/recorder in server room at 450 Toland
    - 25 Van Ness – Avigilon local server/recorder in room 400 at 25 Van Ness
    - 49 South Van Ness – Avigilon local server/recorder in server room at 49 South Van Ness
    - 850 Bryant (HOJ) – Microbiz local server/recorder in server room at HOJ

5. Is a subpoena required before sharing with law enforcement?
    - No.

Appendix A: Department Specific Responses
Department: San Francisco International Airport

1. A description of the product, including vendor and general location of technology.
   The Airport uses Verint Video Management Software (VMS) and, primarily, Pelco Analog and Digital Pan-Tilt-Zoom (PTZ) and fixed cameras. The cameras are installed in public areas of the Airport. Specific to this submission, the cameras are located pre-security.

   The Verint system is a closed system, running on a security local area network that is not exposed to the internet.

2. The specific categories and titles of individuals who are authorized by the Department to access or use the collected information

   - *9202 911 Dispatcher*
   - *9203 911 Dispatch Supervisor*
   - *9212 Security Operations Center (SOC) Analyst*
   - *9213 Airfield Safety Officer*
   - *9220 SOC Supervisor*
   - *9221 Airport Operations Supervisor*
   - *Air Train Staff and Contractors*
   - *Aviation Security System MX Contractors*
   - *Ground Transportation Unit*
   - *Parking Management*
   - *SFPD-AB*

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.

   Public question and complaint can be submitted via the:

   - *Airport Guest Services (Contact SFO)*
   - *Airport public email, phone, or website ((Contact SFO), or*
   - *Airport Commission meetings (How to Address the Commission)*

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

   Data is in local server for 45 days then video files are transferred to Amazon Web Services for up to 1 year and files are deleted after 320 days based on lifecycle policy in AWS.

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

   - No

6. Questions & Concerns

- *In Authorized Use(s) - #3 "incident" should be defined*
- *In Notification – Admin Code Section 19.5 does not apply to Airport. Airport does not intend to post signage at location of each camera. However, Airport will publish public notice on its external website at www.flysfo.com.*
- *In Audits – "processed and utilized" is unclear. Alternate language suggested-- "shared with a 3rd party."*
- *In Audits –departments should not ask public record act requestors to provide their "reasons/intended use for data." "Intended use" is not a consideration when determining whether video footage is discloseable pursuant to a PRA request.*
- *In Data Sharing – 3rd procedure lists "Redact names, scrub faces…" The video is unalterable and names are not contained in the system. In addition, if video footage is subject to disclosure under PRA, scrubbing faces may be inappropriate unless privacy interests are implicated.*
- *In External Data Sharing – data collected can be requested under Public Records Request.*
- *In Data Retention – 1st paragraph states "…department prepares its financial records…" Not sure how this aligns with use of technology.*

Appendix A: Department Specific Responses
Department: Arts Commission

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

   Exacqvision servers. Axis, Hanwha and Samsung Cameras.

   - Main Gallery: 401 Van Ness Avenue, Suite 126 (6 cameras)
   - African American Art & Culture Complex: 762 Fulton Street (9 cameras)
   - Bayview Opera House: 4705 3rd Street (12 cameras – Exacqvision)
   - Mission Cultural Center for Latino Arts: 2868 Mission Street (28 cameras)
   - SOMArts: 934 Brannan Street (15 cameras – Exacqvision)

2. The specific categories and titles of individuals who are authorized by the Department to access or use the collected information
   - Arts Commission Staff:
     - Deputy Director of Programs (0923)
     - Director of Community Investments (1824)
     - Commission Secretary (1452)
     - Office Manager (1840)
   - Law enforcement

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.

   Public can inquire by contacting the Department directly (listed below) or through the City's Public Records Request process.

   401 Van Ness Avenue, Suite 325

   San Francisco, CA 94102

   (415)252-2255

   ART-Info@sfgov.org

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

   Local servers installed by Microbiz Security Company.

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

   - No

Appendix A: Department Specific Responses
Department: Child Support Services

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

Sonitrol is used to protect against unauthorized access to confidential customer data, and for customer and employee safety. Sonitrol monitors physical access to the facility where customer information resides to detect and respond to physical security incidents. Sonitrol surveillance cameras are installed at points of entry, public lobby, and Intake/Interview areas.

Sonitrol's verified alarms are sound-based – not motion-based – so when an alarm is triggered, our monitoring professionals can actually listen to determine whether a break-in is in progress, or whether a false alarm has occurred. If it is a break-in, we immediately dispatch police and relay real-time information to the responding officers. If it is a false alarm, we simply reset the system without bothering you or the police. Because of this ability to verify alarms, Sonitrol has the highest apprehension rate and the lowest false alarm rate in the industry.

2. The specific categories and titles of individuals who are authorized by the Department to access or use the collected information:

CCSF employees:

- *1094- IT Operations Support Admin IV*
- *1093 - IT Operations Support Admin III*
- *0922 – Manager I*
- *1244 - Sr. HR Analyst*
- *0952 - Deputy Director II*
- *0963 - Director III*
- *Contractors – Allied Security Guards*

SFPD – Southern Station:

- *Police Officers*

Departmental access is restricted to SFDCSS IT, SFDCSS Executive Management, SFDCSSHR and Allied Security Guards. Upon request, SFDCSS IT will provide access to

video footage to the above mentioned, as well as SFPD personnel. Executive Management, IT Manager/Security Officer or HR will request IT to review and provide video footage clip(s) of access point records in the event of a security or personnel incident. All staff and contractors are required to sign confidentiality forms annually, complete annual training and submit to Live Scan background checks to meet minimum employment requirements

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.

Customers can submit inquiries by telephone, letter, e-mail, facsimile, in person by visiting the office, or through the customer self-service website.

1. *Department of Child Support Services website: https://sfgov.org/dcss*
2. *Email to: sfdcss@sfgov.org*
3. *Phone: Call 311 or 1-866-901-3212*

Incoming communications from the public are reviewed by a supervisor for immediate handling or assigned for specialized review and resolution. Response time 24-48 hours. Communication information is captured and reported out in monthly management reports.

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

Technical Safeguards: SFDCSS follows restricted access protocols. Only IT Manager and IT Administrators have access to stored video footage and access point records. To protect data from potential breach, misuse or abuse that may result in impacts to the public, data is maintained on secure, department-owned servers. Server backup transmission is secured in accordance with Federal, State and local regulations. Only persons authorized to utilize the data may access the information and are required to maintain records of access. Data is provided to Executive Management, HR and SFPD upon request. Lobby Security Guard personnel have view-only access and monitor live footage during business hours.

Physical Safeguards: Data can only be accessed onsite at SFDCSS – 617 Mission Street or, in the event of a disaster, our secondary backup appliance is stored at SFO The data and data systems are secured during transmission and during rest in accordance with Federal, State and Local regulations.

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

    - No

Appendix A: Department Specific Responses
Department: Emergency Management

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

Cameras are deployed at all entry/exit points for the Combined Emergency Communications Center Building at 1011 Turk St. These include entry points and drive paths to underground parking garage, balcony space to the east face of the building, along the walkway of the west face of the building that is along Turk St, and side space area in the buffer protection zone adjacent to the REC facilities.

2. The specific categories and titles of individuals who are authorized by the Department to access or use the collected information

8300 SFSD, Cadet

8304 or 8504, SFSD Deputies

8306 SFSD Sr. Deputy

8308 SFSD, Sergeant

1842 DEM, Facility Manager

1093 DEM IT Administrator

Access to the system is through designated PC workstations with the appropriate manufacturer proprietary client software. The software requires an assigned User ID and Credential/password before accessing the video. Permissions to export the video are provided on individual account settings.

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.

DEM has the Custodian of Records function that allows the public to seek access to the cameras, or to register complaints or concerns. DEM's external affairs divisions handles public questions or concerns, including Sunshine Requests.

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

   There is currently a total of 28 cameras which most of them are fix point focus and 6 pan-tilt-zoom (PTZ) cameras. The video is recorded across two on-premise video servers

converting the analog video to digital file format utilizing video management software from Exacqvision.

5. Is a subpoena required before sharing with law enforcement?
    - No

Appendix A: Department Specific Responses
Department: Human Resources

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

   DHR's security cameras are non-zoom, fixed surveillance cameras connected to an OpenEye video recording system. The equipment was purchased more than ten years ago, and DHR was unable to locate purchase details.

2. The specific categories and titles of individuals who are authorized by the Department to access or use the collected information

   Video may only be accessed by DHR's 1042 IS Engineer, and only at the request of (a) the Human Resources Director; (b) the DHR Managing Deputy Director; or (c) the Department Personnel Officer.

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.

   Members of the public can register complaints/concerns or submit questions via calls or emails at 311.org. DHR's Director of Finance and Administration will work with the 311 Team to ensure that responses meet or exceed 311's standards.

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

   Data is only available to the IS Engineer, and is only accessible within the DHR Network. Access requires Local Area Network access, software installed, system configuration, software log-in, and passwords. The cameras record on a time loop that eventually overwrites itself. The recording system is not designed for permanent storage.

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

- No

Appendix A: Department Specific Responses
Department: Public Health

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

Lenel On-Guard/Prism and Johnson Control, Inc. P2000 System, Vendors: Comtel and Johnson Control, Inc.

Locations and Number of Cameras:

- Zuckerberg General Hospital: 381 Lenel On-Guard/Prism cameras
- Laguna Honda Hospital: 128 Johnson Control, Inc. cameras

2. The specific categories and titles of individuals who are authorized by the Department to access or use the collected information

- Comtel Service Technicians - Technical support (integrators/maintenance/repairs)
- San Francisco Sheriff Department - SOC
- 7262 Maintenance Planner
- 8300 Sheriff's Cadet
- 0953 Deputy Director III
- 8304 Deputy Sheriff
- 8306 Senior Deputy Sheriff
- 8308 Sheriff's Sergeant
- 8310 Sheriff's Lieutenant
- 8238 Public Safety Communications Dispatcher

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.

Complaints can be sent to Director of Security, Department of Public Health in accordance to the 2020 – SOP – SFDPH Records and Disclosure Policy. Contact information for complaints or concerns:

City and County of San Francisco
1001 Potrero Avenue
San Francisco, CA 94110
Office: 415-206-2577
Cell: 415 926-3669
basil.price@sfdph.org

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

The files at rest are stored on the on premises Lenel system with proprietary encryption.

Appendix A: Department Specific Responses
Department: Technology

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

   DT Critical Infrastructure Camera system (CIC) use Avigilon Control Center video management software to mange and interact with high-definition video. It captures and stores HD video, while intelligently managing bandwidth and storage using High Definition Stream Management (HDSM) technology.

   The CICs are located at the eight Public Safety Radio sites, as well as the DT Public Safety Division headquarters at 200 Paul Ave.

2. The specific categories and titles of individuals who are authorized by the Department to access or use the collected information.

   7362 Communications System Technician
   7368 Senior Communications System Technician
   8234 Fire Alarm Dispatcher
   8236 Chief Fire Alarm Dispatcher

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.

   Members of the public can register complaints or concerns through the following mechanisms:

   - Via a form on the Department of Technology website https://tech.sfgov.org/
   - Send an email to dtis.helpdesk@sfgov.org
   - Call the Citywide Service Desk at (628) 652-5000, or
   - Send a letter via post to 1 S. Van Ness Ave, 2nd floor, San Francisco, CA, 94103

   Regardless of which communication channel a member of the public uses, their inquiry is recorded into ServiceNow, a work management tool in use by the Department of Technology and assigned to a staff member. ServiceNow creates a ticket for each entry, and staff receive an email when assigned to work the ticket. Each ticket has a tracking number, date received and expected due date.

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

   The video recorded by the CIC system is stored locally. DT understands that it may have to store recorded video for a minimum of one year, we will seek to store video for the minimum possible duration.

5. Is a subpoena required before sharing with law enforcement?
   - No

Appendix A: Department Specific Responses
Department: Fire

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

The Fire Department has installed security cameras at its current Station 49 Ambulance/Bureau of Equipment facility as well as its Division of Training. Cameras are mounted on fences and walls for security purposes. In addition, security cameras are part of the plans of two current facilities under construction for the Department.

2. The specific categories and titles of individuals who are authorized by the Department to access or use the collected information

Access to the cameras are limited to a select few members in the Department's Administrative Division. Video is only accessed after a security incident has been identified and is not actively monitored.

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.

Members of the public can register complaints / concerns or submit questions through the Fire Department website and complaint process, or through the Chief's Office. (https://sf-fire.org/how-file-complaint). Constituent calls and complaints to the Fire Department are routed to the appropriate division The appropriate division designee will discuss concerns or complaints with constituent and record details regarding nature of conversation. If additional action is required or requested by caller, the Fire Department commits to a follow-up (by email or telephone) in a timely manner.

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

Data is stored on a secured cloud storage solution for a period of six months. The Department is working with COIT and the City Attorney on any data retention requirement changes.

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

- No

Appendix A: Department Specific Responses
Department: Homelessness and Supportive Housing

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

    1) 440 Turk Street Headquarters
    Cameras: 2x Samsung PNM-7000VD, 18x Samsung XNV-6080R
    Server: exacqVision
    Locations: devices are deployed mostly inside the building. Two cameras are deployed at the gate facing the front gate entrance area and street.

    2) Below technology are being used at shelter:
    Different site might have different type of DVR equipment but a typical DVR equipment would be Honeywell – HRDP16D1T0-R connected to various security cameras.

    Cameras will be mounted on ceiling in vulnerable areas at the shelters & navigation centers. It should be noted that cameras are not mounted in the bathroom or sleeping areas. Same applies for 440 Turk building.

2. The specific categories and titles of individuals who are authorized by the Department to access or use the collected information

    Sr. IS Engineer (1043) and Facilities Manager (7203) are authorized by the Department to access or use the collected information as requested by law enforcement or department HR.

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.

    Constituent calls and complaints to the Department of Homelessness & Supportive housing (HSH) are received by counter personnel and routed to the Shelter & Navigation Center Program manager. Program manager will discuss concerns or complaints with constituent, enter details regarding nature of conversation on excel spreadsheet stored in the department shared drive, referred to as the Security Camera System Constituent Feedback Log ("CFL"). If additional action is required or requested by caller, HSH 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, Program manager shall notify department IT of details and discuss resolution before follow-up with caller. Final outcome and action(s) taken shall be logged onto CFL.

Constituent can also file direct complaint to the Shelter Monitoring Committee and the Shelter Advocates. These organizations work directly with the HSH to address comments or concerns.

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

   The surveillance camera system at 440 Turk Street provides live views and record video footage to a dedicated, secure server. The footage is recorded on the server and stored for a limited amount of time. Data collected or processed by the 440 Turk Street Surveillance Camera System will not be handled or stored by an outside provider or third-party vendor on an ongoing basis. The Department will remain the sole Custodian of Record.

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

   - Yes

Appendix A: Department Specific Responses
Department: Human Services Agency

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

The following is a product inventory and manufacturer's description:

- 1235 Mission:
  - HONEYWELL MAXPRO – RECORDER
  - PELCO DX8100 – RECORDER
  - ANALOG CAMERAS (25)
  - IP CAMERAS (16) – HONEYWELL IP AND 2 AXIS P3708-PVE
- 1440 Harrison:
  - SALIENT – RECORDER
  - IP CAMERAS (12) – HONEYWELL IP
- 170 Otis:
  - HONEYWELL – RECORDER
  - ANALOG CAMERAS (31) – SONY
  - NAS (VM) – RECORDER
  - WIN SERVER 2019 / VAST VIDEO MANAGEMENT SOFTWARE (VMS)
  - DIGITAL IP CAMERAS (6) – VIVOTEK
- 2 Gough:
  - NAS (VM) – RECORDER
  - WIN SERVER 2019 / VAST VIDEO MANAGEMENT SOFTWARE (VMS)
  - DIGITAL IP CAMERAS (2) - VIVOTEK
- 3120 Mission:
  - HONEYWELL – RECORDER
  - ANALOG CAMERAS (4)

- Manufacturers' Product Descriptions:
  - VIVOTEK - VIVOTEK Inc. was founded in February 2000. The Company markets VIVOTEK solutions worldwide, and has become a leading brand in global security surveillance. To fulfill its global strategic footprint, VIVOTEK is committed to building an ecosystem for the IP surveillance industry, and looks forward to long term collaboration and growth with all partners in our shared pursuit of a safe and secure society.
  - PELCO DX8100 - The DX8100 Series digital video recorders (DVRs) are professional security-level DVRs based on a new and innovative hardware platform that is powered by unparalleled and unique high-performance

software. As the security requirements of your business expand into multiple sites and become more diversified, you need a professional DVR that you can quickly and effortlessly increase the channel and recording capacity. •The DX8100 is interoperable with your existing DX8000 DVRs, allowing you to build upon your existing security system. A DX8100 client can operate and administer both the DX8100 and DX8000 within the same network.•When you need to quickly and easily add more security cameras, the new DX8100-EXP 16-channel expansion unit extends the 8- or 16-channel DX8100 to 24 or 32 channels. With or without the channel expansion unit, all of the cameras can now take advantage of the increased frame rate of 2CIF and 4CIF recording. The DX8100 records video up to 480 images per second ips at a maximum CIF image size. •If your security project requirements increase storage capacity, you can extend internal storage up to 3 TB. With the optional DX9200 HDDI, you can further increase the DX8100 storage capacity. Alternately, you can use the DX9200 HDDI as a redundant RAID solution. •As your audio security needs grow, use the DX8108-AUD or DX8116-AUD audio option to add a total of 8 or 16 audio inputs. •Sophisticated video security applications require a network of DVRs to monitor multiple locations. The 10/100/1000 megabit Ethernet port supports today's high-speed networks. You can network your DX8100 and DX8000 systems and remotely operate the DVRs for continuous, motion detection, alarm, ATM/POS, normal scheduled recording, and administer and view live and playback video. For time-critical security applications, you must ensure that all video recordings are synchronized to an accurate time source. The DX8100 supports the network time protocol (NTP), which allows you to synchronize all networked DX8100s to one NTP time server.

- HONEYWELL MAXPRO VMS is an enterprise-class video management and hybrid solution. It enables you to operate the traditional analog, network and IP based video equipment in the same surveillance network. You can deploy thousands of cameras in number of locations, and add many video devices such as recorders and monitors.
- NAS VIRTUAL MACHINE (VM) – The VM is powered by Intel® Xeon® dual core CPU E5-2670 0 @ 2.60GHz x-64 processor, 64-bit Operating System, 4.00 GB of RAM, 75 GB of hard drive space.

- SALIENT NVR SERVER – Salient's hybrid NVRs are industry-leading, value-oriented digital video surveillance systems. Power-built for the rigors of continuous duty operation using advanced components, the 1U rack-mountable PowerPro hybrid NVR delivers the reliability and processing power required for mission critical video surveillance. PowerPro offers a Single Intel Xeon processor with 16GB of memory and up to 48TB of video storage delivering high reliability and processing power. Providing up to 32 analog direct connect channels, this hybrid NVR supports IP and analog cameras in a 1U rack mount unit.
- VIVOTEK's FD8169A is an easy-to-use fixed dome network camera specifically designed for indoor security applications, with a 2MP sensor enabling a viewing resolution of 1920x1080 at a smooth 30 fps. Dynamic and highly adaptable. The FD8169A is an all-in-one camera capable of capturing high quality video at high resolutions of up to 2 Megapixels. It also features POE, Real-time H.264, MJPEG Compression (Dual Codec), Removable IR-cut Filter for Day & Night Function, Built-in IR Illuminators effective up to 20 Meters, SNV (Supreme Night Visibility) for Low Light Conditions, Smart Stream II to Optimize Bandwidth Efficiency, Smart IR Technology to Avoid Overexposure, Supports ONVIF Standard to Simplify Integration and Enhance Interoperability, Support Installation with AM-712 Indoor Conduit Box, VIVOCloud App & Portal for 24/7 Surveillance, and Trend Micro IoT Security
- VIVOTEK's FD8182-F2 is an economic professional indoor fixed dome network cameras in VIVTOTEK's 5MP V-Pro Lite series. Design to provide higher resolution and sharper image with more detail, the FD8182-F2 offers up to 15 fps at 5-Megapixel or 30 fps at 1080p resolution. With powerful 3D Noise Reduction technology and Smart Stream technology, the FD8182-F2 can also optimize resolution for a desired object or area to maximize efficiency of bandwidth usage. Other features include POE, Built-in IR Illuminator Effective up to 30 Meters, WDR Enhancement for Unparalleled Visibility in Bright and Dark Environments, Smart Stream to Optimize Bandwidth Efficiency, 3D Noise Reduction for Low-light Conditions, Two-way Audio, PIR motion sensors, Video Rotation for Corridor View, Support Installation with AM-712 Indoor Conduit Box, VIVOCloud App & Portal for 24/7 Surveillance, and Trend Micro IoT Security

- VIVOTEK's IB8360-W (wireless) is a stylish 2-megapixel mini outdoor bullet network camera, specifically designed for boutique retail applications. Delivering a resolution of 1920x1080 at 30 fps, having IR illuminators effective up to 12 meters, and including SNV technology for low light environments, the remarkable cameras provide users with superior image quality around the clock. It also provide built-in IR Illuminators up to 12 meters, Smart IR Technology to Avoid Overexposure, SNV (Supreme Night Visibility) for Low Light Conditions, Smart Stream II to Optimize Bandwidth Efficiency, Weather-proof IP66-rated Housing, Built-in 802.11 b/g/n WLAN, Compact Size, VIVOCloud App & Portal for 24/7 Surveillance, and Trend Micro IoT Security
- HANWHA PNM SERIES MULTI-SENSOR 360 – Network vandal outdoor Multi-sensor Multi-Directional dome camera, (5MP X 4 sensors) 20MP @ 30fps WDR off/on, motorized vari-focal Lens 2.6x (3.6 ~ 9.4mm) (102.5˚ ~ 38.7˚), triple Codec H.265/H.264/MJPEG with WiseStream II technology, 120dB WDR, Defocus detection, built in analytics, true D/N, 4x SD card, hallway view, HLC, Defog detection, DIS(Gyro sensor), 12VAC/HPoE (power adaptor is included), IP66/IK10, -40°C ~ +55°C (-40°F ~ +131°F)
- HANWHA X SERIES DOME – WiseNet X powered by WiseNet 5 network IR indoor dome camera, 5MP @30fps WDR off/on, 3.7mm fixed focal lens (97.5°), H.265/H.264/MJPEG, WiseStream II compression technology, 120dB WDR, USB port for easy installation, advanced video analytics and sound classification, High powered IR LEDs range of 98', True D/N, dual SD card, hallway view, HLC, defog detection with simple focus, DIS , 12VDC/24VAC/PoE, IK08 rated
- AXIS P3708-PVE - is a fixed dome network camera with three sensors. It gives you a 180º panoramic overview of large areas using a single camera. And it's perfect for use in challenging light conditions, both during the day and at night.
- HONEYWELL – HD4DIRH - 700TVL VFAI WDR TDN IR Mini Dome – Honeywell 960H System Series of cameras provides a wide range of high-quality, feature rich video surveillance options for indoor, outdoor, and low-light applications. 1/3" 960H CCD image sensor, ultra-high resolution image (700TVL), 3D digital noise reduction, digital wide dynamic range, backlight compensation and highlight masking, smart IR technology for even distribution of the IR, 2.8-12 mm varifocal auto iris (VFAI) lens, true day/night

function for vivid color pictures by day and clear black and white pictures at night, excellent low-light performance (0.19 lux color, 0 lux with IR LEDs on), 18 IR LEDs provide up to 50 ft of illumination, depending on scene reflectance, weatherproof, impact-resistant housing (IP66), built-in heater for cold weather operation down to -40 F, breather vent prevents condensation buildup.

- HONEYWELL – HD4D2 – 650 TVL DOME CAMERA – PRODUCT DESCRIPTION NOT FOUND/UNAVAILABLE.
- HONEYWELL – H4L2GR1V – 2 MEGAPIXEL DOME IP CAMERA - Full HD 1080p 50/60 fps image with a ½.8"2 MP sensor, WDR up to 120 dB ensures glare-free images, true day/night provides colour images by day and clear black-and-white images at night with ICR, excellent low-light performance with 3D noise reduction, saving storage and bandwidth together with H.265 High Profile codec, low light technology is able to capture high quality colour images in low light environments, 2.7-13.5 mm, F1.6, motorized focus/zoom lens, H.265 plus, H265, H.264 and MJPEG codec, triple stream support, IR LEDs provide up to 50m (150') of illumination in dimly lit or night time scenes (depending on scene reflectance), smart IR technology provides even distribution of IR, waterproof (IP67) and IK10 vandal resistant camera housing, -40C to 60C working temperature, ONVIF Profile S, G & Q compliant, security features include individual signed certificates and data encryption, cameras can be retrofitted on many existing DVR/NVR installations without requiring additional storage, built-in PoE eliminates separate power supply and associated wiring; 24 V AC/12 V DC inputs where PoE is unavailable, 12 VDC/2W output, supports up to 128 GB micro SDHC (Class 10) card for local video storage when network is interrupted.
- ARECONT – AV2256PM – 2 MEGAPIXLE DOME IP CAMERA - The AV2256PM MegaDome® 2 series network camera is part of Arecont Vision's Wide Dynamic Range line of H.264 MegaDome® 2 series cameras. This fully compliant implementation of H.264 (MPEG 4, Part 10) provides full 1920 x 1080 megapixel resolution at full video frame rates of 32fps. The AV2255AM camera line provides an all-in-one solution with integrated 1080p resolution camera, remote focus, remote zoom, motorized P-iris lens, and IP66 and vandal resistant dome enclosure. With the features of Casino mode, ONVIF Profile S, PSIA conformance, privacy masking, extended motion detection and

flexible cropping, the AV2256PM is a high sensitivity, PoE (IEEE 802.3af) compliant camera. Built with Arecont Vision's massively-parallel MegaVideo® technology, this camera offers over six times the resolution of standard resolution IP cameras with the ability to output full real-time frame rates and deliver the high quality megapixel imaging for both indoor and outdoor applications.

- AXIS – P3707-PE – 8 MEGAPIXEL MULTI-SENSOR 360-DEGREE IP CAMERA - AXIS P3707-PE comprises four camera heads that can be repositioned along a circular track to point in the desired viewing direction. Each camera head can be individually tilted and adjusted to provide a 108° to 54° horizontal field of view for either wide or zoomed-in views. The camera heads can be rotated to support Axis' Corridor Format for optimal coverage of vertically oriented scenes. A specially designed clear cover, with no sharp edges, allows for undistorted views in all directions. AXIS P3707-PE supports individually configurable video streams for each camera head, as well as quad-view streaming, enabling 1080p resolution videos at 12.5/15 frames per second and 720p videos at full frame rate.
- SONY – EX543 – ANALOG CAMERA – PRODUCT DESCRIPTION NOT FOUND/UNAVAILABLE
- TRIVIEW – TFD-CVSH312A1241IR – DOME ANALOG CAMERA – PRODUCT DESCRIPTION NOT FOUND/UNAVAILABLE

2. The specific categories and titles of individuals who are authorized by the Department to access or use the collected information
   - 2966 WELFARE FRAUD INVESTIGATOR
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.

Public:

General compliant and comment forms are available in public areas of all HSA buildings. All complaints are processed on a flow basis.

City and County of San Francisco Employees:

All questions regarding this policy should be directed to the employee's supervisor or to the director. 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.

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

See question #1 for specific storage details. When an incident occurs, images may be recovered from the recorder and preserved on DVD diskettes pursuant to the requirements of a given investigation and evidence retention guidelines. Data is stored with case documents in locked file cabinet and/or evidence vault in secure agency office facility.

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

Appendix A: Department Specific Responses
Department: Port

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

The Port Security CCTV System consists of the following components.

- Arcenot - Omni Directional Day/Night Camera
- Arcenot – Fixed IR Camera
- Arcenot- Day / Night Camera
- Axis – Camera
- Illuminar – Infrared Illuminator
- Raytec- 180 Degree Illuminator
- Vario- Infrared Illuminator
- Exacq- Server
- Exacq- NVR

Port Security Security Camera technology is installed on Port property along the 7.5 miles of San Francisco waterfront. This technology includes CCTV cameras installed on exterior of Pier Bulkhead buildings, Pier Sheds, and Small Craft Harbors. Port Security Camera technology provides layered security protection to multiple MTSA regulated facilities throughout the Port.

2. The specific categories and titles of individuals who are authorized by the Department to access or use the collected information

- Security and Emergency Planning Manager (0922)
- Homeland Security Project Manager (9978)

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.

Members of the public may contact the Port's Custodian of Records or by calling the Port's 24/hr. contact number 415-274-0400

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

The data is stored on servers maintained by the Department of Technology.

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

- No

Appendix A: Department Specific Responses
Department: Rent Board

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

The CIC system records video of the Rent Board's lobby and entrance. In the event of an incident of theft of vandalism, RNT staff will review the recorded video to determine if it has captured the incident.

Q-See QT454-This DVR uses high-performance video processing chips and an embedded Linux operating system for quality image recording and ease of use. It utilizes numerous advanced technologies including the industry-standard H.264 codec to deliver high-quality, smooth videos and dual stream capability for remote viewing. A SATA hard-drive interface offers upgradability and VGA output allows users to connect to any standard TV or monitor for viewing.

The Lobby Cameras are used to protect against harassment, theft, safety or vandalism of the Rent Board's lobby area, which includes publicly accessible computers and other City owned assets.

2. The specific categories and titles of individuals who are authorized by the Department to access or use the collected information

0961 – Department Head

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.

The Department of Human Resources Employee Handbook addresses Employee Use of City Resources and City Computers and Data Information Systems. The Department of Technology defines CIC as a City resource.

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

All data is stored locally.

5. Is a subpoena required before sharing with law enforcement?
    - No

Appendix A: Department Specific Responses
Department: Recreation and Parks

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

Approximately 300 security cameras are located on poles or building facades. Cameras range from 2 to 5 megapixels and most have pan-tilt-zoom capabilities. The video feeds are recorded and retained on a server at each site. If the server is connected to RPD's network, the feed can be streamed to a RPD's Park Ranger Headquarters where they can be monitored for public safety purposes. In some instances, cameras are streamed to the operators on site who are managing the facility and services on RPD's behalf.

As of March 2021, below are the sites with security cameras:

Location	Type
501 Stanyan NVR	Arecont Vision
Betty Ann Ong	Arecont Vision
	Samsung
	Vivotek
Boeddeker Park	Arecont Vision
	Samsung
Conservatory of Flowers GGP	Arecont Vision
	Samsung
Dolores Park	Arecont Vision
Geneva Powerhouse	Samsung
Glen Park Rec	Samsung
Golf Course GGP	Samsung
Herz Park Playground	Arecont Vision
Huntington Park	Arecont Vision
Japanese Tea Garden	AXIS
Maintenance Yard GGP	Samsung
Margret Hayward Complex	Samsung
Portsmouth Square	Samsung
SF Marina	Arecont Vision
Willie Woo Woo Wong	Samsung
COIT Tower	Samsung
Beach Chalet Soccer Field	Samsung
Crocker Amazon	Samsung

RPD is continuously adding cameras to new capital sites and existing facilities (budget permitting).

2. The specific categories and titles of individuals who are authorized by the Department to access or use the collected information

The following individuals may access or use the collected information:

- Park Rangers (8208-8210)
- IT analysts and technical staff (1820 series, 1050 series, 1090 series)

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.***

Members of the public can register complaints/concerns or submit questions to San Francisco Recreation and Parks through several ways:

- Send written correspondence to McLaren Lodge in Golden Gate Park, 501 Stanyan Street, San Francisco, CA 94117
- Call to the RPD Front Desk 415-831-2700
- Send an email to rpdinfo@sfgov.org
- Contact 311.

All calls/complaints from the public received via mail or via call to the RPD Front Desk are routed to the RPD IT HelpDesk and logged in our department's request management system. Any requests from 311 are received in our department's dispatch system and routed to the RPD IT HelpDesk which then is logged in the request management system.
Once the request is tracked in the request management system, IT will work with all relevant parties to ensure completion.

Review of open / closed requests occur with the CIO on a weekly basis.

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

Footage is retained on Exacqvision servers hosted on RPD's network.

Appendix A: Department Specific Responses
Department: War Memorial

1. A description of the product, including vendor and general location of technology.
   Product Description:
   Cameras: Mobotix S15D FlexMount Dual Camera
   Server: Rasilient ApplianceStor90
   Software: Avigilon Control Center Server v6.8.6.4.
   Vendor: N/A
   Location: War Memorial surveillance cameras are located in public areas of all floors in the Veterans Building. Additional cameras are planned for public interior and exterior areas of the Veterans Building.
2. The specific categories and titles of individuals who are authorized by the Department to access or use the collected information
   8207 - Building and Grounds Patrol Officers,
   8211 - Supervisor Building and Grounds Patrol Officer,
   0922 - Director of Security,
   1093 - IT Manager,
   1844 - Facilities Administrator
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.

   Complaints or concerns can be submitted to the Department by sending an email to WarMemorialinfo@sfgov.org.

   Department shall acknowledge and respond to complaints and concerns in a timely and organized response. To do so, Department shall monitor the War Memorial information email box throughout the day during standard business hours. Any communications to that email address are responded to directly or brought to the attention of responsible staff.
4. Specific details on where data will be stored (local, DT, SaaS, Cloud Storage) including name of vendor and retention period.
   Storage Locations:
   Local storage
   Department of Technology Data Center
   Vendor: None
   Retention Period: One (1) year at minimum.
5. Is a subpoena required before sharing with law enforcement?
   - No