Surveillance Impact Report

San Francisco Department of Child Support Services
Security Cameras

As required by San Francisco Administrative Code, Section 19B, departments must submit a Surveillance Impact Report for each surveillance technology to the Committee on Information Technology ("COIT") and the Board of Supervisors.

The Surveillance Impact Report details the benefits, costs, and potential impacts associated with the Department's use of surveillance cameras.

DESCRIPTION OF THE TECHNOLOGY

The San Francisco Department of Child Support Service's (SFDCSS or Department) mission is to empower parents to provide support for their children by furnishing child support services in the form of location of parents, establishment of parenting and support obligations and enforcement of support obligations, thereby contributing to the wellbeing of families and children.

In line with its mission, the Department uses Sonitrol Security System 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.

In line with its mission, the Department shall use security cameras only for the following authorized purposes:

Authorized Use(s):

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

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

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

Department technology may be deployed in the following locations, based on use case:

Points of entries, public lobby, and Intake/Interview areas.

Surveillance Oversight Review Dates

COIT Review: TBD
Board of Supervisors Review: TBD

Technology Details

The following is product description of Sonitrol Security System:

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

A. How It Works

To function, Sonitrol Security System monitors building access and safety using surveillance cameras at points of entries, public lobby, and Intake/Interview areas.

Data collected or processed by security cameras is not handled or stored by an outside provider or third-party vendor on an ongoing basis. The Department will remain the sole Custodian of Record.

IMPACT ASSESSMENT

The impact assessment addresses the conditions for surveillance technology approval, as outlined by the Standards of Approval in San Francisco Administrative Code, Section 19B:

1. The benefits of the surveillance technology outweigh the costs.
2. The Department's Policy safeguards civil liberties and civil rights.
3. The uses and deployments of the surveillance technology are not based upon discriminatory or viewpoint-based factors and do not have a disparate impact on any community or Protected Class.

The Department's use of the surveillance technology is intended to support and benefit the residents of San Francisco while minimizing and mitigating all costs and potential civil rights and liberties impacts of residents.

A. Benefits

The Department's use of security cameras has the following benefits for the residents of the City and County of San Francisco:

☐	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
- ☐ Other

B. Civil Rights Impacts and Safeguards

The Department has considered the potential impacts and has identified the technical, administrative, and physical protections as mitigating measures:

- Administrative Safeguards: Departmental access is restricted to SFDCSS IT, SFDCSS Executive Management, SFDCSS HR and Allied Security Guards. Upon request, SFDCSS IT will provide access to video footage to the above mentioned, as well as SFPD personnel. All staff and contractors are required to complete annual training, sign annual confidentiality forms and submit to Live Scan background checks to meet minimum employment requirements.

- 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.

C. Fiscal Analysis of Costs and Benefits

The Department's use of surveillance cameras yields the following business and operations benefits:

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 eliminating building or patrol officer supervision
X	Staff Safety	Security cameras help identify violations of Department Patron Code of Conduct 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.

The total fiscal cost, including initial purchase, personnel and other ongoing costs is Number of FTE (new & existing)	2 guards *40hr/week*52 weeks*$31.84hr	
Classification	N/A (Security guard contractor hired by HSA)	
	Annual Cost	***One-Time Cost***
Software	$0	
Hardware/Equipment	$7,290.42	
Professional Services	$4,872.24	
Training	$0	
Other	$0	
Total Cost	$144,662.66	
2.1 Please disclose any current or potential sources of funding (e.g. potential sources = prospective grant recipients, etc.). SIR, ASR		
The Department funds its use and maintenance of the surveillance technology by state and federal subvention and receives no county general fund dollars.		

The Department funds its use and maintenance of the surveillance technology through state and federal subvention and receives no county general fund dollars.

COMPARISON TO OTHER JURISDICTIONS

Sonitrol Security System are currently utilized by other governmental entities for similar purposes.

APPENDIX A: Surveillance Impact Report Requirements

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

1. Information describing the Surveillance Technology and how it works, including product descriptions from manufacturers.
Monitor building access and safety using surveillance cameras at points of entries, 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 & watch-in 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. Information on the proposed purpose(s) for the Surveillance Technology.
Sonitrol is used to protect against unauthorized access to confidential customer data, and customer and employee safety. Sonitrol monitors physical access to the facility where customer information resides to detect and respond to physical security incidents. Sonitrol is only used to review footage after a security incident and to watch and monitor surveillance cameras at points of entries, public lobby, and Intake/Interview areas during business hours. Sonitrol is used to prevent loss through theft and unauthorized access and to protect employee safety.
3. If applicable, the general location(s) it may be deployed and crime statistics for any location(s).
Points of entries, public lobby, and Intake/Interview areas.
4. An assessment identifying any potential impact on civil liberties and civil rights and discussing any plans to safeguard the rights of the public.
Administrative Safeguards: Departmental access is restricted to SFDCSS IT, SFDCSS Executive Management, SFDCSS HR and Allied Security Guards. Upon request, SFDCSS IT will provide access to video footage to the above mentioned, as well as SFPD personnel. All staff and contractors are required to complete annual training, sign annual confidentiality forms and submit to Live Scan background checks to meet minimum employment requirements. *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 CSS – 617 Mission Street or, in the event of a disaster, our secondary backup appliance is stored at 200 Paul. The data and data systems are secured during transmission and during rest in accordance with Federal, State and Local regulations.*

5. The fiscal costs for the Surveillance Technology, including initial purchase, personnel and other ongoing costs, and any current or potential sources of funding.

Number of FTE (new & existing)	2 Guards * 40hr/week * 52 weeks * $31.84/hr
Classification	N/A (Security guard contractor hired by HSA)
Software	$0
Hardware/Equipment	$7,290.42
Professional Services	$4,872.24
Training	$0
Other	$0
Total Cost [Auto-calculate]	$144,662.66

SFDCSS is completely funded by state and federal subvention and receives no county general fund dollars.

6. Whether use or maintenance of the technology will require data gathered by the technology to be handled or stored by a third-party vendor on an ongoing basis.

Yes, Sonitrol Security System provides maintenance of the system. Sonitrol has access to audio data, but not surveillance video data; either during or after a security event.

7. A summary of the experience, if any, other governmental entities have had with the proposed technology, including information about its effectiveness and any known adverse information about the technology such as anticipated costs, failures, or civil rights and civil liberties abuses.

[Populated response conditional on previous drop-down selection]