



Committee on Information Technology

Office of the City Administrator

San Francisco City Hall, 1 Dr. Carlton B. Goodlett Place, Suite 352

Minutes

Privacy and Surveillance Advisory Board Meeting City and County of San Francisco

Friday February 12, 2021

9:00 – 11:00 am

WebEx event

Members

Taraneh Moayed – Chair, Assistant Director, Office of Contract Administration

Blake Valenta – Analytics Strategist, DataSF, City Administrator's Office

Brian Roberts – Policy Analyst, Department of Technology

Mark de la Rosa – Acting Chief Auditor Executive, City Service Auditor, Controller's Office

Maria McKee - Director of Research & Planning, Juvenile Probation Department

Matthias Jaime – Director, Committee on Information Technology

Todd Rydstrom – Deputy Controller, Controller's Office

Guy Clarke – IT Governance Director, San Francisco International Airport

Nnena Ukuku – Public Member

1. Call to Order by Chair

COIT Director Matthias Jaime called the meeting to order at 9:02 am.

Mr. Jaime welcomed Guy Clarke, IT Governance Director at the San Francisco International Airport, to the committee.

2. Roll call

Blake Valenta

Brian Roberts

Mark de la Rosa

Maria McKee

Matthias Jaime

Todd Rydstrom

Guy Clarke

Nnena Ukuku

COIT Staff

Emma Fernandez

Department Representatives

Lisa Walton

Sean Cunningham

Sohail Warsi
Calen McEldowney
Dina Quesada
Teresa Scism
Natalie Toledo
John McClellan
Robert Eickwort
Vladimir Rudakov
Alexander Shoyket
Daniel Quach
Wayne Li
Roberto Lombardi
Maureen Singleton
Randle McClure
Tramaine Johnson
Asja Steeves
Mark Powell

Public Members

David Pilpel

3. Approval of Minutes from January 22, 2021 (Action Item)

The minutes from January 22, 2021 were approved unanimously.

4. Review and Approval of Surveillance Technology Policy: Security Camera (Action Item)

COIT Director Matthias Jaime discussed plans to work with departments to standardize the crime statistics information provided in Security Camera Surveillance Impact Reports.

Municipal Transportation Agency

Ms. Lisa Walton, Mr. Sean Cunningham, and Mr. Sohail Warsi presented the Municipal Transportation Agency's Security Camera Policy. The department created their own security camera policy based on the template provided by COIT.

- Differences between MTA policy and standard policy template
 - A new use case was added for enforcing parking and driving violations. MTA monitors video footage to cite vehicles.
 - An additional benefit to the technology was added. MTA uses footage for driving and safety training to show examples of incidents.
 - The data retention period was updated to reflect MTA's technical limitations.
- Location of the cameras
 - SFGO cameras are installed on signal poles and used for monitoring traffic. They may capture members of the public.
 - Facilities cameras are usually in a private MTA facility location.
 - Transit platforms and subway cameras are used to monitor for safety.
 - PARCS cameras are in parking garages and track cars coming in and out and any theft.

- Cameras in transit vehicles record inside and around the buses. There are at least 12 cameras on each bus, enabling a full safety review if there is an incident.
- Public noticing
 - There is signage on buses indicating that there is video and audio recording.
 - There is no public noticing on street poles for SFGO cameras.
- Crime statistics
 - There is a team responsible for pulling video and providing to SFPD. The department could request information about how often this is requested.
 - Could also look into the frequency of incidents on buses – cameras are used any time a vehicle operator pushes the emergency button.
- Process for sharing information with law enforcement
 - Law enforcement reaches out to the MTA security team using a pre-built form. All requests are logged. MTA reviews the footage internally to determine the appropriateness of sharing, and distributes to law enforcement if there is not a question. If there is, it is escalated within the agency and potentially to the City Attorney's office.

Committee members requested more information on the cost of retaining public records and responding to public records requests.

Committee members also noted that classification levels should be included for appropriate MTA roles.

Asian Art Museum

Mr. Calen McEldowney presented the Asian Art Museum's Security Camera Policy. The department adopted the standard security camera template and provided department-specific answers.

- Location of the cameras
 - Cameras are located throughout the museum protecting artwork, staff, and visitors, as well as outside the museum covering sidewalk areas.
- Public noticing
 - There is a notice that recording is occurring at the museum entry.
- Crime statistics
 - The museum maintains logs for all museum incidents. This does not separate out whether video footage was involved.
- Process for sharing information with law enforcement
 - The process is usually initiated by a law enforcement officer requesting video. The museum reviews video to see if there is any relevant information and then shares.

Airport

Ms. Dina Quesada and Ms. Teresa Scism presented the San Francisco International Airport's Security Camera Policy. The department adopted the standard security camera template and provided department-specific answers.

- Location of the cameras

- There are about 4,000 cameras located throughout the airport, in public, external, and secure areas.
- Public noticing
 - There is no current public noticing. The Airport plans to make a posting on flysfo.com.
- Crime statistics
 - SFPD maintains incident logs.
 - The Airport also uses a CAD system that tracks responses to incidents.
- Process for sharing information with law enforcement
 - They have access to video to review in real time.
 - Law enforcement needs to request the file if they want to share it. The Airport shares video from local servers or the cloud with a secure file transfer on a need to know basis.

Committee members requested more information on the cost of retaining public records and responding to public records requests.

Human Services Agency

Ms. Natalie Toledo, Mr. John McClellan, Mr. Robert Eickwort, Mr. Vladimir Rudakov, and Mr. Alexander Shoyket presented the Human Services Agency's Security Camera Policy. The department adopted the standard security camera template and provided department-specific answers.

- Differences from standard template
 - The department provided different use cases from the standard template, but will revise use cases before policy review by COIT.
- Location of the cameras
 - Cameras are located at department buildings throughout the city where client services are provided. Members of the public can be recorded at entrances and exits. The camera quality makes it hard to identify members of the public.
- Public noticing
 - The department does not currently have any public noticing.
- Crime statistics
 - On-site security records incidents on paper.
- Process for sharing information with law enforcement
 - It is rare that law enforcement is involved. It is more likely that the internal investigation unit is using the footage in an investigation that would eventually become part of a package shared with the District Attorney.

Department of Homelessness and Supportive Housing

Mr. Daniel Quach and Mr. Wayne Li presented the Department of Homelessness and Supportive Housing's Security Camera Policy. The department adopted the standard security camera template and provided department-specific answers.

- Location of the cameras
 - Cameras are located at shelters and at the headquarters building. They are generally in public spaces like lobbies, entrances, and exits.
- Public noticing

- The department posts signs that the area is being monitored.
- Crime statistics
 - There is an incident log shared with the facilities team, the IT team, and the shelter team.
- Process for sharing information with law enforcement
 - The facilities manager requires a subpoena from law enforcement. When they have that, they consult with the strategy and external affairs team, and if necessary, law enforcement.

The department will update the data sharing section of the policy to reflect the subpoena requirement.

San Francisco Public Library

Mr. Roberto Lombardi, Ms. Maureen Singleton, Mr. Randle McClure, and Mr. Tramaine Johnson presented the San Francisco Public Library's Security Camera Policy. The department created their own security camera policy based on the template provided by COIT.

- Differences between SFPL policy and standard policy template
 - The data retention period was updated to reflect SFPL's storage limitation of four months.
 - The policy reflects that SFPL requires a subpoena to release footage to law enforcement. The Library will work with internal partners, SFPD, DA, and Sheriff, to release video following an incident, but any other agencies would require a subpoena.
- Location of the cameras
 - There are 155 cameras, 81 of which are in the main library, and the rest located in branch libraries and historic archives (14 locations).
- Public noticing
 - The Library is currently developing signs that will have information on the technology, the location, and the use. These will be installed on the exterior and interior of buildings when the libraries re-open to the public.
- Crime statistics
 - The Library uses an internal software tracking system that allows library employees to record the time and date of any incident.

Committee members requested more information on the cost of retaining public records and responding to public records requests.

Department of Technology

Mr. Brian Roberts presented the Department of Technology's Security Camera Policy. The department adopted the standard security camera template and provided department-specific answers. This policy is specific to the cameras used at department facilities, mainly public safety radio sites. A different set of cameras are governed by Administrative Code Section 19A.

- Location of the cameras
 - Cameras are located at 8 public radio sites. The majority of sites are on rooftops, inaccessible to the public. The Twin Peaks site is at ground level, and people can walk by. There are also cameras at department headquarters. The only collection of video

of members of the public would be someone meeting with the department at headquarters.

- Process for sharing information with law enforcement
 - Footage is shared with law enforcement in cases of an incident like vandalism or theft.

The committee unanimously approved the Security Camera policies for the Asian Art Museum, the Department of Homelessness and Supportive Housing, the Department of Technology, and the San Francisco Public Airport for review at COIT, subject to the following amendments to the template policy (previously discussed).

Amendments to Security Camera template policy:

- Develop a standardized format for reporting crime statistics
- COIT will add information about procedures for sharing data with SFPD that departments shared during PSAB meetings to the appendix.

The Department of Homelessness and Supportive Housing policy was also subject to the following amendments (previously discussed).

Amendments to Department of Homelessness and Supportive Housing policy:

- Edit data sharing section to reflect subpoena requirement.

The San Francisco International Airport policy was also subject to the following amendments (previously discussed).

Amendments to San Francisco International Airport policy:

- Provide information on the cost of retaining public records and responding to public records requests.

The committee unanimously approved the Security Camera policy for the Municipal Transportation Agency for review at COIT, subject to the following amendments to the policy (previously discussed).

Amendments to Municipal Transportation Agency policy:

- Add job classification information to positions.
- Provide information on the cost of retaining public records and responding to public records requests.

The committee unanimously approved the Security Camera policy for the San Francisco Public Library for review at COIT, subject to the following amendments to the policy (previously discussed).

Amendments to San Francisco Public Library policy:

- Provide information on the cost of retaining public records and responding to public records requests.

The committee unanimously approved the Security Camera policy for the Human Services Agency for review at COIT, subject to the following amendments to the policy so that it can be considered with template policies (previously discussed).

Amendments to Human Services Agency policy:

- Revise use cases to align with standard policy template.

5. Review and Approval of Surveillance Technology Policy: DNA Sequencer (Action Item)

Ms. Asja Steeves and Mr. Mark Powell presented an overview of the MiSeq DNA Sequencer technology. The technology performs sequencing of DNA from evidence and reference samples used for comparison. The Crime Lab uses the technology to report on the percentage likelihood that the DNA collected at a crime scene matches a subject's DNA. SFPD needs a warrant to seek a DNA sample of a suspect. The Crime Lab can also run a DNA match against CODIS, Combined DNA Index System, a national database. The Crime Lab is accredited by an independent nonprofit and SFPD complies with a variety of federal and state laws on use of DNA evidence. The use of the MiSeq technology would be paid for by a grant from the Department of Justice and would not require any General Fund support.

SFPD proposes combining the two use cases detailed in the draft policy into one use case:

"Generate sequenced DNA profiles from evidence to search against databases or reference samples for the purpose of accurately and expeditiously identifying, apprehending, arresting, and convicting criminal offenders and exonerating persons wrongly suspected or accused of crime or to identify human remains."

Only SFPD criminalists and the Crime Lab manager have authorized access to the data. Data sharing is authorized only for law enforcement purposes. Data is retained indefinitely.

The committee unanimously approved the MiSeq DNA Sequencer policy for review at COIT, subject to the following amendments to the policy (previously discussed).

- Replace two permitted use cases with single combined permitted use case.
- Clarify that DNA information from excluded samples will not be share with CODIS.
- Add information on federal and state laws governing DNA evidence to the policy.

6. Public Comment

Mr. David Pilpel made public comment to express interest in PSAB discussing the Department of Animal Care and Control's proposed use of facial recognition technology.

7. Adjournment

The meeting adjourned at 10:47 am.