Surveillance Technology Policy

Audio Recorder - ShotSpotter, Inc. ("ShotSpotter")
San Francisco Police Department

The City and County of San Francisco values privacy and protection of San Francisco residents' civil rights and civil liberties. As required by San Francisco Administrative Code, Section 19B, the Surveillance Technology Policy aims to ensure the responsible use of ShotSpotter, Inc. ("ShotSpotter") itself as well as any associated data, and the protection of City and County of San Francisco residents' civil rights and liberties.

PURPOSE AND SCOPE

The Department's mission is: In order protect life and property, prevent crime and reduce the fear of crime, we will provide service with understanding, response with compassion, performance with integrity and law enforcement with vision.

The Surveillance Technology Policy ("Policy") defines the manner in which the ShotSpotter, Inc. ("ShotSpotter") will be used to support this mission, by describing the intended purpose, authorized and restricted uses, and requirements.

This Policy applies to all to department personnel that use, plan to use, or plan to secure ShotSpotter, Inc. ("ShotSpotter"), including employees, contractors, and volunteers. Employees, consultants, volunteers, and vendors while working on behalf of the City with the Department are required to comply with this Policy.

POLICY STATEMENT

The authorized use of ShotSpotter, Inc. ("ShotSpotter") technology for the Department is limited to the following use cases and is subject to the requirements listed in this Policy.

Authorized Use(s):

1. Gunshot detection: Record gunshot sounds and use sensors to locate the origin of the gunshots. Patrol Officers receive gunshot alerts to respond to crime scene.

2. Investigators use ShotSpotter Investigative Portal reports to find shell casing evidence on scene and to further analyze the incident.

All use cases not defined as an authorized use are prohibited.

A ShotSpotter alert will not, on its own, identify an individual, reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, information concerning an individual person's sex life or sexual orientation. Recordings of ambient noise, or any other sound outside of verified gunshots shall be prohibited for use in any investigation and shall not cause police enforcement.

BUSINESS JUSTIFICATION

ShotSpotter, Inc. ("ShotSpotter") supports the Department's mission and provides important operational value in the following ways:

The ShotSpotter system enables SFPD to be aware of gunshots in the absence of witnesses and/or reports to 911 of gunshots. The ShotSpotter system notifies SFPD of verified gunshot events, which expedites police and ambulance response rates to incidents involving illegal gunfire. ShotSpotter Alerts help SFPD locate victims, witnesses, evidence and suspects.

It shall be the policy of the SFPD to properly utilize ShotSpotter to enhance the Department's ability to respond to and investigate violent crimes involving illegal gunfire.

In addition, ShotSpotter, Inc. ("ShotSpotter") promises to benefit residents in the following ways:

☐	Education	
☐	Community Development	
☒	Health	Gun violence and its impacts are a public health concern. Preventing gun violence is an essential component to building health communities.
☐	Environment	
☒	Criminal Justice	ShotSpotter notifications help make the department aware of gunfire events they would have otherwise not have known about. In 2019, only 15% of SF gunfire incidents were called into 911. ShotSpotter alerts enable a fast, precise officer response to unreported gunfire to render aid to victims of a gunshot, secure critical evidence, and apprehend armed individuals.
☐	Jobs	
☐	Housing	
☐	Other	

ShotSpotter, Inc. ("ShotSpotter") will benefit the department in the following ways:

Benefit		Description
☐	Financial Savings	
☒	Time Savings	If a 911 caller reports a gunshot incident, it usually takes several minutes to capture and relay the information to officers often with imprecise data on the exact location. With ShotSpotter, officers receive alerts within 60 seconds of trigger pull with closest address data enabling a faster response to a crime scene to potentially save victims.

☒	Staff Safety	Officers can approach a crime scene more safely with ShotSpotter alerts knowing the precise location and time of the event and whether there are multiple shooters or high capacity weapons being used.
☒	Data Quality	Only 15% of gunshot incidents in SF have an accompanying 911 call (2019). Without ShotSpotter there would be no police response to 85% of gun crime representing over 850 incidents. However, with ShotSpotter, virtually all incidents are captured with an exact location enabling the department to better protect and serve the community.
☐	Other	

POLICY REQUIREMENTS

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

Specifications:	The software and/or firmware used to operate the surveillance technology must be kept up to date and maintained.
Safety:	Surveillance technology must be operated in a safe manner. Surveillance technology should not be operated in a way that infringes on resident civil rights, including privacy, or causes personal injury or property damage.
Data Collection:	Departments shall minimize the use, collection, and retention of Personally Identifiable Information (PII) to what is strictly necessary to accomplish the intended purpose of the surveillance technology. Department shall only collect data required to execute the authorized use case. All data collected by the surveillance technology, including PII, shall be classified according to the City's Data Classification Standard. Should information be incidentally collected that is not necessary to accomplish the intended purpose of the surveillance technology, including information that may be used to identify persons or private information, Department shall remove all incidental PII from raw data. Data types can take the form video, audio, still images. Data formats can take the form of XML, PDF, HTML, Plain Text, JPEG, etc.

The surveillance technology collects the following data types:

Data Type(s)	*Format(s)*	*Classification*
acoustic	.wav format	Level 3

Data Stored by ShotSpotter Related to Gunshot Incident

Data field	Explanation
○ **Audio Snippet**	Gunshot plus up to 1 second before and after to establish ambient noise level
○ **CAD ID**	Police Computer Aided Dispatch ID
○ **Trigger date/time**	
○ **Latitude**	Location data in relation to the gunshot incident: the angular distance of a place north or south of the earth's equator, usually expressed in degrees and minutes
○ **Longitude**	Location data in relation to the gunshot incident: the angular distance of a place east or west of the meridian at Greenwich, England, or west of the standard meridian of a celestial object, usually expressed in degrees and minutes.
○ **Incident Type/Classification**	Single Gunshot, Multiple Gunshot, Possible Gunshot
○ **Number of rounds**	# shots fired
○ **Dispatch address**	Reverse lookup of nearest street address from latitude/longitude using parcel data, Google
○ **City and state**	
○ **Area**	Beat/District
○ **Reviewer tags**	Manually entered data from a ShotSpotter incident reviewer for situational awareness such as multiple shooters, automatic weapon or high capacity weapon
○ **Report**	Investigative Lead Summary that details location and sequence of shots fired
○ **Comments**	Publishing time, acknowledgement from ShotSpotter Incident Review center; any modification to classification

Notification:	Publicly posted signage near the location of the technology is not feasible as the technology is not physically guarded and because of the intent of the technology to detect illegal gunfire the unguarded and unprotected technology is susceptible to vandalism and attempts to disable the intent of the technology.
Access:	All parties requesting access must adhere to the following rules and processes: Authorized personnel may access the browser-based ShotSpotter system via vehicle computers to only access the cloud-based system. SFPD members also have the option to activate ShotSpotter app on their Department issued mobile phones. Authorized personnel must always gain access through a login/password-protected system which records all login access. SFPD has no direct access to actual ShotSpotter sensors. Only ShotSpotter-specified support engineers can use a technology to access the data in the sensors prior to the 30-hour deletion period, if investigators need to search for previous gunshots. SFPD may request data within the first 24 hours, prior to the 30-hour deletion period. 1. Authorized personnel may access the ShotSpotter system via vehicle computers and receive notifications of verified ShotSpotter activations. SFPD may also notify authorized personnel of ShotSpotter activations. Authorized personnel may respond to such notifications based upon priorities as mandated by their supervisors. 2. The ShotSpotter system shall only be used for official law enforcement purposes. 3. Only specifically authorized personnel authorized by the Chief or Chief designee (e.g. personnel with SFPD's Investigations Division) will have access to historical ShotSpotter system data via desktop ShotSpotter system applications. The ShotSpotter system may be used for authorized patrol and investigation purposes. Contacting individuals at locations where ShotSpotter activations occur shall be conducted in accordance with applicable law and policy. 4. Accessing data collected by the ShotSpotter system requires a right to know and a need to know. A right to know is the legal authority to receive information pursuant to a court order, statutory law, or case law. A need to know is a compelling reason to request information such as direct involvement in an investigation or assignment to a unit which responds to gunshot calls (e.g. Patrol Division). 5. Members approved to access ShotSpotter system data may only use data for legitimate law enforcement purposes only, such as when the data relate to gunshots, a specific criminal investigation or department-related civil or administrative action.

6. All verified ShotSpotter system activations are entered into SFPD's computer-aided dispatch (CAD) record management system (RMS) with ShotSpotter system specific ID numbers. Authorized personnel can then query the CAD/RMS system for any and all ShotSpotter system activations.

A. Department employees

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

ShotSpotter Alerts, Application on Department Smart Phones
Employee Job Classification & Title: All sworn members (Police Officer Q-2 through Q-4; Inspector 0380; Sergeant Q-50 through Q-52; Lieutenant Q-60 through Q-62; Captain Q-80 through Q-82; Commander 0488, Deputy Chief 0400; Assistant Chief 0395; Chief of Police 0390)

ShotSpotter Investigator Portal
Employee Job Classification & Title: Sworn and Civilian staff designated by Chief of Police or Command Staff (Police Cadet 8274; Police Service Aide 9209; Police Service Aide Supervisor 8217; Police Officer Q-2 through Q-4; Inspector 0380; Sergeant Q-50 through Q-52; Lieutenant Q-60 through Q-62; Captain Q-80 through Q-82; Commander 0488, Deputy Chief 0400; Assistant Chief 0395; Chief of Police 0390; Crime Scene Investigator 8252; Forensic Latent Examiner 8253; Administrative Analyst 1822; Director of Crime Strategies 0933)

ShotSpotter Forensic Report
Employee Job Classification & Title: ShotSpotter will submit this report at the request of SFPD sworn members (Lieutenant Q-60 through Q-62; Captain Q-80 through Q-82; Commander 0488, Deputy Chief 0400; Assistant Chief 0395; Chief of Police 0390)

- The Department and ShotSpotter

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

- ShotSpotter

B. Members of the public

ShotSpotter data is classified as Level 3, Sensitive and public release is restricted, however each request submitted by a member of the public will be reviewed to determine whether the data can be released. SFPD shall comply with the requirements of the federal and State Constitutions, and federal and State civil procedure laws and rules.

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

The Department must have a subscription to ShotSpotter system and only has access to Reviewed Alerts delivered via the Investigator Portal password-protected internet portal and user interface supplied by ShotSpotter.

ShotSpotter has limited or eliminated audio access for several positions (including SST executives) whose access to audio was not essential. To address, deter and detect possible misuse, ShotSpotter requires supervisor approval before a ShotSpotter employee is permitted to download extended audio. For every instance in which a ShotSpotter employee accesses stored sensor audio, ShotSpotter requires its employees to document what audio was accessed, who accessed the audio, and who approved the download, the law enforcement officer making the request, and the evidentiary basis for the request. Supervisory personnel regularly review this audit trail to ensure that audio is being accessed only when necessary and according to proper procedures. These regular reviews assess which law enforcement agencies may be using the process at a much higher rate, ShotSpotter personnel who listen to a significantly longer duration of audio, or other patterns that may require corrective action.

ShotSpotter's privacy policy can be accessed here:
https://www.shotspotter.com/privacy-policy

Data Sharing:

SFPD will endeavor to ensure that other agencies or departments that may receive data collected by [the Surveillance Technology Policy that it operates] will act in conformity with this Surveillance Technology Policy.

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

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

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

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

- Confirm the purpose of the data sharing aligns with the department's mission.
- Consider alternative methods other than sharing data that can accomplish the same purpose.
- Redact names, scrub faces, and ensure all PII is removed in accordance with the department's data policies.

- Review of all existing safeguards to ensure shared data does not increase the risk of potential civil rights and liberties impacts on residents.
- Evaluation of what data can be permissibly shared with members of the public should a request be made in accordance with the San Francisco's Sunshine Ordinance.
- Ensure shared data will be done in a cost-efficient manner and exported in a clean, machine-readable format.

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

SFPD will comply with the California Public Records Act, the San Francisco Sunshine Ordinance, the requirements of the federal and State Constitutions, and federal and State civil procedure laws and rules.

The Department currently participates in the following sharing practices:

A. Internal Data Sharing

Department shares the following data with the recipients:

- San Francisco District Attorney's Office
- San Francisco Public Defender's Office

Data sharing occurs at the following frequency:

- Frequency depends on cases/incidents

B. External Data Sharing

Department shares the following data with the recipients:

- CGIC Partners
- US Attorney
- ShotSpotter data will only be shared with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law.

Data sharing occurs at the following frequency:

- As needed

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

- Direct the request to ShotSpotter. ShotSpotter may offer redacted data that complies with the Right to Know Law Request and/or Open Public Records Act/Freedom of Information Act, ShotSpotter and its confidential, proprietary

Data and records are protected under the exemptions expressly defined in the Public Records Act, Evidence Code and California Civil Code as follows:

ShotSpotter gunfire alert Data and records are a trade secret, and are exempt from disclosure pursuant to Evidence Code section 1060 which refers to subdivision (d) of Section 3426.1 of the California Civil Code for the definition of trade secret, as follows:

ShotSpotter keeps the gunfire alert Data and records confidential and secret by not releasing them to the public and by including Data restriction rights and confidentiality clauses in all customer agreements. Further, locations of specific sensors, gunshots at or near specific locations, and actual locations of areas covered is a matter of public safety and will not be released under any conditions. Additionally, the data is protected as some or all can be involved in on-going criminal investigations.

Data Retention:	Department may store and retain raw PII data only as long as necessary to accomplish a lawful and authorized purpose. Please list data retention schedules based on the following categories: • Permanent records (i.e., records that are essential): shall be retained and preserved indefinitely • Current records (i.e., records for operational necessity, ready reference, convenience): record retention schedules may vary but generally less than 10 years • Storage records (i.e., records retained offsite): record retentions may vary but generally less than 10 years • Criminal Investigative file retention schedule is subject to evidence laws, CA penal code and statute of limitations. The Department's data retention period and justification are as follows: • ShotSpotter: The sensors delete all acoustic data after 30 hours unless the gunshot-like impulsive acoustic event sends the data to ShotSpotter for analysis. Only verified gunshot data (all impulsive acoustic events loud enough to be heard by multiple sensors and where a location can be calculated) is maintained in perpetuity, both by ShotSpotter HQ as well as on SFPD desktop applications. ShotSpotter does not collect PII data and as such PII data shall not be kept in a form which permits identification of data subjects. ShotSpotter maintains verified gunshot data indefinitely.

- SFPD: Records shall be purged according to the current San Francisco Police Department Records Retention and Destruction Schedule which calls for destruction of intelligence files every two years from the last date of entry with the following exceptions:

    a) a. Information may be maintained if it is part of an ongoing investigation or prosecution.

    b) b. All written memoranda requesting authorization to commence an investigation and subsequent authorizations shall be maintained for not less than five years after termination of the investigation.

    c) c. Records showing violation of these guidelines shall not be destroyed or recollected for the purpose of avoiding disclosure.

    It shall be the policy of the SFPD that once the requisite retention period for a record has passed, the record shall be destroyed unless there are particular circumstances that dictate that the record be retained.

    It shall be the policy of the SFPD to work with contractors providing off-site storage of records to ensure that records are destroyed once the requisite time period for retention has passed

Data will be stored in the following location:

- ☐ Local storage
- ☐ Department of Technology Data Center
- X Software as a Service Product
- ☐ Cloud Storage Provider

Access to ShotSpotter Historical Incidents if Contract is Terminated:

SFPD has access to and the ability to download historical data at any time during the term of the Agreement using the Investigator Portal. Per the service contract with ShotSpotter, SFPD may not, without the prior written consent of ShotSpotter, merge, combine integrate or bundle the Software or the Data, in whole or in part, with other software, hardware, data, devices, systems, technologies, products, services, functions or capabilities. If/When the Department desires to terminate the ShotSpotter contract, SFPD may follow the process as set forth by ShotSpotter, to request exclusive rights the service area's historical data. The associated cost may require the Department to submit a request through the city and county's budget process.

This data shall be subject to the retention period as stated above.

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

Practices: Audio is only temporarily stored (30 hours), and then a very select amount of audio is retained only if the computer algorithm or human reviewer detects an impulsive acoustic event loud enough to be heard by multiple sensors and where a location can be calculated. All other audio is routinely purged from ShotSpotter's systems.

Processes and Applications: The ShotSpotter real-time Incident Review Center (IRC) will review at least 90% of all gunfire incidents within 60 seconds. This human review is intended to confirm or change the machine classification of the incident type, and, depending on the reviewer's confidence level that the incident is or may be gunfire, will result in an alert ("Reviewed Alert") sent to the Customer's dispatch center, patrol car mobile data terminals (MDT), and officer smartphones (via the ShotSpotter App), based on the following criteria: High confidence incident is gunfire; If uncertain an incident is gunfire, it is published as Probable Gunfire.

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. The ShotSpotter Gun Shot Detection Program Manager shall oversee the training program for any members with access to the ShotSpotter system and data.

CONSIDERATIONS FOR SERVICE AREA EXPANSION

The current service area was defined in part by a Violent Crime Reduction Strategy report prepared by SFPD's Crime Analysis Unit(CAU) in 2008. This report determined areas that experienced highest incidences of gun violence and identified five crime reduction zones. SFPD created a Zone Enforcement Strategy based on a study titled "Police Innovation and Crime Prevention: Lessons Learned from Police Research over the Past 20 Years" by Anthony A. Braga, Ph.D. and Davis L. Weisenburd Ph.D. The Zone Enforcement Strategy focused on deploying resources in identified zones to reduce or mitigate crime. ShotSpotter's service area which covers the areas identified in the study.

The Investigations Bureau along with the CAU will continue to review the weekly citywide shooting logs and the annual ShotSpotter report to determine whether there is a year over year increase, over a period of three years, in fatal and non-fatal shooting incidents in non-service areas. If there is a sustained increase in shootings in the non-service area, the Investigations Bureau will make a recommendation to the Chief of Police to consider expanding the ShotSpotter Service Area.

Community meetings will be held in the neighborhoods being considered for expansion. The neighborhood's District Captain, Captain's designees and the Commander of the Investigations Bureau will manage the community feedback sessions along with a ShotSpotter representative.

The community feedback will be provided to the Chief of Police before a decision is made to expand the ShotSpotter Service Area.

ANNUAL PUBLIC REPORTING

SFPD shall issue an annual gun violence report which will include ShotSpotter data. The first annual report will be issued on February 1, 2022 and will be issued on the 1st day of February every year, thereafter. The report will be posted on the SFPD public website, through San Francisco Open Data- DataSF and if requested, will be reported to the Police Commission on an annual basis.

The current SFPD Gun Violence Report lists the following data sets:

- Year-to-date gunfire numbers (four previous years and current YTD)
- Number of shooting victims (non-fatal)
- Number of Homicides with Firearm
- Total Number of Gun Violence Victims

The Annual ShotSpotter report may also include the following:

- Number of SFPD responses due to ShotSpotter alerts only
- Number of SFPD responses due to 911 calls only
- Number of SFPD responses due to ShotSpotter and 911 calls
- Total number of ShotSpotter incidents in coverage area
- Year-end gunfire event totals per District Station

COMPLIANCE

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

Surveillance Technology Policies shall have the same compliance requirements as all Department Written Directives and Police Commission Resolutions.

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

Deputy Chief of Investigations and the Commander of Investigations in addition, each member of the Department belongs to a chain of command. The Officer in Charge (OIC) of that chain of command is responsible for overseeing compliance with all SFPD written directives and the surveillance technology polices. If allegations arise that a member is not in compliance, the OIC will initiate an investigation and will take the appropriate action which could include an investigation of misconduct by Internal Affairs.

Sanctions for violations of this Policy include the following:

San Francisco Police Department will conduct an internal investigation though the Chief of Staff/Internal Affairs (IA) Unit. The results of the investigation will be reported to the Chief of Police, who will determine the penalty for instances of misconduct. Under San Francisco Charter section A8.343, the Chief may impose discipline of up to a 10-day suspension on allegations brought by the Internal Affairs Division or the DPA. Depending on the severity of the allegation of misconduct, the Chief or the DPA may elect to file charges with the Police Commission for

any penalty greater than the 10-day suspension. Any discipline sought must be consistent with principles of just cause and progressive discipline and in accordance with the SFPD Disciplinary Guidelines.

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.
Raw Data:	Information collected by a surveillance technology that has not been processed and cleaned of all personal identifiable information. The distribution and use of raw data is tightly restricted.
Exigent Circumstances	An emergency involving imminent danger of death or serious physical injury to any person that requires the immediate use of Surveillance Technology or the information it provides.
Trade Secret	"Trade secret" means information, including a formula, pattern, compilation, program, device, method, technique, or process, that: 1.) Derives independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use; and 2.) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

AUTHORIZATION

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

QUESTIONS & CONCERNS

Public:

Complaints of Officer Misconduct: Members of the public can register complaints about SFPD activities with the Department of Police Accountability (DPA). DPA, by Charter authority, receives and manages all citizen complaints relating to SFPD. DPA manages, acknowledges and responds to complaints from members of the public.

Concerns and Inquiries: Department shall acknowledge and respond to concerns in a timely manner. To do so, the Department has included a 19B Surveillance Technology Policy page on its public website : https://www.sanfranciscopolice.org/your-sfpd/policies/19b-surveillance-technology-policies. This page includes an email address for public inquiries: SFPDChief@sfgov.org. This email is assigned to several staff members in the Chief's Office who will respond to inquiries within 48 hours.

Allegations of 19B Violations: Members of the public may submit written notice of an alleged violation of Chapter 19B to SFPDChief@sfgov.org. If the Department takes corrective measures in response to such an allegation, the Department will post a notice within 30 days that generally describes the corrective measures taken to address such allegation. The Department will comply with allegation and misconduct processes as set forth by the City Charter.

City and County of San Francisco Employees:

All questions regarding this policy should be directed to the Chief of Police at SFPDChief@sfgov.org. Similarly, questions about other applicable laws governing the use of the surveillance technology or the issues related to privacy should be directed to the Chief of Police at SFPDChief@sfgov.org.

APPENDIX A: Surveillance Technology Policy Requirements

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

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

ShotSpotter manages the cloud-based service with a subscription service which provides the SFPD with access to the following:

- Gunshot Alerts
- Apps for Dispatch, Patrol Officers, Investigators, and District Station Personnel
- Incident Review Center
- Investigative Lead Summary
- Investigator Portal
- Detailed Forensic Report

ShotSpotter Inc. is a California-based company that operates ShotSpotter Flex, a proprietary technology that uses sensors strategically placed around a geographic area to detect, locate, and analyze gunshots, and notify law enforcement. ShotSpotter is the most widely used gunshot detection technology in the United States, currently operating in nearly 100 jurisdictions across the country.

ShotSpotter uses acoustic sensors that are strategically placed in an array of approximately 20 sensors per square mile. These sensors are connected wirelessly to ShotSpotter's centralized, cloud-based application to reliably detect and accurately triangulate (locate) gunshots. Each acoustic sensor captures the precise time and audio associated with impulsive sounds that may represent gunfire. This data, from multiple sensors, is used to locate the incident, which is then filtered by sophisticated machine algorithms to classify the event as a potential gunshot. Expertly trained acoustic analysts, who are located and staffed in ShotSpotter's 24x7 Incident Review Center, then further qualify those highlighted incidents. These analysts ensure and confirm that the events are in fact gunfire. In addition, the analysts can append the alert with other critical intelligence such as whether a full automatic weapon was fired and whether the shooter is on the move. There are three components to the ShotSpotter system:
1. Gunshot Location Detection (GLD) Sensors: Sensors are installed in different coverage areas in San Francisco.

2. ShotSpotter Headquarters (HQ): Sensors send acoustic information to HQ where computer-based machine-learning algorithms are used to analyze the sound. If the sound and visual audio signature match gunfire, the incident file is then passed along to the Incident Review Center (IRC). Acoustic experts at the IRC review incidents within seconds and provide additional information (e.g. number of gunshots, number of guns, types of guns). Confirmed gunshots are pushed out to Communications (dispatch) as well as to the SFPD ShotSpotter software system within seconds.

3. The SFPD ShotSpotter Software System: This system is cloud-based and desktop-based; SFPD authorized personnel can use internet browsers to connect to the ShotSpotter system via SFPD computers. Certain authorized personnel use desktop applications that connect to the ShotSpotter system for more in-depth gunshot analysis.

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

Technology Use:
The ShotSpotter system enables SFPD to be aware of gunshots in the absence of witnesses and/or reports to 911 of gunshots. The ShotSpotter system notifies SFPD of verified gunshot events, which expedites police and ambulance response rates to incidents involving illegal gunfire which will help locate victims, witnesses, evidence (casings, bullets, blood etc.,) and suspects.

PII:
false

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

Authorized Uses:

Gunshot detection: Record gunshot sounds and use sensors to locate the origin of the gunshots.

3.) Patrol Officers receive gunshot alerts to respond to crime scene.
4.) Investigators use ShotSpotter reports to find shell casing evidence on scene and to further analyze the incident .

Rules:
Prohibited Uses:
1. Unauthorized members using an authorized members log in to access historical ShotSpotter system data via desktop ShotSpotter system applications.

2. Using the ShotSpotter system for anything other than official law enforcement purposes.

3. Using ambient noise or any other sound outside of verified gunshots for use in any investigation.

4. Authorized members accessing data collected by the ShotSpotter system absent a right to know and a need to know. A right to know is the legal authority to receive information pursuant to a court order, statutory law, or case law. A need to know is a compelling reason to request information such as direct involvement in an investigation or assignment to a unit which responds to gunshot calls (e.g. Patrol Division).

5. Authorized members approved to access ShotSpotter system data using data for illegitimate purposes

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

Data Type	Formats STP
acoustic	.wav format Mp3

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

Employee Job Classification & Title: Individuals designated by the Chief or Chief-designee: Police Cadet 8274; Police Service Aide 9209; Police Service Aide Supervisor 8217; Police Officer Q-2 through Q-4; Inspector 0380;

Sergeant Q-50 through Q-52; Lieutenant Q-60 through Q-62; Captain Q-80 through Q-82; Commander 0488, Deputy Chief 0400; Assistant Chief 0395; Chief of Police 0390; Crime Scene Investigator 8252; Forensic Latent Examiner 8253; Administrative Analyst 1822; Director of Crime Strategies 0933

1. Authorized personnel may access the ShotSpotter system via vehicle computers and receive notifications of verified ShotSpotter activations. SFPD may also notify authorized personnel of ShotSpotter activations. Authorized personnel may respond to such notifications based upon priorities as mandated by their supervisors.

2. The ShotSpotter system shall only be used for official law enforcement purposes.

3. Only specifically authorized personnel authorized by the Chief or Chief designee (e.g. personnel with SFPD's Investigations Division) will have access to historical ShotSpotter system data via desktop ShotSpotter system applications. The ShotSpotter system may be used for authorized patrol and investigation purposes. Contacting individuals at locations where ShotSpotter activations occur shall be conducted in accordance with applicable law and policy.

4. Accessing data collected by the ShotSpotter system requires a right to know and a need to know. A right to know is the legal authority to receive information pursuant to a court order, statutory law, or case law. A need to know is a compelling reason to request information such as direct involvement in an investigation or assignment to a unit which responds to gunshot calls (e.g. Patrol Division).

5. Members approved to access ShotSpotter system data may only use data for legitimate law enforcement purposes only, such as when the data relate to gunshots, a specific criminal investigation or department-related civil or administrative action.

6. All verified ShotSpotter system activations are entered into computer-aided dispatch (CAD) record management system (RMS) with ShotSpotter system specific ID numbers. Authorized personnel can then query the CAD/RMS system for any and all ShotSpotter system activations.
Department:
SFPD and ShotSpotter
If applicable, contractor or vendor name:
ShotSpotter

Rules and processes required prior to data access or use:

The department must have a subscription to ShotSpotter system and only has access to Reviewed Alerts delivered via the Investigator Portal password-protected internet portal and user interface supplied by ShotSpotter.

ShotSpotter has limited or eliminated audio access for several positions (including SST executives) whose access to audio was not essential. To address, deter and detect possible misuse, ShotSpotter requires supervisor approval before a ShotSpotter employee is permitted to download extended audio. For every instance in which a ShotSpotter employee accesses stored sensor audio, ShotSpotter requires its employees to document what audio was accessed, who accessed the audio, and who approved the download, the law enforcement officer making the request, and the evidentiary basis for the request. Supervisory personnel regularly review this audit trail to ensure that audio is being accessed only when necessary and according to proper procedures. These regular reviews assess which law enforcement agencies may be using the process at a much higher rate, ShotSpotter personnel who listen to a significantly longer duration of audio, or other patterns that may require corrective action.
ShotSpotter's privacy policy can be accessed here: https://www.shotspotter.com/privacy-policy

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

Only authorized and trained personnel are permitted access to the system. The system always requires user and password ID for login. Furthermore, only personnel specifically designated by the Chief or Chief-designee have access to the system desktop applications which provide access to any historical downloadable data Authorized personnel may access the ShotSpotter system via vehicle computers and receive notifications of verified ShotSpotter activations. All verified ShotSpotter system activations are entered into SFPD's computer-aided dispatch (CAD) record management system (RMS) with ShotSpotter system specific ID numbers. Authorized personnel can then query the CAD/RMS system for any and all ShotSpotter system activations. The ShotSpotter verified activations entered into CAD/RMS require personnel to have level two CAD access which must adhere to the California Law Enforcement Telecommunications System (CLETS) guidelines.

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

Retention:
ShotSpotter: The sensors delete all acoustic data after 30 hours unless the gunshot-like impulsive acoustic event sends the data to ShotSpotter for analysis. All impulsive acoustic events loud enough to be heard by three or more sensors and where a location can be calculated are maintained in perpetuity, both by ShotSpotter HQ as well as on SFPD desktop applications.
SFPD: Records shall be purged according to the current San Francisco Police Department Records Retention and Destruction Schedule which calls for destruction of intelligence files every two years from the last date of entry with the following exceptions:
a. Information may be maintained if it is part of an ongoing investigation or prosecution.
b. All written memoranda requesting authorization to commence an investigation and subsequent authorizations shall be maintained for not less than five years after termination of the investigation.
c. Records showing violation of these guidelines shall not be destroyed or recollected for the purpose of avoiding disclosure.

Reason for retention:
ShotSpotter policy and SFPD retention schedule.
Deletion process:
It shall be the policy of the SFPD that once the requisite retention period for a record has passed, the record shall be destroyed unless there are particular circumstances that dictate that the record be retained. It shall be the policy of the SFPD work with contractors providing off-site storage of hardcopy records to ensure that records are destroyed once the requisite time period for retention has passed.

Retention exemption conditions:
ShotSpotter maintains all impulsive events loud enough to be heard by three or more sensors and where a location can be calculated indefinitely.

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

Will the data be accessible to the public:

Members of the public and media may submit a public information request to the Department, however, ShotSpotter keeps the gunfire alert data and records confidential and secret by not releasing them to the public and by including Data restriction rights and confidentiality clauses in all customer agreements. Further, locations of specific sensors, gunshots at or near specific locations, and actual locations of areas covered is a matter of public safety and will not be released under any conditions. Additionally, the data is protected as some or all can be involved in on-going criminal investigations.

Criminal defendants may request to access the ShotSpotter data per the rules of criminal procedure around discovery and inspection. Accessibility will be determined by the courts.

How it can be requested by members of the public: https://www.sanfranciscopolice.org/get-service/public-records-request

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

Name of agency: San Francisco District Attorney's Office, San Francisco Public Defender's Office, US Attorney, CGIC Partners, City Attorney. ShotSpotter data will only be shared with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law.
Justification: Law Enforcement purposes/on-going criminal investigations or prosecutorial process.

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

Training required:
true
Description of training:
The ShotSpotter Gun Shot Detection Program Manager shall oversee the training program for any members with access to the ShotSpotter system and data. Additionally, the Manager shall ensure all members with access have reviewed the Surveillance Technology Policy for ShotSpotter.

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

Process for responding to complaints from members of the public:
The Department of Police Accountability (DPA), by Charter authority, receives and manages all citizen complaints relating to the police department.
Complaints that come to the Department from members of the public will be forwarded to the DPA.
Oversight process:
Should a violation of ShotSpotter occur, San Francisco Police Department will conduct an internal investigation though the Chief of Staff/Internal Affairs (IA) Unit. The results of the investigation will be reported to the Chief of Police, who will consider in determining the charges for instances of misconduct. Under San Francisco Charter section A8.343, the Chief may impose discipline of up to a 10-day suspension on allegations brought by the Internal Affairs Division or the

DPA. Depending on the severity of the allegation of misconduct, the Chief or the DPA may elect to file charges with the Police Commission. Any discipline sought must be consistent with principles of just cause and progressive discipline.

Compliance personnel titles:
SFPD Investigations Commander and Deputy Chief, SFPD and ShotSpotter. In addition, each member of the Department belongs to a chain of command. The Officer in Charge (OIC) of that chain of command is responsible for overseeing compliance with all SFPD policies.

Restrictions:
1. Authorized personnel may access the ShotSpotter system SFPD may also notify authorized personnel of ShotSpotter activations. Authorized personnel may respond to such notifications based upon priorities as mandated by their supervisors.
2. The ShotSpotter system shall only be used for official law enforcement purposes.
3. Only specifically authorized personnel authorized by the Chief or Chief designee (e.g. personnel with SFPD's Investigations Division) will have access to historical ShotSpotter system data via desktop ShotSpotter system applications. The ShotSpotter system may be used for authorized patrol and investigation purposes. Contacting individuals at locations where ShotSpotter activations occur shall be conducted in accordance with applicable law and policy.
4. Accessing data collected by the ShotSpotter system requires a right to know and a need to know. A right to know is the legal authority to receive information pursuant to a court order, statutory law, or case law. A need to know is a compelling reason to request information such as direct involvement in an investigation or assignment to a unit which responds to gunshot calls (e.g. Patrol Division).
5. Members approved to access ShotSpotter system data may only use data for legitimate law enforcement purposes only, such as when the data relate to gunshots, a specific criminal investigation or department-related civil or administrative action.
6. All verified ShotSpotter system activations are entered into SFPD's computer-aided dispatch (CAD) record management system (RMS) with ShotSpotter system specific ID numbers. Authorized personnel can then query the CAD/RMS system for any and all ShotSpotter system activations.

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

Complaint procedures:
Complaints from members of the public will be forwarded to the Department of Police Accountability(DPA) for investigation. DPA manages complaint responses.
Departmental follow-up process:
DPA manages the complaint follow- up process. Surveillance Technology Policies will have the same procedural authority as any Departmental Written Directive. Non-compliance can result in progressive discipline or sustained complaints.
Members of the public can register complaints with the Department of Police Accountability https://sfgov.org/dpa/complaints. *Members of the public can register questions and concerns or submit questions via calls or emails at 311.org.*

Allegation procedures:

Members of the public may submit written notice of an alleged violation of Chapter 19B to SFPDChief@sfgov.org.

If the Department takes corrective measures in response to such an allegation, the Department will post a notice within 30 days that generally describes the corrective measures taken to address such allegation. The Department will comply with allegation and misconduct processes as set forth by the City Charter.

Surveillance Impact Report

Audio Recorder - ShotSpotter, Inc. ("ShotSpotter")
San Francisco Police Department

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 ShotSpotter, Inc. ("ShotSpotter").

DESCRIPTION OF THE TECHNOLOGY

The Department's mission is to protect life and property, prevent crime and reduce the fear of crime, by providing service with understanding, response with compassion, performance with integrity and law enforcement with vision.

In line with its mission, the Department uses ShotSpotter, Inc. ("ShotSpotter") which enables SFPD to be aware of gunshots in the absence of witnesses and/or reports to 911 of gunshots. The ShotSpotter system notifies SFPD of verified gunshot events, which expedites police and ambulance response rates to incidents involving illegal gunfire to help locate victims, witnesses, evidence (casings, bullets, firearms) and suspects.

It shall be the policy of the SFPD to properly utilize ShotSpotter to enhance the Department's ability to respond to and investigate violent crimes involving illegal gunfire.

SFPD shall use ShotSpotter, Inc. ("ShotSpotter") only for the following authorized purposes:

Authorized Use(s):

1. Gunshot detection: Record gunshot sounds and use sensors to locate the origin of the gunshots. Patrol Officers receive gunshot alerts to respond to crime scene.

2. Investigators use ShotSpotter Investigative Portal reports to find shell casing evidence on scene and to further analyze the incident.

All use cases not defined as an authorized use are prohibited.

A ShotSpotter alert will not, on its own, identify an individual, reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, information concerning an individual person's sex life or sexual orientation. Recordings of ambient noise, or any other sound outside of verified gunshots shall be prohibited for use in any investigation and shall not cause police enforcement.

TECHNOLOGY DETAILS

The following a is product description of ShotSpotter, Inc. ("ShotSpotter"):

ShotSpotter Inc. is a California-based company that operates ShotSpotter Flex, a proprietary technology that uses sensors strategically placed in a geographic coverage area to detect, locate, and analyze gunshots, and notify law enforcement. ShotSpotter places acoustic sensors high above the street, typically on buildings. The sensors connect over a private commercial cellular wireless communications network in real-time to the ShotSpotter hosted servers. After a loud, impulsive sound is captured and located by 3 or more ShotSpotter Sensors, an incident is created and a short snippet of audio is sent to the ShotSpotter Incident Review Center (IRC) via secure, high-speed network connections for real-time verification that it is a gunshot. ShotSpotter professional reviewers analyze the audio soundwave visually, and listen to the sound to confirm whether it is gunfire or non-gunfire (e.g. fireworks, car back fire, helicopter, construction etc.). If it is validated as a gunshot, an alert is published and sent directly to the Customer's dispatch center, PSAP, mobile/patrol officers, and any other relevant safety or security personnel, as determined by the Customer (SFPD). The process from trigger pull to published alert takes on average 34 seconds.

Investigative Lead Summary ("ILS"): ShotSpotter provides an on-demand report for investigators available through the ShotSpotter Respond Application. The Investigative Lead Summary (ILS) provides useful details about the approximate location, timing, and sequence of each shot fired during an incident (similar to a DFR below, but not a court-admissible document)

Detailed Forensic Report ("DFR"): ShotSpotter will provide a DFR for any ShotSpotter-detected incidents, including Reviewed Alerts. The DFR is intended to be a court-admissible document used by attorneys as part of a court case for the exact, verified timing, sequence and location of each shot fired.

How It Works:

ShotSpotter uses acoustic sensors that are strategically placed in an array of approximately 20-25 sensors per square mile. These sensors are connected wirelessly to ShotSpotter's centralized, cloud-based application to reliably detect and accurately triangulate (locate) gunshots. Each acoustic sensor captures the precise time and audio associated with impulsive sounds that may represent gunfire. This data, from multiple sensors, is used to locate the incident, which is then filtered by sophisticated machine algorithms to classify the event as a potential gunshot. Expertly trained acoustic analysts, who are located and staffed in ShotSpotter's 24x7 Incident Review Center, then further qualify those highlighted incidents. These analysts ensure and confirm that the events are in fact gunfire. In addition, the analysts can append the alert with other critical intelligence such as whether a fully-automatic weapon was fired or whether multiple shooters are involved. This process typically takes no more than 45 seconds from the time of the actual shooting to the digital alert (with the precise location identified as a dot on a map) popping onto a screen of a computer in the 911 Call Center or on a police officer's smartphone or mobile laptop. There are three components to the ShotSpotter system:

1. Gunshot Location Detection (GLD) Sensors: Sensors are installed in different coverage areas in San Francisco.

2. ShotSpotter Incident Review Center (IRC): Sensors send acoustic information to the cloud where computer-based machine-learning algorithms are used to analyze the sound. If the sound and visual audio signature match gunfire, the incident file is then passed along to the IRC. Acoustic experts at the IRC review incidents within seconds and provide additional information (e.g. multiple shooters, high caliber weapon, automatic weapon). Confirmed gunshots are pushed out to Communications (dispatch) as well as to the SFPD ShotSpotter software system within seconds.

3. ShotSpotter User Software: SFPD authorized personnel can receive ShotSpotter alerts and access historical gunshot incident details for more in-depth investigative analysis using desktop-based, web-based or mobile applications.

All data collected or processed by ShotSpotter, Inc. will be handled or stored by an outside provider or third-party vendor on an ongoing basis. Specifically, data will be handled by ShotSpotter to ensure the Department may continue to use the technology.

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:

A. The benefits of the surveillance technology outweigh the costs.

B. The Department's Policy safeguards civil liberties and civil rights.

C. 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 public safety of visitors and 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 ShotSpotter has the following benefits for the residents of the City and County of San Francisco:

☐	Education	
☐	Community Development	
X	Health	Quicker response and medical assistance for victims of gun violence which is believed to have more positive survival outcomes
☐	Environment	
X	Criminal Justice	ShotSpotter notifications help make the department aware of gunfire events they would have otherwise not have known about. In 2019, only 15% of SF gunfire incidents were called into 911. ShotSpotter alerts enable a fast, precise officer response to unreported gunfire to render aid to victims of a gunshot, secure critical evidence, and apprehend armed individuals.

- Jobs
- Housing
- Other

Additional benefits include:

The Crime Gun Intelligence Center (CGIC) program: CGICs are an interagency collaboration among local police departments, the U.S. Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), and other partners such as state and local prosecutors, to identify perpetrators of gun crime for immediate investigation, apprehension, and prosecution. The SFPD CGIC partnership reduces turnaround times for evidence analysis and improve SFPD's capabilities for connecting guns to crimes that may appear unrelated and more effectively identified guns used in multiple and cross jurisdictional shooting incidents. The Urban Institute has shown that ShotSpotter significantly improves the collection of evidence in the form of shell casings for gun crimes. These casings can be fed into the ATF's NIBIN database to connect gun crimes and identify potential suspects.

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:

ShotSpotter acoustic sensors use ordinary microphones that are similar to ones found in cellphones. They are placed high above the street and are not positioned, tuned or specialized to pick up human voices. The sensors "listen" for gunshot-like sounds and trigger only when detecting an impulsive sound that is instantaneous and sharp. When at least three different sensors detect a gunshot-like sound at the same time and determine a location, they send a short audio snippet to ShotSpotter headquarters that includes 1 second of sound prior to the incident (to establish a baseline of ambient noise), the incident itself and 1 second after. Upon detecting a likely gunshot, trained ShotSpotter personnel listen to a short computer-generated audio snippet of the gunfire to double check that it is actually gunfire. It is highly unusual for a human voice to be included in a snippet. For this to occur, the voice must be loud enough to be heard over the gunfire. In addition, there is no personally identifiable information in any audio snippet.

Since 2012, only authorized ShotSpotter employees have access to audio from sensors. They can only access it under a strict set of conditions and can only provide police a short audio snippet. In 2019 ShotSpotter commissioned an independent privacy audit by the Policing Project at NYU Law School. This end-to-end assessment conducted by objective privacy professionals concluded that ShotSpotter presents an "extremely low risk of audio surveillance". The Policing Project based this finding upon the short amount of audio that is temporarily stored on sensors, the short length of audio snippets that are permanently stored as evidence and the internal controls the company uses to restrict access to audio for authorized employees only.

Human voices and street noise will never trigger a sensor because they do not produce an instantaneous sharp sound and they are not loud enough to be picked up by three or more sensors. That being said, street noise that can include human voices could be captured by a sensor temporarily. All sensor audio, however, is permanently deleted after 30 hours and never

heard by a human unless it was accompanied by a loud, impulse sound thought to be a gunshot. Live streaming of audio is not possible.

Technology and operational mitigations:

• ShotSpotter, not SFPD, is responsible for determining the location(s) for installation of acoustic sensors. Sensors are placed high above the ground typically on top of buildings or sometimes lampposts. At this height, there is more limited ability to pick up street level sounds clearly.

• Determining locations: ShotSpotter works with police agencies using their historical crime data on shootings to determine the desired physical boundaries of the coverage area for the gunshot detection technology. Once the coverage area is set, trained ShotSpotter operations personnel, who are experienced with wide-area array sensor design, use an analytical process to determine how many sensors are needed and where they should be placed in order to achieve reliable detection throughout the area. Factors that go into final sensor location selection include:

- Desired sensor density based on the unique geographical, topographical, and ambient acoustic features of the coverage area
- Relative distance and spacing between other sensors
- Height of building or structure (to better "hear to the horizon" and thus minimize acoustic signal attenuation from far away gunfire)
- Availability of reliable power
- Adequate cellular coverage, signal strength and latency for communications
- Written permission from the property owner to install a sensor

• The sensors are not capable of audio streaming – neither ShotSpotter nor SFPD can listen in on street level sounds in real-time.

• The system permanently deletes all audio that is temporarily stored on the sensor after 30 hours.

• The system only triggers an incident to send downstream when 3 or more sensors hear a loud, impulsive sound. Sensors cannot be triggered by human voices because voices are not impulsive enough or loud enough to be heard by 3 sensors which may be 800 meters or more apart. Thus, the audio of a human voice that may be captured by 1 sensor would be permanently deleted after 30 hours and no police or ShotSpotter employee will have heard that sound.

• If a sound is loud enough and sharp enough to possibly be a gunshot and is detected by 3 or more sensors and a location is able to be determined, the system pulls a short audio snippet of the sound plus 1 second of ambient noise prior to the incident and 1 second after. This audio is interpreted by a machine at first and then reviewed by an acoustic analyst at ShotSpotter Headquarters who is only presented with the audio snippet and is under significant time pressure to process the incident as either a gunshot or to dismiss as a non-gunshot and get on to the next incident. All incidents, whether determined to be a gunshot or non-gunshot, are permanently and securely stored in the cloud to serve as both evidence and to train the machine classifier in the future.

• ShotSpotter security protocols also mitigate gunshot detection data access. ShotSpotter does not provide extended audio to SFPD or any police agency; they will not provide this access even if requested. Additionally, ShotSpotter does not provide actual precise locations of the sensors to SFPD.

• As previously mentioned, the sensors are constantly listening for gunshot-like sounds and storing what is captured for 30 hours (was 72 hours before July 2019), and then deleting the data unless triggered to send the data to the ShotSpotter Cloud for analysis. The 30-hour buffer allows SFPD to request data within 24 hours in cases where gunshots have been identified by police but not picked up by the system or if there is a need to verify if there were other gunshots prior to the authenticated event.

• ShotSpotter policy stipulates that only a limited number of authorized forensic engineers can access the storage buffer of a sensor to retrieve prior recorded data within that 30-hour window and search for other gunshot impulsive sound events. To avoid listening to recorded data on a sensor in a haphazard way, the search for a missing gunshot is first done visually through a secure interface looking for the prevalence of electrical "pulses" strong enough to be a gunshot that occurred around the time of the incident in question.

• Upon receiving a gunshot alert SFPD authorized personnel may find that a voice has been recorded along with gunshot sound, but such voice data is only associated with the actual gunshot data and has no personally identifiable information built in. There is no way to tag any voice audio that is unintentionally recorded when connected to a gunshot.

• SFPD takes data security seriously and safeguards GDT System data by both procedural and technological means. Only authorized and trained personnel are permitted access to the system. The system always requires user and password ID for login. Furthermore, only personnel specifically designated by the Chief or Chief-designee have access to the system desktop applications which provide access to any historical downloadable data.

• ShotSpotter data collected by SFPD shall not be used for the enforcement of Immigration Laws. SFPD complies with SF Admin Code Section 12H and 12I.

C. Fiscal Analysis of Costs and Benefits

The Department's use of ShotSpotter, Inc. yields the following business and operations benefits:

	Benefit	Description
☐	Financial savings	
X	Time savings	If a 911 caller reports a gunshot incident, it usually takes several minutes to capture and relay the information to officers often with imprecise data on the exact location. With ShotSpotter, officers receive alerts within 60 seconds of trigger pull with closest address data enabling a faster response to a crime scene to potentially save victims.

X	Staff safety	Officers can approach a crime scene more safely with ShotSpotter alerts knowing the precise location and time of the event and whether there are multiple shooters or high capacity weapons being used.
X	Improved data quality	Only 15% of gunshot incidents in SF have an accompanying 911 call (2019). Without ShotSpotter there would be no police response to 85% of gun crime representing over 850 incidents. However, with ShotSpotter, virtually all incidents are captured with an exact location enabling the department to better protect and serve the community.
☐	Other	

The total fiscal cost, including initial purchase, personnel and other ongoing costs is

FTE (new & existing)			-
Classification			-
	Annual Cost	***Years***	***One-Time Cost***
Total Salary & Fringe	$0	-	-
Software	$ 530,863 (w/ ~2% increase each year)	*5 years*-	-
Hardware/Equipment	$0	-	-
Professional Services	$		-
Training	$0	-	-
Other	$0	-	-
Total Cost [Auto-calculate]			2,755,491 over 5 years.
2.1 Please disclose any current or potential sources of funding (e.g. potential sources = prospective grant recipients, etc.). SIR, ASR			
SFPD operational budget			

The Department funds its use and maintenance of the surveillance technology through SFPD operational budget.

COMPARISON TO OTHER JURISDICTIONS

Sample results reported from other cities:

- Oakland, CA: ShotSpotter Policy approved by the Oakland Privacy Commission in November 2019.
- Las Vegas Metro Police pilot report indicates 342 gunshot incidents were identified by ShotSpotter in first 9 months of use that the PD would not have known about and a 26% reduction in violent crime. Expanded coverage area to all known hotspots.[1]
- Cincinnati cites a 48% reduction in shootings[2]
- Newport News reports a 13% reduction in shootings with ShotSpotter[3]
- Greenville, NC reports a 33% reduction in gun violence injuries using ShotSpotter[4]
- Chicago cites a drop of over 40% in shootings in the Englewood District in the first year after installation[5]
- Camden County, NJ–46% reduction in homicides by shooting[6]
- Denver–103 arrests and 84-gun recoveries over the course of 3 years[7]
- Bakersfield–22 arrests in first 9 months[8]
- Pittsburgh – 48 arrests and 83 victims found with help of ShotSpotter in 3 years[9]

[1] https://www.youtube.com/watch?v=bK8_oEjQ-gs&t=23s
[2] https://www.wcpo.com/news/crime/shootings-down-nearly-50-percent-in-cincinnati-this-year-police-say
[3] https://www.dailypress.com/news/crime/dp-nw-newport-news-police-2019-year-20200128-p6z2jetrkfd7ljhw6cvblfopxe-story.html
[4] https://www.witn.com/content/news/Greenville-Police-credit-Shot-Spotter-for-lower-crime-stats--567247521.html
[5] https://www.chicagotribune.com/news/breaking/ct-met-superintendent-eddie-johnson-chicago-violence-20171116-story.html
[6] https://www.phillymag.com/news/2015/04/02/camden-reduces-gunfire-by-48-percent/
[7] https://www.thedenverchannel.com/news/crime/denver-police-to-test-shotspotter-system-in-4-different-neighborhoods-with-live-gunfire
[8] https://bakersfieldnow.com/news/local/is-shotspotter-working-in-bakersfield
[9] https://www.post-gazette.com/local/city/2018/03/14/Pittsburgh-City-Council-ShotSpotter-expansion-Wendell-Hissrich-North-Side-Jason-Lando-Darlene-Harris-Deborah-Gross/stories/201803140183

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.

ShotSpotter uses acoustic sensors that are strategically placed in an array of approximately 20 sensors per square mile. These sensors are connected wirelessly to ShotSpotter's centralized, cloud-based application to reliably detect and accurately triangulate (locate) gunshots. Each acoustic sensor captures the precise time and audio associated with impulsive sounds that may represent gunfire. This data, from multiple sensors, is used to locate the incident, which is then filtered by sophisticated machine algorithms to classify the event as a potential gunshot. Expertly trained acoustic analysts, who are located and staffed in ShotSpotter's 24x7 Incident Review Center, then further qualify those highlighted incidents. These analysts ensure and confirm that the events are in fact gunfire. In addition, the analysts can append the alert with other critical intelligence such as whether a fully automatic weapon was fired and whether the shooter is on the move. This process typically takes no more than 45 seconds from the time of the actual shooting to the digital alert (with the precise location identified as a dot on a map) popping onto a screen of a computer in the 911 Call Center or on a police officer's smartphone or MDT (vehicle mobile display terminals) There are three components to the ShotSpotter system:
1. Gunshot Location Detection (GLD) Sensors: Sensors are installed in different coverage areas in San Francisco.
2. ShotSpotter Headquarters (HQ): Sensors send acoustic information to HQ where computer-based machine-learning algorithms are used to analyze the sound. If the sound and visual audio signature match gunfire, the incident file is then passed along to the Incident Review Center (IRC). Acoustic experts at the IRC review incidents within seconds and provide additional information (e.g. number of gunshots, number of guns, types of guns). Confirmed gunshots are pushed out to Communications (dispatch) as well as to the SFPD ShotSpotter software system within seconds.
3. The SFPD ShotSpotter Software System: This system is cloud-based and desktop-based; SFPD authorized personnel can use internet browsers to connect to the ShotSpotter system via SFPD computers. Certain authorized personnel use desktop applications that connect to the ShotSpotter system for more in-depth gunshot analysis.

ShotSpotter Inc. ("SST") is a California-based company that operates ShotSpotter Flex (hereafter referred to as "ShotSpotter"), a proprietary technology that uses sensors strategically placed around a geographic area to detect, locate, and analyze gunshots, and notify law enforcement. ShotSpotter is the most widely used gunshot detection technology in the United States, currently operating in more than 100 jurisdictions. SST's primary customers are local law enforcement agencies. ShotSpotter is gunshot detection technology that uses sophisticated acoustic sensors to detect, locate and alert law enforcement agencies and security personnel about illegal gunfire incidents in real-time. The digital alerts include a precise location on a map (latitude/longitude) with corresponding data such as the address, number of rounds fired, type of gunfire, etc. delivered to any browser-enabled smartphone or mobile laptop device as well as police vehicle MDC or desktop. This information is key to better protecting officers by providing them with increased tactical awareness. It also enables law enforcement agencies to better connect with their communities and bolsters their mission to protect and serve. The ShotSpotter system employs acoustic sensors strategically placed in specified areas (commonly referred to as a "coverage area.") When a gun is fired, the sensors detect the firing of the weapon. The audio triangulation of multiple installed sensors then pinpoints a gunfire location and sends the audio file and triangulation information to

ShotSpotter Headquarters (HQ) for gunshot verification. Verified gunshots and related information are then sent to SFPD in real-time so that SFPD may notify responding officers where guns were fired.

2. Information on the proposed purpose(s) for the Surveillance Technology.

The ShotSpotter system enables SFPD to be aware of gunshots in the absence of witnesses and/or reports of gunshots. The ShotSpotter system notifies SFPD of verified gunshot events, which allows SFPD to quickly respond to gunshots and related violent criminal activity. ShotSpotter expedites police and ambulance response rates to incidents involving illegal gunfire which expedite the location of victims, witnesses, evidence and suspects.

The Crime Gun Intelligence Center (CGIC) Unit conducts a re-canvass of ShotSpotter notifications when multiple gunshots are detected and cartridge cases are not recovered. Returning the following day to re-canvass the neighborhood may encourage witnesses to come forward and provide information as opposed to immediately following the shooting incident. The increased attention to the investigation of shots fired in the neighborhood may aid in building community trust.

3. If applicable, the general location(s) it may be deployed and crime statistics for any location(s).

Sensors are currently in the following neighborhoods: Bayview, Western Addition, Sunnydale/Visitation Valley, Bernal Dwellings/Bernal Heights, Potrero Hill and South of Market

4. An assessment identifying any potential impact on civil liberties and civil rights and discussing any plans to safeguard the rights of the public.

ShotSpotter acoustic sensors use ordinary microphones that are similar to ones found in cellphones. They are placed high above the street and are not positioned, tuned or specialized to pick up human voices. The sensors "listen" for gunshot-like sounds and trigger only when detecting an impulsive sound that is instantaneous and sharp. When at least three different sensors detect a gunshot-like sound at the same time and determine a location, they send a short audio snippet to ShotSpotter headquarters that includes 1 second of sound prior to the incident (to establish a baseline of ambient noise), the incident itself and 1 second after. Upon detecting a likely gunshot, trained ShotSpotter personnel listen to a short computer-generated audio snippet of the gunfire to double check that it is actually gunfire. It is highly unusual for a human voice to be included in a snippet. For this to occur, the voice must be loud enough to be heard over the gunfire. In addition, there is no personally identifiable information in any audio snippet.

Since 2012, only authorized ShotSpotter employees have access to audio from sensors, they can only access it under a strict set of conditions and can only provide police a short audio snippet.

In 2019 ShotSpotter commissioned an independent privacy audit by the Policing Project at NYU Law School. This end-to-end assessment conducted by objective privacy professionals concluded that ShotSpotter presents an "extremely low risk of audio surveillance". The Policing Project based this finding upon the short amount of audio that is temporarily stored on sensors, the short length of audio snippets that are permanently stored as evidence and the internal controls the company uses to restrict access to audio for authorized employees only.

Human voices and street noise will never trigger a sensor because they do not produce an instantaneous sharp sound and they are not loud enough to be picked up by three or more sensors. That being said, street noise that can include human voices could be captured by a sensor temporarily. All sensor audio, however, is permanently deleted after 30 hours and never heard by a human unless it was accompanied by a loud, impulse sound thought to be a gunshot. Live streaming of audio is not possible.

Technology and operational mitigations:

- ShotSpotter, not SFPD, is responsible for determining the location(s) for installation of acoustic sensors. Sensors are placed high above the ground typically on top of buildings or sometimes lampposts. At this height, there is more limited ability to pick up street level sounds clearly.
- The sensors are not capable of audio streaming – neither ShotSpotter nor SFPD can listen in on street level sounds in real-time.
- The system permanently deletes all audio that is temporarily stored on the sensor after 30 hours.
- The system only triggers an incident to send downstream when 3 or more sensors hear a loud, impulsive sound. Sensors cannot be triggered by human voices because voices are not impulsive enough or loud enough to be heard by 3 sensors which may be 800 meters or more apart. Thus, the audio of a human voice that may be captured by 1 sensor would be permanently deleted after 30 hours and no police or ShotSpotter employee will have heard that sound.
- If a sound is loud enough and sharp enough to possibly be a gunshot and is detected by 3 or more sensors and a location is able to be determined, the system pulls a short audio snippet of the sound plus 1 second of ambient noise prior to the incident and 1 second after. This audio is interpreted by a machine at first and then reviewed by an acoustic analyst at ShotSpotter Headquarters who is only presented with the audio snippet and is under significant time pressure to process the incident as either a gunshot or to dismiss as a non-gunshot and get on to the next incident. All incidents, whether determined to be a gunshot or non-gunshot, are permanently and securely stored in the cloud to serve as both evidence and to train the machine classifier in the future.
- ShotSpotter security protocols also mitigate gunshot detection data access. ShotSpotter does not provide extended audio to SFPD or any police agency; they will not provide this access even if requested. Additionally, ShotSpotter does not provide actual precise locations of the sensors to SFPD.
- As previously mentioned, the sensors are constantly listening for gunshot-like sounds and storing what is captured for 30 hours (was 72 hours before July 2019), and then deleting the data unless triggered to send the data to the ShotSpotter Cloud for analysis. The 30-hour buffer allows SFPD to request data within 24 hours in cases where gunshots have been identified by police but not picked up by the system or if there is a need to verify if there were other gunshots prior to the authenticated event.
- ShotSpotter policy stipulates that only a limited number of authorized forensic engineers can access the storage buffer of a sensor to retrieve prior recorded data within that 30-hour window and search for other gunshot impulsive sound events. To avoid listening to recorded data on a sensor in a haphazard way, the search for a missing gunshot is first done visually through a secure interface looking for the prevalence of electrical "pulses" strong enough to be a gunshot that occurred around the time of the incident in question.
- Upon receiving a gunshot alert SFPD authorized personnel may find that a voice has been recorded along with gunshot sound, but such voice data is only associated with the actual gunshot data and has no personally identifiable information built in. There is no way to tag any voice audio that is unintentionally recorded when connected to a gunshot.

5. 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.

Handled by third-party vendor, ongoing: true

Vendor name: ShotSpotter

Special data handling required: true

6. 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.

Sample results reported from other cities:

- Oakland, CA: ShotSpotter Policy approved by the Oakland Privacy Commission in November 2019.
- Las Vegas Metro Police pilot report indicates 342 gunshot incidents were identified by ShotSpotter in first 9 months of use that the PD would not have known about and a 26% reduction in violent crime. Expanded coverage area to all known hotspots.
- Cincinnati cites a 48% reduction in shootings
- Newport News reports a 13% reduction in shootings with ShotSpotter
- Greenville, NC reports a 33% reduction in gun violence injuries using ShotSpotter
- Chicago cites a drop of over 40% in shootings in the Englewood District in the first year after installation
- Camden County, NJ–46% reduction in homicides by shooting
- Denver–103 arrests and 84-gun recoveries over the course of 3 years
- Bakersfield–22 arrests in first 9 months
- Pittsburgh – 48 arrests and 83 victims found with help of ShotSpotter in 3 years

APPENDIX B: SFPD District Stations Included in ShotSpotter Service Area

Southern Station (Company B)
Bayview Station (Company C)
Mission Station (Company D)
Northern Station (Company E)
Ingleside Station (Company H)
Tenderloin Station (Company J)

APPENDIX C: Firearm Homicide by District Station, year over year 9/20/2020

District	2019	2020
Central	0	1
Southern	1	1
Bayview	7	7
Mission	3	4
Northern	3	0
Park	0	0
Richmond	0	0
Ingleside	1	4
Taraval	0	0
Tenderloin	2	5
Total	**17**	**22**

APPENDIX D: Violent Crime Zone Identification, 2008 Report

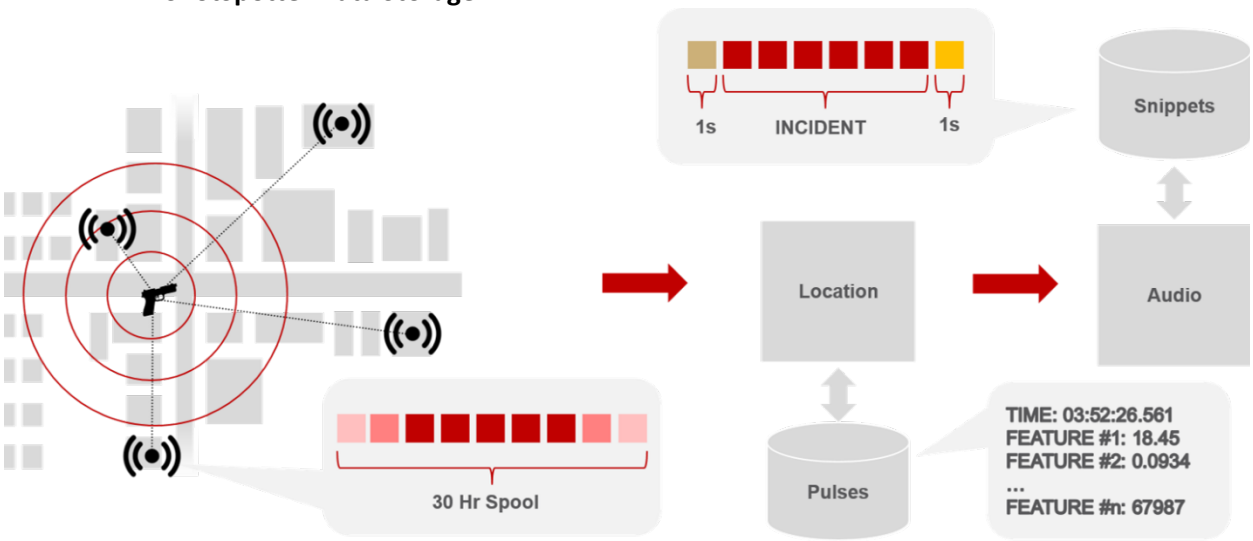
In 2008, SFPD's Crime Analysis Unit (CAU) identified five zones where the majority of violent crimes were taking place. The below five zones are included in the ShotSpotter Service Area.

- Zone 1: Tenderloin/SOMA
- Zone 2: Western Addition
- Zone 3: Mission District
- Zone 4: Bayview District
- Zone 5: Visitacion Valley

SFPD VIOLENT CRIME REDUCTION ZONES

Source: Violent Crime Reduction Strategy
Prepared by Crime Analysis Unit
08/20/2008

APPENDIX E: ShotSpotter Data Storage



APPENDIX F: ShotSpotter Real Time Operating Model