File No. 240330 **Committee Item No.** 6
Board Item No. 4

COMMITTEE/BOARD OF SUPERVISORS

AGENDA PACKET CONTENTS LIST

Committee: Rules Committee **Date** September 9, 2024

Board of Supervisors Meeting **Date** September 24, 2024

Cmte Board

Cmte	Board	
☐	☐	**Motion**
☐	☐	**Resolution**
X	☐	**Ordinance**
X	☐	**Legislative Digest**
☐	☐	**Budget and Legislative Analyst Report**
☐	☐	**Youth Commission Report**
☐	☐	**Introduction Form**
X	☐	**Department/Agency Cover Letter and/or Report**
☐	☐	**Memorandum of Understanding (MOU)**
☐	☐	**Grant Information Form**
☐	☐	**Grant Budget**
☐	☐	**Subcontract Budget**
☐	☐	**Contract/Agreement**
☐	☐	**Form 126 - Ethics Commission**
☐	☐	**Award Letter**
☐	☐	**Application**
☐	☐	**Form 700**
☐	☐	**Information/Vacancies (Boards/Commissions)**
☐	☐	**Public Correspondence**

OTHER **(Use back side if additional space is needed)**

X	☐	Impact Report
X	☐	Technology Policy
☐	☐	
☐	☐	
☐	☐	
☐	☐	
☐	☐	
☐	☐	
☐	☐	

Completed by: Victor Young **Date** Sept. 5, 2024
Completed by: _____ **Date** _____

[Administrative Code - Surveillance Technology Policy - Department of Emergency Management - Gunfire Detection]

Ordinance approving Surveillance Technology Policy for the Department of Emergency Management's use of ShotSpotter, a gunfire detection technology.

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

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

Section 1. Background.

(a) Terms used in this ordinance have the meaning set forth in Administrative Code Chapter 19B ("Chapter 19B").

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

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

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

Section 2. Surveillance Technology Policy Ordinance for the Department of Emergency Management's Use of Gunfire Detection Technology.

(a) Purpose. The Department of Emergency Management seeks Board authorization under Section 19B.2(a) to use the gunfire detection hardware, ShotSpotter, managed and operated by the City at specified locations, to respond to daily emergencies by reporting potential incidents involving gunfire. The Department of Emergency Management's dispatch center will receive notifications of gunshots through the ShotSpotter application and then Department of Emergency Management dispatchers will create calls for service for police

officers to respond to the location where the gunshot(s) were detected. Under the proposed Surveillance Technology Policy (the "Policy"), the Department of Emergency Management may use information collected from gunfire detection technology only for legally authorized purposes, and may not use that information to unlawfully discriminate against people based on race, ethnicity, political opinions, religious or philosophical beliefs, trade union membership, gender, gender identity, disability status, sexual orientation or activity, or genetic and/or biometric data.

(b) Surveillance Impact Report. The Department of Emergency Management submitted a Surveillance Impact Report to COIT for the department's use of ShotSpotter, a gunfire detection technology. A copy of the Surveillance Impact Report is in Board File No. 240330.

(c) Public Hearings and COIT Recommendation. On July 8, 2022, COIT's Privacy and Surveillance Advisory Board held a public hearing to consider the proposed Policy, and on September 15, 2022, COIT held a public hearing to consider and approve the proposed Policy, and voted to recommend the Policy to the Board for approval. A copy of the proposed Policy is in Board File No. 240330, and is incorporated herein by reference.

(d) Findings. The Board hereby finds that the stated benefits of the Department of Emergency Management's use of gunfire detection technology outweigh the costs and risks of use of such Surveillance Technology; that the Policy will safeguard civil liberties and civil rights; and that the uses and deployments of the gunfire detection technology, as set forth in the Policy, will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or a protected class.

Section 3. Approval of Policy.

The Board of Supervisors hereby approves the Department of Emergency Management's Surveillance Technology Policy for use of ShotSpotter, the gunfire detection technology, described in Section 2 of this ordinance and referenced in Section 2(c).

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

APPROVED AS TO FORM:
DAVID CHIU, City Attorney

By: /s/Christina Fletes-Romo
CHRISTINA FLETES-ROMO
Deputy City Attorney

n:\legana\as2024\2400332\01745986.docx

FILE NO. 240330

LEGISLATIVE DIGEST

[Administrative Code - Surveillance Technology Policy - Department of Emergency Management - Gunfire Detection]

Ordinance approving Surveillance Technology Policy for the Department of Emergency Management's use of ShotSpotter, a gunfire detection technology.

Background Information and Proposed Law

Administrative Code Chapter 19B establishes requirements that City departments must follow before they may use or acquire new surveillance technology. A City department must obtain Board of Supervisors approval by ordinance of a surveillance technology policy before: (1) seeking funds for surveillance technology; (2) acquiring or borrowing new surveillance technology; (3) using new or existing surveillance technology for a purpose, in a manner, or in a location not specified in a Board-approved surveillance technology policy; (4) entering into an agreement with a non-City entity to acquire, share, or otherwise use surveillance technology; or (5) entering into an oral or written agreement under which a non-City entity or individual regularly provides the department with data or information acquired through the entity's use of surveillance technology.

The proposed ordinance would approve a policy allowing the Department of Emergency Management ("DEM") to use the gunfire detection hardware, ShotSpotter, managed and operated by the San Francisco Police Department at specified locations, to respond to daily emergencies by reporting potential incidents involving gunfire. DEM's dispatch center will receive notifications of gunshots through the ShotSpotter application and then DEM dispatchers will create calls for service for police officers to respond to the location where the gunshot(s) were detected.

n:\legana\as2024\2400332\01746005.docx

Surveillance Impact Report

Gunshot Detection Hardware and Services
Emergency Management

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 gunshot detection hardware and services.

DESCRIPTION OF THE TECHNOLOGY

The Department's mission is the following:
The San Francisco Department of Emergency Management (DEM) leads the City in planning, preparedness, communication, response, and recovery for daily emergencies, large scale citywide events, and major disasters. DEM is the vital link in emergency communication between the public and first responders, and provides key coordination and leadership to City departments, stakeholders, residents, and visitors.

In line with its mission, the Department uses gunshot detection hardware and services to:

Gunshot detection hardware and services support the mission of our department to respond to daily emergencies by reporting potential incidents involving gunfire. Gunshot detection hardware and services notifications help make the department aware of gunfire events they would have otherwise not have known about.

The Department shall use gunshot detection hardware and services only for the following authorized purposes:

Authorized Use(s):

- Dispatch is notified of gunshots through the ShotSpotter application, and then creates a call for service for police officers to respond to the location.

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

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

Gunshot detection hardware and services technology may be deployed in the following locations, based on use case:

ShotSpotter detection sensors are installed in different coverage areas in San Francisco. Current coverage is within the areas of the following Police Districts:

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

ShotSpotter acoustic sensors are strategically placed in an array of approximately 20-25 sensors per square mile, typically on the tops of buildings or sometimes lampposts.

Technology Details

The following is a product description:

ShotSpotter uses an array of acoustic sensors that are connected wirelessly to ShotSpotter's centralized, cloud-based application to reliably detect and accurately locate gunshots using triangulation. Each acoustic sensor captures the precise time and audio associated with impulsive sounds that may represent gunfire. This data is used to locate the incident and is then filtered by sophisticated machine algorithms to classify the event as a potential gunshot. Acoustic experts, who are located and staffed in's 24×7 Incident Review Center, ensure and confirm that the events are indeed gunfire. They can append the alert with other critical intelligence such as whether a fully automatic weapon was fired or whether there are multiple shooters. This entire process takes less than 60 seconds from the time of the shooting to the digital alert popping onto a screen of a computer in the 911 Call Center or on a patrol officer's smartphone or mobile laptop.

A. How It Works

To function, 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 (DEM Dispatch) as well as to the SFPD ShotSpotter software system within seconds.
3. ShotSpotter Response Software: This software allows certain authorized personnel (SFPD) to use a desktop application that connects to the ShotSpotter system for more in-depth gunshot analysis.

All data collected or processed by Gunshot Detection Hardware and Services will be handled or stored by an outside provider or third-party vendor on an ongoing basis. Specifically, data will be handled by ShotSpotter, Inc. 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:

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

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

A. Benefits

The Department's use of gunshot detection hardware and services has the following benefits for the residents of the City and County of San Francisco:

	Benefit	Description
☐	Education	
☐	Community Development	
X	Health	Gun violence and its impacts are a Public Health concern. Preventing gun violence is an essential component to building healthy communities.
☐	Environment	
X	Criminal Justice	Gunshot detection hardware and services notifications help make the department aware of gunfire events they would have

		otherwise not have known about which is in the interest of Public Safety. In 2019, only 15% of SF gunfire incidents were called into 911.
☐	Jobs	
☐	Housing	
X	Public Safety	Gunshot detection hardware and services alerts enable a fast, precise officer response to unreported gunfire to render Medical aid to victims of a gunshot, secure critical evidence, and apprehend armed individuals which is in the interest of Criminal Justice.
☐	Other	

B. Civil Rights Impacts and Safeguards

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

The department has examined the use of gunshot detection hardware and services in the following potential categories that may impact civil liberties and civil rights. DEM's intent is to safeguard the rights of the public.

- Dignity Loss - No identifiable issues as gunshot detection hardware and services does not contain personally identifiable information.
- Discrimination - No identifiable issues as gunshot detection hardware and services does not identify an individual or reveal any of the following: 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
- Economic Loss - No identifiable issues as gunshot detection hardware and services does not contain personally identifiable information so it cannot lead to identity theft.
- Loss of Autonomy - No identifiable issues as gunshot detection hardware and services does not contain personally identifiable information that could be used or processed by others.
- Loss of Liberty - Gunshot detection hardware and services identifies the location of gunfire, if multiple shooters appear to be involved, and high capacity weapons. Responding police officers may then locate a possible gunfire suspect at the scene or nearby area, potentially leading to detention or arrest based on the responding law enforcement's policies and procedures.
- Physical Harm - No identifiable issues as gunshot detection hardware and services does not cause physical harm or death. In fact, it can help send police officers to render aid at shootings if no witnesses have called 911.
- Loss of Trust - Great care has been taken by SFPD and ShotSpotter (vendor) to ensure the public's trust in gunshot detection hardware and services. Safeguards have been built in, such as audio sensors that only trigger a human review if 3 or more sensors detect a loud, impulsive

sound. Then machine learning or a trained acoustic analyst at Shotspotter (vendor) reviews the audio and makes a determination whether there is possible gunfire. (This screens out cars backfiring, construction noise, fireworks, helicopter, etc.) Then an alert is sent to the Dispatch Center and to SFPD Officers with access to the application. The audio sensors cannot stream live audio and are mounted high above the streets. The audio snippet is restricted to only 1 second before until 1 second after the gunfire. The audio data is purged after 30 hours unless it is identified as gunfire; ShotSpotter security protocols also mitigate gunshot detection data access. ShotSpotter does not provide extended audio to the department; they will not provide this access even if requested. Additionally, ShotSpotter does not provide actual precise locations of the sensors to SFPD or the department.

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.

The administrative safeguards are as follows: Department General Order 6.3 states:"

- Need to Know/Right to Know: The "need to know" and the "right to know" shall exist before any database inquiry is made. If any employee suspects that any request for information from the automated systems does not fit the criteria, even if the requestor is another Department employee, they shall not release the information and shall notify supervisory personnel immediately. Members shall not release confidential from database files to authorized recipients over the telephone unless the member is certain of the identity of the authorized recipients." All gunshot detection hardware and services incidents are logged in CAD and all Operations staff are trained in gunshot detection hardware and services use. Violations of policy are handled through standard retraining and discipline procedures."

The technical safeguards are as follows: For DEM, the data can only be accessed on an application that is password protected.

The physical safeguards are as follows: Access to the building and room that has the ShotSpotter clients installed is only available through keycard access. The building also has video surveillance on the outside perimeter, along with Sheriff deputies guarding the building.

C. Fiscal Analysis of Costs and Benefits

The Department's use of gunshot detection hardware and services yields the following business and operations benefits:

Benefit	Description
Financial Savings	

X	Time Savings	The technology saves time by notifying dispatch of gunshot activations faster than processing a 911 call. This technology is much faster and more accurate with determining the location than witnesses who call 911.
	Staff Safety	
X	Data Quality	The technology improves data quality by providing a calculated location for the gunshots, how many gunshots were detected, whether there were multiple guns involved, and the possibility of a high caliber weapon. Most witnesses are unable to provide this level of detail when calling 911.
	Other	

The fiscal cost, such as initial purchase, personnel and other ongoing costs, include:

Number of FTE (new & existing)	Less than 0.3 FTE per year, comprised of all (8239-8240) Public Safety Communications Supervisors and Coordinators that view activations and (1091-1095) I.T. Operations Support Admin personnel that support trouble-shooting. DEM's role is generally limited to responding to activations and checking that the software is online.	
Classification	- *(8239-8240) Public Safety Communications Supervisors and Coordinators that view activations* - *(1091-1095) I.T. Operations Support Admin personnel*	
	Annual Cost	***One-Time Cost***
Total Salary & Fringe	*Approximately $30,000 per year in salary costs to support ShotSpotter at DEM.*	*Approximately $5,160 in salary costs to train department staff on ShotSpotter.*
Software	*DEM is not responsible for ShotSpotter costs. Please refer to the SFPD policy for ShotSpotter costs.*	*DEM is not responsible for ShotSpotter costs. Please refer to the SFPD policy for ShotSpotter costs.*

Hardware/Equipment	*DEM is not responsible for ShotSpotter costs. Please refer to the SFPD policy for ShotSpotter costs.*	*DEM is not responsible for ShotSpotter costs. Please refer to the SFPD policy for ShotSpotter costs.*
Professional Services	*DEM is not responsible for ShotSpotter costs. Please refer to the SFPD policy for ShotSpotter costs.*	*DEM is not responsible for ShotSpotter costs. Please refer to the SFPD policy for ShotSpotter costs.*
Training	*DEM is not responsible for ShotSpotter costs. Please refer to the SFPD policy for ShotSpotter costs.*	*All dispatchers are trained on how ShotSpotter works, and all supervisors are provided additional training on how to use the client to access, read, and enter incidents. Cost to train a dispatcher is approximately a $30.00 one-time cost, and approximately a $40 one-time cost to train a supervisor based on their average hourly salaries.*
Other	*DEM is not responsible for ShotSpotter costs. Please refer to the SFPD policy for ShotSpotter costs.*	*N/A*
Total Cost	***$30,000.00***	***$5,160***

The Department does not fund the use of ShotSpotter. SFPD owns the contract and pays for the service. Funding for training of DEM staff comes from the DEM budget which comes from the General Fund.

COMPARISON TO OTHER JURISDICTIONS

Gunshot detection hardware and services are currently utilized by other governmental entities for similar purposes.

Surveillance Technology Policy

Gunshot Detection Hardware and Services
Emergency Management

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 gunshot detection hardware and services 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 the following:

The San Francisco Department of Emergency Management (DEM) leads the City in planning, preparedness, communication, response, and recovery for daily emergencies, large scale citywide events, and major disasters. DEM is the vital link in emergency communication between the public and first responders, and provides key coordination and leadership to City departments, stakeholders, residents, and visitors.

The Surveillance Technology Policy ("Policy") defines the manner in which the gunshot detection hardware and services 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 gunshot detection hardware and services, 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 gunshot detection hardware and services technology for the Department is limited to the following use cases and is subject to the requirements listed in this Policy.

Authorized Use(s):

- *Dispatch is notified of gunshots through the ShotSpotter application, and then creates a call for service for police officers to respond to the location.*

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

Departments may use information collected from technology only for legally authorized purposes, and may not use that information to unlawfully discriminate against people based on race, ethnicity, political opinions, religious or philosophical beliefs, trade union membership, gender, gender identity, disability status, sexual orientation or activity, or genetic and/or biometric data. Additionally,

departments may not use automated systems to scan footage and identify individuals based on any of the categories listed in the preceding sentence.

BUSINESS JUSTIFICATION

Gunshot detection hardware and services support the Department's mission and provides important operational value in the following ways:

Gunshot detection hardware and services support the mission of our department to respond to daily emergencies by reporting potential incidents involving gunfire. Gunshot detection hardware and services notifications help make the department aware of gunfire events they would have otherwise not have known about.

In addition, gunshot detection hardware and services promises to benefit residents in the following ways:

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

Gunshot detection hardware and services will benefit the department in the following ways:

Benefit	Description
Financial Savings	

X	Time Savings	The technology saves time by notifying dispatch of gunshot activations faster than processing a 911 call. This technology is much faster and more accurate with determining the location than witnesses who call 911.
	Staff Safety	
X	Data Quality	The technology improves data quality by providing a calculated location for the gunshots, how many gunshots were detected, whether there were multiple guns involved, and the possibility of a high caliber weapon. Most witnesses are unable to provide this level of detail when calling 911.
	Other	

To achieve its intended purpose, ShotSpotter, Inc. (hereinafter referred to as "surveillance technology") 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 (DEM Dispatch) as well as to the San Francisco Police Department ShotSpotter software system within seconds.

3. ShotSpotter Response Software: This software allows certain authorized personnel (SFPD) to use a desktop application that connects to the ShotSpotter system for more in-depth gunshot analysis.

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 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: Department shall only collect data required to execute the authorized use case. All data collected by the surveillance technology, including PII, shall be classified according to the City's Data Classification Standard.

The surveillance technology collects the following data types:

Data Type(s)	*Format(s)*	*Classification*
Audio - Very short audio snippets of the gunshot(s) are gathered by ShotSpotter. From 1 second before until 1 second after the gunshot(s)	.wav	Level 3
Location – The location of the gunshot is triangulated using data gathered by ShotSpotter.	XYZ Coordinates	Level 3

Access: All parties requesting access must adhere to the following rules and processes (please

refer to the data sharing section to ensure all information covered in that section is also included below):

- Only authorized and trained personnel may access the ShotSpotter application via department computers.

Data must always be scrubbed of PII as stated above prior to public use.

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:

- Public Safety Supervisors and Coordinators (8239-8240) - Supervisors view the data once an activation is triggered, and then enter the data into CAD as an incident.
- Public Safety Dispatchers (8238) - Dispatchers can see the ShotSpotter data once it is entered into CAD and then broadcast the incident to responding officers.

B. Members of the public, including criminal defendants

The Department of Emergency Management 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.

Collected data that is classified as Level 1-Public data may be made available for public access or release via DataSF's Open Data portal. Anyone, including criminal defendants, may access such data. Open Data has a Public Domain Dedication and License, and makes no warranties on the information provided. Once public on Open Data, data can be freely shared, modified, and used for any purpose without any restrictions. Any damages resulting from use of public data are disclaimed, including by criminal defendants.

Members of the public, including criminal defendants, may also request access by submission of a request pursuant to San Francisco's Sunshine Ordinance. No record shall be withheld from disclosure in its entirety unless all information contained in it is exempt from disclosure under express provisions of the California Public Records Act or some other statute.

Data Security: Department shall secure PII against unauthorized or unlawful processing or disclosure; unwarranted access, manipulation or misuse; and accidental loss, destruction, or damage. Surveillance technology data collected and retained by the Department shall be protected by the safeguards appropriate for its classification level(s).

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

Access to the data for DEM personnel is limited to four Supervisor workstations on the dispatch floor, which is also kept secure and access is restricted through logged keycards. The software is also always kept up to date, and requires personnel to login to view the data.

Data Sharing: The Department of Emergency Management will endeavor to ensure that other agencies or departments that may receive data collected by the gunshot detection hardware and services Policy will act in conformity with this 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.

The Department of Emergency Management 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)

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

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

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

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

- X Confirm the purpose of the data sharing aligns with the department's mission.
- X Consider alternative methods other than sharing data that can accomplish the same purpose.
- X Redact names, scrub faces, and ensure all PII is removed in accordance with the department's data policies.
- X Review of all existing safeguards to ensure shared data does not increase the risk of potential civil rights and liberties impacts on residents.

X Evaluation of what data can be permissibly shared with members of the public should a request be made in accordance with the San Francisco's Sunshine Ordinance.

X Ensure data will be shared in a cost-efficient manner and exported in a clean, machine-readable format.

The Department of Emergency Management 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:

Type	Recipient
The location of the gunshots, as well as how many gunshots were detected. If multiple shooters or a high capacity weapons is indicated by ShotSpotter then that is disclosed as well.	San Francisco Police Department

Data sharing occurs at the following frequency:

Data is shared whenever there is a notification that gunshots were detected. This can occur daily. In addition, the SFPD maintains their own direct access to ShotSpotter..

B. External Data Sharing

Department shares the following data with the recipients:

Type	Recipient
The location of the gunshots, as well as how many gunshots were detected. If multiple shooters or a high capacity weapons is indicated by ShotSpotter then that is disclosed as well.	Other law enforcement agencies operating within San Francisco.

Data sharing occurs at the following frequency:

As-needed if an activation is within their jurisdiction. .

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

DEM has strict controls for access to gunshot detection hardware and services, as mentioned in other sections, is only accessed by authorized and trained DEM personnel. The data is only transmitted to the San Francisco Police Department or relevant law enforcement agency. SFPD has separately submitted their own Surveillance Technology Policy covering gunshot detection hardware and services.

Before data sharing with any recipient, 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.
- Ensure shared data will be done in a cost-efficient manner and exported in a clean, machine-readable format.
- Refer data request to the San Francisco Police Department as they are responsible for ShotSpotter.
- Review all existing safeguards to ensure shared data does not increase the risk of potential civil rights and liberties impacts on residents.

Data Retention: Department may store and retain raw PII data only as long as necessary to accomplish a lawful and authorized purpose.

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

Retention Period	**Retention Justification**
Data from ShotSpotter is the responsibility of the San Francisco Police Department as they have contracted for the service. DEM does NOT maintain the ShotSpotter data, and instead merely accesses it on behalf of the Police Department in order to dispatch police officers to reports of gunshots. Individual incident data is accessible at DEM for up to one week. ShotSpotter (vendor) maintains the data themselves (it is not stored within DEM). ShotSpotter audio sensory data is permanently deleted after 30 hours unless it was accompanied by a loud, impulse sound thought to be a gunshot, in which case it may be saved for investigative purposes by SFPD. Permanent Records: N/A. Refer to	DEM does not define the retention period and merely has access to the ShotSpotter data for the time period granted by the San Francisco Police Department and ShotSpotter, Inc. (vendor). DEM can only view gunshots that were detected within the previous week. SFPD and ShotSpotter have set the audio retention period at 30 hours so that they can recover incidents during the prior 24 hours. For instance, to check to see if there was additional gunfire prior to an incident or a missed incident.

SFPD. Current Records: Detected gunshots within the previous week are visible in the application. Storage Records: N/A. Refer to SFPD.	

PII data shall not be kept in a form which permits identification of data subjects for any longer than is necessary for the purposes for which the personal data are processed.

Departments must establish appropriate safeguards for PII data stored for longer periods.

Data will be stored in the following location:

☐ Local storage (e.g., local server, storage area network (SAN), network attached storage (NAS), backup tapes, etc.)

☐ Department of Technology Data Center

X Software as a Service Product

☐ Cloud Storage Provider

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

Practices:

- The Department does not store the data on-site, and only accesses the data through a ShotSpotter client application. The data is no longer accessible by the department once the seven-day period passes for each individual incident. Disposal of data is not handled by the department. See SFPD policy for further on data disposal.

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.

At the very least, department shall require all elected officials, employees, consultants, volunteers, and vendors working with the technology on its behalf to read and formally acknowledge all authorized and prohibited uses. Department shall also require that all individuals requesting data or regularly requiring data access receive appropriate training before being granted access to systems containing PII.

All new dispatchers are trained on how the technology works so they can use the data as needed in their interactions with SFPD. Supervisors are also trained on how

to access the application installed on the supervisor computers to look at gunshot detection activation data and then enter that incident into the computer aided dispatch system.

COMPLIANCE

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

The use of gunshot detection hardware and services has the same compliance requirement as all other department directives. Data is only accessed under a need to know and right to know basis. Access to the application is limited to Supervisors.

Department shall be assigned the following personnel to oversee Policy compliance by the Department and third-parties.

- (0923) Operations Manager, Division of Emergency Communications
- (0931) Assistant Deputy Director, Division of Emergency Communications

Sanctions for violations of this Policy include the following:

Violations of the Surveillance Technology Policy follow the same discipline procedures as violations of other directives:

- First Offense: Retraining
- Second Offense: Formal Counseling
- Third Offense: Letter of Reprimand

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.

EXCEPTIONS

Only in exigent circumstances or in circumstances where law enforcement requires surveillance technology data for investigatory or prosecutorial functions may data collected, retained or processed by the surveillance technology be shared with law enforcement.

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.

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 or concerns can be submitted to the Department by:

Members of the public would be directed to SFPD as they are the owners of the technology.

Department shall acknowledge and respond to complaints and concerns in a timely and organized response. To do so, Department shall:

Members of the public would be directed to SFPD as they are the owners of the technology, and it would be up to SFPD to respond to all questions and complaints.

City and County of San Francisco Employees:

All questions regarding this policy should be directed to the employee's supervisor or to the director. Similarly, questions about other applicable laws governing the use of the surveillance technology or the issues related to privacy should be directed to the employee's supervisor or the director.

BOARD of SUPERVISORS

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

M E M O R A N D U M

TO: Mary Ellen Carroll, Executive Director, Dept. of Emergency Management

FROM: Victor Young, Assistant Clerk

DATE: April 8, 2024

SUBJECT: LEGISLATION INTRODUCED

The Board of Supervisors' Rules Committee received the following proposed Ordinance:

File No. 240330

Ordinance approving Surveillance Technology Policy for the Department of Emergency Management's use of ShotSpotter, a gunfire detection technology.

If you have comments or reports to be included with the file, please forward them to Victor Young at the Board of Supervisors, City Hall, Room 244, 1 Dr. Carlton B. Goodlett Place, San Francisco, CA 94102 or by email at: victor.young@sfgov.org.

c: Oliva Scanlon, Dept. of Emergency Management
Michelle Busse, Dept. of Emergency Management

City and County of San Francisco
Master Report

City Hall
1 Dr. Carlton B. Goodlett Place
San Francisco, CA 94102-4689

File Number: 240330 **File Type:** Ordinance **Status:** 30 Day Rule

Enacted: **Effective:**

Version: 1 **In Control:** Rules Committee

File Name: Administrative Code - Surveillance Technology Policy - Department of Emergency Management - Gunfire Detection **Date Introduced:** 04/02/2024

Requester: Department of Emergency Management **Cost:** **Final Action:**

Comment: **Title:** Ordinance approving Surveillance Technology Policy for the Department of Emergency Management's use of ShotSpotter, a gunfire detection technology.

Sponsors: Mayor; Peskin

History of Legislative File 240330

Ver	Acting Body	Date	Action	Sent To	Due Date	Result
1	President	04/02/2024	ASSIGNED UNDER 30 DAY RULE	Rules Committee	05/02/2024	