



CITY OF OAKLAND

## Privacy Advisory Commission

February 5, 2026; 5:00 PM

Oakland City Hall

Hearing Room 1

1 Frank H. Ogawa Plaza, 1<sup>st</sup> Floor

### ***Meeting Agenda***

---

**Commission Members:** *District 1 Representative: Byron White, District 2 Representative: Don Wang, District 3 Representative: Issac Cheng, District 4 Representative: Lou Katz, District 5 Representative: Vacant, District 6 Representative: Gina Tomlinson, District 7 Representative: Vacant, Council At-Large Representative: Henry Gage III, Vice Chair, Mayoral Representative: Jessica Leavitt, Chair*

---

*Each person wishing to speak on items must fill out a speaker's card. Persons addressing the Privacy Advisory Commission shall state their names and the organization they are representing, if any. Members of the public can also raise their hand in Zoom if they have a question on an agenda item. The chair will determine the time allotted to speak on an agenda item.*

1. Call to Order, determination of quorum
2. Open Forum/Public Comment on Non-Agenda matters
3. Information Item:
  - a. Report from Public Works regarding OPD request for video footage.
4. Action Items:
  - a. Annual Reports
    1. Shotspotter Annual Report (OPD)
  - b. Use Policies
    1. Spotspotter - Gunshot Location Detection System (OPD) DGO I-20
    2. GPS Tracker – Vehicle GPS Tracking Device (OPD) I-33
    3. Responsive Easy Charging Products with Dynamic Signals – Evenergi LLC (OPW)

Members of the public can view the meeting live on KTOP or on the City's website at  
<https://www.oaklandca.gov/topics/ktop-tv-10>.

Comment in advance. To send your comment directly to the Privacy Commission and staff BEFORE the meeting starts, please send your comment, along with your full name and agenda item number you are commenting on, to Felicia Verdin at [fverdin@oaklandca.gov](mailto:fverdin@oaklandca.gov). Please note that eComment submissions close one (1) hour before posted meeting time. All submitted public comment will be provided to the Privacy Commission prior to the meeting.

To observe and participate in the meeting via Zoom, go to: <https://us02web.zoom.us/j/85817209915>  
Or One tap mobile: 1 669 444 9171

To participate in the meeting virtually, you must log on via Zoom. If you have a question, please raise your hand in Zoom during open forum and public comment.

For those attending in person, you can complete a speaker card and submit to staff.



## MEMORANDUM

---

**TO:** Floyd Mitchell  
Chief of Police

**FROM:** Gabriel Urquiza, A/Lieutenant,  
RTOC/Ceasefire Section

**SUBJECT:** Gunshot Location Detection  
System (ShotSpotter) – 2024  
Annual Report

**DATE:** August 7th, 2025

---

### Background

Oakland Municipal Code (OMC) 9.64.040: Surveillance Technology “Oversight following City Council approval” requires that for each approved surveillance technology item, city staff must present a written annual surveillance report for Privacy Advisory Commission (PAC). After review by the Privacy Advisory Commission, city staff shall submit the annual surveillance report to the City Council. The PAC shall recommend to the City Council that:

- The benefits to the community of the surveillance technology outweigh the costs and that civil liberties and civil rights are safeguarded.
- That use of the surveillance technology cease; or
- Propose modifications to the corresponding surveillance use policy that will resolve the concerns.

The PAC recommended adoption of OPD Department General Order (DGO) I-20: “Gunshot Location Detection System” at their October 3, 2019 meeting; the report was presented to the City Council on November 19, 2019 and adopted by the City Council via Resolution No. 87937 C.M.S. DGO I-20 requires that OPD provide an annual report to the Chief of Police, the Privacy Advisory Commission (PAC), and the City Council.

### 2024 Data Details

A. A description of how the surveillance technology was used, including the type and quantity of data gathered or analyzed by the technology:

*From the “Surveillance Impact Use Report for the Gunshot Location Detection System:”*

*Part 1 – How the System Works: “The GLD system sensors are designed to detect gunshots based on their acoustic signature (e.g., broad-frequency, impulsiveness and loudness). The utilization of multiple sensors at different distances from a gunshot sound allows the system not only to capture the sound but assign a probability that it is a gunshot and triangulate its precise location based on time difference of arrival. If the machine classifier in the “ShotSpotter Cloud” determines it is likely a gunshot based on computer-learning algorithms, the system will pull a short audio snippet from the sensors that detected it and send it to human analysts at the ShotSpotter Incident Review Center at its headquarters in Newark, CA. The analysts perform an auditory and visual assessment of the audio waveform to make a final determination as part of a two-phased classification process. If confirmed as a gunshot, an alert is published containing*

information such as street address, number of rounds fired, and a short audio snippet of the gunfire event— all within 60 seconds of the trigger pull (29 seconds on average). ”

*From Section 2: Proposed Purpose: “The purpose of GLD is to enable OPD to provide a higher level of the service to the community related to shootings. The system detects, locates and alerts officers of virtually all gunshots in a coverage area in less than 60 seconds enabling officers to respond to and investigate gunshots incidents they would not have known about and to respond to them much more rapidly than waiting for a 911 call. Personnel can better respond to gunshot activity and respond to possible armed individuals as well as to possible gunshot victims through this important real-time data.”*

*ShotSpotter technology was used in the following ways/with the following outcomes in 2024:*

- *The number of times ShotSpotter technology was requested: ShotSpotter alerted OPD to 6,280 gunshot incidents from January 1 – December 31, 2024. Of those alerts, **6,093 (97%) were not called in by the community as a 415GS call type (shots fired)**, and OPD would not have known about them nor have been able to respond in a timely fashion. This information is based on an analysis of calls within 15 minutes and 1,000 feet of a ShotSpotter alert.*
- *ShotSpotter led police to 125 shooting cases, 23 of which were Homicide and 102 were Assault with a Firearm.* OPD was able to provide and coordinate immediate emergency medical response on these shooting cases; OPD personnel believe that several of these victims survived the shootings specifically because of the quick response and subsequent medical attention. In some instances, OPD and medical response occurred within less than two minutes of the ShotSpotter activation. The ShotSpotter alert was within 15 minutes and 1,000 feet of the location where the victim was found. Furthermore, staff believe that there were many more cases where OPD responded to activations and found shooting victims – and where critical medical attention was provided. The 125 cases cited here are the ones where OPD and ShotSpotter staff can conclusively cite the response to the ShotSpotter activations.
- *ShotSpotter activations led OPD to 130 cases where their vehicle and/or dwelling was hit by gunfire. Of these 130 cases, 72 victims were present but not hit by gunfire, and an additional 58 were listed as victims because the property belonged to them.*
- *1,267 crime incident reports (20% of total activations)*
  - *795 (64%) of these incidents resulted in OPD Crime Lab requests for further firearm forensic analysis.*
- *ShotSpotter provided the following additional reports in relation to specific ShotSpotter activations:*
  - **Seven detailed forensic reports**
  - **Court preparation for four cases**
  - **Investigative Lead Summary 536**

B. Whether and how often data acquired through the use of the surveillance technology was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s):

*The following agencies have been provided log-in access to the ShotSpotter System for ongoing usage:*

1. *OPD and the Oakland Housing Authority Police Department entered into a Memorandum of Understanding (MOU) in 2012, following City Council approval, to fund the initial ShotSpotter program in areas of the City and near OHA buildings known for higher levels of gunshots. This MOU allows OPD to share access to the ShotSpotter cloud-based portal with OHA PD personnel (see **Attachment C**). OPD Policy is in the process of being revised to reflect OHA being provided access to the system.*

*These agencies have ongoing log-in access and do not make written requests for access.*

*DGO I-20 Section B – 1. “Authorized Use” states:*

*The Chief of Police or designee shall provide necessary training and/or technical assistance for GLD usage. Only OPD personnel, authorized members of agencies working in contracted partnership with OPD, and members of agencies specifically designated for temporary authorization by the Chief of Police, shall be granted access to OPD’s GLD System. The Chief of Police may designate temporary authorization to utilize OPD’s GLD system to members of agencies working in partnership with OPD within the City of Oakland.*

*Separate from ongoing login access, DGO I-20 provides rules for sharing ShotSpotter System data with outside agencies. Section C-3 of DGO I-20: “GUNSHOT LOCATION DETECTION SYSTEM” – “Releasing or Sharing GLD System Data,” states:*

*“GLD system data may be shared only with other law enforcement or prosecutorial agencies based on a need to know or a right to know, or as otherwise required by law, using the following procedures:*

1. *The agency makes a written request for the ShotSpotter data that includes:*
  - a. The name of the requesting agency.*
  - b. The name of the individual making the request.*
  - c. The need for obtaining the information.*
2. *The request is reviewed by the Bureau of Services Deputy Chief/ Deputy Director or designee and approved before the request is fulfilled.*
3. *The approved request is retained on file and shall be included in the annual report.*

**OPD did not provide specific ShotSpotter data to outside law enforcement agencies in 2024. However, OPD investigators in the Criminal Investigations Division and or other sections of OPD, such as the Ceasefire Section, regularly communicate with personnel from other law enforcement agencies on inter-jurisdictional investigations; these forms of collaboration may involve discussions related to shootings where OPD became informed from ShotSpotter activations. ShotSpotter activations many times may lead to evidence gathering (e.g., victims, witnesses, finding bullet casings, firearms); OPD may share information about evidence (e.g., that bullet casings or other evidence were found in a particular area at a particular time).**

C. Where applicable, a breakdown of what physical objects the surveillance technology hardware was installed upon; using general descriptive terms so as not to reveal the specific location of such hardware; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to:

*OPD has contracted with ShotSpotter to install GLD sensors in different areas (phases) in several parts of the city. The total coverage area for the current ShotSpotter system comprises 18.17 square miles or approximately 32 percent of the city land size (55.93). OPD has chosen to install the sensors in areas most prone to gunshots based upon historical data. Many areas in East and West Oakland now benefit from the GLD system.*

Most sensors are placed approximately 30 feet above ground level to maximize sound triangulation to fixed structures (e.g., buildings); at this altitude, the sensors can only record limited street-level human voice sounds. Furthermore, ShotSpotter only retains the audio for one second prior to a gun shot, and one second after.

D. Where applicable, a breakdown of where the surveillance technology was deployed geographically, by each police area in the relevant year:

**Attachment A** to this report provides the geographic areas of the City of Oakland that comprise the three ShotSpotter “phases” or areas covered under the current OPD-ShotSpotter contract. These areas intersect with all six official OPD Police Areas with a focus on areas where gunfire has historically occurred with greater regularity. **Attachment B** to this report is a weekly public ShotSpotter Activation Report for the week; this later report highlights areas of Oakland where ShotSpotter alerts have most recently occurred.

E. A summary of community complaints or concerns about the surveillance technology, and an analysis of the technology's adopted use policy and whether it is adequate in protecting civil rights and civil liberties. The analysis shall also identify the race of each person that was subject to the technology's use. The Privacy Advisory Commission may waive this requirement upon making a determination that the probative value in gathering this information to evaluate the technology's impact on privacy interests is outweighed by the City's administrative burden in collecting or verifying this information and the potential greater invasiveness in capturing such data. If the Privacy Advisory Commission makes such a determination, written findings in support of the determination shall be included in the annual report submitted for City Council review.

*Staff reached out to each City Council office to ask about possible community complaints or concerns related to this surveillance technology. No community complaints or concerns were communicated to staff.*

*OPD is not able to provide the race of each person connected to each activation since shooting suspects are often unknown. Many times, there is data regarding the race of shooting victims or witnesses (may be self-reported); however, this data is not captured in*

*the same system as ShotSpotter and the administrative burden (6,280 total 2024 activations) to constantly connect the two disparate datasets would overwhelm staff capacity. OPD therefore recommends that the PAC makes the determination, that the administrative burden in collecting or verifying this information as well as the associated potential greater invasiveness in capturing such data outweighs the benefit.*

F. The results of any internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response unless the release of such information is prohibited by law, including but not limited to confidential personnel file information:

*New officers and crime analysts are trained on the ShotSpotter System as part of police officer academies. Officers and analysts are provided direction that covers login, and how to use different views (e.g., time-period).*

*OPD officers have automatic access to ShotSpotter notifications when in patrol vehicles equipped with standard vehicle computers via the ShotSpotter Respond System. ShotSpotter creates a log for every sign-in to their system, which includes the level of access the user has (admin view or dispatch view, which is notification only). OPD and ShotSpotter has verified that for 2024, all users who logged into the system were authorized users.*

*Patrol Officers in vehicles and/or on mobile phones utilize the ShotSpotter Respond System. The Respond System pushes notifications to users – there is no interactivity functionality. Shotspotter can only audit logins for both the Respond and the Insight program. ShotSpotter and OPD staff have verified that all logins were associated with appropriate active employees. Staff regularly removes access from employee emails where staff separate from City employment.*

G. Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response.

*Neither OPD, ShotSpotter, nor the city's IT Department are aware of any data breaches of ShotSpotter data or technology in 2024.*

H. Information, including crime statistics, which helps the community assess whether the surveillance technology has been effective at achieving its identified purposes.

*Table 1 below provides 2024 Part 1 Crime Data. This data illustrates the high levels of both violent crime and property crimes that occur in Oakland including for the 2024 year.*

**Table 1: 2024 OPD Type 1 Crime Data**

**End of Year Crime Report — Citywide**  
**01 Jan. – 31 Dec., 2024**

<b>Part 1 Crimes</b> <i>All totals include attempts except homicides.</i>	2020	2021	2022	2023	2024	Percentage Change 2023 vs. 2024	5-Year Average	2024 vs. 5-Year Average
<b>Violent Crime Index</b> (homicide, aggravated assault, rape, robbery)	6,146	6,735	6,295	7,900	6,361	-19%	6,687	-5%
<b>Homicide – 187(a)PC</b>	102	122	120	119	81	-32%	109	-26%
<b>Homicide – All Other *</b>	7	12	2	7	5	-29%	7	-24%
<b>Subtotal - 187(a)PC + all other</b>	109	134	122	126	86	-32%	115	-25%
<b>Aggravated Assault</b>	3,381	3,686	3,294	3,785	3,231	-15%	3,475	-7%
Assault with a firearm – 245(a)(2)PC	503	609	461	526	354	-33%	491	-28%
<b>Subtotal - Homicides + Firearm Assault</b>	612	743	583	652	440	-33%	606	-27%
Shooting occupied home or vehicle – 246PC	427	544	347	383	246	-36%	389	-37%
Shooting unoccupied home or vehicle – 247(b)PC	222	271	160	150	93	-38%	179	-48%
Non-firearm aggravated assaults	2,229	2,262	2,326	2,726	2,538	-7%	2,416	5%
<b>Rape</b>	223	174	184	204	172	-16%	191	-10%
<b>Robbery</b>	2,440	2,753	2,697	3,792	2,877	-24%	2,912	-1%
Firearm	815	1,136	1,126	1,709	1,136	-34%	1,184	-4%
Knife	174	114	105	152	120	-21%	133	-10%
Strong-arm	976	801	786	1,055	985	-7%	921	7%
Other dangerous weapon	79	73	90	88	95	8%	85	12%
Residential robbery – 212.5(a)PC	93	99	66	111	96	-14%	93	3%
Carjacking – 215(a) PC	303	530	524	677	445	-34%	496	-10%
<b>Burglary</b>	8,703	10,602	14,034	18,881	9,811	-48%	12,406	-21%
Auto	6,231	8,496	11,104	15,086	6,798	-55%	9,543	-29%
Residential	1,266	1,132	1,165	1,498	1,111	-26%	1,234	-10%
Commercial	981	771	1,538	1,876	1,400	-25%	1,313	7%
Other (includes boats, aircraft, and so on)	210	196	209	411	300	-27%	265	13%
<b>Motor Vehicle Theft</b>	8,760	9,399	10,346	15,391	10,439	-32%	10,867	-4%
<b>Larceny</b>	6,147	6,785	9,576	9,975	8,368	-16%	8,170	2%
<b>Arson</b>	196	173	166	123	112	-9%	154	-27%
<b>Total</b>	29,959	33,706	40,419	52,277	35,096	-33%	38,291	-8%

**Table 2: ShotSpotter Activations Resulting in Incident Report for Firearm Crimes by Category in 2024**

<b>Cases by Firearm-Related Crime Type</b>	
Homicide	23
Assault with a Firearm	102
Shoot at an Occupied Home/Vehicle	72
Shoot at an Unoccupied Home/Vehicle	58
Negligent Discharge of a Firearm	958
Weapons Violations (including exhibit/draw)	5
Carjacking with a Firearm (including attempts)	7
Robbery with a Firearm (including attempts)	9
<b>Total Cases</b>	<b>1,234</b>

**Table 3: Firearm Recoveries in 2024 Connected to ShotSpotter Activations illustrate Guns Recovered**

<b>Guns Recovered by Crime Type</b>	
Homicide	4
Assault with a Firearm	12
Shoot at an Occupied Home/Vehicle	2
Shoot at an Unoccupied Home/Vehicle	0
Negligent Discharge of a Firearm	27
Weapons Violations (including exhibit/draw)	3
Carjacking with a Firearm (including attempts)	0
Robbery with a Firearm (including attempts)	2
Other	0
<b>Total Cases</b>	<b>50</b>

- 50 weapons seized.
  - Note: more than one firearm may be from the same incident.
- 1,289 alerts when advanced situational awareness was provided to responding patrol officers on their way to crime scenes in high danger situations that required specific approach tactics such as multiple shooters, high capacity or automatic weapons being used, and drive-by shootings.

- I. Statistics and information about public records act requests regarding the relevant subject surveillance technology, including response rates:

There were 8 total PRR in 2024. 3 are closed and 5 remain open.

Total Requests: 8

Open Requests: 5

24-978  
24-4633  
24-7104  
24-7126  
24-11642

Closed Requests: 3

24-3178  
24-10846

24-13193

J. Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year:

**\$1,052,088 for 7/1/24-9/30/25 was paid in early 2025 for 18.17 square miles of coverage.**

These fees encompass all services ShotSpotter currently provides to Oakland. There are no additional charges for meetings, reports, analysis and training. These funds come from OPD's General Purpose Fund.

K. Any requested modifications to the Surveillance Use Policy and a detailed basis for the request:

*No requests for policy changes at this time.*

OPD is committed to providing the best services to our community while being transparent and instilling procedural justice through daily police activity. This report is compliance with these OPD commitments. OPD hopes that this report helps to strengthen our trust within the Oakland community.

For any questions with this report, please contact Gabriel Urquiza, A/Lieutenant, OPD, Ceasefire Section, at [gurquiza-leibin@oaklandca.gov](mailto:gurquiza-leibin@oaklandca.gov)

Respectfully submitted,

---

Gabriel Urquiza, A/Lieutenant, OPD, RTOC/Ceasefire Section

Reviewed by,  
Anthony Tedesco,  
A/Assistant Chief, Operations

Eric Kim, A/Captain  
OPD, Ceasefire Section

Prepared by:  
Dr. Tracey Jones, Police Services Manager  
OPD, Bureau of Services

## Attachment A - Shot Spotter Coverage Areas

### Phase I with red borders (Activated in 2006): 6.0 square miles\*

East Oakland: East of High Street to 106th Avenue

West Oakland: East of Highway 980 to Frontage Road

### Phase II with blue borders (Activated in 2013): 6.64 square miles

East Oakland: West of High Street to Park Boulevard

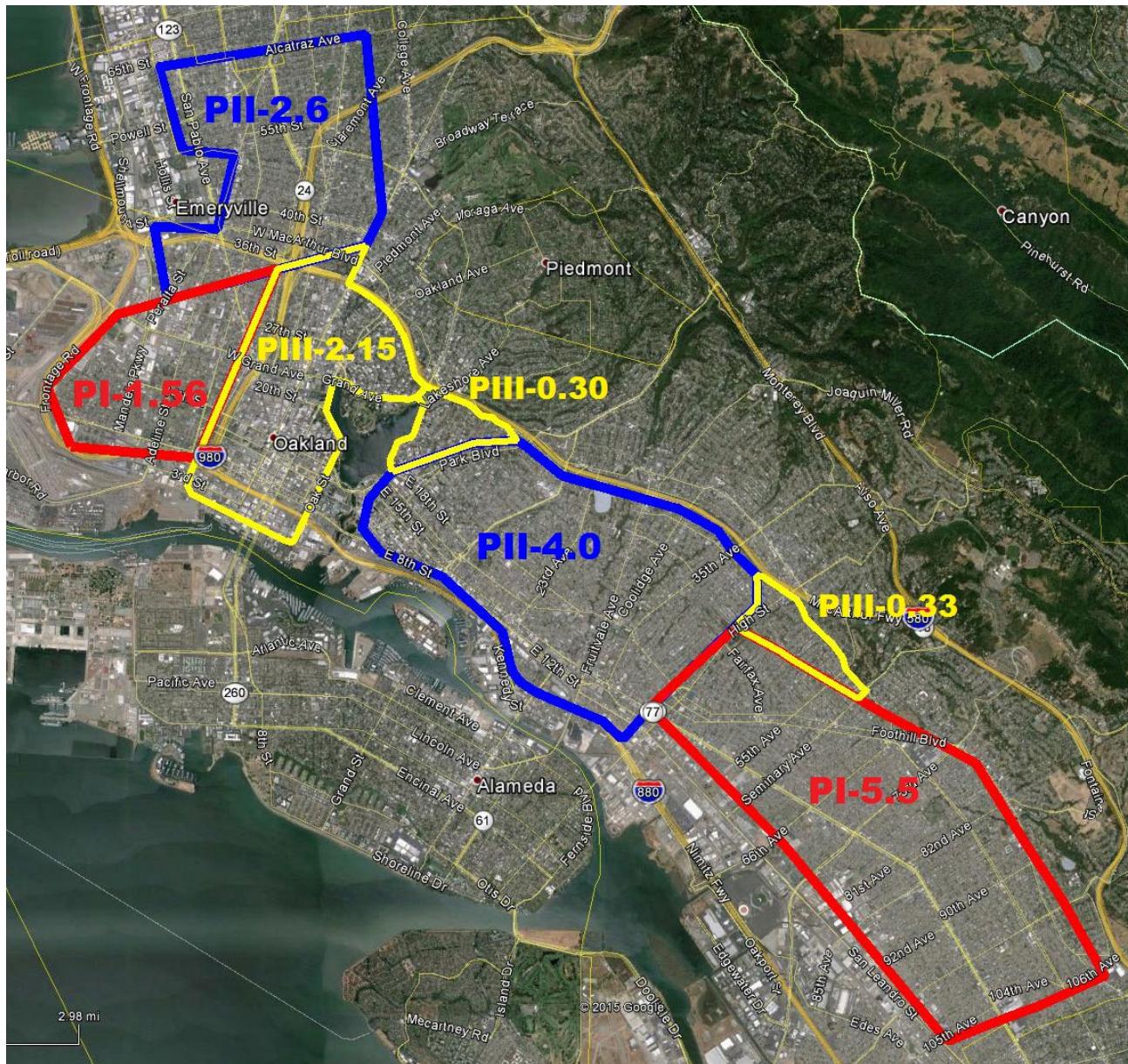
North Oakland: North of Highway 580 to Alcatraz Avenue

### Phase III with yellow borders (Activated in 2016): 2.78 square miles

Downtown Oakland: Jack London Square to about West MacArthur Boulevard

Cleveland Height area: East of Lake Merritt to Highway 580 & Park Boulevard

Maxwell Park: East of High Street to Highway 580 & Mills College



\* While the original contracted coverage total for Phase I was 6.0 mi<sup>2</sup>, an additional 1.06 mi<sup>2</sup> of ShotSpotter coverage was added, at no charge, for a total of 7.06 mi<sup>2</sup> when Phase I service was upgraded and converted to the newer subscription platform in 2011.

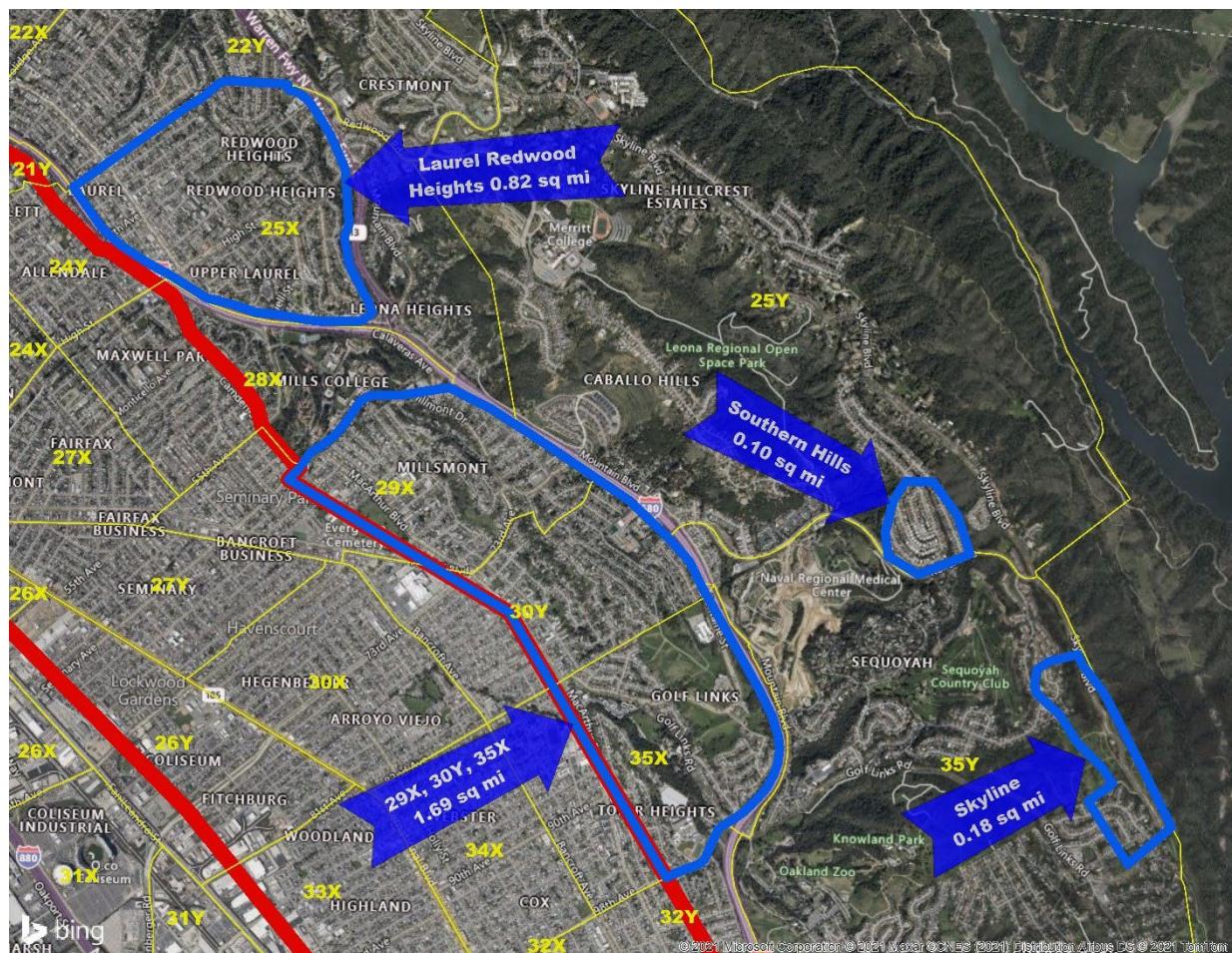
Phase IV with blue borders (Activated in 2021): 2.79 square miles

Laurel Redwood Heights: Covering a portion of Beat 25X

Southern Hills: Covering a portion of Beat 25Y

Millsmont / Golf Links: Covering Beats 29X, 30Y, and 35X

Skyline: Covering a portion of Beat 35Y





## DEPARTMENTAL GENERAL ORDER

### I-20: GUNSHOT LOCATION DETECTION SYSTEM

Effective Date: XX AUG 25

Coordinator: Ceasefire Division

---

The Oakland Police Department believes in protecting and serving its diverse community and city through fair, equitable, and constitutional policing. OPD believes in the usage of technology to aid in this mission and in the investment in contemporary surveillance technology to help improve public safety while still protecting community members' privacy rights. This includes a multipronged approach related to tactics, methodology, and technology that allows for de-escalation in often rapidly evolving situations.

This policy provides guidance and procedure for response, immediate actions, follow up, documentation, and auditing of OPD's Gunshot Location Detection (GLD) System incidents that occur within the City of Oakland.

All data, whether sound or image, generated by OPD's GLD System are for the official use of this department. Because such data may contain confidential information, such data is not open to public review.

#### A. Description of the Technology

OPD uses a GLD System (currently the ShotSpotter® Flex™ system, provided by SoundThinking, Inc. as a part of their Safety Smart Platform) to record gunshot sounds and use sensors to locate the origin of the gunshots. The GLD system enables OPD to be aware of gunshots in the absence of witnesses and/or reports of gunshots to OPD's Communications Division (Communications). The GLD system notifies Communications of verified gunshot events, which allows OPD to quickly respond to incidents of gunfire and related violent criminal activity.

This technology often allows OPD members to respond to incidents of gunfire in a more expedient manner, as the activation notifications are received in near real time. Incidents regarding gunfire are rapidly evolving, and a delay in response by law enforcement, by even minutes, can mean the difference between life and death for the victims of gun violence. This technology allows members of OPD to learn of gunfire incidents, and respond accordingly to the locations where a shooting may have occurred. This response is critical in members being able to render aid to victim(s), locate/secure evidence, and conduct quality preliminary investigations regarding gun violence within the City of Oakland.

#### A – 1. How ShotSpotter Works

OPD's GLD 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 auditory signature consistent with that of a gunshot(s). The audio triangulation of multiple installed sensors then determines an approximate 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 the OPD Communications Division in real-time so that they may notify responding officers where guns were fired.

### **A – 2. The GLD System**

There are three components to GLD system:

1. GLD Sensors: Sensors are installed in different coverage areas in Oakland. Oakland currently has five coverage areas (or phases) where sensors are installed to triangulate gunshots.
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 OPD ShotSpotter Software System within seconds.
3. The OPD ShotSpotter Software System: This system is a web-based system; OPD authorized personnel can use internet browsers or GLD ShotSpotter applications to connect to the ShotSpotter system. Access to the GLD system is controlled via an individual user login and password.

## **B. General Guidelines**

### **B – 1. Authorized Use**

The Chief of Police or designee shall provide necessary training and/or technical assistance for GLD usage. Only OPD personnel and partnering agencies working in contracted partnership with OPD when it expressly and transparently permitted in a written contract and/or MOU, shall be granted access to OPD's GLD System.

The Chief of Police may designate temporary authorization to utilize OPD's GLD system to members of agencies working in partnership with OPD within the City of Oakland.

The GLD system shall only be used for investigating incidents of suspected gunfire. The system shall never be used to record human conversations except where portions of conversations are unintentionally captured in the audio background of gunshot recordings. NOTE: OPD does not have ability to access the real-time audio associated to the GLD system.

### **B – 1. Restrictions on Use**

Department members shall not use or allow others to use the GLDS acoustical recording equipment, software or data for any unauthorized purpose.

### **B – 2. Use Priority**

All GLD activations shall be treated as priority one calls.

### **B-3. Data Access**

1. Authorized personnel may access the GLD system and receive notifications of verified GLD activations. OPD Communications may also notify authorized personnel of GLD activations. Authorized personnel may respond to such notifications based upon priorities as mandated by their supervisors.
2. The GLD system shall only be used for official law enforcement purposes, and accessing the data collected by the GLD 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
3. Only specifically authorized personnel authorized by the Chief or Chief-designee will have access to historical GLD system data via GLD system applications outside of current or ongoing investigations.
4. The GLD system may be used for authorized patrol and investigation purposes. Contacting individuals at locations where GLD activations occur shall be conducted in accordance with applicable law and policy
5. Members approved to access GLD system data may 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 GLD system activations are entered into OPD's computer-aided dispatch (CAD) record management system (RMS) with GLD system-specific ID numbers. Authorized personnel can then query the CAD/RMS system for any and all GLD system activations.

## **C. ShotSpotter Data**

### **C – 1. Data Collection and Retention**

1. GLD acoustic data is recorded when three sensors all record sounds that match the acoustic signatures of gunshots. The sensors are constantly recording a total of 30 hours into acoustical digital .wav format files, and then deleting the data unless triggered to send the data to ShotSpotter for analysis; the buffer allows OPD to request data within 24 hours.
2. 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 is maintained in perpetuity, by ShotSpotter HQ.

### **C – 2. Data Security**

All data will be closely safeguarded and protected by both procedural and technological means:

1. Authorized personnel must always gain access to the GLD system data through a login/password-protected system which records all login access.
2. OPD has no direct access to actual GLD (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 in cases where CID investigators need to search for previous gunshots.

### **C – 3. Use of GLD System Data in Conjunction with Partnering Agencies**

GLD system data may be shared with specified law enforcement and prosecutorial agencies that work in partnership with the Oakland Police Department and operate within the City of Oakland. These agencies have been identified based on their work within the community where the agency requires access due to an investigative need, or to provide situational awareness that would enhance the safety of agency members and the community. Any member of an outside agency that is provided access to the GLD system data is mandated to comply with this policy or be subject to the loss of access to the GLD system data. The following partner agencies are provided access to the GLD system data:

1. Oakland Housing Authority (Police Department) in accordance with Oakland City Council Resolution Number 84119.
2. Alameda County District Attorney's Office with regards to specific investigations involving GLD.

The above listed partnering agencies data shall be listed within the annual report for any 12-month period during which the partnering agency was provided access.

#### **C – 4. Releasing or Sharing GLD System Data to Non-partnering Agencies**

GLD system data may be shared only with other law enforcement or prosecutorial agencies (outside of those listed in Section C-3) based on a need to know or a right to know, or as otherwise required by law, using the following procedures:

1. The agency makes a written request for the ShotSpotter data that includes:
  - a. The name of the requesting agency.
  - b. The name of the individual making the request.
  - c. The need for obtaining the information.
2. The request is reviewed by the Bureau of Investigations Deputy Chief or designee and approved before the request is fulfilled.
3. The approved request is retained on file, and shall be included in the annual report.

Requests for ShotSpotter data by non-law enforcement or non-prosecutorial agencies will be processed as provided in Departmental General Order M-09.1, Public Records Access (Civil Code § 1798.90.55) and per any interagency agreements.

#### **D. GLD System Administration**

OPD's GLD System is installed and maintained by SoundThinking in collaboration with OPD. Oversight of the system as well as data retention and access, shall be managed by OPD's Ceasefire Division. The sensors as well as the system are maintained by SoundThinking.

##### **D – 1. GLD System Coordinator**

The title of the official custodian of the GLD System (ShotSpotter Coordinator) is the Captain of the OPD Ceasefire Division, or designee.

##### **D – 2. GLD System Administrator**

The Ceasefire Captain shall administer the GLD system, implementation and use, in collaboration with OPD's Criminal Investigations Division (CID). The

Ceasefire Captain, or designee, shall be responsible for developing guideline, procedures, and processes for the proper collection, accuracy and retention of GLD System data specifically retained by OPD.

#### **D – 3. Monitoring and Reporting**

The Oakland Police Department will monitor its use of the GLD system to ensure the accuracy of the information collected and compliance with all applicable laws, including laws providing for process, and time period system audits.

Department members should document the use of ShotSpotter-related information when responding to incidents where their response to an activation resulted in a crime report being generated (e.g. shootings, homicides, etc.).

Members should indicate in their report that such technology was used, and, if possible, note what benefit the technology provided (if any). Such benefits could include recovery of weapons, shell casings, identification of suspects, victims, or witnesses, situational awareness, and faster transport to or receipt of medical care, including first aid.

The ShotSpotter Coordinator shall provide the Chief of Police, Privacy Advisory Commission, and Public Safety Committee with an annual report for the previous 12-month period. These reporting procedures will assist in evaluating the efficacy of this policy and equipment.

#### **D – 4. Training**

The Training Section shall ensure that members receive department-approved training for those authorized to use or access the ShotSpotter system.

Trainings for Communications personnel (dispatchers and operators) may include training on how to acknowledge the GLD system activations and how to use the system software to identify activation locations so as to provide information to responding officers.

By Order of

Floyd Mitchell

Chief of Police

---

Date Signed:



## DEPARTMENTAL GENERAL ORDER

### I-33: Vehicle (GPS) Tracker

Effective Date: DD MMM 26

Coordinator: Vehicle Tracker Coordinator, Ceasefire Division

---

The purpose of this policy is to establish guidelines for the Oakland Police Department's use of vehicle GPS tracking devices, for the purpose of furthering the department's mission and goals.

#### **A. PURPOSE OF TECHNOLOGY**

Vehicle GPS tracking technology supports Oakland Police Department investigations by assisting with the apprehension of wanted suspects, the recovery of vehicles, and the advancement of criminal investigations through the lawful collection of vehicle location data. When authorized, this technology allows investigators to identify patterns of movement and corroborate other investigative information. The use of this technology is intended to further legitimate law enforcement objectives while complying with applicable department, legal and constitutional requirements.

#### **B. DESCRIPTION OF THE TECHNOLOGY**

Vehicle GPS tracking technology consists of an electronic device that is attached to a vehicle pursuant to legal authorization and designed to collect location information over time. The device determines the vehicle's location using Global Positioning System satellites and transmits that information through a cellular or similar wireless network to a secure server maintained by the service provider. The device provides its own power and does not tap into the vehicle's on-board systems. Authorized OPD personnel may access the data through a secure software interface to review vehicle location, movement history, and associated date and time information.

The accuracy, frequency, and continuity of location reporting may vary based on environmental conditions, signal availability, device placement, and limitations inherent to satellite and wireless networks. Regardless of the vendor or platform used, all vehicle GPS tracking deployments by OPD are governed by the same legal standards, authorization requirements, departmental policies and city ordinances applicable to surveillance technologies.

#### **C. AUTHORIZED USE**

Vehicle GPS trackers may be used only as part of an active criminal investigation and only when authorized by a search warrant compliant with the California Electronic Communications Privacy Act (CalECPA), codified at California Penal Code section 1546 et seq. Any monitoring and retaining of data generated by a vehicle GPS tracking device requires a search warrant supported by probable cause and signed by a judge, in accordance with Penal Code section 1546.1. A tracking device search warrant shall specify a reasonable length of time that the device may be used, not to exceed 30 days from the date the warrant is issued, unless the court grants an extension for good cause.

Only OPD personnel assigned to, or directly assisting with, the specific investigation for which the vehicle GPS tracking device is authorized may access or utilize the technology. Access to vehicle GPS tracking data shall be limited to personnel with a legitimate right to know and a need to know based on their assigned investigative role. Monitoring, retaining, or reviewing data by personnel not assigned to or assisting with the investigation, or outside the scope of the authorized purpose, is prohibited.

Exigent installation of a vehicle GPS tracking device may occur only when the vehicle is located in a public place and exigent circumstances are present as defined by the California Electronic Communications Privacy Act (CalECPA).

Exigent circumstances are situations where there is an immediate danger of death or serious bodily injury to any person, or where delay in installing the device would risk the loss of critical investigative information related to such danger, consistent with Penal Code section 1546.1(c)(6).

Exigent installation requires approval from an OPD commander at the rank of lieutenant or above.

If a GPS tracker is installed in exigent circumstances, a post hoc search warrant must be sought as soon as practicable and no longer than “within three court days after obtaining the electronic information,” and must document the facts establishing probable cause and the exigent circumstances justifying the installation and any monitoring that occurred, pursuant to Penal Code section 1546.1(h). The Vehicle GPS Tracking Coordinator is to be notified of any exigent installations.

#### **D. DATA COLLECTION**

Vehicle GPS tracking technology collects location information associated with a vehicle, including geographic coordinates and corresponding date and time data. The device determines location through Global Positioning System satellites and transmits that information through a cellular or similar wireless network to a secure server maintained by the service provider. Authorized OPD personnel may access the data through a secure software platform to review historical and real time vehicle movement for investigative purposes.

The data collected is limited to vehicle location and movement information and does not capture audio, video or any form of communications.

#### **E. DATA ACCESS**

Access to live vehicle GPS tracking data is limited to OPD investigators or OPD personnel assisting with ongoing criminal investigations. Live location information may

be accessed only for legitimate law enforcement purposes and in a manner consistent with the scope of the applicable search warrant.

Historical vehicle GPS tracking data collected during the authorized period may be accessed by OPD investigators or OPD personnel assisting with ongoing criminal investigations for review and analysis. Historical data is made available through a secure electronic platform or other Department approved evidence management system such as Axon Evidence.com.

Vehicle GPS tracking data is not accessed, reviewed, or shared for purposes unrelated to lawful law enforcement activities. Any access or disclosure of GPS tracking data must comply with applicable law, court orders, and Department policy. Unauthorized access or use of vehicle GPS tracking data is prohibited.

## **F. DATA PROTECTION**

Vehicle GPS tracking data is stored on the vendor's server during the period of active use. The coordinator shall ensure that the server and its content is properly protected according to best practice for cybersecurity. Access to the vendor portal is limited to OPD personnel using authorized accounts for investigative purposes related to an active criminal investigation.

At the conclusion of the investigation or monitoring period, vehicle GPS tracking data is either deleted from the vendor portal or preserved by exporting the data into a Department approved law enforcement evidence management system, such as Axon Evidence.com, when the data is needed for a criminal prosecution or other lawful purpose. When necessary, data may also be stored on a physical medium protected by a password to limit access. Data that is not needed for evidentiary or investigative purposes is deleted and not retained.

## **G. DATA RETENTION**

Vehicle GPS tracking data that is not identified as relevant to a lawful criminal investigation is retained for no longer than thirty days from the date of collection and is deleted thereafter. This retention period applies to data stored on the vendor platform and is intended to limit the retention of location data that does not have an investigative or evidentiary purpose.

If vehicle GPS tracking data is determined to be relevant to a lawful criminal investigation, prosecution, or court proceeding, the data may be retained for the duration of the legal process. Such data is retained only while the associated criminal matter is pending and is deleted after full adjudication of the court proceeding, including any right to appeal. Data is not retained beyond this period unless otherwise required by law or court order.

## **H. PUBLIC ACCESS**

Data that is collected and retained under this policy is considered a “law enforcement investigatory file” pursuant to Government Code § 7923.600(a) and shall be exempt from public disclosure. Members of the public may request data via public records request pursuant to applicable law regarding Public Records Requests as soon as the criminal or administrative investigations has concluded and/or adjudicated.

## **I. THIRD PARTY DATA SHARING**

Vehicle GPS tracking data is not shared outside the Oakland Police Department absent proper legal authority. Any sharing of vehicle GPS tracking data with another law enforcement agency or prosecuting authority requires a CalECPA compliant search warrant, a court authorized sharing order, or a discovery requirement arising from a criminal prosecution. Informal requests or requests made without supporting legal documentation are not sufficient.

Any outside agency requesting vehicle GPS tracking data must submit a written request to OPD identifying the legal authority for the request and the investigative or prosecutorial need for the data. The request and OPD’s response shall be documented and retained in accordance with Department policy. When legally authorized, data is shared only to the extent permitted by the applicable warrant, court order, or discovery obligation and remains subject to the handling, retention, and protection requirements set forth in this policy.

## **J. TRAINING**

OPD personnel utilizing vehicle GPS tracking technology should receive training on this policy and the legal requirements governing its use, including the California Electronic Communications Privacy Act (CalECPA) and related case law. Training should address lawful authorization requirements, limitations on use, access controls, and data retention obligations associated with vehicle GPS tracking.

OPD personnel responsible for installing, monitoring, or accessing vehicle GPS tracking data should receive training on the operational use of the technology and Department procedures related to its deployment and data handling. Supervisory personnel involved in approving or overseeing the use of vehicle GPS tracking technology should receive training sufficient to ensure compliance with this policy and applicable law.

The Vehicle GPS Tracking Coordinator is responsible for tracking training completion and maintaining associated training records.

## **K. AUDITING AND OVERSIGHT**

The Vehicle GPS Tracking Coordinator is a sworn OPD sergeant assigned to Ceasefire or an equivalent street level enforcement unit designated by the Department. The Coordinator is responsible for tracking all uses of vehicle GPS trackers by OPD. This includes maintaining a record of each deployment, the associated investigation, the legal authority authorizing the use, and the duration of the tracking. The Coordinator ensures that each use of the technology is connected to a CalECPA compliant search warrant or a documented exigency warranting installation, followed by a post hoc search warrant.

The Vehicle GPS Tracking Coordinator reviews vehicle GPS tracking use to ensure compliance with this policy, applicable law, and court orders. This review includes confirming that access to live and historical data was limited to authorized OPD personnel and that data retention and deletion requirements were followed. Any identified issues or noncompliance are addressed through appropriate supervisory or administrative channels.

Information regarding vehicle GPS tracking use may be included in required reporting to the Privacy Advisory Commission and City Council in accordance with Oakland Municipal Code 9.64. This reporting may include aggregate usage information, audit results, and demographic data such as race information when required for reporting purposes. Publicly reportable information is limited to non-investigative data and does not include case specific or personally identifiable information.

## **L. MAINTENANCE**

The Vehicle GPS Tracking Coordinator is responsible for ensuring that vehicle GPS tracking data is managed in accordance with the Data Protection and Data Retention sections of this policy. This includes ensuring that data stored on vendor platforms, physical media, or Department approved evidence management systems is handled consistently with policy requirements.

The Vehicle GPS Tracking Coordinator is also responsible for coordinating with the vendor, when necessary, to address technical issues related to the vehicle GPS tracking system. Maintenance of the tracking devices or associated software is limited to vendor supported processes and does not include modification of the technology by OPD personnel.

By Order of

James Beere  
Chief of Police

Date Signed:

## **OAKLAND POLICE DEPARTMENT**

### **Surveillance Impact Report: Vehicle GPS Tracking Devices**

#### **A. Description:**

Vehicle GPS tracking devices are electronic devices that are attached to vehicles. Once installed, the device collects location information associated with the vehicle by using Global Positioning System satellites and transmitting that information through a cellular or similar wireless network.

The data collected by the device consists of geographic coordinates and associated date and time information. The device provides its own power source and does not connect to or access the vehicle's onboard systems. Installation of the device does not interfere with the normal operation of the vehicle and does not require modification of vehicle components.

Vehicle GPS tracking devices are configured to report location data at intervals determined by investigative needs and technical limitations. The accuracy and frequency of reporting may vary based on environmental conditions, signal availability, and device placement. The technology does not capture audio, video, or the contents of communications.

#### **B. Purpose:**

The Oakland Police Department utilizes vehicle GPS tracking devices to further criminal investigations. Vehicle GPS tracking assists investigators with locating vehicles, identifying patterns of movement, corroborating other investigative information, and supporting the apprehension of wanted suspects.

The technology may be used to monitor vehicle movement in real time or to review historical location data when authorized by law. Vehicle GPS tracking is used in investigations where vehicle movement is relevant to establishing criminal activity or supporting other investigative leads.

#### **C. Location:**

Vehicle GPS tracking data is initially stored on the vendor's server and accessed through a web-based portal by authorized OPD personnel. The technology is not deployed as fixed infrastructure and is installed only on vehicles associated with authorized investigations.

When necessary for evidentiary purposes, vehicle GPS tracking data may be exported from the vendor platform and stored in a department approved evidence management system, such as Axon Evidence.com, or on a password protected physical medium.

#### **D. Impact:**

Vehicle GPS tracking involves the collection of location data over time, which can reveal patterns of movement associated with a vehicle. Location data may show where a vehicle travels, how frequently it visits certain locations, and the duration of stops. When reviewed over an extended period, this information can provide insight into an individual's habits, routines, or associations.

Continuous or repeated tracking increases the intrusiveness of the technology by allowing

investigators to reconstruct travel history and identify recurring locations. Location data may indirectly reveal sensitive information, such as frequent visits to residences, workplaces, or other locations associated with personal activities.

Vehicle GPS tracking may also incidentally collect information related to individuals other than the intended investigative target, including passengers or individuals who regularly interact with the tracked vehicle.

**E. Mitigations:**

The privacy impact of vehicle GPS tracking is mitigated through legal requirements and Department policy that limit when and how the technology may be used. The California Electronic Communications Privacy Act (CalECPA) requires law enforcement to obtain a search warrant supported by probable cause before monitoring or retaining vehicle GPS tracking data, except in narrowly defined exigent circumstances involving the danger of death or serious bodily injury. Any exigent use is subject to post hoc judicial review through a search warrant application that documents the facts giving rise to the emergency.

OPD policy further limits the scope of vehicle GPS tracking by restricting its use to active criminal investigations and requiring that tracking be authorized for a specific vehicle and defined time period. This limits OPD's ability to collect location data beyond what is relevant to the investigation. Access to GPS tracking data is limited to OPD investigators or OPD personnel assisting with ongoing criminal investigations.

Data retention requirements further mitigate privacy impact by limiting how long vehicle GPS tracking data is stored. Data that is not identified as relevant to a lawful investigation is deleted within thirty days of collection. GPS tracking data retained for evidentiary purposes is stored only for the duration of the associated criminal case and is deleted after adjudication of the court proceeding, including any right to appeal.

OPD also mitigates privacy impact through oversight and auditing. Use of vehicle GPS tracking technology is tracked by a designated coordinator, and aggregate usage information is included in reporting to the Privacy Advisory Commission and City Council as required by Oakland Municipal Code 9.64. Public reporting is limited to non-investigative information and does not include case specific or personally identifiable data.

**F. Data Types and Sources:**

Vehicle GPS tracking devices collect the following information:

Geographic location of the vehicle

Date and time associated with each location point

The data is generated by the GPS tracking device and transmitted through cellular or similar wireless networks to the vendor's server. The technology does not collect communications content, audio, video, or vehicle diagnostic data.

**G. Data Security:**

Vehicle GPS tracking data is accessed through the vendor platform using authorized OPD accounts. Access is limited to investigative purposes related to active criminal investigations.

When data is retained for evidentiary purposes, it is stored in Axon Evidence.com or on a password protected physical medium. Access to retained data is limited to authorized OPD personnel in accordance with Department policy.

**H. Fiscal Cost:**

OPD currently possesses twenty-one (21) GPS tracking devices serviced by 3si Security Systems (CovertTrack). The cost of the software and maintenance for each device is \$540 per device, totaling **\$11,340 a year.**

There is a one-time cost for a new/replacement tracking device at \$1095. Devices currently only need to be replaced when it is physically destroyed.

**I. Third Party Dependence:**

Vehicle GPS tracking relies on third party vendors to provide tracking devices, data transmission, and initial data storage. OPD controls access to the data and determines whether data is retained, deleted, or preserved for evidentiary purposes.

Third party vendors do not independently access or disseminate vehicle GPS tracking data collected for OPD investigations.

Vendors only provide technical support for the functionality of the trackers and the access portal.

**J. Alternatives Considered:**

Alternative investigative methods include physical surveillance, license plate reader data, or historical location records obtained through search warrants.

These alternatives may not provide the same level of real time or continuous location information and may be more resource intensive or less effective in time sensitive investigations.

**ALTERNATIVE VENDORS CONSIDERED**

OPD currently utilizes vendor services from 3si Security Systems (Covert Track). OPD purchased devices from Covert Track at a one-time cost. OPD has reviewed alternative vendors to see if there are better alternatives. However, each device is vendor-specific and switching to an alternative vendor would result in an additional cost to purchase all new devices. OPD is conducting on-going quotation of other vendors to ascertain if the fiscal cost of replacing all existing trackers is cheaper than continuing with 3si Security Systems.

The California Highway Patrol (CHP) utilizes a service called Code 5 Group, LLC. CHP is satisfied with the use of their service. The city of Concord utilizes TactiTrack for GPS tracking. They are satisfied with the service. The city of Daly City utilizes Special Services Group, LLC (Ensurity) for GPS tracking. They are satisfied with the use of this service. Most of the Bay Area agencies utilizes the same company as OPD, 3si Security System (Covert Track).

A review of these three companies were conducted. The trackers are all physically similar and there is no advantage with switching to another vendor. The web-based portals are also similar and none of these other vendors offers any additional data security. Fiscally, it is currently not worth switching vendors given the need to replace all existing OPD trackers.

**K. Track Record:**

Vehicle GPS tracking technology is commonly used by local, state, and federal law enforcement agencies as part of criminal investigations. The technology is primarily used in cases involving violent crime, organized criminal activity, and vehicle related offenses.

A number of local agencies utilize GPS tracking devices in their day-to-day operations.

The city of San Francisco does not maintain public stats to their usage but maintain that they only use it for criminal investigations.

The city of Concord also utilizes GPS tracking devices. They do not maintain a usage log but are satisfied in its usage for furthering their criminal investigations.

The City of San Leandro utilizes GPS tracking devices in their criminal investigations. They do not maintain a usage log but are satisfied in its usage for furthering their criminal investigations.



3SI Security Systems Inc  
101 Lindenwood Dr.  
Suite 200  
Malvern PA 19355  
United States

# Invoice - PF

#SO973932

Invoice Date: 01/05/2026  
Customer ID: 165410  
Parent Customer ID:

Bill To	Ship To	TOTAL
Oakland PD - CA 455 7th St Oakland CA 94605 United States	Oakland PD - CA 455 7th St Oakland CA 94605 United States	\$11,340.00
		:

Cycle Month: 00  
Currency: US Dollar  
Memo: August & September Contract Renewal

Terms	PO/WO #	Shipping Method					
Net 30		FedEx Ground®					
Qty	Item	Start Date	End Date	Term (Months)	Rate	Amount	
2	<b>Tracking Service: Stealth</b> Tracking Service: Stealth Renewal Device Admin: Carlos Carrillo Device IDs: 350120022358925 350120022380671	08/01/2025	07/31/2026	12	540.00	\$1,080.00	
17	<b>Tracking Service: Stealth</b> Tracking Service: Stealth Renewal Device Admin: Joe Jochim Device IDs: 353863116271978 357812096922528 352753091420073 350120022383550 353863118221476 350120022382560 353863116253034 353863115017919 350120022376737 350120022380770 350120022382537 357812098573576 353160130292209 353863117909709 353863117908321 353863114986411 350120022383667	08/01/2025	07/31/2026	12	540.00	\$9,180.00	
2	<b>Tracking Service: Stealth</b> Tracking Service: Stealth Renewal Device Admin: Joe Jochim Device IDs: 350120022381166 350120022380135	09/01/2025	08/31/2026	12	540.00	\$1,080.00	



SO973932

1 of 2

Email to Billing@3SI.com

31 of 37



3SI Security Systems Inc  
101 Lindenwood Dr.  
Suite 200  
Malvern PA 19355  
United States

# Invoice - PF

#SO973932

Invoice Date: 01/05/2026  
Customer ID: 165410  
Parent Customer ID:

<b>Subtotal</b>	\$11,340.00
<b>Shipping &amp; Handling</b>	\$0.00
<b>Sales Tax</b>	\$0.00
<b>Total</b>	\$11,340.00

**Remittance Address:**

3SI Security Systems, Inc  
P.O. Box 5146  
New York, NY 10087-5146



SO973932

2 of 2

Email to [Billing@3SI.com](mailto:Billing@3SI.com)

32 of 37

**City of Oakland**  
**Surveillance Technology Use Policy Guidelines**  
**EV Energy Better Fleets**

**A. Purpose**

*On 1-29-25, the City council approved the acceptance of a grant awarded by California Energy Commission Responsive, Easy Charging Products With Dynamic Signals (CEC REDWDS) grant program to EVenergi, LLC in the amount of \$119,157 for the installation of 3 (three) electric vehicle charging stations and their associated fleet management software system and free two years subscriptions of charging Management Solutions Software in the amount of \$119,157. The software loaded on each electric vehicle charger is designed to monitor and manage the power output of each electric vehicle charger based on information around battery state-of-charge and electric utility rates and power capacity. In addition, for CEC grant requirements, analysis will be performed on data such as: power output, energy transferred, vehicle mileage, and dates and times of vehicle charging.*

**B. Authorized Use:** The software will be available to PWA Equipment Service's Division managers to monitor electrical load and vehicle usage.

**C. Data Collection**

- Charger controls
- Smart charging
- Alerts and notifications
- Energy management
- Data aggregation/reporting
- Monitoring/UI

**D. Data Access:**

Only authorized users from EVenergi's team who signed data confidentiality and non-disclosure agreements with the California Energy Commission (CEC) will be able to access data from the software.

**E. Data Protection**

Data is encrypted at rest and in transit with TLS 1.2 encryption. Authorized users have unique log-in and passwords providing unique user access. EVenergi is SOC2 compliant.

**F. Data Retention**

Data retention will align with CEC requirements of three (3) years. After that period, EVenergi will delete the data as per its Data Disposal Procedure. This Procedure outlines steps taken after a customer's contract or agreement has expired (in this case, once the CEC retention period ends). In all cases, data deletion is performed

securely, such that the data cannot be recovered. The specific deletion method may vary based on the storage medium used.

**G. Public Access**

The public cannot access the data or software.

**H. Third Party Data Sharing**

Data will only be shared with the CEC as requested by the CEC. Any public facing data, either disaggregated or aggregated, will be anonymized. No other city department or division other than PWA, Equipment Services Division will be provided access.

**I. Training**

EVenergi will provide software training for authorized users from the City, as well as an electronic manual.

**J. Auditing and Oversight**

The City will assign a project manager who will have administrative rights and access to the software. The project manager will be able to review and control the list of authorized users, as well as their level of access/responsibility (i.e., read-only, edit, full access, etc.). As requested, from time to time, the project manager may request logs to ensure compliance with the City's Surveillance Policy to ensure only authorized users have accessed the software.

**K. Maintenance**

At six month intervals, the Project Manager will review access logs to ensure compliance with the City's Surveillance Policy.

12/12/2024 11:31:04

APPROVED AS TO FORM AND LEGALITY

*Farrah Hussein*  
CITY ATTORNEY'S OFFICE

**OAKLAND CITY COUNCIL**  
**RESOLUTION NO. 90633 C.M.S.**

---

**RESOLUTION:**

**(1) AUTHORIZING THE CITY ADMINISTRATOR TO ACCEPT AND ENTER INTO A GRANT AGREEMENT WITH THE METROPOLITAN TRANSPORTATION COMMISSION (MTC) GRANT PROGRAM IN THE AMOUNT UP TO TWO HUNDRED FIFTY THOUSAND FOR (\$250,000), TO PROVIDE TECHNICAL PLANNING ASSISTANCE FOR CITY'S FLEET ELECTRIFICATION ASSESSMENTS; AND**

**(2) ADOPTING APPROPRIATE CALIFORNIA ENVIRONMENTAL QUALITY ACT (CEQA) FINDINGS**

**WHEREAS**, per City Resolution No. 77842 C.M.S., adopted on June 3, 2003, that City of Oakland will develop and implement "Green Fleet" policy and directed the staff to purchase vehicles powered by alternative fuels whenever possible, and actively pursue federal, state, and other incentive program related to clean air and energy efficiency; and

**WHEREAS**, per City Resolution 88268 C.M.S., adopted on July 28, 2020, that City shall establish goal to achieve community-wide carbon neutrality no later than 2045; and

**WHEREAS**, City Resolution 90511 C.M.S., was adopted on November 12, 2024, to accept grant from Pacific Gas & Electric (PG&E) for the upgrading EV charger's infrastructure and Resolution 90576 C.M.S. was adopted on December 17, to accept \$2,300,000 grant fund from California Energy Commission (CEC) for installation of 100 EV chargers throughout the City, these resolutions build on the City's longstanding commitment to fleet electrification and its 'Green Fleet' policy, as established in Resolution 77842 C.M.S."; and

**WHEREAS**, with 1,570 on-road vehicles in the City's fleet in its fleet and five fleet sites, fleet electrification planning, such as assessing fleets, fleet replacement options, fueling and charging needs, infrastructure siting, costs and impacts, and transition actions are necessary; and

**WHEREAS**, Oakland Public Work has been awarded planning technical assistance grant in the amount up to \$250,000 by the Metropolitan Transportation Commission (MTC), Local Public Fleet Electrification Planning Technical Assistance Program; and

**WHEREAS**, the Metropolitan Transportation Commission will administer consultant service contracts and will incur 100% of the consulting cost up to \$250,000; and

**WHEREAS**, the acceptance of this grant will provide City technical planning assistance up to \$250,000, does not require a matching fund and has no impact on the City's budget; and

**WHEREAS**, the technical planning assistance provided by the MTC grant will support the City's equitable climate goals by improving air quality, reducing greenhouse gas emissions, and advancing environmental justice for Oakland residents, particularly in historically underserved communities; and

**WHEREAS**, staff recommends that the City Administrator be authorized to accept and enter into a grant agreement with the Metropolitan Transportation Commission (MTC) in an amount up to (\$250,000), to provide technical planning assistances for city's electrification assessments; now, therefore, be it

**RESOLVED:** That the City Council authorizes the City Administrator, or designee, to accept and participate in the Metropolitan Transportation Commission (MTC) grant program in an amount up to (\$250,000), to provide technical planning assistances for city's electrification assessments; and, be it

**FURTHER RESOLVED:** That the grant does not require a matching fund or new budget appropriation; and be it

**FURTHER RESOLVED:** That this action is exempt from California Environmental Quality Act ("CEQA") based on the following CEQA Guidelines Sections: Section 15060(c)(2) (No Direct or Reasonably Foreseeable Indirect Physical Change in the Environment); Section 15061(b)(3) (No Significant Effect on the Environment); Section 15301 (Existing Facilities); Section 15304 (Minor Alterations to Land); Section 15307 (Protection of Natural Resources); Section 15308 (Protection of the Environment); and Section 15309 (Inspections), each of which provides a separate and independent basis for CEQA clearance and when viewed collectively provide an overall basis for CEQA clearance. The project, as designed, that will benefit from this grant funding involves minor public or private alterations to the condition of existing facilities through the addition of electric vehicle charging stations throughout the City. The project also serves to protect the City's and region's environment and natural resources through the production and use of alternative sources of energy other than fossil fuels; and be it

**FURTHER RESOLVED:** That City Administrator or designee is authorized to act as an agent to conduct all negotiations and related actions and to sign all applications and agreements that may be necessary for the acceptance or extension of the MTC Local Public Fleet Electrification Planning Technical Assistance grant program; and be it

**FURTHER RESOLVED:** That all contracts issued hereunder shall be reviewed and approved by the City Attorney for form and legality and copied shall be placed on file in the City Clerk's Office; and be it

**FURTHER RESOLVED:** That the City Administrator, or their designee or successor is, hereby authorized to take any other action consistent with this Resolution and its basic purpose.

IN COUNCIL, OAKLAND, CALIFORNIA, **FEB 18 2025**

PASSED BY THE FOLLOWING VOTE:

AYES – BROWN, FIFE, HOUSTON, KAPLAN, RAMACHANDRAN, UNGER, AND  
PRESIDENT PRO TEMPORE GALLO **-7**

NOES –

**1** ABSENT – COUNCIL MEMBER JENKINS (serving as Mayor pursuant to Chapter Section 303)

ABSTENTION –

ATTEST:



ASHA REED

City Clerk and Clerk of the Council of the  
City of Oakland, California