CITY OF OAKLAND

Privacy Advisory Commission

July 8, 2019 5:00 PM
Oakland City Hall
Hearing Room 2
1 Frank H. Ogawa Plaza, 1st Floor
Special Meeting Agenda (in lieu of July 4th Meeting)

***Commission Members**: **District 1 Representative**: Reem Suleiman, **District 2 Representative**: Chloe Brown, **District 3 Representative**: Brian M. Hofer, **District 4 Representative**: Lou Katz, **District 5 Representative**: Raymundo Jacquez III, **District 6 Representative**: Gina Tomlinson, **District 7 Representative**: Robert Oliver, **Council At-Large Representative**: Henry Gage III, **Mayoral Representative**: Heather Patterson*

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.

1. 5:00pm: Call to Order, determination of quorum

2. 5:05pm: Open Forum/Public Comment

3. 5:10pm: Review and approval of the draft June 6 meeting minutes

4. 5:15pm: OPD presentation of Joint Terrorism Task Force Annual Report (2018) – review and take possible action.

5. 5:25pm: IT Department presentation of Online Privacy and Security Policy – review and take possible action.

6. 5:40pm: Surveillance Equipment Ordinance – OPD - ShotSpotter technology Impact Report and proposed Use Policy – review and take possible action.

7. 6:20pm: Surveillance Equipment Ordinance – OPD – Remote Camera Impact Report and proposed Use Policy – review and take possible action.

8. 7:00pm: Adjournment

CITY OF OAKLAND

Privacy Advisory Commission

June 6, 2019 5:00 PM
Oakland City Hall
Hearing Room 1
1 Frank H. Ogawa Plaza, 1st Floor
Meeting Minutes

***Commission Members**: **District 1 Representative**: Reem Suleiman, **District 2 Representative**: Chloe Brown, **District 3 Representative**: Brian M. Hofer, **District 4 Representative**: Lou Katz, **District 5 Representative**: Raymundo Jacquez III, **District 6 Representative**: Gina Tomlinson, **District 7 Representative**: Robert Oliver, **Council At-Large Representative**: Henry Gage III, **Mayoral Representative**: Heather Patterson*

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.

1. 5:00pm: Call to Order, determination of quorum

Members Present: Suleiman, Hofer, Katz, Tomlinson, Oliver, Gage.

2. 5:05pm: Open Forum/Public Comment

There were no public speakers.

3. 5:10pm: Review and approval of the draft May 2 meeting minutes

The May Minutes were approved with 5 ayes and 1 abstention.

4. 5:15pm: Surveillance Equipment Ordinance – SST, Inc. presentation on ShotSpotter technology

The PAC received a presentation from ShotSpotter Inc. (attached) that described the company's goals of accurately identifying when a gun is fired while still protecting privacy. The presentation highlighted changes that have been implemented in the past several years to address privacy concerns; for example, the company's sensor microphones are not able to be listed to in real time—they are only triggered when a shot is detected. Also, there no longer is any live stream ability from the sensors and data is retained for only 72 hours to give law enforcement the opportunity to review when an actual incident occurred.

Member Tomlinson had questions about the storage of data, whether it's a third-party vendor and whether it is cloud based. Member Gage asked about how the company got to a higher accuracy rate (90%) considering past performance when other loud noises would trigger the sensors.

There were two Public Speakers: Michael Katz-Lacabe had questions about two factor authentications, how computer "learning" has improved the system, and about the90% accuracy rate.

Tracey Rosenberg cited a letter she submitted to the PAC about a civil case, Simmons v. Rochester NY in which Shot Spotter has been accused of providing false information to corroborate a police department's claim that a suspect (now plaintiff) shot at police before they shot back. In the case, the plaintiff was acquitted after being shot three times and imprisoned for over a year. Ms. Rosenberg notes that Shot Spotters alleged fabrication of evidence is reason to give pause to entering into a contract with them. also, she suggests adding language into a Use Policy that addresses the vendors communication with OPD.

5. 5:45pm: Surveillance Equipment Ordinance – OPD - ShotSpotter technology Impact Report and proposed Use Policy – review and formation of ad hoc work group. No action on the use policy will be taken at this meeting.

This item was combined with Item 4; an ad hoc group will review and bring back recommendations on a Shot Spotter policy.

6. 6:00pm: Surveillance Equipment Ordinance – DOT - Mobility Data Sharing Impact Report and proposed Use Policy – review and take possible action.

This Impact Statement and Use Policy were presented to the PAC by the Department of Transportation and approved unanimously and forwarded to Council. The PAC was very pleased with the submittal for addressing all of the issues raised in the Surveillance Technology Assessment Questionnaire.

7. 6:30pm: Surveillance Equipment Ordinance – OPD – Remote Camera Impact Report and proposed Use Policy – review and formation of ad hoc work group. No action on the use policy will be taken at this meeting.

This item was continued to July.

8. 7:00pm: Adjournment

CITY OF OAKLAND

MEMORANDUM

TO: Privacy Advisory Commission

FROM: Anne E. Kirkpatrick, Chief of Police

SUBJECT: OPD – FBI 2018 Joint Terrorism Taskforce (JTTF) Annual Report

DATE: June 28, 2019

EXECUTIVE SUMMARY

Ordinance No. 13457 C.M.S. approved by the City Council on October 3, 2017, adds Chapter 9.72.010 to the City of Oakland Municipal Code (OMC) concerning "Law Enforcement Surveillance Operations." OMC 9.72.010 requires that, among other requirements, that by January 31 of each year, the Chief of Police shall provide to the Privacy Advisory Commission (PAC) and City Council, a public report with appropriate public information on the Police Department's work with the Federal Bureau of Investigation (FBI) Joint Terrorism Task Force (JTTF) or other federal law enforcement agency task force in the prior calendar year. The Oakland Police Department (OPD) has already introduced a draft 2018 FBI JTTF Taskforce annual report to the PAC at its February meeting; this report provides updated information for 2018.

STAFFING, EQUIPMENT AND FUNDING

As of January 1, 2018, (1) one employee (sworn OPD officer) was assigned to the FBI JTTF. The officer was assigned to work a standard regular work week of (40) forty hours per week. This officer is assigned to OPD's Intelligence Unit and has a joint duty of also participating and assisting with the FBI JTTF. The officer's duties and reporting responsibilities depend upon whether there is any active counter-terrorism investigation as well as the current needs and priorities of the OPD Intelligence Unit.

The position is compensated as a regular OPD officer; the FBI does not compensate OPD for this position's salary. The officer position works regular hours: 40 hours per week; 1,920 hours per year (approximately). Any overtime (OT) hours specific to taskforce operations are paid by the FBI - in 2018, the OPD JTTF did not work any OT hours related to JTTF duties.

In 2018, the JTTF Officer was on special loan from the Intelligence Unit and assigned to the Bureau of Services for all of 2018; this Officer only participated minimally in JTTF operations (approximately 1-2 times a month).

OTHER RESOURCES PROVIDED

The FBI provided a vehicle, covered all fuel expenditures and allowed access to the FBI JTTF office space and access to FBI data systems. OPD provides the mobile phone used by the Task Force (TF) officer. The officer is not provided with any FBI surveillance equipment.

CASES ASSIGNED TO THE OPD JTTF OFFICER

The JTTF Officer assists the FBI on counter-terrorism cases. In 2018, the OPD JTTF Officer was assigned on special loan to OPD's Bureau of Services (ongoing), and was not assigned to any JTTF Task Force cases as a lead investigator; the limited assistance was due to the OPD JTTF Officer being on special loan away from the JTTF for this year.

The JTTF Task Force Officer was assigned zero (0) cases as lead investigator in 2018. However, the JTTF Officer was assigned to assist on (1) one case, which gained national attention. This was an October 2018 pipe bomb investigation in which Bay Area politicians and members of the media received pipe bombs in the mail. OPD was concerned that local figures in Oakland were also targeted. The OPD JTTF Officer coordinated with the Task Force on investigations (the Task Force determined that no Oakland based officials were targeted, and this information was relayed to City officials)[1]

A past-year example provides context to the nature of OPD's FBI JTTF Task Force. This example is provided as 2018 is the first year for OPD to provide annual reports to the PAC. In 2016 the Task Force investigated the case leading to the arrest of Amer Alhaggagi. The investigation revealed that Alhaggagi planned to: 1) set fires in the hills of Berkeley; 2) strategically place backpack bombs in various public areas around downtown Oakland; 3) sell cocaine laced with rat poison at bars and clubs in Oakland and Berkeley; and 4) detonate a car bomb at a gay nightclub in San Francisco. The FBI learned that in July of 2016, Alhaggagi had applied to the Oakland Police Department for a position as a police Officer. The Oakland JTTF Officer assisted the FBI in identifying Alhagaggi as the subject. Ultimately, the FBI was able to safely arrest him. Alhaggagi was sentenced to 15.5 years' imprisonment because of his conviction on the above-mentioned criminal activity.

"Duty to Warn" is identified as the "requirement to warn U.S. and non-U.S persons of impending threats of intentional killing, serious bodily injury, or kidnapping".[2] The JTTF Officer participated in zero (0) duty to warn cases.

There were zero (0) cases in 2018 where OPD declined to participate after FBI request. The FBI knows that OPD task force officers must comply with all Oakland laws and policies. Furthermore, the FBI commonly works with different jurisdictions and understands that taskforces must collaborate with the particular polices and laws of those jurisdictions.

UNDERCOVER OPERATIONS AND INTERVIEWS

In 2018, the OPD JTTF Officer did not conduct any undercover operations or interviews (JTTF interviews are normally conducted by FBI Agents) - zero (0) were conducted.

In 2018, the OPD JTTF Officer did not take part in any interviews (voluntary or involuntary) - zero (0) were conducted.

In 2018, the OPD JTTF officer did not conduct any assessments - zero (0) assessments conducted. Generally, unless someone were to come to the OPD to report a threat, all assessments begin with

[1] This case occurred before 2018 (the year of this annual report). OPD is including this past information because 2018 is the first reporting year; past information is provided for context as to relevant work related to the JTTF TF.
[2] FBI Duty to Warn – Intelligence Community Directive 191: https://fas.org/irp/dni/icd/icd-191.pdf

the FBI. Procedurally, FBI is notified and an assessment is opened and FBI will then forward the assessment to specific agents.

The OPD JTTF officer does not manage any informant relationships. In 2018, there were zero (0) informant's managed by OPD JTTF. Furthermore, the Intelligence Unit is the Informant Program Coordinator for all OPD informants. A file check was conducted on the JTTF Officer and there were zero (0) informant relationships related to the JTTF[3].

There were no situations in 2018 where the officer conducted undercover operations or managed informants. There were no requests from outside agencies (e.g. Immigration and Customs Enforcement or "ICE") for records or data of OPD. There were no cases where the Task Force Officer was involved or aware of asking an individual's U.S. Person (residency) status. Furthermore, it is OPD Policy that OPD shall not inquire about a citizen's residency status

The FBI is aware of requirements mandated of OPD and its protocols for undercover operations and interviews; the Task Force Officer was always held responsible for following all sworn officer policies and standards.

TRAINING AND COMPLIANCE

The OPD JTTF Officer follows all OPD policies and receives several police trainings, including but not limited to: continual professional training, procedural justice, and annual firearms training. The Officer has also reviewed all provisions of the JTTF MOU. The JTTF Officer as well as supervisor are held responsible by OPD for compliance with all applicable Oakland and California laws.

The OPD JTTF Officer supervisor (Intel Sergeant) conducts mandatory bi-weekly meetings with the officer. Daily and weekly meetings are also held when critical incidents occur.

ACTUAL AND POTENTIAL VIOLATIONS OF LOCAL/STATE LAW

The JTTF OPD Officer had no violations of local, California, or Federal law. OPD Command consults with the Office of the City Attorney to ensure that all polices conform with State and Federal laws. Furthermore, a file check was conducted on the OPD JTTF Officer's complaint history in 2018 and there were zero (0) zero complaints against the officer.

SUSPICIOUS ACTIVITY REPORTING (SARs) and NORTHERN CALIFORNIA REGIONAL INTELLIGENCE CENTER (NCRIC)

OPD submits Suspicious Activity Reports (SARs) to the Northern California Regional Intelligence Center (NCRIC). These reports contain information regarding activity, such as, but not limited to: narcotics, cyber-attacks, sabotage, terrorism threats, officer safety, and human trafficking. NCRIC provides a secure online portal where police agencies can provide this information. NCRIC has shared with OPD that providing false or misleading information to NCRIC is a violation of Federal Law and may be subject to prosecution under Title 18 USC 1001. The JTTF is a recipient of SAR information. The OPD JTTF Officer submitted zero SARs to NCRIC during the 2018 calendar year.

[3] Identities of any informant would never be released to the public as such information is may be dangerous for the life of the informant.

It is unknown how many SAR's OPD Officers received during 2018 as there is no current tracking system.

COMMAND STRUCTURE FOR OPD JTTF OFFICER

The OPD JTTF Officer works under the command structure of OPD; the OPD JTTF Officer reports directly to the OPD Intelligence Unit Supervisor (Sergeant). The Officer also coordinates with the FBI Supervisor, who is also serves as a Counterterrorism Assistant Agent.

Respectfully submitted,

Anne E. Kirkpatrick,
Chief of Police

Reviewed:
Bruce Stoffmacher, Acting Police Services Manager
OPD, Research and Planning Unit, Training Division

Prepared by:
Omar Daza-Quiroz, Sergeant of Police
OPD, Intelligence Unit

Online Privacy and Security Policy

Section A. Introduction

Thank you for visiting the City of Oakland's Web site (http://www.Oaklandnet.com) and reviewing our Privacy and Security Policy. This policy addresses collection, use and security of and access to information that may be obtained through use of Oaklandnet.com. It is provided for informational purposes only. The information presented here is not meant to be a contract of any type, either express or implied, and should not be treated as such by site visitors. The information in this statement and/or the policies described here may change at any time, without prior notice to any visitor.

This notice covers the following topics:

Section B. Information Collected and How it is Used

Information collected if you only browse this site.

If you do nothing during your visit to our web site but browse, read pages, or download information, we will gather and store certain information about your visit. This information does not identify you personally. We automatically collect and store the following information about your visit:

1. The Internet Protocol Address and domain name used. The Internet Protocol address is a numerical identifier assigned either to your Internet service provider or directly to your computer. We use the Internet Protocol Address to direct Internet traffic to you. This address can be translated to determine the domain name of your service provider (e.g. xcompany.com or yourschool.edu). Generally, the City only determines visitor domain names if a security issue is suspected;
2. The type of browser and operating system you used;
3. The date and time you visited this site;
4. The web pages or services you accessed at this site; and
5. The web site you visited prior to coming to this web site.

Information is collected for statistical purposes and to help the City manage the site. The City's web site uses software programs to create summary statistics, which are used for such purposes as assessing what information is of most and least interest, determining technical design specifications, and identifying system performance or problem areas.

For site security purposes and to ensure that this service remains available to all users, the City's web site employs software programs to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage. Except for authorized law enforcement investigations and the security purposes mentioned elsewhere in this notice, no other attempts are made to identify individual users or their usage habits. Raw data logs are used for no other purposes and are scheduled for regular destruction in accordance with public records retention schedules.

What we collect if you volunteer information.

If during your visit to our web site you participate in a survey, send an e-mail, participate in a City hosted mailing list or web-based discussion, or perform some other transaction online, the following additional information will be collected:

1. The e-mail address, and contents of the e-mail, for those who communicate with us via e-mail or who participate in a City hosted mailing list or web-based discussion.
2. Information volunteered in response to a survey.
3. Information volunteered through an online form for any other purpose.
4. Information volunteered by participating in an online transaction with the City.

The information collected is not limited to text characters and may include audio, video, and graphic information formats you send us.

We use your e-mail address to respond to you. It is the City's Policy to not use your e-mail address to send you unsolicited e-mail unless you specifically elect to receive it. Survey information is used for the purpose identified by the survey. Information from other online forms is used only for conducting City business related to the online form.

Information provided for a transaction is used only for the purpose of completing and recording the transaction. Information requested will be no more specific than if a visitor were engaging in the transaction by other means, including by telephone or in-person while visiting a City facility. In all cases, the City strives to collect the minimum information necessary to comply with applicable law or provide the service requested.

The City does not sell, rent or otherwise distribute visitor's information, including electronic mail addresses, to any outside company or organization, unless legally required to do so. This applies to information that may be collected on the City's site and on that of any third party with whom the City contracts to provide Internet related services.

Section C. Personal Information and Choice

You may choose whether to provide personal information online.

"Personal information" is information about a natural person that is readily identifiable to that specific individual. Personal information includes such things as an individual's name, address, and phone number. A domain name or Internet Protocol address is not considered personal information.

We collect no personal information about you unless you voluntarily provide it to us by sending us e-mail, participating in a survey, completing an online form, or engaging in an online transaction. You may choose not to contact us by e-mail, participate in a survey, provide personal information using an online form, or engage in an electronic transaction. However, some information available through this site is specific to individual users. Visitors interested in viewing this user specific information are requested to sign up for a password-protected account. Your choice to not participate in these activities will not impair your ability to browse, read, or download general information provided on the site. Information protected on this site by a password, which is subject to disclosure, may be obtained by contacting the City directly.

If personal information is requested on the web site or volunteered by the user, state law and the federal Privacy Act of 1974 may protect it. However, this information is treated like any other information provided to the City, and may be subject to public inspection and copying if not protected by federal or state law.

If you believe that your personal information is being used for a purpose other than what was intended when submitted, you may contact the person identified in the Contact Information Section of this statement.

Users are cautioned that the collection of personal information requested from or volunteered by children online or by e-mail will be treated the same as information given by an adult, and may be subject to public access.

Section D. Public Access to Information

In the State Of California, Public Disclosure laws exist to ensure that government is open and that the public has a right to access appropriate records and information possessed by City government (The State of California Public Records Act or “CPRA”). At the same time, there are exceptions to the public's right to access public records that serve various needs including the privacy of individuals. Both state and federal laws provide exceptions. The CPRA requires the disclosure of all public records unless a particular record (or particular information contained in a record) is specifically exempt under the CPRA or other applicable law. For example, there is no categorical exemption for residential telephone numbers, residential addresses, or personal e-mail addresses. However, the CPRA does not require the disclosure of "credit card numbers, debit card numbers, electronic check numbers, card expiration dates, or bank or other financial account numbers supplied to [the City] for the purpose of electronic transfer of funds, except when disclosure is expressly required by law".

The CPRA does not authorize the City to give, sell, or provide access to lists of individuals to entities seeking to use the lists for commercial purposes. City practice is to require those who request lists of individuals to sign an affidavit stating that they do not have a commercial purpose (such as contacting those on the list to propose a commercial transaction). However, the City cannot guarantee that a requester will not, despite signing such an affidavit, contact individuals on the list for a commercial purpose.

In the event of a conflict between this Privacy Notice and the Public Records Act or other law governing the disclosure of records, the Public Records Act or other applicable law will control.

Section E. Review and Correction of Personally Identifiable Information

You can review any personally identifiable information we collect about you by using the information in the Contact Information section at the end of this Notice. You may recommend changes to your personally identifiable information you believe to be inaccurate by submitting a request that credibly shows the inaccuracy. We will take reasonable steps to verify your identity before granting access or making corrections.

Section F. Use of Cookies and Applets

"Cookies" are simple text files stored on your computer by your web browser. The City's policy is to limit the use of cookies. However, some of the applications the City builds and purchases utilize cookies to confirm the integrity of online transactions. Cookies used in this manner do not contain personally identifiable information.

Applets are tools downloaded to your computer to work with the software you have. Applets are intended to enhance your browsing experience by enabling you to view information in a unique manner or enable access to information that your computer would otherwise be unable to access without the applet. The City does not currently use applets. If the decision is made to utilize applets users of the City's web site would not be required to use them.

Section G. Security

The City has taken several steps to safeguard the integrity of its data and prevent unauthorized access to information it maintains, including but not limited to authentication, monitoring, auditing, and encryption. Security measures have been integrated into the design, implementation and day-to-day practices of the entire operating environment as part of its continuing commitment to risk management. These measures are designed and intended to prevent corruption of data, block unknown or unauthorized access to our systems and information, and to provide reasonable protection of private information in our possession.

This information should not be construed in any way as giving business, legal, or other advice, or warranting as fail proof, the security of information provided via the City's web site.

Unauthorized attempts to upload information or change information on this service are strictly prohibited and may be punishable under the state Computer Trespass law and federal statutes including the Computer Fraud and Abuse Act of 1986 and the National Information Infrastructure Protection Act.

Section H. Electronic Commerce

Increasingly, you have the option to do business with the City over the Web including making electronic payments for goods and services. Such transactions are allowed only under tightly controlled circumstances, where there are appropriate technological and other safeguards in place to protect financial and other sensitive data.

The provision of this information shall not be construed in any way as giving business, legal, or other advice, or warranting as fail-proof, the security of information provided via the City's web site.

Section I. Avoiding Internet Fraud

Fraudulent scams called "phishing" have been increasing in frequency. "Phishing" involves a victim receiving an e-mail appearing to be from a legitimate business. The "from" line is often forged and the e-mail usually contains authentic looking graphics making it appear to be legitimate. The e-mail may also contain what appears to be a legitimate link to that organization, e.g., http://www.oaklandnet.com. When the victim clicks on this link, they are then taken to what appears to be a legitimate looking website. Criminals can even make your browser's address bar contain the address of the legitimate organization despite the fact that the website is a forgery. Victims are then encouraged to enter personal information including credit card numbers and expiration dates.

It is the City's policy never to request confidential personal or financial information from our customers via an unsolicited e-mail. The City will also never send you an unsolicited e-mail containing a link to a City website where confidential personal or financial information is requested. If you receive such an e-mail, purportedly from the City, you are encouraged to immediately contact the.

For more general information about "phishing" visit the Federal Trade Commission web site. For specific information about a suspected phishing attempt you may have received contact the organization represented in the suspect e-mail.

Section J. Disclaimer

The City's web site has many links to other web sites. These include links to web sites operated by other government agencies, nonprofit organizations and private businesses. When you link to another site, you are no longer on the City's web site and this Privacy Notice will not apply. When you link to another web site, you are subject to the privacy policy of that new site. Visitors linking to another site are encouraged to examine the privacy policy of that site.

Neither the City, or any department, officer, or employee of the City warrants the accuracy, reliability or timeliness of any information published by this system, nor endorses any content, viewpoints, products, or services linked from this system, and shall not be held liable for any losses caused by reliance on the accuracy, reliability or timeliness of such information. Portions of such information may be incorrect or not current. Any person or entity that relies on any information obtained from this system does so at their own risk.

Section K. Contact Information

The City government is made up of several departments. Each department is responsible for the applications it develops including applications that may gather personally identifying information that you volunteer.

To access your personally identifiable information collected, if any, or request correction of factual errors in your personally identifiable information, contact the Department that requests the information. Contact information can be found on the department's web page.

To offer comments about the information presented in this Privacy Notice, you can contact:

By e-mail: KBoyd@oaklandnet.com
By telephone: (510) 238-6365

OAKLAND POLICE DEPARTMENT

Surveillance Impact Use Report for the Gunshot Location Detection System

1. Information Describing the Gunshot Location Detection (GLD) System and How It Works

The Oakland Police Department (OPD)'s GLD system employs acoustic sensors which are strategically placed in specified areas. Currently, OPD contracts with ShotSpotter, Inc., the creator of the ShotSpotter® Flex™ system "Shotspotter." The GLD system sensors are designed to record and recognize gunshots based on their high-frequency impulsive sound and acoustical signature (120 decibels or higher pitch). The utilization of multiple sensors allows the system capture the sound and acoustical signature from different angles (minimum of three sensors) and thus to pinpoint a gunfire location; the sensors then send the audio recording and location data to the "Shotspotter Cloud" for gunshot verification; Shotspotter uses computer-learning algorithms and then human analysts (two phase authentication) to verify gunshot occurrences. Verified gunshots and related information are then quickly sent from the Shotspotter Cloud to the OPD Communications Division and police vehicle terminals (within 60 seconds; 29 seconds on average) so that Communications may notify responding personnel (and personnel can use vehicle computers) of where gunshots were recently fired.

The GLD System also consists of a cloud-based portal accessible via patrol and OPD computers, and desktop applications. Officers or other authorized personnel can receive real-time gunshot notification when logged into the system (in addition to receiving notification from OPD Communications). Authorized personnel (crime analysts) use the desktop applications that connect to the Shotspotter system for more in-depth gunshot pattern analysis.

2. Proposed Purpose

Hundreds of gunshots occur each month in Oakland; in September 2018 alone the system logged 395 total incidents (275 multiple gunshots, 92 single gunshots, and 28 possible gunshots). Fortunately, many gunshots do not lead to actual gunshot victims, although sometimes there are gunshot victims. The gunshot data suggests that when there are witnesses who call 911 to report gunshots, the locations provided by witnesses are often inaccurate. Also, witnesses for whatever reason to do not always notify OPD of their

occurrence; other times there are witnesses. The GLD system allows OPD to become aware in real-time of gunshots when they occur – where they actually occur - when within range of installed GLD system sensors. OPD Communications receive verified gunshot information and can notify officers to respond and officers can directly receive gunshot notifications from their vehicle terminals. 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.

3. Locations Where, and Situations in which GLD System may be deployed or utilized.

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 15.38 square miles or approximately 25 percent of the City. 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. Officers and authorized personnel after receiving OPD training are authorized to access the GLD system in patrol vehicles throughout the City.

4. Impact

GLD SYSTEM technology helps OPD personnel to leverage their street presence and vehicle mobility to respond directly to gunshots without waiting for the public to call 911 and report gunshots. The GLD system helps OPD both as a crime fighting tool and as a community partnership building resource. The GLD system has two major components: 1) Gunshot Notifications (ShotSpotter Flex™ Alert); and 2) Investigative Component (ShotSpotter Flex™ Investigator Portal). The ShotSpotter Flex instantly notifies officers (logged into the system) of gunshots in progress with real-time data delivered to the OPD Communications Section and patrol vehicles. This service enhances officer safety and effectiveness through:

- Real-time access to maps of shooting locations and gunshot audio;
- Actionable intelligence detailing the number of shooters and the
- number of shots fired;
- Pinpointing precise locations for first responders to aid victims,
- search for evidence, and to be able to know where to find witnesses; and
- real-time email notifications of detected activations with shooting location maps and associated audio.

OPD personnel can also utilize GLD system data to know where exactly to attempt to engage neighbors in areas where shots are being fired. Officers use this information to ask community members what they know related to

Comment [RH1]: Ordinance requires "crime statistics for any location(s)."

Comment [RH2]: From the Ordinance- Impact: an assessment of the technology's adopted use policy and whether it is adequate in protecting civil rights and liberties and whether the surveillance technology was used or deployed, intentionally or inadvertently, in a manner that is discriminatory, viewpoint-based, or biased via algorithm;

shots being fired. These initial meetings related to gunfire also serve as starting points for greater contact between residents and OPD officers.

The GLD (Shotspotter) Investigator Portal (IP) provides the OPD Criminal Investigations Division (CID) with historical data for gunshot spatial analysis. This analysis provides CID analysts with a tool for the development of proactive policing strategies - directed patrols can focus in areas where gun fire is habitually detected.

Historic gun crime data (e.g. homicides and strong-arm robberies) already provide OPD personnel with data that suggests where future gun-related crimes are likely to occur – OPD uses this data to focus resources towards high priority areas for a greater police presence. The GLD system provides responding personnel with much more exact data. Therefore, the GLD system does not directly lead to a broader policing footprint. Rather, the GLD system allows personnel to use more intelligence-based policing and respond directly to exact areas where police are needed to find the individuals engaged in gun crimes as well as to respond to the victims of such crimes. The GLD system actually helps OPD to lessen the police patrol presence in parts of the city that already receive a greater policing footprint, by responding more to exact locations that need an immediate police response.

Although rare, GLD system recordings may record human voices even though the system is calibrated to focus on high-pitch gun shot frequencies. The sensors are constantly recording and then deleting the data after 72 hours, unless triggered to send the data to Shotspotter HQ for analysis of a possible gunshot. The sensors truncate the data to a few seconds before to a few seconds after the gunshot sound incident – otherwise street atmosphere sounds are deleted. For a human voice to be both recorded and heard by a human analyst during the verification process, the voice would have to be close enough to a sensor to be recorded, and the utterance would have to occur during the triggering incident.

OPD cannot draw direct causal relationships between the GLD system and gun crime activity. However, OPD's Ceasefire Unit (focused on diminishing the prevalence of gunshot activity) sees correlations between the use of the GLD system and gunshot activity; in 2014 there were 420 incidents of Assault with a firearm (criminal code 245(a)(2)PC)); 2015 saw 342 incidents; 2016 saw 331 incidents; 2017 saw 281 incidents and 2018 saw 277 incidents – a consistent five year decrease.

Deleted: data

Deleted: y

Comment [RH3]: We began using ShotSpotter in 2006. Why starting here with 2014?

Comment [RH4]: Maybe use/move up above to "Locations"? Are these stats citywide or beat/Police Area specific?

5. Mitigations

OPD, in partnership with Shotspotter (GLD system provider) has developed protocols to ensure that the GLD system does not overly burden the public's right to privacy. OPD DEPARTMENTAL GENERAL ORDER (DGO) "I-20 Gunshot Location Detection System" Section B "General Guidelines" explains that:

- Only authorized users may access the GLD system;
- No one may access the system without training;
- Only specifically authorized personnel authorized by the Chief or Chief-designee (e.g. personnel with OPD's Ceasefire Unit and CID crime analysts) will have access to historical GLD system data via desktop GLD system applications.

(DGO) "DGO I-20 Section D "Training" explains that:

Training requirements for employees authorized to use the GLD system include completion of training by the GLD System Coordinator or appropriate subject matter experts as designated by OPD. Such training shall include:

- Applicable federal and state law
- Applicable policy
- Memoranda of understanding
- Functionality of equipment
- Accessing data
- Safeguarding password information and data
- Sharing of data
- Reporting breaches
- Implementing post-breach procedures

Section 4 above (Impact) explains that the GLD system recordings, "may record human voices even though the system is calibrated to focus on high-pitch gunshot frequencies." The Impact Section explains that the GLD System only records a few seconds related to the actual gunshot. Shotspotter sensors send sound files consisting of two seconds before the acoustic incident and up to four seconds after the incident. The system can only send these short sound segments from sensors to the Shotspotter Cloud when three or more sensors record the impuslve sounds indicative of gunshot sound signatures. This hard-coded function of the GLD system helps to ensure that only very short segments of human voice are ultimately recorded and archived into the GLD system. Furthermore, most sensors are placed approximately 30 feet above ground level to maximize sound triangulation; at this altitude, the sensors can only record limited street-level human voice sounds. Furthermore, the one-way sound transmission from the sensors to the Shotspotter Cloud limits the possibility of recording actual conversations; Shotspotter and OPD only receive audio recordings of the impulsive sounds two seconds prior and up to four seconds after the impulsive sound event. The sensors are not enabled for audio streaming – neither ShotSpotter nor OPD can listen in on street level sounds in real-time.

The sensors are constantly recording a total of 72 hours, and then deleting the data unless triggered to send the data to the Shotspotter Cloud for

Comment [RH5]: What fed/state laws apply? What policies apply?

Comment [RH6]: This sentence implies human voices are always recorded and/or part of every snippet, which is untrue. What did you intend to say?

Deleted: altitude

Deleted: ;

analysis – the 72 hour buffer allows OPD to request data within the 72 limit in cases where gunshots have been registered and there is a need to verify if there were other gunshots prior to the authenticated event; Shotspotter policy stipulates that only specific support engineers can use a technology to access the 72 buffer in the sensors to retrieve prior recorded data and search for other gunshot impulsive sound events (this feature is useful when CID investigators need to search for previous gunshots). The sensors truncate the data to a few seconds before to a few seconds after the gunshot sound incident – otherwise street atmosphere sounds are deleted.

6. Data Types and Sources

The GLD system uses acoustical digital data file recordings (.wav files) to send to the Shotspotter Cloud for gunshot frequency verification. Verified gunshot recordings stored on HQ servers can be reviewed by OPD personnel on desktop applications.

Comment [RH7]: From the Ordinance: Data Types and Sources: a list of all types and sources of data to be collected, analyzed, or processed by the surveillance technology, including "open source" data, scores, reports, logic or algorithm used, and any additional information derived therefrom;
(this section should include street noise, automobiles, human voices, etc. as a type of data that may be collected).

7. Data Security

OPD takes data security seriously and safeguards GLD System data by both procedural and technological means. The mitigation section above explains that only authorized and trained personnel will be permitted access to the GLD system. The system always requires user and password ID for login. Furthermore, as explained in the Mitigation Section above, only personnel specifically designated by the Chief or Chief-designee have access to the GLD system desktop applications which provide access to any historical downloadable data.

Comment [RH8]: Form the Ordinance- Data Security: information about the steps that will be taken to ensure that adequate security measures are used to safeguard the data collected or generated by the technology from unauthorized access or disclosure;
(should include info about encryption, private cellular network, etc.)

The GLD technology itself provides many layers of data security. The sensors detect loud high-pitch impulsive sounds; only when such sounds are recorded are audio files captured and sent to HQ and then to OPD; other street sound recordings such as human conversations are thus constantly deleted – audio is deleted from sensors' buffers and permanently deleted within 72 hours. The sensors cannot live stream audio – only audio connected to gunshot-type audio signatures are maintained for data retention. Furthermore, there is no way to tag any conversation that is unintentionally recorded when connected to a gunshot. OPD authorized personnel may find that a voice has been recorded along with gunshot sounds but such voice data is only associated with the actual gunshot data.

Comment [RH9]: What does this mean? You can tag an incident.

8. Costs

OPD entered into the original contract with SST, Inc. in 2006 (Resolution No. 80075 C.M.S.) for the purposes of piloting the gunshot detection system. This initial contract authorized installation of the Shotspotter GLD system in one area of East Oakland for approximately $70,000 per year. In October 2011,

Comment [RH10]: From the Ordinance- Fiscal Cost: the fiscal costs for the surveillance technology, including initial purchase, personnel and other ongoing costs, and any current or potential sources of funding;
(needs more info here)

the City entered into a new contract with SST, Inc (Shotspotter for approximately $84,000 per year. The size and scope of the areas covered by the GLD system has increased such that that system now has 13.68 square miles covered (see Section 3 Areas Covered above). The size and scope results in a large cost – in 2016 the City entered into a new contract for an amount not to exceed $1,637,188 for a three-year (2018-2021) period for the expanded three-phase area.

9. Third Party Depencence

(from the Ordinance-Third Party Dependence: whether use or maintenance of the technology will require data gathered by the technology to be handled or stored by a third-party vendor on an ongoing basis;

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.11" + Indent at: 0.36"

Formatted: Normal, Indent: Left: 0", Right: 0", Space Before: 0 pt, After: 0 pt

Formatted: Font:(Default) Times New Roman, Not Bold

10. Alternatives Considered

OPD officers and investigators rely primarily on traditional members of the public to report gunshot crimes whether or not there are associated gunshot victims. Members of the public, when they witness or hear gunshots (and if they choose to report incidents) often report inaccurate locations. GLD systems have revolutionized real-time intelligence. OPD believes that there is no alternative to a modern GLD system other than having exponentially greater numbers of sworn personnel covering many areas throughout the City and/or using more intrusive forms of recording equipment. Other alternatives would be to continue to rely on less accurate information provided by the public and to have less information about real-time gunshots. These alternatives are not considered useful given the thousands of gunshot incidents which continue to occur each year in Oakland.

11. Track Record of Other Entities

Shotspotter states that it's system is now used in over 90 cities throughout the United States. Cities plagued by high levels of gunshot activity such as Chicago, Washington D.C., Chicago, with the highest municipal homicide rate, cites drops of over 40% in areas where the system has been deployed. Fresno, CA began using the system in 2015, covering 12 square miles of the City. The Pittsburgh, PA Police Department cite evidence that their system has helped them respond to shooting victims in time to rush victims to hospitals and save their lives[1]. The San Diego Police Department also cite evidence that the system allows them to respond much quicker to gunshots in the four areas with systems in which gunshots historically occur more frequently[2]. Cincinnati PD cite ShotSpotter as well as increased gun tracing

Comment [RH11]: From the Ordinance- Track Record: a summary of the experience (if any) other entities, especially government entities, have had with the proposed technology, including, if available, quantitative information about the effectiveness of the proposed technology in achieving its stated purpose in other jurisdictions, and any known adverse information about the technology (such as unanticipated costs, failures, or civil rights and civil liberties abuses).
[no adverse info is provided; ShotSpotter has lost dozens (if not more) of contracts, and the Rochester lawsuit should be mentioned here]

[1] https://www.marketscreener.com/SHOTSPOTTER-INC-35742435/news/Shotspotter-Pittsburgh-police-say-gunshot-sensing-system-helps-save-lives-solve-crimes-26166807/
[2] https://www.nbcsandiego.com/investigations/SDPD-Gun-Shot-Detection-Technology-Led-To-Quicker-Response-

for 47% 2018 decrease in gunshot activity[3].

Times-449630173.html

[3] https://www.wcpo.com/news/crime/shootings-down-nearly-50-percent-in-cincinnati-this-year-police-say

DEPARTMENTAL GENERAL ORDER

I-20: GUNSHOT LOCATION DETECTION SYSTEM

Effective Date: XX Apr 19
Coordinator: Ceasefire Division

The Oakland Police Department (OPD) strives to use technology that promotes accountability and transparency. 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, image, or video data, 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. Purpose.

Comment [RH1]: From the Ordinance- Purpose: the specific purpose(s) that the surveillance technology is intended to advance;

A. Description of the Technology

OPD uses a GLD System (currently the ShotSpotter® Flex™ system, provided by ShotSpotter, Inc. "Shotspotter") 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 quickly notifies Communications of verified gunshot activations, which allows OPD to quickly respond to gunshots and related violent criminal activity.

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 shots fired. The audio triangulation of multiple installed sensors then pinpoints a gunfire location and sends the audio file and triangulation information to Shotspotter Headquarters (HQ) for gunshot verification. Verified gunshots and related information are then sent to Communications in real-time so that Communications 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 cloud-based and desktop-based; OPD authorized personnel can use internet browsers to connect to the Shotspotter system via OPD computers. Certain authorized personnel use desktop applications that connect to the Shotspotter system for more in-depth gunshot analysis.

B. General Guidelines

B – 1. Authorized Users

Personnel authorized to use the GLD system or access information collected through the use of such equipment shall be specifically trained in such technology and authorized by the Chief of Police or designee. Such personnel shall be limited to designated captains, lieutenants, sergeants, officers, police service and/or evidence technicians, and crime analysts unless otherwise authorized.

B – 2. Restrictions on Use

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

2. No member of this department shall operate GLD equipment or access Shotspotter data without first completing department-approved training.

3. Authorized personnel may access the GLD system via vehicle computers and receive notifications of verified GLD activations. OPD Communications may also notify authorized personnel of Shotspotter activations. Authorized personnel may respond to such notifications based upon priorities as mandated by their supervisors.

4. The GLD system shall only be used for official law enforcement purposes.

5. Only specifically authorized personnel authorized by the Chief or Chief-designee (e.g. personnel with OPD's Ceasefire Unit and CID crime analysts) will have access to historical GLD system data via desktop GLD system applications.

The GLD system may be used in conjunction with any routine patrol operation or criminal investigation. Reasonable suspicion or probable cause is not required before using Shotspotter to scan gunshot locations to investigate gunshot evidence and/or related crime scenes.

Comment [RH2]: From the Ordinance - Purpose: the specific purpose(s) that the surveillance technology is intended to advance;
[no need for restrictions to be included – anything not authorized is prohibited]

6. Accessing data collected by the GLD system (currently Shotspotter) 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.

C. Shotspotter Data

C – 1. Data Collection and Retention

GLD system data is currently maintained in perpetuity, both by Shotspotter HQ as well as on OPD's desktop applications. Shotspotter data is not connected to any personal data.

C – 2. Data Security

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

1. Authorized personnel may access the browser-based GLD system via vehicle computers to only access the cloud-based system. Authorized personnel must always gain access through a login/password-protected system which records all login access.

   Only specialized crime analysts and investigators within OPD's Criminal Investigations Division (CID) will be provided access to GLD system desktop applications; desktop applications are only accessible through a login/password-protected system authentication which records all login access.

2. Members approved to access GLD system data under these guidelines are permitted to access the 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.

3. 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. GLD system audits shall be conducted on a regular basis by the Ceasefire Division. The purpose of these audits is to ensure the accuracy of ALPR Information and correct data errors.

C – 3. Releasing or Sharing GLD System Data

GLD system data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law, using the following procedures:

1. The agency makes a written request for the Shotspotter data that includes:

Comment [RH3]: Most of this should go under "Data Access." From the Ordinance - Data Access: the category of individuals who can access or use the collected information, and the rules and processes required prior to access or use of the information;

Comment [RH4]: From the Ordinance- Data Collection: the information that can be collected by the surveillance technology. Where applicable, list any data sources the technology will rely upon, including "open source" data; [this info is missing]

Comment [RH5]: From the Ordinance- Data Retention: the time period, if any, for which information collected by the surveillance technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s), the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond that period; [no justification is provided. Furthermore, this is confusing because "system data" is undefined. OPD does not have access to the sensors. They only receive audio snippets of verified gunshots]

Comment [RH6]: This should be titled "Data Protection." From the Ordinance- Data Protection: the safeguards that protect information from unauthorized access, including encryption and access control mechanisms;

Comment [RH7]: Similar to comment above – this needs to be moved to Data Access.

Comment [RH8]: Need to include "need to know/right to know."

a. The name of the requesting agency.
b. The name of the individual making the request.
c. The intended purpose of 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.

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 Shotspotter in collaboration with OPD. Oversight of the system as well as data retention and access, shall be managed by OPD's Ceasefire Division.

Comment [RH9]: Need to expand a bit. From the Ordinance- Maintenance: The mechanisms and procedures to ensure that the security and integrity of the surveillance technology and collected information will be maintained.

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.

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.

The Shotspotter Coordinator shall provide the Chief of Police, Privacy Advisory Commission, and Public Safety Committee with an annual report that contains following for the previous 12-month period:

1. The number of Shotspotter activations received by the OPD.
2. A list of agencies other than OPD that were authorized to use the equipment.
3. A list of agencies other than the OPD that received information from use of the equipment.
4. Information concerning any violation of this policy.

5. Total costs for maintenance, licensing and training, if any.
6. The results of any internal audits and if any corrective action was taken.

The above information and reporting procedures will assist in evaluating the efficacy of this policy and equipment.

Comment [RH10]: Intended as a supplement to the Ordinance's Annual Reporting requirements?

D – 4. Training

The Training Section shall ensure that members receive department-approved training for those authorized to use or access the Shotspotter system and shall maintain a record of all completed trainings.

Training requirements for employees authorized to use the GLD system include completion of training by the GLD System Coordinator or appropriate subject matter experts as designated by OPD. Such training shall include:

- Applicable federal and state law
- Applicable policy
- Memoranda of understanding
- Functionality of equipment
- Accessing data
- Safeguarding password information and data
- Sharing of data
- Reporting breaches
- Implementing post-breach procedures

Comment [RH11]: What laws and policies are applicable?

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.

Training updates are required annually.

By Order of

Anne E. Kirkpatrick
Chief of Police

Date Signed:

OAKLAND POLICE DEPARTMENT

Surveillance Impact Use Report for Remote and Live-Stream ~~Mobile~~ Camera Systems~~s~~

1. Information Describing Remote and Live-Stream~~Mobile~~ Camera Systems (RLSC)~~s~~ and How They Work

OPD utilizes different types of cameras to capture single image and video data. Cameras that are strictly manually operated are not considered "surveillance technology" under the Oakland Surveillance Ordinance No. 13489 C.M.S. However, some cameras ~~RMCs~~ allow for remote access and/or live-streaming~~real-time remote access viewing~~ of activity. ~~captured by the RMC lens.~~ Single image and video cameras~~RMC~~s may be manufactured with data transmitting technology or be outfitted by OPD with separate camera transmitters. Remote-control functions allow personnel to observe and/or record activity without being near potentially dangerous situations. Live-stream access allows personnel to observe situations in real-time and have the option to respond immediately when situations require immediate response. Remote~~Mobile~~ functionality allows cameras~~RMCs~~ to be moved and positioned as the need requires.

RMCs may have their own power supply or attached to a utility pole so as to utilize electricity for power. In either case, RLSCs~~RMCs~~ offer personnel critical situational and evidentiary information in a safe way.

RLSC~~MC~~s store visual (and sometimes audio) data with either internal storage and/or by transmitting data in real-time to a remote OPD location.

2. Proposed Purpose

RMCs are used by OPD authorized personnel to gather evidence during undercover operations as well as during large events where there is a greater probability that criminal activity may occur and public safety is more likely to be impacted; the City's Surveillance Technology Ordinance[1] ~~defines~~ "large-scale event(s)" as events "attract(ing) ten thousand (10,000) or more people with the potential to attract national media attention that provides a reasonable basis to anticipate that exigent circumstances may occur." OPD may also use live stream cameras on poles held by officers to observe smaller events in the scores or hundreds of people where the same conditions exist.

[1] Ordinance No. 13489C.M.S. passed by the City Council on May 15, 2018

~~mass-events personnel are deployed to observe and promote public safety.~~ Live stream image and video capture allow investigators to observe activity related to suspected criminal activity.

3. Locations Where, and Situations in which RLSCs~~GLD System~~ may be deployed or utilized.

A RLSC~~MC~~ may be used anywhere in the public right of way within the City of Oakland. Personnel may use hand-held cameras with live-viewing capabilities within in the public right of way within the City of Oakland; however, these cameras are generally only used for mass-person events to as to provide situational awareness during events where public safety must be monitored (e.g. large protests or parades). OPD ~~RMCs~~ may also request that a utility company install a remote camera ~~RMC to a~~on an electricity utility pole for powered live-remote viewing. OPD will only request to install a such a camera ~~RMC~~ to a utility pole with a court order compelling ~~allowing~~ the utility company to install the camera.

4. Impact

RLSC~~MC~~s offer evidentiary and situational awareness in numerous ways that challenge measurement. Mass events where thousands of people gather require that police personnel see where people are moving in real-time to better ensure that resources are provided as needed to ensure public safety.

OPD's Criminal Investigations Division (CID) and Intel Unit occasionally need to monitor street locations with remote live-view cameras to gather evidence related to suspects in criminal cases. RLSC~~MC~~s can provide useful evidence about particular suspects relating to violent criminal activity.

OPD recognizes that any use of cameras to record activity which occurs in the public right of way raises privacy concerns. There is concern that the use of RMCs can be utilized to identify the activity, behavior, and/or travel patterns of random individuals. However, OPD does not randomly employ this technology throughout the City. Rather, RLS~~M~~Cs installed on utility poles (after obtaining a court order) are used in specific situations to gather evidence about particular individuals connected to particular criminal investigations. The scope and use of such technology is narrow and limited. Therefore, OPD believes that the impact to public privacy is similarly narrow and limited.

5. Mitigations

All live-stream cameras ~~RMCs~~ shall be housed and secured within ~~IT~~ OPD's IT Unit ~~or Intel Unit~~ lockers and not accessible with to the public or to personnel

without permission to use such equipment. Regular camera data from live-stream cameras shall be uploaded onto a secure computer with user and email password protection. For data that is captured and used as evidence, such data shall be turned in and stored as evidence. Otherwise, camera data will be destroyed after 30 days.

OPD does not possess remote cameras which are affixed to utility poles. Rather, OPD relies on its partnership with the Bureau of Alcohol, Tobacco, and Firearms (ATF) through the ATF Taskforce to directly install remote cameras, when approved by a judge in a court order, as part of a documented investigation (ATF personnel install and de-install the camera equipment). Generally, each request to install a remote camera to a utility pole is connected violent criminal activity (gun crimes, homicides, gun sales and/or major narcotic traffic activity).

~~OPD will consider providing RMC data to other law enforcement (LE) agencies if and when such agencies make a written request for the RMC data that includes:~~

~~a. The name of the requesting agency.~~
~~b. The name of the individual making the request.~~
~~c. The intended purpose of obtaining the information.~~

~~Such requests will be reviewed by the Bureau of Services Deputy Chief/ Deputy Director or designee and approved before the request is fulfilled. Approval requests shall be retained on file. Requests for RMC 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.~~

OPD will monitor its use of RLSC~~MC~~s to ensure the accuracy of the information collected and compliance with all applicable laws, including laws providing for process, and time period system audits. ~~-~~The IT Unit ~~RMC System~~ Coordinator and/or designated staff shall provide the Chief of Police, Privacy Advisory Commission, and Public Safety Committee with an annual report that contains following for the previous 12-month period following a reporting structure agreed upon by the Privacy Advisory Commission.

6. Data Types and Sources

RLS~~M~~Cs that record directly onto an internal memory device (e.g. secure digital (SD) card) operate similar to consumer digital video cameras. These types of cameras contain an internal storage device for storing audio and video data – an integrated element that can be connected to a computer for data downloads, or a removable device (e.g. SD card) which can be connected to a computer for digital downloads.

RLS~~M~~Cs can be mounted to telescoping monopods to simply extend the range of a RLS~~M~~C. In these instances the pole merely extends the reach of the camera. RMCs mounted to monopods operate similarly to other RMCs in terms of recording and storage functions.

Cameras~~RMCs~~ may be connected to a transmitter which allows for real-time transmission and remote live-stream viewing. Transmitters can use different formats (e.g. cellular 3G/4G LTE, WiFi, Ethernet, and Microwave). Transmitters can be connected to static single image digital cameras or video cameras. Transmitters allow the live-stream images or video to be viewed on a screen with the appropriate data connection and reception technology. The transmitters specifically transmit the data to a receiver where the data can then be viewed.

7. Data Security

All RMCs shall be housed and secured within IT Unit or Intel Unit lockers and not accessible with to the public or to personnel without permission to use such equipment. Regular camera data shall be uploaded onto secure computer with user and email password protection. For data that is captured and used as evidence, such data shall be turned in and stored as evidence. Otherwise, camera data will be destroyed after 30 days.

Judges approve remote cameras to be affixed to utility poles to record public right of way views for 30 days or less (90 days maximum). OPD archives video sections relevant to investigation (permanent retention) and deletes other non-evidentiary video footage.

8. Costs

OPD currently has owns four transmitters from TVU networks that allow standard single shot or video cameras to live-stream data to OPD's Administration Building or the City's Emergency Operations Center (this data is not recorded). These transmitters are approximately eight years old. OPD does not currently pay for ongoing maintenance service; the cost to upgrade the unsupported system would cost about $120,000 for a two-year maintenance contract and then $12,000 for additional years. OPD is planning to use approximately $130,000 from the Justice Assistance Grant (JAG) Program[2] to pay four new modern TVU Networks transmitters. OPD does not bear costs related to ATF remote camera installations.
~~TBD~~

9. Third Party Dependence

OPD uses TVU Networks-brand transmitter for live-stream video camera monitoring. ~~TBD~~OPD relies on the ATF to install remote cameras to utility

[2] https://www.bja.gov/jag/

poles (with court order approval).

10. Alternatives Considered

OPD officers and personnel rely primarily on traditional policing techniques to monitor large events and to gather evidence related to criminal investigations. For decades evidence gathering also includes the use of cameras, sometimes with live-stream transmitters, to record images, video and audio. Police personnel must maintain some level of situational awareness when hundreds and thousands of people gather on public streets and threats to public safety increase. Alternatives to live-stream ~~camersa~~cameras would include having more officers and personnel deployed during every mass-event. Such a deployment extends beyond OPD budget capacity.

OPD relies on remote view cameras for investigations as described above. There is no clear alternative to capturing actionable image, video and/or audio.

11. Track Record of Other Entities

There is no well documented public record of RLSCs. However, a recent case concerning remote cameras illustrates legal considerations: the Tenth Circuit Court of Appeals decided in "*United States v. Cantu[i]"* (October 2017) in which the court discussed whether the use of a utility pole camera that viewed the front of Cantu's residence violated his rights under the Fourth Amendment[3]. The relevant facts of Cantu, taken directly from the case, are as follows: ~~TBD~~ On appeal, the issue was whether the warrantless use of camera on a utility pole that viewed the front of his residence (public right of way) violated rights under the Fourth Amendment. The Court in *Cantu* noted that the police did not install the camera on Cantu's property, thus there was no trespass; Also, the Court concluded that Cantu did not have a reasonable expectation of privacy where he was walking with the rifle.

Formatted: Font color: Custom Color(RGB(34,34,34)), Pattern: Clear (White)

[3] https://www.llrmi.com/articles/legal_update/2017_united_states_v_cantu/

DEPARTMENTAL GENERAL ORDER

##: REMOTE OR LIVE-STREAM~~AND~~ CAMERAS (RLSC)

Effective Date: ~~XX Apr 19~~
Coordinator: Information Technology Unit, Bureau of Services Division

The Oakland Police Department (OPD) uses technology to more effectively promote public safety; OPD also strives to institute policies that promote accountability and transparency. This policy provides guidance and procedure for the use, documentation, and auditing of live-stream mobile cameras.

All data, whether sound, image, or video data, generated by different types of camera recording technology are ~~OPD's~~ RLSC ~~systems are~~ for the official use of this department. Because such data may contain confidential information, such data is not open to public review.

A. Purpose of the Technology

A – 1. Authorized Use

There are different situations that can occur in the City of Oakland which will justify the use of live-stream cameras and/or remote control cameras that may record and/or allow for live streaming from remote locations. Large events with numerous people (e.g. protests, sporting events, parades, large festivals) can attract individuals seeking to engage in violent criminal behavior and/or large-scale property destruction. Authorized personnel utilizing cameras with live-streaming transmitters can provide important situational awareness to OPD; OPD can better respond to sudden dangerous activity (e.g. aggravated assault) with this remote situational awareness.

Formatted: Indent: First line: 0"

Specific criminal investigations also benefit from remote-functioning cameras that record the public right of way in particular locations where serious criminal activity occur is believed to occur.

Formatted: Indent: Left: 0.49", Right: 0.29", Space After: 6 pt

Personnel authorized to use RLSCs or access information collected through the use of such equipment shall be specifically trained in such technology and authorized by the Chief of Police or designee. Any sworn officer may utilize hand-held live-stream cameras with the approval of OPD's Information Technology (IT) Unit Coordinator. Remote cameras installed to utility poles for remote power and use may only be employed by any OPD by first receiving: 1) a court order from a judge authorizing the restricted camera use in a specific location for a specified number of days; and 2) the OPD Intel Unit Supervisor.

~~uch personnel shall be limited to designated captains, lieutenants, sergeants, officers, police service and/or evidence technicians, and crime analysts unless otherwise authorized.~~

A – 2. Prohibited Use

1. Department members shall not use, or allow others to use RLS~~M~~C equipment, software or data for any unauthorized purpose.

~~No member of this department shall operate~~ RLSC ~~equipment or access the internally stored~~ RLSC ~~data without first completing department-approved training.~~

2. The RLS~~M~~C systems shall only be used for official law enforcement purposes. No OPD personnel is authorized to install cameras to utility poles; personnel shall coordinate utility pole camera installation with third-party partners (such as the Bureau of Alchohol Tobacco and Firearms (ATF)) after receiving Intel Unit Supervisor approval as well as a court order from a judge.

3. Only specifically authorized personnel authorized by the Chief or Chief-designee (e.g. personnel with OPD's IT ~~nformation Technology~~ Unit and Criminal Investigations Division (CID) investigators, Internal Affairs Division personnel, crime analysts, the Office of the District Attorney) will have access to RLS~~M~~C audio and video data and system applications.

4. Accessing data collected by RLS~~M~~C systems 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 criminal or administrative investigation.

B. Description of the Technology

B– 1. General Description of Remote or Live Stream Cameras

~~**A – 1. How Remote and Mobile Cameras (RLSC) Work**~~

RLSCs can be self-contained devices that record audio and video, which either: 1) store data onto an internal storage device; or 2) transmit data in real-time through various digital transmission formats.

1. RLSCs that record directly onto an internal memory device (e.g. secure digital (SD) card) operate similar to consumer digital video cameras. These types of cameras contain an internal storage device for storing audio and video data – an integrated element that can be connected to a computer for data downloads, or a removable device (e.g. SD card) which can be connected to a computer for digital downloads.
2. RLSCs can be mounted to telescoping monopods to simply extend the range

Formatted: Indent: Left: 0.5", Hanging: 0.25"

Formatted: No bullets or numbering

Formatted: Indent: Left: 0.5", Hanging: 0.25"

Formatted: List Paragraph, Right: 0", Space After: 6 pt, Numbered + Level: 1 + Numbering Style: A, B, C, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.5"

Formatted: Indent: Left: 0.5", Hanging: 0.25"

of a RLSC. In these instances the pole merely extends the reach of the camera. RLSCs mounted to monopods operate similarly to other RLSCs in terms of recording and storage functions.

3. RLSCs may be connected to a transmitter which allows for real-time transmission and remote live-stream viewing. Transmitters can use different formats (e.g. cellular 3G/4G LTE, WiFi, Ethernet, and Microwave). Transmitters can be connected to static single image digital cameras or video cameras. Transmitters allow the live-stream images or video to be viewed on a screen with the appropriate data connection and reception technology. The transmitters specifically transmit the data to a receiver where the data can then be viewed.

B– 2.How Cellular Remote or Live-Stream Cameras WorkRLSC

Live-stream transmitters can be attached to ~~Some RLSCs are~~ standard consumer-type cameras ~~that that can be held and operated by personnel~~so that images and/or video can be transmitted. These RLSCs ~~may also be affixed to a variable lens's for different views. RLSCs~~ can be attached to a camera monopod and used like a standard digital video camera; the monopod in this case extends the cameras perspective beyond arms ~~–~~reach so that personnel extend the range of view (beyond corners, above head-level in a crowd, or in other related situations). RLSCs attached to monopods/tripods provide greater viewing access and promote safety where personnel may need to exercise caution before moving into unknown situations.

Some cameras~~RLSCs~~ may also be attached to utility poles for real-time and long-term remote viewing. In such cases RLSCs may be powered through electricity of the utility pole or via portable battery power. In either case, RLSCs offer personnel critical situational and evidentiary information in a safe way.

C. ~~C.~~ RLSCRLSC Data Collection

C – 1. Live-Stream Camera Information Collected
~~Data Collection and Retention~~

Live-stream camera ~~RLSC system~~ data is maintained by ~~both by currently maintained by either: 1)~~ the OPD ~~Information Technology (~~IT~~)~~ Unit within in the Bureau of Services (BOS)~~; or 2) by the Intel Unit~~. Personnel using live-stream cameras (cameras with attached transmitters) ~~RLSCs from the Intel Unit sh~~shall return RLSCs at the end of their shift to the IT Unit. The IT~~Intel~~ Unit RLSC Coordinator shall download the data onto secure IT~~ntel~~ Unit computer~~s~~ within 24 hours of receiving returned RLSC equipment.

The IT~~ntel~~ Unit shall maintain all RLSC data for 30 days unless notified by the Chief of Police or designee (e.g. Internal Affairs Captain or Criminal Investigations personnel) that the image and video data is needed for an

Formatted: Indent: Left: 0"

Formatted: Space After: 6 pt, Numbered + Level: 1 + Numbering Style: A, B, C, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.5", Widow/Orphan control

Formatted: Indent: Left: 0.49", First line: 0", Right: 0.29"

investigation. The IT ~~OPD~~ Unit RLSC Coordinator ~~and/or assigned personnel issued the RLSC~~ is responsible for recovering the data from the RLSC.

Data that is part of an investigation shall be provided to the appropriate personnel as a separate digital data file, kept permanently as part of the official investigation record.

The IT Unit shall delete all RLSC data left on installed on IT Unit computers after 30 days unless otherwise notified to maintain the data as part of an investigation as detailed above.

C – 2. Remote Camera Information Collected

The Intel Unit is responsible for the use and coordination of remote cameras attached to utility poles for remote power, use and viewing. The Intel Unit is authorized to participate with the ATF and/or other approved taskforce partners on the installation of remote cameras. The ATF and/or other approved taskforce partner will be responsible for the collection of pole camera image and video data. Only image and video data needed for lawful police investiagtions and for evidence shall be maintained indefinitely by OPD; the Intel Unit shall be responsible for maintain this data.

C – 3. Limitations on Information Collected

Remote pole camera image and video data shall only be generated with the approval of a judge's court order; a pole camera may only be used during the allowed recording period, which is usually 30 days or less, and generally never more than 60 days.

C – 4. Monitoring and Reporting

The Oakland Police Department will monitor its use of the RLSC 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.

The IT Coordinator, Intel Unit Coordinator, or other designated OPD personnel shall provide the Chief of Police, Privacy Advisory Commission, and City Council ~~Public Safety Committee~~ with an annual report that contains following for the previous 12-month period:

1. The number of times a RLSC was deployed, and type of deployment.
2. The number of times RLSC data was used as part of an investigation.
2. A list of agencies other than OPD that were authorized to use the equipment.
3. A list of agencies other than the OPD that received information from use of

Formatted: Indent: Left: 0"

Formatted: Body Text, Indent: Left: 0.49", Right: 0.29", Add space between paragraphs of the same style, No bullets or numbering, Tab stops: Not at 1.5"

Formatted: Body Text, Right: 0.15"

Formatted: Body Text, Indent: Left: 0.49", Right: 0.29", Space After: 6 pt

Formatted: Indent: Left: 0.49", Right: 0.29", Space After: 6 pt

the equipment.

4. Information concerning any violation of this policy.
5. Total costs for maintenance, licensing and training, if any.
6. The results of any internal audits and if any corrective action was taken.

The above information and reporting procedures will assist in evaluating the efficacy of this policy and equipment.

D. Data Access

D – 1. OPD Data Access

OPD's RLSC system oversight as well as data retention and access, shall be managed by OPD's Information Technology Unit under the BOS, or designee.

D – 2. RLSC System Coordination

The IT Unit Coordinator is responsible for ensuring systems and processes are in place for the proper collection, accuracy and retention of live-stream camera system data. The Intel Unit Supervisor is responsible for ensuring that all use of remote utility pole installed cameras are used in accordance with all OPD policies and procedures outlined in this policy.

D – 3. Third Party Data Access

OPD may use remote cameras owned and operated by the ATF and/or other approved law enforcement partners. OPD personnel may only use camera technology from other law enforcement agencies such as the ATF with the express written permission of the Intel Unit supervisor.

RLSC system data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law, using the following procedures:

1. The agency makes a written request for the RLSC data that includes:

   a. The name of the requesting agency.
   b. The name of the individual making the request.
   c. The intended purpose of 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.

Requests for RLSC data by non-law enforcement or non-prosecutorial agencies will be processed as provided in Departmental General Order M-09.1, Public

Formatted: Indent: Left: 0", Tab stops: 0.5", Left + 1", Left + 1.5", Left + 2", Left + 2.5", Left + 3", Left + 3.5", Left + 4", Left + 4.58", Left

Formatted: Font: Times New Roman, 12 pt, Bold, Not Expanded by / Condensed by

Formatted: Font: Bold, Not Expanded by / Condensed by

Formatted: List Paragraph, Right: 0", Space After: 6 pt, Numbered + Level: 1 + Numbering Style: A, B, C, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.5"

Formatted: Indent: Left: 0.25", Hanging: 0.5"

Formatted: Indent: Left: 0.25"

Formatted: Indent: Left: 0.25"

Formatted: Font: Not Bold

Records Access (Civil Code § 1798.90.55) and per any interagency agreements.

E. Data Retention

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

1. All live-stream cameras ~~RLSCs~~ shall be housed and secured within IT Unit or ~~Intel Uni~~t lockers. All RLSC data downloaded from RLSCs shall be uploaded onto secure user and email password protected IT Unit computers and / or Intel Unit computers.

~~2.~~ For data that is captured and used as evidence, such data shall be turned in and stored as evidence. ~~Those are the protocols used PEU or IAD or RMM systems.~~

~~2.~~

3. Members approved to access RLSCs under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data related to an administrative or criminal investigation, or for training purposes.

D – 4. Training

The Training Section shall ensure that members receive department-approved training for those authorized to use or access live-stream cameras. The Intel Unit shall ensure that members authorized to view remote pole camera data are properly trained by the Intel Unit. The Training Division shall ~~the Shotspotter system and~~ shall maintain a record of all completed trainings. (Civil Code § 1798.90.51; Civil Code §1798.90.53).

By Order of

Anne E. Kirkpatrick
Chief of Police

Date Signed:

Formatted: Tab stops: 0.5", Left + 1", Left + 1.5", Left + 2", Left + 2.5", Left + 3.15", Centered

Formatted: List Paragraph, Right: 0", Space After: 6 pt, Numbered + Level: 1 + Numbering Style: A, B, C, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.5"

Formatted: Indent: Left: 0.25"

Formatted: Indent: Left: 0", First line: 0"

Formatted: Indent: Left: 0", First line: 0", Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.75" + Indent at: 1"

Formatted: Font: (Default) Times New Roman, 12 pt, Bold

Formatted: Normal, No bullets or numbering