



Privacy Advisory Commission
September 4, 2025; 5:00 PM
Oakland City Hall
Hearing Room 1
1 Frank H. Ogawa Plaza, 1st Floor
Regular Meeting Agenda

Commission Members: *District 1 Representative: Vacant District 2 Representative: Don Wang, District 3 Representative: Brian Hofer, District 4 Representative: Lou Katz, District 5 Representative: Vacant, District 6 Representative: Gina Tomlinson, District 7 Representative: Sean Everhart, 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. Approve Meeting Minutes
 - April 3, May 1 and June 5, 2025
4. Informational Item
 - a. Data Sharing policy for ALPR as pertains to ICE
5. Action Items:
 - a. Annual Reports
 1. CrimeTracer Forensic Logic 2024 (OPD)
 2. Cellebrite 2024 (OPD)
 3. Pen Register (OPD)
 4. ShotSpotter (OPD)
 - b. Use Policies
 1. OPD Community Safety Camera Systems (OPD)

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. 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.



Privacy Advisory Commission
April 3, 2025; 5:00 PM
Oakland City Hall
Hearing Room 1
1 Frank H. Ogawa Plaza, 1st Floor
DRAFT Regular Meeting Minutes

Commission Members: *District 1 Representative: Reem Suleiman, District 2 Representative: Don Wang, District 3 Representative: Brian Hofer, Chair, District 4 Representative: Lou Katz, District 5 Representative: Vacant, District 6 Representative: Gina Tomlinson, District 7 Representative: Sean Everhart, Council At-Large Representative: Henry Gage III, Vice Chair, Mayoral Representative: Jessica Leavitt*

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

In attendance: Chair Leavitt, Vice Chair Gage, Commissioners Tomlinson, Everhart, Wang, Katz, Hofer

2. Open Forum/Public Comment on Non-Agenda matters

- Assata Olugbala
- Gene Hazzard

3. Review and approval of the draft November 20, February 6 and March 3 meeting minutes

Motion to approve minutes by Commissioner Hofer, seconded by Vice Chair Gage. Minutes approved unanimously.

- Assata Olugbala

4. Review and Possible Action on Federal Task Force Ordinance – OPD – Annual Reports:

- a. Drug Enforcement Agency (DEA)
- b. Alcohol, Tobacco, Firearms and Explosives (ATF)
- c. Secret Service
- d. United States Marshall Service (USMS)
- e. Federal Bureau of Investigation Violent Crimes - Safe Streets (FBI)
- f. Federal Bureau of Investigation Child Exploitation (FBI)

Lt. Jeffrey Smoak provided an update on the Secret Service annual report (item 4c). He redrafted the report and met with the taskforce officers and discussed the role they play in the taskforce, including compliance with state and local laws. There were no reported violations. The LT also reached out to the City Attorney's Office, and they are willing to provide an annual training on the appropriate laws and policies guiding the taskforces work.

Acting Lt. DeSean Spencer provided an update on the FBI Child Exploitation taskforce. He shared information in the annual report, including the types of cases that the taskforce handles.

Lt. Gabriel Urquiza reported out on USMS and DEA annual reports and the technology used by the taskforce. He shared the specific changes that were made to each annual report.

Commissioners asked questions of the OPD presenters and additional details as needed. The PAC also discussed the FBI and Child Exploitation taskforces and the technology used, reporting, and disclosure of any possible violations. Additional data sharing is needed. Amadis Sotelo agreed to provide guidance on data sharing options to ensure that OPD is following state and local law as it relates to the Federal Taskforce Ordinance.

Commissioner Hofer moved to approve all the reports, excluding the ATF annual report. Second by Commissioner Katz. Motion approved unanimously.

Public Comment:

Gene Hazzard

Assata Olugbala

5. Review and Possible Action on Unmanned Aerial System (UAS or Drone) 2024 Annual Report

Lt. Omar Daza-Quiroz from the Bureau of OPD Investigations provided an overview on the report that was included in the agenda packet. These technologies went live in 2022. Commissioners had questions about

the data that is collected to track when the technology is used. There is no personally identifiable information collected in the process.

Vice Chair Gage moved acceptance and second by Commissioner Everhart.

Discussion: Chair Hofer added that per the Surveillance Technology Ordinance the benefits outweigh the cost.

Public Comment: Assata Olugbala

Motion passed unanimously.

6. Review and Possible Action on ATF Bodyworn Cameras – MOU Addendum

Acting Lt. Gabriel Urquiza provided an update on this item, the updated MOU was included in the agenda packet. The MOU addendum clarified changes in the policy related to ATF and circumstances for when the Bodyworn Cameras will be used. The MOU follows state guidelines for OPD to document in writing when data will be shared with ATF in connection with a critical incident. This allows officers to participate in enforcement activities with the federal taskforce.

Vice Chair Gage moved that the PAC accept and approve the MOU as presented by staff, forward to Council with a recommendation and note that there are concerns that officers will operate with a slightly different set of guidelines.

Second by Chair Leavitt

Commissioners Tomlinson, Everhart, Vice Chair Gage and Leavitt all voted - yes

Commissioners Wang, Hofer voted no

Commissioner Katz - abstained.

Public Comment: Asata Olugbala

7. Review and Possible Action on the Forward Looking Infrared (FLIR) 2024 Annual Report

Officer Brian Mart provided an update on this item. He shared that this policy was developed in the hopes that the department would get a fixed wing aircraft. The camera was only used for training purposes. No data was retained.

Chair Leavitt moved to forward this item to City Council with a recommendation to approve and that the benefits outweigh the costs.

Second by Commissioner Everhart

Motion passed unanimously.

Public Comment: Assata Olugbala

8. Review and Possible Action on Sanctuary Contracting Ordinance – Presentation of Annual Report by Assistant to the City Administrator, Felicia Verdin

OPD and city departments are aware of the Sanctuary Contracting Ordinance.

Commissioner Hofer moved to forward to accept the annua report and forward to City Council.

Discussion: City officials should be advised that Lexus Nexus is now on the prohibited list as they have agreed to provide data to ICE.

Second by Vice Chair Gage.

Public Comment: Assata Olugbala

Motion passed unanimously.

Meeting adjourned.



Privacy Advisory Commission
May 1, 2025; 5:00 PM
Oakland City Hall
Hearing Room 1
1 Frank H. Ogawa Plaza, 1st Floor
Draft Meeting Minutes

Commission Members: *District 1 Representative: Reem Suleiman, District 2 Representative: Don Wang, District 3 Representative: Brian Hofer, Chair, District 4 Representative: Lou Katz, District 5 Representative: Vacant, District 6 Representative: Gina Tomlinson, District 7 Representative: Sean Everhart, Council At-Large Representative: Henry Gage III, Vice Chair, Mayoral Representative: Jessica Leavitt*

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

In attendance: Vice Chair Gage, Commissioners Tomlinson, Katz, Hofer, Everhart.

Excused: Chair Leavitt and Commissioner Wang

2. Open Forum/Public Comment on Non-Agenda matters

No Public Comment

3. Information Item:

- a. Report from Public Works regarding OPD request for video footage.

Michael Tecson with Oakland Publics Works provided an update on two requests for footage that were captured on illegal dumping cameras. In both cases Michael downloaded the footage and provided it to OPD officers.

Commissioner Hofer move acceptance of the report, second by Everhart. Motion passed unanimously.

4. Action Items:

- a. April 3, 2025 PAC minutes – Staff withdrew minutes from the agenda.

b. Annual Reports

1. Biometric Crime Lab (OPD)

OPD staff Cheng provided an update on this item. She explained that all cost of the equipment were updated to the appendix. There is no need to update the impact report each year since it was already approved. In the future, only the annual report needs to be provided with an update on the use of the technology.

There were no questions from Commissioners on this item.

Vice Chair Gage moved to forward the item to council that the benefits of the technology outweigh the cost and no civil liberties will be impacted.

Motion was revised to include a waiver of the race reporting requirement.

Second by Commissioner Hofer. Motion passed unanimously.

2. ALPR/FLOCK (OPD)

Dr. Beckman provided a high level overview of the ALPR annual report included in the agenda packet. For the period from July 2024 to the end of 2024 there were approximately 189 million license plate reads that the technology processed. Additional data was included in the report.

Commissioners had a discuss about data collection, usage and retention schedules.

Public Comment:

- Isaac Cheng from the Chinatown Chamber of Commerce provided information on the camera network in Chinatown and spoke in support of this item.

Vice Chair recommended establishing an ad hoc regarding ALPR/FLOCK. Members Hofer, Everhart, Tomlinson and Katz agreed to serve on the ad hoc committee and meet with LT. Urquiza.

Commissioner Hofer requested the revised contract and manual.

3. ATF (OPD)

Lt. Urquiza provided an update on this item in the agenda packet. There were two edits in the report pertaining to surveillance equipment, the GPS tracker and poll camera systems that are owned by ATF. Vice Chair Gage clarified that the GPS tracker requires a search warrant, poll camera requires

that OPD get a court order. The search warrant and court order are not technically required by law.

Commissioner Hofer made a motion to accept the item and forward to City Council. Second by Commissioner Everhart. Motion passed unanimously.

c. Use Policies

1. OPD Community Safety Camera Systems

Lt. Urquiza provided an overview of the community safety systems policy and the effort to integrate existing and emerging technology on a single platform. The goal is to expand the existing Flock Operating System to bring in live and historical camera video to make it easier for officers to conduct canvasses or locate vehicles related to illegal activity. The general purpose of the technology is to deter crime and provide a focused approach with minimal impact on the community. The system will allow officers to get evidence quickly using the Flock camera network, different computer systems can integrate with Flock. Businesses need to opt into sharing the video data.

Commissioners asked about the retention schedule. City owned cameras could be subject to a 90 day retention period.

Public Comment:

- Issac Cheng, Chinatown Chamber of Commerce spoke in support of this item.

Vice Chair Gage requested commissioners serve on an ad hoc committee regarding this item. Commissioners Katz, Everhart, Tomlinson and Hofer agreed to serve on the ad hoc committee. OPD expressed a sense of urgency for the PAC to approve the item. Commissioner Hofer requested a proposed contract and manual from OPD.



Privacy Advisory Commission
June 5, 2025; 5:00 PM
Oakland City Hall
Hearing Room 1
1 Frank H. Ogawa Plaza, 1st Floor
DRAFT Meeting Minutes

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

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

In attendance: Chair Leavitt, Vice Chair Gage, Commissioners Hofer, Everhart, Thomlinson, Katz and Wang.

Absent: none

2. Open Forum/Public Comment on Non-Agenda matters

No public comment.

3. Approve April 3, 2025 PAC minutes

Item removed from the agenda by staff.

4. Action Items:

a. Annual Reports

1. CrimeTracer Forensic Logic 2024 (OPD)
2. Cellebrite 2024 (OPD)
3. Pen Register (OPD)
4. Live Stream (OPD)

5. Unused Tech 2025 (OPD)

OPD withdrew the first 3 annual reports. The subject matter expert was not available.

Dr. Beckman provided an update on the Live Stream item. The technology was not deployed. The technology is typically deployed during civil unrest and is useful when necessary. Commissioners discussed the pros and cons of the technology including cost.

Commissioner Tomlinson made a motion that the benefits outweigh the cost and civil liberties and civil rights are safe guarded. Second by Everhart. The item passed unanimously.

No public comment.

6. Apricot data management system (Department of Violence Prevention)

Caitlin Grey with DVP provided a detailed PowerPoint presentation on this item. She included information on the data sharing agreement, staffing users and usage data. Ms. Grey also provided information about the collection of group level data. She indicated that there were no community complaints or concerns raised about Apricot 360 related to its protection of civil rights and civil liberties.

The DVP proposed the following modifications to the policy include presenting individual and groups services separately, removed references to community healing and school VIP Program Strategies and to use provide appropriate data privacy training for DVP staff.

Commissioners asked questions regarding costs, audits of user lists, and data privacy training. Questions were also asked about any public records request, and none had been made. The commissioners also raised questions about consent rates.

Commissioner Wang moved to forward the report to the City Council with the finding that the benefits outweigh the costs with the proposed modification to the use policy about monitoring or coordination. Second by Commissioner Everhart.

Commissioner Wang revised his motion to the annual report to include the consent rate. Commissioner Everhart confirmed his second.

The motion passed unanimously.

No public comment.

a. Use Policies

1. OPD Community Safety Camera Systems (OPD)

OPD Acting Lieutenant Urquiza from the Ceasefire Section provided an update on this item. He presented an overview of the changes to Department General Order I32.1. The policy is a partnership between the public and private sector and integrates camera systems that already exist on the Flock operating system platform in commercial districts. This is a fixed camera device. The goal is to prevent crime and obtain evidence quickly to bring criminals to justice.

Commissioners discussed developing an MOU and expressed concerns regarding data being shared with outside agencies.

Commissioner Hofer provided an update from the ad hoc committee. He indicated the proposal has changed multiple times. This is a real time crime center and FLOCK OS is the brain. He shared additional details about the draft contract and that the PAC will review the data ownership section.

Hofer made a motion to continue the item to the next meeting and the ad hoc committee will continue it's review of this item. Second by Commissioner Everhart. Motion passed unanimously.

Public Comment:

- Savlan Hauser, Jack London Improvement District indicated that the cameras are a valuable tool for community safety in downtown.
- Isaac Cheng with Oakland Chinatown spoke in support of the item via Zoom.

b. Proposed Ordinance

1. The No Stolen Data Ordinance

Commissioner Hofer provided an update on this item. He shared that some vendors are using stolen data, violate terms and take private data without consent and put it into their products. The goal is to guard against these practices and prohibit doing business with vendors that have these practices. A first review of the item occurred during this meeting and is aligned with the Sanctuary Contracting Ordinance. The PAC will need to review the item.

Vice Chair Gage recommended establishing an ad hoc committee on this item. Commissioners Gage, Tomlinson and Hofer volunteered to serve on an ad hoc committee to further discuss the proposed ordinance.



AGENDA REPORT

TO: Jestin D. Johnson
City Administrator

FROM: Floyd Mitchell
Chief of Police

SUBJECT: Oakland Police Department's Data
Sharing Policy For Automated License
Plate Readers

DATE: July 17, 2025

City Administrator Approval

Date:

RECOMMENDATION

Staff Recommends That City Council Receive Informational Report On The Oakland Police Department's Data Sharing Policy For Automated License Plate Readers Including All Policies Related To Sharing Information With Immigration And Customs Enforcement (ICE)

EXECUTIVE SUMMARY

Councilmember Charlene Wang requested a report on the Oakland Police Department's Automated License Plate Readers' (ALPR) data sharing policy. This item was scheduled on July 17, 2025, at the Rules Committee meeting for the July 22, 2025, Public Safety Committee meeting.

ANALYSIS AND POLICY ALTERNATIVES

There are four attachments included in response to this request: *Attachment A*) OPD's official ALPR policy; *Attachment B*) ALPR annual report which was presented on May 1 at the Privacy Advisory Commission (PAC) meeting; *Attachment C*) Policy 415; and *Attachment D*) OPD's media statement regarding an article released July 14, 2025, by the San Francisco Standard initially stating, "Oakland cops gave ICE license plate data". The San Francisco Standard later changed their title to "Oakland Police fulfilled a request related to an ICE investigation on one occasion." As stated in the media release, *no member of the Oakland Police Department was involved in this alleged sharing of ALPR information with Immigration and Customs Enforcement (ICE)*. These documents will elucidate what OPD's data sharing policy is per this request.

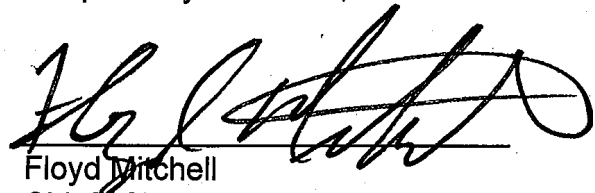
Public Safety Committee
July 22, 2025

ACTION REQUESTED OF THE CITY COUNCIL

Staff Recommends That City Council Receive Informational Report On The Oakland Police Department's Data Sharing Policy For Automated License Plate Readers Including All Policies Related To Sharing Information With Immigration And Customs Enforcement (ICE)

For questions regarding this report, please contact Acting Lt. Gabriel Urquiza-Leibin, at GUrquiza-Leibin@oaklandca.gov.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'F. Mitchell', is written over a horizontal line.

Floyd Mitchell
Chief of Police
Oakland Police Department

Reviewed by:
A/Lt. Gabriel Urquiza-Leibin
OPD, CGIC/Real-Time Operations Center

Prepared by:
Dr. Tracey Jones
Police Services Manager I
OPD, Research and Planning

Attachments (4):

- A. ALPR Policy
- B. ALPR 2024 Annual Report
- C. OPD Policy 415
- D. OPD Media Statement re: San Francisco Standard article



DEPARTMENTAL GENERAL ORDER

I-12: AUTOMATED LICENSE PLATE READERS

Effective Date: 14 AUG 24

Coordinator: Information Technology Unit

This policy provides guidance for the capture, storage and use of digital data obtained through the use of ALPR technology while recognizing the established privacy rights of the public.

A. Definitions**A - 1. Automated License Plate Reader (ALPR)**

A device that uses cameras and computer technology to compare digital images of vehicle license plates to lists of known information of interest.

A - 2. Hot List

A list of license plates associated with vehicles of interest compiled from one or more databases including, but not limited to the Stolen Vehicle System (SVS), NCIC, and local BOLO alerts.

A - 3. Hit

Alert from the ALPR system that a scanned license plate may be in the National Crime Information Center (NCIC) or other law enforcement database for a specific reason including, but not limited to, being related to a stolen car, wanted person, missing person or domestic violence protective order.

B. Description of the Technology: *Information describing the surveillance technology and how it works.*

OPD uses Automated License Plate Reader (ALPR) technology to capture and store digital license plate data and images. There are two components to the ALPR system:

1. Automated License Plate Readers

Device components include cameras which can be attached to vehicles or fixed objects and a vehicle-based computer that processes the photographs and compares the data against California Department of Justice (CA DOJ) hot lists. Data are transmitted for comparison (the hot lists are downloaded to the vehicle at the start of the patrol shift and then compared from that list). Authorized/designated personnel can also manually enter license plates to internal OPD generated hot lists only accessible to personnel authorized/designated to access the OPD ALPR system.

2. ALPR Database

A central repository stores data collected and transmitted by the Automated License Plate Readers.

C. Purpose of the Technology

ALPR technology works by automatically and indiscriminately scanning all license plates on vehicles that are publicly visible. ALPR reads these license plates, compares the license plate characters against Hot Lists, and stores the characters along with the date, time, and location where the photograph was taken. This process allows for two functions by ALPR:

- Immediate (real time) comparison of the license plate characters against Hot Lists listing vehicles that are stolen or sought in connection with a crime and/or with OPD-generated internal lists.
- Storage of the license plate characters – along with the date, time, and location where the photography was taken – in a database that is accessible to enforcement agencies with authorized access (as defined in “Authorized Use” below) for investigative query purposes.

D. Authorized Uses

The specific uses that are authorized, and the rules and processes required prior to such use.

D - 1. Authorized Users

Personnel authorized/designated to use ALPR equipment or access information collected through the use of such equipment shall be specifically trained in such technology. Sworn personnel, Police Service Technicians (PST), or other authorized/designated Department personnel may use the technology. Authorized users other than sworn personnel or PSTs must be designated by the Chief of Police or designee.

D - 2. Authorized Use

➤ Real-Time Identification

The sworn personnel/technician shall verify an ALPR response through the California Law Enforcement Telecommunications System (CLETS) before possibly taking enforcement action that is based solely on an ALPR alert.

Once an alert is received, the operator shall confirm that the observed license plate from the system matches the license plate of the observed vehicle.

Members will not take any police action that restricts the freedom of any individual based solely on an ALPR alert unless it has been fully validated, by visually verifying that the license plate characters on the vehicle match those in the database, and that the make, model, color and all other known identifying characteristics likewise match.

➤ Hot Lists

The Department shall only use the following hot lists: Stolen Vehicle System (“SVS”), National Crime Information Center (“NCIC”) lists, CA DOJ lists, Amber and Silver alerts, and custom BOLO lists pertaining solely to missing or at-risk persons, witness locates, burglaries, grand

theft, and violent crime investigation. Hot lists shall be obtained or compiled from sources as may be consistent with the purposes of the ALPR system set forth in this Policy. Hot lists utilized by the Department's ALPR system may be updated by agency sources more frequently than the Department may be uploading them and thus the Department's ALPR system will not have access to real time data. Occasionally, there may be errors in the ALPR system's read of a license plate. Therefore, an alert alone shall not be a basis for police action (other than following the vehicle of interest). Prior to initiation of a stop of a vehicle or other intervention based on an alert, Department members shall undertake the following:

Department members will document all stops from hot list alerts by indicating the positive ALPR Hit, i.e., with an arrest or other enforcement action on a computer generated spreadsheet that **shall include** at minimum;

1. the Department member's name that responded to the alert,
2. the justification for responding to the alert,
3. the related case number,
4. the disposition code,
5. time and date of the response, and
6. any known next steps or follow up (e.g. forwarding case to District Attorney, alerting owner to recovered stolen vehicle).

➤ **Database Investigative Queries**

Historical searches of scanned plates is permissible solely for missing or at-risk persons, witness locates, burglaries, grand theft, violent crime investigation, and in response to any subpoena, warrant, or other court order. Accessing the data shall be based on a standard of Reasonable Suspicion or greater. For each query, the Department **shall** record;

1. the date and time the information is accessed,
2. the license plate number or other data elements used to query the ALPR system,
3. the username of the person who accesses the information, and, as applicable, the organization or entity with whom the person is affiliated, and
4. the purpose for accessing the information. These records shall be attached to the annual report required by O.M.C. 9.64 et seq.

➤ **General Hot Lists** (such as SVS and NCIC) will be automatically downloaded into the ALPR system a minimum of once a day with the most current data overwriting the old data.

- D - 3.** All entries and updates of specific Hot Lists within the ALPR system will be documented by the requesting Department member within the appropriate

general offense report. All entries shall be approved by the ALPR Administrator (or his/her designee) before initial entry within the ALPR system. The hits from these data sources should be viewed as informational; created solely to bring the officers attention to specific vehicles of interest that might have been associated with criminal activity.

All Hot Plates and suspect information entered into the ALPR system will contain the following information as a minimum:

1. Entering Department member's name.
2. Related case number.
3. Justification for entering the plate and/or other identifying information onto the Hot List.
4. Date and time of entry.

E. Restrictions on Use

E - 1. Permitted/Impermissible Uses

All ALPR recordings collected from ALPR cameras installed on Oakland property are the property of the Oakland Police Department. Department personnel may only access and use the ALPR system consistent with this Policy. The following uses of the ALPR system are specifically prohibited:

- **Invasion of Privacy:** Except when done pursuant to a court order such as a search warrant, it is a violation of this Policy to utilize the ALPR to record license plates except those of vehicles that are exposed to public view (e.g., vehicles on a public road or street, or that are on private property but whose license plate(s) are visible from a public road, street, or a place to which members of the public have access, such as the parking lot of a shop or other business establishment). OPD shall make reasonable efforts to restrict the usage of the ALPR technology to the public right of way and other public property in alignment with this restriction.
- **Harassment or Intimidation:** It is a violation of this Policy to use the ALPR system to harass and/or intimidate any individual or group.
- **Use Based on a Protected Characteristic:** It is a violation of this policy to use the ALPR system or associated scan files or hot lists solely because of a person's, or group's race, gender, religion, political affiliation, nationality, ethnicity, sexual orientation, disability, or other classification protected by law.
- **Personal Use:** It is a violation of this Policy to use the ALPR system or associated scan files or hot lists for any personal purpose.
- **First Amendment Rights:** It is a violation of this policy to use the ALPR system or associated scan files or hot lists for the purpose or known effect of infringing upon First Amendment rights.

- **Medical Rights:** No data from ALPR shall be used or shared with other agencies for the purpose of pursuing criminal charges or civil enforcement against individuals for obtaining, providing, or supporting reproductive health care services, to ensure that medical rights of residents of and visitors to Oakland, a Sanctuary City, remain intact.

The Oakland Police Department or the City of Oakland shall solicit written documentation from the requesting agency confirming that the requested data from ALPR is not intended to be used for the prohibited purposes set forth herein. Such information shall be provided to all OPD sworn personnel responsible for providing the requested data.

Department members shall not use, or allow others to use, the equipment or database records for any unauthorized purpose (Civil Code §798.90.51.; Civil Code § 1798.90.53).

1. No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.
2. No ALPR operator may access department, state or federal data unless otherwise authorized/designated to do so pursuant to Section E “Data Access” below.
3. Accessing data collected by ALPR requires a right to know and a need to know. A right to know is the legal authority to receive information pursuant to a state or federal statute, applicable case law, or a court order. A need to know is a compelling reason to request information such as involvement in an active investigation.

F. 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.

ALPR technology works by automatically scanning license plates on vehicles that are publicly visible. ALPR reads these license plates, compares the license plate characters (as well as vehicle attributes such as vehicle color or make and model with some ALPR systems) against specific databases, and stores the characters along with the date, time, and location where the photograph was taken, in a database.

G. 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.

Department sworn personnel, police service technicians, or other authorized/designated Department personnel may use the technology. Authorized/designated users other than sworn personnel or PSTs must be designated by the Chief of Police or designee.

Data may not be shared with out of state or federal agencies, per California law.

The Oakland Police Department does not permit the sharing of ALPR data gathered by the city or its contractors/subcontractors for purpose of federal immigration enforcement, pursuant to the California Values Act (Government Code § 7282.5; Government Code § 7284.2 et seq) – these federal immigration agencies include Immigration and Customs Enforcement (ICE) and Customs and Border Patrol (CPB).

All data and images gathered by the ALPR are for the official use of this department. Some information may not be disclosable to the general public. Investigatory records are not generally disclosable in response to a public records request. Non-investigatory records shall be disclosed in response to a public records request.

H. Data Protection

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

All data shall be safeguarded and protected by both procedural and technological means. OPD shall observe the following safeguards regarding access to and use of stored data (Civil Code § 1798.90.51; Civil Code § 1798.90.53):

1. All ALPR server data shall be accessible only through a login/password-protected system capable of documenting all access of information by username, license number or other data elements used in the search, name, date, time and purpose. (Civil Code § 1798.90.52).
2. Data will be transferred from ALPRs to the designated storage per the ALPR technology data transfer protocol.

I. 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.

All ALPR data uploaded to the server shall be purged from the server at the point of 30 days from initial upload. ALPR information may be retained outside this retention limit solely for the following purposes:

1. Active Criminal Investigations
2. Missing or at-risk Persons Investigations
3. Investigations from other law enforcement or prosecutorial agencies where there is a legal obligation to retain information.

J. Public Access: *how collected information can be accessed or used by members of the public, including criminal defendants.*

Requests for ALPR information by non-law enforcement or non-prosecutorial agencies will be processed in accordance with Civil Code § 1798.90.55, Government Code § 7920.000 et seq., this policy, and applicable case law and court orders.

K. Third Party Data Sharing: *If and how other City departments, bureaus, divisions, or non-City entities can access or use the information, including any required justification or legal standard necessary to do so and any obligations imposed on the recipient of the information.*

ALPR server data may be shared only as otherwise permitted by law and this policy. All data and images gathered by the ALPR are for the official use of this Department.

OPD has executed an MOU that grants CHP access to OPDs ALPR data for the duration of the MOU.

OPD personnel may share ALPR server data when there is a legal obligation to do so, such as a subpoena, court order or warrant to share such information, such as the following:

- a District Attorney's Office for use as evidence to aid in prosecution, in accordance with laws governing evidence;
- a Public Defender's Office or criminal defense attorney via the District Attorney's Office in accordance with applicable California criminal discovery laws;
- California law enforcement agencies as part of a formal criminal or administrative investigation;
- a party to civil litigation, or other third parties, in response to a valid court order only.

When there is no legal obligation to provide the requested data, requests for ALPR server data from other California law enforcement agencies shall be made in writing and may only be approved by the BOS Deputy Director/Chief or designee per the 3-step protocol below. These requests shall be maintained in a secure folder so that information about these requests can be shared in required annual reports with the PAC. Server access shall be restricted only to authorized/designated OPD personnel who will extract the required information and forward it to the requester.

1. The requesting party shall have 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, case law, or sworn officer status. A need to know is a compelling reason to request information such as direct involvement in an investigation.
2. The Department shall record the requesting party's name and document the

right and need to know the requested information.

3. The Department shall record whether the request was honored or denied, the reason for such action, and the name of the Department officer that processed the request.

L. Training: *The training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology.*

The Training Section shall ensure that members receive department-approved training for those authorized/designated to use or access the ALPR system and shall maintain a record of all completed trainings. (Civil Code § 1798.90.51; Civil Code §1798.90.53).

Training requirements for employees shall include the following:

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

M. Auditing and Oversight

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

Login/Log-Out Procedure. To ensure proper operation and facilitate oversight of the ALPR system, all users will be required to have individual credentials for access and use of the systems and/or data, which has the ability to be fully audited. It is the responsibility of the Department under this policy to actively pursue software and hardware upgrades that are needed to maintain full compliance with Section K of the use policy.

The records of Database Investigatory Queries, Third Party Data Sharing, and Hot List entries shall be incorporated into the annual report required by O.M.C. 9.64 et seq.

ALPR system audits shall be conducted annually to ensure proper system functionality and that designated personnel are using the system according to policy rules via sample audits, and reviews of training records. The size of these audits shall be large enough to provide a statistically significant representation of the

data collected.

N. Maintenance

The mechanisms and procedures to ensure that the security and integrity of the surveillance technology and collected information will be maintained.

N - 1. ALPR Administration

All installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the BOS. The BOS may contract with an ALPR service provider for installation and maintenance assistance.

N - 2. ALPR Administrator

The BOS Deputy Director/Chief shall be the administrator of the ALPR program, and shall be responsible for developing guidelines and procedures to comply with the requirements of Civil Code § 1798.90.5 et seq. The BOS Deputy Director/Chief is responsible for ensuring systems and processes are in place for the proper collection, and retention of ALPR data.

N - 3. ALPR Coordinator:

The title of the official custodian of the ALPR system is the ALPR Coordinator.

N - 4. Monitoring and Reporting

The Oakland Police Department will ensure that the system is remains functional according to its intended use and monitor its use of ALPR technology to ensure the proper functionality of the system as defined in the policy guidelines of this document, including required audits, training, and data access records.

N - 5. The ALPR Coordinator shall provide the Chief of Police, Privacy Advisory Commission, and Public Safety Committee with an annual report pursuant to OMC 9.64 (Oakland Surveillance Technology Ordinance).

By Order of,


Floyd Mitchell
Chief of Police

Date: 8-14-24



MEMORANDUM

TO: PAC

FROM: OPD

SUBJECT: ALPR Annual Report

DATE: APRIL 24, 2025

Background

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

- The benefits to the community of the surveillance technology outweigh the costs, and 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.

Department General Order I-12 titled *Automated License Plate Readers* (DGO I-12) is the policy that provides guidance on the use of Automated License Plate Readers (ALPR) at the Oakland Police Department. This DGO was reviewed by the PAC and approved by City Council on July 16th, 2024.

2024 Annual Report Details

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

How the Technology is Used

The Oakland Police Department (OPD) utilizes Flock Safety (Flock) camera technology to power its Automated License Plate Reader (ALPR) system. These cameras are mounted on pre-existing city infrastructure, such as light poles or traffic light poles, or they can be mounted utilizing a pole provided by Flock. Once mounted, these cameras take still photos which focus on a vehicle to ensure a clear view of the license plate.

The Oakland Police Department primarily utilizes the Flock system in two ways.

1. To assist in active criminal investigations which have just occurred. The OPD will utilize ALPR to search where a crime just occurred. OPD personnel can enter a vehicle's license plate (if one was provided) or enter a partial license plate (if one was provided) or search a camera location (if no license plate is provided) and attempt to identify the suspect vehicle(s) or vehicle(s) of interest. The vehicle's images are then distributed to OPD Officers via interdepartmental email in attempt to locate and stop and detain any occupant(s). These vehicles are then hot listed via Flock in order to notify/alert officers when the vehicle passes an ALPR. Officers can respond to the location of the alert(s) in an attempt to locate the vehicle.

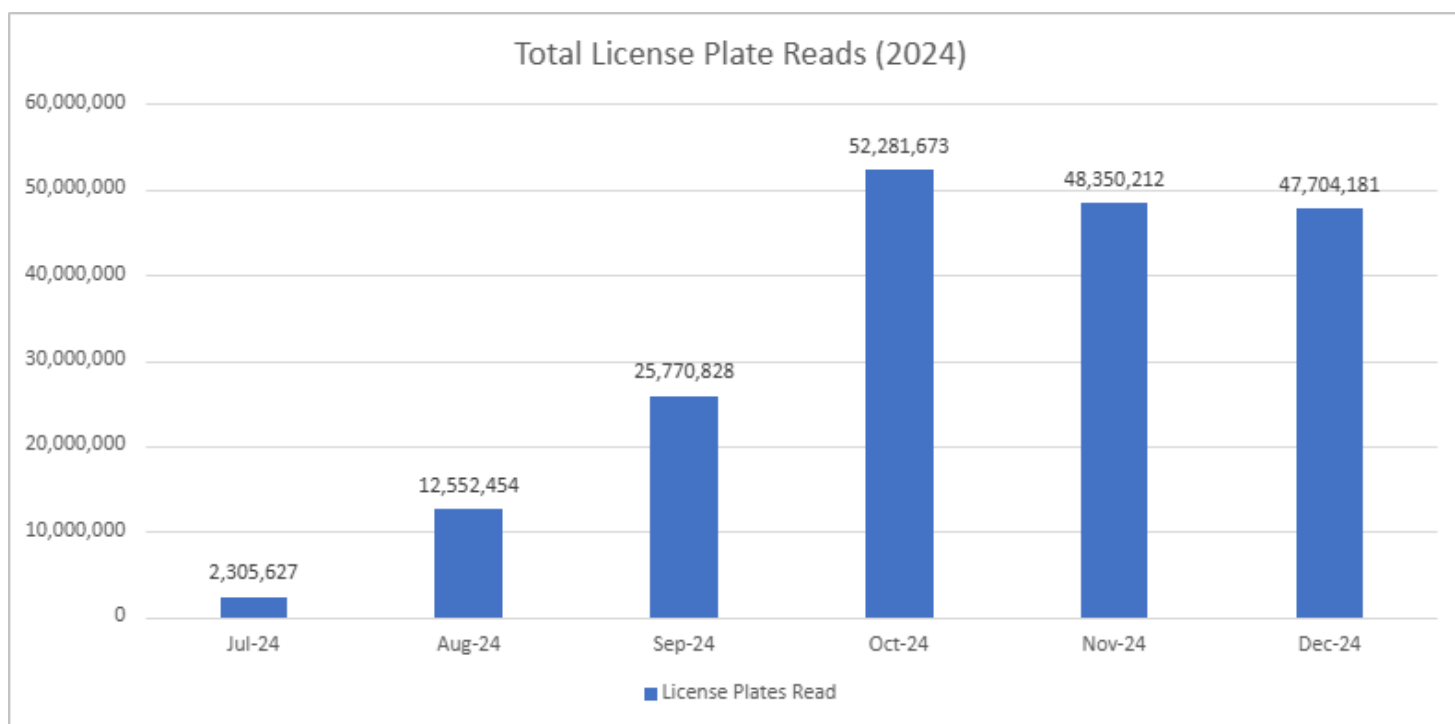
2. To assist in follow-up criminal investigations which have occurred in the past (30) thirty days. OPD will search ALPR locations of areas where crimes have occurred to attempt to identify vehicle(s) of interest that were involved in previous crimes. When vehicle(s) of interest are identified, images are distributed via interdepartmental email in attempt to locate and stop and identify any occupant(s). These vehicle(s) are then hot listed in order to notify/alert officers when the vehicle(s) passes an ALPR. Officers can respond to the location in attempt to locate the vehicle.

Type and Quantity of Data

Photos of vehicle license plates is the primary data that is collected. This data is retained for 30 days, as required by DGO I-12.

Figure A below shows the amount of license plate reads, month over month. Please note that the same license plate can be read multiple times a day, if that license plate passes by the same or different cameras during its travel. From July 2024 through December 2024, there was a total of 188,964,975 license plate reads by Flock cameras assigned to OPD in the City of Oakland.

Figure A

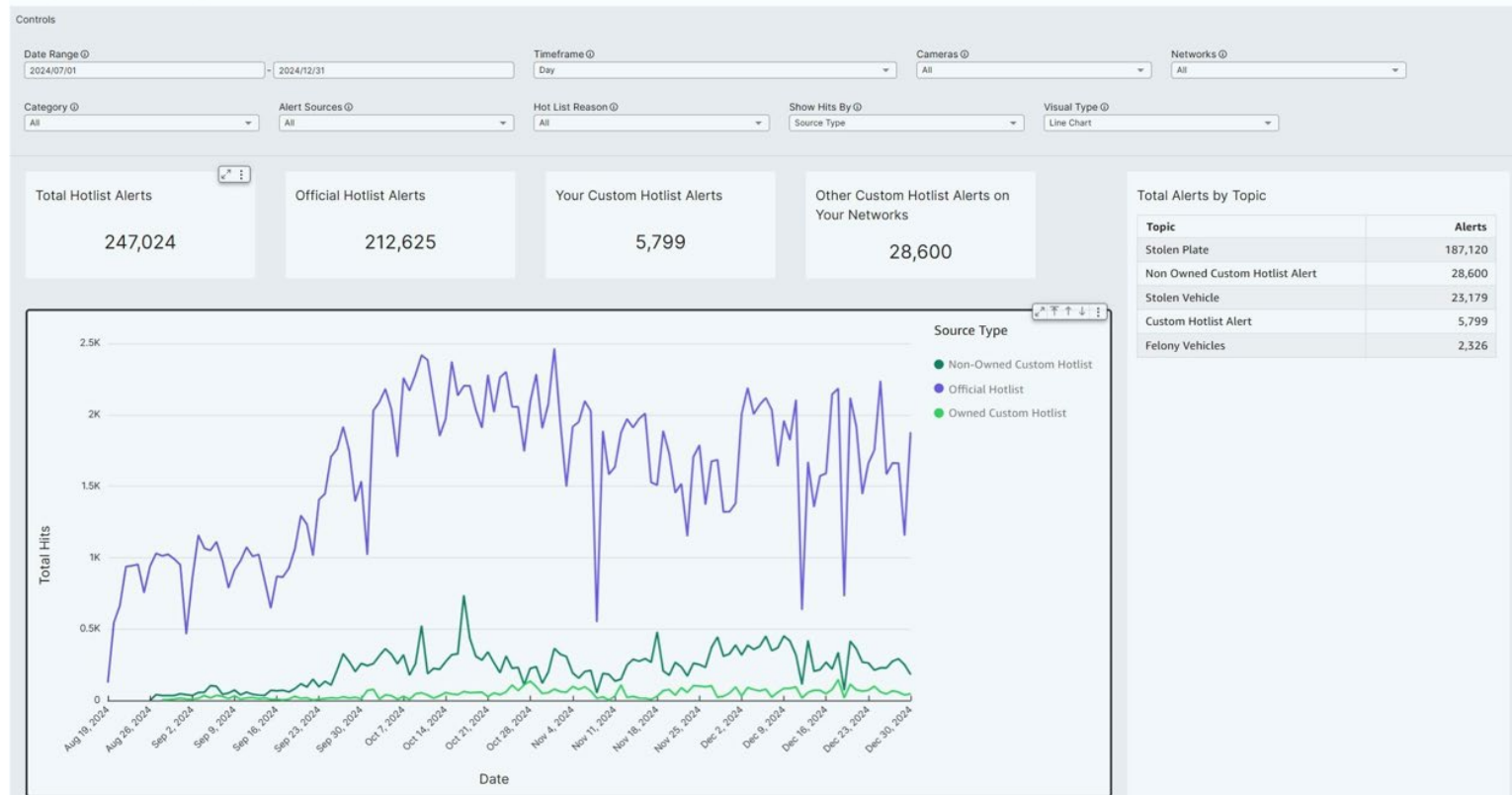


For hotlists, there was a total of 247,024 hotlist alerts, with 212,625 alerting from an official hotlist, 5,799 alerting from an OPD custom hotlist, and 28,600 custom hot list alerts created by other departments that utilized OPDs Flock images, from July 1st, 2024, through December 31st, 2024. This data is visualized in **Figure B** below.

Figure B.

Hot List Hits Report

Summary of hot list hits over time. Updates are made every 24 hours.



The top five alert types were stolen plate (187,120), non-owned custom hotlist alert, which is an alert created by another agency using Flock and shared with OPD (28,600), stolen vehicle (23,179), an alert from an OPD custom hotlist (5,799) and 2,326 felony vehicles.

Consulting with outside larger agencies, OPD discovered that larger agencies turned off “stolen plate” and “stolen vehicle” alerts for several reasons. The number of alerts were astronomical compared to other types of alerts and the staffing and resources within the department did not allow for proper response to these alerts/notifications. OPD did consider having Flock enable alerts for “stolen plate” and “stolen vehicle” during concentrated times (e.g., early hours between 0100 hours and 0400 hours when calls for service might be less than regular business hours). Flock is still attempting to configure this feature within the product. Without proper staffing or a concentrated configuration within Flock, OPD cannot respond to such alerts given the number of calls for service (e.g., priority calls and emergency calls) OPD receives daily.

When alerts for felony vehicles are received, OPD Officers will either broadcast or distribute email notifications via interdepartmental emails in order for officers to respond to the location and conduct an area check. At times, OPD will also request plain clothes officers, and/or air support (Argus) to respond to the location to assist with locating the felony vehicle(s). A multitude of officers within OPD have been provided ALPR training and been provided access; these officers range from Patrol, Community Resource Officers (CRO), Crime Reduction Team (CRT), Ceasefire (CF), Walking Units, Argus, Traffic, and Investigations.

Custom hot lists can have a variety of responses. They range from responding to conducting an enforcement action or identifying the reads and alerts to further one's investigation.

Outside agencies do not always provide OPD with a response or notify OPD of their hot lists and outcomes. Each agency has access to their own Success Stories feature via the Flock 'Edit Outcome' link; which allows agencies to document their enforcement actions.

Quarterly, there are Flock meetings where Bay Area agencies come together to discuss success stories and improvements which can be made to the Flock products and areas where they would like to see the system improved. At times, outside agencies will share their success stories, such as the one listed here:

- SLPD was dispatched to an armed robbery (firearm) at the Quick Stop located at 1001 MacArthur Blvd in San Leandro. Recorded video surveillance was obtained from the interior and exterior of Quick Stop. The Primary Officer recognized the suspect vehicle associated with a vehicle burglary from February 13, 2025. A records check showed the suspect vehicle was reported stolen to the Oakland Police Department on January 28, 2025. (OPD Case 25-4569). Detectives utilized both San Leandro Flock and Oakland Flock. The Oakland Flock (Camera #194) was utilized as it led detectives to the area of Fruitvale Avenue and E 27th Street. Detectives canvassed this area waiting for additional Flock hits. SLPD Detectives located the suspect vehicle (Toyota Tacoma CA <redacted>) parked and occupied at 2301 Foothill Blvd. OPD's Argus Unit (helicopter) responded and assisted SLPD detectives. The suspect was safely taken into custody. The suspects clothing worn during the armed robbery, cash from the robbery, beanie worn during the armed robbery and firearm were all located on the suspect person and in the stolen Tacoma.

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 Oakland Police Department has shared our Flock ALPR Data with the following entities in 2024:

- Alameda (City) Police Department
- Alameda County Sheriff's Office
- Alameda County Sheriff's Office- Dublin Police
- Burlingame Police Department
- CA State Parks
- Cal Fire - Law Enforcement
- California Highway Patrol
- Campbell PD
- Colma Police Department
- Concord (CA) PD
- Daly City Police Department
- Danville PD
- Dixon Police Department
- East Bay Regional Park District Police
- East Palo Alto Police Department
- El Cerrito PD
- Emeryville Police Department
- Fairfield California Police Department

Fremont Police Department
Hayward Police Department
Livermore Police Department
Los Altos PD
Marin County Sheriff's Office
Mountain View Police Department
Napa County Sheriff's Office
Northern California Regional Intelligence Center (NCRIC)
Newark (CA) Police Department
Novato PD
Piedmont Police Department
Pleasant Hill Police Department
Pleasanton Police Department
Redwood City PD
Richmond (Calif) Police Department
Sacramento County Sheriff's Office
San Bruno Police Department
San Francisco Police Department
San Leandro Police Department
San Mateo County Sheriff's Office
San Mateo Police Dept
San Ramon Police Dept.
Santa Barbara Sheriff's Office
Santa Clara County Sheriff's Office
Santa Clara Police Department
SF District Attorney's Office
Solano County Sheriff's Office
Sunnyvale Department of Public Safety
Union City PD
Vacaville Police Department
Vallejo Police Department
Watsonville Police Department

To obtain access to our Flock database, each organization had to fill out a permission form and agree to the following questions:

- Do you agree to the following: I confirm, on behalf of my agency or department, in compliance with state law, OPDs ALPR data SHALL NOT be used or shared with other agencies for the purpose of pursuing criminal charges or civil enforcement against individuals for obtaining, providing, or supporting reproductive or gender affirming health care services, to ensure that the medical and legal rights of residents of and visitors to Oakland, a Sanctuary City, remain intact.
- Do you agree to the following? I confirm, on behalf of my agency or department, that anytime we access OPDs ALPR data, there will be a need to know and right to know.
- Do you agree to the following? I confirm, on behalf of my agency or department, that anytime we access OPDs ALPR data, we will document the following: PC/VC related to the incident, and the department incident or administrative investigation number.

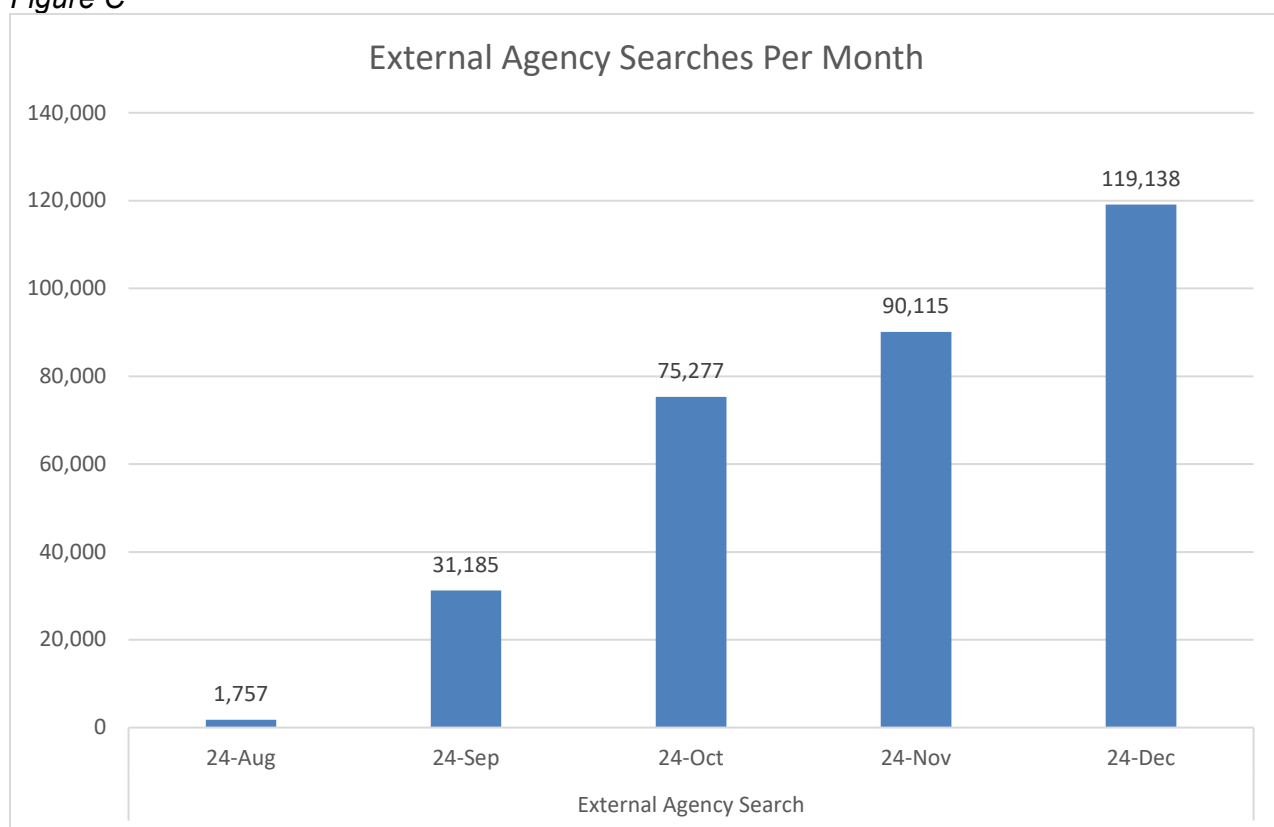
After agreeing to those three questions, the requesting agency was granted access, with approval being logged in a spreadsheet. This information is in **Attachment A – PAC 2024 Annual Report Data** on the tab called “Third Party Data Sharing”. Any time our information is accessed, a log is created and kept in the Flock system. The second question in the permission form states that agencies will only request to search against

our database if they have the need to know and right to know, therefore, any searches the agency completes after signing the permission form meets the obligations required with DGO I-12. This permission form was reviewed and approved by the PAC Chair, Brian Hofer, on July 9th, 2024.

OPD is working with Flock to distribute the OPD Permission form to agencies who have not received it. Each agency, like OPD, have Flock administrators, who will fill out the form. Of note, OPD has discovered that other agencies have begun to similarly send their own respective permission forms to grant access to their information.

Figure C shows the number of searches that have been done against our data, month over month, in 2024. All the entities listed previously can execute searches against our data. If there is a match in our system, they will be presented with a screenshot which shows the following information:

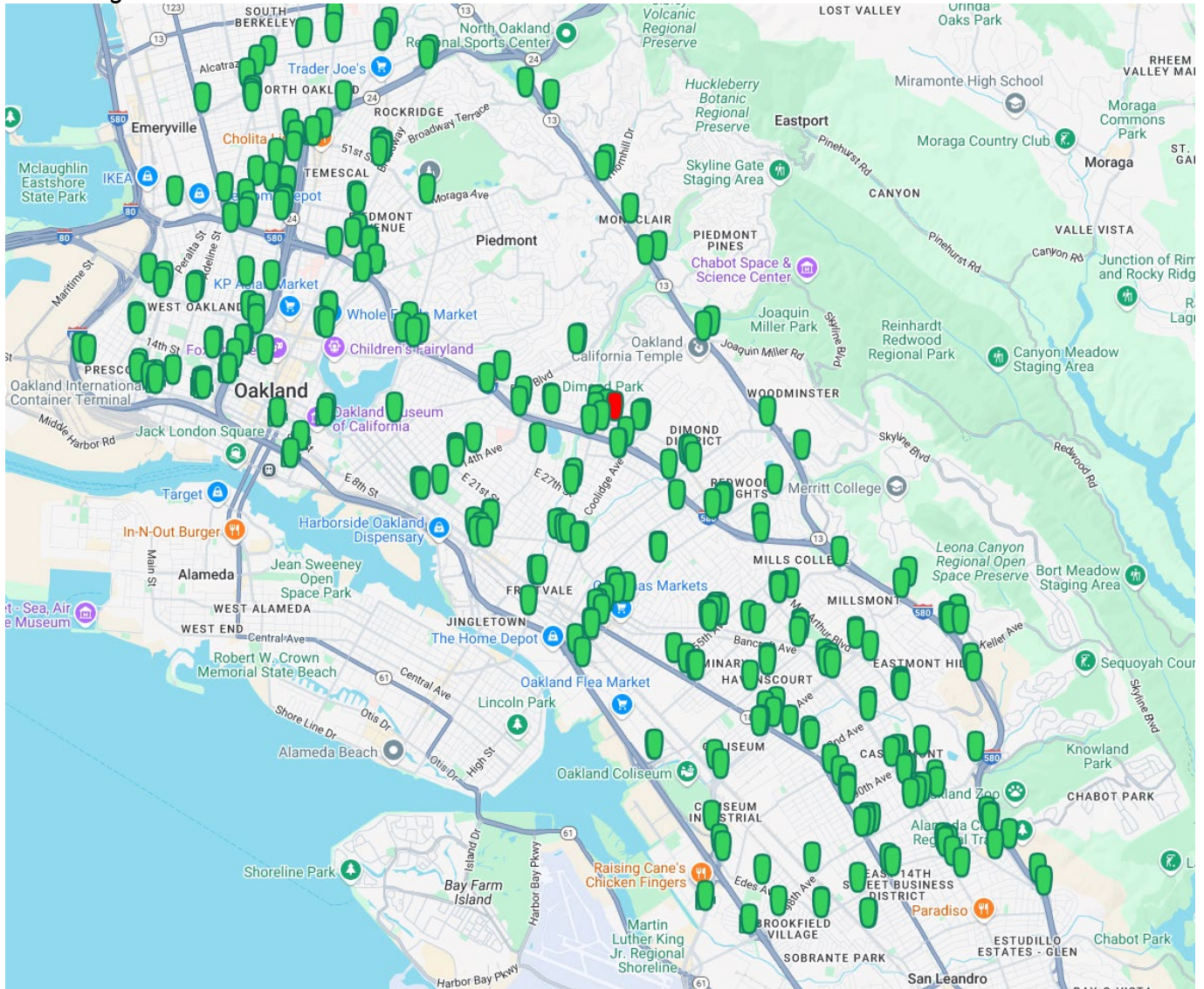
Figure C



- 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:

Working in conjunction with the OPD, Flock analyzed heat maps as it relates to violent crime and property crime (stolen vehicles, burglaries, and grand theft) and identified the main egress and ingress locations to these hot spots. As a result, 290 locations were selected for camera placement. These cameras are currently the only source of data, that are OPD assigned, feeding into the Flock system. Further information is provided below in **Figure D**:

Figure D



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

A total of 290 ALPR cameras were funded and deployed throughout the City of Oakland. There are six geographical policing areas that OPD identifies: Area 1 – Area 6.¹

Based on crime data and identifying the main egress and ingress locations to these hot spots, the 290 cameras were deployed within the respective six areas as follows:

- Area 1: 44
- Area 2: 57
- Area 3: 23
- Area 4: 55
- Area 5: 51
- Area 6: 60

¹ [City of Oakland | Oakland Police Areas](#)

- 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.

The Oakland Police Department requests a waiver of this requirement, as Flock Cameras cannot determine the race of an individual, since the primary focus is on capturing the vehicle license plate. In addition, OPD has not received specific feedback from the public on the ALPR system in 2024, outside of PRR requests, which are summarized in Section I.

- 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:

The Oakland Police Department is not aware of any violations or potential violations of the Surveillance Use Policy.

Per DGO I-12, "the records of database investigatory queries, third party data sharing, and hot list entries shall be incorporated into the annual report..."

In addition, "ALPR system audits shall be conducted annually to ensure proper system functionality and that designated personnel are using the system according to policy rules via sample audits and reviews of training records".

To satisfy the first requirement, please see [Attachment A – PAC 2024 Annual Report Data](#). In this spreadsheet, there are several tabs that house the specific data being requested. The tab labeled Third Party Data Sharing lists all the organizations which have access to search against OPDs database of images in Flock. The tab labeled Hot List Entries has the hot lists which OPD created. Finally, the database investigative queries were split into two tabs, Database Queries (AugSepOct), which houses all investigative queries from August, September and October in 2024 and Database Queries (NovDec), which houses all investigative queries performed in November and December 2024. While cameras were first installed in July, OPD started training in August and that is when searches began.

The audit information begins on the tab labeled Database Queries Audit. This audit was done by doing a randomized audit of 398 records. Originally, 400 records were selected, but one was a test search and the other generated an error upon data extraction and had to be removed from the dataset. OPD then looked at the "reason" provided for the search. Per DGO I-12, there are several elements that are required to perform a database investigative search: the date and time the information is accessed, the license plate number or other data elements used to query the system, the username of the person who accesses the information, and the purpose for accessing the information.

This information is labeled as the Database Queries Audit Tab in the spreadsheet. The fields labeled as RD/LP Included and Type of Crime Included were the basis of the audit. Since the Flock system logs of all the other information by default when a user initiates a database investigative query, the users are left to enter their reasons manually.

To meet the requirements defined in DGO I-12, OPD has asked staff to standardize their reason to include the report number or incident number, which can start with RD (which stands for Records Division) or LOP (which designates the CAD incident as bellowing to Law – Oakland Police). In addition, we ask that users put in the crime associated with the search, preferably in the form of the penal code or vehicle code, but a written crime reason is also acceptable. Based on this criteria, 398 records were evaluated. Below are the results of the audit, which show that OPD had a report or incident number included in 99% of the audited files and had the crime included in 97% of the audited files.

Total RD/LP "Yes"	395
Total RD/LP "No"	3
Total Type of Crime "Yes"	388
Total Type of Crime "No"	10
RD/LP Included - Audit Pass Rate	99%
Crime Included - Audit Pass Rate	97%

While DGO I-12 only calls for an annual audit, OPD began auditing records to meet these standards immediately. During the first few months of training, OPD sent out weekly or bi-weekly emails identifying users who had incomplete search parameters. This tenacity ensured that our new users understood the requirement and reinforced the importance of properly documenting database investigative queries, as required by DGO I-12. Emails are still sent out periodically to remind individuals of the requirements.

DGO I-12 also calls for a review of training records to ensure that only authorized users are utilizing the ALPR system. Please refer to the tab labeled Training Roster to see a list of all individuals at OPD who have been trained on the policy and use of the Flock ALPR system. There are approximately 246 people who have been trained as of the writing of this report. A random selection of 25 users was selected from those who were audited in the Database Queries Audit. Of the 25 selected users, all 25 were found to have completed training.

As it relates to user/access management, OPD does not manually disable users who separate from the department, as Flock utilizes single sign on with the City of Oakland's Microsoft Office 365 application. When a member or employee separates from the department, the Information Technology Department (ITD) is responsible for disabling the Microsoft Office 365 account, which will, in turn, disable the Flock account.

- 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:

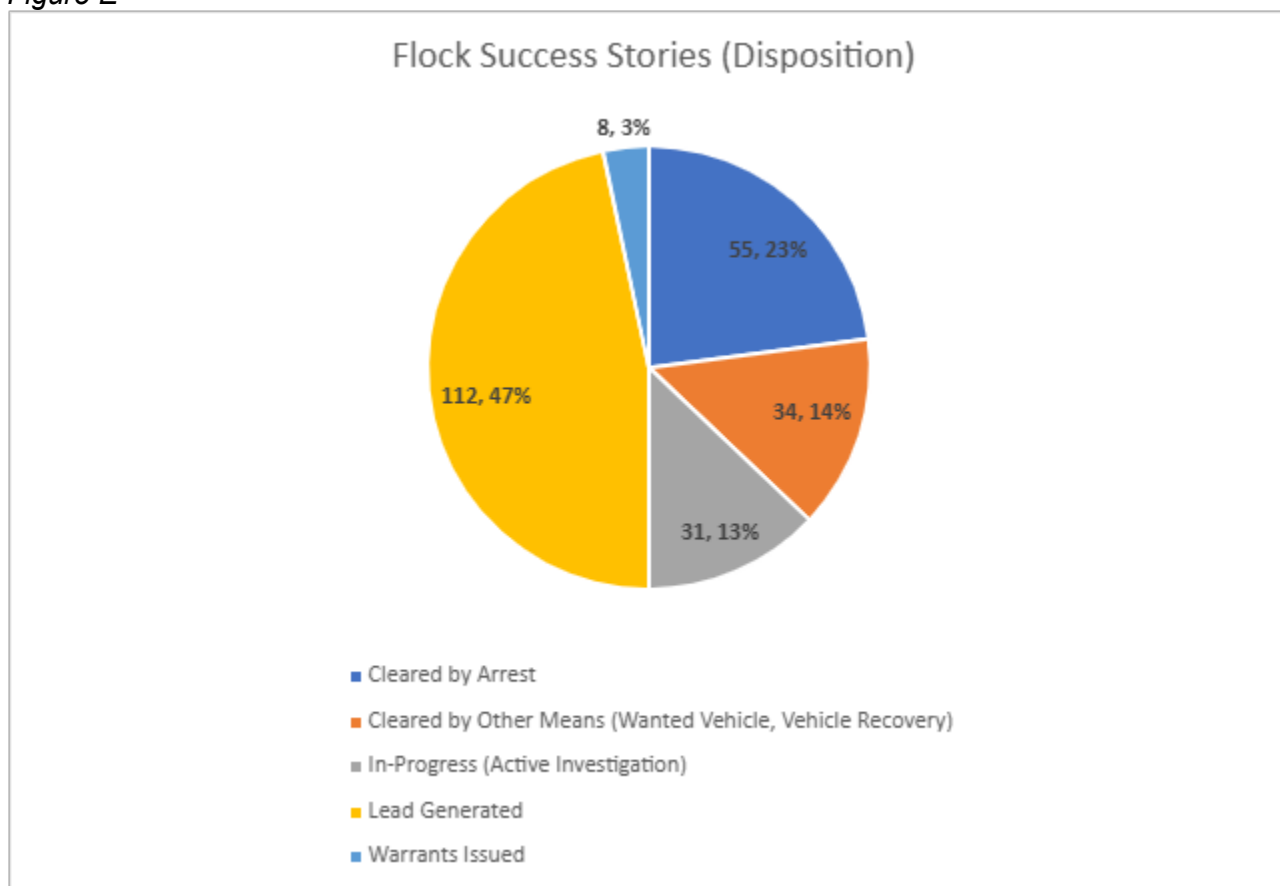
The Oakland Police Department reached out to Flock and on January 14th, 2025, received a response from Flock attesting that "Flock did not suffer any security breaches as it relates to our infrastructure, [or] unauthorized access to data collected by the surveillance technology". The Director of Risk and Compliance at Flock was copied on the response, which was authored by our Customer Success Manager at Flock.

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

OPD was also able to better track the outcomes of utilizing ALPR as an investigative tool. All the information that follows can be found on the tabs labeled Flock Outcomes (Enforcement) and Flock Outcomes Metrics in the PAC 2024 Annual Report Data spreadsheet.

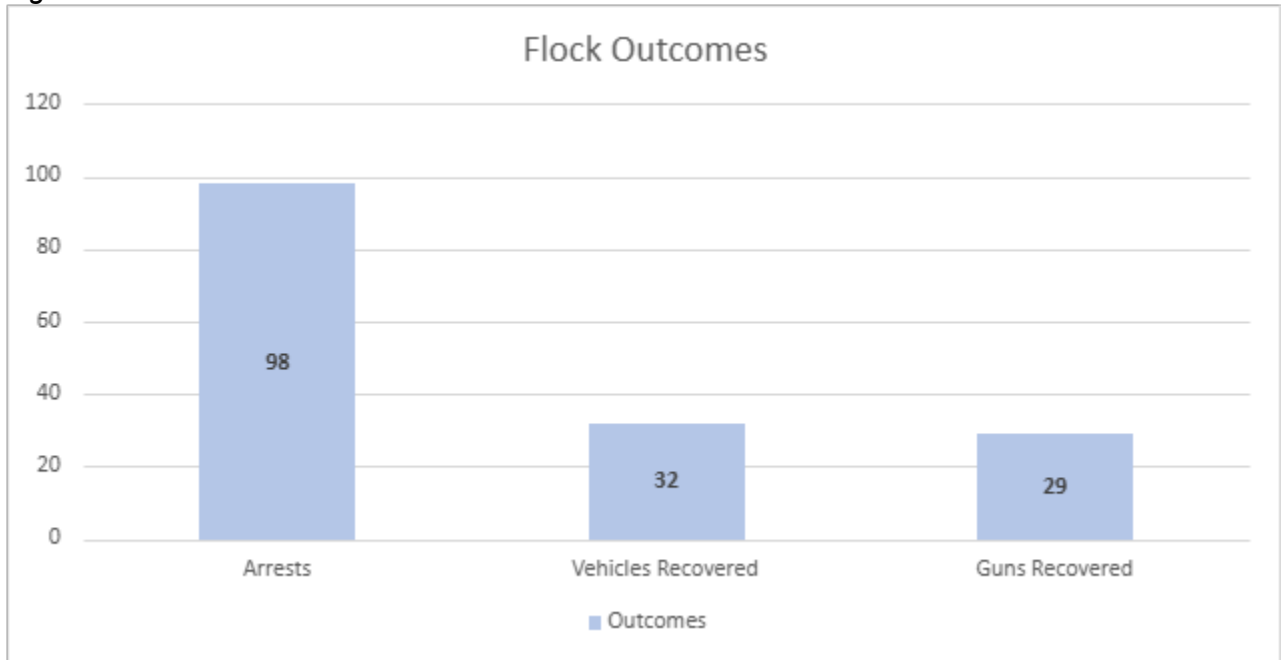
As shown in **Figure E** below, OPD logged a total of 240 enforcement actions in Flock from August 2024 through February of 2025. Based on these actions, OPD was able to generate 112 leads, 55 were cleared by arrests, 34 were cleared by other means such as vehicle recovery, 31 are in-progress investigations, and 8 warrants were issued.

Figure E



Summarization of all outcomes shows that OPD made 98 arrests, recovered 32 vehicles, and recovered 29 guns, as seen in **Figure F** below:

Figure F



OPD, through a manual review of the data, was able to determine the offense linked to each of these outcomes as listed below in **Table A**. Some areas of note are Robbery+, which includes elements such as armed robbery or a strongarmed robbery, which had 38 arrests, 17 vehicles recovered, and 4 guns recovered. In addition, Flock was used to make 7 arrests, recover 2 vehicles, and recover 8 guns in homicide/murder/manslaughter investigations. Moreover, for Robberies, OPD made 15 arrests, recovered 2 vehicles and 3 guns. Finally, for aggravated assault, OPD recorded 10 arrests, and 6 guns recovered. In the short few months that OPD has had Flock, it has proved an invaluable investigative tool.

OPD has quickly identified vehicle(s) of interest related to crimes and quickly identified vehicle(s) utilized in a series of crimes. These still images are sent via email to officers and hot listed and officers have had quickly solved cases.

Table A

Offense	Arrests	Vehicles Recovered	Guns Recovered
Aggravated Assault	10	0	6
Burglary	2	2	0
Carjacking	3	2	0
Criminal Threats/Domestic Violence	2	0	0
Felony Evading	5	0	0
Homicide	3	2	5
Motor Vehicle Theft	5	5	0
Human Trafficking	3	0	1

Murder/Manslaughter	4	0	3
Prostitution	1	0	2
Rape	1	0	0
Robbery	15	2	3
Robbery +	38	17	4
Weapons Possession	1	0	2
Weapons Possession +	4	0	2
Other	1	2	1
Total	98	32	29

Finally, here are three example cases that demonstrate the usefulness of Flock cameras to OPD:

- RD#24-044602: On 06 Sep 24, a robbery occurred in the area of 3315 High St. Surveillance cameras captured the suspect vehicle. Investigators utilized FLOCK technology to help identify recent locations for the suspect vehicle. Within 6 hours, Ceasefire officers and the OPD helicopter located the vehicle and some of the suspects in the act of committing another robbery. The helicopter's presence interrupted that robbery and then followed the suspects throughout the city, eventually arresting two suspects near the Rockridge BART station. Additional suspects were identified and warrants for their arrests have been obtained. This is still an active investigation. The suspects referenced herein are male, adult, Oakland residents.
- RD#24-044939: On 08 SEP 24, around 1830 hours, a road rage incident occurred in the area of 19th Street and Market St. The two involved drivers exited their vehicles and engaged in an argument. One of the two drivers fired a gun towards the other driver. The other driver was not injured. The suspect fled the scene. Nearby surveillance cameras captured images of the suspect's vehicle. Investigators utilized FLOCK technology to alert nearby law enforcement agencies as to the description of the vehicle. On 13 Sep 24, officers with the Newark Police Department located and arrested the suspect based on the alerts disseminated by OPD. The arrestee was a male, juvenile, in possession of a handgun.
- RD# 24-045769: A PC246 (Shooting at a Building) occurred on 12 Sep 24, at about 1824 hours in front of 8501 International Blvd (Allen Temple Baptist Church). Surveillance video captured images of a suspect vehicle. On 14 Sep 24, investigators utilized FLOCK technology to identify a possible match, sharing that information with field units. Within 12 hours, OPD officers had located the suspect vehicle and arrested the driver in possession of a firearm. The driver provided a statement to investigators linking him to the shooting of the Church. The arrestee is a male, adult, Oakland resident.

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

OPD received four (4) Public Records Requests (PRRs) in 2024 that were related to ALPR technology, three are responded to and one awaits completion of our response. The requests are summarized below:

- 24-10626 – Requesting a list of all Flock camera locations
- 24-1170 – Requesting the names of agencies with whom OPD shared Flock data, the agencies from which OPD receives Flock data, the names of agencies with whom OPD shared hotlist information and the names of

agencies from which OPD received hotlist data from. The request also asked for the number of total plate detections and total hotlist detections for 2024.

- 24-12841 – which asked for all records related to any surveillance technology – this is still pending due to large of amount of data it will generate
- 24-5161 – which asked for any ALPR logs, names of agencies who we receive data from, names of agencies who receive hotlist information from OPD, hits or detections from hotlists, and any communications between OPD and Kaiser Permanente relating to ALPR

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:

The estimated cost for Flock for the first year is approximately \$500,000, due to the way that cameras were prorated based on their use in the first contract year. OPD anticipates that the next year of Flock service will cost approximately \$1,000,000 and this will come out of the Oakland Police Department's budget. Funds will be allocated from the General-Purpose Fund (1010), Information Technology Unit Org. (106410), Contract Services Account (54919), Administrative Project (1000008), Agency-wide Administrative Program (PS01).

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

OPD has no requests 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, Dr. Carlo M. Beckman, at cbeckman@oaklandca.gov.

Respectfully submitted,

Dr. Carlo M. Beckman

Dr. Carlo M. Beckman, Project Manager II
OPD, Bureau of Risk Management, Information Technology & Fleet

Reviewed by:
Dr. Tracey Jones, Police Services Manager I
OPD, Bureau of Risk Management, Research & Planning

Prepared by:
Dr. Carlo M. Beckman, Project Manager II
OPD, Bureau of Risk Management

Lt.. Omar Daza-Quiroz
OPD, Bureau of Investigations

A/Lt. Gabriel Urquiza
OPD, Bureau of Investigations, Real-Time Operations Center

Policy

415

Oakland Police Department

Policy Manual

Immigration

415.1 PURPOSE AND SCOPE

The purpose of this immigration policy is to provide guidance and direction to the members of the Oakland Police Department (OPD) on Federal, State, and local immigration laws.

The responsibility for enforcement of immigration laws rests solely with the U.S. Immigration and Customs Enforcement agency (ICE) under the direction of the United States Department of Homeland Security (DHS), and not with local or state law enforcement agencies. OPD is committed to equal enforcement of the law and equal service to the public regardless of a person's immigration status. This commitment increases our effectiveness in protecting and serving the entire community.

415.2 DUE PROCESS RIGHTS OF ALL PERSONS

OPD shall not provide federal immigration agencies access to individuals solely for the purpose of immigration enforcement.

If OPD receives a federal immigration detainer request for an individual in OPD custody, Officers shall provide the individual with a copy of the request.

Officers shall not inquire or request proof of immigration status or citizenship when providing services or benefits except where the receipt of such benefits or services is contingent upon one's immigration status, such as in the processing of a U visa or T visa.

Individuals with limited English proficiency must be given access to translation or interpretation and must receive documents in their native language if available.

415.3 FEDERAL LAW

The responsibility for enforcement of immigration laws rests solely with ICE, under the direction of DHS.

Immigration detainers or requests, sometime called "ICE holds," are not compulsory. Instead, they are merely requests enforceable at the discretion of the agency holding the arrestee. Federal regulations define immigration detainers as "requests" rather than commands.¹ Courts have also held that ICE detainers are voluntary requests that "do not and cannot compel a state or local law enforcement agency to detain suspected aliens subject to removal."² Thus, local agencies are "free to disregard [an] ICE detainer."³

¹ 8 C.F.R. § 287.7(a).

² *Galarza v. Szalczyk*, 745 F.3d 634 (3rd Cir. 2014); see also *Flores v. City of Baldwin Park*, No. CV 14-9290-MWF, 2015 WL 756877, at *4 (C.D. Cal. Feb. 23, 2015) ("federal law leaves compliance with immigration holds wholly within the discretion of states and localities").

³ *Galarza*, 745 F.3d at 645.

Oakland Police Department

Policy Manual

Immigration

The mere fact that an individual is unlawfully in the United States is not a criminal offense.⁴ Thus, unlawful presence in the United States, by itself, does not justify continued detention beyond that of an individual's normal release date. This applies even where ICE or United States Customs and Border Protection (CBP) provide an OPD officer with administrative forms that use the terms "probable cause" or "warrant." A lawful detention under the Fourth Amendment must be supported by probable cause that a person has committed a crime.⁵

415.4 CITY POLICY

Members of OPD shall not:

- Enforce or assist ICE in the enforcement of violations of civil immigration laws
- Initiate investigations or use personnel or resources where the only objective is to discover whether an individual is in violation of a civil immigration law
- Detain individuals for a violation of civil immigration law⁶

415.5 REQUESTS FOR ASSISTANCE FROM DHS OR ICE

Unless the circumstances present an imminent danger to officer or public safety, requests by DHS or ICE for any operational assistance from OPD (including but not limited to ICE detainer requests), shall immediately be directed to the watch commander on duty for approval, who in turn shall immediately notify the Chief of Police, or the Chief's designee.

In the event a determination needs to be made about whether an ICE detainer request should be fulfilled, the Chief of Police, or the Chief's designee, shall consider the merits of each request carefully. In making this determination, the Chief, or Chief's designee, shall comply with the California TRUST Act,⁷ assess whether the individual poses a risk to public or officer safety, and consider the availability of OPD personnel and resources necessary to comply with the request.

415.6 INFORMATION SHARING

OPD does not collect any information regarding a person's immigration status, unless the information is gathered specifically for the purposes of completing U visa or T visa documents.

Officers shall not share non-public information about an individual's address, upcoming court date, or release date with ICE or CBP. Officers shall respond to an ICE or CBP request for non-public information only when a judicial warrant accompanies the request.

⁴ *Arizona v. United States*, 567 U.S. 387, 132 S. Ct. 2492, 2505 (2012); *Melendres v. Arpaio*, 695 F.3d 990, 998, 1000 (9th Cir. 2012).

⁵ *Gerstein v. Pugh*, 420 U.S. 103, 120 (1975).

⁶ See November 29, 2016, Oakland City Council "Resolution Denouncing Tactics Used to Intimidate Immigrants Residing in Oakland and Re-affirming the City's Declaration as a City of Refuge" (Resolution No. 86498).

⁷ See Gov't Code, §§ 7282, 7282.5. The TRUST Act limits the discretion of law enforcement officials to detain an individual pursuant to a federal immigration detainer request, should an agency choose to do so, unless two conditions are met. First, the continued detention must "not violate any federal, state, or local law, or any local policy," and second, the detainee must have a qualifying criminal history as enumerated in Government Code section 7282.5(a) or be the subject of an outstanding federal felony arrest warrant.

Immigration

415.7 U VISA AND T VISA NONIMMIGRANT STATUS

Under certain circumstances, federal law allows temporary immigration benefits, known as a U visa, to victims and witnesses of certain qualifying crimes. Similar immigration protection, known as a T visa, is available for certain qualifying victims of human trafficking.

Any request for assistance in applying for a U visa or T visa should be forwarded in a timely manner to the Special Victims Section (SVS) Lieutenant for review and endorsement. The SVS Lieutenant may consult with the assigned investigator to confirm the applicant is cooperative with the investigation.

The SVS Lieutenant or their designee shall approve or deny the request and complete the certification or declaration, if appropriate, within the time frame required under Penal Code § 679.10(h).⁸ The instructions for completing certification and declaration forms can be found on the U.S. Department of Homeland Security (DHS) website and under Penal Code § 679.10.

The OPD website has information regarding the U visa or T visa application process as well as a non-profit organization that can assist with the application process.

⁸ "A certifying entity shall process an I-918 Supplement B certification within 90 days of request, unless the noncitizen is in removal proceedings, in which case the certification shall be processed within 14 days of request." Penal Code § 697.10(h).



For Immediate Release: July 14, 2025

OPD News:

An article released today by the *San Francisco Standard* initially stated, "*Oakland cops gave ICE license plate data.*" It went on to say, "*Oakland Police fulfilled a request related to an ICE investigation on one occasion.*" Both versions are misleading and do not accurately reflect the Oakland Police Department's data-sharing agreement with other California and local law enforcement agencies.

To be clear, no member of the Oakland Police Department was involved in this alleged sharing of ALPR information with Immigration and Customs Enforcement (ICE).

Oakland began using its current Automated License Plate Reader (ALPR) system in July 2024. ALPR cameras capture and read license plate information to aid in the investigative process. This system has become a valuable tool in helping our officers solve crimes more efficiently, locate homicide and robbery suspects, and recover firearms. By providing timely and accurate information, ALPR technology helps our officers respond quickly to public safety threats.

Consistent with SB 34, OPD shares ALPR data with more than 80 California local and state law enforcement agencies. All of these agencies, including OPD, are subject to the California Values Act, which prohibits agencies from using resources for immigration enforcement purposes.

In compliance with city policy, OPD does not enforce or assist Immigration and Customs Enforcement (ICE) officials in enforcing civil immigration law violations.

Additionally, ALPR data captured within the City of Oakland shall not be used in violation of Oakland's Sanctuary City Ordinance.

In OPD's data sharing request form, we require all agencies using our system to "be in compliance" with state law.

As it relates to the sharing of data with any federal agency, OPD is verifying that any access conducted by its members related to APLR data remains consistent with state law, including SB 34 (California Civil Code section 1798.90.5 et seq.) and the California Values Act (Gov Code section 7284 et seq.).

We (OPD) are very conscientious and sensitive to the use of emerging technology while continuing to explore solutions to support public safety, protect people's right to privacy, and build community trust.

We are committed to transparency, accountability, and maintaining the trust of our community. We value our relationship with our media partners and want to ensure and encourage that the information they provide is accurate.



MEMORANDUM

TO: PAC

FROM: Yun Zhou, Sergeant of Police
OPD, Criminal Investigation Division

SUBJECT: Forensic Logic CopLink /
CrimeTracer System – 2024
Annual Report

DATE: May 12, 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 PAC, 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.

Oakland Police Department (OPD) Department General Order (DGO) I-24: Forensic Logic CopLink / LEAP, as well as OMC 9.64.040 together require that OPD provide an annual report to the Chief of Police, the PAC, and Public Safety Committee. The information provided below is compliant with these annual report requirements.

DGO I-24 explains that authorized members may use CopLink for the purpose of searching the system in the service of conducting criminal investigations, such as apprehending subjects, locating and returning stolen property, as well as in the protection of the law enforcement officers encountering the individuals described in the system. Authorized purposes also include other appropriate OPD organizational investigations (e.g., internal affairs, missing persons, and use of force investigations).

In 2023, CrimeTracer was introduced as the next iteration of CopLink. Forensic Logic also rebranded to SoundThinking. The product being used by OPD is now called SoundThinking CrimeTracer. OPD began migrating its user accounts in August of 2023 from CopLink to CrimeTracer. Functionally, it is the same product and consists of the same features and security. The only change made to the product is the name, logo and color scheme. Since the 2023 Annual Report, OPD has referred to the product as CrimeTracer.

Captain Nicholas Calonge, Criminal Investigation Division Commander, was the Program Coordinator for 2024.

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

CrimeTracer search technology is used regularly by both OPD sworn field / patrol personnel and command staff. Search parameters include the following criteria which are submitted to a search engine where data originating from law enforcement records, calls for service, field interviews, arrest/booking records and citations are stored:

- License plate numbers
- Persons of interest
- Locations
- Vehicle descriptions
- Incident numbers
- Offense descriptions/penal codes
- Geographic regions (e.g., Police Beats or Police Areas)

Data is stored in an FBI Criminal Justice Information Service (CJIS) compliant repository in the Microsoft Azure GovCloud.

In 2024, there were a total of 423 users accounts who conducted Forensic Logic searches, for a total of 204,750 separate queries. Table below breaks down this search data by month and by distinct user and total searches.

Table 1: OPD CrimeTracer Searches; by Distinct User and Search Totals – 2024

CrimeTracer

Search Type	January	February	March	April	May	June
<i>Number of OPD distinct users in each month</i>	174	234	258	255	263	276
<i>Number of searches conducted</i>	15,068	15,838	17,104	17,386	20,604	18,278

Search Type	July	August	September	October	November	December
<i>Number of OPD distinct users in each month</i>	282	268	253	214	196	200
<i>Number of searches conducted</i>	19,756	19,443	18,521	16,646	12,563	13,543

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):

Data searched with the CrimeTracer system is entirely acquired from incident reports, citations, calls for service and field interviews that have already been recorded in originating Records Management Systems, Computer Aided Dispatch Systems, and Mobile Field Reporting Systems – from both OPD systems as well as from other law enforcement agency systems (other SoundThinking client agencies). The data is collected from OPD systems at least once every 24 hours; once the data is collected and resides in the SoundThinking

cloud repository, it is made available to agencies subscribing to the service who are permitted by their agency command staff to access CJIS information.

CrimeTracer does not keep statistics on who searched and viewed the data shared, but the system can be audited for a specific search.

Data sourced from the Oakland Police Department cannot be accessed by US DHS ICE nor US DHS CBP staff.

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

The CrimeTracer service is a web portal accessible by authorized OPD users on OPD computers with an appropriate user-id and password (criteria for both defined by FBI CJIS Security Addendum). OPD data sources that provide data accessible to the search tool include the following:

- Arrest records
- Field contacts
- Incident reports
- Service calls
- ShotSpotter Activations
- Stop Data reports
- Traffic Accident reports

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

Not applicable. The technology is a web portal that is accessible to computers on the OPD network.

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 PAC 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 PAC makes such a determination, written findings in support of the determination shall be included in the annual report submitted for City Council review.

No community complaints or concerns were communicated to staff in 2024.

OPD is not able to provide the race of each person connected to each query. The technology is intended as a search engine of records (section C), not all queries would contain the race data of the person subject to the technology's use. OPD would have to individually evaluate tens of thousands of searches to provide the requested race data. Staff

recommends the PAC makes the 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.

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

No internal audit was conducted on CrimeTracer in 2024.

Staff was not made aware of any criminal or administrative investigation pertaining to the misuse of the technology in 2024.

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

There were no identifiable data breaches or known unauthorized access during 2024.

H. Information, including case examples, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes:

Homicide Case Examples

During the investigation of a homicide in the first quarter of 2024, the investigator searched CrimeTracer for prior incident reports involving the victim. One report detailed a recent argument involving the victim and another individual. A further search of field contact data showed the same individual had been contacted in the vicinity of the homicide scene days prior. This individual was later identified as the suspect and arrested.

During the investigation of a homicide in the third quarter of 2024, officers recovered a vehicle description from a witness. A CrimeTracer search of traffic accident reports found a recent collision involving a matching vehicle. The listed driver had prior arrests for firearm-related offenses. Further searches linked the driver to the scene, and the individual later identified as the homicide suspect.

Shooting Case Example

During the investigation of a shooting in the second quarter of 2024, the investigator reviewed prior ShotSpotter activations near the scene. A CrimeTracer search of field contacts within the activation radius showed an individual stopped minutes after a prior incident. That individual matched the description of the suspect provided by a witness. A review of prior arrests confirmed a history of gun-related charges. This information assisted in proving this individual to be the shooting suspect.

Burglary Case Examples

During the investigation of a residential burglary in the second quarter of 2024, officers identified a unique item stolen from the scene. A search in CrimeTracer showed a recent field contact where the same item was described in the narrative in the possession of a

particular individual. Investigators followed up and later arrested the individual for the burglary.

Robbery Case Example

In the first quarter of 2024, patrol officers responded to a robbery where the suspect fled in a vehicle. The license plate was provided by a witness. A CrimeTracer search located a recent contact report involving the vehicle. One of the listed occupants had multiple prior arrests for robbery and was wearing clothing matching the description given by the victim. That individual was eventually arrested for the robbery.

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

There are no existing or newly opened public records requests relating to the technology.

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

Description		Amount
Contract Start Date 7/1/2025 Contract End Date 6/30/2026		
197-0000-04 CrimeTracer	CrimeTracer Enterprise Subscription for Term 7/1/2025-6/30/2026	\$227,500.00
197-0000-04 CrimeTracer	COPLINIK Connect	\$10,000.00
197-0000-04 CrimeTracer	CompStat, per user subscription (60 users @ \$1,000 each)	\$0.00
197-0000-04 CrimeTracer	General Purpose and Maintenance Services	\$25,000.00
		Total \$262,500.00

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

No requests for changes at this time.



MEMORANDUM

TO: PAC

FROM: Sgt. Y. Zhou
OPD, Criminal Investigation Division

SUBJECT: Annual Report – Cellebrite / Mobile
Forensic Extraction Device

DATE: MAY 13, 2025

Background

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

- The benefits to the community of the surveillance technology outweigh the costs, and 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.

Sgt. Y. Zhou is currently the program coordinator for OPD's mobile device extraction.

2024 Annual Report Details

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

Cellebrite Premium (current version being used by OPD) is used to extract data from a mobile device. The tool supports both logical and physical extractions, allowing access to data including call logs, SMS/MMS, contacts, browser history, application data (e.g., WhatsApp, Facebook, Signal), emails, GPS/location data, and deleted content when available. The amount and type of data gathered depends on the device model, operating system, and encryption level. The Cellebrite tool does not conduct live surveillance; it performs a one-time data extraction from a seized device.

OPD has owned and used an old Cellebrite UFED device prior to bringing the mobile forensic extraction policy to PAC. OPD began the required data collection in February 2024 when the policy was passed. However, OPD did not acquire the updated Cellebrite device until July 2024. The difference between these two devices is significant. Prior to the acquiring the updated Cellebrite device in July 2024, OPD has no real capability to extract data from a locked device without the passcode.

OPD utilizes the Cellebrite tools in both administrative and criminal investigations. Administratively, OPD is required to conduct random quarterly audits of work phones belonging to OPD members. OPD Internal investigations will also download and examine member work phones pertaining to internal investigations. Given the nature of these investigations, the program coordinator can only facilitate the extraction of OPD work

phones and do not know whether these phones were selected as a random audit or as part of an investigation. From February 2024 to December 2024, OPD has conducted 30 internal work phone searches. OPD members are required to provide a passcode to IAD for these extractions, as such, they are equally as successful on the older Cellebrite or the newer Cellebrite device.

For criminal investigations, OPD is allowed to conduct consent, exigency, and search warrant searches of mobile devices / tablets. From February 2024 to December of 2024, OPD has conducted 1 consent search of a mobile device and 271 searches of a mobile device pursuant to a search warrant.

From February to June of 2024, when OPD was utilizing the older Cellebrite UFED device, OPD extracted or attempted to extract data from 35 devices as pertaining to a criminal investigation. After acquiring the updated Cellebrite device, 237 devices were extracted or attempted to be extracted by OPD as pertaining to a criminal investigation. Out of those devices, 39 devices were unable to be extracted by OPD.

Extractions by Investigation Type (February – June 2024)

Investigation Type	Number of Extractions
IAD (Internal Affairs)	26
Homicide	25
Robbery	7
Felony Assault (Shooting, stabbing, non-fatal)	3

All non-IAD related devices were accessed and extracted pursuant to a search warrant.

Extractions by Investigation Type (July – December 2024)

Investigation Type	Number of Extractions
Homicide	110
Robbery	46
Felony Assault (Shooting, stabbing, non-fatal)	40
Firearm-related (Brandishing, illegal possession)	18
Sexual Assault	13
Burglary	6
IAD (Internal Affairs)	4
Human Trafficking	3
Hit and Run	1

Only one device was downloaded with the consent of the owner in a robbery investigation; the owner of the device was a suspect in the robbery and provided consent to search his / her device during a recorded interview with OPD investigators. All other non-IAD related devices were accessed pursuant to a search warrant.

- 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):

OPD shares mobile device extraction data obtained through Cellebrite with prosecutorial agencies as part of ongoing criminal prosecutions. The data is shared with agencies such as the Alameda County District Attorney's Office and federal prosecutorial office as part of the routine discovery process. These disclosures are made at the request of the prosecuting attorney and are standard practice during the course of prosecution. OPD does not maintain separate records of each instance in which data is shared for discovery, as these requests are part of the broader prosecution effort and not tracked independently by OPD. OPD has not shared any Cellebrite extraction data with U.S. Immigration and Customs Enforcement (ICE), the Department of Homeland Security (DHS), or U.S. Customs and Border Protection (CBP).

- 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:

The Cellebrite Premium phone extraction tool is located within the OPD CID office and connected to a computer that access the OPD network. It is not taken into the field. The tool is used on mobile devices or tablets (both Android and iOS) either as part of a criminal investigation or OPD internal audit / investigation. It extracts data stored on the device, including internal memory, SIM cards, and SD cards when present. It is not connecting to any live data feeds or external surveillance sources.

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

N/A. The device is not deployed in the field.

- 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.

No community complaints or concerns were communicated to staff in 2024.

No racial data was gathered for internal OPD work phone searches.

Extractions Conducted as Part of a Criminal Investigation by Race

Black	176
Hispanic	65
White	13
Asian	9
Unknown	9

The racial data for nine devices being unknown is due to the identity of the owner is unknown, or the data was not gathered. Only one search as part of a criminal investigation was not pursuant to a search warrant, the race of the owner of the device was identified as Black.

OPD's use policy allows OPD to conduct forensic extraction of these devices in a criminal investigation either pursuant to a search warrant, via consent, or life / death exigency. In 2024, only one consent search was conducted. The search was sought during a recording interview, the manner in which the consent was sought and given was recorded. All other searches were done via search warrants authorized and signed by judges. Officers would have to articulate to judges, under penalty of perjury, the facts in which relevant evidence exists on these devices relating to the crime(s) they are investigating. Given these safeguards, OPD's adopted use policy is adequate in protecting the civil rights and civil liberties of the individuals whom the department is using the technology on.

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:

One internal audit was conducted in November of 2024. The program coordinator compared the usage log automatically generated by the Cellebrite device to the audit usage log maintained by OPD. All usage of the device correlated to an entry in the OPD usage log. There was no unauthorized or undocumented usage of the Cellebrite device.

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:

There were no known data breaches or known unauthorized access during 2024.

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

Homicide

During the investigation of a 2025 homicide, a suspect was identified. A search warrant was authored for the suspect's wireless account, but it was submitted outside of the window for specialized location records. Because of this, the investigation had to rely on limited location data generated only by calls and text messages. When the suspect was arrested, his phone was seized and a Cellebrite download was conducted pursuant to a search warrant. The report documented additional location data that was not captured by

the wireless company. The new location data pinpointed the suspect's location before and after the murder and provided important evidence in the case.

Robbery Series #1

In the second quarter of 2024, a series of eight armed robberies including two where victims were struck by gunfire occurred. A suspect was taken into custody and the Cellebrite was used to extract data from the suspect's electronic device. The data extracted included data connections, media and messages that led to the suspect being charged for the entire series of robberies.

Robbery Series #2

From September 2024 to October 2024, at least four major robbery series occurred within the City of Oakland. These series all had major commonalities between them, targeting mostly Hispanic day laborers in the early morning hours. The robberies were committed in quick succession as the driver would stay in the vehicle, and multiple suspects would exit, armed with firearms and demand money. The suspects would often pistol-whip the victims if any resistance was encountered. During these incidents, up to nine victims would be robbed at a time.

Multiple suspects were taken into custody during the course of the series. Multiple cellular phones were extracted by use of the Cellebrite. The data on these phones included communications, media, data connections and cellular connections between the suspects. The data was critical in charging three suspects in the series and led directly to their prosecution.

Robbery Series #3

In January 2024, a series of an armed carjacking and seven armed robberies occurred in the City of Oakland. One suspect was taken into custody the following day and his cellular device was extracted via Cellebrite. The information within the device led to investigators identifying four other suspects within the series. The information would not have been obtained via any other source during the investigation and proved invaluable when one suspect later committed a shooting prior to his arrest. The data was used for both the robbery cases as well as the attempted homicide case.

Robbery Series #4

In June 2024, a robbery series involving two carjackings and two commercial business takeovers with rifles occurred in the City of Oakland. Data from the suspects' devices was later used to identify them both as suspects of a separate human trafficking case as well as a separate robbery and kidnapping.

Robbery Shooting

In April 2024, a robbery and attempted homicide occurred in the City of Oakland. One suspect was taken into custody and his device was processed by Cellebrite. Media, communication, and data logs from the device led to the positive identification of two other suspects. The data from the other two suspects' devices assisted in the prosecution of the two. One suspect was charged due to the key evidence on his device, which was recovered from a forensic extraction.

Attempted Homicide

In July 2024, an attempted homicide occurred in the City of Oakland. Two victims were shot, and one was paralyzed permanently. Cellebrite was used to extract both suspects' electronic devices. The media, log files, communications, and device connections were used as evidence to charge the suspects with the shooting.

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

There are no existing or newly opened public records requests relating to the technology.

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:

The cost to acquire and operate Cellebrite Premium for June 2024 to June 2025 was \$96,688.95.

The renewal for Cellebrite Premium from June 2025 to June 2026 has increased to \$107,769.38

The expected renewal cost for Cellebrite from June 2026 to June 2027 will be \$130,095, and is subject to change.

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

1. OPD is requesting to transition from referring to the tool by its trademark name when the policy was first developed, Cellebrite UFED, to referring to the tool as its purpose, a mobile forensic extraction tool. This is to avoid confusion as the company renames the service provided to OPD. For context, this tool was named Cellebrite UFED, to now Cellebrite Premium and soon to be renamed Cellebrite Inseyets. This would not change the legal and policy requirement that OPD has to follow to use this tool, it would only facilitate ease of future reporting.
2. OPD is also requesting additional funding for the renewal of Cellebrite, given the expected increase in cost for the June 2026 to June 2027 renewal.

When OPD was still using the older Cellebrite UFED device from February to June of 2024, it was only utilized 35 times in a criminal investigation. Mostly in homicides. After upgrading in July, the usage increased to 237 times and involving other serious crimes. This significant increase reflects the device's value in terms of capability and the need for digital evidence in criminal investigations. Additional funding to maintain this digital evidence capability of OPD is essential for its investigative capability.

3. OPD requests that future data gathered regarding the race of each person subject to the technology's use be limited to extractions not done pursuant to a search warrant—i.e., consent or exigent circumstance searches.

In warrant-based extractions, the search is authorized by a judge based on a sworn affidavit establishing probable cause. The race of the individual is not a factor in the legal standard or the judge's decision to issue the warrant. Because of that, there is no clear probative value in tracking race data for these cases when evaluating potential impacts on civil rights or civil liberties.

Collecting and verifying race data for all warrant-based extractions also creates an administrative burden, particularly in cases where the phone owner is unknown,

there are multiple subjects, or race data was not otherwise collected during the investigation. Trying to gather this information can be intrusive in itself.

Given these concerns, OPD recommends limiting race tracking to consent and exigent searches, where officer discretion plays a more direct role and where the data may be more meaningful in identifying potential disparities.



MEMORANDUM

TO: PAC

FROM: Sgt. Y. Zhou
OPD, Criminal Investigation Division

SUBJECT: Annual Report – Pen Registers

DATE: MAY 13, 2025

Background

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

- The benefits to the community of the surveillance technology outweigh the costs, and 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.

Sgt. Y. Zhou is currently the program coordinator for OPD's pen register system.

2024 Annual Report Details

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

The pen register operates in real-time, recording metainformation about outgoing and incoming communications as they occur. It helps investigators to establish connections between individuals, track patterns of communication, and gather evidence related to the timing and frequency of calls. It may help establish connections between individuals and gain insights into the relationships and activities of the suspects. Pen register data also further corroborates other evidence, provides leads for further follow-up investigations, and assists with tracking of wanted suspects.

OPD utilizes the Gladiator pen register system to receive and analyze data provided by telecommunication companies. OPD began tracking its pen register usage in May 2024 as required. All usage of the pen register system in 2024 involved cell phones.

From May 2024 to December 2024, OPD's pen register system was used 118 times across 61 separate investigations. OPD obtained search warrants prior to the usage of the system for all but one incident, in which a danger to the public required the system to be used under exigency, but a post-hoc warrant was obtained. The majority of the investigations involved violent crimes.

In May 2024, a suspect committed two separate sexual assaults in two days. OPD identified the suspect and was attempting to locate/arrest this person. Given the risk to the public, OPD applied for an exigent pen register to facilitate the apprehension of the suspect. A post-

hoc search warrant was obtained for the exigent usage of the system within the required timeline.

Pen Register Usage by Crime Type – 2024

Crime Type	Installations (Uses)	Investigations
Felony Assaults (non-fatal shooting / stabbing)	14	11
Burglary	3	3
Death Threat	1	1
Vehicular Manslaughter	1	1
Stolen Vehicle	1	1
Sexual Assault / Rape	4	1
Illegal Firearm Possession	4	3
Human Trafficking	2	2
Robbery	13	11
Homicide	75	27
Total	118	61

- 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):

OPD shares data obtained through its pen register system with prosecutorial agencies as part of ongoing criminal prosecutions. The data is shared with agencies such as the Alameda County District Attorney's Office and federal prosecutorial office as part of the routine discovery process. These disclosures are made at the request of the prosecuting attorney and are standard practice during the course of prosecution. OPD does not maintain separate records of each instance in which data is shared for discovery, as these requests are part of the broader prosecution effort and not tracked independently by OPD. OPD has not shared any pen register data with U.S. Immigration and Customs Enforcement (ICE), the Department of Homeland Security (DHS), or U.S. Customs and Border Protection (CBP).

- 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:

The surveillance technology is a web-based interface that displays metadata provided to OPD by telecommunication companies, specifically outgoing and incoming call logs, dialed numbers, timestamps, and associated subscriber information where permitted. No content of communications is captured. The system interfaces with data sources from these companies as authorized through search warrants or other applicable legal processes.

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

N/A. This technology is not deployed in the field. It is a web-based interface.

- 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.

There were no community complaints or concerns reported in 2024 related to the use of the pen register system. All uses of the technology were conducted under valid legal authority. Of the 118 uses:

117 were executed after obtaining a search warrant in advance.

1 use was conducted under exigent circumstances, followed by a post-hoc search warrant. The race of the owner of the phone was Black.

The adopted use policy requires a legal process for every deployment and includes supervisory and judicial oversight to ensure compliance with civil rights protections. Based on our review, the policy remains adequate in safeguarding civil liberties and ensuring due process.

The race of the phone owner was identified in each of the 118 uses, with the following breakdown:

Race / Ethnicity	Number of Uses
Black	101
Hispanic	12
Asian	3
White	1
Other	1

No misuse or discriminatory application of the technology was identified.

- 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:

Internal audit is conducted on a monthly basis. The program coordinator compares the invoices from phone companies to the audit usage log maintained by OPD. All invoices were correlated to an entry in the OPD audit log. There was no authorized usage of the pen register service.

- 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:

There were no identifiable data breaches or known unauthorized access during 2024.

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

Pen registers and trap and trace devices (hereby collectively referred to as pen registers) support OPD investigations by assisting with the apprehension of wanted suspects and furthering criminal investigations by identifying communication patterns and connections between individuals. These tools are not used to identify suspects, but rather to track communication activity once a known suspect has been identified through other investigative means.

Homicide Case

During the investigation of a homicide in the second quarter of 2024, officers obtained a pen register order for the suspect's phone. Real-time data from the device showed repeated activity near a specific neighborhood. Surveillance was set up in that area, leading officers to observe the suspect entering a residence. A perimeter was established and the suspect was taken into custody. A follow-up search warrant at the residence yielded valuable evidence to the homicide case.

Robbery Case

In the third quarter of 2024, a robbery suspect was evading capture after a series of armed incidents. Investigators obtained a pen register on the suspect's cell phone. Call data suggested the suspect was frequently in contact with individuals in East Oakland. Officers conducted surveillance based on the pen register activity and located the suspect at a convenience store. The suspect was arrested without incident.

Attempted Homicide Case

Following a shooting in the first quarter of 2024, officers identified a suspect and secured a pen register search warrant. Activity on the phone helped confirm the suspect was still in the Bay Area and led to focused surveillance in a particular corridor. While conducting surveillance, officers observed the suspect in a vehicle. A felony stop was conducted, and the suspect was taken into custody.

Burglary Case

Investigators were attempting to locate a suspect wanted for numerous residential burglaries. A pen register search warrant was served on the suspect's significant other's cell phone. After analyzing the data, a phone number for the suspect was developed. Another pen register search warrant on that phone number helped OPD with locating the suspect and arresting him/her.

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

There are no existing or newly opened public records requests relating to the technology.

- 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:

ITEM DESCRIPTION	SKU	QTY	UNIT PRICE \$	SUB-TOTAL \$
Enterprise Pkg - Real Time ESPA/ST/PRTT (1) concurrent license includes total of three named users	E-RT-PKG-ANN	3	4,725.00	14,175.00
Enterprise ESPA (1) concurrent license includes total of three named users	E-ESPA-ANN	4	1,575.00	6,300.00
Enterprise IQ Express Portal OSS - IQ Express Portal - Sold annually	E-IQ-ANN	1	2,500.00	2,500.00
Enterprise Mobile App G-Scout Mobile App - Single User License	E-APP-ANN	3	350.00	1,050.00
<hr/>				
Period of Performance : One year from date of purchase order.	SUBTOTAL			24,025.00
	TAX			0.00
	TOTAL			\$24,025.00

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

No requests for changes at this time.



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 regarding 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 received 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-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 regarding 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 received 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

DEPARTMENTAL GENERAL ORDER
OAKLAND POLICE DEPARTMENT

I-20

Effective Date

Floyd Mitchell

Chief of Police

Date Signed:



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

Part 1 Crimes <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
Violent Crime Index (homicide, aggravated assault, rape, robbery)	6,146	6,735	6,295	7,900	6,361	-19%	6,687	-5%
Homicide – 187(a)PC	102	122	120	119	81	-32%	109	-26%
Homicide – All Other *	7	12	2	7	5	-29%	7	-24%
Subtotal - 187(a)PC + all other	109	134	122	126	86	-32%	115	-25%
Aggravated Assault	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%
Subtotal - Homicides + Firearm Assault	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%
Rape	223	174	184	204	172	-16%	191	-10%
Robbery	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%
Burglary	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%
Motor Vehicle Theft	8,760	9,399	10,346	15,391	10,439	-32%	10,867	-4%
Larceny	6,147	6,785	9,576	9,975	8,368	-16%	8,170	2%
Arson	196	173	166	123	112	-9%	154	-27%
Total	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

Cases by Firearm-Related Crime Type	
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
Total Cases	1,234

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

Guns Recovered by Crime Type	
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
Total Cases	50

- *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

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

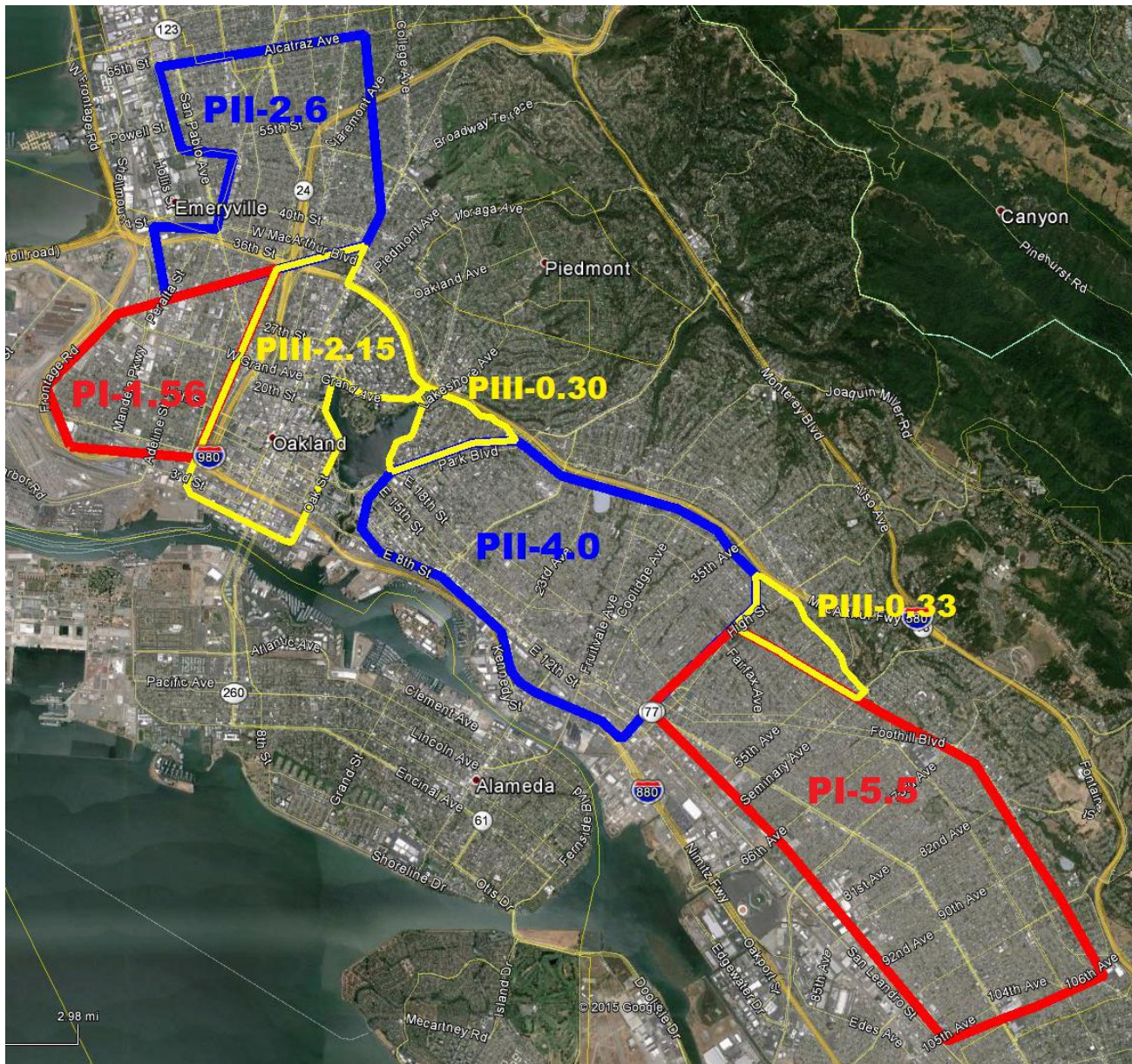
North Oakland: North of Highway 580 to Alcatraz Avenue

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 mi², an additional 1.06 mi² of ShotSpotter coverage was added, at no charge, for a total of 7.06 mi² when Phase I service was upgraded and converted to the newer subscription platform in 2011.

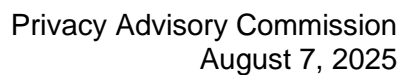
Phase IV with blue borders (Activated in 2021): 2.79 square miles

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-32.1: Community Safety Camera Systems – Camera Registry and Department Remote Access to Public/Private Owned Surveillance Camera Systems

Effective Date: XX Nov XX
Coordinator: Bureau of Investigations

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 for the capture, storage, and use of digital data obtained through the use of Community Safety Camera Systems technology while recognizing the established privacy rights of the public.

A. Definitions

A - 1. Community Safety Camera

A fixed camera device, owned and/or controlled by the City of Oakland or a private/public entity, with the capability of live streaming and/or recording videographic data, where the owner/controller of the device and its associated data has explicitly provided authorization to the Oakland Police Department to access historical and/or live videographic data in the furtherance of a criminal investigation.

Community Safety Cameras Include:

- Any camera owned/managed by the Oakland Police Department that is installed in a public place and accessed by the Department, outside of cameras installed for Department facility security.
- Any camera owned and/or controlled by a private/public entity, not under the control of the Oakland Police Department, that is accessed by the Department pursuant to this policy.

A - 2. Operating System

The Flock Operating System (FlockOS) is a cloud-based public safety platform designed to integrate and manage data from various sources, including video, license plate recognition (LPR), and gunshot detection systems. It provides real-time investigative information and retrospective investigation capabilities to support the full spectrum of Departmental operations. FlockOS has a native Video Management System VMS platform but also is capable of integrating with outside VMS systems.

A - 3. Video Management System (VMS)

A Video Management System (VMS) is software designed to process, store, and manage video footage from multiple surveillance cameras. VMS software operates as a central management system, linking and consolidating multiple camera systems onto a single platform, while offering tools for monitoring, recording, and analyzing video data in real-time or from recorded archives.

B. Description of the Technology

OPD uses the Community Safety Camera Systems (CS Camera Systems) and associated VMS/OS technology as a form of crime deterrence, and when necessary, to capture and store digital image data related to criminal activity and active criminal investigations.

B - 1. Technology Integration Platform - Flock Operating System (FlockOS)

The Flock Operating System is the basis of the Department's Technology Integration platform (TIP). The operating system allows the Department to integrate existing technology in a more cohesive and comprehensive way, while also assisting with the coordination of field operations and investigative bodies to address specific disruptive criminal activities in our community with precision and efficiency.

B - 2. Fixed Line of Sight Camera System

Line of sight cameras are fixed-position surveillance camera devices that capture visual data from a defined area.

B - 3. Pan-Tilt-Zoom (PTZ) Camera Systems

1. Pan: This function allows the camera to rotate horizontally, covering a broad field of view. PTZ cameras can rotate up to 360 degrees, allowing the camera system to replicate the view of a person located in the same position of the camera.
2. Tilt: This feature enables the camera to move vertically. Tilting up and down helps to cover different vertical angles and ensure that both high and low areas can be observed.
3. Zoom: PTZ cameras come equipped with optical zoom lenses that allow you to zoom in on specific objects or areas without losing image quality. This is useful for detailed inspection or the tracking of moving objects.
4. Remote Control: PTZ cameras can be controlled remotely via various interfaces, such as dedicated control panels, computer software, or mobile apps. This flexibility allows operators to adjust the camera's position and zoom level in real time.

C. Purpose of the Technology

OPD accessed CS Camera Systems and associated VMS and Operating Systems are intended to deter criminal activity within specific public areas and enhance the Department's ability to address disruptive criminal activity within the community. These disruptive crimes include theft, vehicle theft, human trafficking, reckless driving, sideshow/takeovers, felony evasion, burglaries, robberies, shootings, and homicides. Many criminal investigations hinge upon the availability and quality of surveillance video as evidence that is later used in the prosecution of criminal cases. While physical surveillance may also accomplish these goals, it is limited due to the financial cost, the availability of resources, and the physical demands upon members of the Department. CS Camera Systems have the capability of enhancing the Department's ability to address the types of criminal activity that are disruptive within the community while also acting as a resource multiplier within the Department. It is the expressed intent of the Department to use this technology to facilitate informed enforcement on those involved in specific disruptive criminal activities and to mitigate collateral impact upon the community.

The Department also recognizes that CS Camera Systems have the capability of assisting with community safety efforts beyond the role of the law enforcement, and intends to utilize CS Camera Systems to assist the Oakland Fire Department and other partnering emergency services in their Public Safety functions.

D. Authorized Uses

D - 1. Authorized Users

Personnel authorized/designated to use CS Camera System equipment or access information collected through the use of such equipment shall be specifically trained in such technology. Sworn personnel, Police Service Technicians (PST), or other authorized/designated Department personnel may use the technology.

Authorized users other than sworn personnel or PSTs must be designated by the Chief of Police or designee.

D - 2. Authorized Use

➤ Recording of Public Areas

Access to CS Camera Systems that are installed with a view of a public area shall be done so under expressed permission provided by the owner/controller of the device and its associated data. OPD shall only record and retain video data in furtherance of a criminal or administrative investigation.

➤ Recording an Area Subject to a Reasonable Expectation of Privacy

CS Camera Systems shall not be used in areas where there is a reasonable expectation of privacy unless under exigent circumstances..

➤ Recordings During Exigent Circumstances

CS Camera Systems may be used during exigent circumstances that include hostage situations, barricaded suspects, kidnappings, and active shooter

situations. If a CS Camera System is used for exigent circumstances, a search warrant shall be sought within 72 hours, and the exigent use shall be documented within the annual report and reported to the Privacy Advisory Committee (PAC) and the next available PAC meeting.

E. Restrictions on Use

E - 1. Permitted/Impermissible Uses

Department personnel may only access and use the CS Camera System consistent with this Policy. Recordings retained by the Department related to criminal investigations are the property of the Oakland Police Department. The following uses of the CS Camera System are specifically prohibited:

- **Invasion of Privacy:** Except when done pursuant to a court order such as a search warrant, it is a violation of this Policy to utilize the CS Camera System to intentionally record or transmit images of any location where a person would have a reasonable expectation of privacy (e.g., residence, enclosed yard, enclosed structure) unless exigent circumstances exist. If a CS Camera System is used for exigent circumstances, a search warrant shall be sought within 72 hours, and the exigent use shall be documented within the annual report (in accordance with Section D-2 of this policy).
- **Harassment or Intimidation:** It is a violation of this Policy to use the CS Camera Systems with the intent to harass and/or intimidate any individual or group.
- **Use Based on a Protected Characteristic:** It is a violation of this policy to use CS Camera Systems to target a person or group solely because of a person's, or group's race, gender, religion, political affiliation, nationality, ethnicity, sexual orientation, disability, or other classification protected by law.
- **Facial Recognition:** It is a violation of this policy for Department members to use CS Camera Systems in conjunction with Facial Recognition technology.
- **Motion Activated Object Tracking Technology:** It is a violation of this policy to utilize motion activated object tracking technology, *if* the technology selectively tracks objects or subjects using Personal Identifying Information (PII) or factors such as race, gender, religion, political affiliation, nationality, ethnicity, sexual orientation, disability, or other classification protected by law.
- **Personal Use:** It is a violation of this Policy to use the CS Camera Systems or associated data for any personal purpose.
- **First Amendment Rights:** It is a violation of this policy to use the CS Camera Systems or associated data for the intended purpose of infringing upon First Amendment rights.

- **Audio Data:** It is a violation of this policy to utilize Department owned CS Camera Systems to capture or store audio data.

Department members shall not use, or allow others to use, the equipment or database records for any unauthorized purpose.

1. No member of this department shall operate CS Camera System equipment or access CS Camera System data without first completing department-approved training.
2. No CS Camera System operator may access department, state or federal data unless otherwise authorized/designated to do so pursuant to Section G “Data Access” below.
3. Accessing data collected by CS Camera 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 state or federal statute, applicable case law, or a court order. A need to know is a compelling reason to request information such as involvement in an active investigation.

The Department should make reasonable efforts to avoid viewing CS Camera Systems that inadvertently capture public areas outside of sensitive facilities, such as medical clinics, reproductive health facilities, houses of worship, or other sensitive locations; absent an investigative need to do. When technologically possible, the Department should consider utilizing “masking” or “blurring” features available on certain VMS platforms to mask entrances or buildings determined to be sensitive facilities. CS Camera Systems shall not be used to specifically target a person or group solely because of a person's, or group's race, gender, religion, political affiliation, nationality, ethnicity, sexual orientation, disability, or other classification protected by law.

F. Data Collection

CS Camera Systems live-streams and records photographic and videographic data utilizing mounted camera systems. The data is stored through a Video Management System (VMS), which may only be accessed by authorized personnel and requires an individual username/password.

G. Data Access

G - 1. General Data Access Guidelines

Department sworn personnel, police service technicians, or other authorized/designated Department personnel may use the technology. Authorized/designated users other than sworn personnel or PSTs must be designated by the Chief of Police or designee.

The Oakland Police Department does not permit the sharing of CS Camera System data gathered by the city or its contractors/subcontractors for the purpose of federal

immigration enforcement, pursuant to the California Values Act (Government Code § 7282.5; Government Code § 7284.2 et seq) – these federal immigration agencies include Immigration and Customs Enforcement (ICE) and Customs and Border Patrol (CPB).

All data and images gathered and retained by CS Camera Systems related to criminal investigations are for the official use of this department. Some information may not be disclosable to the general public. Investigatory records are not generally disclosable in response to a public records request. Non-investigatory and otherwise non-exempt records shall be disclosed in response to a public records request.

G - 2. Tiered CS Camera Data Access

The CS Camera System is segmented into tiers of access, to provide robust community safety capabilities while also ensuring privacy safeguards are present. By assigning access levels based on roles and responsibilities, sensitive footage can be restricted to authorized personnel, reducing the risk of misuse or breaches. It also allows for more efficient monitoring, as different sections within the Department can focus on the data relevant to their needs without being overwhelmed by unnecessary information. This structured approach balances transparency, accountability, and privacy protection.

Real-Time Camera Access – Only specific Department members designated by the CS System Administrator(s) and/or Chief of Police shall have access to Real-time (live) camera access while supporting field operations. Real-time access shall be utilized strictly in the furtherance of an active investigation. The CS System Administrator shall keep a record of Department members who are authorized real-time camera access. Access to real-time cameras shall be limited to members who have been approved by the Operations Center Commander, Ceasefire Commander, CID Commander, or Chief of Police. The Operations Center Commander is responsible for maintaining a list of authorized members who are provided access to real-time camera data.

Authorized Department members may live-stream real-time surveillance video to any member of the Department (with a need-to-know, right-to-know) related to incidents where the live surveillance video may assist in enhancing the member(s) ability to safely address a critical incident related to the following:

- Where a subject(s) is believed to be armed with a weapon capable of inflicting injury.
- Where a subject has demonstrated violent behavior, made threats of violence towards themselves or others, and/or the previous actions of the subject pose a danger to the public, officers, or themselves¹.

¹ This includes but is not limited to, flight (on foot or utilizing a vehicle), assault, self-harm, and/or a history of barricading themselves.

- To assist with detaining a subject(s) related to a felony investigation.

Live-stream surveillance video may assist members with establishing additional time and distance with engaged subjects, maximizing the use of available cover, and fostering conditions that enable effective de-escalation during enforcement efforts.

Historical Data Access – Any member of the Department who is trained and provided access to the CS Camera System may access historical video data related to a specific criminal or administrative investigation; similar to the current process of conducting a physical canvass for video surveillance. Physically canvassing for video is time and resource-consuming. It often requires the owner/controller of the device to be present and either the Department member or possessor of the equipment to be familiar with how to access and export the video data.

If the owner/controller provides explicit consent by opting in to sharing video data through the VMS and/or FlockOS system, Department members can access historical video data remotely, making the process more efficient for the member and owner/controller of the physical camera system.

Historical Data access shall be documented by recording the following:

1. The date and time the information is accessed,
2. The associated report or incident number,
3. The username of the person who accesses the information,
4. The purpose for accessing the information.

H. Data Protection

All data shall be safeguarded and protected by both procedural and technological means. OPD shall observe the following safeguards regarding access to and use of stored data:

- All CS Camera System server data shall be accessible only through a login/password-protected system capable of documenting all access of information by username or other data elements used such as date and time of access.
- All data shall be accessed via a Department approved securely connected device.

I. Data Retention

It is understood by the Department that CS Camera Systems and their associated data, not under the control of the Department, may have different retention schedules than that of the Department.

All CS Camera System data uploaded to a Video Management System (VMS) owned by the Department shall be purged 90 days from the initial upload. CS Camera

System information may be retained outside this retention limit solely for the following purposes:

1. Active Criminal Investigations
2. Active Administrative Investigations
3. Missing or at-risk Persons Investigations
4. Investigations from other law enforcement or prosecutorial agencies where there is a legal obligation to retain information.

Any data retained for the above-described investigative purposes shall be stored on Evidence.com in accordance with Appendix A of this policy.

J. Public Access

All images and recordings uploaded by the CS Camera System and retained related to an investigation are for the official use of this department. Some information may not be disclosable to the general public. Investigatory records are not generally disclosable in response to a public records request. Non-investigatory records shall be disclosed in response to a public records request. Requests for information by non-law enforcement or non-prosecutorial agencies will be processed in accordance with Government Code §7920 et seq, this policy, and applicable case law and court orders.

K. Third Party Data Sharing of Data Retained by the Department

K - 1. CS Camera System Sharing with Legal Obligation

OPD personnel may share downloaded retained recorded CS Camera System data and associated metadata when there is a legal obligation to do so, such as a subpoena, court order or warrant to share such information, such as the following:

- a federal, state, or local criminal prosecutor's office for use as evidence to aid in prosecution, in accordance with laws governing evidence;
- a Public Defender's Office or criminal defense attorney via the District Attorney's Office in accordance with applicable California criminal discovery laws;
- California law enforcement agencies as part of a formal criminal or administrative investigation;
- a party to civil litigation, or other third parties, in response to a valid court order only.

CS Camera System server data may be shared only as otherwise permitted by law and this policy. All data and images gathered by the CS Camera System are for the official use of this Department.

K - 2. CS Camera System Sharing without Legal Obligation

When there is no legal obligation to provide the requested data, requests for downloaded retained recorded CS Camera System data and associated metadata from other California law enforcement agencies shall be made in writing and may only be approved by the Ceasefire Commander or designee per the 3-step protocol below. These requests shall be maintained in a secure folder so that information about these requests can be shared in required annual reports with the PAC. Server access shall be restricted only to authorized/designated Department personnel who will extract the required information and forward it to the requester.

- The requesting party shall have 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, case law, or sworn officer status. A need to know is a compelling reason to request information such as direct involvement in an investigation.
- The Department shall record the requesting party's name and document the right and need to know the requested information.
- The Department shall record whether the request was honored or denied, the reason for such action, and the name of the Department officer that processed the request.

L. Training

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

Training requirements for employees shall include the following:

- Applicable policy
- Functionality of equipment
- Accessing data
- Sharing of data

M. Auditing and Oversight

Login/Log-Out Procedure. To ensure proper operation and facilitate oversight of the CS Camera System, all users will be required to have individual credentials for access and use of the systems and/or data, which has the ability to be fully audited. It is the responsibility of the Department under this policy to actively pursue software and hardware upgrades that are needed to maintain full compliance with Section K of the use policy.

The records of the number of deployments of Department owned CS Camera Systems, Third Party Data Sharing related to Section K – 2 of this Policy, and any exigent use of CS Camera Systems shall be incorporated into the annual report

required by O.M.C. 9.64 et seq.

CS Camera System audits shall be conducted annually to ensure proper system functionality and that designated personnel are using the system according to policy rules via sample audits, and reviews of training records. The size of these audits shall be large enough to provide a statistically significant representation of the data collected.

N. Maintenance and Administration

N - 1. CS Camera System Administration

All installation and maintenance of Department owned CS Camera equipment, as well as CS Camera System data retention and access, shall be managed by the Ceasefire Section and Assistant Chief of Police.

N - 2. CS Camera System Administrators

The Ceasefire Commander and CGIC/Operations Center Commander shall be the administrators of the CS Camera System program and shall be responsible for developing guidelines and procedures to comply with the requirements of Civil Code § 1798.90.5 et seq. The Ceasefire Captain is responsible for ensuring systems and processes are in place for the proper collection, and retention of CS Camera System data.

N - 3. CS Camera System Coordinator:

The title of the official custodian of the CS Camera System is the CS Camera System Coordinator.

N - 4. Monitoring and Reporting

The Oakland Police Department will ensure that the system remains functional according to its intended use and monitor its use of CS Camera System technology to ensure the proper functionality of the system as defined in the policy guidelines of this document, including required audits, training, and data access records.

The CS Camera System Coordinator shall provide the Chief of Police, Privacy Advisory Commission, and Public Safety Committee with an annual report pursuant to OMC 9.64 (Oakland Surveillance Technology Ordinance).

DEPARTMENTAL GENERAL ORDER
OAKLAND POLICE DEPARTMENT

I-32.1

Effective
XX Jun 25

By Order of

Floyd Mitchell
Chief of Police

Date Signed:

Appendix A

Category Name	Retention Period	Legal Retention Requirements
Violent Felony / DOA	Indefinite	Statute of Limitations (SOL)
Misdemeanor Case (including report, statements, cite, or arrest)	2 yrs	SOL
Felony Case (including report, statements, cite, or arrest - no violent felonies or sex crimes)	3 yrs	SOL
Missing Person / Runaway	Indefinite	SOL (Possible homicide)
Sex Crimes	Indefinite	SOL
Vehicle Pursuit	5 yrs	Administrative SOL
Sergeants / Commanders Admin	2 yrs	Possible IA/DLI - Sergeant/etc. to update category if so
IA/DLI	Indefinite	Administrative SOL
Use of Force - Levels 1 and 2	Indefinite	Administrative SOL

DEPARTMENTAL GENERAL ORDER
OAKLAND POLICE DEPARTMENT

I-32.1

Effective
XX Jun 25

Use of Force - Levels 3 and 4	Indefinite	Administrative SOL
Felony - Filed by DA	20 yrs	SOL plus appeals
Homicide	Indefinite	SOL
Misdemeanor - Filed by DA	10 yrs	SOL plus appeals
Legal - OCA/Records/Authorized Users Only	Indefinite	City Attorney's Office (CAO) Order
Collision - 901C	Indefinite	CAO Order
Collision - Major Injury / Fatal	Indefinite	SOL

Flock Safety + CA - Oakland PD

Flock Group Inc.
1170 Howell Mill Rd, Suite 210
Atlanta, GA 30318

MAIN CONTACT:
Kyle Egkan
kyle.egkan@flocksafety.com
7144690389



EXHIBIT A
ORDER FORM

Customer: CA - Oakland PD
Legal Entity Name: CA - Oakland PD
Accounts Payable Email: cbeckman@oaklandca.gov
Address: 455 7th St Oakland, California 94607

Initial Term: 36 Months
Renewal Term: 24 Months
Payment Terms: Net 30
Billing Frequency: Annual Plan - First Year Invoiced at Signing.
Retention Period: 30 Days

Hardware and Software Products

Annual recurring amounts over subscription term

Item	Cost	Quantity	Total
Flock Safety Platform			\$900,000.00
Flock Safety Flock OS			
FlockOS ™	Included	1	Included
Flock Safety LPR Products			
Flock Safety Falcon ®	Included	300	Included

Professional Services and One Time Purchases

Item	Cost	Quantity	Total
One Time Fees			
Flock Safety Professional Services			
Professional Services - Standard Implementation Fee	\$650.00	125	\$81,250.00
Professional Services - Advanced Implementation Fee	\$1,900.00	40	\$76,000.00
Professional Services - Existing Infrastructure Implementation Fee	\$150.00	135	\$20,250.00
Subtotal Year 1:			\$1,077,500.00
Annual Recurring Subtotal:			\$900,000.00
Estimated Tax:			\$0.00
Contract Total:			\$2,877,500.00

*Taxes shown above are provided as an estimate. Actual taxes are the responsibility of the Customer. This Agreement will automatically renew for successive renewal terms of the greater of one year or the length set forth on the Order Form (each, a "**Renewal Term**") unless either Party gives the other Party notice of non-renewal at least thirty (30) days prior to the end of the then-current term.*

Billing Schedule

Billing Schedule	Amount (USD)
Year 1	
At Contract Signing	\$1,077,500.00
Annual Recurring after Year 1	\$900,000.00
Contract Total	\$2,877,500.00

*Tax not included

Product and Services Description

Flock Safety Platform Items	Product Description	Terms
Flock Safety Falcon ®	An infrastructure-free license plate reader camera that utilizes Vehicle Fingerprint® technology to capture vehicular attributes.	The Term shall commence upon first installation and validation of Flock Hardware.
One-Time Fees	Service Description	
Installation on existing infrastructure	One-time Professional Services engagement. Includes site & safety assessment, camera setup & testing, and shipping & handling in accordance with the Flock Safety Advanced Implementation Service Brief.	
Professional Services - Standard Implementation Fee	One-time Professional Services engagement. Includes site and safety assessment, camera setup and testing, and shipping and handling in accordance with the Flock Safety Standard Implementation Service Brief.	
Professional Services - Advanced Implementation Fee	One-time Professional Services engagement. Includes site & safety assessment, camera setup & testing, and shipping & handling in accordance with the Flock Safety Advanced Implementation Service Brief.	

FlockOS Features & Description

Package: Essentials

FlockOS Features	Description
Community Cameras (Full Access)	Access to all privately owned Flock devices within your jurisdiction that have been shared with you.
Unlimited Users	Unlimited users for FlockOS
State Network (LP Lookup Only)	Allows agencies to look up license plates on all cameras opted in to the statewide Flock network.
Nationwide Network (LP Lookup Only)	Allows agencies to look up license plates on all cameras opted in to the nationwide Flock network.
Direct Share - Surrounding Jurisdiction (Full Access)	Access to all Flock devices owned by law enforcement that have been directly shared with you. Have ability to search by vehicle fingerprint, receive hot list alerts, and view devices on the map.
Time & Location Based Search	Search full, partial, and temporary plates by time at particular device locations
License Plate Lookup	Look up specific license plate location history captured on Flock devices
Vehicle Fingerprint Search	Search footage using Vehicle Fingerprint™ technology. Access vehicle type, make, color, license plate state, missing / covered plates, and other unique features like bumper stickers, decals, and roof racks.
Flock Insights/Analytics page	Reporting tool to help administrators manage their LPR program with device performance data, user and network audits, plate read reports, hot list alert reports, event logs, and outcome reports.
ESRI Based Map Interface	Flock Safety’s maps are powered by ESRI, which offers the ability for 3D visualization, viewing of floor plans, and layering of external GIS data, such as City infrastructure (i.e., public facilities, transit systems, utilities), Boundary mapping (i.e., precincts, county lines, beat maps), and Interior floor plans (i.e., hospitals, corporate campuses, universities)
Real-Time NCIC Alerts on Flock ALPR Cameras	Alert sent when a vehicle entered into the NCIC crime database passes by a Flock camera
Unlimited Custom Hot Lists	Ability to add a suspect’s license plate to a custom list and get alerted when it passes by a Flock camera

By executing this Order Form, Customer represents and warrants that it has read and agrees to all of the terms and conditions contained in the Master Services Agreement attached. The Parties have executed this Agreement as of the dates set forth below.

FLOCK GROUP, INC.

Customer: CA - Oakland PD

By: _____

By: _____

Name: _____

Name: _____

Title: _____

Title: _____

Date: _____

Date: _____

PO Number: _____

Master Services Agreement

This Master Services Agreement (this “**Agreement**”) is entered into by and between Flock Group, Inc. with a place of business at 1170 Howell Mill Road NW Suite 210, Atlanta, GA 30318 (“**Flock**”) and the entity identified in the signature block (“**Customer**”) (each a “**Party**,” and together, the “**Parties**”) on this the 18 day of August 2023. This Agreement is effective on the date of mutual execution (“**Effective Date**”). Parties will sign an Order Form (“**Order Form**”) which will describe the Flock Services to be performed and the period for performance, attached hereto as **Exhibit A**. The Parties agree as follows:

RECITALS

WHEREAS, Flock offers a software and hardware situational awareness solution through Flock’s technology platform that upon detection is capable of capturing audio, video, image, and recording data and provide notifications to Customer (“**Notifications**”);

WHEREAS, Customer desires access to the Flock Services (defined below) on existing devices, provided by Customer, or Flock provided Flock Hardware (as defined below) in order to create, view, search and archive Footage and receive Notifications, via the Flock Services;

WHEREAS, Customer shall have access to the Footage in Flock Services. Pursuant to Flock’s standard Retention Period (defined below) Flock deletes all Footage on a rolling thirty (30) day basis, except as otherwise stated on the **Order Form**. Customer shall be responsible for extracting, downloading and archiving Footage from the Flock Services on its own storage devices; and

WHEREAS, Flock desires to provide Customer the Flock Services and any access thereto, subject to the terms and conditions of this Agreement, solely for the awareness, prevention, and prosecution of crime, bona fide investigations and evidence gathering for law enforcement purposes, (“**Permitted Purpose**”).

AGREEMENT

NOW, THEREFORE, Flock and Customer agree that this Agreement, and any Order Form, purchase orders, statements of work, product addenda, or the like, attached hereto as exhibits and incorporated by reference, constitute the complete and exclusive statement of the Agreement of the Parties with respect to the subject matter of this Agreement, and replace and supersede all prior agreements, term sheets, purchase orders, correspondence, oral or written communications and negotiations by and between the Parties.

1. DEFINITIONS

Certain capitalized terms, not otherwise defined herein, have the meanings set forth or cross-referenced in this Section 1.

1.1 “**Anonymized Data**” means Customer Data permanently stripped of identifying details and any potential personally identifiable information, by commercially available standards which irreversibly alters data in such a way that a data subject (i.e., individual person or entity) can no longer be identified directly or indirectly.

1.2 “**Authorized End User(s)**” means any individual employees, agents, or contractors of Customer accessing or using the Services, under the rights granted to Customer pursuant to this Agreement.

1.3 “**Customer Data**” means the data, media and content provided by Customer through the Services. For the avoidance of doubt, the Customer Data will include the Footage.

1.4. “**Customer Hardware**” means the third-party camera owned or provided by Customer and any other physical elements that interact with the Embedded Software and the Web Interface to provide the Services.

1.5 “**Embedded Software**” means the Flock proprietary software and/or firmware integrated with or installed on the Flock Hardware or Customer Hardware.

1.6 “**Flock Hardware**” means the Flock device(s), which may include the pole, clamps, solar panel, installation components, and any other physical elements that interact with the Embedded Software and the Web Interface, to provide the Flock Services as specifically set forth in the applicable product addenda.

1.7 “**Flock IP**” means the Services, the Embedded Software, and any intellectual property or proprietary information therein or otherwise provided to Customer and/or its Authorized End Users. Flock IP does not include Footage (as defined below).

1.8 “**Flock Network End User(s)**” means any user of the Flock Services that Customer authorizes access to or receives data from, pursuant to the licenses granted herein.

1.9 “**Flock Services**” means the provision of Flock’s software and hardware situational awareness solution, via the Web Interface, for automatic license plate detection, alerts, audio detection, searching image records, video and sharing Footage.

1.10 “**Footage**” means still images, video, audio and other data captured by the Flock Hardware or Customer Hardware in the course of and provided via the Flock Services.

1.11 “**Hotlist(s)**” means a digital file containing alphanumeric license plate related information pertaining to vehicles of interest, which may include stolen vehicles, stolen vehicle license plates, vehicles owned or associated with wanted or missing person(s), vehicles suspected of being involved with criminal or terrorist activities, and other legitimate law enforcement purposes. Hotlist also includes, but is not limited to, national data (i.e., NCIC) for similar categories, license plates associated with AMBER Alerts or Missing Persons/Vulnerable Adult Alerts, and includes manually entered license plate information associated with crimes that have occurred in any local jurisdiction.

1.12 “**Installation Services**” means the services provided by Flock for installation of Flock Services.

1.13 “**Retention Period**” means the time period that the Customer Data is stored within the cloud storage, as specified in the product addenda.

1.14 “**Vehicle Fingerprint™**” means the unique vehicular attributes captured through Services such as: type, make, color, state registration, missing/covered plates, bumper stickers, decals, roof racks, and bike racks.

1.15 “**Web Interface**” means the website(s) or application(s) through which Customer and its Authorized End Users can access the Services.

2. SERVICES AND SUPPORT

2.1 Provision of Access. Flock hereby grants to Customer a non-exclusive, non-transferable right to access the features and functions of the Flock Services via the Web Interface during the Term, solely for the Authorized End Users. The Footage will be available for Authorized End Users to access and download via the Web Interface for the data retention time defined on the Order Form (“*Retention Period*”). Authorized End Users will be required to sign up for an account and select a password and username (“*User ID*”). Customer shall be responsible for all acts and omissions of Authorized End Users, and any act or omission by an Authorized End User which, including any acts or omissions of authorized End user which would constitute a breach of this agreement if undertaken by customer. Customer shall undertake reasonable efforts to make all Authorized End Users aware of all applicable provisions of this Agreement and shall cause Authorized End Users to comply with such provisions. Flock may use the services of one or more third parties to deliver any part of the Flock Services, (such as using a third party to host the Web Interface for cloud storage or a cell phone provider for wireless cellular coverage).

2.2 Embedded Software License. Flock grants Customer a limited, non-exclusive, non-transferable, non-sublicensable (except to the Authorized End Users), revocable right to use the Embedded Software as it pertains to Flock Services, solely as necessary for Customer to use the Flock Services.

2.3 Support Services. Flock shall monitor the Flock Services, and any applicable device health, in order to improve performance and functionality. Flock will use commercially reasonable efforts to respond to requests for support within seventy-two (72) hours. Flock will provide Customer with reasonable technical and on-site support and maintenance services in-person, via phone or by email at support@flocksafety.com (such services collectively referred to as “*Support Services*”).

2.4 Upgrades to Platform. Flock may make any upgrades to system or platform that it deems necessary or useful to (i) maintain or enhance the quality or delivery of Flock’s products or services to its agencies, the competitive strength of, or market for, Flock’s products or services, such platform or system’s cost efficiency or performance, or (ii) to comply with applicable law. Parties understand that such upgrades are necessary from time to time and will not diminish the quality of the services or materially change any terms or conditions within this Agreement.

2.5 Service Interruption. Services may be interrupted in the event that: (a) Flock's provision of the Services to Customer or any Authorized End User is prohibited by applicable law; (b) any third-party services required for Services are interrupted; (c) if Flock reasonably believe Services are being used for malicious, unlawful, or otherwise unauthorized use; (d) there is a threat or attack on any of the Flock IP by a third party; or (e) scheduled or emergency maintenance ("***Service Interruption***"). Flock will make commercially reasonable efforts to provide written notice of any Service Interruption to Customer, to provide updates, and to resume providing access to Flock Services as soon as reasonably possible after the event giving rise to the Service Interruption is cured. Flock will have no liability for any damage, liabilities, losses (including any loss of data or profits), or any other consequences that Customer or any Authorized End User may incur as a result of a Service Interruption. To the extent that the Service Interruption is not caused by Customer's direct actions or by the actions of parties associated with the Customer, the time will be tolled by the duration of the Service Interruption (for any continuous suspension lasting at least one full day). For example, in the event of a Service Interruption lasting five (5) continuous days, Customer will receive a credit for five (5) free days at the end of the Term.

2.6 Service Suspension. Flock may temporarily suspend Customer's and any Authorized End User's access to any portion or all of the Flock IP or Flock Service if (a) there is a threat or attack on any of the Flock IP by Customer; (b) Customer's or any Authorized End User's use of the Flock IP disrupts or poses a security risk to the Flock IP or any other customer or vendor of Flock; (c) Customer or any Authorized End User is/are using the Flock IP for fraudulent or illegal activities; (d) Customer has violated any term of this provision, including, but not limited to, utilizing Flock Services for anything other than the Permitted Purpose; or (e) any unauthorized access to Flock Services through Customer's account ("***Service Suspension***"). Customer shall not be entitled to any remedy for the Service Suspension period, including any reimbursement, tolling, or credit. If the Service Suspension was not caused by Customer, the Term will be tolled by the duration of the Service Suspension.

2.7 Hazardous Conditions. Flock Services do not contemplate hazardous materials, or other hazardous conditions, including, without limit, asbestos, lead, toxic or flammable substances. In the event any such hazardous materials are discovered in the designated locations in which Flock is to perform services under this Agreement, Flock shall have the right to cease work immediately.

3. CUSTOMER OBLIGATIONS

3.1 Customer Obligations. Flock will assist Customer Authorized End Users in the creation of a User ID. Authorized End Users agree to provide Flock with accurate, complete, and updated registration information. Authorized End Users may not select as their User ID, a name that they do not have the right to use, or any other name with the intent of impersonation. Customer and Authorized End Users may not transfer their account to anyone else without prior written permission of Flock. Authorized End Users shall not share their account username or password information and must protect the security of the username and password. Unless otherwise stated and defined in this Agreement, Customer shall not designate Authorized End Users for persons who are not officers, employees, or agents of Customer. Authorized End Users shall only use Customer-issued email addresses for the creation of their User ID. Customer is responsible for any Authorized End User activity associated with its account. Customer shall ensure that Customer provides Flock with up to date contact information at all times during the Term of this agreement. Customer shall be responsible for obtaining and maintaining any equipment and ancillary services needed to connect to, access or otherwise use the Flock Services. Customer shall (at its own expense) provide Flock with reasonable access and use of Customer facilities and Customer personnel in order to enable Flock to perform Services (such obligations of Customer are collectively defined as “*Customer Obligations*”).

3.2 Customer Representations and Warranties. Customer represents, covenants, and warrants that Customer shall use Flock Services only in compliance with this Agreement and all applicable laws and regulations, including but not limited to any laws relating to the recording or sharing of data, video, photo, or audio content.

4. DATA USE AND LICENSING

4.1 Customer Data. As between Flock and Customer, all right, title and interest in the Customer Data, belong to and are retained solely by Customer. Customer hereby grants to Flock a limited, non-exclusive, royalty-free, irrevocable, worldwide license to use the Customer Data and perform all acts as may be necessary for Flock to provide the Flock Services to Customer. Flock does not own and shall not sell Customer Data.

4.2 Customer Generated Data. Flock may provide Customer with the opportunity to post, upload, display, publish, distribute, transmit, broadcast, or otherwise make available, messages,

text, illustrations, files, images, graphics, photos, comments, sounds, music, videos, information, content, ratings, reviews, data, questions, suggestions, or other information or materials produced by Customer (“***Customer Generated Data***”). Customer shall retain whatever legally cognizable right, title, and interest in Customer Generated Data. Customer understands and acknowledges that Flock has no obligation to monitor or enforce Customer’s intellectual property rights of Customer Generated Data. Customer grants Flock a non-exclusive, irrevocable, worldwide, royalty-free, license to use the Customer Generated Data for the purpose of providing Flock Services. Flock does not own and shall not sell Customer Generated Data.

4.3 Anonymized Data. Flock shall have the right to collect, analyze, and anonymize Customer Data and Customer Generated Data to the extent such anonymization renders the data non-identifiable to create Anonymized Data to use and perform the Services and related systems and technologies, including the training of machine learning algorithms. Customer hereby grants Flock a non-exclusive, worldwide, perpetual, royalty-free right to use and distribute such Anonymized Data to improve and enhance the Services and for other development, diagnostic and corrective purposes, and other Flock offerings. Parties understand that the aforementioned license is required for continuity of Services. Flock does not own and shall not sell Anonymized Data.

5. CONFIDENTIALITY; DISCLOSURES

5.1 Confidentiality. To the extent required by any applicable public records requests, each Party (the “***Receiving Party***”) understands that the other Party (the “***Disclosing Party***”) has disclosed or may disclose business, technical or financial information relating to the Disclosing Party’s business (hereinafter referred to as “***Proprietary Information***” of the Disclosing Party). Proprietary Information of Flock includes non-public information regarding features, functionality and performance of the Services. Proprietary Information of Customer includes non-public data provided by Customer to Flock or collected by Flock via Flock Services, which includes but is not limited to geolocation information and environmental data collected by sensors. The Receiving Party agrees: (i) to take the same security precautions to protect against disclosure or unauthorized use of such Proprietary Information that the Party takes with its own proprietary information, but in no event less than commercially reasonable precautions, and (ii) not to use (except in performance of the Services or as otherwise permitted herein) or divulge to any third person any

such Proprietary Information. The Disclosing Party agrees that the foregoing shall not apply with respect to any information that the Receiving Party can document (a) is or becomes generally available to the public; or (b) was in its possession or known by it prior to receipt from the Disclosing Party; or (c) was rightfully disclosed to it without restriction by a third party; or (d) was independently developed without use of any Proprietary Information of the Disclosing Party. Nothing in this Agreement will prevent the Receiving Party from disclosing the Proprietary Information pursuant to any judicial or governmental order, provided that the Receiving Party gives the Disclosing Party reasonable prior notice of such disclosure to contest such order. At the termination of this Agreement, all Proprietary Information will be returned to the Disclosing Party, destroyed or erased (if recorded on an erasable storage medium), together with any copies thereof, when no longer needed for the purposes above, or upon request from the Disclosing Party, and in any case upon termination of the Agreement. Notwithstanding any termination, all confidentiality obligations of Proprietary Information that is trade secret shall continue in perpetuity or until such information is no longer trade secret.

5.2 Usage Restrictions on Flock IP. Flock and its licensors retain all right, title and interest in and to the Flock IP and its components, and Customer acknowledges that it neither owns nor acquires any additional rights in and to the foregoing not expressly granted by this Agreement. Customer further acknowledges that Flock retains the right to use the foregoing for any purpose in Flock's sole discretion. Customer and Authorized End Users shall not: (i) copy or duplicate any of the Flock IP; (ii) decompile, disassemble, reverse engineer, or otherwise attempt to obtain or perceive the source code from which any software component of any of the Flock IP is compiled or interpreted, or apply any other process or procedure to derive the source code of any software included in the Flock IP; (iii) attempt to modify, alter, tamper with or repair any of the Flock IP, or attempt to create any derivative product from any of the foregoing; (iv) interfere or attempt to interfere in any manner with the functionality or proper working of any of the Flock IP; (v) remove, obscure, or alter any notice of any intellectual property or proprietary right appearing on or contained within the Flock Services or Flock IP; (vi) use the Flock Services for anything other than the Permitted Purpose; or (vii) assign, sublicense, sell, resell, lease, rent, or otherwise transfer, convey, pledge as security, or otherwise encumber, Customer's rights. There are no implied rights.

5.3 Disclosure of Footage. Subject to and during the Retention Period, Flock may access, use, preserve and/or disclose the Footage to law enforcement authorities, government officials, and/or third parties, if legally required to do so or if Flock has a good faith belief that such access, use, preservation or disclosure is reasonably necessary to comply with a legal process, enforce this Agreement, or detect, prevent or otherwise address security, privacy, fraud or technical issues, or emergency situations.

6. PAYMENT OF FEES

6.1 Billing and Payment of Fees. Customer shall pay the fees set forth in the applicable Order Form based on the billing structure and payment terms as indicated in the Order Form. If Customer believes that Flock has billed Customer incorrectly, Customer must contact Flock no later than thirty (30) days after the closing date on the first invoice in which the error or problem appeared to receive an adjustment or credit. Customer acknowledges and agrees that a failure to contact Flock within this period will serve as a waiver of any claim. If any undisputed fee is more than thirty (30) days overdue, Flock may, without limiting its other rights and remedies, suspend delivery of its service until such undisputed invoice is paid in full. Flock shall provide at least thirty (30) days' prior written notice to Customer of the payment delinquency before exercising any suspension right.

6.2 Notice of Changes to Fees. Flock reserves the right to change the fees for subsequent Renewal Terms by providing sixty (60) days' notice (which may be sent by email) prior to the end of the Initial Term or Renewal Term (as applicable).

6.3 Late Fees. If payment is not issued to Flock by the due date of the invoice, an interest penalty of 1.0% of any unpaid amount may be added for each month or fraction thereafter, until final payment is made.

6.4 Taxes. Customer is responsible for all taxes, levies, or duties, excluding only taxes based on Flock's net income, imposed by taxing authorities associated with the order. If Flock has the legal obligation to pay or collect taxes, including amount subsequently assessed by a taxing authority, for which Customer is responsible, the appropriate amount shall be invoice to and paid by Customer unless Customer provides Flock a legally sufficient tax exemption certificate and Flock shall not charge customer any taxes from which it is exempt. If any deduction or

withholding is required by law, Customer shall notify Flock and shall pay Flock any additional amounts necessary to ensure that the net amount that Flock receives, after any deduction and withholding, equals the amount Flock would have received if no deduction or withholding had been required.

7. TERM AND TERMINATION

7.1 **Term.** The initial term of this Agreement shall be for the period of time set forth on the Order Form (the “**Term**”). Following the Term, unless otherwise indicated on the Order Form, this Agreement will automatically renew for successive renewal terms of the greater of one year or the length set forth on the Order Form (each, a “**Renewal Term**”) unless either Party gives the other Party notice of non-renewal at least thirty (30) days prior to the end of the then-current term.

7.2 **Termination.** Upon termination or expiration of this Agreement, Flock will remove any applicable Flock Hardware at a commercially reasonable time period. In the event of any material breach of this Agreement, the non-breaching Party may terminate this Agreement prior to the end of the Term by giving thirty (30) days prior written notice to the breaching Party; provided, however, that this Agreement will not terminate if the breaching Party has cured the breach prior to the expiration of such thirty (30) day period (“**Cure Period**”). Either Party may terminate this Agreement (i) upon the institution by or against the other Party of insolvency, receivership or bankruptcy proceedings, (ii) upon the other Party's making an assignment for the benefit of creditors, or (iii) upon the other Party's dissolution or ceasing to do business. In the event of a material breach by Flock, and Flock is unable to cure within the **Cure Period**, Flock will refund Customer a pro-rata portion of the pre-paid fees for Services not received due to such termination.

7.3 **Survival.** The following Sections will survive termination: 1, 3, 5, 6, 7, 8.3, 8.4, 9, 11.1 and 11.6.

8. REMEDY FOR DEFECT; WARRANTY AND DISCLAIMER

8.1 **Manufacturer Defect.** Upon a malfunction or failure of Flock Hardware or Embedded Software (a “*Defect*”), Customer must notify Flock’s technical support team. In the event of a Defect, Flock shall make a commercially reasonable attempt to repair or replace the defective Flock Hardware at no additional cost to the Customer. Flock reserves the right, in its sole discretion, to repair or replace such Defect, provided that Flock shall conduct inspection or testing within a commercially reasonable time, but no longer than seven (7) business days after Customer gives notice to Flock.

8.2 **Replacements.** In the event that Flock Hardware is lost, stolen, or damaged, Customer may request a replacement of Flock Hardware at a fee according to the reinstall fee schedule (<https://www.flocksafety.com/reinstall-fee-schedule>). In the event that Customer chooses not to replace lost, damaged, or stolen Flock Hardware, Customer understands and agrees that (1) Flock Services will be materially affected, and (2) that Flock shall have no liability to Customer regarding such affected Flock Services, nor shall Customer receive a refund for the lost, damaged, or stolen Flock Hardware.

8.3 **Warranty.** Flock shall use reasonable efforts consistent with prevailing industry standards to maintain the Services in a manner which minimizes errors and interruptions in the Services and shall perform the Installation Services in a professional and workmanlike manner. Services may be temporarily unavailable for scheduled maintenance or for unscheduled emergency maintenance, either by Flock or by third-party providers, or because of other causes beyond Flock’s reasonable control, but Flock shall use reasonable efforts to provide advance notice in writing or by e-mail of any scheduled service disruption.

8.4 **Disclaimer.** THE REMEDY DESCRIBED IN SECTION 8.1 ABOVE IS CUSTOMER’S SOLE REMEDY, AND FLOCK’S SOLE LIABILITY, WITH RESPECT TO DEFECTS. FLOCK DOES NOT WARRANT THAT THE SERVICES WILL BE UNINTERRUPTED OR ERROR FREE; NOR DOES IT MAKE ANY WARRANTY AS TO THE RESULTS THAT MAY BE OBTAINED FROM USE OF THE SERVICES. EXCEPT AS EXPRESSLY SET FORTH IN THIS SECTION, THE SERVICES ARE PROVIDED “AS IS” AND FLOCK DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A

PARTICULAR PURPOSE AND NON-INFRINGEMENT. THIS DISCLAIMER ONLY APPLIES TO THE EXTENT ALLOWED BY THE GOVERNING LAW OF THE STATE MENTIONED IN SECTION 11.6.

8.5 **Insurance.** Flock will maintain commercial general liability policies as stated in Exhibit B.

8.6 **Force Majeure.** Parties are not responsible or liable for any delays or failures in performance from any cause beyond their control, including, but not limited to acts of God, changes to law or regulations, embargoes, war, terrorist acts, pandemics (including the spread of variants), issues of national security, acts or omissions of third-party technology providers, riots, fires, earthquakes, floods, power blackouts, strikes, supply chain shortages of equipment or supplies, financial institution crisis, weather conditions or acts of hackers, internet service providers or any other third party acts or omissions.

9. LIMITATION OF LIABILITY; INDEMNITY

9.1 **Limitation of Liability.** NOTWITHSTANDING ANYTHING TO THE CONTRARY, FLOCK, ITS OFFICERS, AFFILIATES, REPRESENTATIVES, CONTRACTORS AND EMPLOYEES SHALL NOT BE RESPONSIBLE OR LIABLE WITH RESPECT TO ANY SUBJECT MATTER OF THIS AGREEMENT OR TERMS AND CONDITIONS RELATED THERETO UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY, PRODUCT LIABILITY, OR OTHER THEORY: (A) FOR LOSS OF REVENUE, BUSINESS OR BUSINESS INTERRUPTION; (B) INCOMPLETE, CORRUPT, OR INACCURATE DATA; (C) COST OF PROCUREMENT OF SUBSTITUTE GOODS, SERVICES OR TECHNOLOGY; (D) FOR ANY INDIRECT, EXEMPLARY, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES; (E) FOR ANY MATTER BEYOND FLOCK'S ACTUAL KNOWLEDGE OR REASONABLE CONTROL INCLUDING REPEAT CRIMINAL ACTIVITY OR INABILITY TO CAPTURE FOOTAGE; OR (F) FOR ANY AMOUNTS THAT, TOGETHER WITH AMOUNTS ASSOCIATED WITH ALL OTHER CLAIMS, EXCEED THE FEES PAID AND/OR PAYABLE BY CUSTOMER TO FLOCK FOR THE SERVICES UNDER THIS AGREEMENT IN THE TWELVE (12) MONTHS PRIOR TO THE ACT OR OMISSION THAT GAVE RISE TO THE LIABILITY, IN EACH CASE, WHETHER OR NOT FLOCK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF

LIABILITY OF SECTION ONLY APPLIES TO THE EXTENT ALLOWED BY THE GOVERNING LAW OF THE STATE REFERENCED IN SECTION 10.6.

NOTWITHSTANDING ANYTHING TO THE CONTRARY, THE FOREGOING LIMITATIONS OF LIABILITY SHALL NOT APPLY (I) IN THE EVENT OF GROSS NEGLIGENCE OR WILLFUL MISCONDUCT, OR (II) INDEMNIFICATION OBLIGATIONS.

9.2 Responsibility. Each Party to this Agreement shall assume the responsibility and liability for the acts and omissions of its own employees, officers, or agents, in connection with the performance of their official duties under this Agreement. Each Party to this Agreement shall be liable for the torts of its own officers, agents, or employees.

9.3 Flock Indemnity. Flock shall indemnify and hold harmless Customer, its agents and employees, from liability of any kind, including claims, costs (including defense) and expenses, on account of: (i) any copyrighted material, patented or unpatented invention, articles, device or appliance manufactured or used in the performance of this Agreement; or (ii) any damage or injury to property or person directly caused by Flock's installation of Flock Hardware, except for where such damage or injury was caused solely by the negligence of the Customer or its agents, officers or employees. Flock's performance of this indemnity obligation shall not exceed the fees paid and/or payable for the services rendered under this Agreement in the preceding twelve (12) months.

10. INSTALLATION SERVICES AND OBLIGATIONS

10.1 Ownership of Hardware. Flock Hardware is owned and shall remain the exclusive property of Flock. Title to any Flock Hardware shall not pass to Customer upon execution of this Agreement, except as otherwise specifically set forth in this Agreement. Except as otherwise expressly stated in this Agreement, Customer is not permitted to remove, reposition, re-install, tamper with, alter, adjust or otherwise take possession or control of Flock Hardware. Customer agrees and understands that in the event Customer is found to engage in any of the foregoing restricted actions, all warranties herein shall be null and void, and this Agreement shall be subject to immediate termination for material breach by Customer. Customer shall not perform any acts which would interfere with the retention of title of the Flock Hardware by Flock. Should Customer default on any payment of the Flock Services, Flock may remove Flock Hardware at

Flock's discretion. Such removal, if made by Flock, shall not be deemed a waiver of Flock's rights to any damages Flock may sustain as a result of Customer's default and Flock shall have the right to enforce any other legal remedy or right.

10.2 Deployment Plan. Flock shall advise Customer on the location and positioning of the Flock Hardware for optimal product functionality, as conditions and locations allow. Flock will collaborate with Customer to design the strategic geographic mapping of the location(s) and implementation of Flock Hardware to create a deployment plan ("***Deployment Plan***"). In the event that Flock determines that Flock Hardware will not achieve optimal functionality at a designated location, Flock shall have final discretion to veto a specific location, and will provide alternative options to Customer.

10.3 Changes to Deployment Plan. After installation of Flock Hardware, any subsequent requested changes to the Deployment Plan, including, but not limited to, relocating, re-positioning, adjusting of the mounting, removing foliage, replacement, changes to heights of poles will incur a fee according to the reinstall fee schedule located at (<https://www.flocksafety.com/reinstall-fee-schedule>). Customer will receive prior notice and confirm approval of any such fees.

10.4 Customer Installation Obligations. Customer is responsible for any applicable supplementary cost as described in the Customer Implementation Guide, attached hereto as Exhibit C ("***Customer Obligations***"). Customer represents and warrants that it has, or shall lawfully obtain, all necessary right title and authority and hereby authorizes Flock to install the Flock Hardware at the designated locations and to make any necessary inspections or maintenance in connection with such installation.

10.5 Flock's Obligations. Installation of any Flock Hardware shall be installed in a professional manner within a commercially reasonable time from the Effective Date of this Agreement. Upon removal of Flock Hardware, Flock shall restore the location to its original condition, ordinary wear and tear excepted. Flock will continue to monitor the performance of Flock Hardware for the length of the Term. Flock may use a subcontractor or third party to perform certain obligations under this agreement, provided that Flock's use of such subcontractor or third party shall not release Flock from any duty or liability to fulfill Flock's obligations under this Agreement.

11. MISCELLANEOUS

11.1 Compliance With Laws. Parties shall comply with all applicable local, state and federal laws, regulations, policies and ordinances and their associated record retention schedules, including responding to any subpoena request(s).

11.2 Severability. If any provision of this Agreement is found to be unenforceable or invalid, that provision will be limited or eliminated to the minimum extent necessary so that this Agreement will otherwise remain in full force and effect.

11.3 Assignment. This Agreement is not assignable, transferable or sublicensable by either Party, without prior consent. Notwithstanding the foregoing, either Party may assign this Agreement, without the other Party's consent, (i) to any parent, subsidiary, or affiliate entity, or (ii) to any purchaser of all or substantially all of such Party's assets or to any successor by way of merger, consolidation or similar transaction.

11.4 Entire Agreement. This Agreement, together with the Order Form(s), the reinstall fee schedule (<https://www.flocksafety.com/reinstall-fee-schedule>), and any attached exhibits are the complete and exclusive statement of the mutual understanding of the Parties and supersedes and cancels all previous or contemporaneous negotiations, discussions or agreements, whether written and oral, communications and other understandings relating to the subject matter of this Agreement, and that all waivers and modifications must be in a writing signed by both Parties, except as otherwise provided herein. None of Customer's purchase orders, authorizations or similar documents will alter the terms of this Agreement, and any such conflicting terms are expressly rejected. Any mutually agreed upon future purchase order is subject to these legal terms and does not alter the rights and obligations under this Agreement, except that future purchase orders may outline additional products, services, quantities and billing terms to be mutually accepted by Parties. In the event of any conflict of terms found in this Agreement or any other terms and conditions, the terms of this Agreement shall prevail. Customer agrees that Customer's purchase is neither contingent upon the delivery of any future functionality or features nor dependent upon any oral or written comments made by Flock with respect to future functionality or feature.

11.5 Relationship. No agency, partnership, joint venture, or employment is created as a result of this Agreement and Parties do not have any authority of any kind to bind each other in any respect whatsoever. Flock shall at all times be and act as an independent contractor to Customer.

11.6 Governing Law; Venue. This Agreement shall be governed by the laws of the state in which the Customer is located. The Parties hereto agree that venue would be proper in the chosen courts of the State of which the Customer is located. The Parties agree that the United Nations Convention for the International Sale of Goods is excluded in its entirety from this Agreement.

11.7 Special Terms. Flock may offer certain special terms which are indicated in the proposal and will become part of this Agreement, upon Customer's prior written consent and the mutual execution by authorized representatives ("***Special Terms***"). To the extent that any terms of this Agreement are inconsistent or conflict with the Special Terms, the Special Terms shall control.

11.8 Publicity. Flock has the right to reference and use Customer's name and trademarks and disclose the nature of the Services in business and development and marketing efforts.

11.9 Feedback. If Customer or Authorized End User provides any suggestions, ideas, enhancement requests, feedback, recommendations or other information relating to the subject matter hereunder, Agency or Authorized End User hereby assigns to Flock all right, title and interest (including intellectual property rights) with respect to or resulting from any of the foregoing.

11.10 Export. Customer may not remove or export from the United States or allow the export or re-export of the Flock IP or anything related thereto, or any direct product thereof in violation of any restrictions, laws or regulations of the United States Department of Commerce, the United States Department of Treasury Office of Foreign Assets Control, or any other United States or foreign Customer or authority. As defined in Federal Acquisition Regulation ("FAR"), section 2.101, the Services, the Flock Hardware and Documentation are "commercial items" and according to the Department of Defense Federal Acquisition Regulation ("DFAR") section 252.2277014(a)(1) and are deemed to be "commercial computer software" and "commercial computer software documentation." Flock is compliant with FAR Section 889 and does not contract or do business with, use any equipment, system, or service that uses the enumerated banned Chinese telecommunication companies, equipment or services as a substantial or essential component of any system, or as critical technology as part of any Flock system. Consistent with DFAR section 227.7202 and FAR section 12.212, any use, modification, reproduction, release, performance, display, or disclosure of such commercial software or commercial software documentation by the U.S. Government will be governed solely by the terms of this Agreement and will be prohibited except to the extent expressly permitted by the terms of this Agreement.

11.11 **Headings.** The headings are merely for organization and should not be construed as adding meaning to the Agreement or interpreting the associated sections.

11.12 **Authority.** Each of the below signers of this Agreement represent that they understand this Agreement and have the authority to sign on behalf of and bind the Parties they are representing.

11.13 **Conflict.** In the event there is a conflict between this Agreement and any applicable statement of work, or Customer purchase order, this Agreement controls unless explicitly stated otherwise.

11.14 **Morality.** In the event Customer or its agents become the subject of an indictment, contempt, scandal, crime of moral turpitude or similar event that would negatively impact or tarnish Flock's reputation, Flock shall have the option to terminate this Agreement upon prior written notice to Customer.

11.15 **Notices.** All notices under this Agreement will be in writing and will be deemed to have been duly given when received, if personally delivered; when receipt is electronically confirmed, if transmitted by email; the day after it is sent, if sent for next day delivery by recognized overnight delivery service; and upon receipt to the address listed on the Order Form (or, if different, below), if sent by certified or registered mail, return receipt requested.

11.16 **Non-Appropriation.** Notwithstanding any other provision of this Agreement, all obligations of the Customer under this Agreement which require the expenditure of funds are conditioned on the availability of funds appropriated for that purpose. Customer shall have the right to terminate this Agreement for non appropriation with thirty (30) days written notice without penalty or other cost.

FLOCK NOTICES ADDRESS:

1170 HOWELL MILL ROAD, NW SUITE 210

ATLANTA, GA 30318

ATTN: LEGAL DEPARTMENT

EMAIL: legal@flocksafety.com

Customer NOTICES ADDRESS:

ADDRESS:

ATTN:

EMAIL:

EXHIBIT B
INSURANCE

Required Coverage. Flock shall procure and maintain for the duration of this Agreement insurance against claims for injuries to persons or damages to property that may arise from or in connection with the performance of the services under this Agreement and the results of that work by Flock or its agents, representatives, employees or subcontractors. Insurance shall be placed with insurers with a current A. M. Best rating of no less than “A” and “VII”. Flock shall obtain and, during the term of this Agreement, shall maintain policies of professional liability (errors and omissions), automobile liability, and general liability insurance for insurable amounts of not less than the limits listed herein. The insurance policies shall provide that the policies shall remain in full force during the life of the Agreement. Flock shall procure and shall maintain during the life of this Agreement Worker's Compensation insurance as required by applicable State law for all Flock employees.

Types and Amounts Required. Flock shall maintain, at minimum, the following insurance coverage for the duration of this Agreement:

- (i) **Commercial General Liability** insurance written on an occurrence basis with minimum limits of One Million Dollars (\$1,000,000) per occurrence and Two Million Dollars (\$2,000,000) in the aggregate for bodily injury, death, and property damage, including personal injury, contractual liability, independent contractors, broad-form property damage, and product and completed operations coverage;
- (ii) **Umbrella or Excess Liability** insurance written on an occurrence basis with minimum limits of Ten Million Dollars (\$10,000,000) per occurrence and Ten Million Dollars (\$10,000,000) in the aggregate;
- (iii) **Professional Liability/Errors and Omissions** insurance with minimum limits of Five Million Dollars (\$5,000,000) per occurrence and Five Million Dollars (\$5,000,000) in the aggregate;
- (iv) **Commercial Automobile Liability** insurance with a minimum combined single limit of One Million Dollars (\$1,000,000) per occurrence for bodily injury, death, and property coverage, including owned and non-owned and hired automobile coverage; and

(v) **Cyber Liability** insurance written on an occurrence basis with minimum limits of Five Million Dollars (\$5,000,000).

Account name: 10103370

CITY OF OAKLAND CA
7101 EDGEWATER DR BLDG 5
OAKLAND CA 94621-3001

SHIP-TO

CITY OF OAKLAND POLICE DEPARTMENT
455 7TH ST
OAKLAND CA 94607-3940

We deliver according to the following terms:

Payment Terms : Net 30 days
Ship Via : Insight Assigned Carrier/Ground
Terms of Delivery : FOB DESTINATION
Currency : USD

Customer understands, accepts and agrees that this purchase is subject to Flock Safety's End User License Agreement, available at: <https://www.flocksafety.com/terms-and-conditions-eula>

TERM START: Unless otherwise noted, the Term shall commence upon first installation and validation of Flock Hardware

TERM: 12 Months

COVERAGE DATES: 08/01/2025 - 07/31/2026

RETENTION PERIOD: 30 days

BILLING: Project will be invoiced 100% upon issuance of PO

Proposed Special Terms: The Term of this contract shall be from 08/01/2025 - 07/31/2026. This Agreement supersedes any and all previously executed agreement between the Parties, relating to the provision of services by Flock to Customer and any exhibits attached

Quotation

Quotation Number : [0228698604](#)
Document Date : 08-AUG-2025
PO Number :
PO Release :
Sales Rep : Alfred Lam
Email : ALFRED.LAM@INSIGHT.COM
Phone : +13102254052
Sales Rep 2 : Katheleen Jackson
Email : KATHELEEN.JACKSON@INSIGHT.COM
Phone : +13103375206

Material	Material Description	Quantity	Unit Price	Extended Price
FOS-ENHANLPR-T9	FLOCK OS ENHANCED LPR (701-1000 OFFICERS) Coverage Dates: 01-AUG-2025 - 31-JUL-2026 STATE OF CALIFORNIA NASPO CLOUD SOLUTIONS(# AR2485/ 7-17-70-40-01)	1	44,550.00	44,550.00
FOS-ELITE-T9	FLOCK OS ELITE (701-1000 OFFICERS) Coverage Dates: 01-AUG-2025 - 31-JUL-2026 STATE OF CALIFORNIA NASPO CLOUD SOLUTIONS(# AR2485/ 7-17-70-40-01)	1	89,100.00	89,100.00
FLCK-FALCON-2-LE	FLOCK GROUP FALCON INFRASTRUCTURE- POWER + LTE), LICENSE PLATE RECOGNITION CAMERA WITH VEHICLE FINGERPRINT™ + MACHINE LEARNING SOFTWARE AND REAL- ALERTS FOR UNLIMITED USERS Coverage Dates: 01-AUG-2025 - 31-JUL-2026 STATE OF CALIFORNIA NASPO CLOUD SOLUTIONS(# AR2485/ 7-17-70-40-01)	274	2,970.00	813,780.00
FLCK-FALCON-LR	Flock Speed Cam - Law Enforcement grade - Vehicle speed license plate recognition camera with Vehicle Fingerprint - Proprietary machine learning - Real-Time Alerts for Unlimited users - LTE AC Power only Coverage Dates: 01-AUG-2025 - 31-JUL-2026 STATE OF CALIFORNIA NASPO CLOUD SOLUTIONS(# AR2485/ 7-17-70-40-01)	16	4,950.00	79,200.00

Material	Material Description	Quantity	Unit Price	Extended Price
FLCK-CONDOR-PTZ	Flock's Software Service & Support - Live Streaming & Video Recording Coverage Dates: 01-AUG-2025 - 31-JUL-2026 STATE OF CALIFORNIA NASPO CLOUD SOLUTIONS(# AR2485/7-17-70-40-01)	40	2,970.00	118,800.00
PS-IMP-CONDOR-STD	FLOCK CONDOR PROFESSIONAL SERVICES - IMPLEMENTATION FEE STATE OF CALIFORNIA NASPO CLOUD SOLUTIONS(# AR2485/7-17-70-40-01)	40	742.50	29,700.00
Product Subtotal				1,145,430.00
Services Subtotal				29,700.00
TAX				0.00
Total				1,175,130.00

Lease & Financing options available from Insight Global Finance for your equipment & software acquisitions. Contact your Insight account executive for a quote.

Thank you for choosing Insight. Please contact us with any questions or for additional information about Insight's complete IT solution offering.

Sincerely,

Alfred Lam
+13102254052
ALFRED.LAM@INSIGHT.COM

Katheleen Jackson
+13103375206
KATHELEEN.JACKSON@INSIGHT.COM

Any purchase and use of Citrix Cloud Platform and Citrix Enterprise Software-As-A-Service ("SaaS") Subscriptions is subject to the following Citrix terms of use: <https://www.insight.com/CitrixNaspoTerms>

To purchase under this contract, your agency must be registered with OMNIA Partners Public Sector.

Insight Global Finance has a wide variety of flexible financing options and technology refresh solutions. Contact your Insight representative for an innovative approach to maximizing your technology and developing a strategy to manage your financial options.

This purchase is subject to Insight's online Terms of Sale unless you are purchasing under an Insight Public Sector, Inc. contract vehicle, in which case, that agreement will govern.

SOFTWARE AND CLOUD SERVICES PURCHASES: If your purchase contains any software or cloud computing offerings ("Software and Cloud Offerings"), each offering will be subject to the applicable supplier's end user license and use terms ("Supplier Terms") made available by the supplier or which can be found at the "terms-and-policies" link below. By ordering, paying for, receiving or using Software and Cloud Offerings, you agree to be bound by and accept the Supplier Terms unless you and the applicable supplier have a separate agreement which governs.

Insight's online Terms of Sale can be found at the "terms-and-policies" link below.

<https://www.insight.com/terms-and-policies>

Oakland Police Department Community Safety Camera Registry

OPD accessed Community Safety Camera Systems and associated VMS and Operating Systems are intended to deter criminal activity within specific public areas and enhance the Department's ability to address disruptive criminal activity within the community. These disruptive crimes include theft, vehicle theft, human trafficking, reckless driving, sideshow/takeovers, felony evasion, burglaries, robberies, shootings, and homicides. Many criminal investigations hinge upon the availability and quality of surveillance video as evidence that is later used in the prosecution of criminal cases.

Please complete the following form in order to consent to devices under your management or control participating in the Community Safety Camera System. Please utilize the link below to review the Department Policy related to CS Camera Systems. (**Department General Order DGO I-32.1**) <https://public.powerdms.com/OAKLAND/documents/3942866>

^{*} Required

1. Name of the individual, business or institution that will contribute to the Community Safety Camera System. Please also provide contact information [name, phone number and/or email] in the event the Department would need to contact you related to an investigation. (This information will be used for internal management purposes and will not be disclosed unless necessary for a legal proceeding, by court order or other lawful request). ^{*}

2. Location of the privately owned camera system (This information will be used for internal management purposes and will not be disclosed unless necessary for a legal proceeding, by court order or other lawful request). ^{*}

3. I consent to, and understand that real-time and historical data related to camera devices participating in the CS Camera System may be accessed by authorized members of the Oakland Police Department related to specific investigations as related by Department Policy (DGO I-32.1). ^{*}

☐ Yes, and understand and provide consent

☐ No

4. By authorizing the Oakland Police Department to access camera systems as part of the Community Safety Camera network, you acknowledge that The Oakland Police Department does not permit the sharing of CS Camera System data gathered by the city or its contractors/subcontractors for the purpose of federal immigration enforcement, pursuant to the California Values Act (Government Code § 7282.5; Government Code § 7284.2 et seq) – these federal immigration agencies include Immigration and Customs Enforcement (ICE) and Customs and Border Patrol (CPB). *

☐ Yes

☐ No

5. I understand and acknowledge that providing access to camera systems is not a replacement for private security, that these devices/feeds will not be constantly monitored by the Department, and that providing access does not guarantee immediate response by members of the Department for crimes in progress. *

☐ Yes, I understand and acknowledge

☐ No

6. I understand and acknowledge that participation in the Camera Safety Community Camera Registry disallows the use of all and any facial recognition technology. *

☐ Yes

☐ No

7. I understand and agree to the following:

While private cameras are not subject to the same placement approvals as police-owned systems, participants shall make good faith efforts to: Avoid placing cameras in ways that capture sensitive spaces or conduct continuous surveillance of individuals not engaged in suspected criminal activity; Angle or limit fields of view to reduce visibility of private residences or sensitive community facilities; Implement masking, privacy zones, or field-of-view restrictions when feasible. *

☐ Yes

☐ No

This content is neither created nor endorsed by Microsoft. The data you submit will be sent to the form owner.

 Microsoft Forms