CITY OF OAKLAND

Privacy Advisory Commission
Meeting Agenda

Oakland City Hall, Hearing Room 1
1 Frank H. Ogawa Plaza

Thursday June 4, 2026
5:00 PM

PUBLIC PARTICIPATION

The Privacy Advisory Commission encourages public participation in its meetings. Members of the public may observe and/or provide public comment in the following ways:

OBSERVE THE MEETING

By Zoom:
To observe the meeting via video conference, please click the following link at the noticed meeting time:
https://us02web.zoom.us/j/85817209915

By Phone:
Call he number below:

+1 669 444 9171

Instructions for joining by phone are available at:
https://support.zoom.us/hc/en-us/articles/201362663

PROVIDE PUBLIC COMMENT

Public comment may be submitted in the following ways, within the time allotted for each eligible agenda item:

• Submit written comment in advance:
Email your comment, full name, and the agenda item number to Michelle NewRingeisen at MNewRingeisen@oaklandca.gov no later than one (1) hour before the posted meeting time. All timely submissions will be shared with the Selection Panel prior to the meeting.

• Complete a speaker card during the meeting.

• Raise your hand on Zoom during public comment or open forum and staff will call on you to speak for the time allotted by the Chair.

For questions regarding these procedures, please contact Michelle NewRingeisen at
MNewRingeisen@oaklandca.gov

CITY OF OAKLAND

Privacy Advisory Commission
Meeting Agenda

Oakland City Hall, Hearing Room 1
1 Frank H. Ogawa Plaza

Thursday June 4, 2026
5:00 PM

I. CALL TO ORDER
The Chair opens the meeting and officially begins proceedings.

II. ROLL CALL
The Clerk Calls roll to confirm member attendance to determine if there is a quorum (5 members) to conduct business.

Commissioners: Byron White, Issac Cheng, Gina Tomlinson, Vice Chair Henry Gage III, Chair Jessica Leavitt,

III. PUBLIC COMMENT
During Public Comment, members of the public may comment on any a**gendized items** within the Commission's jurisdiction when called.

IV. APPROVAL OF MINUTES
The Panel reviews the draft minutes from a prior meeting and may take action to approve them as presented or with revisions.

1. April 2nd Meeting Minutes

V. OPD REQUEST (APRIL 2026) FOR SURVEILLANCE FOOTAGE PURSUANT TO THE PUBLIC WORKS DEPARTMENT'S SURVEILLANCE USE POLICY FOR ILLEGAL DUMPING CAMERAS
Summary of OPD requests for surveillance footage related to a fatal hit-and-run investigation, including footage provided from multiple Public Works POD locations and timeframes on April 16, 2026.

VI. AUTOMATED LICENSE PLATE READERS (ALPR) REPORT
2025 OPD Annual Report on OPD's usage of Automated License Plate Readers (ALPR)

VII. BIOMETRIC CRIME LAB REPORT
2025 OPD Annual Report on OPD's use of Criminalistics Laboratory DNA Instrumentation and Analysis Software Biometric Technology

VIII. UNMANNED AERIAL SYSTEM "DRONES" REPORT
2025 OPD Annual Report on the use of Unmanned Aerial System (UAS) which is an unmanned aircraft of any type that can sustain directed flight, whether preprogrammed or remotely controlled (commonly referred to as an unmanned aerial vehicle (UAV) or drone

IX. FORWARD LOOKING INFRARED (FLIR) REPORT
2025 OPD Annual Report on the use of OPD's forward looking infrared (FLIR) 8500 cameras which are able to obtain live video and record video concurrently. These cameras have been utilized by its patrol helicopters for the past decade.

CITY OF OAKLAND

Privacy Advisory Commission
Meeting Agenda

Oakland City Hall, Hearing Room 1
1 Frank H. Ogawa Plaza

Thursday June 4, 2026
5:00 PM

X. LIVESTREAM TRANSMITTERS REPORT
2025 OPD Annual Report on the use of OPD's Livestream transmitters which are attached to handheld video cameras; these cameras were not in use in 2025

XI. DGO: I-12/ALPR Policy
Review of OPD's revised I-12/Automated License Plate Readers (ALPR) policy

XII. ANNUAL SURVEILLANCE TECHNOLOGY REPORT – DEPARTMENT OF VIOLENCE PREVENTION APRICOT DATA MANAGEMENT SYSTEM
2026 Annual Report on the Department of Violence Prevention's Apricot Data Management System, a case management and grant administration platform used to collect, store, manage, and report information related to service delivery, client outcomes, and funded agency performance.

XIII. Open forum
Members of the public may speak on **non-agendized** items within the Panel's jurisdiction.

ADJOURNMENT

Do you need an ASL, Cantonese, Mandarin or Spanish interpreter or other assistance to participate? Please email Michelle NewRingeisen at MNewRingeisen@oaklandca.gov or call (510) 238- or (510) 238-2007 for TDD/TTY five days in advance.

¿Necesita un intérprete en español, cantonés o mandarín, u otra ayuda para participar? Por favor envíe un correo electrónico a Felicia Michelle NewRingeisen at MNewRingeisen@oaklandca.govo llame al (510) 238-7857 o al (510) 238-2007 para TDD/TTY por lo menos cinco días antes de la reunión. Gracias.

你需要手語,西班牙語,粵語或國語翻譯服務嗎?請在會議前五個工作天電郵
Michelle NewRingeisen at MNewRingeisen@oaklandca.gov 或 致電 (510) 238-7857

Privacy Advisory Commission
Draft Meeting Minutes

Oakland City Hall, Hearing Room 1
1 Frank H. Ogawa Plaza

April 2, 2026
5:00 PM

I. Called To order

II. Roll Call

Byron White - Present | Don Wang – Excused | Issac Cheng – Present
Lou Katz – Present | Gina Tomlinson – Excused – 1st part | Vice Chair Henry Gage III - Present | Chair Jessica Leavitt – Present

III. Public Comment

IV. Approval of Meeting Minutes

March 2, 2026 Meeting Minutes

Discussion: No Discussion

Motion: Approve the March 2, 2026 meeting minutes as listed on the agenda with no changes by Vice Chair Gage

Seconded by: Commissioner Byron White

Vote:

Issac Cheng Y	Lou Katz Abstain	Gina Tomlinson Excused
Don Wang Ex	Byron White Y	Vice Chair Henry Gage III Y
Ch Jessica Leavitt Y		

Result: Motion passes 4Y, 1 Abstain, 2 excused

V. Reports

A. Pen Register

Discussion:
Information on this report was presented by Sergeant Zhou of the Oakland Police Department (OPD) detailing the use of the Pen Register tool for investigation and apprehension. The tool is a real-time surveillance tool that enables investigators to view communication (but not content). Additional discussion on the data generated by the tool, volume of usage and how the use of the tool is authorized took place. OPD will add information to the report indicating that no violations or potential violations of the City's surveillance policy were identified.

Motion: Vice Chair Henry Gage III
Move the report to Council with a favorable recommendation finding that the benefits to the community of the surveillance technology outweigh the costs and that civil liberties and civil rights are safeguarded.

Second: Commissioner Lou Katz

Roll Call Vote:
Isaac Cheng – Y Lou Katz – Y Gina Tomlinson - Y
Byron White - Y Vice Chair Henry Gage III - Y
Chair Jessica Leavitt – Y Don Wang – E

Result: Motion passes 6Y and 1 excused

B. Pen Cellbrite

Discussion:
Information on this report was presented by Sergeant Zhou of the Oakland Police Department (OPD) detailing the use of the Pen Cellbrite tool for investigation and apprehension. Additional discussion on the data generated by the tool, volume of usage and how the use of the tool is authorized took place.

Motion: Vice Chair Henry Gage III
Move the report to Council with a favorable recommendation finding that the benefits to the community of the surveillance technology outweigh the costs and that civil liberties and civil rights are safeguarded.

Second: Chair Jessica Leavitt

Roll Call Vote:
Isaac Cheng – Y Lou Katz – Y Gina Tomlinson - Y
Byron White - Y Vice Chair Henry Gage III - Y
Chair Jessica Leavitt – Y Don Wang - E

Result: Motion passes 6Y and 1 excused

C. Crime Tracer

Discussion:
With Crime Tracer sunsetting on June 30, 2026, OPD discussed the technology use over the past year as well as the Department's recommendation to move to a new system, Peregrine to ensure continuity and availability of records search capacity for the City. The functionality of Crime Tracer (and any new system) allows OPD to search among multiple City systems to track data.

The PAC clarified that they were voting on the annual report only, and not the switch to a new vendor. Additional language to specify that the use policy was vendor neutral was also discussed. PAC's role and the City's contracting process was also discussed along with contracting policy, the City's technology governance and security review process.

Motion: Commissioner Isaac Cheng
Recommend to the Council the approval of the annual report, proposing modifications to (a) strike the request in the annual report to change to a new vendor, and (b) any new vendor would be required to comply with the use policy.

Second: Chair Jessica Leavitt

Roll Call Vote:

Isaac Cheng – Y	Lou Katz - N	Gina Tomlinson-Y
Byron White – Y	Vice Chair Henry Gage III - Y	
Chair Jessica Leavitt – Y	Don Wang - E	

Result: Motion passes 5Y, 1N and 1 excused

D. ShotSpotter

Discussion:
Lieutenant Gabriel Urquiza-Leibin of OPD presented the Department's annual report for ShotSpotter for 2025. OPD shared basic information on the parameters of the system as well as data collected. ShotSpotter has been an important tool for OPD, and the Department will continue using the technology in the coming years. In addition to the data the tool provides, it has been critical in helping OPD identify exact areas where shots fired have occurred.

Motion: Vice Chair Henry Gage III
Move the report to Council with a favorable recommendation finding that the benefits to the community of the surveillance technology outweigh the costs and that civil liberties and civil rights are safeguarded.

Second: Commissioner Byron White

Roll Call Vote:
Isaac Cheng – Y Lou Katz – Y Gina Tomlinson - Y
Byron White - Y Vice Chair Henry Gage III - Y
Chair Jessica Leavitt – Y Don Wang - E

VI. Surveillance Use Policy and Surveillance Impact Report for Consideration

ITEM REMOVED FROM THE AGENDA PRIOR TO THE START OF THE MEETING.

Discussion:

Motion:

Second:

Roll Call Vote:

CITY OF OAKLAND

MEMORANDUM

TO: James P. Beere,
Interim Chief of Police

FROM: Omar Daza-Quiroz, A/Deputy Chief
OPD, Bureau of Investigations

SUBJECT: OPD Crime Lab Biometrics DNA Analysis Technology 2025 Annual Report

DATE: April 2026

Background

Oakland Municipal Code (OMC) 9.64.040: Surveillance Technology "Oversight following City Council approval" requires that for approved surveillance technology items (by the Privacy Advisory Commission per OMC 9.64.020 and by City Council per OMC 9.64.030), city staff must present a written annual surveillance report for Privacy Advisory Commission (PAC). OMC 9.64.040 requires that, after City Council approval of surveillance technology, OPD provide an annual report for PAC review before submitting to City Council. After review by the PAC, the PAC shall make a recommendation to the City Council that considers and articulates:

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

Legislative History
The PAC recommended City Council adoption of the "Oakland Police Department (OPD) Criminalistics Laboratory DNA Instrumentation and Analysis Software Biometric Technology Use Policy on October 1, 2020; following the PAC's vote, the City Council adopted Resolution No. 88388 C.M.S. on December 1, 2020. This resolution approved OPD's use of Criminalistics Laboratory DNA Instrumentation and Analysis Software Biometric Technology. An updated Biometric Technology Use Policy and Impact Report were approved along with the required annual report adopted under:

- Resolution No. 89458 C.M.S. filed October 20, 2022
- Resolution No. 89931 C.M.S. filed September 14, 2023
- Resolution No. 90365 C.M.S. filed June 26, 2024

This memorandum is intended to serve and comply with the annual reporting mandate.

2025 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:

General Overview

The Oakland Police Department (OPD) Criminalistics Laboratory's (Crime Lab) Forensic Biology/DNA unit utilizes specialized DNA collection and analysis instrumentation and software to perform forensic DNA testing. During this lengthy and complicated process, one step removes and purifies DNA from cells (digestion/extraction), another quantitates how much DNA is present and lastly, by amplifying and analyzing Short Tandem Repeats (STR) in the DNA using Polymerase Chain Reaction (PCR) and separated by Capillary Electrophoresis (CE), forensic DNA profiles are generated. Software is involved in the following processes: (i) collection and processing of STR DNA fragment data; (ii) interpretation of DNA data into DNA profiles used for comparison purposes. At the end of all processes, a determination can be made as to whether a DNA sample collected from a crime scene can be associated with a known individual through a comparison of evidentiary (crime scene) and known reference DNA profiles. Statistical weight is provided for all inclusion comparisons.

Specifics: How DNA testing was used in 2025

The Forensic Biology Unit analyzed 414 requests between January 1, 2025 to December 31, 2025. Over 2165 items of evidence were examined, from which 5153 samples were subjected to digestion and extraction using the Versa and EZ1/2 instruments. Scientist subjected 5199 samples to quantitation analysis using the SpeedVac, Qiagility, and QuantStudio 5 instruments and 1908 samples were subjected to amplification and typing methods using the ProFlex and 3500 instruments. The DNA profiles were processed with FaSTR and ArmedXpert software.

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):

Discovery to the Alameda County District Attorney's Office was provided in 43 cases. A standard discovery packet includes the reports, technical and administrative review sheets, case notes, attachments, contact log, resume, interpretation guidelines, photographs, electronic data, and any supporting documents.

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 Biometric Use Policy covers the specific technology covered. In general, the digestion, quantitation, normalization/amplification, typing, interpretation and databasing are housed in the laboratory of the Police Administration Building (PAB). Database equipment is located in a secure location elsewhere in the PAB as disclosed in the Use Policy. Currently, no equipment resides outside of these locations.

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

All evidence was analyzed at the laboratory located in the PAB. No other locations are authorized. The laboratory services crimes that occur in all areas of the City of Oakland.

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. The laboratory did not receive any complaints through its feedback process.

The laboratory request for services form does not collect race information. It could be argued that requiring information that is not necessary for analysis, such as race, could be biasing; indeed, it would be a great invasion of privacy to capture this data since it is irrelevant to the analyses performed. Furthermore, the race of individuals subject to the DNA analysis technology's use is not revealed during evaluation of evidence as non-coding regions of DNA are typed and do not contain this information. Therefore, staff recommends that the PAC waive the requirement to identify the race of each person subject to the technology's use and make a determination that the probative value in gathering this information to evaluate the technology's impact on privacy interests is outweighed by the potential greater invasiveness in capturing such data.

F. The results of any internal audits, any information about violations or potential violations of the Surveillance Use Policy (SUP), 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:

All Forensic Biology personnel and relevant management were required to review and sign that they understood and would abide by the Surveillance Use Policy and the Impact Reports. Under accreditation, the Laboratory actively seeks feedback from its customers and no concerns were conveyed regarding violations or concerns around the SUP. Lastly, the Laboratory has a means to identify risks through Incident Response. Staff are encouraged to participate in Incident Response by filing Incident Alerts where there were concerns. No violations or potential violations were identified by any of these routes.

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 laboratory maintains an active security program where the security of alarmed portions of the laboratory are tested and results recorded. There were no unexplained alarm events and there were no faults in the alarmed systems that were tested. There were no breaches to the laboratory space nor to the physical equipment that it houses.

The CODIS server is on a dedicated intranet line that uses encryption on both the sender and receiver ends of any communication from/to the server. There was no indication of security lapses in this system.

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

The efficacy of the OPD Criminalistics Laboratory DNA analysis program is illustrated by citing the following compelling statistics:

The laboratory completed 414 requests in 2025. These are further broken out by crime type in Table 1 below

Table 1: OPD Crime Laboratory DNA Analysis Requests in 2025

Crime Type	**Number of Requests**
Homicide/ Attempted Homicide	97
Sexual Assault/Kidnapping	208
Assault/Other Criminal	29
Robbery/Burglary/Auto Theft	17
Hit and run/Carjacking	20
Weapons	42
Cold Case (prior to 2008)	1
Total	**414**

CODIS hits in 2025 – One hundred twenty-two DNA profiles were uploaded to the CODIS database. The laboratory had 239 associations (hits); 66 hits to named individuals whose identity were unknown, four hits to unsolved forensic cases, and 58 hits to previously solved forensic cases.

Thus, forensic DNA analysis is an important tool to investigate and provide potential leads for a variety of crimes that occur in the City of Oakland.

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

There were no public record requests for DNA cases in 2025.

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:

Procurement of instruments is costly and is typically amortized over many budget cycles. Ongoing maintenance is imperative to ensure reliability of the instruments is remediated quickly should a problem occur. The reagents/kits and supplies to conduct testing are also steep.

The primary funding source for annual maintenance are federal grants; however, when grant funding falls short general funds are utilized. The total costs of procuring and maintaining the equipment are shown by Category of testing and platform below:

Digestion/Extraction

- EZ1: $63,000 to purchase and $5,570 annual maintenance
- EZ2: $61,250 to purchase (x2 instruments = $122,500) and $6,774 to maintain; 2 instruments for $13,548 annual maintenance
- Versa 1100: $85,000 to purchase and $12,000 annual maintenance

Liquid Handler

- Qiagility: $33,100 to purchase (x3 instruments = $99,300) and $6,492 to maintain; 3 instruments for $19,476 annual maintenance
- Hamilton STARlet: $108,000 to purchase (x2 instruments = $216,000) and $14,339 annual maintenance ($11,213 for full year for 1 instrument and $3,126 prorated for the 2nd instrument)

DNA Quantitation

- QuantStudio 5: $57,000 to purchase (x2 instruments = $114,000) and $7,530 to maintain; 2 instruments for $15,060 annual maintenance

DNA Normalization / Amplification

SpeedVac: $4,000 to purchase, no maintenance
ProFlex Thermalcyclers: $14,000 to purchase (x2 instruments = $28,000), no maintenance

DNA Typing

3500: $135,000 to purchase, $13,900 annual maintenance

DNA Interpretation

STRmix: $66,000 to upgrade, $24,970 annual maintenance
FaSTR: $37,000 to purchase, $8,750 annual maintenance
ArmedExpert: $15,000 to purchase, no maintenance

The cost of testing reagents/kits was approximately $210,000, however, this does not include consumables such as scalpels, masks, gloves, plastics, slides nor serological test kits.

Total purchase cost (born over several years): $1,110,800
Total maintenance cost, 2025: $127,613

Total testing cost reagents/kits, 2025: $210,000
Estimate of consumables: $150,000

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

The 2024-approved Surveillance Impact Report (SIR) and Biometric Technology Use Policy (SUP) were reviewed. There are no requests to substantively modify the SIR outside of placing the annual cost updates into an Appendix.

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, Criminalistics Laboratory Manager, at opdcrimelab@oaklandca.gov.

Reviewed by:
Omar Dara-Quiroz, A/Deputy Chief
OPD, Bureau of Investigations

Tracey Jones, Police Services Manager
OPD, BRM, Research and Planning

Prepared by:
Bonnie Cheng, A/Crime Lab Manager
Forensic Biology Unit Supervisor
OPD, Criminalistics Laboratory

Rebecca Jewett, Forensic Biology Unit Technical Leader
OPD, Criminalistics Laboratory

CITY OF OAKLAND

TO: PAC

FROM: Omar Daza-Quiroz, Acting Deputy Chief
OPD, Bureau of Investigations

SUBJECT: Automated License Plate Reader (ALPR) Annual Report

DATE: APRIL 17, 2026

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. An updated version of I-12 is attached to this report (Attachment B) for review and request of approval from the PAC.

2025 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.

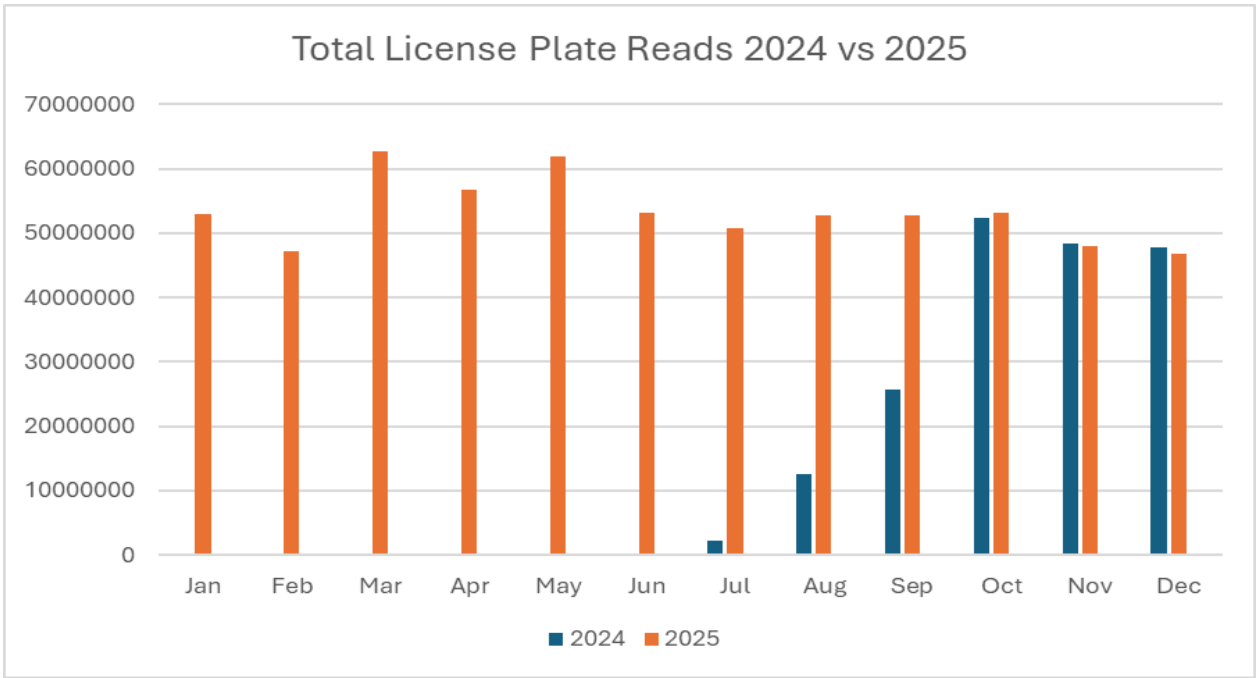
1. To assist in active criminal investigations which have just occurred. The OPD will utilize ALPR to search where a crime just occurred. OPD personnel can enter a vehicle's license plate (if one was provided) or enter a partial license plate (if one was provided) or search a camera location (if no license 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 are 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 in 2025 and shows in comparison to 2024. 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. 2025 was the first full year OPD utilized Flock cameras and there was a total of 638,747,333 license plate reads by Flock cameras assigned to OPD in the City of Oakland.

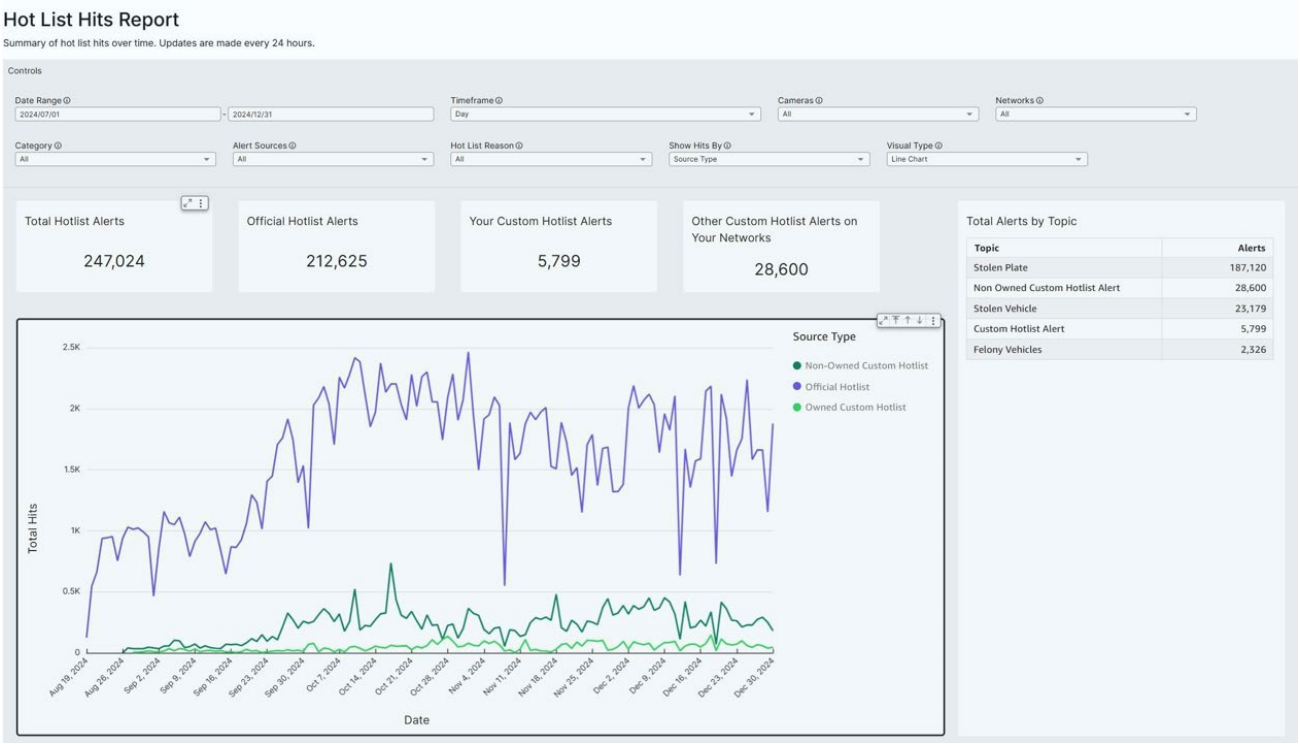
Figure A



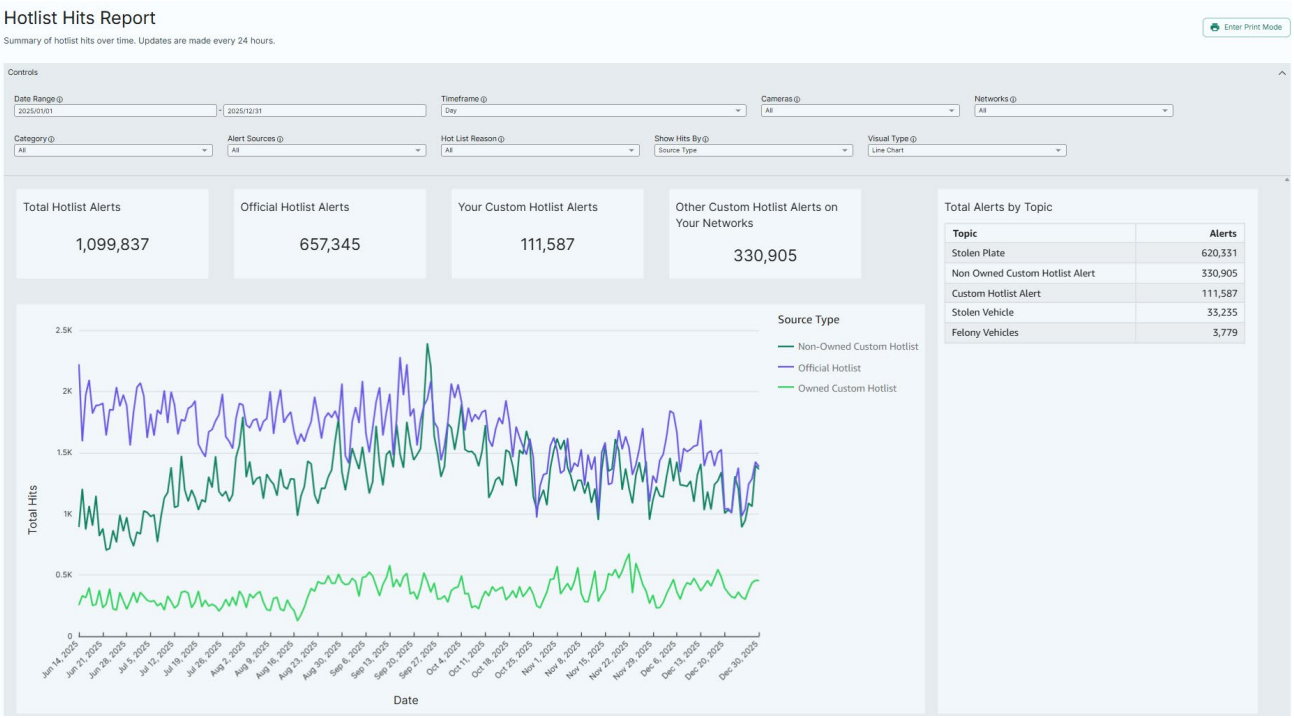
For hotlists, there was a total of 1,099,837 vs 247,024 (2024) hotlist alerts in 2025, with 657,345 vs 212,625 (2024) alerting from an official hotlist, 111,587 vs. 5,799 (2024) alerting from an OPD custom hotlist, and 330,905 vs 28,600 (2024) custom hot list alerts created by other departments that utilized OPDs Flock images. As a reminder 2024 year-end stats were from July through December 31, 2024 and 2025 stats were from January 1st, 2025 – December 31st, 2025.his data is visualized in ***Figure B*** below.

Figure B.

2024 Data



2025 Data



In both 2024 and 2025, OPD's top five alert types were stolen plate (620,331 vs. 187,129 (2024), non-owned custom hotlist alert, which is an alert created by another agency using Flock and shared with OPD 528,600 vs.330,905 (2024), stolen vehicle 33,235 vs.23,179 (2024), an alert from an OPD custom hotlist (111,587 vs. 75,799 (2024) and felony vehicles 92,326 vs 3,779 (2024).

Due to the overwhelming number of alerts for “stolen vehicle” and “stolen plate” compared to the other types of alerts and the staffing and resources within the department, alerts for these types remain deactivated. Flock is still working to enable a feature to allow selective notification of these types of alerts during lower call volume hours, but at this time no such feature exists. At this time 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). In 2024, with the rollout of Flock, a multitude of officers within OPD were 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. OPD has continued to increase the number of trained officers with access to the system. At this time approximately 350 members of OPD have received the required training.

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. OPD does not have access to any agency's success stories, as such outside agencies do not have access to OPD’s success stories.

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:

- OPD responded to a Flock alert for a felony shooting vehicle responsible for a shooting in the City of Berkeley. Officers were able to locate the vehicle and initiated a vehicle pursuit. The OPD Helicopter (Argus) took over the pursuit and continued to follow the vehicle throughout Oakland. Two subjects were eventually detained after exiting the vehicle. A search of the suspect vehicle was conducted, and (3) three firearms and a large quantity of ammunition was located in the vehicle. Both subjects were arrested for multiple felony charges as well as outstanding felony warrants.

- OPD officers responded to a Flock alert for a Richmond Carjacking vehicle located in Oakland. Due to the real time alerting within Flock OPD officers along with Richmond PD officers were able to respond to the area and were able to safely apprehend the driver of the vehicle without incident.

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 2024/2025:

2024 Shared Agencies	2025 Shared Agencies
Alameda (City) Police Department	Fremont CA PD
Alameda County Sheriff's Office	Santa Clara CA PD
Alameda County Sheriff's Office-Dublin Police	Mountain View CA PD (Santa Clara County)
Burlingame Police Department	Pleasanton CA PD
CA State Parks	Hillsborough CA PD
Cal Fire - Law Enforcement	California State Parks
California Highway Patrol	Brisbane CA PD
Campbell PD	San Mateo County CA SO
Colma Police Department	San Joaquin County CA SO
Concord (CA) PD	Daly City CA PD
Daly City Police Department	Redwood City CA PD
Danville PD	Contra Costa County CA SO
Dixon Police Department	Concord CA PD
East Bay Regional Park District Police	Newark CA PD
East Palo Alto Police Department	Cal Fire
El Cerrito PD	Hayward CA PD
Emeryville Police Department	Piedmont CA PD
Fairfield California Police Department	Solano County CA SO
Fremont Police Department	El Cerrito CA PD
Hayward Police Department	Vallejo CA PD
Livermore Police Department	Burlingame CA PD
Los Altos PD	Danville CA PD
Marin County Sheriff's Office	Colma CA PD
Mountain View Police Department	Brentwood CA PD
Napa County Sheriff's Office	San Francisco CA PD
Northern California Regional Intelligence Center (NCRIC)	Novato CA PD
Newark (CA) Police Department	East Palo Alto CA PD
Novato PD	Emeryville CA PD
Piedmont Police Department	Palo Alto CA PD
Pleasant Hill Police Department	Livermore CA PD
Pleasanton Police Department	Alameda County CA SO
Redwood City PD	East Bay Parks CA PD
Richmond (Calif) Police Department	Campbell CA PD
Sacramento County Sheriff's Office	Sonoma County CA SO
San Bruno Police Department	Milpitas CA PD
San Francisco Police Department	San Jose CA PD
San Leandro Police Department	California Highway Patrol
San Mateo County Sheriff's Office	University of California, Berkeley
	Union City CA PD
	Pleasant Hill CA PD
	San Leandro CA PD
	West Sacramento CA PD
	Santa Rosa CA PD
	San Bruno CA PD
	Sausalito CA PD
	San Mateo CA PD
	Fairfield CA PD
	San Ramon CA PD

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

Dublin CA PD (ACSO)
Berkeley CA PD
Pacifica CA PD
Richmond CA PD
Belmont CA PD
San Francisco District Attorney CA
Sacramento CA DA
Petaluma CA PD
Capitola CA PD
Rohnert Park Department of Public Safety (CA)
Sacramento CA PD
Marin County CA SO
Moraga CA PD
Central Marin CA PD
Town of Los Gatos CA
Solano County DA CA
Sunnyvale CA PD
Los Altos CA PD
Alameda CA PD
Walnut Creek CA PD

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

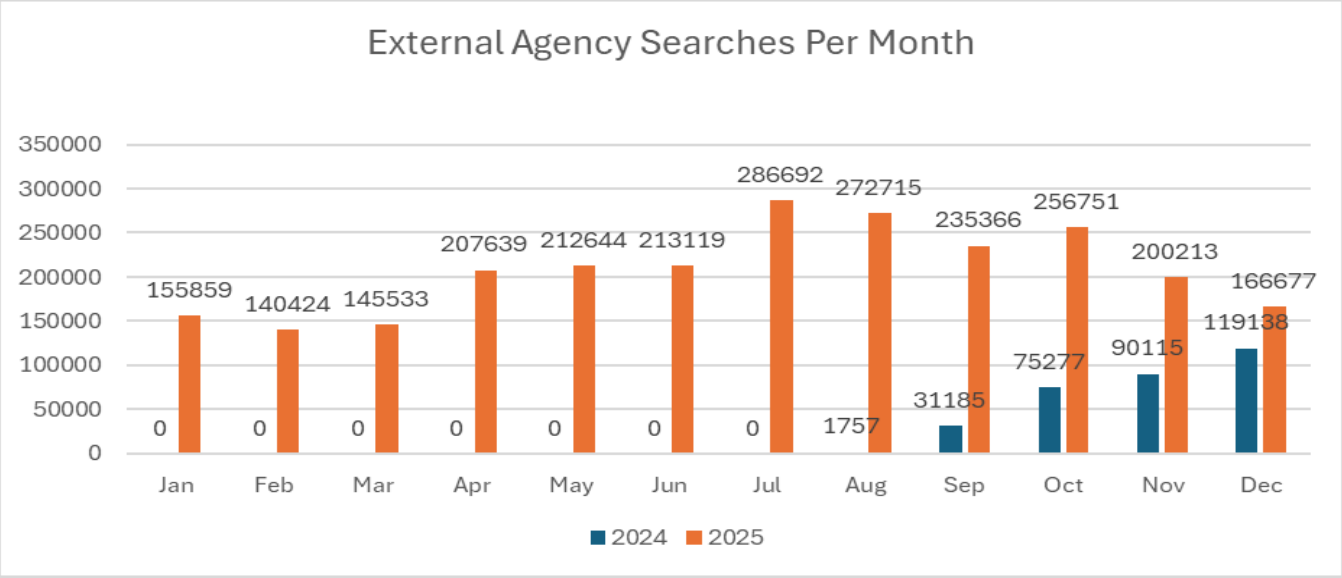
- Do you agree to the following: I confirm, on behalf of my agency or department, in compliance with state law, OPDs ALPR data SHALL NOT be used or shared with other agencies for the purpose of pursuing criminal charges or civil enforcement against individuals for obtaining, providing, or supporting 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 2025 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.

Currently, in April 2026, the OPD created a new sharing agreement which has been reviewed and approved by the City Attorney's Office, which provides further restrictions in accordance with recommendations from council codified under CMS 91008. (Attachment C). OPD is currently in the process of distributing this form to agencies which have previously been granted access to OPD data.

Figure C shows the number of searches that have been done against our data, month over month, in 2024 vs. 2025. Again, Flock came online in July 2024, and no external searches were conducted prior to that time. 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. <u>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</u>:

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 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. These cameras are currently the only source of data, that are OPD assigned, feeding into the Flock system.:

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

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

[1] City of Oakland | Oakland Police Areas

- Area 4: 55
- Area 5: 51
- Area 6: 60

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 was made aware of the below Opposing and Supporting comments as it relates to the technology. The below chart shows the categories of such comments.

Comments Opposing	**Comments Supporting**
Risk to vulnerable communities & concerns for Sanctuary Law violations • Fear Flock ALPR data will be used by ICE or other agencies to target immigrants, undermining Oakland's Sanctuary policies and increasing community fear.	Crime deterrence and reduction • Belief that Flock cameras are contributing to significant drops in robberies and helping deter repeat offenders.
Lack of safeguards, oversight, and accountability • Concerns about insufficient data protections, weak enforcement mechanisms, lack of civilian oversight, and inadequate penalties for vendor violations.	Improved investigative capacity • Cameras provide valuable leads for solving crimes, recovering stolen vehicles, and interrupting crime patterns—especially important given staffing shortages.
Data sharing & privacy concerns • Worry that collected data could be accessed by non-Californian state entities	Privacy-conscious design • System does not use facial recognition or collect demographic data, with policies in place to limit misuse and regulate data sharing.

Comparison to alternative approach • Citing Richmond's approach as a better model.	Legal safeguards in place • State law restricts sharing ALPR data with federal agencies, intended to prevent use for immigration enforcement.
	No strong alternative tools • Concern that without Flock OPD would have a weakened ability to maintain public safety due to limited staffing and resources.

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 2025 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. The internal organization records were split into two tabs, Database Queries Jan-May and Jun-Dec, which houses all investigative queries performed in 2025.

The audit information begins on the tab labeled Database Queries Audit. This audit was done by doing a randomized audit of 500 records. Originally, 500 records were selected, four of these returned as "DAYTIME SEARCH FOR BEST RESULTS" which is a system-generated phrase by Flock, when a user runs a normal plate search and then clicks "best daytime image". The platform automatically runs a secondary search to pull the clearest daytime image. The automatic follow-up query is what gets logged. These entries do not represent separate, independent searches. The original search data is maintained in the audit for full compliance. For that reason, these searches were omitted from the statistics. 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. In December 2024 Flock updated the search format to a dropdown format which removed the ability to enter Freeform text for offense type. OPD now has a specific list of search reasons which must be selected by the user prior to conducting a query within the system. A second box requires the user to enter an associated LOP or RD number. The third box is another drop down box which has a list of Penal Code, California Vehicle Code or Oakland Municipal Codes related to the search reason first selected. Each of these boxes must be filled out prior to conducting a search against the system.

The full list of currently allowable search reasons is contained in attachment D.

Based on this criteria, 496 records were evaluated. Below are the results of the audit, which show that OPD had a report or incident number included in 98% of the audited files and had the crime included in 100% of the audited files.

Total RD/LP "Yes"	488
Total RD/LP "No"	8
Total Type of Crime "Yes"	496
Total Type of Crime "No"	0

RD/LP included - Audit Pass Rate	98%
Crime Included - Audit Pass Rate	100%

OPD has continued to conduct routine audits of searches conducted by OPD personnel to ensure compliance with DGO I-12. Emails are sent out periodically to update individuals of policy 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 353 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:

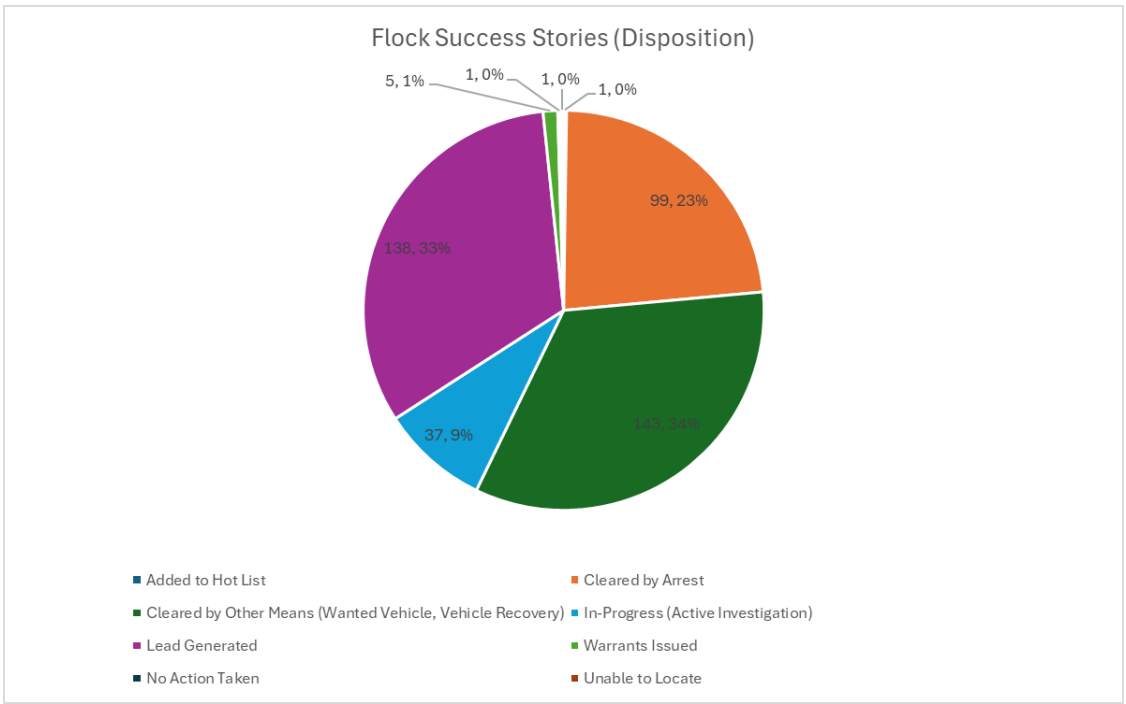
The Oakland Police Department confirmed via the Flock Security Portal Statement of Compliance which confirmed that Flock did not suffer any security breaches as it relates to their infrastructure.

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

OPD continues to 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 2025 Annual Report Data spreadsheet.

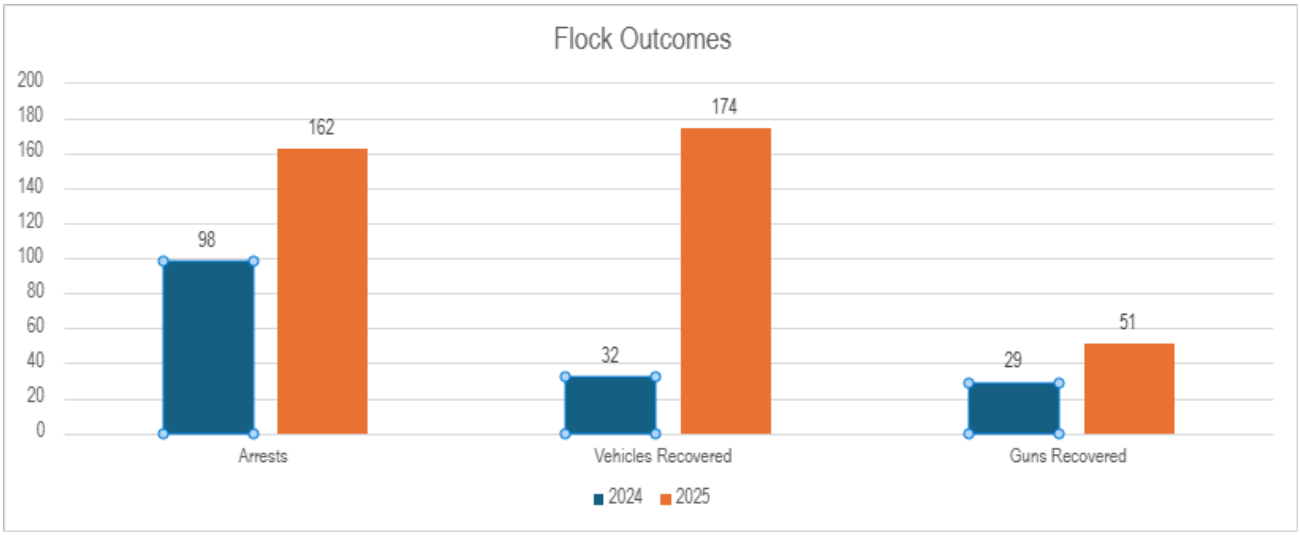
As shown in ***Figure E*** below, OPD logged a total of 425 vs 240 (2024) success stories in Flock from January 2025 through December 2025. Based on these actions, OPD was able to generate 425 vs.112 (2024) leads, 99 vs 55 (2024) were cleared by arrests,143 vs 34 (2024) were cleared by other means such as vehicle recovery, 37 vs 31 (2024) are in-progress investigations, and 5 vs 8 (2024) warrants were issued.

Figure E



Summarization of all outcomes shows that OPD made 162 vs 98 (2024) arrests, recovered 174 vs 32 (2024) vehicles, and recovered 51 vs 29 (2024) 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***. Areas of note include robbery and robbery +, which had a combined 35 arrests, 11 vehicles recovered and 5 firearms recovered. Flock also assisted in the arrest of 22 carjacking suspects, 11 human trafficking suspects and 16 suspects related to firearms offenses.

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.

Offense	**Arrests**	**Vehicles Recovered**	**Guns Recovered**
Aggravated Assault	12	1	4
Burglary	7	0	0
Carjacking	22	8	4
Felony Evading	12	0	0
Motor Vehicle Theft	4	0	0
Murder/Manslaughter	19	0	16
Human Trafficking	11	0	4
Rape	4	0	0
Robbery	20	6	4
Robbery +	15	5	1
Weapons Possession	16	1	12
Other	20	4	5
Total	**162**	**25**	**50**

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

- RD# 25-048437 Flock technology was used to identify an armed robbery suspect vehicle. Vehicle had switched plate at the time. Flock technology was used to successfully identify

true identity of vehicle based on previous hits, leading to the direct identification of one of the armed robbery suspects and a warrant of arrest.

- RD # 25-009125 OPD Air Support Unit officers were on a routine patrol flight in OPD Helicopter "Argus" when they received a flock alert for a robbery vehicle through the flock mobile app. Air Support Unit officers were able to spot the vehicle travelling E/B along International Blvd which coincided with the alerts and coordinated with ground units for a takedown. The vehicle fled and with the assistance of ACSO Air, ACSO ground units, and ACCRAT, 3 subjects were detained in the city of Hayward with the driver being taken into custody. OPD units then responded to Hayward to take over the investigation. Driver had an outstanding warrant for 211.

- Throughout 2025 over 140 sideshow related vehicles were identified and located with the assistance of Flock Technology. Seizure warrants were authored for these vehicles which resulted in a court ordered tow along with a 30 day hold for each vehicle.

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

OPD received sixteen (16) Public Records Requests (PRRs) in 2025 that were related to ALPR technology, eleven are responded to and five await completion of our response. The requests are summarized below:

- 25-6339 – which asked for network and organizational audits (complete)
- 25-8866 – Requesting contracts, policies, documents, emails related to acquisition and implementation of Flock cameras along with network and organization audits (Fulfillment pending).
- 25-9053 – which asked for contract data (complete)
- 25-9414 – which asked for data related to hotlists maintained within Flock (complete)
- 25-9415 – which asked for network and organizational audits as well as network share agreements (Fulfillment pending).
- 25-9970 – which requested all camera locations (complete).
- 25-10951 – which requested network and organizational audits (Fulfillment pending)
- 25-11188 – which asked for data related to success stories and incidents which utilized Flock cameras (Fulfillment pending).
- 25-11890 – which asked for images and data from a specific timeframe (advised no responsive records).
- 25-11903 – which asked for information regarding Flock Camera at Broadmoor and San Leandro (complete)
- 25-12073 – which asked for images from search data (advised no responsive records).
- 25-12152 – which asked for data related to a stolen vehicle (advised unable to fulfill request).
- 25-12208 – which asked for information regarding camera functionality (advised no responsive records).
  25-12599 – which asked for information regarding all OPD users who have had Flock access (complete).

- 25-12811 - which asked for network and organizational audits (Fulfillment pending)
- 25-12820 – which asked for data related to Flock usage and encampments (advised no responsive records).

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:

On October 13, 2023, Oakland City Council adopted Resolution 89952 approving OPD and authorizing the City Administrator to enter into a $1,200,000 in state loan funding to purchase ALPR Technology and Services. There was a three-year agreement to Flock Safety at a cost of $1,077,500 for the first year, $900,000 for year two and year three for a total amount not to exceed $2,877,500.

The estimated cost for Flock for the first year is approximately $1,200,000, 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 $900,000 and the third will be $900,000 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 drafted an amended Use Policy for ALPR (attachment B). The OPD Use Policy is documented under Departmental General Order (DGO) I-12. I-12 has been amended to expand the allowable uses to better align with the council's directive towards I-32.1 which was documented in Oakland City Council Resolution 91008 C.M.S.

The primary changes to DGO I-12 include:
1) A comprehensive list of allowable search reasons within the ALPR system to include illegal dumping.
2) Specific prohibitions of the use of OPD ALPR data for gender affirming, reproductive health, and immigration related activities.
3) Implementation of a two-key approval process for new sharing agreements with outside agencies to allow access to OPD ALPR Data.
4) Amended Sharing Agreement Form, which affirms the above as well as requires outside agencies to affirm that they will comply with OPD Policy for searches as well as SB 34 and SB 54. This document has been produced in conjunction with the City Attorney's Office.

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, Lt Omar Daza-Quiroz, at odaza-quiroz@oaklandca.gov, or Lt. Gabriel Urquiza at GUrquiza-Leibin@oaklandca.gov

Respectfully submitted,

James P. Beere, Interim Chief of Police
OPD, Office of the Chief of Police

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

A/DC. Omar Daza-Quiroz
OPD, Bureau of Investigations

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

Ofc. Brandon Mart
OPD, Information Technology & Fleet

Attachments (4):
A: 3rd Party Data Sharing (link)
B: Update DGO I-12
C: Sharing Agreement
D: Allowable search reasons

DEPARTMENTAL GENERAL ORDER

I-12: AUTOMATED LICENSE PLATE READERS

Effective Date: 2 April 2026
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.

Definitions

(a) **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.

(b) **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.

(c) **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.

A. 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.

B. 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:

1. 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.
2. 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.

C. Authorized Uses: *The specific uses that are authorized, and the rules and processes required prior to such use.*

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.

2. Authorized Use

(A) **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.

(1) **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:

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

(B) **Database Investigative Queries**: Historical searches of scanned plates are permissible for crimes/incidents including illegal dumping, theft, vehicle theft, human trafficking, reckless driving, sideshow/takeovers, felony evasion, burglaries, robberies, firearms offenses, shootings, and homicides. Accessing the data shall be based on a standard of Reasonable Suspicion or greater. See attachment **A** for full list of allowable search reasons.

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.

1. 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.
2. 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:

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

3. Restrictions on Use

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:

(1) 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.

(2) Harassment or Intimidation: It is a violation of this Policy to use the ALPR system to harass and/or intimidate any individual or group.

(3) 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.

(4) 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.

(5) 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.

(6) 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, or gender affirming care in California to ensure that medical rights of residents of and visitors to Oakland, a Sanctuary City, remain intact.

(7) Immigration: No data from ALPR shall be used or shared with local or state agencies for the purpose of federal immigration enforcement.

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).

a. No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.

b. No ALPR operator may access department, state or federal data unless otherwise authorized/designated to do so pursuant to Section E "Data Access" below.

c. 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.

D. 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.

E. 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.

F. 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.

G. 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.

H. 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.

I. 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.
- **Oakland Public Works (OPW)** and/or the **City Attorney's Office** for the purpose of evaluating and supporting the enforcement of the City's **administrative and civil penalties related to illegal dumping**.
- 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.

When there is no legal obligation to provide the requested data, requests to access the 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, unless an approved sharing agreement allows continual access. (See attachment B for current sharing agreement)

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.

Two-Key Approval System-barring exigent circumstances, no sharing relationship, data-access grant, or modification of sharing permissions may occur unless approved through a two-key system consisting of:

a) The Chief Privacy Officer in the City Administrator's Office; and

b) Oakland Police Department's Information Technology Director;

c) In the event of an exigent circumstance the City Administrator's Chief Privacy Officer will be informed 72 hours after the exigency ends, and should be reported out to the Privacy Commission at the next meeting.

J. 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

K. ***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.

Audits shall also be conducted annually of searches conducted by outside agency against OPD ALPR data. The size of these audits shall be large enough to provide a stat.

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

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.
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.
3. **ALPR Coordinator:** The title of the official custodian of the ALPR system

is the ALPR Coordinator.

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.
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,

James P. Beere
Interim Chief of Police Date: _____

Attachment A

- Animal Offenses (cruelty/neglect)
- Arson
- Assault/Battery Offenses
- Assault/Battery Offenses (Domestic)
- Burglary/Breaking & Entering
- Child Abuse/Neglect
- Criminal Motor Vehicle Offense (incl. Road Rage/Reckless)
- Destruction/Damage/Vandalism of Property
- Driving Under the Influence (DUI/DWI/OWI/OVI)
- Drugs/Narcotics
- Hit and Run/Car Accident
- Homicide/Death Investigation
- Human Trafficking
- Illegal Dumping/Littering
- Indecent Exposure/Lewd
- Kidnapping/Abduction
- Larceny/Theft Offenses
- Material Witness
- Missing/Endangered Person/Runaway
- Motor Vehicle Theft/Stolen
- Obstructing the Police (Fleeing/Eluding)
- Pornography/Obscene Material
- Property Recovery (Civil Enforcement)
- Prostitution
- Robbery
- Sex Offenses
- Stalking
- Stolen Property Offenses
- Terrorism/Terroristic Threats
- Threats/Harassment
- Wanted Person (Arrest Warrant/Fugitive)
- Weapons Offense (Guns/Shots Fired)
- Welfare Check

1. Name of the law enforcement organization requesting access.
2. Contact information of the person requesting access on behalf of the named organization (Please include name, email, address, phone number, and, if applicable, serial number).
3. Contact information for person in charge of ALPR data at the named organization if different from above (Please include, name, email address, phone number, and, if applicable, serial number).
4. I confirm on behalf of my organization, that the organization is a "public agency" within the definition of Cal. Civil Code, §1798.90.5(f).
5. I confirm, on behalf of my organization, that my organization will only access OPD's ALPR data when it has a right to know and a need to know ALPR information. The right to know is the legal authority.
6. I confirm, on behalf of my organization, that any time we access OPD's ALPR data, we will document the applicable statutory violation (e.g., Penal Code or Vehicle Code section), and my organization's
7. I confirm, on behalf of my organization, that any access by our organization to OPD's ALPR data will comply with authorized uses as outlined in OPD DGO I-12
8. I confirm, on behalf of my agency or department, that any access by our organization to OPD's ALPR data will be in compliance with state law including SB 34 (codified in Cal. Civil Code, § 1798.90.5 e
9. I confirm, on behalf of my organization, that incompliance with state law OPD's ALPR data shall not and will not be used or shared with other agencies for the purpose of pursuing criminal charges or c
10. I confirm, on behalf of my organization, that OPD's ALPR data shall not and will not be used or shared with other agencies for the purpose of federal immigration enforcement.

Approved offense types in Flock

- Animal Offenses (cruelty/neglect)
- Arson
- Assault/Battery Offenses
- Assault/Battery Offenses (Domestic)
- Burglary/Breaking & Entering
- Child Abuse/Neglect
- Criminal Motor Vehicle Offense (incl. Road Rage/Reckless)
- Destruction/Damage/Vandalism of Property
- Driving Under the Influence (DUI/DWI/OWI/OVI)
- Drugs/Narcotics
- Hit and Run/Car Accident
- Homicide/Death Investigation
- Human Trafficking
- Illegal Dumping/Littering
- Indecent Exposure/Lewd
- Kidnapping/Abduction
- Larceny/Theft Offenses
- Material Witness
- Missing/Endangered Person/Runaway
- Motor Vehicle Theft/Stolen
- Obstructing the Police (Fleeing/Eluding)
- Pornography/Obscene Material
- Property Recovery (Civil Enforcement)
- Prostitution
- Robbery

- Sex Offenses
- Stalking
- Stolen Property Offenses
- Terrorism/Terroristic Threats
- Threats/Harassment
- Wanted Person (Arrest Warrant/Fugitive)
- Weapons Offense (Guns/Shots Fired)
- Welfare Check

CITY OF OAKLAND

MEMORANDUM

TO: James Beere,
Interim Chief of Police

FROM: Jonathan Vanerwegen, Sergeant,
SOD, Air Support Unit

SUBJECT: Forward Looking Infrared (FLIR)-2025 Annual Report

DATE: APRIL 2026

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.

The PAC recommended adoption of the OPD Department General Order (DGO) I-29: "Aircraft Mounted Camera (AMC) use policy" at their September 7, 2023 meeting; the report was presented to the City Council on December 5, 2023 and adopted by the City Council via Resolution No. 89995 C.M.S. DGO I-29 requires that OPD provide an annual report to the Chief of Police, the Privacy Advisory Commission (PAC), and the City Council.

2025 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 technology was not used during the past year. No data was recorded or retained during the past year in accordance with DGO I-29.

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):

No outside agencies received data from the use of the surveillance technology.

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 two patrol helicopters which are equipped with a FLIR 8500 camera. These cameras have been utilized by those helicopters for the past decade. The cameras are able to obtain live video and record video concurrently. These recordings are subject to the restrictions and retention of DGO I-29.

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

The camera was not used during the past year.

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.

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:

All officers assigned to the Air Support Unit who have access to the technology were provided training on the requirements and policy associated with DGO I-29. Because no recordings were made during the 2025 year, no possible access to stored data by unauthorized persons is possible.

A compliance check of the activations during the previous year show that no improper use of the AMC was found to have occurred.

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 unauthorized access during the year of 2025.

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

The cameras were not used during the last year. The policy was primarily developed for the implementation of a new camera on a fixed wing aircraft that has not been purchased.

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

There have been no PRA requests regarding the Air Unit Cameras since the approval of DGO I-29 in 2023.

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 equipment is owned outright by the department/city and has no ongoing operating cost other than the cost to operate the helicopters themselves. The cameras are no longer serviced by the manufacturer and any issues that may arise in the future regarding their functionality will likely require replacement at a cost TBD.

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 Jonathan Vanerwegen, Sergeant, OPD, Air Support Unit, at jvanerwegen@oaklandca.gov

Reviewed by,
Eriberto Perez-Angeles, Acting Captain
OPD, Special Operations Division

Tracey Jones, Police Services Manager
OPD, Research and Planning Unit

Prepared by:
Jonathan Vanerwegen, Sergeant

DEPARTMENTAL GENERAL ORDER

I-12: AUTOMATED LICENSE PLATE READERS

Effective Date: 2 April 2026
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.

Definitions

(a) **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.

(b) **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.

(c) **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.

A. 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.

B. 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:

1. 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.
2. 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.

C. Authorized Uses: *The specific uses that are authorized, and the rules and processes required prior to such use.*

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.

2. Authorized Use

(A) **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.

(1) **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:

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

(B) **Database Investigative Queries**: Historical searches of scanned plates are permissible for crimes/incidents including illegal dumping, theft, vehicle theft, human trafficking, reckless driving, sideshow/takeovers, felony evasion, burglaries, robberies, firearms offenses, shootings, and homicides. Accessing the data shall be based on a standard of Reasonable Suspicion or greater. See attachment **A** for full list of allowable search reasons.

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.

1. 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.
2. 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:

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

3. Restrictions on Use

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:

(1) 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.

(2) Harassment or Intimidation: It is a violation of this Policy to use the ALPR system to harass and/or intimidate any individual or group.

(3) 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.

(4) 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.

(5) 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.

(6) 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, or gender affirming care in California to ensure that medical rights of residents of and visitors to Oakland, a Sanctuary City, remain intact.

(7) Immigration: No data from ALPR shall be used or shared with local or state agencies for the purpose of federal immigration enforcement.

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).

a. No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.

b. No ALPR operator may access department, state or federal data unless otherwise authorized/designated to do so pursuant to Section E "Data Access" below.

c. 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.

D. 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.

E. 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.

F. 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.

G. 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.

H. 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.

I. 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.
- **Oakland Public Works (OPW)** and/or the **City Attorney's Office** for the purpose of evaluating and supporting the enforcement of the City's **administrative and civil penalties related to illegal dumping**.
- 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.

When there is no legal obligation to provide the requested data, requests to access the 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, unless an approved sharing agreement allows continual access. (See attachment B for current sharing agreement)

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.

Two-Key Approval System-barring exigent circumstances, no sharing relationship, data-access grant, or modification of sharing permissions may occur unless approved through a two-key system consisting of:

a) The Chief Privacy Officer in the City Administrator's Office; and

b) Oakland Police Department's Information Technology Director;

c) In the event of an exigent circumstance the City Administrator's Chief Privacy Officer will be informed 72 hours after the exigency ends, and should be reported out to the Privacy Commission at the next meeting.

J. 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

K. ***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.

Audits shall also be conducted annually of searches conducted by outside agency against OPD ALPR data. The size of these audits shall be large enough to provide a stat.

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

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.
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.
3. **ALPR Coordinator:** The title of the official custodian of the ALPR system

is the ALPR Coordinator.

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.
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,

James P. Beere
Interim Chief of Police Date: _____

Attachment A

- Animal Offenses (cruelty/neglect)
- Arson
- Assault/Battery Offenses
- Assault/Battery Offenses (Domestic)
- Burglary/Breaking & Entering
- Child Abuse/Neglect
- Criminal Motor Vehicle Offense (incl. Road Rage/Reckless)
- Destruction/Damage/Vandalism of Property
- Driving Under the Influence (DUI/DWI/OWI/OVI)
- Drugs/Narcotics
- Hit and Run/Car Accident
- Homicide/Death Investigation
- Human Trafficking
- Illegal Dumping/Littering
- Indecent Exposure/Lewd
- Kidnapping/Abduction
- Larceny/Theft Offenses
- Material Witness
- Missing/Endangered Person/Runaway
- Motor Vehicle Theft/Stolen
- Obstructing the Police (Fleeing/Eluding)
- Pornography/Obscene Material
- Property Recovery (Civil Enforcement)
- Prostitution
- Robbery
- Sex Offenses
- Stalking
- Stolen Property Offenses
- Terrorism/Terroristic Threats
- Threats/Harassment
- Wanted Person (Arrest Warrant/Fugitive)
- Weapons Offense (Guns/Shots Fired)
- Welfare Check

CITY OF OAKLAND

MEMORANDUM

TO: PAC

FROM: Gabriel Urquiza, OPD
Real-Time Operations

SUBJECT: Live stream transmitter – 2025 Annual Report

DATE: May 2026

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.

Oakland Police Department (OPD) I-23: Live Stream Transmitter Use Policy governs OPD's use of Live Stream Transmitters; the policy was approved by the City Council on April 21, 2020 through Resolution No. 88099 C.M.S., as well as OMC 9.64.040, requires that OPD provide an annual report to the Chief of Police, the Privacy Advisory Commission (PAC), and the City Council. The information provided below is compliant with the annual report policy requirements of OMC 9.64.040 and DGO I-23.

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

   OPD did not used the livestream transmitter technology in 2025.

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):

   No data was collected with this technology in 2025 since it was not deployed.

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 t

specific location of such hardware; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to:

The transmitters are attached to handheld video cameras. These cameras are physically held by officers when in use.

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

The live stream transmitters were not deployed in 2025.

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.

OPD did not used the livestream transmitter technology in 2025.

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:

There was no usage of the technology in 2025.

- The technology was properly stored with the OPD Information Technology Unit (ITU).
- OPD is not aware of any policy violations from use of the live stream transmitters in 2025.

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:

OPD is not aware of any breaches or unauthorized access to this data in 2025.

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

N/A

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

There were no PRRs regarding this technology in 2025.

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:

$11,500 for cellular connectivity.

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

No requests for 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, Lt. Gabriel Urquiza, at gurquiza-leibin@oaklandca.gov.

Respectfully submitted,

Gabriel Urquiza
Lieutenant of Police
Real-Time Operations
OPD Ceasefire Section

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

Prepared by:
Gabriel Urquiza
Lieutenant of Police
Real-Time Operations
OPD Ceasefire Section

CITY OF OAKLAND

MEMORANDUM

TO: PAC

FROM: Omar Daza-Quiroz, Acting Deputy Chief
OPD, Bureau of Investigations

SUBJECT: Unmanned Aerial System (UAS or Drone) – 2025 Annual Report

DATE: April 2026

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.

The PAC voted unanimously to recommend City Council adoption of OPD's Departmental General Order (DGO) I-25: Unmanned Aerial System (UAS) Use Policy on May 14, 2020. The City Council adopted Resolution No. 88454 C.M.S. which approved OPD's DGO I-25. OMC 9.64.040 requires that, after City Council approval, OPD provide an annual report to the Chief of Police, the Privacy Advisory Commission (PAC), and the City Council.

A/DC Omar Daza-Quiroz is currently the UAS Program Coordinator and has been since 2022.

2025 Data Points

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 Unmanned Aerial System (UAS)"

An Unmanned Aerial System (UAS) is an unmanned aircraft of any type that is capable of sustaining directed flight, whether preprogrammed or remotely controlled (commonly referred to as an unmanned aerial vehicle (UAV) or drone, and all of the supporting or attached components designed for gathering information through imaging, recording, or any other means.

UAV are controlled from a remote-control unit (similar to a tablet computer). Wireless connectivity lets pilots view the UAV imagery from a birds-eye perspective. UAV pilots can leverage control unit applications to pre-program specific GPS coordinates and create an automated flight path for the drone. (This is mainly conducted for mapping purposes or known preflight destinations. OPD has not utilized this feature as it does not have mapping software. Similar to

previous years, OPD still does not have mapping software, but has utilized UAVs to assist in crime scene video documentation. If funding becomes available, OPD would consider and request mapping software to assist in crime scene documentation of large-scale crime scenes (e.g., homicides, shootings, fatal collisions.)

UAV have cameras so the UAS pilot can view the aerial perspective. UAS proposed for use by OPD, and any other outside law enforcement agency, use secure digital (SD) memory cards to record image and video data; SD cards can be removed from UAV after flights to input into a computer for evidence uploading.

Total deployments of UAS technology in previous years, to include 2025 as follows:

Year	Total UAS Deployments
2023	220
2024	126
2025	130
Total	476

In 2025 the OPD, with the assistance of outside law enforcement agencies, deployed UAS technology 131 (one hundred and thirty-one) times. This is an increase of 5 (five) deployments and missions from prior year 2024, which saw 126 (one hundred and twenty-six) deployments and missions. This is roughly a 41% reduction compared to 2023. OPD's UAS Program went live in March of 2022. Of the 131 deployments and missions in 2025, one (1) deployment and mission was conducted by Alameda County Sheriff's Office (ACSO); there were no other outside agencies which deployed or assisted OPD in UAS deployments within the City of Oakland in 2025. As stated in the 2023-2024 Annual Reports, at times ACSO, or neighboring agencies with similar UAS Programs, will offer their services prior to being requested[1], or at times OPD UAS pilots are not on duty, unavailable or have insufficient resources (UAS fleet or personnel) to properly deploy. However, all agencies will only deploy if requested or approved by an OPD commander and if policy requirements are met.

OPD Electronic Services Unit (ESU) created a spreadsheet in 2022 to track and monitor all UAS deployments, including outside agency deployments. In 2022, Lieutenant O. Daza-Quiroz sent a department wide email mandating all commanders who deploy UAS to author documentation, similar to the protocol for use of the Emergency Rescue / Armored Vehicles. The process allowed for appropriate documentation. In 2023, commanders distributed Military Equipment Utilization (MEU) notifications via email when any militarized equipment was utilized, which included UAS deployments from OPD or outside agencies. This made it easy to track any outside agency deployments that ESU was not on scene for. ESU was also directed to manually input their deployments into a Microsoft Teams Excel Spreadsheet in order to keep property documentation.

Table 1 below details OPD, ACSO, and other outside agencies deployments in 2025 and compares it to 2023-2024 deployments.

[1] ACSO has access to OPD radio channels and can monitor; ACSO personnel at times can respond to a call for service.

Table 1: 2025 OPD & Outside Agency UAS Deployments

Incident Type	2023	2024	2025	2025 Outside Agency
Mass casualty incidents	*0*	*0*	*0*	*0*
Disaster management	*0*	*0*	*2*	*0*
Missing or lost persons	*5*	*0*	*0*	*0*
Hazardous material releases	*0*	*0*	*0*	*0*
Sideshow events	*3*	*5*	*4*	*0*
Rescue operations	*3*	*0*	*0*	*0*
Training	*15*	*10*	*14*	*0*
Barricaded suspects	*49*	*22*	*26*	*1*
Hostage situations	*0*	*0*	*0*	*0*
Armed suicidal persons	*1*	*0*	*0*	*0*
Arrest of armed and/or dangerous persons	*70*	*47*	*48*	*0*
Scene documentation for evidentiary or investigation value	*3*	*2*	*3*	*0*
Operational pre-planning	*0*	*0*	*1*	*0*
Service of high-risk search and arrest warrants	*71*	*38*	*32*	*0*
Exigent circumstances	*0*	*0*	*0*	*0*
Total	***220***	***126***	***130***	***1***

There was one outside agency deployment that occurred within the City of Oakland and described below:

- 16Jun25 - 79th Ave & Alder Street - PC 211: OPD requested ACSO UAS to assist with locating four robbery suspects who fled from a vehicle on foot. CHP Air was overhead and advised of heat signature from a backyard in the area. OPD had located and detained one suspect prior to ACSO arrival. ACSO UAS was utilized to search the surrounding area but nothing of note was seen. Two other subjects surrendered to canine announcements. ACSO UAS conducted multiple flights in the area but did not locate any significant heat signatures or suspects.

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):

Outside Law Enforcement Agencies (ACSO) assisted in one (1) UAS deployments in Oakland in 2025. Because of this, the UAS aircraft that they used captured and stored data. If requested, these agencies provide OPD with the recordings and the outside agencies store the information in their logs per their respective policy requirements. No outside entity made any requests to OPD to share any of OPD's data acquired using OPDs UAS, nor did OPD share any data acquired through OPDs UAS with outside entities.

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 technology was never installed upon fixed objects.

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

Table 2 below details the Police Areas where UAS were deployed in 2023-2025.

Table 2: OPD UAS Deployment by Police Area

Deployment by Area	***Total Deployments in 2023***	***Total Deployments in 2024***	***Total Deployments in 2025***
Area 1	*39*	*24*	*18*
Area 2	*11*	*10*	*7*
Area 3	*30*	*13*	*17*
Area 4	*34*	*13*	*17*
Area 5	*39*	*22*	*28*
Area 6	*40*	*29*	*31*
*Outside City**	*26*	*15*	*13*
Total*	***219***	***126***	***131***

** Deployments outside the city consist of assistance provided by OPD UAS to local agencies or provided to assist OPD enforcement activities that took place outside the city of Oakland.*

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 was made aware of the below Opposing and Supporting comments as it relates to the technology. The below chart shows the categories of such comments. Staff was noticed of 2 messages Opposing and 1 message Supporting of the technology.

Comments Opposing	Comments Supporting
General opposition to drone surveillance	Support for Drone first-responder program

• Concern about expanding mass surveillance, including for addressing illegal dumping	
OPD use of Flock surveillance systems that connect privately-owned Ring doorbells, business cameras, and drones into one nationwide tracking network. • ICE and other federal agencies have confirmed they can access these databases for deportation investigations	Remote license plate readers, cameras, and drones, has already been deployed in key areas to aid law enforcement in deterring and investigating criminal activity. • These types of devices have demonstrated measurable success in other communities, providing real-time data to law enforcement, and helping prevent and solve crimes.

Table 3 below provides race data related to 2023-2025 UAS deployments.

Table 3: Race of Detainees Connected to OPD UAS Deployments in 2025

	Race – Female 2023	Race – Female 2024	Race – Female 2025	Race – Male 2023	Race – Male 2024	Race – Male 2025
Black	74	30	48	104	84	99
Hispanic	36	14	48	95	35	102
Asian	7	2	3	17	3	18
White	4	1	5	12	6	10
Other	10	3	6	17	7	2
Total	**131**	**50**	**110**	**245**	**135**	**231**

OPD will know the race of detainees connected to UAS deployments. However, the race of all individuals involved in many UAS deployments is not known (e.g., cases such as armed and dangerous or barricaded suspects, where no suspect is ever discovered or detained). There could also be UAS uses for missing persons where the person's identity is not entirely known nor discovered (there were zero deployments related to missing persons in 2025). The number of detainees in 2025 was higher than in 2024. There was an outlying incident where a shooting occurred at a warehouse hosting a party that led to most of the increase in detainees in 2025 (25-032736, 75 detainees). For this incident, 50 of the detainees were male Hispanics and 25 were female Hispanics, which contributed to a significant portion of the increase in the number of Hispanic detainees in 2025 relative to 2024. The number of deployments were similar in 2024 and 2025 with 126 and 131 deployments respectively.

F. <u>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</u>

file information

The OPD Electronic Services Unit (ESU) maintained a list of all UAS deployment logs for record and tracking purposes. This list was reviewed periodically for accuracy and for assessment of any policy violations. All OPD commanders, per policy, were directed to send communications to ESU for any UAS use – similar to OPD protocols for use of Emergency Rescue Vehicles (ERV) / Armored Suburban. No policy violations were found, and no corrective actions were warranted nor needed in 2025. There was also zero in 2023-2024.

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 unauthorized access during the year of 2025, similar to that of 2023-2024.

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

Similar to 2023-2024, in reviewing the 2025 data associated with UAS deployments it was apparent that the unit has been effective at achieving safer outcomes for members of the community, officers, and those we have contacted during investigations.

During this review period OPD had an increase in 4 deployments and/or missions from prior year, which totaled 131. Specific records were kept tracking the efficacy of those deployments with the following results:

- Since tracking began in 2022, subject location success rates started at 75%, dipped to 70% in 2023, then increased to 83% in 2024 before returning to 75% in 2025, indicating overall stable performance with a notable peak in 2024
- Again, similar to previous years, arrest or armed and/or dangerous persons, service of high-risk search and arrest warrants and barricaded suspects saw the highest deployments.
- UAS deployments continue to provide aerial views and interior clearance for police officers, which in turn help mitigate use of force and allow for quicker resolutions. It is this real-time intelligence that allows for negotiation when subjects are located hiding and allows for mitigated use of force incidents. Not all subjects are always hiding when a UAV is overhead or searching an interior dwelling. However, real time intelligence allows officers to understand the layout of the dwelling or have a clear understanding of subjects emerging from dwellings and surrendering. In 2023, 376 subjects were located by the UAS. In 2024, this number decreased to 185 subjects being located. 2025 saw an increase to 341, which is on par with 2023. It is important to note that not all subjects captured through UAV deployment cameras were arrested but it highlights the importance of real-time intelligence and providing additional technology to police officers.
- 80 firearms were recovered from the scenes where UAS were deployed. The firearms were either located during a search of the flight path a suspect took, observed being discarded by suspect(s) during surround and callouts in rear yards or located by officers during searches of areas.

- All police areas (Area 1 – Area 6) had UAS deployments. Similar to 2024, Areas 1, 5 and 6 the most deployments while Areas 2, 3 and 4 had the least number of deployments/missions.
- In 2024, we had 184 canine requests with 48 deployments (two of those resulting in bites). In 2025, the Canine Unit had 161 requests, 86 deployments, assisted with 34 surrenders without bites, and had no bites for the year. This is a 12.5% decrease in requests from the previous year. Although there were more deployments, there were no bites associated with those deployments compared to 2024.
- OPD also deployed UAS on two occasions for disaster management operations. In coordination with the Oakland Fire Department (OFD), OPD UAVs were deployed to support fire response and recovery efforts as follows:
    - July 4, 2025 – 4-Alarm Fire Response (54th Ave & E. 8th St): OPD UAVs were deployed during a large-scale structure fire involving both residential and commercial properties. Real-time aerial imagery and infrared capabilities enhanced situational awareness, allowing responders to identify fire "hot spots," coordinate evacuations, and support fire suppression efforts. This deployment contributed to the protection of at least one residence from ignition and facilitated the safe evacuation of nearby occupants, with no reported injuries to responding personnel.
    - July 8, 2025 – Post-Incident Fire Assessment: Following containment of the fire, OPD UAVs were deployed to assist OFD with disaster management and recovery operations. Aerial and thermal imaging provided real-time intelligence to identify residual heat zones and potential re-ignition risks, improving operational safety and efficiency by reducing the need for personnel to enter structurally compromised areas.

As previously discussed in 2023-2024 annual reports, the number of deployments were the highest for persons who were considered armed and/or dangerous. 2025 was no different with these criteria being the number one deployment reason and seeing 48 deployments. Because of the ability to deploy UAS, responding emergency personnel were better able to create an environment of de-escalation. Absent the UAS, officers would typically resort to calling out the Entry Team, deploying a canine, or physically clearing the area with a search team for the subject(s). All these options have potential for chance encounters resulting in the possibility of force escalation. These options decrease safety for everyone involved to include the community, subjects being searched for, and the officers.

The number of deployments in each category were similar to that of 2024, which saw a similar total number of deployments across the board. A shortcoming can be the lack of usage for missing persons, sideshow, and crime scene documentation. ESU has advised Watch Commanders that UAS can be requested during missing person search, especially during at risk missing persons. Additionally, there existed more than four incidents of sideshow throughout the city of Oakland in all of 2025 and Commanders also understand that UAS can be deployed for such incidents. As far as criminal follow-up investigations as they relate to homicides, shootings and fatal hit and run collisions, investigators have been advised to reach out to their respective commanders if they believe the deployment of a UAV can assist in video recording of the scene through aerial view.

A sample below outlines just a few of the successful UAS deployments that provided officers with increased safety and conditions for de-escalation:

1. *Date: 28FEB25*
   RD: 25-008621
   Location: 1321 Peralta St, Oakland CA
   Summary: Patrol officers located and attempted to detain a warrant suspect. The suspect fled from officers, ran into an apartment building. Containment of the area was quickly set up. Intel developed that the suspect was possibly armed with a firearm. ESU/UAV was requested to assist with the search and to arrest of the suspect. An exterior drone was deployed to check the roof of the building. The suspect was taken into custody, and a firearm was recovered from the roof.

   This incident highlights the use of the drone to quickly gather visual intelligence in areas where sending officers may be unsafe. The use of the drone is also used as a de-escalation tactic to mitigate the use of force and chance encounter with the suspect. The drone located the suspect to provide real time updates and visual intelligence of the suspect's location and actions so that a tactical plan can be developed to detain and apprehend the suspect.

2. *Date: 04MAR25*
   RD# 25-010160
   Location: 1925 17th Ave, Oakland CA
   Summary: SRS West executed a search warrant of an illegal gambling shack at 1925 17th Ave. ESU/UAVs were requested and utilized to provide overwatch during the surround and call out of the property in the event subjects started to flee from the area and/or discard evidentiary items/weapons.

   An interior drone was utilized to locate several subjects who were barricaded and hiding within the attic and the illegal establishment. Pole camera was utilized to clear the inside of the property in hard-to-reach areas that may have been unsafe to send officers. At the conclusion of this incident, a total of seven individuals were detained and evidence including a firearm was recovered.

   This incident highlights the use of the drone to provide overwatch for ground units to enhance their safety from suspects by providing real time visual intelligence. Interior drones were imperative in locating subjects who were evading and hiding from police detention and contact. By locating these subjects who were hiding from officers, tactical plans were developed to safely take the subjects into police detention/custody.

3. *Date: 19APR25*
   RD: 25-0173318
   Location: 9850 Holly St, Oakland CA
   Summary: Patrol officers responded to a ShotSpotter activation. When they arrived on scene, they contacted the victim who advised they observed their neighbor (S1) fire multiple rounds into the air. When the victim confronted S1, he brandished the firearm and threatened to kill the victim. S1 then fled back into his apartment. The apartment building was evacuated of all occupants, and a surround and callout was initiated by patrol.

   ESU/UAV was requested for assistance. Exterior drones were utilized to provide overwatch and to relay live visual intelligence of the target location. Interior drones, pole cams and

robots were used clear the suspect's apartment. After receiving information that the suspect may be hiding in the attic of the apartment complex, a Blue Alert was initiated. Shortly after ESU Operators flew an interior drone into the attic. S1 surrendered and was safely taken into custody.

This highlights the use of various ESU Equipment to enhance the safety of officers and for the suspect. By utilizing the listed equipment, it mitigates less risk of an officer having a chance encounter with the suspect. By having the interior drone locating the suspect in the attic, it prevented an officer from placing himself/herself in a dangerous situation where force options may have been used. By having technology and equipment locating the suspect, a tactical plan was developed to safely apprehend the suspect.

4. *Date: 10JUL25*
   RD: 25-025284
   Location: 845 92nd Ave, Oakland, cA
   Summary: ESU was requested to assist with a call regarding a shooting suspect who was located within a business. The suspect had reportedly fired off several rounds inside of the office and had made comments to friends and family about committing suicide. ESU responded and assisted with aerial overwatch for ground units. An interior drone was used to check the interior of the office space. The interior drone located the subject with an apparent GSW to his head. A loaded handgun was found next to the subject.

   This highlights the use of the interior drone to locate armed subjects to prevent officers from having to engage an armed and suicidal subject. By doing so, it can provide additional time to negotiate with the arm subject to surrender or may prevent an officer involved shooting, if the subject was determined to commit suicide by cop. For this scenario, the interior drone located the deceased armed subject.

5. *Date: 04JUL25*
   Location: 5301 E.8th St, Oakland CA
   Summary: On 4 Jul 25, at approx. 1657 hrs. OPD Patrol Units observed a large fire in the area of 54th Ave. & San Leandro Blvd. Oakland Fire Department responded to the scene and requested OPD Units to assist with traffic control posts and emergency evacuations in the 5300 block of E 8th Ave. OFD advised that the fire was determined to be a 4-alarm fire meaning a designation used by fire departments to indicate a large, complex fire requiring a significant response. The area is a mixture of residential homes and commercial buildings with the potential for the fire spreading quickly. A 4-alarm fire could potentially result in serious bodily injury or death to area residents and first responders as well as significant property damage. The deployment of drones was to assist OFD and OPD Officers with emergency rescue of area residents who were in immediate danger and identify "hot spots" with the hope of faster containment of the fire. The utilization of the drones assisted OFD with saving a home from catching on fire in the middle of the structure fires, and to safely evacuate the residents without harm. The drones also assisted OPD Units with emergency evacuation of the residents in the 5300 block of E 8th St. No OPD or OFD Injuries reported. OFD Command updated OPD stating 3 large commercial buildings were destroyed by the fire and it was not known if the buildings were occupied at the time due to the building being unsafe to enter.

   On 08JUL25, OFD Requested for OPD Drones to assist with providing an aerial overview of the scene to determine where OFD needed to provide fire services. ESU/UAV operators utilized infrared technology on the drone to assist OFD determine where the "hot spots"

where so that they can put those "hot spots" out and prevent the fire from reigniting or damaging additional structures.

This highlights the use of the drone visual capabilities to provide visual intelligence for disaster management to enhance the safety of first responder personnel on scene and to save homes and provide additional layers of safety measures for residents that require first responder services. The infrared technology on the exterior drones provides thermal intelligence so that fire personnel can assess and determine if they need to respond to provide fire services.

6. *Date: 23JUN25*
   RD: 25-027412
   Location: 663 35th St, Oakland CA
   Summary: Officers located a suspect of a shooting at this location. A surround and call-out was initiated to take the suspect into custody. UAVs were requested to provide overwatch for the search warrant. While providing overwatch, the UAV caught a suspect throwing the firearm out of a window. The suspect was safely taken into custody and a firearm was recovered.

   This highlights the drone's visual capabilities to provide overwatch and live visual intelligence. The drone was able to capture a firearm being discarded from the residence, which was recovered for evidentiary purposes.

7. *Date: 27JUL25*
   RD: 25-032736
   Location: 926 85th Ave, Oakland CA
   Summary: Officers responded to the area for several ShotSpotter activations. Officers arrived on scene and determined there was a shooting victim who succumbed to his injuries. This incident was believed to have stemmed from a large warehouse party. Multiple subjects fled into the warehouse and adjacent yards. UAVs were requested to provide overwatch, identify people fleeing, and search the interior of the warehouse for the suspects. Numerous of people (about 75 people) were detained and multiple firearms were recovered.

   While detaining people, at least 4 people broke through the perimeter and fled the area. A UAV operator was able to capture this and follow the suspects several of blocks as they ran through yards. The UAV operator was able to provide responding and arresting officers of the subjects' location and other subjects' last known location for a search.

8. *Date: 29JUL25*
   RD#25-033132
   Location: 67th Ave and Foothill Blvd, Oakland CA
   Summary: Officers responded to the area of 68th Ave and Bancroft Ave for a person screaming. Once on scene, officers observed a suspect exit a vehicle leaving a firearm inside. The suspect fled on foot and a perimeter was established to take the suspect into custody. ESU/UAV was requested to assist with locating the suspect. An exterior drone was deployed. The exterior drone's infrared located a heat source emanating from a tent where the suspect was observed fleeing towards. UAV and Officers located the suspect hiding under clothing, and he was taken into police custody.

9. *Date: 25AUG25*
   RD: 25-037308

Location: 1519 Alice St, Oakland CA
Summary: On 25 AUG 25 around 1800 hours officers were dispatched to reports of criminal threats involving a firearm. Officers arrived on scene and attempted to detain the suspect. The suspect barricaded himself inside the residence. ESU was requested to assist in locating the suspect in the residence. The drone observed the subject exiting the closet in the bedroom. The drone maintained visual on the suspect until he was safely brought into custody.

10. *Date: 20NOV25*
RD: 25-050759
Location: 2200 E.12th St, Oakland CA
Summary: OPD patrol located a white BMW in the Valero parking lot (2200 E 12th St). The vehicle was determined to be an armed robbery vehicle. A high-risk stop was initiated but the single occupant refused to exit. A Blue Alert was initiated to take the suspect into custody. UAVs were used to provide overwatch and to provide real time updates of the suspect's movements. UAVs were used to check the interior of the vehicle for weapons. The suspect was safely taken into custody with a firearm located on his person.

As UAS deployments increase in response to demands from calls for service, the OPD expects continuous positive outcomes from the use of this technology.

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

There were zero UAS PRR requests in 2025. There was one in 2024 and zero in 2023.
- PRR 24-8854 (2024)

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 UAS unit currently has 1 Lieutenant, 2 Sergeants and 22 Officers. These members engage in 240 hours of training annually to ensure compliance with Department policy and FAA regulations. The member's training is conducted during their regular scheduled shifts, when possible, minimizing costs. Officers not assigned to specialized units and working patrol will normally have to backfill for themselves, which can create overtime costs. Adjusting for top rate salary, the training is estimated to cost $365,745.60 (for 22 top step officers), $38,361.60 (for 2 sergeants) and $22,185.60 (for 1 Lieutenant), or $426,292.80 total.

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

In 2023 there were slight modifications to the DGO I-25 due to Assembly Bill (AB) 481 which required California law enforcement agencies to obtain approval of a Military Equipment Use Policy. City of Oakland Police Commission and OPD reviewed the policy and provided minor edits and additions. The Police Commission and Public Safety approved the changes.

OPD is committed to providing the best services to our community while being transparent and instilling trust through constitutional and procedurally just policing. This report follows these OPD commitments. OPD hopes that this report helps to strengthen our trust within the Oakland community.

Reviewed by:

Tracey Jones, Police Services Manager
OPD, BRM, Research and Planning Unit

Prepared by:
Omar Daza-Quiroz, Acting Deputy Chief
OPD, Bureau of Investigations

Annual Surveillance Report for Surveillance Technology

Department of Violence Prevention Apricot Data Management System - June 2026

A. System Use

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

- Response: The Apricot data management system (Apricot) was used by approximately 36 staff from the Department of Violence Prevention (DVP) and 170 staff from community-based organizations funded by the DVP to deliver community violence intervention services. Direct service staff used the system to enter data on enrollment, service engagement, milestone achievement, and outcomes for individuals served, as well as attendance, duration, and content for group services. Supervisory staff used the system to monitor service delivery and track performance metrics. Grant management staff used the system to track budget spenddown, track progress on contract deliverables, and receive and process quarterly invoices. DVP program staff used the system to coordinate services between agencies and support the effective implementation of services. Lastly, the DVP's data and evaluation staff used the system to summarize service delivery and outcome data for external reports, monitor the completion of participant consent forms and adherence to service eligibility criteria, and identify and remediate data entry errors.

  Many services funded by the DVP and delivered by direct service staff require the collection of individual-level data. Users enter individual-level data in Apricot by first completing a participant record and a program enrollment form. Users then complete forms related to the type of service delivery. Table 1 provides the number of participant records and related service forms entered by users in Apricot from January 1, 2025, to December 31, 2025.

  Table 1. Apricot forms completed for individual services from January 1, 2025, to December 31, 2025.

Apricot form	Approximate number of records entered
Emergency relocation	92
Employment	37
Family and victim support	17
Housing	236
Incentive	2,819
Intake and needs assessment	188
Life map goal	1,907
Participant record	2,398
Program enrollment	2,563
Service note	71,588
Service referral	2,633

Users also enter data in Apricot related to group services or outreach and response activities. Table 2 provides the approximate number of forms completed for these services.

Table 2. Apricot forms completed for group services or outreach and response activities from January 1, 2025, to December 31, 2025.

Apricot form	Approximate number of records entered
Crisis navigation response	253
Group activities and events	1,755
Hospital response	69
Shooting and homicide response	201
Violence interruption	2,034

B. Data Sharing

- Prompt: Please provide information about 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).

- Response: Deidentified data on services delivered and personally identifiable information (PII) for participants who provided their consent was shared with the following two parties, as approved in the use policy:

    a) Urban Institute, for the independent third-party evaluation of Measure Z spending and programs, as authorized by the City Council Resolution No. 89139, Professional Services Agreement 18001, and the corresponding data-sharing agreement.

    b) Urban Institute, for the independent third-party evaluation of the DVP's Board of State and Community Corrections' California Violence Intervention and Prevention (CalVIP) grant, as authorized by the City Council Resolution No. 89367, Professional Services Agreement 13898, and the corresponding data-sharing agreement.

C. Installation & Application

- Prompt: Where applicable, provide 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.

- Response: Not applicable as Apricot is a cloud-based software.

D. Deployment Breakdown

- Prompt: Where applicable, provide a breakdown of where the surveillance technology was deployed geographically, by each Police Area in the relevant year.

- Response: Not applicable as Apricot is a cloud-based software.

E. Community Complaints

- Prompt: Provide 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.

- Response: There have been no complaints or concerns raised about Apricot related to its protection of civil rights and civil liberties. DVP data and evaluation staff have communicated with numerous grantees to integrate their feedback regarding ways to improve the user-friendliness of the system.

  The adopted use policy is adequate in protecting civil rights and liberties. Service delivery information entered in Apricot is limited to high-level information about frequency, duration, and outcomes of service delivery. Entry of PII is only required for adult services related to group violence; it is not required for services related to gender-based violence or for youth services. When PII is entered, data are only visible to staff within the agency entering the data and select staff from the DVP who perform data and evaluation or service coordination roles; they are not visible to other agencies funded by the DVP. PII is only shared with external evaluation partners for individuals who consent to having their data shared externally for evaluation purposes. Table 3 provides race and ethnicity data for participants whose data was entered in Apricot from January 1, 2025, to December 31, 2025.

  Table 3. Race and ethnicity data for participants whose data were entered in Apricot from January 1, 2025, to December 31, 2025.

Race	Percentage
African American	45%
Asian	3%
Hispanic or Latino	24%
Multi-Racial	7%
White	5%

Race	Percentage
Other	1%
Missing	15%

F. Internal Audits & Compliance

- Prompt: Provide 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.

- Response: DVP data and evaluation staff regularly review record audits of Apricot. There have not been any violations or potential violations of the use policy to date.

G. Data Breaches or Other Unauthorized Access

- Prompt: Provide 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.

- Response: There have been no data breaches or unauthorized access to the Apricot system.

H. Efficacy

- Prompt: Provide information, including crime statistics, that help the community assess whether the surveillance technology has been effective at achieving its identified purposes.

- Response: Data collected through Apricot have allowed DVP staff to perform the following tasks:

    a) **Monitor service delivery to ensure alignment with best practices.** In 2024, the City of Oakland reimplemented the Ceasefire-Lifeline strategy for reducing gun violence. The DVP delivers the Lifeline part of the strategy, which involves providing intensive life coaching and violence interruption services to individuals who are at highest risk of drawing or driving gun violence. Performance reports generated through Apricot based on data entered by DVP direct service staff allow DVP supervisors and leadership to continuously monitor services to ensure they are being delivered with fidelity to the evidence-based model. Oakland ended 2025 with reductions of 49% in homicides and shootings compared to 2023, suggesting that this work has been highly successful in reducing group-driven violence.

    Additionally, DVP staff were able to review services delivered by funded community-based organizations to ensure they met expectations outlined in

grant scopes of work. In cases when service delivery was not happening as expected, DVP staff were able to provide technical support and guidance to agencies. For example, after reviewing data entered by an agency funded to deliver emergency housing services to survivors of gender-based violence, DVP staff realized that participants were consistently being directed to shelters instead of receiving the option for temporary hotel stays, as outlined in the agency's scope of work. DVP staff had a conversation with agency staff about this service expectation and the agency adjusted its offerings for clients going forward. This is one of many examples of how reviewing service data on a regular basis has allowed DVP staff to support enhanced service delivery from funded agencies.

b) **Coordinate group violence services.** DVP staff who coordinate group violence services, including violence interruption activities, relocation, and life coaching, were able to access data entered by funded agencies to coordinate service response across agencies. For instance, supervisors who coordinate violence interruption activities were able to access information entered by each of the four agencies funded to perform violence interruption work to monitor the status of these activities and determine next steps. Additionally, the program officer who coordinates emergency relocation services was able to review referral requests and approve or deny them, after which approved requests were sent to a funded agency to process.

c) **Understand coordinated access to services.** The DVP strives to engage participants in multiple services funded through its network of community-based organizations to address multiple needs that clients have related to their vulnerabilities to violence. Apricot allows the DVP to determine how many funded services each participant accesses; Table 4 provides the percent of clients engaged in one or more group violence services from January 1, 2025, to December 31, 2025. In the next year, the DVP intends to facilitate stronger referral pathways and coordination across agencies to achieve higher percentages of participants accessing more than one service.

Table 4. Number of services accessed by participants in the group violence strategy from January 1, 2025, to December 31, 2025.

Number of services accessed	Percent of clients served
1	94%
2	5%
3 or more	1%

d) **Summarize and share service data with public oversight bodies and external funders to justify continued funding.** DVP data and evaluation staff created reports that summarized aggregate service data for councilmembers and commissioners who oversee the allocated of DVP funding for community-based contracts. These data have been instrumental in justifying continued financial investments in violence prevention and

intervention services in Oakland by providing a clear picture of the services delivered and the demographics of people served. Additionally, data and evaluation staff used data collected through Apricot to complete quarterly and biannual grant reports for external funders to justify a continued financial investment.

e) **Evaluate services to assess impact.** Data collected in Apricot have served as the primary source of data for impact evaluations of violence intervention services funded by public ballot measures, as well as evaluations of external grants from the California Board of State Community Corrections and Kaiser Permanente.

I. Public Records Requests

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

- Response: There have been no public records requests pertaining to Apricot.

J. Total Annual Costs

- Prompt: Provide the 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.

- Response: The annual cost of Apricot in Fiscal Year (FY) 2026-2027 is $125,000. Approximately $63,000 will come from the DVP's General Purpose Fund allocation and approximately $62,000 will be funded by external grants.

K. Requested Use Policy Amendments

- Prompt: Please describe any requested modifications to the Surveillance Use Policy and provide a detailed basis for the request.

- Response: The DVP is requesting one modification to the use policy. The current use policy states that PII is not entered for individuals receiving services related to gender-based violence. The DVP would like to modify this to state that PII is not required for individuals receiving services related to gender-based violence. Data may be entered if individuals provide their informed consent. This is the same approach taken for all youth services related to gun violence intervention.

Apricot Use Policy
City of Oakland Department of Violence Prevention

The Department of Violence Prevention (DVP) has a mandate to reduce levels of gun violence, intimate partner violence, commercial sexual exploitation, and trauma associated with these forms of violence in Oakland. Each year, the DVP distributes approximately $13 million to community-based organizations (CBOs) in Oakland that deliver intervention services related to these forms of violence. The DVP also provides direct services in the areas of intensive life coaching and violence interruption.

A. Purpose

The Apricot data management system, developed by Bonterra (formerly Social Solutions Global, Inc.), enables the DVP and its funded CBOs to track information that is essential to effective service delivery and grant management. Direct service staff use the system to enter data on enrollment, service engagement, milestone achievement, and outcomes for individuals served, as well as attendance, duration, and content for group services. Supervisory staff use the system to monitor services delivered by direct service staff and track performance metrics. Grant management staff use the system to track budget spenddown, track progress on contract deliverables, and receive and process quarterly invoices. DVP program staff use the system to coordinate services across agencies and support the effective implementation of services. DVP data and evaluation staff use the system to summarize service delivery and outcome data for external reports, monitor the completion of participant consent forms and adherence to service eligibility criteria, and identify and remediate data entry errors. Lastly, external evaluators use data entered in Apricot to assess the implementation and impact of services delivered or funded by the DVP.

B. Authorized Use

Data stored in Apricot is accessed on a need-to-know and right-to-know basis, meaning that DVP and CBO staff members only have access to information that is essential to their job function. Categories of Apricot system usage are described below.

- **Service delivery:** Direct service and supervision staff employed by the DVP and funded CBOs use Apricot to track information on participant enrollment, contacts, progress towards milestones, service referrals, and other aspects of service delivery. Direct service staff include individuals such as case managers and life coaches who work directly with participants to deliver services or programming. Supervision staff are supervisors of direct service staff.

- **Service coordination and monitoring:** Select staff members within the DVP who coordinate and monitor services have access to data entered by CBOs to ensure services are delivered in a timely, responsive, and coordinated manner.

- **Grant management:** Grant management staff from CBOs use the system to complete quarterly grant reports, enter quarterly expenses, access approved quarterly invoices, and submit budget or scope modifications. Grant management staff from the DVP use the system to track grantees' budget spenddown, receive and process budget or scope modifications, track grantees' progress on contract deliverables, monitor the completion of participant consent forms and adherence to service eligibility criteria, and receive and process quarterly invoices.

- **Reporting and evaluation:** DVP data and evaluation staff use the system to summarize service delivery and outcome data for a variety of external audiences, including councilmembers, commissioners, and external funders. These staff perform monthly data quality assurance checks to identify and remediate data entry errors, and they extract and prepare data for external evaluators.

- **External evaluation:** External evaluators contracted by the City of Oakland use data from Apricot to evaluate the effectiveness of services delivered by the DVP and funded CBOs. Evaluators seek and receive institutional review board (IRB) approval prior to commencing research activities. Once IRB approval is obtained, evaluators only have access to personally-identifiable information for individuals who have signed a consent form agreeing to have their identifiable data shared with a third-party evaluator. For participants who do not sign a consent form, evaluators receive deidentified or aggregate data.

C. Data Collection

Service delivery data are entered into Apricot by direct service staff employed by the DVP and contracted CBOs. **Tables 1 and 2** provide an overview of the types of data collected through each Apricot form.

Table 1. Types of data collected through Apricot forms used for individual services.

Form	Types of data fields
Family and victim support	1. Date next-of-kin information received 2. Date next-of-kin successfully contacted 2. Types and amount of support provided (e.g. basic needs, funeral/vigil planning, victim of crime application)
Housing placement	1. Dates housed 2. Housing type (e.g. permanent, transitional, shelter) 3. Funding disbursement date and amount where applicable
Incentives	1. Date of disbursement 2. Incentive amount 3. Justification for incentive
Intake and needs assessment	1. Date of intake and needs assessment 2. Other questions specific to strategy or service provider
Job placement: Work experience	1. Dates employed 2. Wages at beginning and end of employment 3. Weekly hours worked at beginning and end of employment 4. Type of employment (subsidized vs. permanent)
Life map goals	1. Goal start date, status and completion date 2. Goal category and current progress notes 2. Planned and accomplished actions associated with goals
Participant record	1. Name and date of birth 2. Contact information 3. Demographic information (race, gender, education, language spoken at home) 4. Employment status

Form	Types of data fields
	5. Housing status 6. School information, if applicable 7. Names and contact information of important people, if participant chooses to provide (e.g. probation officer)
Program enrollment	1. Date and source of referral 2. Dates of enrollment and exit 3. Type of program 4. Evaluation consent response 5. Basic needs check, if applicable 6. Eligibility screener, if applicable 7. Reason for exit
Referral to services	1. Date of referral 2. Type of service referral 3. Name of organization referred to
Service notes	1. Date, service provided, contact method, who was the meeting with, duration, and service notes 2. Flex funds provided, if applicable 3. Type of legal assistance provided, if applicable

Table 2. Types of data collected through Apricot forms for group services and response activities.

Form	Types of data fields
Group activity	1. Date, location, and duration of activity 2. Number and type (e.g. students, residents, teachers) of people in attendance 3. Type of activity (e.g. training, support group) 4. Attendance
Employer profile	1. Name of employer 2. Contact information for employer 3. Type of employment field
Crisis navigation	1. Date and location of contact 2. Basic demographic information (age, gender, race) 3. Yes/No: Was safety plan developed? 4. Yes/No: Did the individual agree to short-term case management? 5. Yes/No: Did you make a referral? 6. Referral details, if applicable
Hospital response	1. Date and location of initial notification 2. Date and time of visits for service 3. Initials and demographics of individual visited 4. Yes/No: Was safety plan developed? 5. Yes/No: Did the individual agree to short-term case management?
Relocation referral	1. Referring staff name, agency and contact details 2. Name, contact info and demographic info (age, gender, race) of individual being relocated 3. Number of individuals in the family 4. Date and types of relocation support requested 5. Date and result of request for relocation support/funding

Form	Types of data fields
Shooting and homicide incident	1. Date and time of notification 2. Location of incident 3. Date and time of notification to network 4. Location of victim, injury type, homicide (yes/no), number of people injured 5. Notes on follow-up and retaliation level
Violence interruption	1. Date and duration of interaction 2. Violence Interrupter name, type (community, DVP, school) and agency name if applicable 3. Type of activity 4. Number of people interacted with and who they talk to (impacted person, influencer, other community member) 5. Location of conversation 6. If the interaction is related to any active conflicts or shooting/homicide incident 7. Was a safety assessment conducted 6. Outcome of conversation

Tables 3 and 4 identify the types of data CBOs are expected to enter for services related to gun violence and gender-based violence, respectively. For services that require individual-level data, Tables 3 and 4 also identify whether personally-identifiable information (PII) is required. PII is any information that can be used to distinguish one person from another and can be used to deanonymize previously anonymous data. For services that do not require entry of PII, which includes all gender-based violence services and youth services, PII should only be entered if the participant (and a guardian, in the case of minors) completes a consent form agreeing for their PII to be entered. In cases when participants do not agree, CBOs should use unique identifiers in place of PII. Unique identifiers are numeric codes that link to a key with participant names and dates of birth by CBOs outside the Apricot database. Evaluation of CBO performance by the DVP will not be contingent on the rate of consent. If a CBO has a consent rate that is less than 80%, the DVP will work with the CBO to explore options for increasing rates.

Table 3. Categories of data entered in Apricot for services related to gun violence.

Activity	Is individual-level data entered?	Is PII required?	Is group-level data entered?
Adult employment	Yes	Yes	Yes
Adult life coaching	Yes	Yes	No
Emergency relocation	Yes	Yes	No
Family and victim support	Yes	Yes	Yes
Healing	Yes	Yes	Yes
Hospital-based intervention	Sometimes	Yes	No
Violence interruption	No	N/A	No
Youth diversion	Yes	No	No
Youth employment	Yes	No	Yes
Youth life coaching	Yes	No	No

Table 4. Categories of data entered in Apricot for services related to gender-based violence.

Activity	Is individual-level data entered?	Is PII required?	Is group-level data entered?
24-hour hotlines	No	N/A	No
Crisis response	Sometimes	No	No
Emergency shelter	Yes	No	No
Healing services	Yes	No	Yes
Legal advocacy	Yes	No	No
Life coaching	Yes	No	No
Transitional housing	Yes	No	No

For activities that require PII, CBOs are encouraged to notify participants that their name and date of birth are documented in Apricot for purposes of effective service delivery and coordination. Participants are also asked to complete a consent form regarding potential access to their PII by a third-party evaluator. Completion of this consent form is strongly encouraged but is not a requirement of service delivery for any strategy, and participants are able to decline having their PII accessed by a third-party evaluator if they wish. Additionally, CBOs in the DVP network are not evaluated based on their rates of participant consent to sharing data with an external evaluator.

D. Data Access

The DVP takes special care to ensure that data within Apricot are accessed on a need-to-know and right-to-know basis, meaning that staff are only be able to access information that is essential to their job function. Apricot allows administrators to restrict access to individual forms, records, and fields for staff members based on their pre-determined access requirements. An overview of data access levels for categories of staff employed by the DVP and contracted CBOs is provided below:

Funded CBOs

- ***Direct service staff and supervisors*** have access to individual- and group-level service delivery data entered by members of their agency only. Direct service staff and supervisors do NOT have access to service-delivery data for participants being served by other agencies, even if they are the same participants.

- ***Grant management staff*** have access to contract and fiscal documents such as budgets, invoices, and quarterly reports for their agency only. These staff members also have access to aggregate service delivery data pertaining to contract deliverables, which are automatically calculated based on data entered by direct service staff. Grant management staff do not have access to individual participant records or PII.

DVP

- ***Direct service staff and supervisors*** have access to individual- and group-level service delivery data entered by DVP staff. Direct service staff and supervisors within the DVP do NOT have access to service-delivery data for participants being served by other agencies, even if they are the same participants.

- ***Service coordination and monitoring*:** Select staff members within the DVP who coordinate and monitor services have access to data entered by CBOs to ensure services are delivered in a timely, responsive, and coordinated manner.

- ***Grant management staff*** have access to contract and fiscal documents such as budgets, invoices, and quarterly reports for all grantees. These staff members also have access to aggregate service delivery data pertaining to contract deliverables, which are automatically calculated based on data entered by direct service staff. Grant management staff do not have access to individual participant records or PII.

- ***Data and evaluation staff*** have access to all forms and data entered in Apricot, whether by DVP or CBO staff.

Unauthorized use of the system by any staff person with any level of access will lead to disciplinary action, which could include the termination of a CBO's grant agreement and cessation of funding or, with respect to City of Oakland employees, discipline up to and including termination.

E. Data Protection

Apricot has comprehensive measures in place to maintain data privacy and security. The system sits behind a firewall that extensively controls, tracks, and reports access to the system's internal infrastructure. Apricot meets current U.S. Department of Housing and Urban Development (HUD) domestic violence standards, Homeless Management Information System (HMIS) standards, and Social Security Administration data management and security protocols, as well as minimum required Family Educational Rights and Privacy Act (FERPA) and HIPAA standards. Data entered into Apricot are automatically encrypted while in transit between a user's computer and the system's servers, as well as while at rest. Additionally, users accessing Apricot servers do so via a secure HTTPS connection. More information on privacy and security for the Apricot system is included in **Attachment A.**

F. Data Retention

Agencies that collect PII for participants based on their funded activities are required to retain the PII for three years following service completion to ensure that data are available for evaluations conducted by external evaluators, which can last for up to three years following service delivery. At the end of three years, agencies will delete PII unless exempted based on legal requirements. Anonymous service delivery data should be retained for an additional four years to allow the DVP to monitor trends in service delivery over time. At the conclusion of seven years, individual-level data will be permanently deleted from Apricot unless exempted due to legal requirements.

G. Public Access

There is absolutely no public access to individual-level participant data in Apricot. As with any government record, a member of the public may submit a Public Records Act request, but only aggregate data (no PII) would be released subject to applicable federal, state, and local privacy or confidentiality laws. If the DVP receives a request of this nature, staff will work with the City Attorney's Office to respond to the request without sharing PII. The DVP will also notify any contracted CBOs impacted by the data request as soon as reasonably possible. To date, the City of Oakland has only received requests through the Public Records Act for aggregate-level data pertaining to its violence prevention and intervention services.

Aggregate data from Apricot is available in evaluation reports published by third-party evaluation firms and may be shared through public tables, charts, or dashboards created by the DVP.

H. Third Party Data Sharing

External evaluators contracted by the City of Oakland use data in Apricot to evaluate the effectiveness of funded programs. External evaluators only have access to PII for individuals who sign a consent form allowing their PII to be shared with a third-party evaluator. For participants who do not sign a consent form allowing access to their PII, external evaluators receive deidentified or aggregate data.

I. Training

The DVP's data and evaluation staff have attended Apricot training sessions, such as the Certified Apricot Administrator Training, which review Apricot's configuration and tips and tricks for training end users. In addition, DVP staff has access to numerous Apricot trainings through the training library. Using these tools, the DVP's data and evaluation staff train direct service staff, supervisors, and contract and fiscal staff within the DVP and contracted CBOs on how to use Apricot. This includes general trainings, trainings specific to activities, and ongoing options for one-on-one training, support, and technical assistance. All trainings specify appropriate usage of the system pertaining to data privacy and security as outlined in this use policy, and all trained staff members sign a copy of the use policy indicating that they have read and understand it. Trainings also discuss consequences of inappropriate system usage, which could include termination of a CBO's grant agreement and cessation of funding or, with respect to City of Oakland employees, discipline up to and including termination.

Additionally, all staff within the DVP who have access to participant-level data entered by CBOs complete a training called *About Privacy and Confidentiality for Non-HIPAA Covered Entities* from Relias Academy at least once every two years.

J. Auditing and Oversight

The DVP's data and evaluation staff monitor compliance with this use policy of staff within the DVP and contracted CBOs. All actions in the system (add, edit, delete, view, etc.) are accessible through audit log reports built into the system for administrator monitoring that DVP's data and evaluation staff review regularly. Any indication of inappropriate system usage is thoroughly investigated by the DVP in consultation with the City Attorney's Office. Inappropriate system usage could result in termination of a CBO's grant agreement and cessation of funding or, with respect to City of Oakland employees, discipline up to and including termination.

K. Maintenance

Bonterra's security mechanisms and procedures are built on the Soc2 Type II Framework with HIPAA amendment and audited by third-party security experts annually to ensure compliance with best-in-class technical safeguards, processes, policies, and procedures. Bonterra has an extensive cloud security team led by their Chief Information Security Officer that uses a broad set of tools for monitoring security, vulnerability, integrity, and uptime across over 19,000 customers. A complete copy of Bonterra's Soc2 Type II has been shared with City of Oakland staff who have signed a non-disclosure agreement, including data and evaluation staff from the DVP and staff from the Information Technology Department.

L. Evaluation

On an annual basis, the DVP shall present a report regarding Apricot usage to the Privacy Advisory Commission and, subsequently, to the City Council, for an evaluation. Such evaluation shall include what data was collected, how it was used, consent rates of contracted CBOs, and any recommended changes to the use policy.

Apricot 360 Annual Report

Department of Violence Prevention (DVP)

Jenny Linchey
Deputy Chief of Grants, Programs, and Evaluation

Ulises Sanchez
Data & Evaluation Specialist

CITY OF OAKLAND

Overview of Apricot 360

- Cloud-based system developed by Bonterra for use by social service providers to track service delivery and grant management.
- Approved by the Privacy Advisory Commission in July 2022.
- Approved by City Council in July 2022.
- Implemented by the DVP in January 2023, replacing Cityspan.
- Annual report approved by the PAC in June 2024 and June 2025.

Uses of Apricot 360

- **Direct service staff** use the system to track enrollment, service engagement, milestones, and outcomes for individual services and to track attendance, duration, and content for group services.

- **Supervisory staff** use the system to monitor service delivery and track performance metrics.

Uses of Apricot 360

- **Grant management staff** use the system to track budget spenddown, track progress on contract deliverables, and receive and process quarterly invoices.

- **Program staff** used the system to coordinate services between agencies and support the effective implementation of services.

- **Data and evaluation staff** use the system to summarize service delivery and outcome data for external reports, monitor consent forms and eligibility criteria, and identify data entry errors.

One-Year Report: System Usage

- From January 1, 2025, to December 31, 2025, the system was used by approximately 36 staff from the DVP and 170 staff from community organizations.

One-Year Report: System Usage

Table 1. Apricot 360 forms completed for services that require the collection of individual-level data from January 1, 2025, to December 31, 2025.

Apricot form	Number of records entered
Participant record	2,398
Program enrollment	2,563
Service note	71,588
Service referral	2,633
Life map goal	1,907
Intake and needs assessment	188
Housing placement	236
Emergency relocation	92
Incentive	2,819

One-Year Report: System Usage

Table 2. Apricot 360 forms completed for services that require the collection of group-level data from January 1, 2025, to December 31, 2025.

Apricot form	Number of records entered
Crisis navigation response	253
Group activities and events	1,755
Hospital response	69
Shooting and homicide response	201
Violence interruption	2,034

One-Year Report: Data Sharing

Deidentified data for all participants and personally identifiable information (PII) for participants who provided their consent was shared with the following two parties, as approved in the use policy:

- Urban Institute, for their evaluation of Measure Z.
- Urban Institute, for their evaluation of DVP work funded by a state grant.

One-Year Report: Community Complaints

- There have been no complaints or concerns raised about Apricot 360 related to its protection of civil rights and civil liberties.

- DVP data and evaluation staff communicate with grantees on an ongoing basis to integrate their feedback regarding ways to improve the user-friendliness of the system.

One-Year Report: Protecting Civil Liberties

- Service delivery information entered in Apricot is limited to high-level information about the number and duration of service contacts and service outcomes.

- PII is only required for adults receiving services related to gun violence. It is not required for youth or individuals receiving services related to gender-based violence.

One-Year Report: Protecting Civil Liberties

- For services that involve entry of PII, data are only visible to staff within the agency entering the data and select DVP staff who perform data and evaluation or service coordination roles; they are not visible to other agencies funded by the DVP.

- PII is not entered for youth clients whose parents/caregivers do not consent to the entry of their child's PII.

- PII is only shared with evaluation partners for clients who consent to having their data shared externally for evaluation.

One-Year Report: Protecting Civil Liberties

Table 3. Race and ethnicity data for participants who data was entered in Apricot 360 from January 1, 2025, to December 31, 2025.

Race	Percentage
African American	45%
Asian	3%
Hispanic or Latino	24%
Multi-Racial	7%
White	5%
Other	1%
Missing	15%

One-Year Report: Audits, Breaches, and Requests

- DVP data and evaluation staff regularly review record audits of Apricot 360. There have not been any violations or potential violations of the use policy to date.

- There have been no data breaches or unauthorized access to the Apricot 360 system.

- There have been no public records requests pertaining to Apricot 360.

One-Year Report: Annual Costs

- The annual cost of Apricot in Fiscal Year 2026-2027 is $125,000.

- Approximately half will come from the DVP's General Purpose Fund allocation and half will be funded by external grants.

One-Year Report: Efficacy

Apricot 360 has allowed the DVP to:

- Monitor service delivery to ensure alignment with best practices including the Ceasefire-Lifeline model, which led to a reduction of 49% in shootings and homicides from 2023 to 2025.
- Coordinate service delivery within the group violence strategy.
- Summarize and share service data with public oversight bodies and external funders to justify continued funding.
- Evaluate services to assess impact.

One-Year Report: Proposed Modification

The DVP is proposing the following amendment:

- Current use policy states that PII is not entered for individuals receiving services related to gender-based violence.
- We want to modify this to state that PII is not required for individuals receiving services related to gender-based violence. Data may be entered if individuals provide their informed consent.
- This is the same approach taken for all youth services related to gun violence intervention.

Thank You