CITY OF OAKLAND

Privacy Advisory Commission

May 1, 2025; 5:00 PM
Oakland City Hall
Hearing Room 1
1 Frank H. Ogawa Plaza, 1st Floor
Regular Meeting Agenda

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

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

1. Call to Order, determination of quorum

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

3. Information Item:
    a. Report from Public Works regarding OPD request for video footage.

4. Action Items:
    a. April 3, 2025 PAC minutes
    b. Annual Reports
        1. Biometric Crime Lab (OPD)
        2. ALPR/FLOCK (OPD)
        3. ATF (OPD)

    c. Use Policies
        1. OPD Community Safety Camera Systems (OPD)

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

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

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

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

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

Oakland Police Department Criminalistics Laboratory
DNA Instrumentation and Analysis and Software
Surveillance Impact Report
April 2025

1. Description

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. This is a biometric analysis which produces potentially sensitive information.

During the lengthy and complicated process to obtain a DNA profile from evidence or a reference sample, numerous steps may be necessary including, but not limited to: Digestion, Extraction, Quantitation, Normalization/Amplification, Typing, Interpretation, and Database upload.

OPD does not use Forensic DNA Analysis to surveil residents of Oakland; indeed, it is unlawful to analyze samples and upload them to Combined DNA Index System (CODIS) when no articulable nexus to a crime exists.

2. Purpose

At the end of all DNA analysis processes described previously, 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 reference DNA profiles.

3. Location

The DNA instruments and analysis software are housed in the Criminalistics Laboratory and may not be used elsewhere without disclosure to the Laboratory's accreditation agency ANAB [ANAB = American National Standards Institute (ANSI) National Accreditation Board] and revalidation.

4. Impact

The proposed biometric use policy covers how and when information is to be disseminated, as well as prohibitions against disclosures outside those listed. Civil Rights and liberties are adequately protected in that all samples are to be collected pursuant to search warrant, other legal means, or by documented consent. Nothing in the forensic DNA analysis allows for data collection to be discriminatory, viewpoint-based or biased by algorithm; in fact, the results of DNA analysis can, in a scientifically unbiased manner, include or (more importantly to privacy) exclude a person of interest. OPD recognizes that biometric analysis technology and associated data, if used in ways that violate accreditation, legal standards and uses described and referenced herein, would constitute inappropriate use.

5. Mitigations

The OPD Crime Lab mitigates against the impact of unlawful evidence submissions by requiring that all samples subject to DNA analysis are collected pursuant to search warrant, other legal means, or by documented consent.

Inappropriate uses of DNA biometric analysis technology and associated data are mitigated by:

(1) Limiting access to the instrumentation and records.
    a. Only staff authorized to work in the Crime Lab have access.
    b. Sign-in and escort are required of all guests.
    c. The laboratory is locked during business hours and locked and alarmed after hours.
(2) Existence of written policies regarding care of data and casefiles.
    NOTE: The use of the term "secure servers" throughout this Impact Report is on the basis of working with the Information Technology Department (ITD) in 2020 to develop terminology in this document. ITD is responsible for the preservation, fidelity and security of the data described herein.
    a. Instrument software is in limited access locations and are hosted on secure servers.
    b. DNA analytical data are kept on secure network drives.
(3) Existence of written policies precluding wide dissemination of records.
    a. Legal Discovery for Criminal or Civil trials is honored.
    b. California Public Records Act (CPRA) requests are subject to limitations as specified in the Biometric Technology Use Policy.

6. Data Types and Sources

The instruments described previously collect data during one step in the process and may be passed along to another. Data generated by each instrument are stored in a proprietary format readable only by the protocol software or may be converted to tables to be used electronically or printed. The Use Policy indicates how raw data and paper casefiles are to be handled and stored.

7. Data Security

Criminalists and Forensic Technicians with duties in the Forensic Biology/DNA unit shall be the only Crime Laboratory personnel authorized to use the DNA collection and analysis software in casework, and only after completing a comprehensive training program and qualifying test, at which time, with the Supervisor's recommendation, the Crime Laboratory Manager issues a written authorization. No one else shall have the authority to grant access to use the DNA instrumentation or software in casework. Criminalists and Forensic Technicians are granted access to one another's cases only for the purpose of complying with discovery, documenting quality checks, verifications or peer review. Interns also are authorized to use the DNA collection and analysis software for special projects, not casework, and only after receiving necessary training and under the supervision of a qualified Criminalist. Data are stored on secure servers hosted in the Laboratory or by the Department.

8. Fiscal Cost

The following platforms are used to analyze DNA samples. Costs are listed in Appendix A and reflect the values reported to the Privacy Commission in the Annual Report.

Digestion / Extraction

- EZ1 Advanced XL DNA purification instruments
- EZ2 DNA purification instruments and software
- Versa 1100 instrument

Liquid Handler

- Qiagility instrument
- Hamilton STARlet instrument

DNA Quantitation

- QuantStudio 5 Real-Time PCR DNA quantitation instrument

DNA Normalization / Amplification

- SpeedVac concentrator
- ProFlex thermal cycler

DNA Typing

- 3500 genetic analyzer

DNA Interpretation

- STRmix
- FaSTR
- Armed Expert

In 2024, costs included:
Total purchase cost (born over several years): $1,110,800
Total maintenance cost: $90,185
Total testing cost reagents/kits: $126,000
Estimate of consumables: $150,000

Grants, Proposition 69 funds, and Operations and Maintenance budgets have historically covered these costs. Refer to Appendix A for specifics.

9. Third Party Dependence

Electronic data are retained indefinitely on secure server or network drives and do not require a third party. Hardcopy data present in paper casefiles are currently stored under laboratory control. In the future, if storage needs for hardcopy files exceed capacity, a Departmentally- approved records retention facility will be used as articulated in the

Biometric Use policy.

10. Alternatives

The DNA analysis instruments and software have been validated and meet or exceed both accreditation requirements and industry standards. Alternatives have either been found to be inferior or would require time-exhaustive and expensive validation to replace the current platform with other technology.

11. Track Record

STR-based DNA analysis as a technology has extensive and longstanding documentation as a standard and effective method to analyze DNA. The methods using these technologies in total are employed by many private and government (local, state, federal) forensic and clinical laboratories. There is no known adverse information extant about the technology.

CITY OF OAKLAND

MEMORANDUM

TO: Floyd Mitchell, Chief of Police

FROM: Frederick Shavies, Deputy Chief OPD, Bureau of Investigations

SUBJECT: OPD Crime Lab Biometrics DNA Analysis Technology 2024 Annual Report

DATE: April 11, 2025

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 to comply with the annual reporting mandate.

2024 Data Details

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

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 2024

The Forensic Biology Unit analyzed 352 requests between January 1, 2024 to December 31, 2024. Over 1,941 items of evidence were examined, from which 4,283 samples were subjected to digestion and extraction using the Versa and EZ1/2 instruments. Scientist subjected 4,304 samples to quantitation analysis using the SpeedVac, Qiagility, and QuantStudio 5 instruments and 1,599 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 27 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. As for the geographic location of crimes, this is not collected by the laboratory in a way that can be disseminated easily. The address may be reported on the request for laboratory services form, but it is not required for analysis to proceed. 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.

NOTE: The use of the term "secure servers" throughout this report, the Biometric Use Policy, and the Surveillance Impact Report is based on working with the Information Technology Department (ITD) in 2020 to develop terminology. ITD is responsible for the preservation, fidelity and security of the data described herein.

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 352 requests in 2024. These are further broken out by crime type in Table 1 below

Table 1: OPD Crime Laboratory DNA Analysis Requests in 2024

Crime Type	**Number of Requests**
Homicide/ Attempted Homicide	92
Sexual Assault/Kidnapping	156
Assault	24
Robbery/Burglary/Auto Theft	16
Hit and run/Carjacking	11
Weapons	43
Cold Case (prior to 2008)	10
Total	**352**

CODIS hits in 2024 – Eighty-six DNA profiles were uploaded to the CODIS database. The laboratory had one hundred and twenty associations (hits); fifty-eight hits to named individuals whose identity were unknown, five hits to unsolved forensic cases, and fifty-seven 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 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:

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 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 $3,700 annual maintenance*
- *EZ2: $61,250 to purchase (x2 instruments = $122,500) and $4,500 to maintain; 2 instruments for $9,000 annual maintenance*
- *Versa 1100: $85,000 to purchase and $5,500 annual maintenance*

Liquid Handler

- *Qiagility: $33,100 to purchase (x3 instruments = $99,300) and $4,250 to maintain; 3 instruments for $12,750annual maintenance*
- *Hamilton STARlet: $108,000 to purchase (x2 instruments = $216,000)*

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, $21,525 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 $140,000, 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, 2024: $90,185
Total testing cost reagents/kits, 2024: $126,000
Estimate of consumables: $150,000

The cost / benefit analysis in the form of Return on Investment (ROI) calculations place the societal cost of each homicide at

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. Updates of annual costs in the SIR were made. Whereas the costs resided in the main SIR document, the recommendation is to place the costs into an Appendix so-as to not invalidate the SIR simply due to shifts in expenses. Since these costs are reported to the Privacy Commission annually as part of the mandatory reporting requirement, invalidating the SIR due to cost fluctuations was not reasonable. The Appendix will serve to document the expenses on an annual basis. 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 ssachs@oaklandca.gov.

Respectfully submitted,

_____

Reviewed by:
Frederick Shavies, Deputy Chief
OPD, Bureau of Investigations

Prepared by:
Bonnie Cheng, Forensic Biology Unit Supervisor
OPD, Criminalistics Laboratory

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

Sandra Sachs, PhD, Crime Lab Manager
OPD, Criminalistics Laboratory

Tracey Jones, Police Services Manager
OPD, Bureau of Risk Management, Research and Planning

Oakland Police Department Criminalistics Laboratory
DNA Instrumentation and Analysis and Software
Surveillance Impact Report
Appendix A

April 2025

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 a non-negligible contribution to the total costs.

Procuring and maintaining the equipment expenses are shown by Category of testing and platform below:

Digestion/Extraction
- EZ1: $63,000 to purchase and $3,700 annual maintenance
- EZ2: $61,250 to purchase (x2 instruments = $122,500) and $4,500 to maintain; 2 instruments for $9,000 annual maintenance
- Versa 1100: $85,000 to purchase and $5,500 annual maintenance

Liquid Handler
- Qiagility: $33,100 to purchase (x3 instruments = $99,300) and $4,250 to maintain; 3 instruments for $12,750 annual maintenance
- Hamilton STARlet: $108,000 to purchase (x2 instruments = $216,000)

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, $21,525 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 $126,000, 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
Maintenance cost, 2024: $90,185
Testing cost reagents/kits, 2024: $126,000
Estimate of consumables: $150,000

CITY OF OAKLAND

MEMORANDUM

TO: PAC **FROM:** OPD

SUBJECT: ALPR Annual Report **DATE:** APRIL 24, 2025

Background

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

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

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

2024 Annual Report Details

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

How the Technology is Used

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

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

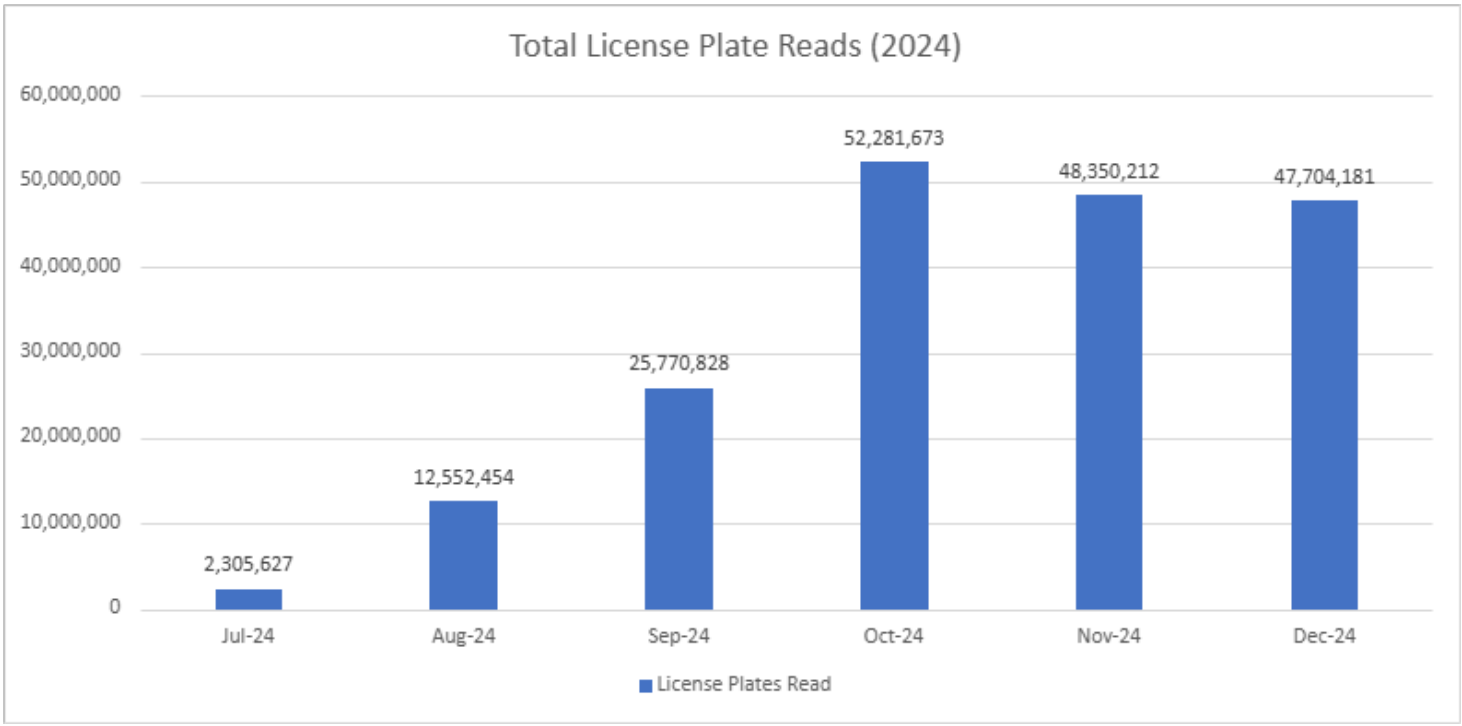
1. To assist in active criminal investigations which have just occurred. The OPD will utilize ALPR to search where a crime just occurred. OPD personnel can enter a vehicle's license plate (if one was provided) or enter a partial license plate (if one was provided) or search a camera location (if no license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

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

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

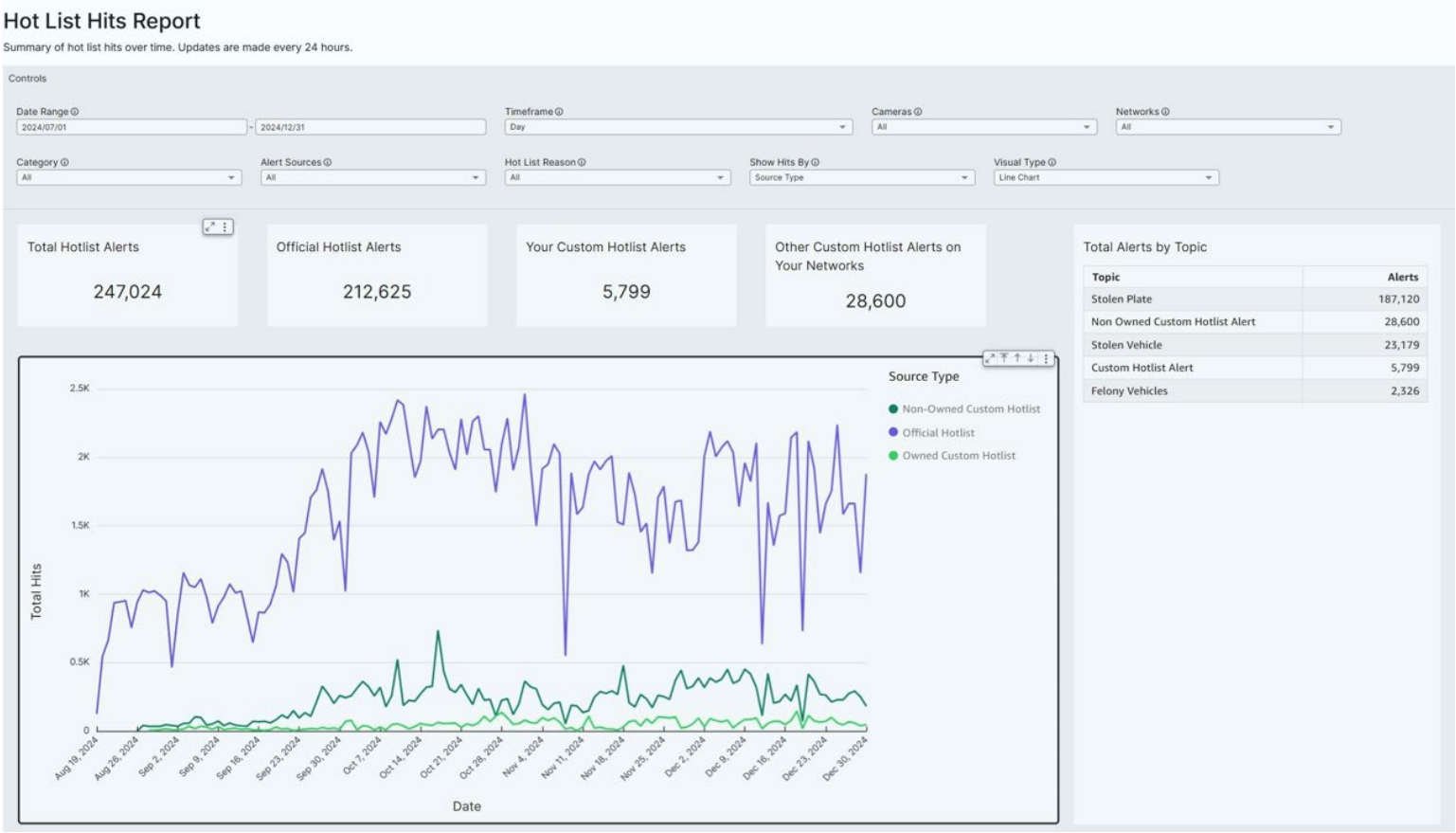
Figure A below shows the amount of license plate reads, month over month. Please note that the same license plate can be read multiple times a day, if that license plate passes by the same or different cameras during its travel. From July 2024 through December 2024, there was a total of 188,964,975 license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

Figure A



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

Figure B.



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

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

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

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

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

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

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

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

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

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

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

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

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

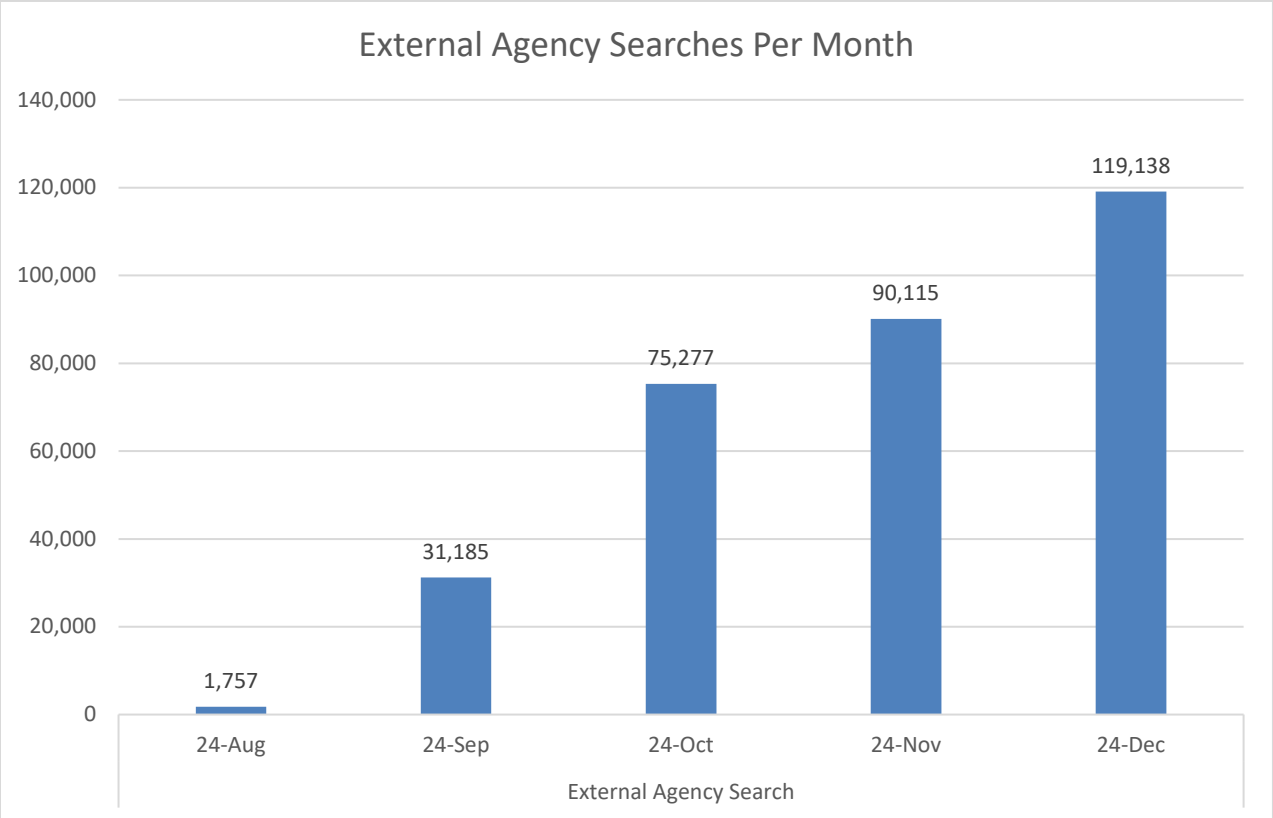
After agreeing to those three questions, the requesting agency was granted access, with approval being logged in a spreadsheet. This information is in ***Attachment A – PAC 2024 Annual Report Data*** on the tab called "Third Party Data Sharing". Any time our information is accessed, a log is created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

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

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

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

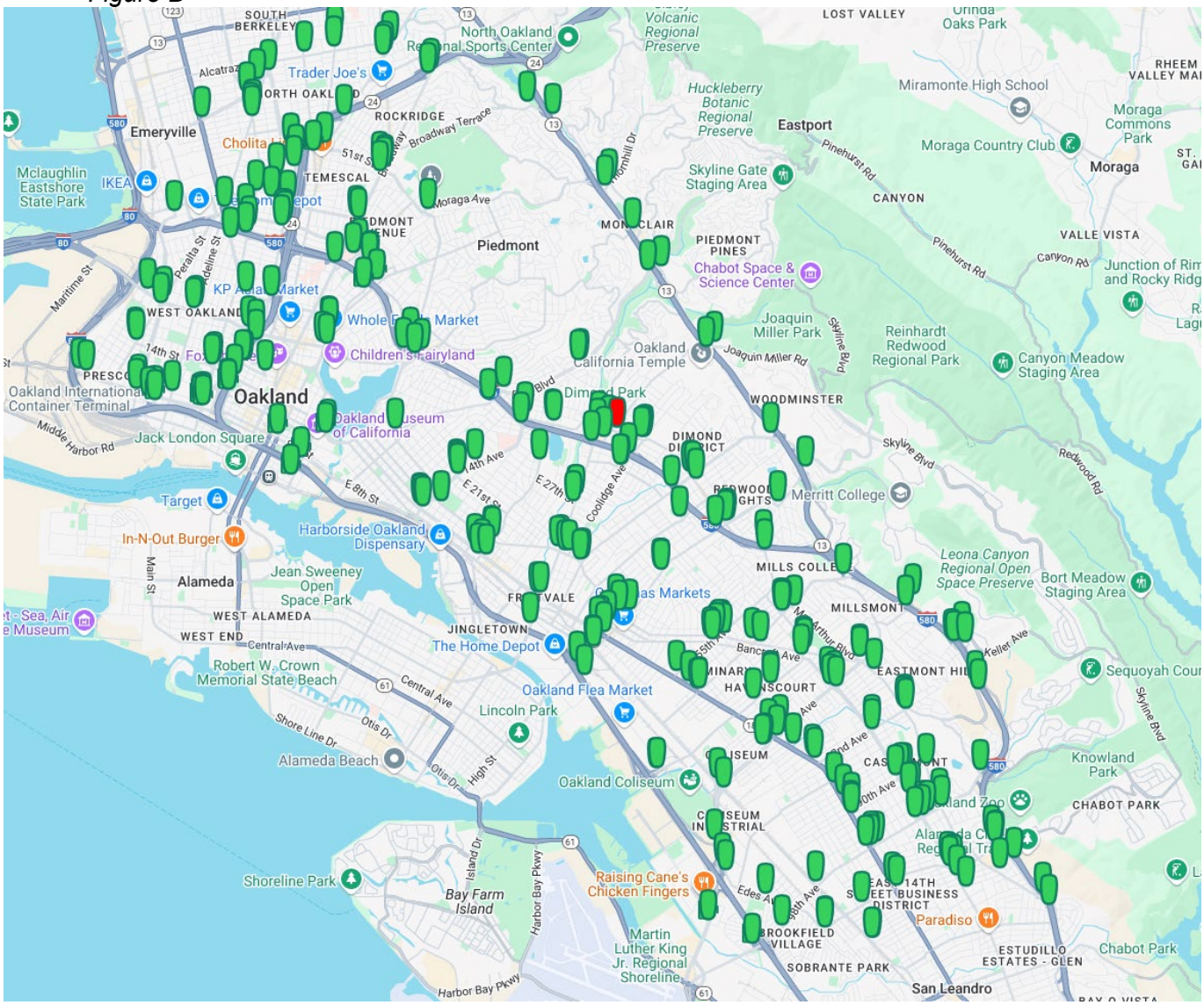
Figure C



C. <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 currently the only source of data, that are OPD assigned, feeding into the Flock system. Further information is provided below in ***Figure D***:

Figure D



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

A total of 290 ALPR cameras were funded and deployed throughout the City of Oakland. There are six geographical policing areas that OPD identifies: Area 1 – Area 6.[1]

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

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

[1] City of Oakland | Oakland Police Areas

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

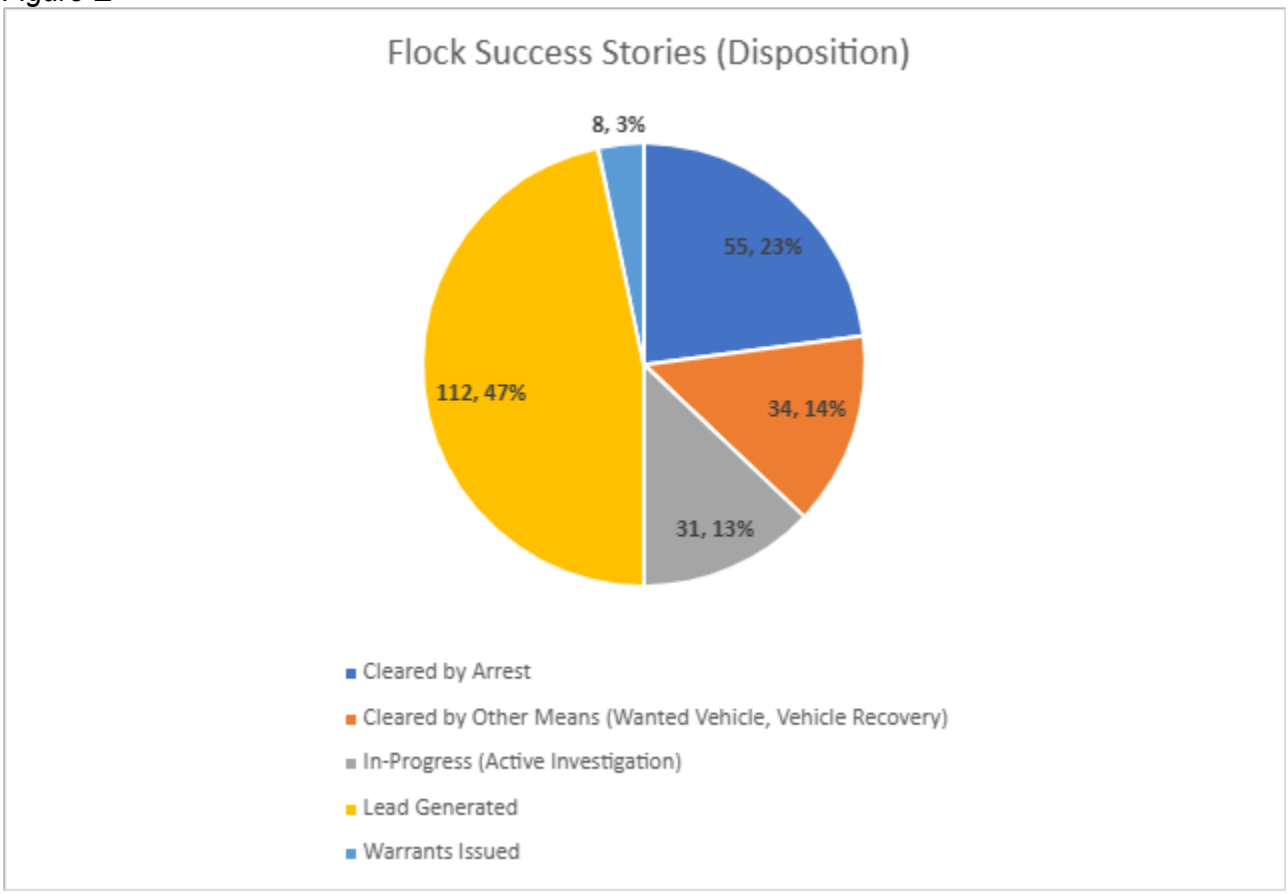
The Oakland Police Department reached out to Flock and on January 14th, 2025, received a response from Flock attesting that "Flock did not suffer any security breaches as it relates to our infrastructure, [or] unauthorized access to data collected by the surveillance technology". The Director of Risk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

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

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

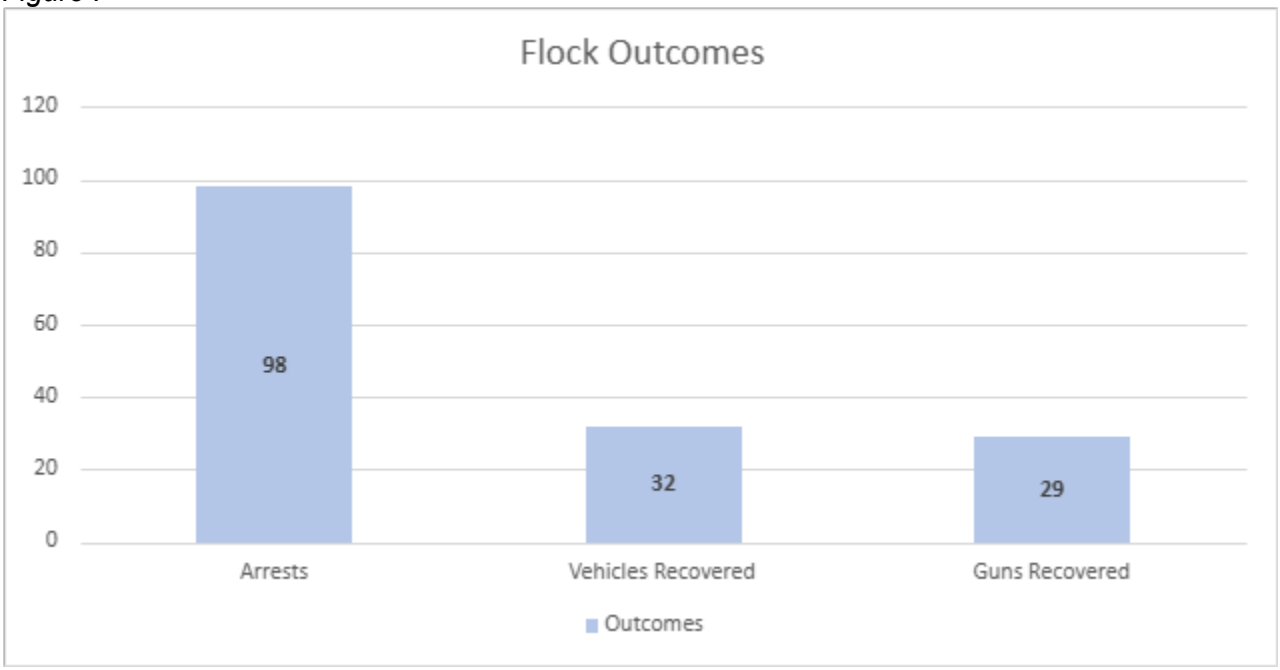
As shown in ***Figure E*** below, OPD logged a total of 240 enforcement actions in Flock from August 2024 through February of 2025. Based on these actions, OPD was able to generate 112 leads, 55 were cleared by arrests, 34 were cleared by other means such as vehicle recovery, 31 are in-progress investigations,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

Figure E



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

Figure F



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

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

Table A

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

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

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

- RD#24-044602: On 06 Sep 24, a robbery occurred in the area of 3315 High St. Surveillance cameras captured the suspect vehicle. Investigators utilized FLOCK technology to help identify recent locations for the suspect vehicle. Within 6 hours, Ceasefire officers and the OPD helicopter located the vehicle and some of the suspects in the act of committing another robbery. The helicopter's presence interrupted that robbery and then followed the suspects throughout the city, eventually arresting two suspects near the Rockridge BART station. Additional suspects were identified and warrants for their arrests have been obtained. This is still an active investigation. The suspects referenced herein are male, adult, Oakland residents.

- RD#24-044939: On 08 SEP 24, around 1830 hours, a road rage incident occurred in the area of 19th Street and Market St. The two involved drivers exited their vehicles and engaged in an argument. One of the two drivers fired a gun towards the other driver. The other driver was not injured. The suspect fled the scene. Nearby surveillance cameras captured images of the suspect's vehicle. Investigators utilized FLOCK technology to alert nearby law enforcement agencies as to the description of the vehicle. On 13 Sep 24, officers with the Newark Police Department located and arrested the suspect based on the alerts disseminated by OPD. The arrestee was a male, juvenile, in possession if a handgun.

- RD# 24-045769: A PC246 (Shooting at a Building) occurred on 12 Sep 24, at about 1824 hours in front of 8501 International Blvd (Allen Temple Baptist Church). Surveillance video captured images of a suspect vehicle. On 14 Sep 24, investigators utilized FLOCK technology to identify a possible match, sharing that information with field units. Within 12 hours, OPD officers had located the suspect vehicle and arrested the driver in possession of a firearm. The driver provided a statement to investigators linking him to the shooting of the Church. The arrestee is a male, adult, Oakland resident.

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

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

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

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

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

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

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

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

OPD has no requests at this time.

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

For any questions with this report, please contact, Dr. Carlo M. Beckman, at cbeckman@oaklandca.gov.

Respectfully submitted,

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

---

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

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

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

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

OAKLAND POLICE DEPARTMENT
Alcohol Tobacco and Firearms (ATF)
2024 Annual Report

OPD ATF Taskforce

The OPD ATF Taskforce supports firearm related investigations. The firearm investigations are often associated with Crime Guns identified through the National Integrated Ballistic Information Network (NIBIN), unserialized firearms (Ghost Guns), Convicted Felons in possession of firearms and the tracing or tracking of firearms through E-Trace. The Taskforce also provides OPD CID with access to forensic resources to support investigations involving gun violence in Oakland. The Taskforce also provides resources to the OPD Crime Gun Intelligence Center (CGIC). OPD CGIC utilizes the National Integrated Ballistic Information Network (NIBIN), which provides crucial intelligence about firearms related crimes committed in Oakland and the San Francisco Bay Area. ATF Special Agents and OPD Taskforce Officer/s frequently respond to assist several Bay Area Law Enforcement Agencies and the Oakland Police Department to conduct investigations of individuals or groups who victimize Oakland residents. The Taskforce also supports the Ceasefire program in the adoption of State firearm cases involving repeated violent Felons identified through Ceasefire.

Staffing

1. Number of full and part time OPD officers assigned to ATF Task Force: One full-time Officer. One full-time NIBIN analyst is currently assigned to OPD to assist with analytical data related to NIBIN Investigations.
2. Number of hours worked as ATF Task Force Officer: Regular 40 hours per week. However, the current task force officer remains flexible and can be assigned to other OPD operations based on OPD needs and priorities and whether there are active investigations.
3. Funding source for ATF Task Force Officer salary: OPD Budget – funded by OPD General Purpose Fund. Overtime related to ATF OPD Taskforce investigations are funded by OPD.

Other Resources Provided

1. **Communication equipment:** ATF handheld radio, cellular phone & computer monitors.
2. Surveillance equipment: GPS Trackers and Pole Cameras (ATF owns and installs utility pole cameras which are utilized in some cases. A court order with judicial approval is required prior to any installation.)
3. Clerical/administrative staff hours: NIBIN Analyst: Regular 40 hours per week.
4. **Funding sources for all the above:** ATF Budget.

Cases

1. **Number of cases ATF Task Force Officer was assigned to:** 17– a breakdown of these cases provided below:

    - ATF was notified of a subject selling firearm. This subject utilizes social media as a means listing his firearms for sale. After a long thorough investigation, a search warrant was authored. During the executing of the warrant, it was discovered that the subject would post fake photos and did not have any firearms at his residence.
    - ATF investigated the trafficking of firearms. After several CI buy operations, it was determined that the firearms were being purchased and transported from Arizona. The investigation led to multi-agency take down which led to the arrest of several subjects.
    - ATF investigated the trafficking of firearms out of the Stockton area. Several operations were conducted to purchase these firearms. The arrest of these subjects is still pending.
    - ATF Oakland assisted Stockton PD with a firearms investigation case. The case yielded one arrest.
    - The ATF Oakland investigated several subjects involved in trafficking firearms in the bay area. The case is still ongoing but has already yielded more than 10 firearms.
    - ATF Oakland and US Marshalls conducted surveillance and executed a search warrant for a murder suspect in Oakland.
    - Oakland ATF along with Ceasefire conducted an operation to locate and arrest several subjects who were wanted in connection to a series of burglaries. Oakland ATF executed 2 search warrants and recovered several evidence.
    - CGIC notified the Oakland ATF office about a subject who was the primary aggressor in a shooting. A federal warrant was authored and executed. The subject was arrest under federal charges. The case is currently pending in federal court.
    - Oakland ATF assisted the NY division on a trafficking case. The Oakland ATF executed a warrant in the city of Concord and recovered several key pieces of evidence for the NY division.
    - Oakland ATF assisted the US Marshalls with the execution of a warrant. The structure was a duplex. During the search ATF was able to locate a suspect hiding in the attic and take him into custody without further incident.
    - US Marshalls and Oakland ATF collaborated in locating and arresting a subject who had been arrested several times this year in possession of a firearm. The subject resisted arrest but was ultimately detained and arrested. The subject was found to have a firearm on their possession. Due to several factors, the subject was charged federally.
    - Oakland ATF is in constant communication with the OPD homicide division regarding active unsolved murders. These cases often have evidence that require the assistance of ATF lab.

2. Number of "duty to warn" cases: None
3. General types of cases: Firearms investigations, NIBIN/CGIC investigations and Federally adopted State firearm cases.
4. Number of times the ATF asked OPD to perform/OPD declined to perform: None.
a. Reason for OPD declination (e.g. insufficient resources, local/state law): N/A

Note: When criteria is met for federal charging, consideration is provided to ATF through task force or officer.

Operations

1. Number of times use of undercover officers were approved: 0
2. Number of instances where OPD Task Force officer managed informants: 0
3. Number of cases involving informants that ATF Task Force Officer worked on: All cases except adopted cases from local .
4. Number of requests from outside agencies (e.g. ICE) for records or data of OPD: None.
a. Number of such requests that were denied: N/A
b. Reason for denial: N/A
5. Whether ATF Task Force Officer was involved in any cases where USPER (U.S. person status) information was collected: No.

Training and Compliance

1. Description of training given to ATF Task Force Officer by OPD to ensure compliance with Oakland and California law: The OPD officer assigned to the ATF Task Force follows all OPD policies and has received several trainings, including but not limited to: continual professional training, Procedural Justice Training and annual firearms training. The officer has also reviewed all provisions of the ATF Task Force MOU which is still pending.
2. Date of last training update: Continuous Professional Training, 2024. Monthly training and quarterly training.
3. Frequency with which ATF Task Force Officer briefs OPD supervisor on cases: Weekly

Actual and Potential Violations of Local/State Law

1. Number of actual violations: OPD will provide information on law and/or policy violations that are in connection with an officer's task force work, and subject to release under California's Public Records Act, Government Code section 6254 (the "PRA") and/or Cal. Penal Code 832.7. Disclosure of violations not connected to task force work is outside the scope of OMC 9.72. Disclosure of violations beyond those mandated or permitted by statute to be disclosed would violate the prohibition on disclosing personnel or other confidential records set forth in Cal. PC 832.7 & 832.8OPD will provide information on violations that are subject to release under California's Public Records Act (the "PRA"), Government Code section 6254. Release of any of violations not covered by the PRA, however, would violate California law (832.7), as there is only one officer assigned to this task force. There were no actual violations.
2. Number of potential violations: None.
3. Actions taken to address actual or potential violations: The officer follows OPD policies. OPD leadership consults with the Office of the City Attorney to ensure that all policies conform to State and Federal laws.
4. Recommendations by OPD to address prevention of future violations: OPD will continue to consult with the Office of the City Attorney to ensure that personnel continue to follow federal, state, and local laws and policies. Going forward, they will consult on a biannual basis. OPD will also consult with the Privacy Advisory Commission about any proposed changes.

Suspicious Activity Reports (SARs) and Northern California Regional Intelligence Center (NCRIC)

1. Whether OPD Task Force Officer submits SARs to NCRIC: No
2. Whether OPD officer receives SAR information: No

Command Structure for OPD Task Force Officer

1. Reports to whom at ATF? Resident Agent in Charge (RAC) Dillon Phillips.
2. Reports to whom at OPD? Acting Sergeant Joseph Jochim and Lieutenant Eric Kim and Acting Captain Steve Valle

DEPARTMENTAL GENERAL ORDER

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

Effective Date: XX Nov XX
Coordinator: Bureau of Investigations

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

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

A. Definitions

A - 1. Community Safety Camera

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

A - 2. Operating System

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

A - 3. Video Management System (VMS)

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

B. Description of the Technology

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

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

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

B - 2. Fixed Line of Sight Camera System

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

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

1. Pan: This function allows the camera to rotate horizontally, covering a broad field of view. PTZ cameras can rotate up to 360 degrees, allowing the camera system to replicate the view of a person located in the same position of the camera.

2. Tilt: This feature enables the camera to move vertically. Tilting up and down helps to cover different vertical angles and ensure that both high and low areas can be observed.

3. Zoom: PTZ cameras come equipped with optical zoom lenses that allow you to zoom in on specific objects or areas without losing image quality. This is useful for detailed inspection or the tracking of moving objects.

4. Remote Control: PTZ cameras can be controlled remotely via various interfaces, such as dedicated control panels, computer software, or mobile apps. This flexibility allows operators to adjust the camera's position and zoom level in real time.

C. Purpose of the Technology

OPD accessed CS Camera Systems and associated VMS and Operating Systems are intended to deter criminal activity within specific public areas and enhance the Department's ability to address disruptive criminal activity within the community. These disruptive crimes include theft, vehicle theft, human trafficking, reckless driving, sideshow/takeovers, felony evasion, burglaries, robberies, shootings, and homicides. Many criminal investigations hinge upon the availability and quality of surveillance video as evidence that is later used in the prosecution of criminal cases. While physical surveillance may also accomplish these goals, it is limited due to the financial cost, the availability of resources, and the physical demands upon members of the Department. CS Camera Systems have the capability of enhancing the Department's ability to

address the types of criminal activity that are disruptive within the community while also acting as a resource multiplier within the Department. It is the expressed intent of the Department to use this technology to facilitate informed enforcement on those involved in specific disruptive criminal activities and to mitigate collateral impact upon the community.

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

D. Authorized Uses

D - 1. Authorized Users

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

D - 2. Authorized Use

- **Recording of Public Areas**

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

- **Recording an Area Subject to a Reasonable Expectation of Privacy**

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

- **Recordings During Exigent Circumstances**

  CS Camera Systems may be used during exigent circumstances that include hostage situations, barricaded suspects, kidnappings, and active shooter situations. If a CS Camera System is used for exigent circumstances, a search warrant shall be sought within 72 hours, and the exigent use shall be documented within the annual report and reported to the Privacy Advisory Committee (PAC) and the next available PAC meeting.

E. Restrictions on Use

E - 1. Permitted/Impermissible Uses

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

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

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

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

F. Data Collection

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

G. Data Access

G - 1. General Data Access Guidelines

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

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

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

G - 2. Tiered CS Camera Data Access

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

Real-Time Camera Access – Only specific Department members designated by the CS System Administrator(s) and/or Chief of Police shall have access to Real-time (live) camera access while supporting field operations. Real-time access shall be utilized strictly in the furtherance of an active investigation. The CS System Administrator shall keep a record of Department members who are authorized real-time camera access.

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

- Where a subject(s) is believed to be armed with a weapon capable of inflicting injury.
- Where a subject has demonstrated violent behavior, made threats of violence towards themselves or others, and/or the previous actions of the subject pose a danger to the public, officers, or themselves[1].
- To assist with detaining a subject(s) related to a felony investigation.

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

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

If the owner/controller provides explicit consent by opting in to sharing video data through the VMS and/or FlockOS system, Department members can access historical

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

video data remotely, making the process more efficient for the member and owner/controller of the physical camera system.

Historical Data access shall be documented by recording the following:

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

H. Data Protection

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

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

I. Data Retention

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

All CS Camera System data uploaded to a Video Management System (VMS) owned by the Department shall be purged 90 days from the initial upload. CS Camera System information may be retained outside this retention limit solely for the following purposes:

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

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

J. Public Access

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

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

K - 1. CS Camera System Sharing <u>with</u> Legal Obligation

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

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

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

K - 2. CS Camera System Sharing <u>without</u> Legal Obligation

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

- The requesting party shall have a right to know, and a need to know. A right to know is the legal authority to receive information pursuant to a court order,

statutory law, case law, or sworn officer status. A need to know is a compelling reason to request information such as direct involvement in an investigation.

- The Department shall record the requesting party's name and document the right and need to know the requested information.
- The Department shall record whether the request was honored or denied, the reason for such action, and the name of the Department officer that processed the request.

L. Training

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

Training requirements for employees shall include the following:

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

M. Auditing and Oversight

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

The records of the number of deployments of Department owned CS Camera Systems, Third Party Data Sharing related to Section K – 2 of this Policy, and any exigent use of CS Camera Systems shall be incorporated into the annual report required by O.M.C. 9.64 et seq.

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

N. Maintenance and Administration

N - 1. CS Camera System Administration

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

N - 2. CS Camera System Administrators

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

N - 3. CS Camera System Coordinator:

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

N - 4. Monitoring and Reporting

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

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

By Order of

Floyd Mitchell

Chief of Police Date Signed:

Appendix A

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

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

Surveillance Impact Report

Community Safety Camera Systems – Camera Registry and Department Remote Access to Public/Privately Owned Surveillance Camera Systems

A. Description

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

B. Purpose

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

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

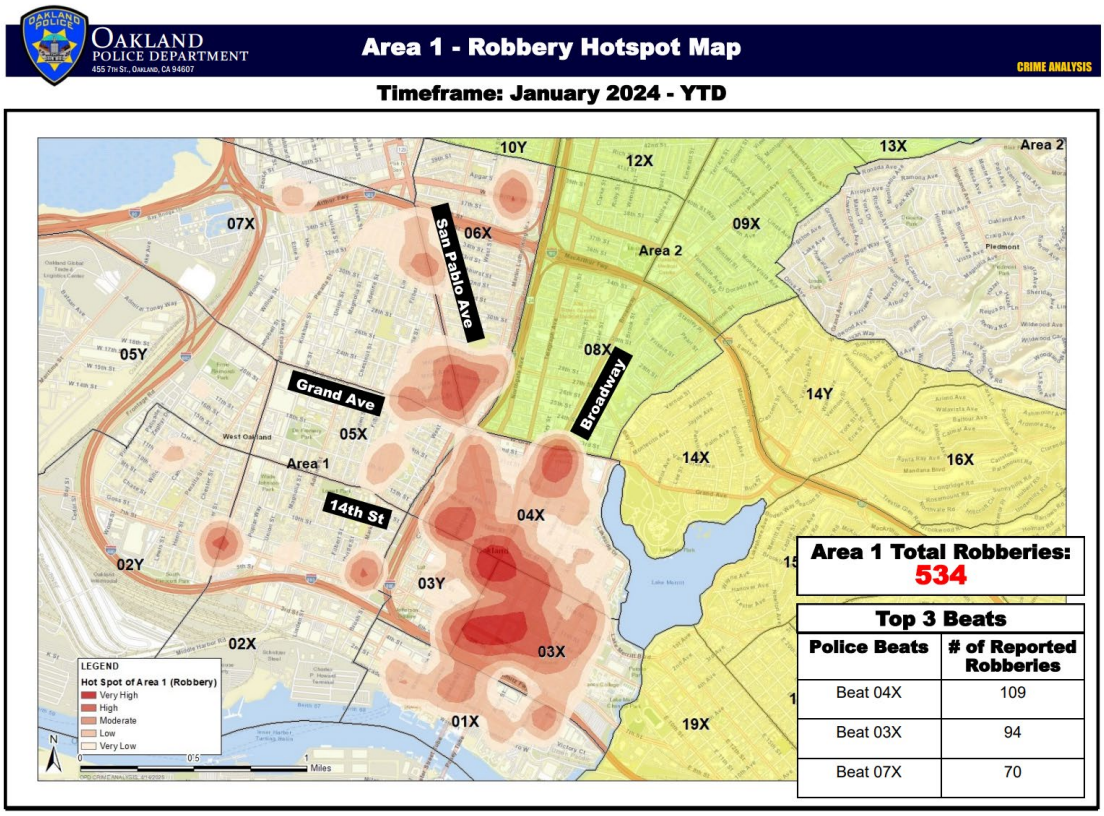
C. Location

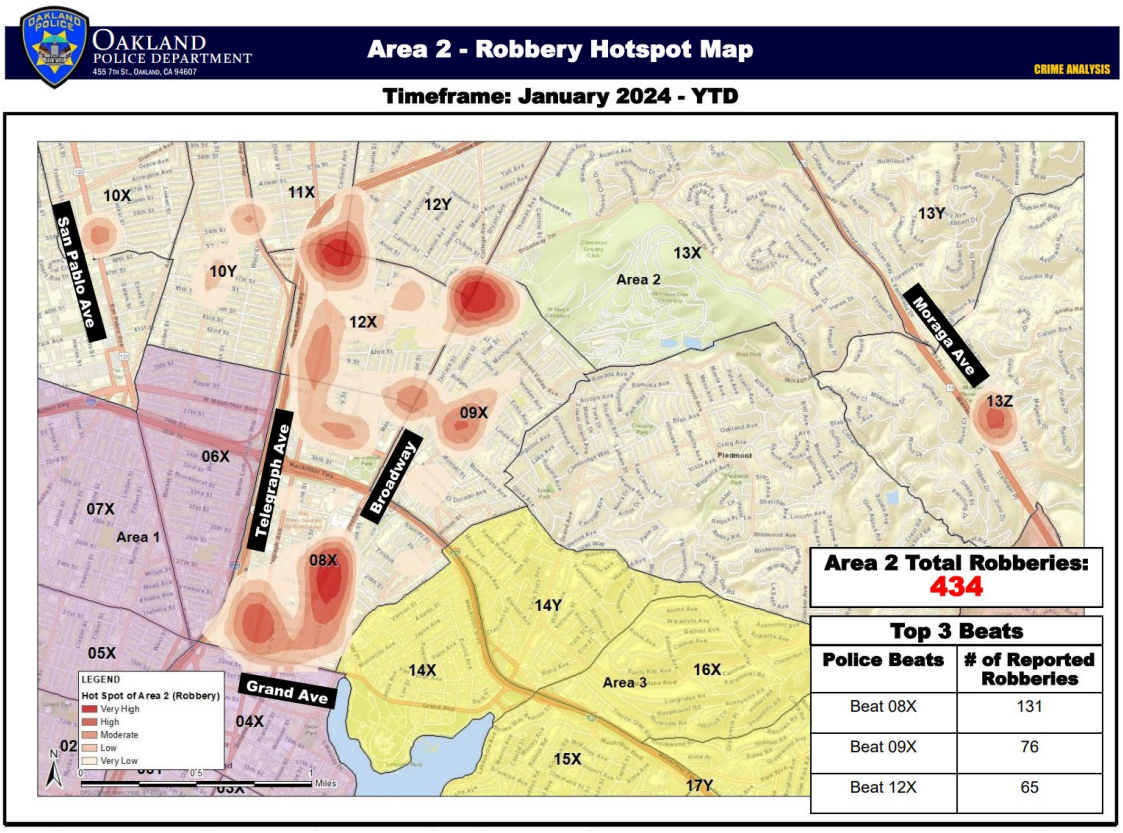
Community Safety Camera Systems will be utilized in areas throughout the City, specifically in business corridors, main thoroughfares, or in areas where violent and/or disruptive criminal activity is occurring (based on crime data analysis).

While specific locations have not yet been identified, the below map shows a general coverage area of proposed initial public/private collaboration areas. This

collaboration program has also been expanded to the Hegenberger/98th Ave business corridor. Department owned/managed devices are intended to be used to supplement existing camera systems, or to be placed in areas where there are not yet public/private collaboration projects. It is the long-term goal of the Department to expand this type of collaboration to additional business corridors impacted by disruptive criminal activity, including but not limited to, The Fruitvale, Laurel, Lakeshore, International, Bancroft, Piedmont Ave, and College Ave business areas.

Included below is a visual representation (hotspot/heatmap) of crime data related to robbery incidents within the same general geographical area (Oakland PD Districts 1 where existing private camera systems exist. The heatmap shows concentrations of robbery events using a spectrum of red color coding, with the dark red representing high concentrations robbery events. The areas with heavy concentrations of robberies shows substantial overlap with the collaborative private camera coverage areas. Similar analysis has been conducted city-wide, but also included burglaries, robberies, and shooting incidents. This analysis will be used to inform future efforts towards expansion of the CS Camera System program.





D. Impact

Community Safety Camera Systems are intended to deter specific criminal activity and to facilitate focused enforcement when necessary. Community Safety Camera Systems will not be utilized with the intent to surveil a person or group based on race, gender, religion, political affiliation, nationality, ethnicity, sexual orientation, disability, or other classification protected by law. Department managed/owned CS Camera Systems will be deployed in areas related to specific criminal activities, informed by crime data, analysis, and investigative knowledge.

E. Mitigations

The CS Camera System policy prohibits the use of CS Camera Systems for, invasion of privacy, harassment or intimidation, based on protected characteristics, in conjunction with facial recognition, personal use, to violate first amendment rights, or to capture audio data (**DGO I-32.1 – Section E-1**). Annual audits related to the use of the technology will be conducted. It is the Department's explicit intention to use this technology in a manner that mitigates collateral impacts upon the community with a focused approach related to subjects involved in specific criminal activity.

CS Camera Systems are intended to initially be used in commercial areas and main thoroughfares throughout the city where existing city and commercial infrastructure exist. The Department will deploy Department owned/managed devices based on crime data, with a focus on violent crime.

F. Data Types and Sources

The CS Camera System captures visual data which is retained along with associated metadata.

G. Data Security

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

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

H. Fiscal Cost

The estimated starting cost for this project is approximately $200,000-300,000 depending on the number of devices purchased by the Department. The devices are intended to integrate into the existing Flock Operating System at a cost of approximately $80,000 per year (requiring an upgrade to Flock OS Elite). The Department will seek funding through grants, donated/provided equipment, or alternative funding (as an alternative to general funds, or to reimburse general funds) to facilitate the initial purchase/acquisition of this technology and the requisite video management systems. Retained data will be stored on an existing platform at no additional cost.

I. Third Party Dependence

The CS Camera Systems will initially rely on vendor or partnering agency assistance related to mobilizing the devices and maintaining them. Retained data will be stored through the existing Evidence.com (Axon), consistent with other stored evidence-related data.

J. Alternatives

Alternatives to the use of this technology would be the use of physical manned surveillance, or manual "canvassing" for video that captures criminal activity, which is costly both in terms of fiscal cost, time, and being physically taxing (and at points potentially dangerous) for Department members. There is also the opportunity to mitigate the need to begin, or continue, a pursuit in areas where a vehicle involved in criminal activity can be observed remotely. In certain circumstances, the location can be determined utilizing this technology, to allow the Department to conduct enforcement in an area that may have less of an impact on uninvolved members of the community.

The CS Camera Systems are meant to act as a force multiplier by using technology to augment or replace physical surveillance by Department members.

K. Track Record

Camera systems similar to CS Camera Systems have been utilized throughout the United States, including in Charlotte (North Carolina), Atlanta (Georgia), and San Francisco. The devices are critical in the prosecution of violent crimes, as they often capture important information of evidentiary value, including capturing, burglaries, robberies, and shootings on video and documenting visual evidence that led to the identification and prosecution of those involved. It should be noted that similar information is already captured by privately owned surveillance devices and VMS systems, which are accessed later by the Department. The current process is time consuming and delays action related to investigations. Evidence is frequently lost or not recovered due to time constraints or being overwritten.

The Oakland Police Department intends to use this technology with a narrow, focused approach to meet the investigatory needs of the Department, while also respecting and safeguarding the privacy rights of the community.

Surveillance Impact Report

Community Safety Camera Systems – Camera Registry and Department Remote Access to Public/Privately Owned Surveillance Camera Systems

A. Description

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

B. Purpose

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

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

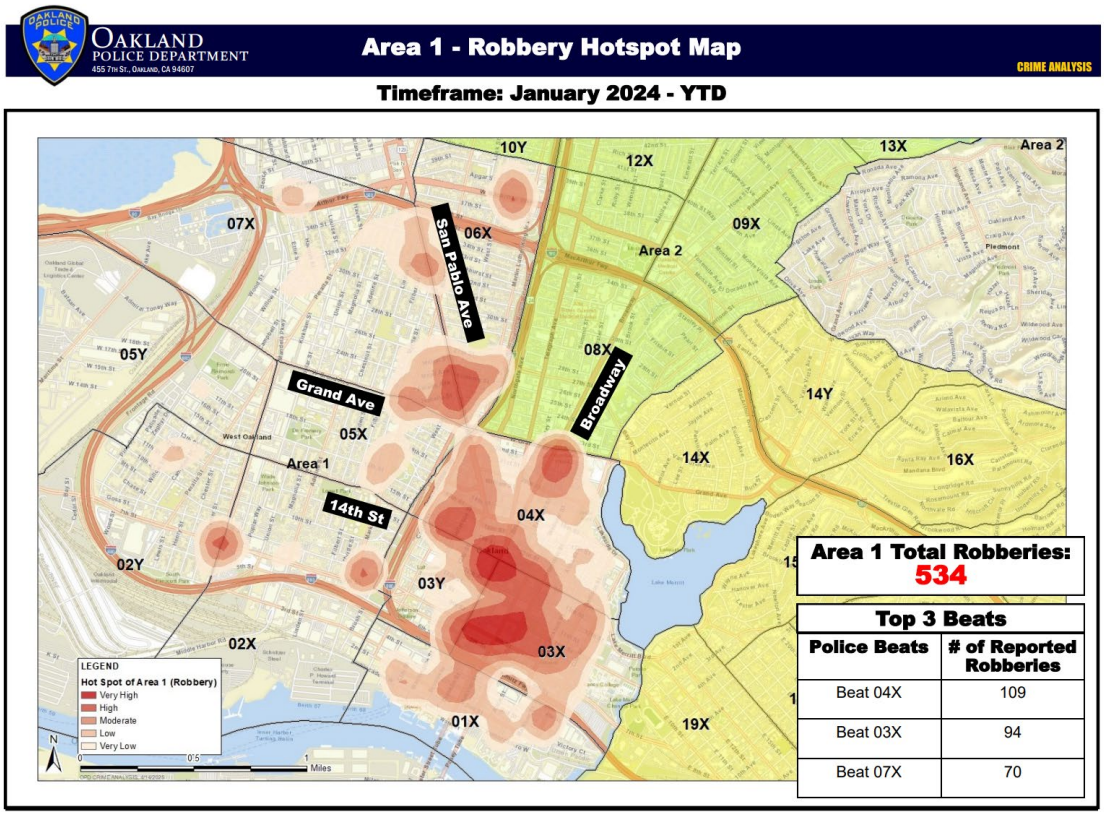
C. Location

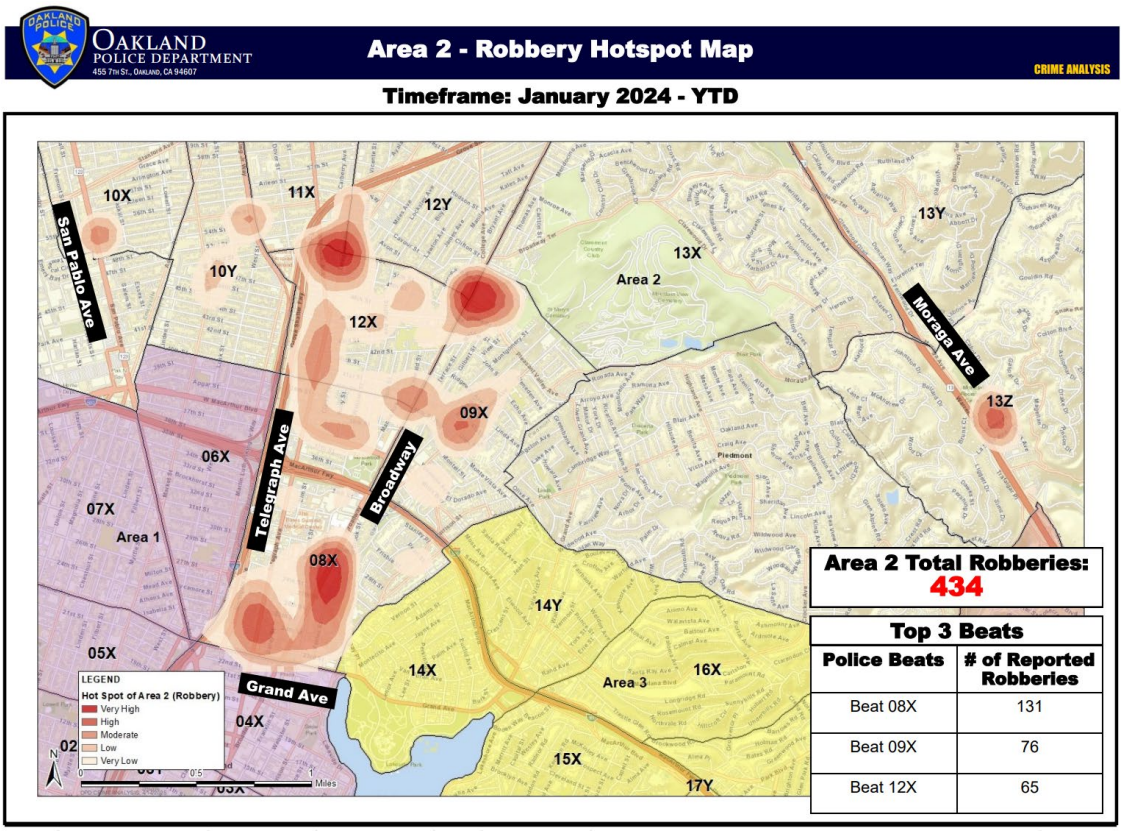
CS Camera Systems will be utilized in areas throughout the City, specifically in business corridors, main thoroughfares, or in areas where violent and/or disruptive criminal activity is occurring (based on crime data analysis).

While specific locations have not yet been identified, the below map shows a general coverage area of proposed initial public/private collaboration areas. This

collaboration program has also been expanded to the Hegenberger/98th Ave business corridor. Department owned/managed devices are intended to be used to supplement existing camera systems, or to be placed in areas where there are not yet public/private collaboration projects. It is the long-term goal of the Department to expand this type of collaboration to additional business corridors impacted by disruptive criminal activity, including but not limited to, The Fruitvale, Laurel, Lakeshore, International, Bancroft, Piedmont Ave, and College Ave business areas.

Included below is a visual representation (hotspot/heatmap) of crime data related to robbery incidents within the same general geographical area (Oakland PD Districts 1), where existing private camera systems exist. The heatmap shows concentrations of robbery events using a spectrum of red color coding, with the dark red representing high concentrations robbery events. The areas with heavy concentrations of robberies shows substantial overlap with the collaborative private camera coverage areas. Similar analysis has been conducted city-wide, but also included burglaries, robberies, and shooting incidents. This analysis will be used to inform future efforts towards expansion of the CS Camera System program.





D. Impact

Community Safety Camera Systems are intended to deter specific criminal activity and to facilitate focused enforcement when necessary. Community Safety Camera Systems will not be utilized with the intent to surveil a person or group based on race, gender, religion, political affiliation, nationality, ethnicity, sexual orientation, disability, or other classification protected by law. Department managed/owned CS Camera Systems will be deployed in areas related to specific criminal activities, informed by crime data, analysis, and investigative knowledge.

E. Mitigations

The CS Camera System policy prohibits the use of CS Camera Systems for, invasion of privacy, harassment or intimidation, based on protected characteristics, in conjunction with facial recognition, personal use, to violate first amendment rights, or to capture audio data (**DGO I-32.1 – Section E-1**). Annual audits related to the use of the technology will be conducted. It is the Department's explicit intention to use this technology in a manner that mitigates collateral impacts upon the community with a focused approach related to subjects involved in specific criminal activity.

CS Camera Systems are intended to initially be used in commercial areas and main thoroughfares throughout the city where existing city and commercial infrastructure exist. The Department will deploy Department owned/managed devices based on crime data, with a focus on violent crime.

F. Data Types and Sources

The CS Camera System captures visual data which is retained along with associated metadata.

G. Data Security

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

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

H. Fiscal Cost

The estimated starting cost for this project is approximately $200,000-300,000 depending on the number of devices purchased by the Department. The devices are intended to integrate into the existing Flock Operating System at a cost of approximately $80,000 per year (requiring an upgrade to Flock OS Elite). The Department will seek funding through grants, donated/provided equipment, or alternative funding (as an alternative to general funds, or to reimburse general funds) to facilitate the initial purchase/acquisition of this technology and the requisite video management systems. Retained data will be stored on an existing platform at no additional cost.

I. Third Party Dependence

The CS Camera Systems will initially rely on vendor or partnering agency assistance related to mobilizing the devices and maintaining them. Retained data will be stored through the existing Evidence.com (Axon), consistent with other stored evidence-related data.

J. Alternatives

Alternatives to the use of this technology would be the use of physical staffed surveillance, or manual "canvassing" for video that captures criminal activity, which is costly both in terms of fiscal cost, time, and being physically taxing (and at points potentially dangerous) for Department members. There is also the opportunity to mitigate the need to begin, or continue, a pursuit in areas where a vehicle involved in criminal activity can be observed remotely. In certain circumstances, the location can be determined utilizing this technology, to allow the Department to conduct enforcement in an area that may have less of an impact on uninvolved members of the community.

The CS Camera Systems are meant to function as a force multiplier by using technology to augment or replace physical surveillance by Department members.

K. Track Record

Camera systems similar to CS Camera Systems have been utilized throughout the United States, including in Charlotte (North Carolina), Atlanta (Georgia), and San Francisco. The devices are critical in the prosecution of violent crimes, as they often capture essential information of evidentiary value, including capturing, burglaries, robberies, and shootings on video and documenting visual evidence that led to the identification and prosecution of those involved. It should be noted that similar information is already captured by privately owned surveillance devices and VMS systems, which are accessed later by the Department. The current process is time consuming and delays action related to investigations. Evidence is frequently lost or not recovered due to time constraints or being overwritten.

The Oakland Police Department intends to use this technology with a narrow, focused approach to meet the investigatory needs of the Department, while also respecting and safeguarding the privacy rights of the community.