CITY OF OAKLAND

Privacy Advisory Commission

June 1, 2023 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**: Chloe Brown, **District 3 Representative**: Brian Hofer, Chair, **District 4 Representative**: Lou Katz, **District 5 Representative**: Omar De La Cruz, **District 6 Representative**: Gina Tomlinson, **District 7 Representative**: Robert Oliver, **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.

1. Call to Order, determination of quorum

2. Review and approval of the draft April 15 meeting minutes

3. Open Forum/Public Comment

4. Sanctuary Contracting Ordinance – CPO – Presentation of Annual Report
    a. Review and take possible action

5. Surveillance Technology Ordinance – OPD – Annual Reports
    a. Review and take possible action on the annual reports for ShotSpotter, Unmanned Aerial Vehicles/Drones, StarChase/GPS Tracker, Biometric Crime Lab

6. Surveillance Technology Ordinance – DPW – Illegal Dumping Cameras 1) Annual Report, and 2) Proposed Amended Use Policy
    a. Review and take possible action on the annual report and use policy

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 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.

Each person wishing to speak on items must fill out and submit a speaker's card to staff prior to the meeting. Members of the public can address the Privacy Advisory Commission in-person only and shall state their names and the organization they are representing, if any.

To observe the meeting via Zoom, go to: https://us02web.zoom.us/j/83505090768
Or One tap mobile: +1 669 900 9128

CITY OF OAKLAND

Privacy Advisory Commission

April 15, 2023; 9:00 AM
Oakland City Hall
Hearing Room 3
1 Frank H. Ogawa Plaza, 1st Floor
Special Meeting Minutes

***Commission Members**: **District 1 Representative**: Reem Suleiman, **District 2 Representative**: Chloe Brown, **District 3 Representative**: Brian Hofer, Chair, **District 4 Representative**: Lou Katz, Vice Chair **District 5 Representative**: Omar De La Cruz, **District 6 Representative**: Gina Tomlinson, **District 7 Representative**: Robert Oliver, **Council At-Large Representative**: Henry Gage III **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.

1. Call to Order, determination of quorum

2. IAPP Conference Report Back –by Felicia Verdin

   Felicia Verdin, Assistant to the City Administrator provided an update on the IAPP Global Privacy Summit that was held April 1-4 in Washington, DC.

3. Role of Chief Privacy Officer – by Joe DeVries
   a. Incorporating into existing PAC framework
   b. Succession/resource needs

Deputy City Administrator Joe DeVries provided an update on the role of the Chief Privacy Officer to track Privacy policies and train city staff on impact statements and use polices.

Mr. DeVries discussed the need to create internal administration instructions on Privacy requirements to memorialize city policies and procedures, as an example there is an internal working group that created an inclusive community engagement policy. A memo can also be written to brief city departments on the template for use policies and impact statements. All policies must have all the components before it is

presented to the PAC. Training on the surveillance ordinance and other privacy policies can also be conducted through citywide training.

It was determined that an ad-hoc needs to be created to further clarify the role of the Chief Privacy Officer and its connection to the Chief Security Officer in the Department of Information and Technology, in addition to discussing other internal City of Oakland policies and practices.

4. Community Engagement Strategy
    a. Remote Presentation by Hector Dominguez – City of Portland
    b. Discuss elements needed for successful engagement

Hector Dominquez presented a PowerPoint and discussed the City of Portland's success with engaging the community in their privacy work.

Questions were raised regarding their budget, participation, outreach. There were additional questions asked about how public comment was gathered. All funding was provided by the City of Portland. Business associations were engaged through their chamber and other community partners participate in their privacy work. There are also a group of privacy champions that are in engaged in Portland's privacy efforts.

5. Impact Assessment/Threat Matrix - by Kelsey Finch – see her PowerPoint
    a. Presentation and training

Kelsey Finch, senior associate, privacy and data protection with Aleada Consulting presented information about a range of topics pertaining to privacy. She discussed the involvement of privacy forums to create

peer connections and information sharing, including the need for an enterprise data management approach.

Ms. Finch also discussed the need for community engagement and bringing in diverse voices. Get people from the community on the team. She provided an example of how Long Beach created digital equity surveys to involve the community.

She explained that on the government side we can do a better job of articulating potential harms by creating better scenarios of the need for privacy policies and programs. Ms. Finch indicated that this can be done by providing real actual examples of emotional distress, for example. It would be helpful to review Privacy Impact Assessment (PIA) in the federal government and look at what problems are trying to be resolve specifically.

She discussed the steps of a Privacy Risk Assessment to create processes, templates an instructions and create contingency plan. Furthermore, Ms. Finch discussed the need for transparency and accountability to build public trust. She also discussed smart data management and the need for sustainable.

6. Surveillance Ordinance Training – by Chair Hofer

Chair Hofer engaged the Commission and staff in an exercise on impact statements and proposed use policies.

7. PAC Needs – by Chair Hofer

Chair Hofer led a discussion of potential funding request to further support the work of the PAC to engage the community.

CITY OF OAKLAND

Privacy Advisory Commission

April 15, 2023; 9:00 AM
Oakland City Hall
Hearing Room 3
1 Frank H. Ogawa Plaza, 1st Floor
Special Meeting Minutes

He also discussed the need for succession planning in the PAC and the impact of upcoming term limits and the need for an annual election. Appointments take place at the end of March. Chair Hofer indicated that his term ends 2025 and he wants to be chair one more year. He expressed his interest to set up the next generation of PAC members in a good way. He also suggested that a few different vice chairs could serve in the role over a year long period.

There was a discussion about Infrastructure needs and systems to track due dates, policies, and policy writing. Logigate was a mentioned as a possible system.

There is a desire by the PAC to better engage with City Departments outside the scope of existing ordinances (Privacy Principles, general data collection and security practices, public facing materials).

Additionally, an ad-hoc could be formed to improve the information that the PAC provides publicly in the following areas:

- Website improvements
- Social media presence
- Process to receive complaints or inquiries from the public
- Notice to stakeholders for community engagement (staff was requested to email the PAC with Neighborhood Council information, including the beat locator).

CITY OF OAKLAND

Annual Report

TO: Privacy Advisory Commission

FROM: Joe DeVries, Chief Privacy Officer

SUBJECT: Impact of Implementing, Tracking and Reporting Ordinance N.O. 13540 C.M.S. - Sanctuary City Contracting and Investment Ordinance

DATE: May 25, 2023

Executive Summary

The Sanctuary City Contracting and Investment Ordinance (Ordinance N.O. 13540 CMS) was adopted by the City Council in June 2019 and requires that by April 1 of each year, the City Administrator shall certify compliance with this ordinance by preparing a written report. By May 1 of each year, the City Administrator shall submit to the Privacy Advisory Commission a written, public report regarding compliance with Sections 2.23.030 and 2.23.040 over the previous calendar year.

At minimum, this report must (1) specify the steps taken to ensure implementation and compliance with Sections 2.23.030 and 2.23.040, (2) disclose process issues, and (3) detail actions taken to cure any process deficiencies. After receiving the recommendation of the Privacy Advisory Commission, if any, the City Administrator shall schedule and submit the written report to the City Council for review and adoption.

Background

The Sanctuary City Contracting and Investment Ordinance prohibits the City from contracting with any person or entity that provides the United States Immigration and Customs Enforcement (ICE), United States Customs and Border Protection (CBP), or Department of Health and Human Services Office of Refugee Resettlement (HHS/ORR) with any "Data Broker", "Extreme Vetting", or "Detention Facilities" services unless the City Council makes a specific determination that no reasonable alternative exists. The ordinance also prohibits the City from investing in any of these companies and requires the City to include notice of these prohibitions in any Requests for Proposals (RFPs), Requests for Qualifications (RFQs), and any construction or other contracting bids.

As is the case in many government entities, the City uses its existing competitive (non-construction services) procurement processes to require compliance with federal, state and local mandates relative to the use of public funds in the purchase of goods and service. For example,

in the late 1980's the City adopted a policy to prohibit doing business with entities that also contract with companies involved in nuclear arms proliferation. In 2013, the City took a stand against contractors doing business with the State of Arizona due to its adoption of legislation that unfairly targeted persons of Hispanic decent in routine traffic stops.

The Sanctuary City Contracting and Investment Ordinance is a response to efforts implemented during the previous presidential administration by ICE, including its efforts to target Sanctuary Cities with stepped up enforcement efforts and the impact those efforts have had on the Oakland community. There has been strong local interest in these types of ICE raids and deportations both politically and in the media, however, ICE has taken much more drastic steps to gather data on individuals that could ultimately be far more impactful.

Ensuring Compliance

"Schedule I"

The Sanctuary City Contracting and Investment Ordinance (Ordinance N.O. 13540 CMS) is promulgated through "Schedule I" as attached. Any entity wishing to contract with the City of Oakland must self-certify with the Schedule I that they do not have any contracts with ICE, CBP, or HHS/ORR. The Schedule I is submitted along with other contract schedules to the Department of Workplace and Employment Standards (DWES). Staff forward copies of all received Schedule I's to the Chief Privacy Officer. If any contractor cannot self-certify, then a further review of the proposed contract will occur to determine if there are grounds for a waiver.

During the reporting period:

There were no City of Oakland contractors who declined to sign the Schedule I and seek a waiver.

Disclosure of Process Issues

There were no negative process issues during this reporting period and based on past performance, staff believe the disclosure process is working well.

Actions Taken to Cure Deficiencies

There were no identified deficiencies in this reporting period to cure.

Investment Prohibitions

The CPO provided the list of prohibited contractors to the Department of Finance to ensure no new investments are made in any of these firms moving forward. As noted during the development of the ordinance, most of the City's investments are in bonds and there are strict guidelines on how a municipality can invest its dollars. Department of Finance agreed to check

the list of prohibited entities on a semi-annual basis. The Department reported that in the year 2022, no investments in the prohibited entities were made.

Respectfully submitted,

Joe DeVries,
Chief Privacy Officer

For questions, please contact Joe DeVries, Chief Privacy Officer, at (510) 238-3083.

CITY OF OAKLAND

MEMORANDUM

TO: Darren Allison, Interim Chief of Police

FROM: Drennon Lindsey, Deputy Chief OPD, Bureau of Investigations

SUBJECT: OPD Crime Lab Biometrics DNA Analysis Technology 2022 Annual Report

DATE: June 1, 2023

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 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. In 2022, 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.

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

2022 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 2022

The Forensic Biology Unit analyzed 310 requests between January 1, 2022 to December 31, 2022. Over 1,900 items of evidence were examined, from which 4,044 samples were subjected to digestion and extraction using the Versa and EZ1 instruments. Scientist subjected 4,094 samples to quantitation analysis using the SpeedVac, Qiagility, and QuantStudio 5 instruments and 1,671 samples were subjected to amplification and typing methods using the ProFlex and 3500 instruments. The DNA profiles were processed with GMIDX or 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 25 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.

A CODIS cloud-based server location is under evaluation as a replacement for the server in the PAB. The details of this location and security would be handled under the auspices of the City of Oakland ITD policy and procedure and would meet or exceed industry standard for handling of secure servers.

NOTE: The use of the term "secure servers" throughout this report is on the basis of 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.

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:

Staff reached out to each City Council office to ask about possible community complaints or concerns related to this surveillance technology. No community complaints or concerns were communicated to staff. 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. There were no identifiable data breaches or unauthorized access during the year 2022.

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 310 requests in 2022. These are further broken out by crime type in **Table 1** below:*

Table 1: OPD Crime Laboratory DNA Analysis Requests in 2022

Crime Type	**Number of Requests**
Homicide	99
Attempted Homicide	5
Rape	97
Other Sexual Assault (not rape)	24
Assault	29
Robbery	9
Burglary	6
Carjacking	4
Hit and run	1
Auto Theft	1
Weapons	29
Other Person	1
Other Criminal	3
Control Substance	2
Total	**310**

CODIS hits in 2022 – One hundred and forty-three DNA profiles were uploaded to the CODIS database. The laboratory had two hundred and twenty-seven associations (hits); eighty-two hits to named individuals whose identity was unknown, eleven hits to unsolved forensic cases, and sixty-four 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 analysis.

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 cost / benefit analysis in the form of Return on Investment (ROI) calculations place the societal cost of each homicide at $10,000,000 and a return seen of $135[1] per dollar spent on violence reduction. Similarly, economic studies show that investigating sexual assaults results in $81[2] saved per dollar spent.

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 (x3 instruments = $189,000) and $2,990 to maintain; 3 instruments for $8,970 annual*
- *EZ2: $61,250 to purchase (x2 instruments = $122,500 and $3,959 to maintain; 2 instruments for 7,918 annual maintenance*
- *Versa 1100: $85,000 to purchase and $5,000 annual maintenance*

DNA Quantitation

- *Qiagility: $33,100 to purchase (x3 instruments = $99,300) and $3,433 to maintain; 3 instruments for $10,308 annual maintenance*
- *QuantStudio 5: $57,000 to purchase (x2 instruments = $114,000) and $6,280 to maintain; 2 instruments for $12,560 annual maintenance*

DNA Normalization / Amplification

SpeedVac: $4,000 to purchase, no maintenance

[1] Abt, Thomas (2019). Bleeding Out: The devastating consequences of urban violence—and a bold new plan for peace in the streets. Chapter 11, p. 208.
[2] Wang and Wein (2018) Journal of Forensic Sciences, Analyzing Approaches to the Backlog of Untested Sexual Assault Kits in the USA, July 2018, Vol. 63, No. 4, pp. 1110-1121.

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

DNA Typing
3500: $135,000 to purchase, $11,550 annual maintenance

DNA Interpretation
STRmix: $66,000 to upgrade, $31,830 annual maintenance
FaSTR: $37,000 to purchase, $8,000 annual maintenance
ArmedExpert: $15,000 to purchase, no maintenance

The cost of testing reagents/kits was approximately $131,000; however, this does not include consumables such as scalpels, masks, gloves, plastics, slides nor serological test kits.

Total purchase cost (born over several years): $894,800
Total maintenance cost, 2022: $96,136
Total testing cost reagents/kits, 2022: $131,000
Estimate of consumables: $140,000

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

The 2022 approved Surveillance Impact report (SIR) and Biometric Technology Use Policy (SUP) were reviewed. Updates of like-for-like instrument improvements (specifically EZ1 platform upgraded to EZ2 previously disclosed) and annual costs are included. Language about ITD role in securing data was added to both the SIR and SUP similar to the note at the end of paragraph C above. There are no requests to substantively modify the Use Policy outside of this.

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 about this report, please contact Dr. Sandra Sachs, Criminalistics Laboratory Manager, at ssachs@oaklandca.gov.

Respectfully submitted,

_____

Reviewed by:
Drennon Lindsey
Deputy Chief, Bureau of Investigations

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

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

Patrick Paton, Quality Assurance Supervisor
OPD, Criminalistics Laboratory

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

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

Oakland Police Department Criminalistics Laboratory
DNA Instrumentation and Analysis Software
Biometric Technology Use Policy
June 2023

1. Purpose

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.

The technology within the scope of this Biometric Technology Use Policy includes:

Digestion / Extraction

- **Aurora Biomed**: Versa 1100 liquid handler instrument and VERSAware software for automated cell digestion and microscope slide preparation.
- **Qiagen:** EZ1 Advanced XL instrument, EZ2 instrument and Investigator Protocol (Software) for extraction and purification of DNA.

DNA Quantitation

- **Qiagen:** QIAgility Liquid Handler Robots and computers for rapid, high-precision automated PCR setup (also used for Normalization/Amplification and DNA Typing).
- **Applied Biosystems**: QuantStudio 5 Real Time PCR systems and QuantStudio 5 System Detection Software for determination of quantity and quality (degradation level) for a DNA sample.

DNA Normalization / Amplification – STR (autosomal and Y)

- **ThermoFisher Scientific**: SpeedVac DNA Concentrator for concentrating low quantity DNA samples.
- **ThermoFisher Scientific**: ProFlex Thermalcyclers for PCR amplification of STR DNA fragments.

DNA Typing – STR (autosomal and Y)

- **ThermoFisher Scientific**: Applied Biosystems 3500 Series Genetic Analyzer and Data Collection Software is designed for data collection in human identification (HID) applications. The Crime Laboratory uses/intends to use this software to collect STR DNA data from amplified samples. This software normalizes genetic data and creates "hid" files to be used by data processing (FaSTR) and interpretation (ArmedXpert, STRmix) software.

DNA Interpretation – STR (autosomal and Y)

- **NicheVision**: FaSTR software is used for review and evaluation of sizing and genotyping data generated from the genetic analyzers. This analysis software can be configured to set analysis parameters, edit raw data, and aids to prepare data for further interpretation into DNA profiles.
- **NicheVision**: ArmedXpert Analysis Software is used for streamlined DNA typing interpretation resulting in reduced time spent on DNA mixture interpretation. It also uses published and validated population DNA allele frequencies to calculate DNA profile frequency estimates to aid in providing the weight of any inclusion comparison drawn between an evidence sample and a known reference.
- **NicheVision**: STRmix™ software combines established and validated biological modelling and complex mathematical processes to use a continuous model to interpret a wide range of complex DNA profiles. It can compare these DNA profiles to a reference profile and calculate the weight of the comparison using well established Likelihood Ratio statistics.

DNA Databasing

- **HP**: Server for the Combined DNA Index System (CODIS) and peripheral computers used to enter and search evidence DNA profiles against legally obtained reference samples (Convicted Offenders, Arrestees, Missing Persons) and other evidence profiles.

The forensic evidence analyzed by the Forensic Biology Unit develops biometric data, however, the Department does not use it in a surveillance capacity (prospectively), it uses it to solve crimes that have already occurred (retrospectively).

The Forensic Biology/DNA Unit focuses most analytical efforts on violent crimes. Homicides and most sexual assault crimes do not have a statute of limitations. The unit analyzes a wide range of other crime types: robberies, burglaries, thefts, assault, weapons, which may have statute of limitations; however, legal enhancements of penalties (for example 209 PC, aggravated kidnapping) exist, so a 211 PC can be enhanced to a life sentence. It is not the purview of the laboratory to determine the legal status of cases. Laboratory-generated evidence may be used in criminal or civil proceedings. Federal Rules of Civil Procedure 37(e) imparts a duty to preserve potentially relevant evidence including electronically stored information (ESI) for civil trials.

2. Authorized Use

The DNA instrumentation and analysis software described above shall be used primarily on evidence or reference samples submitted by law enforcement and collected pursuant to a search warrant, other legal means, or by documented consent. The DNA instrumentation and analysis software shall be used solely for aiding in criminal or civil investigations; for validating new methods and for special projects designed to evaluate improvements to the forensic DNA collection and analysis process, collecting data for statistical studies or lecture presentations; and for quality assurance purposes. To the latter, reference samples from Crime Laboratory staff members, staff family members, interns, and OPD personnel who

have access to evidence from crime scenes, property storage areas, or the operational areas of the Crime Lab may be processed using the DNA instrumentation and analysis software. This is necessary as a part of the chain of processes used to develop DNA profiles to measure or detect a contamination event in the unit, should it occur. All other uses are prohibited.

The DNA instrumentation and analysis software shall not be used for personal, non-law-enforcement-related purposes; and shall not be used to surveil, harass, intimidate, or discriminate against any individual or group. The Criminalistics Division and Forensic Biology/DNA unit each maintain manuals [Laboratory Operations and Quality Assurance Manual (LOQAM) and standard operating procedures (SOP)] to which all Forensic Biology/DNA unit staff train annually and are required to adhere. LOQAM and the Forensic Biology/ DNA unit SOPs provide rules and procedures on what elements shall be present in a validation study, data and conclusions from validation studies performed, rules on conducting research and any published results. Failure to follow these rules and procedures may result in discipline.

3. Data Collection

The data collected attests to the purity or amount of the DNA and usually also contains genetic information, specifically STR DNA marker alleles (types) that collectively constitute a forensic DNA profile that has the potential to characterize or identify a single individual. (Note: identical twins typically have identical forensic DNA profiles, since they are derived from a single fertilized egg, or zygote).

The Forensic Biology unit maintains an in-house Quality Control (QC) database. The QC database contains DNA profiles obtained from the following sources:

1. by consent from OPD staff (current and past) and their family members.
2. OPD personnel that may enter the chain of custody for an evidence item or has other contact within the scope of the case,
3. Samples provided by accredited proficiency test providers. The samples are anonymized by the test provider; the test providers are subject to strict confidentiality requirements by the accrediting bodies. The laboratory has no access to the source of these samples.

The purpose and use of the QC database is twofold: 1) for casework quality control checks to ensure that the process worked correctly (positive control) and 2) to determine if there is possible contamination from a known individual to a casework sample. At this time, there are no victim references in the QC database. Such profiles have never been, nor are they allowed to be, used for the identification of an individual in a criminal matter. Further clarification: no victim DNA profiles can be entered or used in the QC database.

4. Data Access

Criminalists and Forensic Technicians with duties in the Forensic Biology/DNA unit shall be the only Crime Laboratory personnel authorized to use the DNA instrumentation 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 DNA instruments or software in casework. Criminalists and Forensic Technicians are granted access to one another's cases only for the purpose of discovery or CPRA requests, documenting quality checks, verifications or peer review. Interns also are authorized to use the DNA instrumentation and analysis software for special projects, not casework, and only after receiving necessary training and under the supervision of a qualified Criminalist.

5. Data Protection

All data generated using the DNA instrumentation and analysis software shall be securely maintained at all times in a limited access location, or on a secure server*. To evaluate and interpret the DNA analytical data, authorized personnel shall only use computers on secure network drives.

* The Laboratory's remote server, which hosts network drives, is secure because it is physically under lock and key and limits electronic access to current laboratory staff and ITD personnel. Additionally, a separate local server is secured by lock and key during business and after hours, alarm after hours and by running the server on a dedicated intranet line that uses encryption on both the sender and receiver ends of any communication from/to the server. NOTE: The use of the term "secure servers" or "secure network" throughout this Use Policy 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.

6. Data Retention

There is no statute of limitations on most of the cases the Forensic Biology/DNA unit analyzes. For crime types that do have statute of limitations, penalty enhancements may make it such that a decision to impose a life sentence may be rendered and civil duty to preserve ESI and electronic evidence exists; therefore, data are retained indefinitely on secure server or network drives. No hard drive leaves laboratory custody without ensuring that all sensitive data has been removed and is irretrievable from the device. Hard copies of case files containing the laboratory report, notes, and instrument printouts are similarly retained indefinitely under Crime Lab control with secure, limited-access areas, or at a Departmentally approved Records Retention facility. Retained data may be used if questions pertaining to the case in question arise, or if an investigation into a quality issue arises and is documented in Incident Response.

7. Public Access

Members of the public shall have no direct access to the DNA instrument data generated. If requested under the California Public Records Act (CPRA), the Crime Lab shall deny the request on the ground that such data is exempt from disclosure under the investigative exemption (Government Code section 6254(f), (k) and 6255), Evidence Code Section 1040 and perhaps other exemptions, unless and until they are made publicly available in criminal proceedings. If such a CPRA request is made or if a subpoena or court order is issued for such DNA instrumentation and analysis data, the data shall be made public or deemed exempt from public disclosure pursuant to state or federal law, after consultation with the Oakland City Attorney's Office as needed. Criminal defendants are entitled access to the data via third-party data-sharing described in the next section.

8. Third-Party Data-Sharing

Following the completion and review of a specific case, the case file and data are disseminated only to the law enforcement customer and/or City Attorney and/or prosecuting attorney and assisting staff. The material shall be subject to discovery in criminal or civil proceedings and is the means by which criminal defendants are entitled to obtain a copy of the casefile and the data contained therein. The case file and data (including copies) shall not be shared with anyone else without a court order. In addition, crime scene samples that qualify for search in the California State DNA Index System (SDIS) and National DNA Index System (NDIS) (components of the Combined Index System or CODIS database), are uploaded to SDIS according to the NDIS Operational Procedures Manual (https://www.fbi.gov/file-repository/ndis-operational-procedures-manual.pdf/view). Suspect DNA profiles that qualify for search are uploaded to SDIS pursuant to California Penal Code 297.

Accessing data collected by the Forensic Biology/DNA unit requires either a right to know or a need to know. A right to know is the legal authority to receive information pursuant to a court order, statutory law, or case law (covered in Section 4. Data Access). A need to know is a compelling reason to request information such as being the OPD Investigator assigned to the case for which DNA analysis has been requested.

Forensic Biology/DNA data may be shared only with other law enforcement agencies based on a need to know and a right to know, or as otherwise required by law, using the following procedures:

1. The agency makes a written request for the Forensic Biology/DNA data that includes:
   a. The name of the requesting agency.
   b. The name of the individual making the request.
   c. The need for obtaining the information.

2. The request is reviewed by the Bureau of Investigation Deputy Chief or designee and is approved before the request is fulfilled.

3. The approved request is retained on file, and shall be included in the annual report

9. Training

Forensic Technicians and Criminalists in the Forensic Biology/DNA unit shall complete a comprehensive training program and shall not embark on any casework with the DNA instrumentation and analysis software until they have successfully taken a relevant qualifying test. Once qualified, they shall take proficiency tests bi-annually. Interns shall be authorized to use the DNA instrumentation and analysis software for special projects, and not casework, only after receiving necessary training and under the supervision of a qualified Criminalist. Criminalists, Forensic Technicians, and interns in the Forensic Biology/DNA unit shall be provided with a copy of the DNA instrumentation and analysis software Biometric Technology Use Policy. The Crime Lab Manager and Criminalist IIIs are responsible for providing oversight of the training program, ensuring comprehension of policies and documenting adherence.

10. Auditing and Oversight

The Forensic Biology/DNA unit is overseen by two supervisors and by Crime Lab upper management (Crime Lab Manager and Quality Supervisor), all of whom shall oversee compliance with this Biometric Technology Use Policy and Standard Operating Procedures via Administrative and Quality Reviews of casework, policy updates and annual Internal Audits. Additionally, the Crime Lab is accredited by the American National Standards Institute (ANSI) National Accreditation Board (ANAB), which provides oversight to the operation of the Forensic Biology Unit. The Crime Lab is assessed by ANAB on an annual basis. Moreover, the Forensic Biology/DNA unit complies with the Federal Bureau of Investigation (FBI)'s Quality Assurance Standards (QAS) for Forensic DNA Testing Laboratories. The Forensic Biology unit is audited to the FBI's QAS annually, alternating internal and external audits.

11. Maintenance

The mechanism to ensure the security and integrity of the tools, instrumentation and data are insured by oversight provided by the Forensic Biology/DNA unit Supervisors and upper management as defined in the "Auditing and Oversight" section above.

Oakland Police Department Criminalistics Laboratory
DNA Instrumentation and Analysis and Software
Surveillance Impact Report
June 2023

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

Digestion / Extraction

- Three EZ1 Advanced XL DNA purification instruments and software are in the laboratory; the cost of one new instrument is approximately $63,000. Currently, two EZ2 DNA purification instruments have had grant funds identified for purchase. The current ongoing annual upkeep of the instrument is approximately $3,100 per instrument.
- One Versa 1100 liquid handler instrument is in the laboratory; the cost of one replacement instrument is approximately $85,000. The annual maintenance cost is approximately $6,800 per instrument.

DNA Quantitation

- Three Qiagility liquid handler instruments are in the laboratory; the cost of one replacement instrument is approximately $33,100. The annual maintenance cost is approximately $2,700 per instrument.
- Two QuantStudio 5 Real-Time PCR DNA quantitation instruments are in the laboratory; the cost of two new replacement instruments is $114,000. The current ongoing annual upkeep of both instruments is approximately $10,200.

DNA Normalization / Amplification

- One SpeedVac concentrator is in the laboratory; the cost of one replacement instrument is approximately $4,000. No annual maintenance cost.
- Two ProFlex thermal cyclers are in the laboratory; the cost of one replacement ProFlex instrument is approximately $14,000. No annual maintenance cost.

DNA Typing

- One 3500 genetic analyzer; the cost of which was $135,000. The annual maintenance cost is approximately $6,000.

DNA Interpretation

- STRmix upgrade cost $66,000; annual maintenance costs run ~$12,000 annually
- FaSTR cost approximately $37,000.
- Armed Expert acquisition cost approximately $15,000

Grants, Proposition 69 funds, and Operations and Maintenance budgets have historically covered these costs.

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: Darren Allison,
Interim Chief of Police

FROM: Anwawn Jones, Sergeant
OPD, Intel Unit

SUBJECT: Cellular Site Simulator – 2022 Annual Report

DATE: May 2023

Background

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

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

Oakland Police Department (OPD) Department General Order (DGO) I-11: Cellular Site Simulator (CSS) Usage and Privacy, requires that OPD provide an annual report to the Chief of Police, the Privacy Advisory Commission (PAC), and Public Safety Committee. The information provided below is compliant these annual report requirements.

***The technology has reached its lifespan and is unusable. The company stopped building the machines.

2021 Data Points

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

The Cell Site Simulator Surveillance (CSS) Impact report explains that, "Cellular site simulators, as governed by this policy, function by transmitting as a cell tower. In response to the signals emitted by the simulator, cellular devices in the proximity of the simulator identify it as the most attractive cell tower in the area and thus transmit signals to the simulator that identify the device in the same way that they would a networked tower.

CSS receives signals and uses an industry standard unique identifying number assigned by a device manufacturer or cellular network provider to distinguish between incoming signals until the targeted device is located. Once the cellular site simulator identifies the specific cellular device for which it is looking, it will obtain the signaling information relating only to that particular phone, rejecting all others.

The authorized purposes for using CSS interception technology and for collecting information using that technology to:

a. Locate missing persons
b. Locate at-risk individuals
c. Locate victims of mass casualty incidents
d. Assist in investigations involving danger to the life or physical safety of an individual
e. Apprehend fugitives

The technology was not used in 2022.

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):

DGO I-11 does provide that OPD may share CSS data with other law enforcement agencies that have a right to know and a need to know[1], such as an inspector with the District Attorney's Office. However, no CSS data would be downloaded, retained, or shared. No data was generated or shared with any agency because it was not actually used in 2022.

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:

CSS is not attached to fixed objects.

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

CSS was not utilized anywhere in the City in 2022.

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

[1] DGO I-11 explains that a right to know is the legal authority to receive information pursuant to a court order, statutory law, or case law.

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

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

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

There were no uses in 2022 and thus no need for any audits. There were no policy violations.

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

There were no identifiable data breaches or unauthorized access during the year of 2022.

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

Tech was not used in 2022.

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

There are no existing or new public records requests for the 2022 calendar year.

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.

Zero ($0.00). OPD did not incur any maintenance, licensing, or training costs.

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.

Respectfully submitted,

Drennon Lindsey, Deputy Chief
OPD, Bureau of Investigations

Reviewed by,
Roland Holmgren, Captain
OPD, Violent Crimes Operations Center

Prepared by:
Anwawn Jones, Sergeant
OPD, Intel Unit

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

CITY OF OAKLAND

MEMORANDUM

TO: Darren Allison,
Interim Chief of Police

FROM: Eriberto Perez-Angeles, Captain
OPD, Bureau of Investigations

SUBJECT: Pursuit Mitigation System (StarChase) – 2022 Annual Report

DATE: May 25, 2023

Background

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

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

Oakland Police Department (OPD) Department General Order (DGO) I-22: Pursuit Mitigation System requires that OPD provide an annual report to the Chief of Police, the Privacy Advisory Commission (PAC), and Public Safety Committee. The information provided below is compliant with the annual report policy requirements of DGO I-22 as well as OMC 9.64.040.

Acting Captain Rosin, Bureau of Field Operations I, Area 2, is currently the Pursuit Mitigation System Coordinator.

DGO I-22 explains that "StarChase," a private company, manufactures and supports its Pursuit Mitigation GPS Tag Tracking System. The "StarChase" system is a pursuit management technology that contains a miniature GPS tag and a launcher mounted in a police vehicle.
The GPS Tag and Track Launcher System are comprised of a less-than-lethal, dual barrel GPS launcher which contains two GPS Tags (1 per barrel) mounted in the vehicle grille or on a push bumper. The launcher is equipped with compressed air and an eye-safe laser for assisting with targeting before launching the GPS Tag.

2022 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:

GPS Tag technology was not deployed in 2022.

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):

GPS Tag technology was not deployed in 2022.

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:

n/a

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

GPS Tag technology was not deployed in 2022.

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

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

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

There were no audits as the technology as GPS Tag technology was not deployed in 2022.

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

There were no identifiable data breaches or unauthorized access during the year of 2022.

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

GPS Tag technology was not deployed in 2022.

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

There were no public records requests (open or closed) related to GPS Tag technology in 2022.

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:

GPS Tag technology was not deployed in 2022 and there were zero costs.

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

No requests for changes at this time.

OPD is committed to providing the best services to our community while being transparent and instilling procedural justice through daily police activity. This report is compliance with these OPD commitments as well as the reporting requirements of OMC 9.64.040. OPD hopes that this report helps to strengthen our trust within the Oakland community.

Respectfully submitted,

_____

Reviewed by,
Drennon Lindsey, Deputy Chief
OPD, Bureau of Investigations

Eriberto Perez-Angeles, Captain
OPD, Bureau of Investigations

Prepared by:
Tracey Jones, Police Services Manager
OPD, Research and Planning Section

CITY OF OAKLAND

MEMORANDUM

TO: Darren Allison, Interim Chief of Police

FROM: Drennon Lindsey, Deputy Chief OPD, Bureau of Investigations

SUBJECT: Live stream transmitter– 2022 Annual Report

DATE: May 4, 2023

Background

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

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

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

Sergeant Ann Pierce is currently the Live Stream / Video Team Program Coordinator.

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

OPD did not used the livestream transmitter technology in 2022

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

No data was collected with this technology in 2022

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

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

The live stream transmitters were not deployed in 2022.

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.

This technology was not used in 2022.

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

There was no usage of the technology in 2022.

- Technology was properly stored with the OPD Information Technology Unit (ITU).
- OPD is not aware of any policy violations from use of the live stream transmitters in 2022.

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

There were no identifiable data breaches or unauthorized access during the year of 2022.

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

N/A

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

There were no PRRs regarding this technology in 2022.

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

$11,500 for cellular connectivity.

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

No requests for changes at this time.

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

Respectfully submitted,

_____

Drennon Lindsey, Deputy Chief
OPD, Bureau of Investigations

Reviewed by,
Roland Holmgren, Captain
OPD, Violent Crimes Operations Center

Prepared by:
David Pullen, Officer
OPD, Bureau of Services, Information Technology Unit

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

CITY OF OAKLAND

MEMORANDUM

TO: Darren Allison, Interim Chief of Police

FROM: Drennon Lindsey, Deputy Chief OPD, Bureau of Investigations

SUBJECT: Mobile Fingerprint ID– 2022 Annual Report

DATE: May 4, 2023

Background

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

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

The City Council adopted Resolution 88095 C.M.S. on April 7, 2020 which approved the OPD Mobile ID Surveillance Use Policy as well as the Surveillance Impact Report.

OPD does not currently possess any Mobile Identification Devices (MID)s and there was zero (0) MID usage by OPD in 2022. The Alameda County Sheriff's Office (ACSO), the lead sponsor of the MID program, is currently upgrading the devices with technology provider. OPD will appoint an internal MID Coordinator when OPD is able to receive and deploy upgraded units.

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

   OPD did not possess nor deploy MIDs in 2022.

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):

   There was no usage and no data generated in 2022.

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:

MIDs are not attached to any fixed objects.

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

OPD did not deploy MIDs anywhere in the City in 2022.

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

There were no community complaints or concerns.

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

There was no usage of MIDs and no data or usage to audit.

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

There were no identifiable data breaches or unauthorized access during the year of 2022.

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

Non applicable based on zero usage.

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

There were no PRRs regarding this technology in 2022.

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:

There was no MID usage and no cost to OPD.

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

No requests for changes at this time.

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

Respectfully submitted,

_____

Drennon Lindsey, Deputy Chief
OPD, Bureau of Investigations

Reviewed by,
Roland Holmgren, Captain
OPD, Violent Crimes Operations Center

Prepared by:
David Pullen, Officer
OPD, Bureau of Services, Information Technology Unit

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

CITY OF OAKLAND

MEMORANDUM

TO: Darren Allison, Interim Chief of Police

FROM: Trevelyon Jones, Captain, Ceasefire Section

SUBJECT: Gunshot Location Detection System (ShotSpotter) – 2022 Annual Report

DATE: May 25, 2023

Background

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

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

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

2022 Data Details

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

From the "Surveillance Impact Use Report for the Gunshot Location Detection System:"

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

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

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

ShotSpotter technology was used in the following ways/with the following outcomes in 2022:

- The number of times ShotSpotter technology was requested: ShotSpotter alerted OPD to 7,562 unique gunshot incidents from January 1 – December 31, 2022. Of those alerts**, 7,481 (99%) were not called in by the community as a 415GS call type (shots fired),** and OPD would not have known about them nor have been able to respond in a timely fashion. This information is based on an analysis of calls within 15 minutes and 1,000 feet of a ShotSpotter alert.
- ShotSpotter led police to **199 shooting cases, 28 of which were Homicide and 171 were Assault with a Firearm.** OPD was able to provide and coordinate immediate emergency medical response on these shooting cases; OPD personnel believe that several of these victims survived the shootings specifically because of the quick response and subsequent medical attention. In some instances, OPD and medical response occurred within less than two minutes of the ShotSpotter activation. The ShotSpotter alert was within 10 minutes and 1,000 feet of the location where the victim was found. Furthermore, staff believe that there were many more cases where OPD responded to activations and found shooting victims – and where critical medical attention was provided. The 199 cases cited here (171 injury cases) are the ones where OPD and ShotSpotter staff can conclusively cite the response to the ShotSpotter activations.
- ShotSpotter activations led OPD to **162 cases where their vehicle and/or dwelling was hit by gunfire. Of these 162 cases, 71 victims were present but not hit by gunfire, and 91 were listed as victims because the property belonged to them.**
- 1,789 crime incident reports (24% of total activations)
  - 1,252 (70%) of these incidents resulted in OPD Crime Lab requests for further firearm forensic analysis.
- ShotSpotter provided the following additional reports in relation to specific ShotSpotter activations:
  - **Eleven detailed forensic reports**
  - **Court preparation for seven cases**
  - **Investigative Lead Summary 1,181**

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

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

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

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

DGO I-20 Section B – 1. "Authorized Use" states:

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

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

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

1. The agency makes a written request for the ShotSpotter data that includes:
   a. The name of the requesting agency.
   b. The name of the individual making the request.
   c. The need for obtaining the information.
2. The request is reviewed by the Bureau of Services Deputy Chief/ Deputy Director or designee and approved before the request is fulfilled.
3. The approved request is retained on file and shall be included in the annual report. There were no outside agency ShotSpotter data requests for OPD in 2022.

OPD investigators in the Criminal Investigations Division and or other sections of OPD such as the Ceasefire Section and Violent Crime Operations Center regularly communicate with personnel from other law enforcement agencies on interjurisdictional investigations; these forms of collaboration may involve discussions related to shootings where OPD became informed from ShotSpotter activations. ShotSpotter activations many times may lead to evidence gathering (e.g., finding bullet casings); OPD may share information about evidence (e.g., that bullet casings were found in a particular area at a particular time). For prosecutorial purposes, OPD investigators may provide ShotSpotter data to be included with

the investigative criminal case packet as relevant evidence to the District Attorney's Office as part of the case charging process and/or discovery.

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

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

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

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

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

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

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

OPD is not able to provide the race of each person connected to each activation since shooting suspects are often unknown. Many times, there is data regarding the race of

shooting victims or witnesses (may be self-reported); however, this data is not captured in the same system as ShotSpotter and the administrative burden (7,562 total 2022 activations) to constantly connect the two disparate datasets would overwhelm staff capacity. OPD therefore recommends that the PAC makes the determination, that the administrative burden in collecting or verifying this information as well as the associated potential greater invasiveness in capturing such data outweighs the benefit.

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

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

OPD officers have automatic access to ShotSpotter notifications when in patrol vehicles equipped with standard vehicle computers via the ShotSpotter Respond System. ShotSpotter creates a log for every sign-in to their system, which includes the level of access the user has (admin view or dispatch view, which is notification only). OPD and ShotSpotter have verified that for 2022, all users who logged into the system were authorized users.

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

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

There were no identifiable data breaches or unauthorized access during the year of 2022.

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

Table 1: ShotSpotter Activations Resulting in Incident Report for Firearm Crimes by Category in 2022

Cases by Firearm-Related Crime Type	
Homicide	28
Assault with a Firearm	171
Shoot at an Occupied Home/Vehicle	71
Shoot at an Unoccupied Home/Vehicle	91
Negligent Discharge of a Firearm	1,363
Weapons Violations (including exhibit/draw)	11
Carjacking with a Firearm (including attempts)	4
Robbery with a Firearm (including attempts)	19
Total Cases	**1,758**

Table 2: Firearm Recoveries in 2022 Connected to ShotSpotter Activations illustrate Guns Recovered

Guns Recovered by Crime Type	
Homicide	12
Assault with a Firearm	19
Shoot at an Occupied Home/Vehicle	2
Shoot at an Unoccupied Home/Vehicle	0
Negligent Discharge of a Firearm	38
Weapons Violations (including exhibit/draw)	9
Carjacking with a Firearm (including attempts)	1
Robbery with a Firearm (including attempts)	1
Other	1
Total Cases	**83**

- 83 weapons seized.
  - Note: more than one firearm may be from the same incident.
- 967 alerts when advanced situational awareness was provided to responding patrol officers on their way to crime scenes in high danger situations that required specific approach tactics such as multiple shooters**,** high capacity or automatic weapons being used, and drive-by shootings. Some of the alerts had more than one situational awareness tag amounting to 1,230 tags within those 967 alerts.

Table 4: Cases Where ShotSpotter Notifications Resulted in Firearm-Related Crimes being written

Cases by Firearm-Related Crime Type	
Homicide	28
Assault with a Firearm	171
Shoot at an Occupied Home/Vehicle	71
Shoot at an Unoccupied Home/Vehicle	91
Negligent Discharge of a Firearm	1,363
Weapons Violations (including exhibit/draw)	11
Carjacking with a Firearm (including attempts)	4
Robbery with a Firearm (including attempts)	19
Total Cases	**1,758**

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

There were 25 total PRR in 2022. 20 are closed and *4 remain open.

22-1338
22-2190
22-3599
22-3757
22-4463
22-5180
22-5665
22-6018
22-6019
22-6625
22-6900
22-6911
22-7134
*22-7709
*22-8250
22-8789
22-8850
22-9599
22-9600
*22-9601
*22-9602
22-9774
22-9775

22-9776
22-9777

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:

Total paid in 2022 was $798,486 for 18.17 square miles of coverage. These fees encompass all services ShotSpotter currently provides to Oakland. There are no additional charges for meetings, reports, analysis and training. These funds come from OPD's General Purpose Fund.

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

No requests for policy changes at this time.

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

For any questions with this report, please contact Trevelyon Jones, Captain, OPD, Ceasefire Section, at tjones@oaklandca.gov

Respectfully submitted,

Trevelyon Jones

_____

Trevelyon Jones, Captain, OPD, Ceasefire Section

Reviewed by,
Drennon Lindsey,
Deputy Chief, Bureau of Investigations

Steve Valle, Lieutenant
OPD, Criminal Investigations Division

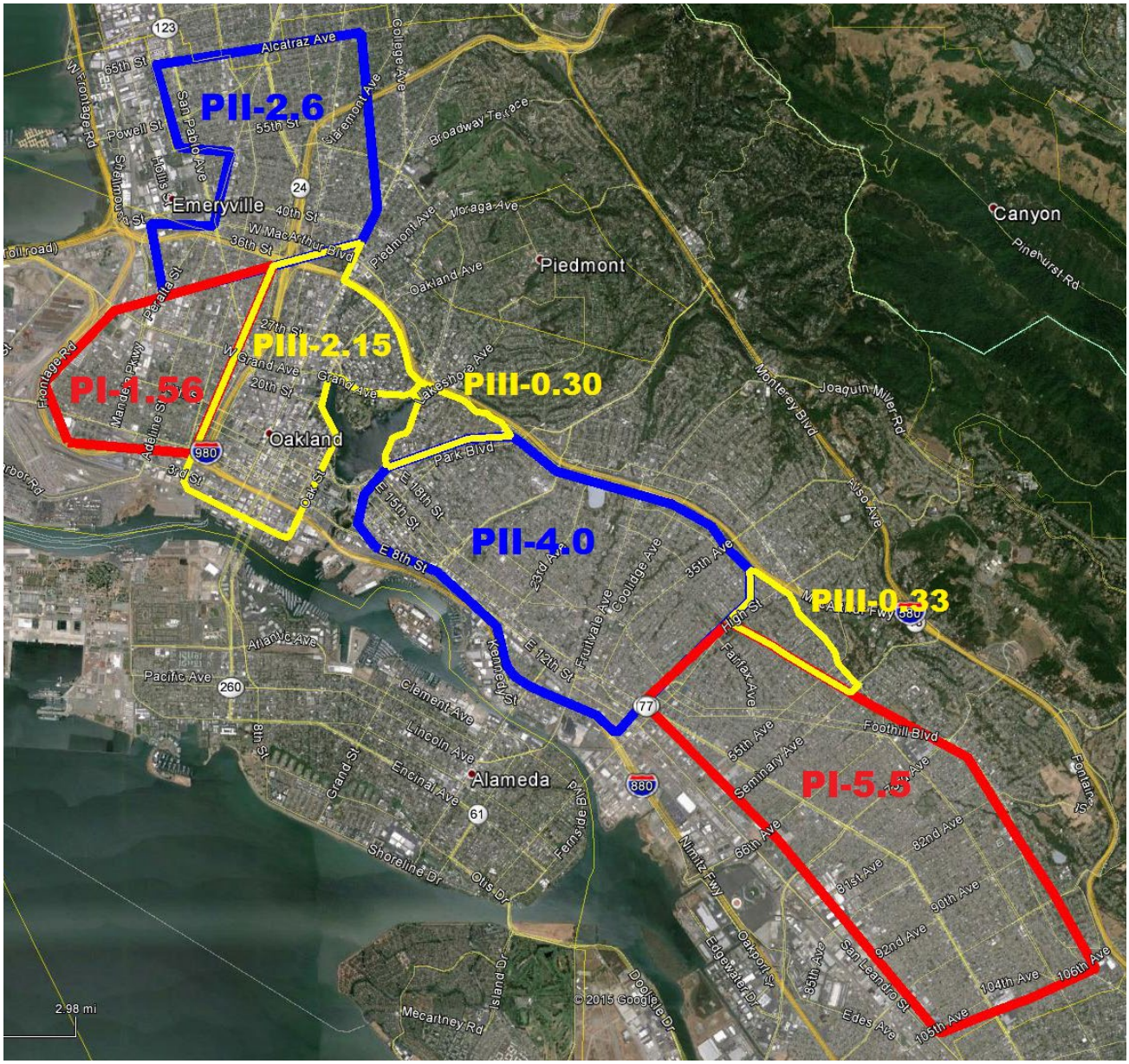
Prepared by:
Tracey Jones, Police Services Manager
OPD, Bureau of Services

Attachment A - Shot Spotter Coverage Areas

Phase I with red borders (Activated in 2006): 6.~~2~~ 0 square miles*
East Oakland: East of High Street to 106th Avenue
West Oakland: East of Highway 980 to Frontage Road

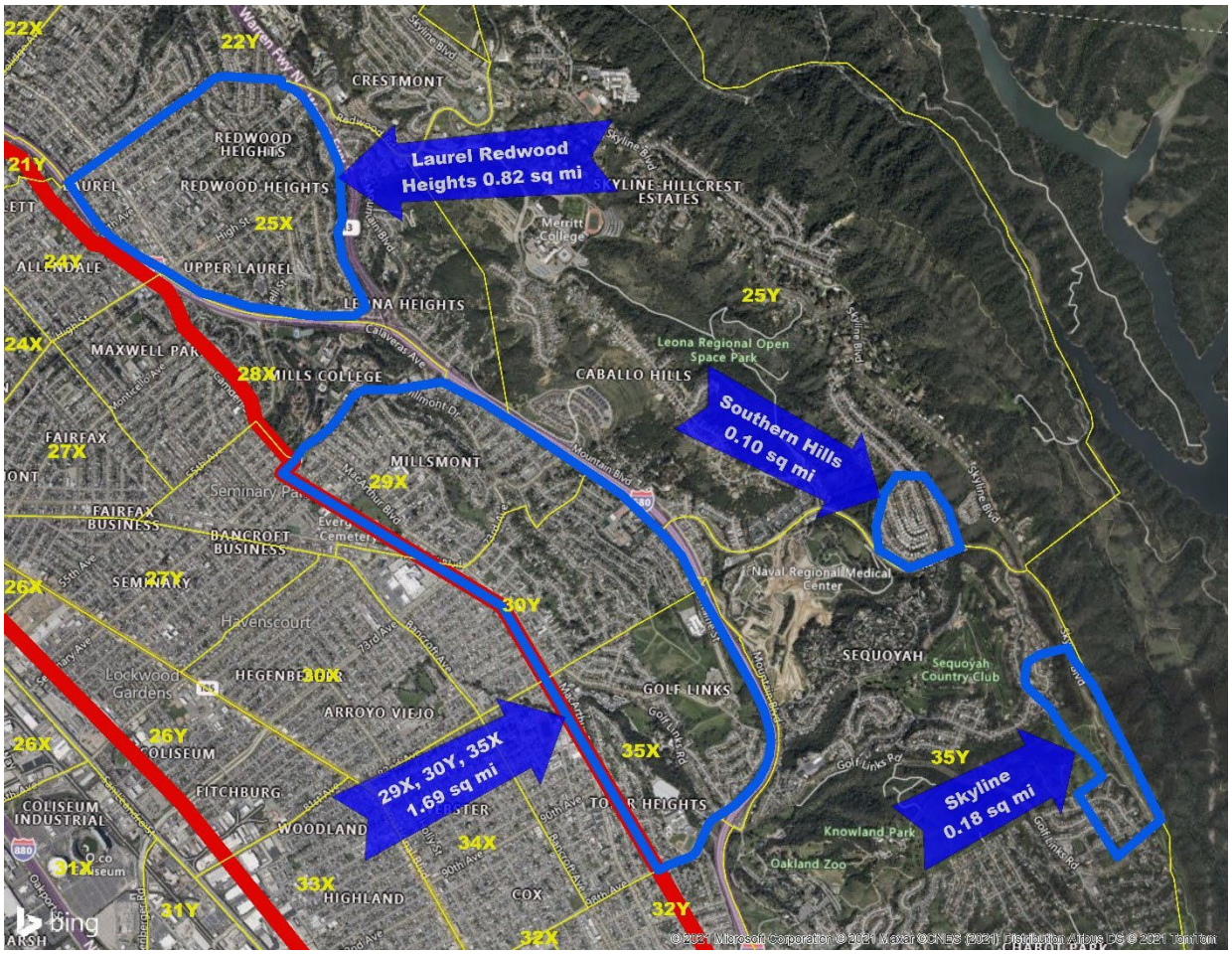
Phase II with blue borders (Activated in 2013): 6.64~~~~ square miles
East Oakland: West of High Street to Park Boulevard
North Oakland: North of Highway 580 to Alcatraz Avenue

Phase III with yellow borders (Activated in 2016): 2.78 square miles
Downtown Oakland: Jack London Square to about West MacArthur Boulevard
Cleveland Height area: East of Lake Merritt to Highway 580 & Park Boulevard
Maxwell Park: East of High Street to Highway 580 & Mills College



* While the original contracted coverage total for Phase I was 6.0 mi², an additional 1.06 mi² of ShotSpotter coverage was added, at no charge, for a total of 7.06 mi² when Phase I service was upgraded and converted to the newer subscription platform in 2011.

Phase IV with blue borders (Activated in 2021): 2.79 square miles
Laurel Redwood Heights: Covering a portion of Beat 25X
Southern Hills: Covering a portion of Beat 25Y
Millsmont / Golf Links: Covering Beats 29X, 30Y, and 35X
Skyline: Covering a portion of Beat 35Y

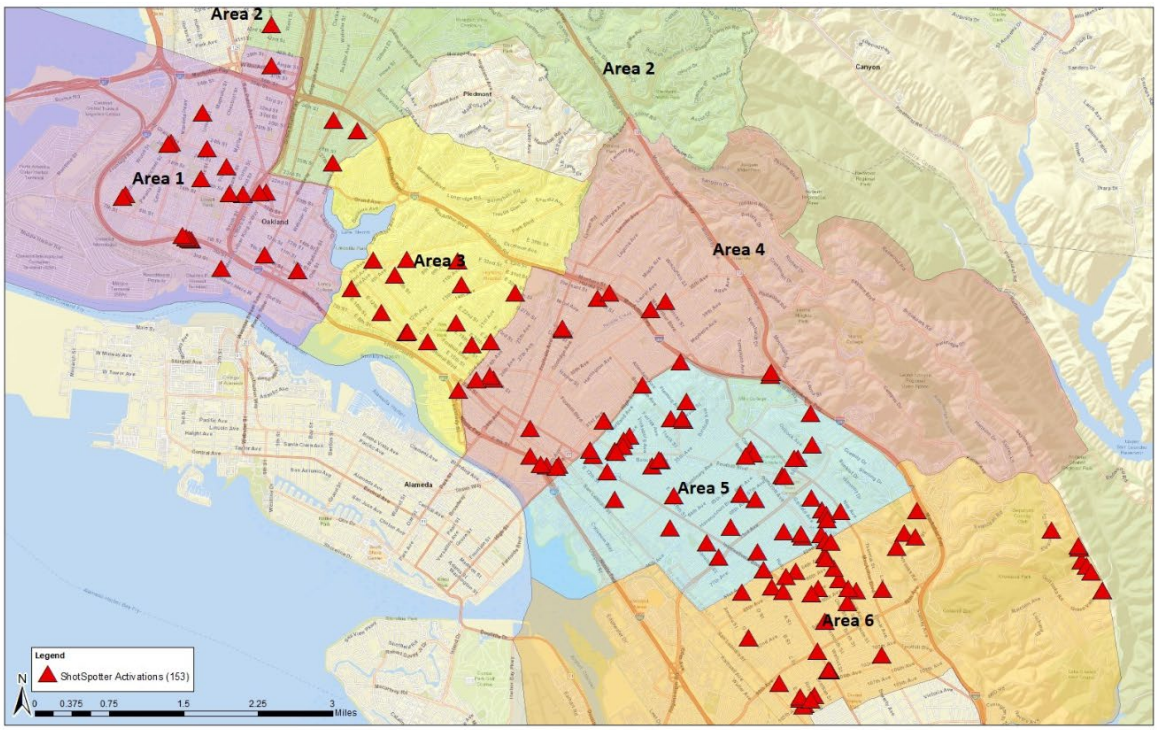

Laurel Redwood Heights 0.82 sq mi
Southern Hills 0.10 sq mi
29X, 30Y, 35X 1.69 sq mi
Skyline 0.18 sq mi
CRESTMONT
REDWOOD HEIGHTS
SKYLINE-HILLCREST ESTATES
Merritt College
Leona Regional Open Space Park
CABALLO HILLS
MILLSMONT
FAIRFAX BUSINESS
BANCROFT BUSINESS
Naval Regional Medical Center
SEQUOYAH
Sequoyah Country Club
GOLF LINKS
Havenscourt
Lockwood Gardens
ARROYO VIEJO
COLISEUM
FITCHBURG
COLISEUM INDUSTRIAL
WOODLAND
HIGHLAND
COX
Knowland Park
Oakland Zoo
bing

ATTACHMENT B

OAKLAND POLICE DEPARTMENT
455 7TH ST., OAKLAND, CA 94607 | OPDCRIMEANALYSIS@OAKLANDNET.COM
CRIME ANALYSIS

Weekly ShotSpotter Activations Report — Citywide
10 Apr. – 16 Apr., 2023

ShotSpotter Activations	Weekly Total	YTD 2021	YTD 2022	YTD 2023	YTD % Change 2022 vs. 2023	3-Year YTD Average	YTD 2023 vs. 3-Year YTD Average
Citywide	153	2,817	2,583	2,269	-12%	2,556	-11%
Area 1	20	275	270	210	-22%	252	-17%
Area 2	7	80	87	74	-15%	80	-8%
Area 3	15	287	260	250	-4%	266	-6%
Area 4	21	435	460	378	-18%	424	-11%
Area 5	46	943	754	607	-19%	768	-21%
Area 6	44	797	752	750	0%	766	-2%



All data sourced via ShotSpotter Insight.

Produced by the Oakland Police Dept. Crime Analysis Unit.

CITY OF OAKLAND

MEMORANDUM

TO: Darren Allison, Interim Chief of Police

FROM: Drennon Lindsey, Deputy Chief of Police OPD, Bureau of Investigations

SUBJECT: Unmanned Aerial System (UAS or Drone) – 2022 Annual Report

DATE: May 25, 2023

Background

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

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

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

Lieutenant Daza-Quiroz is currently the UAS Program Coordinator.

2022 Data Points

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

From the "Surveillance Impact Use Report for the Unmanned Aerial System (UAS)"

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

UAS are controlled from a remote-control unit (similar to a tablet computer). Wireless connectivity lets pilots view the UAV its surroundings from a birds-eye

perspective. UAV pilots can leverage control unit applications to pre-program specific GPS coordinates and create an automated flight path for the drone.

UAS have cameras so the UAS pilot can view the aerial perspective. UAS proposed for use by OPD and/or the Alameda County Sheriff's Office use secure digital (SD) memory cards to record image and video data; SD cards can be removed from UAS after flights to input into a computer for evidence.

UAS technology was used in the following ways/with the following outcomes in 2022:

One Hundred and Thirty-Two (132) uses. OPD responded to One Hundred and Nine (109) deployments and missions. Alameda County Sheriff's Office (ACSO) or neighboring agencies with UAS Programs responded to twenty-three (23) requests. Sometimes ACSO will offer their services prior to being requested[1]. However, all agencies will only deploy if requested or approved by an OPD commander and if policy requirements are met. OPD Electronic Support Unit (ESU) has created a spreadsheet to track and monitor outside agency deployments. Lt. O. Daza-Quiroz sent a department wide email mandating all commanders who deploy drones to author documentation, similar to the protocol for use of the Emergency Rescue / Armored Vehicles. This process has allowed for appropriate documentation.

Table 1 below details the deployments of OPD and ACSO Drones in 2022 in the City of Oakland

Table 1: 2022 OPD & ACSO Drone Deployments

Incident Type	***OPD***	***ACSO***	***Total***
Mass casualty incidents	*0*	*0*	*0*
Disaster management	*1*	*0*	*1*
Missing or lost persons	*3*	*0*	*3*
Hazardous material releases	*0*	*0*	*0*
Sideshow events	*4*	*0*	*4*
Rescue operations	*4*	*1*	*5*
Training	*4*	*0*	*4*
Barricaded suspects	*16*	*7*	*23*
Hostage situations	*0*	*2(HPD)*	*2*
Armed suicidal persons	*0*	*0*	*0*
Arrest of armed and/or dangerous persons	*53*	*7*	*60*
Scene documentation for evidentiary or investigation value	*2*	*0*	*2*
Operational pre-planning	*0*	*0*	*0*
Service of high-risk search and arrest warrants	*22*	*0*	*22*
Exigent circumstances	*0*	*0*	*0*
Total	***109***	***23***	***132***

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

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):

Twenty-Three (23) times. Outside Law Enforcement Agencies (ACSO, Hayward PD) assisted in 23 UAS deployments in Oakland in 2022. Because of this, the UAS aircrafts that they used captured and stored data. These agencies provide OPD with the recordings and stored the information in their logs per their respective policy requirements. No outside entity made any requests to OPD to share any of OPD's data acquired using OPDs UAS, nor did OPD share any data acquired through OPDs UAS with outside entities.

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

The technology was never installed upon fixed objects.

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

Table 2 below details the Police Areas where UAS were deployed in 2022.

Table 2: OPD UAS Deployment by Police Area

Deployment by Area	***Total Deployments***
Area 1	*21*
Area 2	*8*
Area 3	*21*
Area 4	*26*
Area 5	*27*
Area 6	*24*
*Outside City**	*5*
Total*	***132***

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

E. A summary of community complaints or concerns about the surveillance technology, and an analysis of the technology's adopted use policy and whether it is adequate in protecting civil rights and civil liberties. The analysis shall also identify the race of each person that was subject to the technology's use. The Privacy Advisory Commission may waive this requirement upon making a determination that the probative value in gathering this information to evaluate the technology's impact on privacy interests is outweighed by

the City's administrative burden in collecting or verifying this information and the potential greater invasiveness in capturing such data. If the Privacy Advisory Commission makes such a determination, written findings in support of the determination shall be included in the annual report submitted for City Council review

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

Table 3 below provides race data related to 2022 UAS deployments.

Table 3: Race of Detainees Connected to OPD UAS Deployments in 2022

	Race – Female	***Race - Male***	***Total***
Black	*27*	*81*	*108*
Hispanic	*16*	*42*	*58*
Asian	*0*	*13*	*13*
White	*4*	*4*	*8*
Other	*1*	*12*	*13*
Total	***48***	***152***	***200***

OPD knows the race of detainees connected to UAS deployments. However, the race of all individuals involved in many UAS deployments is not known. There are cases such as barricaded suspects, where no suspect is ever discovered or detained. There could also be UAS uses for missing persons where the person's identity is not entirely known nor discovered.

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 OPD Electronic Surveillance Unit (ESU) maintained a list of all UAS deployment logs for record and tracking purposes. This list was reviewed periodically for accuracy and for assessment of any policy violations. All OPD commanders were directed to send communications to ESU for any UAS request or use – similar to OPD protocols for use of Emergency Rescue / Armored Vehicles. No policy violations were found, and no corrective actions were warranted nor needed in 2022.

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

There were no identifiable data breaches or unauthorized access during the year of 2022.

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

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

During this review period OPD had over 100 deployments. Specific records were kept tracking the efficacy of those deployments with the following results:

- During a deployment, there was about a 75% chance of a subject being located. Nearly half of those deployments were for potentially armed and/or dangerous subjects.
- As a result, over 140 subjects were located by the UAS and this resulted in about 76 arrests.
- 65 firearms were recovered when UAS were deployed in 2022.
- The Entry Team (SWAT Team) saw a decrease in Blue Alert deployments. In 2023 there has only been one Entry Team deployment at the time this report was authored. This decrease in deployments represents reduced emotional trauma to the community and significant fiscal savings for the city.
- Canine deployments were reduced by nearly 20%.

Over 60 of the deployments were for persons who were considered armed and/or dangerous. Because of the ability to deploy UAS, responding emergency personnel were better able to create an environment of de-escalation. Absent the UAS, officers would typically resort to calling out the Entry Team, deploying a canine, or physically clearing the area with a search team for the subject(s). All of these options have potential for chance encounters resulting in the possibility of force escalation. These options decrease safety for the officers and the subjects of our contacts.

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

1. *Officers located an armed carjacking vehicle parked in the 1400 blk of Fruitvale Av. The suspect was asleep within the driver's seat, and it was unknown if he was currently armed. UAS were deployed as overwatch and one suspect was taken into custody. 23-002487*
2. *Officers responded to a report of multiple gunshots heard in the area. Officers recognized the location from the previous incident. Officers were advised by a community member that the person at this location was seen shooting guns. Officers observed the suspect exiting the location while wearing a bullet proof vest, who was then detained. A security sweep was conducted and 16 firearms and over 100 spent casings were located. 23-001708.*
3. *OPD Ceasefire units conducted a stop on a driver of a stolen vehicle believed to be involved in a recent carjacking. A second suspect barricaded himself inside of a hotel room. A Surround and Call Out protocol was initiated and a search warrant was obtained for a search of the room. Although the suspect was GOA, the suspect's clothing and a firearm were located in the room. 23-003067*
4. *Officers responded to a shot spotter activation. During the course of the preliminary investigation officers determined that a shootout occurred and one of the parties fled inside REDACTED 85th Ave. A surround and callout was initiated. Numerous individuals were detained and a firearm was recovered. 23-005620*
5. *CID Officers were conducting an investigation when they were shot at with a firearm. Argus followed the suspect in which one suspect ran into*

REDACTED Delaware Ave. UAV were deployed to search the residence for suspect. 1 suspect was located and placed under arrest. 23-008000

As UAS deployments increase in response to demands from the City, we expect continuous positive outcomes from the use of this technology.

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

There was only 1 Drone PRR (PRR 22-3024) request in 2022.

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

The UAS unit currently has ten members. These members engage in 240 hours of training annually to ensure compliance with Department policy and FAA regulations. The member's training is conducted during their regular scheduled shifts minimizing costs. Adjusting for top rate salary, the training is estimated to cost $158,327.00 for 2023 and will be paid for by the Department.

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

No requests for policy changes at this time.

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

Respectfully submitted,

_____

Drennon Lindsey, Deputy Chief
OPD, Bureau of Investigations

Reviewed by,
David Elzey, Captain
OPD, CID

Prepared by:
Omar Daza Quiroz, Lieutenant
OPD, Electronic Support Unit (ESU)

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

City of Oakland

Public Works Department Surveillance Impact Report for Illegal Dumping Surveillance Cameras

A. **Description:**

The ***Portable Observation Device,*** or POD, is an all-in-one, portable surveillance system. The i4POD-P has four (4) cameras and includes a digital video recorder, a cellular router and a wifi transmitter – all housed in an easy to move and mount enclosure. The POD is plug and play; the City needs only to supply 110v power to activate system.

i4POD-P with 4 cameras includes:

- One (1) stationary camera
- Three (3) pan/tilt/zoom (PTZ) cameras that offer 360-degree views and zoom at 12x optical and 10x digital to enable flexibility to capture exactly what the user wants to see. Other POD components include:

Digital video recorder (DVR): The POD DVR records video to a 2TB hard drive. It also streams encrypted video to the user using the POD desktop software, browser or smartphone app. Video footage can be viewed live, searched, played back and downloaded via cellular or wifi connection.

Cellular router: Router uses internet service providers (ISPs) for connectivity, enabling user to access DVR and all other functions remotely.

Wifi transmitter: Wifi transmitter sends a wireless signal similar to a home or office router. It offers secondary access to a DVR and all of its functions if cellular signal is not available or if video is too large to transmit via cellular. User will drive up to a POD and connect an authorized laptop to the wifi signal, as one would at home or office.

Satellite POD:

- One (1) stationary camera
- One (1) PTZ camera

Satellite PODs are secondary POD(s) deployed to increase the number of viewable angles into an area when surveilling a location with multiple ingress and egress points or a wide area that requires additional PTZ cameras to cover the area properly. Satellite PODs are connected to the primary POD via wireless transmitters and can be located up to half a mile away from the primary POD so long as there is a clear line of sight between the wireless transmitters.

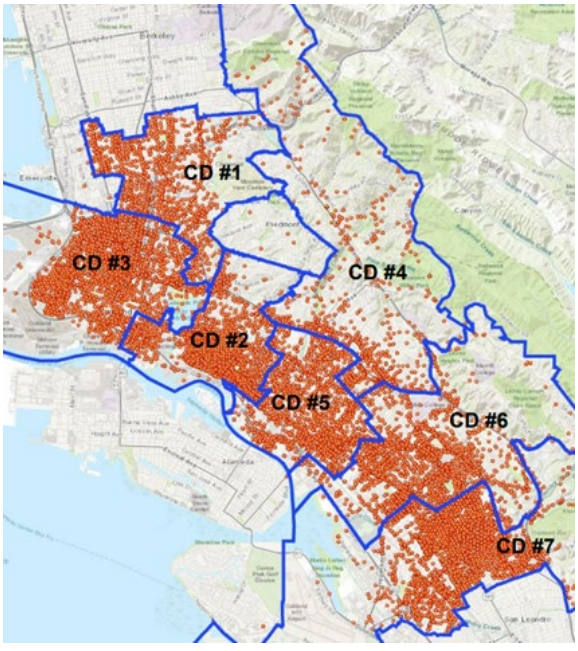
License Plate Reader (LPR) Camera

- One (1) stationary camera
- One (1) UNV LPR video camera

The LPR camera is a video camera with infrared lighting and filters that specializes in enhancing a license plate's readability. It is deployed as one of two cameras on a Satellite POD to operate in tandem with a main POD. The LPR camera's video data will record to the POD's DVR, similar to the POD's PTZ cameras. The LPR camera's license plate data are enhanced images of license plates. These images are stored locally on a SD card inside the LPR camera. They are separate from the DVR data storage and must be extracted from the LPR camera using a web browser interface. The LPR camera's 128 GB SD card's storage capacity is significantly less than the POD DVR's hard drive and will automatically overwrite itself when full. The number of days of storage will depend on the number of license plates the LPR camera captures. On average, the SD card can store license plates data for 7-10 days.

The proposed LPR cameras will utilize basic features such as live view, playback, PTZ and image control functions such as focus, exposure, lighting, color, etc. Smart features referenced in Section 5.6 of the *LPR Network Camera User Manual V3.0* will not be used by City staff as those enhanced functions require more advance DVR equipment and connection to the Cloud.

B. **Purpose:**



FY21-22 Illegal Dumping Work Orders Completed by KOCB

Illegal dumping is a complex and multi-faceted problem that has been affecting the City of Oakland (City) for a number of years. City leaders have been working to develop a variety of strategies and programs to combat the rise of debris on city streets and public lands. This type of activity reduces the health and safety of Oakland's neighborhoods and disproportionally affects economically disadvantaged communities of color. The City's Illegal Dumping Surveillance Camera Program (Camera Program) is a critical component of these efforts. The goal of the Camera Program is to enforce against those who are illegally dumping debris throughout the city. The surveillance cameras offer the City a viable tool to enhance the investigative work performed by Oakland Public Works' (OPW's)

Environmental Enforcement Unit (EEU) that is comprised of eight (8) Environmental Enforcement Officers (EEOs), a Clean Community Supervisor, and an Administrative Analyst. The EEOs are primarily tasked with enforcing illegal dumping using various tactics to hold illegal dumpers accountable for their actions, including forensic investigations involving thorough inspections of illegally dumped debris, and as of March 2022, monitoring video footage captured by surveillance cameras installed at illegal dumping hotspots throughout the city.

C. **Location:**

Cameras will be placed citywide, in the public right of way, nearest to chronic dumping “hotspots”. Hotspots often contain dumping where there is insufficient evidence connecting the debris to dumpers and therefore are ideal for surveillance cameras. Public rights of way include but are not limited to city assets such as street light poles, traffic signal poles, and other public assets like bus stop shelters (through coordination with AC Transit), and city-installed wooden posts. The City may also explore installing POD units on private properties through local business/private resident partnerships.

The POD’s tamper-proof housing unit is installed using simple mounting straps. Installations are performed by Keep Oakland Clean & Beautiful (KOCB) staff with bucket truck certification. Presently,15 PODs are deployed at various hotspots throughout the City, as identified by Cityworks data that is refreshed every two to three months.

D. **Impact:**

OPW recognizes that all people have an inalienable right to privacy and are committed to protecting and safeguarding this right. OPW does not seek to track movement of individuals. However, OPW understands that the public may be concerned that video surveillance, and the retention and analysis of video information over time could potentially be used to generate a detailed profile of an individual’s movement or be abused for other inappropriate purposes.

Specifically, OPW recognizes the following public concerns:

- **Identity capture.** The public may be concerned that the cameras will capture personally identifiable information without notice or consent. Although POD surveillance cameras do not independently generate information that identifies vehicle occupants, license plate information can be used to determine the registered owner. In addition, vehicle occupants or immediate surroundings (including addresses) may be pictured. As a result, it is possible that individuals with access to this data could do additional research to identify the individual.

- **Misidentification.** The public may be concerned that individuals may be misidentified as the person driving a vehicle and doing the dumping. This could lead to enforcement actions against such individuals in error.
- **Activity monitoring.** The public may be concerned that the cameras' data will enable individuals' behaviors to be revealed to and/or monitored by OPW or other government agencies, their partners or affiliates, companies interested in targeted marketing, and/or the public. Such concerns may include basic information about when individuals are in certain locations, as well as concerns about what government or individuals may infer from this data (i.e., marital fidelity, religious observance, or political activity). Although video recordings and license plate numbers are gathered from public places, this could conflict with an individual's expectation of locational privacy.

E. **Mitigations:**

OPW will take multiple steps to mitigate privacy concerns:

- OPW will use the POD surveillance system in accordance with the proposed *Illegal Dumping Surveillance Cameras Use Policy* (attached), as well as all applicable laws, policies, and administrative instructions.

- OPW will not use or deploy the POD system in a discriminatory, viewpoint-based, or biased manner. EEU staff will apply a data-driven approach to deploying surveillance cameras as a general practice.

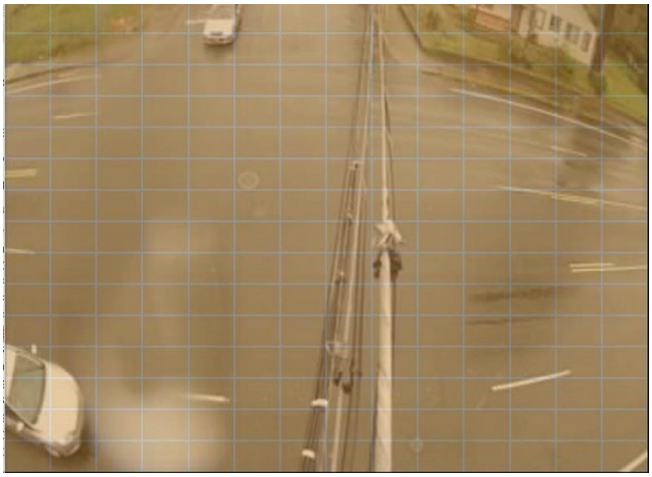
- Surveillance systems will be deployed for the purpose of capturing illegal dumping activities only. POD units will be installed in public rights of way (and potentially at local businesses and private properties through local business/ private resident partnerships) at or near known hotspots where chronic dumping occurs.

- Due to concerns with artificial intelligence (AI), the POD surveillance system was selected for its limited features while delivering the very basic surveillance functions approved by the Privacy Advisory Commission (PAC). The legacy system lacks the higher processing power and AI capabilities of current-day surveillance systems that enable end users to minimize recordings of general/ unrelated activities. However, routine video recordings not downloaded will be destroyed automatically and permanently by the DVR every 14 days, when new video overwrites the oldest recordings.

- The POD system (i.e., cameras and software) does not contain analytics that track movement of individuals. To minimize the public being unnecessarily

recorded, the POD's DVR may be set to record based on motion detection via pixel changes to specified areas of a camera's field of vision.

Example of how the City can select specific areas to activate motion-based recording.



- Similarly, the LPR Camera's 128 GB SD card will automatically overwrite itself when full, which occurs on average every 7-10 days. The rate at which the data on an SD card is overwritten depends on the amount of license plate images the LPR Camera captures.

- All license plate information will be captured manually/visually by EEU staff and will be referred to the Office of the City Attorney (OCA) for DMV records. NOTE: Oakland Municipal Codes permit EEOs to cite both the dumper AND the owner of the vehicle used in a dumping incident. A robust appeal process is in place for individuals to appeal a citation if they feel they were cited in error.

- OPW will not purchase the additional equipment required to enable the POD's audio feature.

- OPW will limit admin/super user access to add/delete users and/or change user access to two (2) OPW Managers.

- OPW will retain and use video footage and license plate information strictly for the enforcement of illegal dumping and will only forward footage containing illegal dumping activities to the OCA, assigned Hearing Officer, OPD and/or Alameda County's District Attorney's Office for prosecution. At the discretion of the OPW Director, video data and license plate information may be shared with the City Administrator's Office (CAO) and City Councilmembers.

- Downloaded video recordings will be purged once filed claims, pending litigations, and/or criminal investigations conclude. Screenshots of dumping and license plate photos will be retained as attachments to the EEO's Cityworks work order to track citation process. Attachments are not searchable in Cityworks.

- OPW will conduct annual audits of video footage and license plate information stored in secure folder to ensure compliance with Use Policy and to verify that authorized users and administrators are following Use Policy.

- OPW shall report within 72 hours any Oakland Police Department (OPD) request for video recordings captured by POD units to the Chief Privacy Officer and Privacy Advisory Commission (PAC) Chair. OPD's request will describe the nature of the investigation for which the video data is being requested. This information will be reported to the PAC at its next regularly scheduled meeting.

- OPW will seek the Privacy Advisory Commission's review and recommendation prior to making changes to the POD's use.

F. **Data Types and Sources:**

- Image, video recordings
- Snapshots of license plate information as visible in LPR video recordings
- Audit logs (when explicitly queried)
    - User Log-ins/ Log-outs by IP address
    - Profile Management (add, edit, delete users; settings imported/exported)

  The audit log also tracks device specific events such as:
    - Recordings stopped and started
    - Reboots
    - Power On
    - Time syncs

G. **Data Security:**

Per *Public Works Department Surveillance Technology Use Policy for Illegal Dumping Surveillance Cameras*:

Data Access – The City of Oakland has sole access to POD video data and LPR camera license plate data. However, vendor Security Lines U.S. has been granted temporary access to the surveillance system to provide ongoing technical support.

Individuals authorized to access and/or view surveillance camera information include:

Oakland Public Works –

- OPW Director and OPW Bureau of Environment's Assistant Director will be given access to view video data.

- KOCB Operations Manager, who oversees the EEU, will be able to add/delete users and will be granted admin/super user access.

- OPW Bureau of Environment's AdministrativeServices Manager, who administers the Illegal Dumping Surveillance Camera Use Policy, will be able to add/delete users and be given admin/super user access.

- EEU staff – Clean Community Supervisor, EEU Administrative Analyst, EEU Administrative Assistant, and EEOs – who will be tasked with checking cameras for illegal dumping activities and remote monitoring the POD units, will be given access to view video, control PTZ cameras, as well as search and download video evidence. EEU staff will not have the ability to add/delete users.

Data Protection – There are three different levels of security to safeguard the POD's video data.

1. Cellular router level: An authorized user's computer must be recognized by the cellular router ("Router") before s/he can gain access to the POD system. Personnel with "admin/super user" profiles will specify which computers' IP addresses the Router recognizes. A unique username/password is required to configure the Router.

2. Desktop software level: To interface with the POD system, proprietary POD software will be installed on an authorized user's computer. A unique username/password is required to access software. Different levels of POD access – view only, PTZ camera control, video search & download, and admin/super user access – may be assigned to different personnel by the admin/super user.

3. DVR level (for mobile phone application only): Each POD has its own DVR. To access a specific POD's recordings, a separate username/password is required to access the DVR associated with that POD. Like the desktop software, users may be added or removed and given different levels of access.

Video data encryption takes place as the POD cameras record to the DVR. Satellite POD's video data is stored on the Main POD's DVR. LPR camera's video data will record locally to the POD's DVR, similar to PTZ cameras on a POD. The LPR camera's license plate data are enhanced images of license plates. These images are stored locally on a SD card inside the LPR camera and must be extracted from the LPR camera using a web browser interface. They are separate from the DVR

data storage.

Data Retention – There are 3 ways video data are retained.

1. DVR hard drive: The POD DVR records video to the hard drive housed inside the POD unit. The hard drive automatically overwrites the oldest recordings every 14 days. Routine video recordings not downloaded will be purged automatically and permanently by the DVR, when new video is saved on top of the oldest recordings.

2. Video from the License Plate Reader (LPR) camera is recorded to the POD's DVR, similar to the POD's other PTZ cameras and follows the same 14-day overwrite schedule. The enhanced license plate images are stored in the 128GB SD card inside the LPR camera, separate from the DVR. A 128GB SD card can store license plates data for an average of 7-10 days before overwriting occurs. The actual number of days of storage, however, will depend on the number of license plates the LPR camera captures at the subject location.
3. Downloaded videos and images: Video will only be downloaded when it contains adequate evidence of illegal dumping to warrant possible enforcement actions. An authorized user will download the video clips via the POD desktop software to a secure OPW folder. License Plate information captured by LPR cameras will be downloaded from the web browser interface as an image. The image will include a picture of some, if not all, of the subject vehicle and the license plate information.

The POD cameras are not monitored in real-time. Video footage on each POD is reviewed by EEU staff Monday through Friday up to two times a day between the hours of 7am and 4pm. Screenshot photos of dumper, dumper's vehicle, dumped material and license plate information used in citation and appeal processes will be stored as attachments in EEO Work Orders in Cityworks. Downloaded video clips are saved to a secure EEU shared folder and will be purged per legal guidance once filed claims, pending litigation, and/or criminal investigations and prosecutions conclude.

Public Access – Except where prohibited or limited by law, the public may request access to the City's video data through public records requests. However, prior to the release of any information to a surveillance-related public records request, staff will consult with the City Attorney's Office for review and guidance.

Third Party Data Sharing – There is no third-party data sharing with the POD surveillance system. The vendor cannot access the City's video data through the POD software unless previously arranged by authorized personnel listed in section **D. Data Access** and only for technical support purposes. Computers with IP addresses entered by the City's admin/super user are the only computers permitted to access the PODs (See section **E. Data Protection**). The POD surveillance system data is transmitted does not connect to the Cloud.

Other City departments or non-City entities that may view or use POD video recordings are:

City Attorney's Office (OCA) –

- Assigned City Attorney staff handling illegal dumping related matters will view select video clips 1) to ascertain the viability of the video evidence, and 2) to work up a case to initiate legal actions to prosecute the dumper for violations of the Oakland Municipal Code. Security access to the POD system is not required.
- Assigned City Attorney staff handling litigation matters and/or the City's compliance with the Public Records Act and Sunshine Ordinance may request PW staff hold and not destroy video footage that might be relevant to such matters. For the same purposes, assigned City Attorney staff may hold and view video footage when necessary. In the course of pending litigation, video footage may be subject to discovery and disclosed with or without a court order. In these instances, City Attorney staff handling litigation matters will make reasonable efforts to narrowly tailor disclosure to the greatest extent possible to comply with the City's legal obligations but also preserve footage that might normally be withheld under this Policy.

Administrative Hearing Officer –

- Assigned Administrative Hearing Officer may view select video clips in the course of adjudicating illegal dumping cases via the City's administrative hearings (due process hearings for violators that appeal the City's determinations on violations). Security access to the POD system is not required.

Oakland Police Department (OPD)/ Alameda County District Attorney's (DA's) Office

- In the event POD cameras capture illegal dumping of the scale and/or nature that warrant criminal investigations, EEU staff may share select video clips with OPD and/or the DA's Office for further illegal dumping investigatory and enforcement actions. Security access to the POD system is not required.
- In the event POD cameras capture general illegal activity that reasonably appears to constitute "violent forcible crimes" as defined by OPD's Departmental General Order J-04 – Pursuit Driving Appendix A, Paragraph H: "Violent Forcible Crime," Environmental Enforcement Unit (EEU) staff shall promptly download the relevant video footage, forward said recording to OPD for possible investigatory and enforcement action, and log the incident. This log shall be incorporated into the annual report required by O.M.C. [Oakland Municipal Code] 9.64.040
- OPW shall report within 72 hours any Oakland Police Department (OPD)

request for video recordings captured by POD units to the Chief Privacy Officer and Privacy Advisory Commission (PAC) Chair. OPD's request will describe the nature of the investigation for which the video data is being requested. This information will be reported to the PAC at its next regularly scheduled meeting.

OPW may also authorize other City staff with "occasional, as-needed" view-only access. To be approved, City staff must submit a written request to the OPW/BOE - KOCB Ops Manager or the OPW/BOE – Administrative Services Manager. The KOCB Ops Manager or the Administrative Services Manager will approve or deny access based on Use Policy guidelines or at OPW Director's direction. Third parties are granted view-only access and are not given downloading rights to prevent data sharing. Lastly, at the discretion of the OPW Director, video data and license plate information may be shared with the City Administrator's Office (CAO) and City Councilmembers.

H. **Fiscal Cost:**

Funding will be sourced from KOCB's O&M budget in Illegal Dumping (ORG 30674) and Environmental Enforcement (ORG 30676) Units. Staff will request City Council's approval for additional funding during future Budget Development process. If the current request for additional technologies is approved, the projected total annual costs are as follows:

ILLEGAL DUMPING SURVEILLANCE PROGRAM ANNUAL COSTS (FY2023-2024)				
Equipment-Related Costs	**Quantity**	**Cost**	**One-Time**	**Ongoing**
Additional PODs*	4	10,000	$ 40,000.00	
Cellular Boosters*	18	1,000	$ 18,000.00	
LPR Cameras*	20	2,800	$ 56,000.00	
Miscellaneous Replacement Parts	-	-		$ 5,000.00
Monthly Technical Support	12	3,500		$ 42,000.00
SUBTOTAL			$ 114,000.00	$ 47,000.00
Personnel Costs	**Quantity**	**Annual Personnel Cost** (Fully Burdened)	**Percentage of Surveillance Work**	**Surveillance Personnel Cost**
Analyst II	1	200,259	15%	$ 30,038.85
EEO (Salary I)	3	195,927	20%	$ 117,556.20
EEO (Salary II)**	2	171,446	20%	$ 68,578.40
Painter	1	216,118	5%	$ 10,805.90
SUBTOTAL				$ 216,173.45
TOTAL ANNUAL COSTS (FY23-24)			**One-Time**	**Ongoing**
			$ 114,000.00	**$ 263,173.45**

**Equipment purchased may be prorated based on available funds*

***EEO staff may increase by three (3) FTEs for a total of 8 EEOs if current vacancies are filled*

Time required to perform job duties associated with the new surveillance cameras will likely necessitate one additional administrative personnel. An Administrative Assistant II position was approved but funds to hire have been frozen for Fiscal Year 2023-2024.

I. **Third Party Dependence:**

Cellular service is provided by the City's Internet Service Providers (ISPs). The POD Surveillance System does not connect to the Cloud. Vendor Security Lines U.S. cannot access the City's video data through the POD software; however, they have been granted temporary access to the surveillance system to provide technical support.

J. **Alternatives:**

Status Quo - Do not deploy surveillance cameras. There will not be any financial outlay for surveillance cameras. However, illegal dumping abatement costs will likely continue to rise precipitously if the City continues operation as is. The City will need to answer to the constituents demanding the City take decisive action against dumpers. The City will continue to struggle with addressing dumping at chronic hotspots.

Sting Operations with OPD - Request assistance from OPD to conduct sting operations at chronic hotspots to catch dumpers in the act. While conducting some sting operations throughout the city may add another tool to the toolbox for catching illegal dumpers, this option would not be a viable comprehensive replacement to surveillance cameras because: 1) it is labor intensive and cost prohibitive; 2) OPD has indicated a lack of resources to assist with illegal dumping enforcement due to the need to enforce higher priority crimes; 3) it would take many more resources and time to catch the same amount of illegal dumpers that can be caught with cameras.

Hire More EEOs - Bring on more EEOs to patrol hot spots and to catch dumpers. This is not a viable long-term solution because: 1) it will be cost prohibitive to hire enough EEOs to provide adequate coverage of areas prone to chronic dumping; 2) more EEOs does not necessarily translate to greater success in catching dumpers if there is insufficient evidence to prosecute. Without supporting evidence, the only way an EEOs can catch a dumping violator is to witness the individual in the act of dumping, and that is a rare event because dumpers are deterred if they see an enforcement vehicle near a dump site.

K. **Track Record:**

San Leandro, Sacramento, Fremont, Alameda, Livermore, and Milpitas are just a few of the regional municipalities using the POD surveillance system. In October 2021,

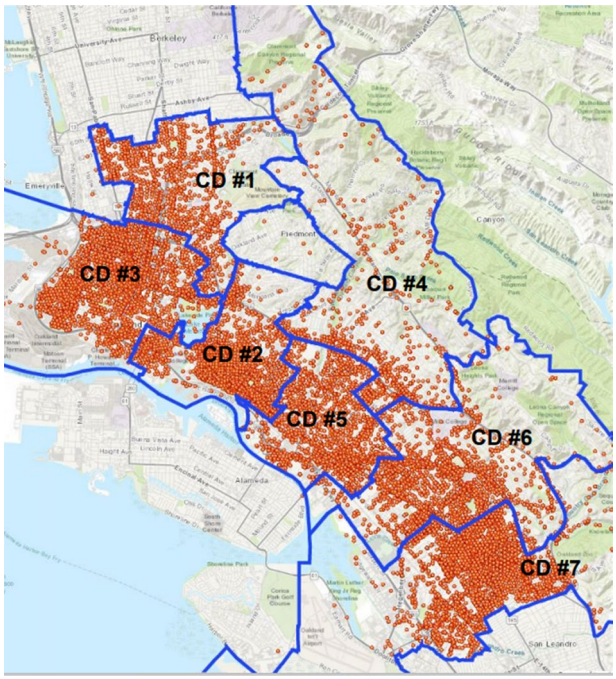
OPW staff solicited product reviews from the City of Alameda and the City of Livermore. Both cities gave full endorsements for the product. Key features of the POD system that garnered positive reviews were:

- Tamper-proof housing unit: weather-tested, near-indestructible casing
- Easy set-up: system only requires 110v power, mounting bracket, and mounting straps to install
- Mobile: easy to move unit to other locations
- Reliability: minimal downtime with stable cellular service
- Minimal maintenance: simple design makes for minimal maintenance
- Simple to use
- Clean, crisp video images

Neither Security Line U.S. nor the POD system has experienced any data breach since its introduction in 2009.

City of Oakland
Public Works Department Proposed Surveillance Technology Use Policy
for Illegal Dumping Surveillance Cameras

A. Purpose



FY21-22 Illegal Dumping Work Orders Completed by KOCB

Illegal dumping is a complex and multi-faceted problem that has been affecting the City of Oakland (City) for a number of years. City leaders have been working to develop a variety of strategies and programs to combat the rise of debris on city streets and public lands. This type of activity reduces the health and safety of Oakland's neighborhoods and disproportionally affects economically disadvantaged communities of color. The City's Illegal Dumping Surveillance Camera Program (Camera Program) is a critical component of these efforts. The goal of the Camera Program is to enforce against those who are illegally dumping debris throughout the city. The surveillance cameras offer the City a viable tool to enhance the investigative work performed by Oakland Public Works' (OPW's) Environmental Enforcement Unit (EEU) that is comprised of eight (8) Environmental Enforcement Officers (EEOs), a Clean Community Supervisor, and an Administrative Analyst. The EEOs are primarily tasked with enforcing illegal dumping using various tactics to hold illegal dumpers accountable for their actions, including forensic investigations involving thorough inspections of illegally dumped debris, and as of March 2022, monitoring video footage captured by surveillance cameras installed at illegal dumping hotspots throughout the city.

This is an updated Use Policy for the operation of the ***Portable Observation Device*** or POD – a surveillance system by Security Lines, U.S. – and seeks to add two products to the surveillance system to increase the efficacy and success of the camera program. These products are the Satellite PODs and License Plate Reader (LPR) cameras.

The goal of installing PODs, Satellite PODs and LPR Cameras near chronic dumping hotspots is to capture video evidence that identifies dumpers that produces supporting information needed to build credible cases for citations and prosecution. The issuance of citations and the prosecution of chronic illegal dumpers using video evidence serve as a deterrent to would-be dumpers who must weigh the benefits of dumping against the higher risk of getting caught by the cameras. By raising awareness of the presence of the cameras and the frequency with which dumpers are caught and cited, the cameras will

increasingly serve as an ongoing visual deterrent to potential dumpers. **Satellite PODs** allow EEOs to increase viewing angles and viewable range to a dumping site by linking wirelessly one or more PODs to the main POD. Satellite PODs' additional point/tilt/zoom (PTZ) cameras are particularly useful when surveilling locations with multiple ingress and egress points or large stretches of roadway.

LPR Camera is a video camera with infrared lighting and filters that specializes in enhancing a license plate's readability. Surveillance data from March 2022 through February 2023 revealed that, of the 492 illegal dumping incidents captured by the PODs, 55% or 271 incidents were cases where citations could not be issued because EEOs were unable to see or read the license plate information clearly. Most often, the difficulty with reading license plates was a result of poor camera angles or poor video imaging. Adding Satellite PODs and LPR cameras to the POD surveillance system will maximize the EEOs' ability to identify dumpers, issue more citations, and have video evidence that can lead to the prosecution of chronic dumpers.

B. Authorized Use

The use of the POD surveillance system, Satellite POD, and LPR camera is authorized solely for surveilling illegal dumping activity in the City of Oakland.

Only staff with a need to know and a right to know will have access to recordings captured by the POD system. See sections **D. Data Access,** and **H. Third Party Data Sharing**, for a list of individuals who will be authorized to access and/or view surveillance data.

Camera Placement: PODs are installed based on a hotspot list to maintain unbiased, non-viewpoint-based deployments. The hotspot list used is a ranked list of the most frequently dumped sites in Oakland. It is derived from analyzing top dumping locations based on the number of constituents' service requests and on the volume of KOCB work orders as per OPW's work productivity software Cityworks. The hotspot list is refreshed every two to three months to provide EEOs the most current dumping locations for camera placement. Additionally, cameras may be deployed at the Public Works Director's direction or for illegal dumping sting operations.

Redeployment: A POD is moved to the next location on the hotspot list once an EEO confirms there has been no recorded dumping for 14 consecutive days. Cameras remain in location until bucket truck-certified staff are arranged to move the POD.

C. Data Collection

Data collection occurs inside a POD housing unit. Video captured from the cameras are recorded directly to the digital video recorder's (DVR's) hard drive (2 TB SATA). DVRs do not possess artificial intelligence (AI) or analytics such as facial recognition. The

POD surveillance system does not connect to the Cloud.

Similarly, the Satellite PODs and License Plate Reader (LPR) cameras do not connect to the Cloud. The Satellite PODs do not possess AI nor facial recognition. The LPR cameras' facial recognition features is inaccessible when not connected to the Cloud.

Audit Log – The audit log tracks system ties each action to a user for events such as:

- User Log-ins/ Log-outs by IP address
- User Management (add, edit, delete users; settings imported/exported)

Audit Log data resides locally on each DVR and requires an explicit query to be accessed. OPW owns the Audit Log data. It is accessible by password protected staff only.

Enforcement Data – Enforcement data is information that an EEO captures when he/she issues a citation or takes other enforcement action. Enforcement data is entered into custom fields in OPW's Cityworks application and is accessible by a query from City staff with Cityworks access. EEU staff also retain a manual log separate from Cityworks that shows when they check POD footage, if any dumping was found, and a brief description of the dumper(s) and dumped materials. The document is only accessible by EEU staff through a secure shared folder.

D. Data Access

Only designated City of Oakland staff have access to POD video data and LPR camera license plate data. The vendor, Security Lines U.S., cannot access the City's video data through the POD software. However, they have been granted temporary access to the surveillance system to provide ongoing technical support. Individuals authorized to access and/or view surveillance camera information include:

Oakland Public Works –

- OPW Director and OPW Bureau of Environment's Assistant Director will be given access to view video data.
- KOCB Operations Manager, who oversees the EEU, will be able to add/delete users and will be granted admin/super user access.
- OPW Bureau of Environment's Administrative Services Manager, who administers the Illegal Dumping Surveillance Camera Use Policy, will be able to add/delete users and be given admin/super user access.
- EEU staff – Clean Community Supervisor, EEU Administrative Analyst, EEU Administrative Assistant, and EEOs – who will be tasked with checking cameras for illegal dumping activities and remote monitoring the POD units, will be given access to view video, control PTZ cameras, as well as search and download video evidence. EEU staff will not have the ability to add/delete users.

E. Data Protection

Since its introduction to the market in 2009, the POD surveillance system has never been hacked. POD DVRs are Linux-based; downloaded video is encrypted; and video recordings cannot be played using standard video players (e.g., Windows Media Player).

There are three different levels of security to safeguard the POD's video data.

1. Cellular router level: An authorized user's computer must be recognized by the cellular router ("Router") before s/he can gain access to the POD system. Personnel with "admin/super user" profiles can specify which computers' IP addresses the Router recognizes. A unique username/password is required to configure the Router.

2. Desktop software level: To interface with the POD system, proprietary POD software is installed on an authorized user's computer. A unique username/password is required to access software. Different levels of POD access – view only, PTZ camera control, video search & download, and admin/super user access – may be assigned to different personnel by the admin/super user.

3. DVR level (for mobile phone application only): Each POD has its own DVR. To access a specific POD's recordings, a separate log-in is required to access each DVR. Like the desktop software, users may be added or removed and given different levels of access.

Video data encryption takes place as the POD cameras record to the DVR. Satellite POD's video data is stored on the Main POD's DVR. LPR camera's video data will record to the POD's DVR, similar to PTZ cameras on a POD. The LPR camera's license plate data are enhanced images of license plates. These images are stored locally on a SD card inside the LPR camera and must be extracted from the LPR camera using a web browser interface. They are separate from the DVR data storage. The LPR camera's 128 GB SD card can store license plates data for an average of 7-10 days, at which point it becomes full and automatically overwrites itself. However, the actual number of days of storage will depend on the number of license plates the LPR camera captures.

Downloaded video images and license plate information in the form of screenshots are stored in the Cityworks app as supporting documentation for citations issued. Downloaded video clips are saved to a secure EEU shared folder.

F. Data Retention

There are 3 ways video data are retained.

1. DVR hard drive: The POD DVR records video to the hard drive housed inside the POD unit. The hard drive automatically overwrites the oldest recordings every 14 days. Routine video recordings not downloaded are overwritten automatically and permanently by the DVR, when new video is saved on top of the oldest recordings.

2. Video from the License Plate Reader (LPR) camera is recorded to the POD's DVR, similar to the POD's other PTZ cameras and follows the same 14-day overwrite schedule. The enhanced license plate images are stored in the 128GB SD card inside the LPR camera, separate from the DVR. A 128GB SD card can store license plates data for an average of 7-10 days before overwriting occurs. The actual number of days of storage, however, will depend on the number of license plates the LPR camera captures at the subject location.
3. Downloaded videos and images: Video will only be downloaded when it contains adequate evidence of illegal dumping to warrant possible enforcement actions. An authorized user will download the video clips via the POD desktop software to a secure OPW folder. License Plate information captured by LPR cameras will be downloaded from the web browser interface as an image. The image will include a picture of some, if not all, of the subject vehicle and the license plate information.

The POD cameras are not monitored in real-time. Video footage on each POD is reviewed by EEU staff Monday through Friday up to two times a day between the hours of 7am and 4pm. Screenshot photos of dumper, dumper's vehicle, dumped material, and license plate information used in citation and appeal processes will be stored as attachments in EEO Work Orders in Cityworks. Downloaded video clips are saved to a secure EEU shared folder and will be purged per legal guidance once filed claims, pending litigation, and/or criminal investigations and prosecutions conclude.

G. Public Access

Except where prohibited or limited by law, the public may access the City's video data through public records requests. However, prior to the release of any information to a surveillance-related public records request, staff will consult with the City Attorney's Office for review and guidance.

H. Third Party Data Sharing

There is no third-party data sharing with the POD surveillance system. The POD Surveillance System does not connect to the Cloud. The vendor cannot access the City's video data through the POD software unless previously arranged by authorized

personnel listed in section **D. Data Access** and only for technical support purposes. Computers with IP addresses entered by the City's admin/super user are the only computers permitted to access the PODs (See section **E. Data Protection**). Other City departments or non-City entities that may view or use POD video recordings are:

City Attorney's Office (OCA) –

- Assigned City Attorney staff handling illegal dumping related matters will view select video clips 1) to ascertain the viability of the video evidence, and 2) to work up a case to initiate legal actions to prosecute the dumper for violations of the Oakland Municipal Code. Security access to the POD system is not required.
- Assigned City Attorney staff handling litigation matters and/or the City's compliance with the Public Records Act and Sunshine Ordinance may request OPW staff hold and not destroy video footage that might be relevant to such matters. For the same purposes, assigned City Attorney staff may hold and view video footage when necessary. In the course of pending litigation, video footage may be subject to discovery and disclosed with or without a court order. In these instances, City Attorney staff handling litigation matters will make reasonable efforts to narrowly tailor disclosure to the greatest extent possible to comply with the City's legal obligations but also preserve footage that might normally be withheld under this Policy.

Administrative Hearing Officer –

- Assigned Administrative Hearing Officer may view select video clips in the course of adjudicating illegal dumping cases via the City's administrative hearings (due process hearings for violators that appeal the City's determinations on violations). Access to the POD system is not required.

Oakland Police Department (OPD)/ Alameda County District Attorney's (DA's) Office –

- In the event POD cameras capture illegal dumping of the scale and/or nature that warrant criminal investigations, EEU staff may share select video clips with OPD and/or the DA's Office for further illegal dumping investigatory and enforcement actions. Security access to the POD system is not required.
- In the event POD cameras capture general illegal activity that reasonably appears to constitute "violent forcible crimes" as defined by OPD's Departmental General Order J-04 – Pursuit Driving Appendix A, Paragraph H: "Violent Forcible Crime," Environmental Enforcement Unit (EEU) staff shall promptly download the relevant video footage, forward said recording to OPD for possible investigatory and enforcement action, and log the incident. This log shall be incorporated into the annual report required by O.M.C. [Oakland Municipal Code] 9.64.040
- OPW shall report within 72 hours any Oakland Police Department (OPD) request for video recordings captured by POD units to the Chief Privacy Officer and

Privacy Advisory Commission (PAC) Chair. OPD's request will describe the nature of the investigation for which the video data is being requested. This information will be reported to the PAC at its next regularly scheduled meeting.

OPW may also authorize other City staff with "occasional, as-needed" view-only access. To be approved, City staff must submit a written request to the OPW/BOE - KOCB Ops Manager or the OPW/BOE – Administrative Services Manager. The KOCB Ops Manager or the Administrative Services Manager will approve or deny access based on Use Policy guidelines or at OPW Director's direction. Third parties are granted view-only access and are not given downloading rights to prevent data sharing. Lastly, at the discretion of the OPW Director, video data and license plate information may be shared with the City Administrator's Office (CAO) and City Councilmembers.

I. Training

Training is available in video tutorials and written formats on vendor Security Lines U.S.'s website in a members-only area. One on one remote training is also available. The Administrative Services Manager in OPW's Bureau of Environment conducts training with authorized POD users as needed. Trainings include review of this Use Policy and reviewing operational procedures required to adhere to the Policy.

J. Auditing and Oversight

The Administrative Services Manager in OPW's Bureau of Environment shall conduct annual assessments to ensure authorized users comply with the Use Policy.

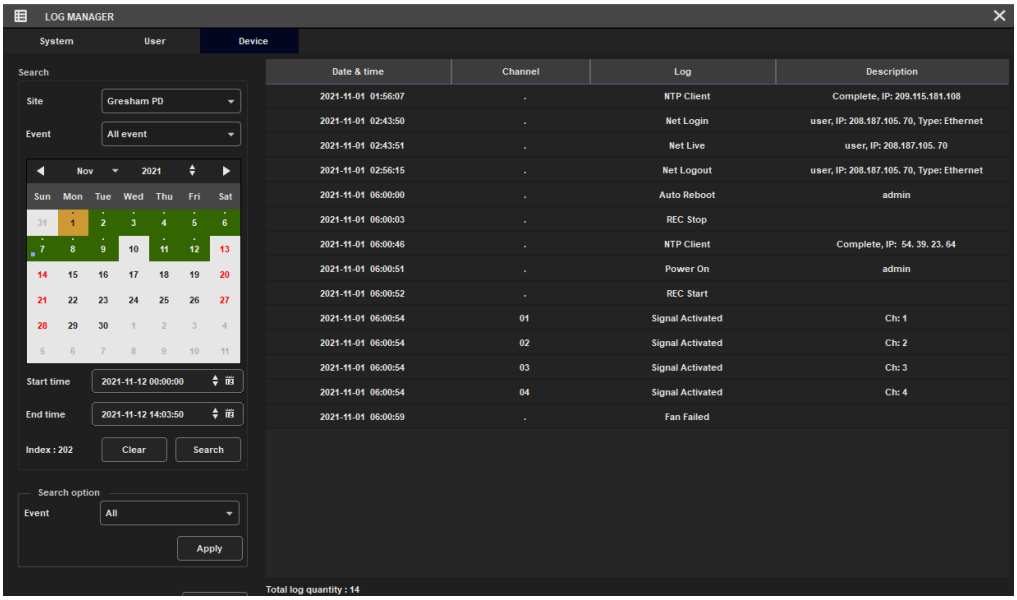
All POD user and device activity are logged. Designated admin/super users can access and view audit logs at the camera level. The audit log tracks system ties each action to a user for events such as:

- User Log-ins/ Log-outs by IP address
- User Management (add, edit, delete users; settings imported/exported)

The audit log also tracks device specific events such as:

- Recordings stopped and started
- Reboots
- Power On
- Time syncs

Example of audit log.



K. Maintenance

Security Lines U.S. offers but does not require a maintenance contract. The POD's simple, rugged design requires minimal maintenance. Vendor and existing client testimonials suggest that maintenance, when required, constituted the occasional replacement of a hard drive or camera cover, which most client organizations service themselves.

However, as the City relocates the PODs more often than other agencies, staff is exploring a service contract with Security Lines, U.S. to provide routine equipment tune-ups, installation services, and system support to ensure reliable performance.