CITY OF OAKLAND

MEMORANDUM

TO: Darren Allison, Acting Chief of Police

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

SUBJECT: OPD Crime Lab Biometrics DNA Analysis Technology 2023 Annual Report

DATE: April 17, 2024

Background

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

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

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

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

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

2023 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 2023

The Forensic Biology Unit analyzed 382 requests between January 1, 2023 to December 31, 2023. Over 2,255 items of evidence were examined, from which 4,969 samples were subjected to digestion and extraction using the Versa and EZ1/2 instruments. Scientist subjected 5,038 samples to quantitation analysis using the SpeedVac, Qiagility, and QuantStudio 5 instruments and 2,197 samples were subjected to amplification and typing methods using the ProFlex and 3500 instruments. The DNA profiles were processed with FaSTR and ArmedXpert software.

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

Discovery to the Alameda County District Attorney's Office was provided in 33 cases. A standard discovery packet includes the reports, technical and administrative review sheets, case notes, attachments, contact log, resume, interpretation guidelines, photographs, electronic data, and any supporting documents.

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

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

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

All evidence was analyzed at the laboratory located in the PAB. No other locations are authorized. As for the geographic location of crimes, this is not collected by the laboratory in a way that can be disseminated easily. The address may be reported on the request for laboratory services form, but it is not required for analysis to proceed. The laboratory services crimes that occur in all areas of the City of Oakland.

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

No community complaints or concerns were communicated to staff. The laboratory did not receive any complaints through its feedback process.

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

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

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

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

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

In terms of data, the City of Oakland was subjected to a ransomware attack that rendered all but essential services offline. The attack was first detected on the evening of Wednesday February 8, 2023. By Thursday morning it became evident that the attack was serious and widespread throughout the City of Oakland; however, it did not at that time appear to have reached Laboratory files. On Thursday afternoon we were ordered by the City's Internet Technology Department (ITD) to immediately sever our network connections in order to limit the proliferation of the ransomware.

The full scope and impact of the attack was not communicated to the laboratory; however, it was confirmed a ransomware attack known as ".PLAY" (hereinafter, "the virus") was responsible. As the virus spread, it encrypted and presumably copied data. According to City of Oakland notifications, it has been confirmed that some data including personnel records was copied and released to the public on the "dark web".

All data on the laboratory's network share was encrypted and tagged with the .PLAY file tag, indicating at least that the data was accessible to the malware group. The City has disclosed few details about what information was taken and what has been released. It is not known whether the network share data was stolen or has been included in the data that has been released by the .PLAY ransomware group.

All cloud-based data, which includes the Laboratory's controlled documents, appeared to have been unaffected. However, databases that host the Police Department's property and evidence unit (PEU) system and the Laboratory Information Management System (LIMS) were offline for several weeks. At this point it has only been confirmed that we lost database connectivity and .PLAY affected some files. The laboratory has not been informed whether the data contained in the LIMS SQL Server based back end database was taken.

The CODIS server was not affected by the data breach. The CODIS server is on a dedicated intranet line that uses encryption on both the sender and receiver ends of any communication from/to the server.

The full extent of the data breach is not known to laboratory staff. The city has been advised by outside counsel not to discuss what, if any, information they have on the contents of the stolen files. We have also been informed that we many never know the extent to which files were access. To date, the laboratory has received no confirmation that casework data was among the data release in the unauthorized data breach. Laboratory staff has appealed to top management of ITD to provide a detailed statement on the extent of the information to

the City of Oakland's Privacy Advisory Committee. ITD has responded with only a general statement with no specifics.

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

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

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

The laboratory completed 382 requests in 2023. These are further broken out by crime type in Table 1 below

Table 1: OPD Crime Laboratory DNA Analysis Requests in 2023

Crime Type	**Number of Requests**
Homicide	104
Attempted Homicide	10
Rape	102
Other Sexual Assault (not rape)	42
Assault	38
Robbery	14
Burglary	1
Carjacking	8
Hit and run	6
Weapons	49
Other Person	3
Other Criminal	1
Control Substance	1
Cold Case	3
Total	**382**

CODIS hits in 2023 – One hundred and thirty-five DNA profiles were uploaded to the CODIS database. The laboratory had one hundred and thirty associations (hits); sixty-one hits to named individuals whose identity were unknown, seven hits to unsolved forensic cases, and sixty-two 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 is one public record requests for sexual assault kits collected between 2015 – 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:

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 $3,290 to maintain; 3 instruments for $9,870 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 $3,776 to maintain; 3 instruments for $11,328 annual maintenance*
- *QuantStudio 5: $57,000 to purchase (x2 instruments = $114,000) and $7,030 to maintain; 2 instruments for $14,060 annual maintenance*

DNA Normalization / Amplification

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

DNA Typing

3500: $135,000 to purchase, $13,050 annual maintenance

DNA Interpretation

STRmix: $66,000 to upgrade, $21,402 annual maintenance
FaSTR: $37,000 to purchase, $8,000 annual maintenance
ArmedExpert: $15,000 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.

The cost of testing reagents/kits was approximately $140,000, however, this does not include consumables such as scalpels, masks, gloves, plastics, slides nor serological test kits.

Total purchase cost (born over several years): $894,800
Total maintenance cost, 2023: $90,628
Total testing cost reagents/kits, 2023: $140,000
Estimate of consumables: $150,000

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

The 2022 approved Surveillance Impact report and Biometric Technology Use Policy (SUP) were reviewed. Updates of annual costs are included. 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 with this report, please contact, Criminalistics Laboratory Manager, at ssachs@oaklandca.gov.

Respectfully submitted,

_____

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

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

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

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