CITY OF OAKLAND

Privacy Advisory Commission

September 3, 2020 5:00 PM
Zoom Online Meeting
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**: Heather Patterson*

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.

Please click the link below to join the webinar:

https://us02web.zoom.us/j/82465546845

Or iPhone one-tap :

US: +16699009128, 82465546845# or +13462487799, 82465546845#

Or Telephone:

Dial(for higher quality, dial a number based on your current location):

US: +1 669 900 9128 or +1 346 248 7799 or +1 253 215 8782 or +1 301 715 8592 or +1 312 626 6799 or +1 646 558 8656

Webinar ID: 824 6554 6845

International numbers available: https://us02web.zoom.us/u/kcZciaXqOb

1. Call to Order, determination of quorum
2. Open Forum/Public Comment
3. Review and approval of the draft August meeting minutes

4. Surveillance Equipment Ordinance – OPD – Forensic Logic Impact Report and proposed Use Policy - review and take possible action.

5. Surveillance Equipment Ordinance – OPD – Exigent Circumstances Use Reports – review and take possible action.

6. Surveillance Equipment Ordinance – OPD – Live Stream Use Reports – review and take possible action.

7. Surveillance Equipment Ordinance Amendments – Hofer/Patterson/Gage – review and take possible action.

    a. Prohibition On Predictive Policing And Remote Biometric Surveillance Technology
    b. Annual Report metrics and due dates
    c. Additional cleanup language

8. Sanctuary Contracting Ordinance – CPO – Annual Report – review and take possible action.

CITY OF OAKLAND

Privacy Advisory Commission

August 6, 2020 5:00 PM
Zoom Online Meeting
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, **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**: Heather Patterson*

---

1. Call to Order, determination of quorum

Members Present: Hofer, Gage, Suleiman, Brown, Katz, De La Cruz, Tomlinson, Oliver.

2. Open Forum/Public Comment

One Speaker: Asada Olugbala spoke about two items; first her belief that people's cameras should be on during meetings (not just audio) and about the collection of bad data leading to tragic results such as what happened to Brianna Taylor.

3. Review and approval of the draft July meeting minutes

The Minutes were adopted unanimously with one correction, the spelling of Sameena Usman's name.

4. Surveillance Equipment Ordinance – DOT – Automated License Plate Reader Annual Report – review and take possible action.

Michael Ford. The City's Parking Manager presented the annual report and received questions.

One Public Speaker was called: Asada Olugbala asked why, if the state considered these devices constitutional, was the PAC reviewing its use. She also asked about data retention and whetherthe data was purged and how quickly.

Member Katz asked about Disabled parking placards and whether ALPR inadvertently issued tickets to those with placards. Michael Ford explained that all tickets are still manually generated, the ALPR just helps create efficiencies as to identifying potential violators.
Member Suleiman asked about the efficacy of the investment and whether it was measurable. Michael Ford noted that he sees a doubling of productivity for the technicians using the system.
Member Tomlinson asked about whether penetration testing was done and Michael Ford was unaware but did ask Conduent (the contractor) to provide audit trials and notify him of any breaches.
The Report was adopted unanimously.

5. Surveillance Equipment Ordinance – OPD – Forensic Logic Impact Report and proposed Use Policy - review and take possible action.

The focus of the discussion of the Forensic Logic Use Policy was on data sharing with outside agencies. Bruce Stoffmacher with OPD tried to illustrate how data sharing improves working relationships and results, sighting the ATF Gun Tracing efforts that Oakland is part of. He also noted that Forensic Logic had a feature that could block data based on SB54 rules to prevent ICE from getting it.

Captain Bassett also noted the usefulness of data sharing but some PAC Commissioners questioned the use. Member Katz asked what the utility of sharing with a Texas jurisdiction is. DC Holmgren spoke and noted that it is very common for Oakland to find a wanted homicide suspect as far away as Texas or Florida and that these pieces of information make that possible.

Member De La Cruz and Suleiman both asked if the list of agencies was complete and what agencies OPD did not want to compromise on. It was asked if the reason for the search/data sharing could be filtered in the system.

Th item will be brought back in September.

6. Surveillance Equipment Ordinance Amendments – Hofer/Patterson/Gage – review and take possible action.

Chari person Hofer opened by calling for Public Speakers and one person spoke: Asada Olugbala stated that Predictive Policing (which would be restricted in the proposed modifications to the ordinance) is very problematic because it relies on biased data to begin with.

The group discussed the definition of Predictive Policing and the annual reporting schedules but agreed to have an ad hoc group continue to meet with OPD and bring back recommendations in September.

DEPARTMENTAL GENERAL ORDER

I-24: FORENSIC LOGIC COPLINK

Effective Date:

Coordinator: Information Technology Unit

FORENSIC LOGIC COPLINK

The purpose of this order is to establish Departmental policy and procedures for the use of the Forensic Logic, LLC. CopLink Data System

VALUE STATEMENT

The purpose of this policy is to establish guidelines for the use of the Forensic Logic, LLC. CopLink law enforcement data search system. The Oakland Police Department (OPD) uses crime databases to provide OPD personnel with timely and useful information to investigate crimes and analyze crime patterns.

A. Purpose: *The specific purpose(s) that the surveillance technology is intended to advance*

Forensic Logic, Inc. ("Forensic Logic") built a data warehouse that integrates and organizes data from databases such as Computer Assisted Dispatch (CAD) and Records Management System (RMS) and other law enforcement information systems from different law enforcement agencies. Forensic Logic provides two core services for OPD: 1) crime analysis reports; and 2) data search.

1. Crime Analysis Report Production – Forensic Logic categorizes and organizes incidents by offense types that allows OPD crime analysts to produce crime analysis reports such as point in time year-to-date and year-to-year comparisons. The categorization takes thousands of penal code types and organizes the data in a comprehensive manner to tabulate data into standard Federal Bureau of Investigation (FBI) Uniform Crime Report Part One and Part Two crimes.
2. Search – OPD data (e.g., CAD/RMS) is searchable with other agency law enforcement data. Personnel can use the system to search crime reports for structured data (e.g., suspect names) and unstructured data (e.g., a vehicle description). The cloud-based search system is accessible via a secure internet web browser requiring user authentication from vehicle mobile data terminal (MDT), web-enabled computers on the OPD computer

network, or via OPD-issued and managed mobile devices.

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

The authorized uses of Forensic Logic system access are as follows:

- Crime Analysis Report Production – Authorized members may use the customized system to organize OPD crime data into Crime Analysis Reports. Forensic Logic built a system that categorizes thousands of penal codes based on hierarchical crime reporting standards, into a concise, consumable report template.
- CopLink Search – Authorized members may use CopLink for the purpose of searching the system in the service of conducting criminal investigations, such as apprehending subjects, locating and returning stolen property, as well as in the protection of the law enforcement officers encountering the individuals described in the system. Authorized purposes also include other appropriate OPD organizational investigations (e.g., internal affairs, missing persons, and use of force investigations).

Rules and Processes Prior to use

- Only sworn law enforcement personnel or authorized professional staff employed and working under the supervision of a law enforcement agency (typically crime analysts and dispatchers) may access the Forensic Logic CopLink network.
- OPD personnel authorized to use Forensic Logic CopLink receive required security awareness training prior to using the system. Forensic Logic requires users to have the same training to access the Forensic Logic CopLink network as users are required to be trained to access data in CLETS, the FBI NCIC system or NLETS. Users are selected and authorized by OPD and OPD warrants that all users understand and have been trained in the protection of Criminal Justice Information (CJI) data in compliance with FBI Security Policy. All Forensic Logic CopLink users throughout the Forensic Logic CopLink network have received required training and their respective law enforcement agencies have warranted that their users comply with FBI CJI data access requirements.
- Users shall not use or allow others to use the equipment or database records for any unauthorized purpose; authorized purposes consist only of queries related to authorized investigations, internal audits, or for crime analysts to produce crime analysis reports. The purpose of the Forensic Logic CopLink network is to provide a computerized database for ready access by a criminal justice agency making an inquiry and for prompt disclosure of information in the system from other criminal justice agencies about crimes and criminals. Users are required to abide by the Terms of Service of the Forensic Logic CopLink network when they access the system. The Terms of Service that every User agrees to include the following statements:
    1. *I will use the Forensic Logic Coplink Network™ only for the administration of criminal justice or the administration of data required to be stored in a secure sensitive but unclassified data environment.*

2. *I will respect the confidentiality and privacy of individuals whose records I may access.*
3. *I will observe any ethical restrictions that apply to data to which I have access, and to abide by applicable laws or policies with respect to access, use, or disclosure of information.*
4. *I agree not to use the resources of the Forensic Logic Coplink Network™ in such a way that the work of other users, the integrity of the system, or any stored data may be jeopardized.*

I am forbidden to access or use any Forensic Logic Coplink Network™ data for my own personal gain, profit, or the personal gain or profit of others, or to satisfy my personal curiosity.

- The following warning is displayed for every user session prior to user sign on:

  WARNING: *You are accessing sensitive information including criminal records and related data governed by the FBI's Criminal Justice Information System (CJIS) Security Policy. Use of this network provides us with your consent to monitor, record, and audit all network activity. Any misuse of this network and its data is subject to administrative and/or criminal charges. CJIS Security Policy does not allow the sharing of access or passwords to the Forensic Logic Coplink Network™. The data content of the Forensic Logic Coplink Network™ will not be considered for use as definitive probable cause for purposes of arrests, searches, seizures or any activity that would directly result in providing sworn testimony in any court by any participating agency. Information available in the Forensic Logic Coplink Network™ is not probable cause, but indicates that data, a report or other information exists in the Records Management System or other law enforcement, judicial or other information system of an identified participating agency or business.*

  In accordance with California Senate Bill 54, applicable federal, state or local law enforcement agencies shall not use any non-criminal history information contained within this database for immigration enforcement purposes. This restriction does not pertain to any information that is regarding a person's immigration or citizenship status pursuant to 8 U.S.C. §§ 1373 and 1644.

- Accessing CopLink data requires a right to know and a need to know. A right to know is the legal authority to receive information pursuant to a court order, statutory law, or case law. A need to know is a compelling reason to request information such as direct involvement in a criminal investigation.

C. ***Data Collection:*** *The information that can be collected by the surveillance technology. Where applicable, list any data sources the technology will rely upon, including "open source" data;*

Forensic Logic has created a file transfer protocol to automatically ingest several data systems into the Forensic Logic CopLink system. These databases include

CAD/RMS and FBR. Additionally, OPD is discussing the possibility of incorporating National Integrated Ballistic Information Network (NIBIN) firearm shell casing data into the system. No ALPR data collected by OPD-owned technology shall be extracted by Forensic Logic's systems. An exhaustive list of data sets ingested by Forensic Logic CopLink from OPD data sources follows.

Data Source Collected	**Collection Status**	**Retention Policy**	**Access Conditions**
Arrest	Active	Perpetual	Only law enforcement; US DHS prohibited
Field Contacts	Active	Perpetual	Only law enforcement; US DHS prohibited
Incident Reports	Active	Perpetual	Only law enforcement; US DHS prohibited
Calls for Service	Active	Perpetual	Only law enforcement; US DHS prohibited
Stop Data	Active	Perpetual	Only law enforcement; US DHS prohibited
Traffic Accident	Active	Perpetual	Only law enforcement; US DHS prohibited
ShotSpotter	Active	Perpetual	Only law enforcement; US DHS prohibited
ATF NIBIN Ballistics	Proposed	Perpetual	Only law enforcement; US DHS prohibited

There are several "Elements of the Search" component – all of which are specialized presentations of search[1]: (see related Surveillance Impact Report for a detailed analysis:

- The search bar;
- The Tag Cloud element - how search results are visualized by increasing the font size in a Tag Cloud to be representative of the number of occurrences;
- Facet search - organizes search capabilities into a number of static

[1] See related Surveillance Impact Report for a detailed description of each 'search' module

categories (e.g. offense descriptions, agencies);

- Time Search - permits users to quickly drill down to specific time periods;
- Timeline search - organizes the data visually on a timeline;
- Geospatial search - permits a user to select geographies (e.g. Beats or Areas; areas around schools, custom areas);
- Search Charting Module - organizes search results into categories visualized by bar charts;
- Link Chart - produces a visualization of records that are linked based on several criteria including name, offense and location.

Forensic Logic CopLink also consists of the following modules:

- CopLink Connect (formerly called forums);
- CopLink Dashboard, and CopLink Trace (gun-tracing);
- CopLink Connect - a secure internal communication system for intra-agency CJIS-compliant communications.

D. Data Access: *The category of individuals who can access or use the collected information, and the rules and processes required prior to access or use of the information*

Authorized users include all sworn personnel, Crime Analysts, Police Evidence Technicians, personnel assigned to OIG, and other personnel as approved by the Chief of Police.

OPD data in the Forensic Logic CopLink system is owned by OPD and not Forensic Logic and is drawn from OPD underlying systems. OPD personnel shall follow all access policies that govern the use of those originating OPD technologies.

OPD's Information Technology (IT) Unit shall be responsible ensuring ongoing compatibility of the Forensic Logic CopLink System with OPD computers and MDT computer systems. OPD's IT Unit will assign personnel to be responsible for ensuring system access and coordinate with Forensic Logic. CopLink Search users are managed through a centralized account management process by Forensic Logic support personnel.

E. Data Protection: *The safeguards that protect information from unauthorized access, including encryption and access control mechanisms;*

Forensic Logic constantly processes large streams of criminal justice information (CJI) and thus must comply with the provisions of the Criminal Justice Information Services (CJIS) Division of the Federal Bureau of Investigation (FBI) and the FBI

Security Management Act of 2003 and CJIS Security Policy. Forensic Logic, along with their partner at Microsoft Azure Government and the National Law Enforcement Telecommunications System (NLETS), have developed strong CJIS-compliant data security protocols.

F. *Data Retention*: *The time period, if any, for which information collected by the surveillance technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s), the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond that period;*

Forensic Logic follows the data retention schedules reflective of OPD's data retention schedules. Data that is deleted from OPD CAD/RMS or other systems will be automatically deleted from Forensic Logic CopLink system. OPD can also request that OPD data be expunged from the Forensic Logic CopLink system where appropriate based on changes to incident files.

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

The Weekly Crime Analysis Reports prepared using Forensic Logic's analysis of OPD crime data are regularly made available to the public on OPD's website. The CopLink system is only provided for OPD personnel and is not available to the public.

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

Other than selected individuals with a right to access at ITD, no other non-OPD City entities may access the Forensic Logic system. Many law enforcement agencies (city police departments and county sheriff offices) utilize Forensic Logic CopLink. ***Attachment A*** to this Use Policy provides a list of agencies[2] that are clients of Forensic Logic and have access to OPD data through CopLink Search.

Many ~~I~~law enforcement agencies that are clients of Forensic Logic have access to OPD data through CopLink – a complete list is provided in ***Appendix D*** to the CopLink Surveillance Impact Report. ~~in the following CA counties currently either have access and/or contribute or plan to contribute data to the Forensic Logic CopLink network.~~

[2] This list represents all agencies who are able to see OPD data. These agencies do not actually necessarily see OPD data; OPD data only comes up in a search result list if something in the record has the same terms as those that a user puts into the search box. The further away from the location of the incident, an OPD record is unlikely to be in the top few results pages unless the exact person is found.

Commented [BH1]: This category pertains to data, not a report. This needs to be addressed.

Commented [BS2R1]: The reports are a function of the technology and represent a form of "public access."

Commented [BH3]: Huh?

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

OPD's IT Unit shall ensure the development of training regarding authorized system use and access.

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

The OPD IT Unit will manage audit requests in conjunction with Forensic Logic, Inc.

Commented [BH4]: From whom?

Commented [BS5R4]: The intent here it to explain who in OPD is responsible internally rather than detail the actual information of a potential audit, similar to saying that IT unit is responsible for annual report below.

Per FBI CJIS Security Policy, Paragraph 5.4, Forensic Logic logs information about the following events and content and a report can be produced upon request at any time.

5.4.1.1 Events

The following events shall be logged:

1. Successful and unsuccessful system log-on attempts.
2. Successful and unsuccessful attempts to use:
    a. access permission on a user account, file, directory or other system resource;
    b. create permission on a user account, file, directory or other system resource;
    c. write permission on a user account, file, directory or other system resource;
    d. delete permission on a user account, file, directory or other system resource;
    e. change permission on a user account, file, directory or other system resource.
3. Successful and unsuccessful attempts to change account passwords.
4. Successful and unsuccessful actions by privileged accounts.
5. Successful and unsuccessful attempts for users to:
    a. access the audit log file;
    b. modify the audit log file;
    c. destroy the audit log file.

5.4.1.1.1 Content

The following content shall be included with every audited event:

1. Date and time of the event.

2. The component of the information system (e.g., software component, hardware component) where the event occurred.
3. Type of event.
4. User/subject identity.
5. Outcome (success or failure) of the event.

OPD's IT Unit shall provide the Chief of Police, Privacy Advisory Commission, and City Council with an annual report that covers use of Forensic Logic's CopLink and Crime Reporting modules during the previous year. The report shall include all report components compliant with Ordinance No. 13489 C.M.S.

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

Forensic Logic, Inc. shall be responsible for all system maintenance per the OPD-Forensic Logic, Inc "software as a service" or (SAAS) contract model.

By Order of

Susan E. Manheimer

Chief of Police Date Signed:

OAKLAND POLICE DEPARTMENT

Surveillance Impact Report:

Forensic Logic, Inc. CopLink Search and Crime Report System

A. Description: Crime Analysis Report System and CopLink Search, and How they Work

The Forensic Logic, Inc. ("Forensic Logic") supported crime analysis report system is based on a comprehensive categorization and organization of California penal code offense types that allows OPD crime analysts to produce various crime reports such as point in time, year-to-date and year-to-year comparisons. The categorization takes thousands of penal code types and organizes the data into several hierarchies in a comprehensive manner to tabulate data into standard Federal Bureau of Investigation (FBI) Uniform Crime Reporting (UCR) Part One and Part Two crimes.

The CopLink search engine combines criminal justice information from various law enforcement systems owned and operated by agencies throughout the United States. Forensic Logic maintains a secure data warehouse within the Microsoft Azure Government Cloud. Core datasets include computer-aided dispatch (CAD) and record management system (RMS) crime incident data (see "Elements of the Search" on "Data Types and Sources Section – pages 14,15 below for list of features).

Forensic Logic first built their data warehouse by focusing on search engine technology; they built indexing algorithms to understand natural language, decode law enforcement vernacular, extract entities and relationships from the data, and then rank results based on the seriousness of the offense and the proximity to a user's location and time of event. The original LEAP search system allowed for the aggregation of structured, semi-structured and unstructured data into a common repository.

International Business Machines (IBM) originally acquired CopLink in 2012; Forensic Logic has since purchased CopLink from IBM and begun to integrate the two systems under the brand of Forensic Logic CopLink.

Crimes committed in Oakland are sometimes connected to crimes, suspects, and evidence from crimes in neighboring cities. The Forensic Logic CopLink system integrates data that may come from outside agencies but that relates to crime that occurs in Oakland. Additionally,

providing OPD data to other agencies in the region empowers those agencies to better investigate crimes that have a nexus to Oakland.

Forensic Logic CopLink takes the diverse data sources and types and uses algorithms to rank searches based on a hierarchical weighted logic system. For example, data connected to more serious and violent crime is ranked higher; data related to more geographically close data is ranked higher; and more recent data is ranked higher.

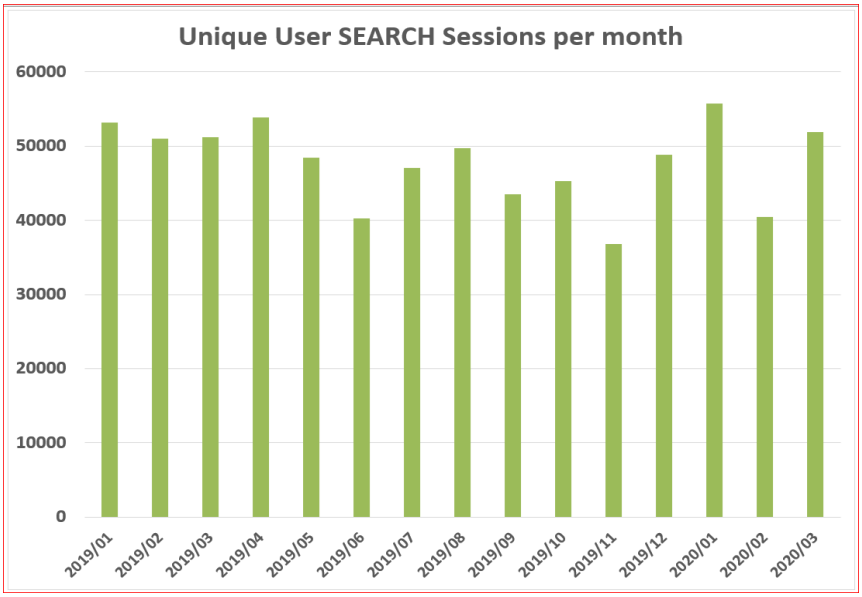
B. Proposed Purpose

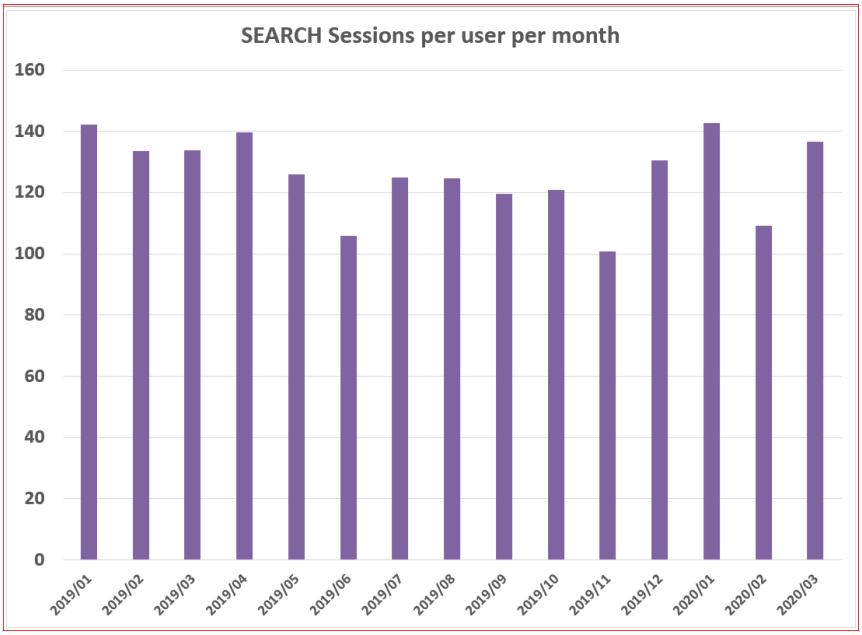
Forensic Logic provides three core services for OPD: a) crime analysis report production; b) search; and c) technical assistance**.**

1. Crime Analysis Report Production – Forensic Logic has built a comprehensive categorization and data organization structure that allows OPD crime analysts to better access OPD's own data - the categorization takes thousands of penal code types and organizes the data in a comprehensive manner to tabulate data into standard Federal Bureau of Investigation (FBI) UCR Part One and Part Two crimes.

   These reports provide useful information about crime trends in easily consumable formats (year-to-date, point in time, and year-to-year comparisons). The reports summarize key crime types such as robberies and burglaries, summarizing hundreds of sub-penal codes. The reports are also sub-divided into each of the five police areas. These reports are regularly used by both the Office of the Mayor and City Council as well as members of the public. These reports are also used by Community Resource Officers (CROs) to present crime updates to Neighborhood Crime Prevention Councils (NCPCs) throughout the City. The technology allows for a streamlined process that would take orders of magnitude in additional staff hours were crime analysts to compile the reports using only OPD-owned technology.

2. Search – Officers and other assigned personnel need access to well organized law enforcement data to solve serious and violent crime, such as homicides and robberies. The following tables provide data on actual OPD Forensic Logic CopLink search usage (unique searches by month, number of searches per officer per month).


Unique User SEARCH Sessions per month
60000
50000
40000
30000
20000
10000
0
2019/01
2019/02
2019/03
2019/04
2019/05
2019/06
2019/07
2019/08
2019/09
2019/10
2019/11
2019/12
2020/01
2020/02
2020/03


SEARCH Sessions per user per month
160
140
120
100
80
60
40
20
0
2019/01
2019/02
2019/03
2019/04
2019/05
2019/06
2019/07
2019/08
2019/09
2019/10
2019/11
2019/12
2020/01
2020/02
2020/03

CopLink: Critical Tool for Crime Investigations

Criminal Investigation Division (CID) investigators use the Forensic Logic CopLink search capability (formerly known as LEAP) daily and run the majority of their cases through the search portal to look for suspects or any leads. The following examples highlight some of the many ways LEAP / CopLink is used many times every day by CID investigators, patrol officers, and officers assigned to special units:

- An officer assigned to OPD's Ceasefire Strategy[1] was provided a nickname for a shooting suspect, but was not provided any further identifying information. The officer conducted a query of the nickname in CopLink and due to the uniqueness of the nickname was able to determine her identity from a human-trafficking investigation. The nickname apparently was the alias that she used during that arrest. The officer conducted additional queries using the suspect's true name and found numerous contacts between her and the primary shooting suspect. The large majority of these contacts were from the Las Vegas, NV metro area, and this provided an important new source of information**.**

- There was a shooting in January 2020 in West Oakland. A typo caused an incorrect telephone number to be entered into OPD's CAD. The investigator was nonetheless able to find additional contact information for the witness in CopLink using different variations of the witness' name; this search led to a good telephone number from a report she had filed the previous year. The officer called this witness and she provided useful information which led to a charge in the case.

- A CID investigator was able to identify a suspect using CopLink in a serious sexual assault case and connect the suspect to two additional reports where he is listed as suspect of similar sexual assaults – San Leandro PD and Hayward PD were also able to connect the same suspect to their cases using CopLink.

- An officer who was investigating a violence against woman crime[2] found a suspect who was also linked to a similar prior crime; the officer was able to connect with this previous victim, obtain testimony and provide a level of support and justice that so far had not occurred. The OPD officer was able to combine data from the cases to further the investigation of each case.

- A homicide investigator was able to recently connect a nickname

[1] https://www.oaklandca.gov/topics/oaklands-ceasefire-strategy
[2] https://www.justice.gov/ovw/about-office

to a legal name of a suspect of in a recent homicide, now charged by the District Attorney's Office; this officer confirms using LEAP / CopLink on almost every homicide investigation over several years.

- A CopLink search revealed the suspect vehicle involved in a recent East Oakland robbery was also involved in one in City of San Francisco. The investigator collaborated with the San Francisco Police Department (SFPD) and ultimately wrote an arrest warrant.

- A CopLink search on an auto burglary suspect vehicle, revealed that the suspect vehicle was connected to several other auto burglaries. Officers located and towed the suspect vehicle. The vehicle is now being analyzed by OPD evidence technicians for more clues.

- A firearm assault and shooting case resulted in an arrest and charge, as video footage showed a unique SUV; officers used CopLink to search for the SUV using descriptive terms, which led to an address and search warrant.

The CopLink platform facilitates the revelation of information vital to the expeditious and successful conclusion of criminal investigations in two ways: (i) through the collection of many types of structured and unstructured (e.g. text narratives) law enforcement data originating from many different law enforcement agencies; and (ii) the continuous ranking of the data as it enters the CopLink platform based on a number of factors including seriousness of offense, proximity to a user's search location and recency of the data so a user conducting a search finds the information being sought in the first pages of the resulting list of documents.

As is often the case, offenders are mobile and have had encounters with law enforcement in many jurisdictions and the collection of data from multiple law enforcement agencies in the CopLink platform provides broader coverage for the search engine to locate related information.

CopLink Usage with Federal Partners

Commented [BS1]: Changed from "by"

OPD relies on several partnerships with local and federal agencies for regular ongoing support with investigations into serious violent crime. OPD is part of a Council-approved partnership with the United States Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), focusing in particular on firearms-related felonies. The ATF San Francisco Field Division has two units with personnel who have access to CopLink. These units are the Crime Gun Enforcement Team (CGET) in

Oakland, CA and the Crime Gun Intelligence Center (CGIC) in Dublin, CA. The CGET is an investigative unit comprised of ATF Special Agents and state/local Task Force Officers focused on the investigation and prosecution of suspects related to violent crime, specifically gun violence, in the Alameda County and Contra Costa County areas (also includes Vallejo). The CGIC is comprised of ATF Special Agents and Intelligence Research Specialists focused on the analysis of gun violence and NIBIN leads for the entire San Francisco Field Division, which covers Northern California and Nevada.

Many of the shootings investigated by CGIC and CGET unfortunately occur within the City of Oakland. CopLink allows quick access to information related to these shooting events, which is vital to determining the viability of leads based on ballistic testing (NIBIN). The analysis of these leads along with the partnership between the ATF CGIC, CGET and the OPD CGIC allows investigators from both OPD and ATF to conduct investigations aimed at both solving shootings as well as perfecting cases on violent offenders to decrease the volume of violent crime in the area. CopLink is also utilized to identify suspects and, their criminal associates, vehicles, and residences. This type of search is important in both conducting investigations into these violent criminals, but also in locating and arresting them once charges have been filed. CopLink is used daily by ATF personnel to access OPD reports and the reports of other agencies in the area. Information is used for criminal investigations and the analysis of violent crime only. The CGET, as the primary ATF user of LEAP, only conducts investigations related to firearm violence, illegal firearm possession by violent offenders, and the trafficking of firearms to gangs and/or other persons likely to be engaged in violence. No other federal agency is a part of the CGET or has access to CopLink through ATF. Without CopLink, it would be virtually impossible, to analyze NIBIN leads, which often incorporate numerous crime guns and numerous jurisdictions outside of OPD. Without the quick access CopLink provides, it would take countless man hours to ascertain details, which lead to the identification of shooters, as well as the prosecution of individuals for those shootings. Without this information, many violent crime investigations in the Oakland area would not only take much longer, but would be less likely to come to fruition due to the volume of violent crime in the city.

There are FBI personnel working at the Police Administration Building (PAB) as part of the Council-approved FBI Safe Streets Taskforce. Through this partnership, both OPD-assigned officers and FBI personnel collaborate on investigations using separate firewall-protected computer networks for computer-related research - OPD personnel and FBI personnel utilize separate CopLink accounts. The FBI and OPD personnel use CopLink daily to investigate violent sexual offenders as part of support for OPD's Special Victims Section (focusing on human

and sexual trafficking crimes). These types of crimes do not conform to city borders and investigators need access to data for a larger geographic area.

3. Technical Assistance

   OPD occasionally solicits Forensic Logic's technical expertise to integrate and tabulate data such as from OPD Field Based Reporting systems to analyze stop data. Forensic Logic has also assisted OPD with the following projects over the past few years:

   a. The development of the first OPD CompStat weekly review using both interactive Google Earth maps and detailed Area maps and reports;
   b. The development of the first Stop Data search and analysis system employed by the Federal Independent Monitoring Team and used successfully by OPD to achieve many of the criteria required of Task 34 of the NSA; staff from the OPD Office of the Inspector General still use CopLink for risk management assessments.
   c. The evaluation and analysis of OPD's reporting to the FBI of monthly UCR reports to confirm that incidents were reported correctly and in a timely manner; and
   d. The facilitation of the Forensic Logic search roduct for use on OPD mobile devices in the field.

C. Locations Where, and Situations in which the Forensic CopLink System may be deployed or utilized.

The technology is provided to patrol officers, investigators, and other appropriate personnel. The system is also used within the Department primarily by crime analysts to produce weekly and customized crime reports that are used by the Mayor's Office and the City Council. The Weekly Crime Report (April 20-26, 2020) (see ***Appendix A*** at end of this report) was produced by the OPD Crime Analysis Unit with the assistance of Forensic Logic and their offense categorization developed to compile the report. The report provides data on Type 1 crimes occurring in Oakland during the week of April 20-26, 2020 with comparisons to the year to date 2018, 2019, and 2020.

D. Impact

The aggregation of data will always cause concern of impacts to public privacy. Data collected and stored in the Forensic Logic CopLink network has previously been collected by law enforcement agencies in an originating data

source. Those data sources include calls for service (originated in Computer Aided Dispatch systems); incident reports, field contacts and arrests (originated in Records Management Systems); time and location where firearms have been discharged (originated from from Gunshot Location Systems); time, location, description and disposition of on-view field contacts; warrants and wants from probation, parole and court systems; booking information and mug shots (originated from Jail Management Systems); and description of events reported by the public compiled in drug hotline and other tip lines. Data is already collected, stored and shareable with other law enforcement agencies by OPD.

Oakland residents who may not have a legal immigration status have a right to privacy. The California Values Act (SB 54 [3]) is enacted to ensure that (barring exceptions contained in the law), no state and local resources are used to assist federal immigration enforcement. Forensic Logic has developed protocols described below in the mitigations section which mitigate the potential for the release of data which could impact immigration status-related privacy rights.

OPD understands that members of the Oakland community as well as the Privacy Advisory Commission (PAC) are concerned about potential privacy impacts associated with OPD's use of ALPR. For this reason, for the past five years OPD has not allowed its ALPR data to be entered into Forensic LEAP Search or Forensic Logic CopLink system and all prior collected ALPR data has been expunged from the system – even though many other participating agencies share ALPR data, and OPD could benefit from this data commingled in the Forensic Logic CopLink system.

Forensic Logic complies with all federal (e.g. FBI CJIS Security Addendum), state (e.g. SB 54) and local laws (e.g. Oakland Sanctuary City Ordinance[4]) associated with use of collected law enforcement data. This includes, in the state of California and many individual jurisdictions, the prohibition on the use of facial recognition and the analysis of body worn camera video data.

E. Mitigations

OPD and Forensic Logic utilize several strategies to mitigate against the potential for system abuse and/or data breach.

System Mitigations

In accordance with CJIS Security Policy (CSP) 5.8[5], the Forensic Logic CopLink application keeps all user access and activity logs, which can be made available to agency command staff and/or administrators at any time – OPD has the ability to

[3] https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB54

[4] https://oakland.legistar.com/LegislationDetail.aspx?ID=3701155&GUID=8153C1B0-B9FC-4B29-BDDE-DF604DEDAEAD&Options=&Search=

[5] https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center

request detailed query logs of OPD personnel CopLink usage. Per FBI CJIS Security Policy v5.8, Paragraph 5.4, Forensic Logic logs information about the following events and content and a report can be produced upon request at any time:

5.4.1.1 Events

The following events shall be logged:

1. *Successful and unsuccessful system log-on attempts.*
2. *Successful and unsuccessful attempts to use:*
    a. access permission on a user account, file, directory or other system resource;
    b. create permission on a user account, file, directory or other system resource;
    c. write permission on a user account, file, directory or other system resource;
    d. delete permission on a user account, file, directory or other system resource;
    e. change permission on a user account, file, directory or other system resource.
3. *Successful and unsuccessful attempts to change account passwords.*
4. *Successful and unsuccessful actions by privileged accounts.*
5. *Successful and unsuccessful attempts for users to:*
    a. access the audit log file;
    b. modify the audit log file;
    c. destroy the audit log file.

5.4.1.1.1 Content

The following content shall be included with every audited event:

1. *Date and time of the event.*
2. *The component of the information system (e.g., software component, hardware*
component) where the event occurred.
3. *Type of event.*
4. *User/subject identity.*
5. *Outcome (success or failure) of the event.*

Therefore, OPD has the ability to conduct audits if there is reason to believe the system is not being used in accordance with criminal investigation protocols. *Data Security Mitigations*

Section G below (Data Security) provides an in-depth explanation of the many ways the Forensic Logic CopLink system itself is secure to data breaches. Data that is deleted from OPD CAD/RMS or other systems is automatically deleted from

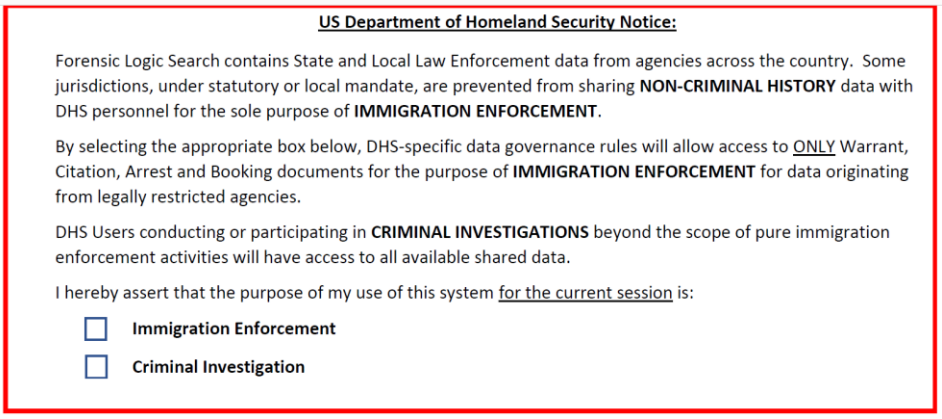
the Forensic Logic CopLink system.

Safeguards in Alignment with Oakland and California Immigrant Legal Protections

Forensic Logic has created technical mitigations to ensure that cities in California and elsewhere can use Forensic Logic CopLink while complying with SB54 and similar sanctuary city laws. Forensic Logic allows participating agencies to elect how their agency-generated data is shared within the Forensic Logic CopLink system.

Firstly, agencies such as OPD can specify that no data be shared with select federal law enforcement users – regardless of whether the query is for immigration-specific purposes. OPD has specified (current and future contracts) this protocol for sharing data so that no OPD data is shared with ICE or its Homeland Security Investigations (HSI) section

Forensic Logic partners with several federal agencies: The Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), the FBI, and the U.S. Marshals Service (two of the 94 U.S. Attorney Districts). Forensic Logic did have one contract with Immigrations, Customs and Enforcement (ICE) that expired on May 15, 2020. However, Forensic Logic is not seeking to further contract with ICE or other agencies prohibited from Oakland partnership under OMC 2.23.030. This contract, in fact, was created to examine how Forensic Logic could best isolate police agency data from any Department of Homeland Security (DHS)[6] searches. Some police departments (such as Oakland) want to ensure that ICE never has access to their data, while there are also agencies that only want ICE's HSI Section to have access for purely criminal (non-immigration) type investigations. Forensic Logic CopLink has since developed the following logic model in these cases for Department of Homeland Security queries:



This system does not apply to Oakland since Oakland data is never available to any DHS agencies – or to other federal agencies OPD may in the future

[6] ICE is one of several agencies organized within the umbrella DHS agency.

specify.

Data Access Safeguards

Indexing of public data into CopLink provides another tool that balances function and privacy mitigations. Some agencies subscribe to public data databases such as Thomson Reuters CLEAR (TRC). The Forensic Logic CopLink network has indexed abstracts (summary information lacking details) of certain public records available in the TRC service so that a single search in the Forensic Logic CopLink search service will reveal that the TRC service has more information about the topic. The data itself is not actually in CopLink – just an index of data type (similar to a library card catalog), similar to how common search engines index data without actually containing the data. Therefore, OPD cannot access this type of data (since OPD does not subscribe to TRC) - and the CopLink system queries will not show that more information is available in TRC.

OPD data additionally cannot be accessed by ICE nor other non-authorized agencies via the National Law Enforcement Telecommunications System (NLETS)[7]. NLETS is the main interstate justice and public safety network in the nation for the exchange of law enforcement, criminal justice, and public safety-related information. NLETS is a private, not-for-profit corporation owned by all 50 U.S. states; the user population is made up of all of the United States and its territories, all Federal agencies with a justice component, selected international agencies, and a variety of strategic partners that serve the law enforcement community-cooperatively exchanging data. NLETS provides two basic functions:

1. A communication network that switches queries primarily from law enforcement officers to law enforcement sensitive data stored at state Departments of Motor Vehicles (DMV) and the FBI National Crime Information Center (NCIC) where among other data sets, data about stolen vehicles and felony warrants is collected; and
2. A co-location and virtual data center where vendors associated with law enforcement (e.g. Forensic Logic) can rent space, power and virtual machines (computer servers) in a CJIS protected physical environment.

For the most part, NLETS does not store or collect data (only the message queries from its users and message responses), but rather transmits data directly to authorized users over its network from data owners such as the DMV and NCIC where stolen vehicle and felony warrant data is centralized. OPD incident data is not stored in NLETS; therefore, neither ICE nor other agencies can utilize CopLink and NLETS to access OPD data.

[7] https://www.nlets.org

F. Data Types and Sources

Forensic Logic has created file transfer protocol data feeds to automatically ingest several data systems into the CopLink system. These data include CAD/RMS, field-based reporting module data, calls for service, and ShotSpotter data that could be used to populate an ATF eTrace[8] gun tracing form. Additionally, OPD is discussing the possibility of incorporating National Integrated Ballistic Information Network (NIBIN) firearm shell casing data into the system.

An exhaustive list of data sets ingested by Forensic Logic CopLink from OPD data sources follows.

Data Source Collected	Collection Status	Retention Policy	Access Conditions
Arrest	Active	Perpetual	Only law enforcement; US DHS prohibited
Field Contacts	Active	Perpetual	Only law enforcement; US DHS prohibited
Incident Reports	Active	Perpetual	Only law enforcement; US DHS prohibited
Calls for Service	Active	Perpetual	Only law enforcement; US DHS prohibited
Stop Data	Active	Perpetual	Only law enforcement; US DHS prohibited
Traffic Accident	Active	Perpetual	Only law enforcement; US DHS prohibited
ShotSpotter	Active	Perpetual	Only law enforcement; US DHS prohibited
ATF NIBIN Ballistics	Proposed	Perpetual	Only law enforcement; US DHS prohibited

The purpose of the Forensic Logic CopLink network is to provide a computerized database for ready access by a criminal justice agency making an inquiry and for prompt disclosure of information in the system from other criminal justice agencies about crimes and criminals. This information assists authorized agencies in criminal justice and related law enforcement objectives, such as apprehending subjects, locating missing persons, locating and returning stolen property, as well as in the

[8] https://www.atf.gov/resource-center/fact-sheet/fact-sheet-etrace-internet-based-firearms-tracing-and-analysis

protection of the law enforcement officers encountering the individuals described in the system (see ***Appendix B*** below for a list of all agencies that are clients of Forensic Logic and have access to OPD data through CopLink Search[9]).

There are many types of OPD data that, by policy and process, will not be sent to Forensic Logic CopLink or to other Forensic Logic CopLink client agencies. The following data types and sources are not sent to Forensic Logic:

- OPD ALPR data
- Data from other City of Oakland Departments (e.g., code compliance data from Planning and Zoning).
- Unverified data from ongoing investigations
- Intelligence briefings
- Body worn camera video
- Data that includes the identities of confidential informants
- Any data that is categorized as criminal intelligence subject to 28 CFR Part 23 analysis or processing of booking or other photos for the purposes of identification of the subject using facial recognition[10] capabilities

There are three services that Forensic Logic provides to OPD: 1) Crime Report Production; 2) Search; and 3) technical assistance.

Forensic Logic provides its Search services as an enterprise subscription available to all sworn officers and authorized professional staff operating under the auspices of the Chief of Police.

There are several elements to the "Search" system – all of which are specialized presentations of the analysis capability within the Forensic Logic CopLink network:

- There is a more structured search capability than exists in the Search product that allows users to specify the parameters for each structured field in a report. An additional capability permits the structured search to be saved and directed to constantly monitor new data as it enters the system so that users are notified when the search terms satisfy new data. For example, if one is seeking a vehicle with a particular vehicle tag, they

[9] This list represents all agencies who are able to see OPD data. These agencies do not actually necessarily see OPD data; OPD data only comes up in a search result list if something in the record has the same terms as those that a user puts into the search box. The further away from the location of the incident, an OPD record is unlikely to be in the top few results pages unless the exact person is found.

[10] Forensic Logic Product Modules (see ***Appendix C***) shows that the older "Legacy" previously owned by IBM offered a feature called "FaceMatch" facial recognition. This system was used to provide five other faces similar to a suspect photo so victims and witnesses can look at the "6-pack" of faces and attempt to identify a person or suspect, similar to a line-up. Face-match is not in OPD's LEAP – rebranded as CopLink and Forensic Logic is not incorporating this technology into the new CopLink.

can create that search and request that any time that same vehicular tag is mentioned in a future report that I am to be notified.

- There is a reporting module that flexibly allows users to structure reports based on offense categories, time frames and geographical areas.
- There is a mapping component that allows one to visualize records in a particular region based on a number of structured data in a large number of data fields
- The geonet capability places linked incidents on a map so that both geospatial characteristics and common linked characteristics of crimes can be visualized
- The timeline feature organizes linked incidents by ordering the incidents chronologically and displaying those incidents on a map with connector lines illustrating the chronological timeline of the events

All of the modules above are included with the subscription to the the Forensic Logic CopLink network and are not provided independently. OPD has negotiated an enterprise subscription to the Forensic Logic CopLink product at no additional charge so all OPD sworn officers and authorized professional staff under the auspices of the Chief of Police will have access to all capabilities at no additional fee.

There are several “Elements of the Search” component – all of which are specialized presentations of search:

- The search bar operates exactly as a user would expect a google search to operate with the one exception being the ranking of results is optimized for law enforcement rather than advertising (as is the focus of a Google search since advertisers financially support the operation of the Google search capability).
- The Tag Cloud element is another presentation of how search results are visualized by increasing the font size in a Tag Cloud to be representative of the number of occurrences that a particular phrase occurs in the Forensic Logic CopLink system or a subset of the data.
- The Facet search is a tool that organizes search capabilities into a number of static categories such as offense descriptions, agencies, document types and vehicle tags, amongst other categories.
- The time search capability permits users to quickly drill down to specific years, months, days or times of incidents with simple button selections.
- Timeline search organizes the same data visually on a timeline so incidents and calls for service in subsets resulting from a Google-like search can be organized chronologically.
- Geospatial search permits a user to select geographies such as Beats or Areas; areas around schools; or custom areas selected using the user’s mouse to draw areas on a map in order to visualize and select incident

reports associated with the specific geographic region.

- The search Charting module organizes search results into categories visualized by bar charts such as offense descriptions, time of day, day of week, vehicle model and agency Beat amongst other data fields.
- The link chart capability produces a visualization of records that are linked based on a number of criteria including name, offense and location.

All of the search modules above are included with the enterprise subscription to the CopLink SEARCH service in the Forensic Logic CopLink network and are not provided independently

Forensic Logic provides its services as a Named User subscription available to selected sworn staff and authorized professional staff operating under the auspices of the Chief of Police.

Forensic Logic CopLink can also consists of the following modules: CopLink Connect (formerly called forums); CopLink Dashboard, and CopLink Trace. (gun-tracing). CopLink Connect is a secure internal communication system for intra-agency CJIS-compliant communications. OPD does use this system to securely share investigations information internally between personnel – no information is shared with any agency outside of OPD. Alternatives to this system are email or non-CJIS-compliant systems (e.g. box.com). OPD utilized CopLink Dashboard in the past (see "Proposed Purpose" Section above as well continued here in "Data Types and Sources" below) for use with stop data analysis. OPD now uses other non-Forensic Logic systems for stop data analysis and does not use CopLink Dashboard; OPD does not have access to the Dashboard module.

CopLink Trace is a system used for gun-tracing; OPD does not have access to this module and does not utilize this module.

OPD occasionally calls upon Forensic Logic for technical assistance, to collaborate on tasks where data can be used to solve a particular problem. An example of projects that Forensic Logic has undertaken for OPD where Forensic Logic did not charge additional fees include:

- Development of weekly CompStat reporting and presentation system displayed on google Earth illustrating location of major offenses on a map as well as all arrests and field contacts
- Re-development of weekly CompStat reports to comply with request of Chief William Bratton when he consulted for OPD
- Reconciliation of incident activity and confirmation of accuracy of OPD reporting to CA DOJ and FBI of monthly Uniform Crime Reporting statistics
- Conversion of transcribed citations and hard copy stop data reports for use by Federal monitor to clear Task 34 of NSA
- Ongoing consulting of how Stop Data reports should be recorded in OPD CAD system for optimal reporting as required by Federal Monitor

- Analysis of stop data for use in Federal Monitor reports
- Development of prototype stop data analysis capability that revealed certain geodemographic groups in Oakland may have been disproportionately searched when stopped but such searches resulted in nothing illicit found during search
- Development of prototype officer conduct dashboard that compared officers, patrols and areas using stop data information to determine if there was disproportionate minority contact.

G. Data Security

Forensic Logic constantly processes large streams of criminal justice information (CJI) and thus must comply with the provisions of the Criminal Justice Information Services (CJIS) Division of the Federal Bureau of Investigation (FBI) and the FBI Security Management Act of 2003 and CJIS Security Policy[11]. Forensic Logic, along with their partner at Microsoft Azure Government and the National Law Enforcement Telecommunications System (NLETS), have developed strong CJIS-compliant data security protocols.

a. Account Management – OPD personnel who use Forensic Coplink have access accounts that are created, deleted and managed by local Administrators (OPD) with special access permissions to the system. CopLink SEARCH (formerly LEAP) users are managed through a centralized account management process by Forensic Logic support personnel. OPD is working with the Oakland Information Technology Department (ITD) to incorporate the Microsoft Active Directory email authentication protocol, so that the system authenticates when the user has a currently authorized user login identification and password.

b. Microsoft Azure Government Cloud Protocols - Azure Government services handle data that is subject to several CJIS-type government regulations and requirements (e.g. such as FedRAMP (fedramp.gov), NIST 800.171 (DIB)[12], CJIS). One strategy is that Azure Government uses physically isolated datacenters and networks (located in U.S. only). All devices connecting to the Azure infrastructure are authenticated before access is granted. Only trusted devices with registered IP's are permitted to connect. Connections directly to NLETS are only provided via virtual private network (VPN).

c. Encryption - Data in Transit: In accordance with CSP 5.10.1.2.1, all traffic transmitted outside of the secured environment is encrypted with Transport Layer Security (TLS), using RSA[13] certificates and

[11] https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center
[12] https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final
[13] RSA is a public key encryption algorithm that cannot be broken in a timely manner by even the largest computer

FIPS 140-2 certified cyphers. Data at Rest: All Azure GovCloud storage solutions use Azure Encrypted Managed Disks. No data at rest shall be removed from the secured environment for any reason. Forensic Logic CopLink Data residing on Forensic Logic computers located at the NLETS data center is also encrypted at rest.

d. User Authentication and Authorization - All authorized users must maintain and enter a valid user id/strong password combination to gain access to the system. Passwords must be changed every 90 days and must adhere to Basic Password Standards listed in CSP v5.8 Paragraph 5.6.2.1.1. In addition to user and device authentication mechanisms, the system employs a two-factor advanced authentication services. These services provide a single use, time-sensitive token, delivered to a mobile device, tablet or computer, which must be entered into the logon process in order to gain access from devices outside of the physically secured location. Upon successful logon, access to specific objects are authorized based on Access Control Lists (ACLs) in accordance with CSP 5.5.2.4

e. Personnel Screening, Training and Administration - In accordance with CSP 5.12.1.1, all Forensic Logic employees are fingerprinted, background checked and required to read and sign the FBI Security Addendum located in Appendix H of the CSP. All employees have also successfully completed Level Four Security Awareness Training in accordance with CSP 5.2.1.4.

H. Costs

A new proposed contract will cost the City approximately $188,006 for the period of July 1, 2020 through June 30, 2021, and then $456,700 for the period of July 1, 2021 to June 30, 2023.

I. Third Party Dependence

OPD relies on Forensic Logic, Inc. as a private company to provide OPD with access to its data warehouse, search engine, and crime reporting tools. The combination of the prior LEAP Search combined with the CopLink system create a unique product with national scope.

J. Alternatives Considered

No other product or company can realistically provide OPD with both the complex crime report support and search functionality provided by Forensic Logic.

networks: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf
https://en.wikipedia.org/wiki/FIPS_140-2

The former Omega Group (now a division of Central Square) provides crimemapping capabilities and is an OPD vendor. Its public facing product is limited to 180 days of visualization; is limited to no more than approximately 500 incidents on a map simultaneously (for reference Oakland had 685 burglaries, 777 auto thefts and 481 aggravated assaults recorded just in May 2020); and not all incidents are visualized as certain incident types are filtered out.

Forensic Logic has built a customized crime report system that reaches back to more than a decade to compare crime types at the agency, area and beat level and is explained above that would require Oakland to expend significant time and resources to replicate even with a new vendor.

In the immediate term, OPD would have less access to its own CAD/RMS data – the current system is very outdated; OPD is in the process of implementing a new Motorola-based CAD/RMS system[14] but even once that process is complete later in 2020 or 2021, OPD will require continued access to Forensic Logic's much more accessible format for querying OPD CAD/RMS data. The Oakland Police Department has not contracted Motorola to convert the entire history of crime incidents from its existing outdated system to the new CAD/RMS system and therefore, Forensic Logic will retain the only historical searchable information for those incidents not converted into the new CAD/RMS. Similarly, OPD would need to dedicate months of non-available Oakland Information Technology Department (ITD) expertise to develop the algorithms Forensic Logic created to sift and sort OPD CAD/RMS data into usable crime analysis reports upon which the Mayor's Office and the City Council have come to rely.

No other vendor currently provides the local, regional and national law enforcement data needed by OPD to assist in criminal investigations. Authorized OPD personnel could, however, access many types of data contained in Forensic Logic CopLink, without using the Forensic Logic CopLink system. Native OPD systems such as CAD/RMS, Alameda County's CRIMS, OPD Field Based Reporting (or FBR, for recording stop data), and ShotSpotter can be accessed through their direct system portals. However, accessing each system separately takes more time; in the case of current CAD/RMS is complicated and even more time consuming; and does not aggregate the information from the multiple data sources into a common result that provides multi-data set situational awareness. More fundamentally, Forensic Logic CopLink makes each dataset more powerful through connection to data in other systems, where OPD personnel would not otherwise know to connect the data without laborious efforts. For example, if an investigator knows which agency may have useful information, they can contact that agency (e.g., BART Police), and ask the agency to manually query their data system to look for the relevant information.

[14] OPD's CAD-RMS contract was finalized in December 2017; a contract for the second phase of work was signed in 2019.

However, in many cases, OPD investigators would not know which agency to call and it would be very difficult to call many agencies to ask for leads in different types of cases.

K. Track Record of Other Entities

Many other police agencies in the Bay Area, in California, and nationally utilize the Forensic Logic CopLink System. In fact, Oakland benefits significantly from the IBM CopLink acquisition by Forensic Logic due to the concentration of California agencies that were customers of CopLink. Data from the California Counties of Orange, Santa Clara, San Mateo, Contra Costa, Stanislaus, Monterey; most of southern Oregon; Las Vegas NV Metro area; all of Arizona are already available to OPD and integrations with the Counties of San Francisco, San Diego, Los Angeles. Santa Barbara, and the Spokane, WA area are underway.

OPD staff spoke with an investigator with SFPD in the production of this report. The investigator explained that LEAP / CopLink is by far the most useful source of law enforcement data and that this tool makes crime investigations much more effective. In a recent SFPD case related to numerous sexual assaults, SFPD was able to find similar cases in another county that allowed investigators to contact other victims; the other victims provided additional suspect information which was invaluable in the recent arrest of the suspect.

OAKLAND
POLICE DEPARTMENT
455 7th St., Oakland, CA 94607 | OPDCRIMEANALYSIS@OAKLANDNET.COM
CRIME ANALYSIS

Weekly Crime Report—Citywide
20 Apr. — 26 Apr., 2020

Part 1 Crimes *All totals include attempts except homicides.*	Weekly Total	YTD 2018	YTD 2019	YTD 2020	YTD % Change 2019 vs. 2020	3-Year YTD Average	YTD 2020 vs. 3-Year YTD Average
Violent Crime Index (homicide, aggravated assault, rape, robbery)	80	1,636	1,781	1,752	-2%	1,723	2%
Homicide – 187(a)PC	1	17	24	16	-33%	19	-16%
Homicide – All Other *	-	6	2	1	-50%	3	-67%
Aggravated Assault	45	768	848	854	1%	823	4%
Assault with a firearm – 245(a)(2)PC	6	78	88	94	7%	87	8%
Subtotal - Homicides + Firearm Assault	7	101	114	111	-3%	109	2%
Shooting occupied home or vehicle – 246PC	6	75	81	95	17%	84	14%
Shooting unoccupied home or vehicle – 247(b)PC	1	25	37	39	5%	34	16%
Non-firearm aggravated assaults	32	590	642	626	-2%	619	1%
Rape	5	65	70	75	7%	70	7%
Robbery	29	786	839	807	-4%	811	0%
Firearm	12	292	290	244	-16%	275	-11%
Knife	3	50	36	74	106%	53	39%
Strong-arm	8	342	383	380	-1%	368	3%
Other dangerous weapon	1	26	25	21	-16%	24	-13%
Residential robbery – 212.5(a)PC	1	27	31	28	-10%	29	-2%
Carjacking – 215(a) PC	4	49	74	60	-19%	61	-2%
Burglary	65	2,892	4,096	3,865	-6%	3,618	7%
Auto	36	2,158	3,290	3,171	-4%	2,873	10%
Residential	10	497	549	391	-29%	479	-18%
Commercial	13	191	212	210	-1%	204	3%
Other (Includes boats, aircraft, and so on)	2	38	37	47	27%	41	16%
Unknown	4	8	8	46	475%	21	123%
Motor Vehicle Theft	111	2,072	2,053	2,364	15%	2,163	9%
Larceny	49	1,987	2,165	2,029	-6%	2,060	-2%
Arson	1	52	36	46	28%	45	3%
Total	306	8,645	10,133	10,057	-1%	9,612	5%

THIS REPORT IS HIERARCHY BASED. CRIME TOTALS REFLECT ONE OFFENSE (THE MOST SEVERE) PER INCIDENT.

These statistics are drawn from the Oakland Police Dept. database. They are unaudited and not used to figure the crime numbers reported to the FBI's Uniform Crime Reporting (UCR) program. This report is run by the date the crimes occurred. Statistics can be affected by late reporting, the geocoding process, or the reclassification or unfounding of crimes. Because crime reporting and data entry can run behind, all crimes may not be recorded.

** Justified, accidental, foetal, or manslaughter by negligence. Traffic collision fatalities are not included in this report.*
PNC = Percentage not calculated — Percentage cannot be calculated.
All data extracted via the LEAP Network.

Ad Hoc Group motion to recommend that the City Council approve a Forensic Logic Use Policy subject to the following conditions:

1. Authorized uses shall be limited to: 1) Crime Report Production (as written in OPD's proposed use policy presented to the PAC on September 3, 2020); and 2) Search (as written in OPD's proposed use policy presented to the PAC on September 3, 2020)

2. The contract between the City and Forensic Logic shall include the following provisions:
    a. OPD owns all data and any information derived from such data
    b. The vendor shall make a customized version of its software available to OPD, allowing only for crime report production and search as stated in the proposed policy's authorized uses. OPD may use Forensic Logic to search its own records and those of any third parties. OPD's data shall not be made available via the Forensic Logic platform to any third parties, except for entities located within Alameda County.
    c. Termination for convenience and/or immediate termination for material breaches, to include:
        i. If Forensic Logic bids on any contracts subject to our Sanctuary Contracting Ordinance
        ii. If Forensic Logic provides any additional features to OPD beyond the two above approved uses (and features needed to support the functionality of the approved uses), absent future council approval.
        iii. If Forensic Logic allows OPD data to be available via the Forensic Logic platform to any third parties located outside of Alameda County, absent future council approval.
    d. If approved by the City Council, and prior to its execution, the contract shall be provided to the Chair of the PAC and the Chief Privacy Officer, to ensure the above provisions have been incorporated.

CITY OF OAKLAND

MEMORANDUM

TO:	Privacy Advisory Commission	**FROM:**	Roland Holmgren, Deputy Chief, OPD
SUBJECT:	Use of Unapproved Surveillance Technology Under Exigent Circumstances: March 16 and 27, 2020	**DATE:**	April 4, 2020

RECOMMENDATION

Receive information use of unapproved surveillance technology under exigent circumstances in accordance with Oakland Municipal Code (OMC) 9.64.035 and forward to the City Council.

EXECUTIVE SUMMARY

In accordance with OMC 9.64.035, the Oakland Police Department (OPD) used surveillance technology under exigent circumstances /Carjacking and Barricaded Shooting Suspects). The technology is Unmanned Aerial System (UAS), commonly known as a drone.

BASIS FOR EXIGENCY

RD #20-014304
Incident: # LOP200311000316
Location: 1700 90th Avenue

On Mar 16, 2020, at about 10:07 PM, OPD Officers observed a vehicle involved in a series of armed carjackings. OPD Officers attempted to conduct an enforcement stop on the vehicle, but the vehicle fled from officers. A pursuit ensued and ended when the suspect vehicle collided into private property. The suspect passenger of the vehicle was taken into custody and the suspect driver fled on foot and entered a residential yard.

The OPD helicopter was not available due to flight time; the California Highway Patrol (CHP) responded to the scene. OPD Command authorized the deployment of the Bearcat (armored vehicle) and the use of UAS to apprehend the suspect (suspected to be armed). The OPD K-9 unit was also utilized. Due to the residence's visual restrictions (trees, brush, fences, etc), OPD Command elected to utilize the Alameda County Sheriff's Office (ACSO) UAS to assist the CHP helicopter.

Both the CHP Helicopter and ALCO UAS were able to pinpoint and locate the suspect; OPD personnel were able to locate the suspect and take him safely into custody. There were no reported injuries or complaints.

RD #20-016458
Incident: #LOP200327000634
Location: 8477 Enterprise Way Rm#127 (Quality Inn)

On Mar 27, 2020 at about 4:51 PM OPD officers were dispatched to a report of shooting. Upon their arrival, officers were advised that the shooters (suspects) had entered a hotel room. There were no victims located at the scene. OPD Command authorized deployment of the BearCat and armored SUV vehicle.

Traditional air support was available, but not needed because the suspects had isolated themselves and barricaded themselves in one hotel room. The OPD K-9 unit were not on-duty. ACSO overheard OPD radio transmissions and responded to the scene with their UAS and their K-9 unit. However, the UAS was not utilized. Successful communication was established with the suspects, who later exited and were detained. One loaded handgun was recovered within the room. The shooting suspect was positively identified and arrested. There were no reported injuries or complaints.

DEVICE USE INFORMATION

The UAS detection equipment was provided by, and operated by ACSO – on March 16, 2020 incident.

Video Recorded

The UAS recorded video of the area where it was deployed.

Retention of Recordings

Per ACSO policy, the video recording will be maintained by ACSO for three years.

Usefulness in Arresting Suspect/s

The UAS was utilized in connection with the March 16, 2020 residential yard search. The armed suspect had fled from officers in a carjacked vehicle. The suspect crashed the vehicle then hid in a nearby residential yard. The UAS (and CHP Helicopter) provided much-needed real-time intelligence. Due to limited lighting the FLIR infrared camera was utilized and ultimately located the suspect.

The UAS was not used in connection with the one arrest on March 27, 2020. The area encompassed a hotel and the suspects had barricaded themselves inside one hotel room. The UAS was not utilized because suspects surrendered.

COMPLIANT USE

The following information relating to helicopter and UAS is required by OMC 9.64.035, and shows that each technology was used in accordance with the OMC.

A. The UAS detection equipment was used solely to respond to the exigency.
B. Use of the UAS detection equipment ceased when the exigency ended.
C. Only data related to the exigency was kept.

D. This report is being provided to the Privacy Advisory Commission with a recommendation that it be forwarded to City Council.

OPD never had possession of the UAS detection equipment. ACSO maintained possession of the equipment during the entire equipment usage period.

Reviewed by:
Roland Holmgren, Deputy Chief
Bureau of Field Operations

Philip Best, Police Services Manager
OPD, Training Division, Research and Planning Section

Prepared by:
Omar Daza-Quiroz, Acting Lieutenant
OPD, Bureau of Field Operations

Bruce Stoffmacher, Management Assistant
OPD, Training Division, Research and Planning Section

CITY OF OAKLAND

MEMORANDUM

TO:	Privacy Advisory Commission	**FROM:**	Roland Holmgren, Deputy Chief
SUBJECT:	Use of Unapproved Surveillance Technology Under Exigent Circumstances – April 7 and 16, 2020	**DATE:**	May 4, 2020

RECOMMENDATION

Receive information use of unapproved surveillance technology under exigent circumstances in accordance with Oakland Municipal Code (OMC) 9.64.035 and forward to the City Council.

EXECUTIVE SUMMARY

In accordance with OMC 9.64.035, the Oakland Police Department (OPD) used surveillance technology under exigent circumstances /Carjacking and Barricaded Shooting Suspects). The technology is Unmanned Aerial System (UAS), commonly known as a drone.

BASIS FOR EXIGENCY

RD# 20-017997
Incident: LOP200407000889
Location: Fairmount and Pearl St

On Apr 6, 2020, at about 2:00 PM, an armed takeover robbery occurred at the Verizon Store, located at 2054 Mountain Blvd. The suspects entered the store armed with pistols and held the store at gunpoint. The suspects stole thousands of dollars' worth in loss and then fled the scene.

On Apr 7, 2020 OPD officers located the vehicle, which was used in the robbery, driving in Oakland. One subject from the vehicle was detained when he exited from the vehicle at a liquor store. The vehicle then fled from the officers. The OPD helicopter was available and followed the vehicle to Fairmount and Pearl St. The (2) two remaining suspects exited the vehicle and hid in residential yards. Officers set a perimeter. The robbery had occurred the day prior and was a "takeover" of a business. It was unknown if the suspects were armed on this date, but caution was taken.

Several areas were obstructed from the helicopter's view. OPD Command requested the use of UAS from the Alameda County Sherriff's Office (ACSO). One suspect surrendered prior to ACSO UAS deployment. ACSO deployed their UAS, but could not locate any additional suspects. It was discovered the third, and remaining suspect had broken the perimeter.

RD #20-019452
Incident: # LOP200416000027
Location: 1402 92nd Ave.

On Apr 16, 2020, at about 12:54 AM, OPD was advised of a person, who was armed with a gun in the 1400 blk of 92nd Ave. The armed gunman pointed a firearm at a person and threatened to kill him. As OPD arrived on scene, several subjects fled into nearby yards. OPD immediately established a perimeter. Through preliminary investigations it was determined there was more than one suspect involved and an armed robbery attempt had occurred.

The OPD command authorized the deployment of the BearCat. It was determined that neither OPD nor CHP air support was available. OPD command authorized ACSO UAS to locate the individuals, believing that the suspects were armed with firearms and having no air support available. The UAS was utilized and did not locate any suspects hiding in the yards.

As the investigation continued, it was discovered that the suspects had already fled from the perimeter prior to it being set up. No suspects were located or arrested.

DEVICE USE INFORMATION

The UAS detection equipment was provided by, and operated by the Alameda County Sheriff's Office (ACSO) – on both April 7 and April 16, 2020 incidents.

Video Recorded

The UAS recorded video of the area where it was deployed.

Retention of Recordings

Per ACSO policy, the video recording will be maintained by ACSO for three years.

Usefulness in Arresting Suspect/s

The UAS was utilized in connection with the April 7, 2020 residential yard search. The potentially armed robbery suspects had fled from officers. The suspects hid in a nearby residential yard. The UAS provided much-needed real-time intelligence by assisting in surveying the immediate area.

The UAS was utilized in connection with the April 16, 2020 residential yard search. Officers observed several subjects, who were possibly armed, flee into residential yards. The UAS assisted in surveying the yards. The area in question was residential yards. The UAS discovered no subjects were hiding in the yards and it was discovered the suspects had broken the perimeter.

COMPLIANT USE

The following information relating to helicopter and UAS is required by OMC 9.64.035, and shows that each technology was used in accordance with the OMC.

A. The UAS detection equipment was used solely to respond to the exigency.
B. Use of the UAS detection equipment ceased when the exigency ended.
C. Only data related to the exigency was kept.

D. This report is being provided to the Privacy Advisory Commission with a recommendation that it be forwarded to City Council.

OPD never had possession of the UAS detection equipment. ACSO maintained possession of the equipment during the entire equipment usage period.

Reviewed by:
Roland Holmgren, Deputy Chief
Bureau of Field Operations

Philip Best, Police Services Manager
OPD, Training Division, Research and Planning Section

Prepared by:
Omar Daza-Quiroz, Acting Lieutenant
OPD, Bureau of Field Operations

Bruce Stoffmacher, Management Assistant
OPD, Training Division, Research and Planning Section

CITY OF OAKLAND

MEMORANDUM

TO: Privacy Advisory Commission

FROM: Roland Holmgren, Deputy Chief of Police

SUBJECT: Use of Unapproved Surveillance Technology Under Exigent Circumstances: June 3 and June 24, 2020

DATE: June 26, 2020

RECOMMENDATION

Receive information use of unapproved surveillance technology under exigent circumstances in accordance with Oakland Municipal Code (OMC) 9.64.035 and forward to the City Council.

EXECUTIVE SUMMARY

In accordance with OMC 9.64.035, the Oakland Police Department (OPD) used surveillance technology under exigent circumstances /Carjacking and Barricaded Shooting Suspects). The technology is Unmanned Aerial System (UAS), commonly known as a drone.

BASIS FOR EXIGENCY

RD #20-027338
Incident: # LOP200603000135
Location: 5714 Harmon Av, Oakland (Beat 27)

On June 3, 2020, at approximately 5:33 am, OPD officers responded to the 5700 block of Harmon Avenue on a ShotSpotter gunshot activation. Upon arrival, officers began to check the neighborhood and observed someone (through a residence window) inside of the residence shooting a pistol. Officers requested the Armored SUV and Rescue Vehicle (BearCat). While on scene the suspect leaned out the window, with a rifle, and began shooting at officers. A resident from the same address ran outside and officers rescued her from the immediate danger.

The rescued resident told OPD Officers her husband (the suspect) was inside of the residence armed with a rifle and pistol. Additionally, there were two juveniles (his children) held hostage in the residence.

OPD Command requested OPD helicopter support as well as outside agency air support. The OPD helicopter was not available and there were no outside agencies with air support; OPD therefore requested support from the Alameda County Sheriff's Office (ACSO) UAS Unit. ACSO deployed two drones in the area in order to obtain visual information regarding the residence, yard and rooftop.

OPD also requested assistance from the OPD Tactical Operations Team. At Approximately 6:16pm, the suspect surrendered his children and himself safely to OPD.
The residence was searched, and a handgun and rifle were recovered.

RD# 20-030695
Inc# LOP200623001004
Location 1733 8th St (Report location)

On June 24, 2020 around 12:50pm, the Special Victims Unit (SVU) / Missing Persons was investigating the disappearance of a missing 12-year-old female juvenile. During the preliminary investigation, it was discovered the juvenile was texting male adults and possibly involved in sexual trafficking. SVU requested the assistance of local Federal Bureau of Investigation (FBI) personnel as well as the ACSO UAS Unit.

SVU identified several key locations where the juvenile may be located based on prior investigation data. OPD and FBI conducted several vehicle and foot checks. ACSO UAS flew overhead and conducted aerial checks to locate any similar juvenile matching the description wearing the same clothing provided by the mother. Nobody matching the description was located.

The juvenile would later be located safely on 25Jun20.

RD# 20-030726
Incident: LOP200624000051 and LOP200623001130
Location: 1000 Blk Calcot Pl, Oakland (20X)

On June 24, 2020, at approximately 11:52pm, OPD Officers responded to 1000 Block of Calcot Place on a report of a shooting. Upon their arrival they located a victim of a shooting, who would later succumb to their injuries. The area was adjacent to train tracks and just below the 23rd Avenue 880 Freeway Overpass.

At approximately 1:19am, OPD Officers continued their preliminary investigations surrounding the homicide. At this time OPD Officers observed a vehicle leave the area of the investigation at a high rate of speed. Immediately thereafter, multiple gunshots were fired in the direction of the officers (confirmed via ShotSpotter gunshot activation). OPD officers on scene took cover behind vehicles and fixed objects. OPD officers then observed a green colored laser pointed in the direction of the officers. As OPD Officers maintained cover behind vehicles, they noticed that a subject was observed standing on the overpass, in a position of tactical advantage – putting officers at greater risk. OPD Officers immediately told the suspect to raise his hands and the suspect immediately fled on foot.

OPD Command approved deployment of the Armored SUV and Rescue Vehicle (BearCat) and also requested ACSO UAS support. OPD helicopters and outside agency helicopters were not available. ACSO deployed two drones in the dark areas beneath the overpass, which encompassed the train tracks.

A search of the area was conducted, and no subjects (or vehicle observed fleeing the area) were located. Multiple expended casings were located near the area where the suspect vehicle had fled.

DEVICE USE INFORMATION

The UAS detection equipment was provided by, and operated by ACSO at the June 3, 2020 and both of the June 24, 2020 incidents.

Video Recorded

The UAS recorded video of the area where it was deployed.

Retention of Recordings

Per ACSO policy, the video recording will be maintained by ACSO for three years.

Usefulness in Arresting Suspect/s

- The UAS was utilized in connection with the June 3, 2020 residential yard searches. The barricaded suspect was heavily armed with a rifle and pistol in the residence and had held two juveniles' hostage. The suspect had shot at OPD Officers, who were taking cover behind the armored rescue vehicles. The UAS provided much-needed real-time intelligence. The UAS assisted in surveying the yards and rooftop. The UAS usage allowed OPD Officers real time intel in order to determine if the suspect would attempt to flee from the rear or side entrances/windows.
- The UAS was utilized in connection with the June 24, 2020 missing person investigation. OPD Officers were investigating a missing person at risk, who may had been involved in sex trafficking. The UAS assisted in quickly searching multiple areas. The Juvenile was not located by UAS and would later be found the following day.
- The UAS was utilized in connection with the June 24, 2020 train track search. OPD officers were investigating a homicide in the City of Oakland when they were fired upon by suspect(s). Officers maintained cover until other responding officers responded. The UAS assisted in surveying the train tracks and area under the overpass, which was dark. The UAS discovered no subjects were hiding.

COMPLIANT USE

The following information relating to helicopter and UAS is required by OMC 9.64.035, and shows that each technology was used in accordance with the OMC.

A. The UAS detection equipment was used solely to respond to the exigency.
B. Use of the UAS detection equipment ceased when the exigency ended.
C. Only data related to the exigency was kept.
D. This report is being provided to the Privacy Advisory Commission at its next meeting with a recommendation that it be forwarded to City Council.

OPD never had possession of the UAS detection equipment. ACSO maintained possession of the equipment during the entire equipment usage period.

Reviewed by:
Roland Holmgren, Deputy Chief
Bureau of Field Operations

Prepared by:
Omar Daza-Quiroz, Lieutenant
OPD, Bureau of Field Operations

Bruce Stoffmacher, Management Assistant
OPD, Training Division, Research and Planning Section

C I T Y O F OA K L A N D

Memorandum

ATTN:	Joe Devries, Director of Interdepartmental Operations and Chief Privacy Officer
FROM:	Randall Wingate, OPD, Support Operations Division
DATE:	August 31, 2020
RE:	Report on Video Stream Usage: May 29 – June 2, 2020

This memorandum summarizes the use of Live Stream Transmitters by the Oakland Police Department (OPD), in support of the specified event.

RD# or Incident #: 20-026554
Date of Incident: 29 MAY 20
Type of Event: Protest
Was EOC/DOC activated: YES
Number of Video Streams provide to EOC/DOC: No streams were provided.
Summary: No video streams were used for this event.

RD# or Incident #: 20-026713
Date of Incident: 30 MAY 20
Type of Event: Protest
Was EOC/DOC activated: YES
Number of Video Streams provide to EOC/DOC: 2 video streams
Summary: Video Teams were requested by Lieutenant C. Shannon on 30 May 20. Two video streams were provided by the Video Teams to the EOC.

RD# or Incident #: 20-026817
Date of Incident: 31 MAY 20
Type of Event: Protest
Was EOC/DOC activated: YES
Number of Video Streams provide to EOC/DOC: 2 video streams
Summary: Video Teams were requested for the next protest event at the end of the 30 MAY 20 event. Two video streams were provided by the Video Teams to the EOC.

RD# or Incident #: 20-027034
Date of Incident: 01 JUN 20
Type of Event: Protest
Was EOC/DOC activated: YES
Number of Video Streams provide to EOC/DOC: 2 video streams
Summary: Video Teams were requested for the next protest event at the end of the 31 MAY 20 event. Two video streams were provided by the Video Teams to the EOC.
RD# or Incident #: 20-027193

Date of Incident: 02 JUN 20
Type of Event: Protest
Was EOC/DOC activated: YES
Number of Video Streams provide to EOC/DOC: 2 video streams
Summary: Video Teams were requested for the next protest event at the end of the 1 JUN 20 event. Two video streams were provided by the Video Teams to the EOC.

RD# or Incident #: 20-027341
Date of Incident: 03 JUN 20
Type of Event: Protest
Was EOC/DOC activated: YES
Number of Video Streams provide to EOC/DOC: 2 video streams
Summary: Video Teams were requested for the next protest event at the end of the 2 JUN 20 event. Two video streams were provided by the Video Teams to the EOC. The video streams were not activated.

Inez Ramirez III
Sergeant of Police
Bureau of Services Administration
Oakland Police Department

C I T Y O F OA K L A N D

Memorandum

ATTN: Joe Devries, Director of Interdepartmental Operations and Chief Privacy Officer
FROM: Randall Wingate, Captain, OPD, Support Operations Division
DATE: August 31, 2020
RE: Report on Video Stream Usage: July 25, 2020

This memorandum summarizes the use of Live Stream Transmitters by the Oakland Police Department (OPD), in support of the specified event.

RD# or Incident #: 20-036638
Date of Incident: 25 JUL 20
Type of Event: Protest
Was EOC/DOC activated: YES
Number of Video Streams provide to EOC/DOC: 2 video streams
Summary: Video Teams were requested by Lieutenant C. Shannon on 23 JUL 20. Two video streams were provided by the Video Teams to the EOC.

Inez Ramirez III
Sergeant of Police
Bureau of Services Administration
Oakland Police Department

C I T Y O F OA K L A N D

Memorandum

ATTN:	Joe Devries, Director of Interdepartmental Operations and Chief Privacy Officer
FROM:	Randall Wingate, OPD, Support Operations Division
DATE:	August 31, 2020
RE:	Report on Video Stream Usage: August 28/29, 2020

This memorandum summarizes the use of Live Stream Transmitters by the Oakland Police Department (OPD), in support of the specified event.

RD# or Incident #: 20-042759
Date of Incident: 28 AUG 20
Type of Event: Protest
Was EOC/DOC activated: YES
Number of Video Streams provide to EOC/DOC: 3 video streams
Summary: Video Teams were requested by Lieutenant C. Shannon on 27 AUG 20. Three video streams were provided by the Video Teams to the EOC.

RD# or Incident #: 20-042912
Date of Incident: 29 AUG 20
Type of Event: Protest
Was EOC/DOC activated: YES
Number of Video Streams provide to EOC/DOC: 3 video streams
Summary: Video Teams were requested at the end of the 28 AUG 20 event. Three video streams were provided by the Video Teams to the EOC.

Inez Ramirez III
Sergeant of Police
Bureau of Services Administration
Oakland Police Department

Chapter 9.64 - REGULATIONS ON CITY'S ACQUISITION AND USE OF SURVEILLANCE TECHNOLOGY

Sections:

9.64.010 - Definitions.

The following definitions apply to this Chapter.

1. "Annual Surveillance Report" means a written report concerning a specific surveillance technology that includes all the following:

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

B. Whether and how often data acquired through the use of the surveillance technology was directly shared with outside entities ~~if known and if practicable~~, the name of any recipient entity ~~if known and if practicable~~, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s);[BS1]

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;

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

E. A summary of community complaints or concerns about the surveillance technology, and an analysis of the technology's adopted use policy and whether it is adequate in protecting civil rights and civil liberties. The analysis shall identify the race of each person that was subject to the technology's use. The Privacy Advisory Commission may determine, on an individual policy basis, to waive the obligation to identify the race of each person if the probative value is outweighed by the administrative burden and 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.

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.

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;

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

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

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; and

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

2. ”Biometric Surveillance Technology” means any computer software that uses Face Recognition Technology or Other Remote Biometric Recognition in real time or on a recording or photograph.

3. "City" means any department, agency, bureau, and/or subordinate division of the City of Oakland as provided by Chapter 2.29 of the Oakland Municipal Code.

4. "City Staff" means City personnel authorized by the City Administrator or designee to seek City Council approval of surveillance technology in conformance with this Chapter.

5. "Continuing Agreement" means an agreement that automatically renews unless terminated by one (1) party.

6. "Exigent Circumstances" means a law enforcement agency's good faith belief that an emergency involving danger of, or imminent threat of the destruction of evidence regarding, death or serious physical injury to any person requires the use of surveillance technology or the information it provides.

7. "Face Recognition Technology" means (A) an automated or semi-automated process that assists in identifying or verifying an individual based on an individual's face; or (B) logs characteristics of an individual’s face, head, or body to infer emotion, associations, expressions, or the location of an individual.

8. "Large-Scale Event" means an event attracting ten thousand (10,000) or more people with the potential to attract national media attention that provides a reasonable basis to anticipate that exigent circumstances may occur.

9. “Other Remote Biometric Recognition” means (A) an automated or semi-automated process that (i) assists in identifying an individual, capturing information about an individual, or otherwise generating or assisting in generating information about an individual based on

physiological, biological, or behavioral characteristics ascertained from a distance; (ii) uses voice[BS2] recognition technology; or (iii) logs such characteristics to infer emotion, associations, activities, or the location of an individual, and (B) does not include identification based on fingerprints or palm prints that have been manually obtained during the course of a criminal investigation or detention.

10. "Personal Communication Device" means a mobile telephone, a personal digital assistant, a wireless capable tablet and a similar wireless two-way communications and/or portable internet accessing devices, whether procured or subsidized by a city entity or personally owned, that is used in the regular course of city business.

11. “Predictive Policing Technology” means computer algorithms that use preexisting data to forecast or predict places or times that have a high risk of crime, or individuals or groups who are likely to commit a crime. This definition does not include computer algorithms used solely to visualize, chart, or map past criminal activity (e.g. heat maps).

12. "Police Area" refers to each of the geographic districts assigned to a police commander and as such districts are amended from time to time.

13. "Surveillance" or "Surveil" means to observe or analyze the movements, behavior, data, or actions of individuals. Individuals include those whose identity can be revealed by license plate data when combined with any other record.

14. "Surveillance Technology" means any software, electronic device, system utilizing an electronic device, or similar technological tool used, designed, or primarily intended to collect, retain, analyze, process, or share audio, electronic, visual, location, thermal, olfactory, biometric, or similar information specifically associated with, or capable of being associated with, any individual or group. Examples of surveillance technology include, but is not limited to the following: cell site simulators (Stingrays); automatic license plate readers; gunshot detectors (ShotSpotter); facial recognition software; thermal imaging systems; body-worn cameras; social media analytics software; gait analysis software; video cameras that record audio or video, and transmit or can be remotely accessed. It also includes software designed to monitor social media services or forecast criminal activity or criminality, biometric identification hardware or software.

"Surveillance technology" does not include the following devices or hardware, unless they have been equipped with, or are modified to become or include, a surveillance technology as defined above:

A. Routine office hardware, such as televisions, computers, credit card machines, badge readers, copy machines, and printers, that is in widespread use and will not be used for any surveillance or law enforcement functions;

B. Parking Ticket Devices (PTDs);

C. Manually-operated, non-wearable, handheld digital cameras, audio recorders, and video recorders that are not designed to be used surreptitiously and whose functionality is limited to manually capturing and manually downloading video and/or audio recordings;

D. Surveillance devices that cannot record or transmit audio or video or be remotely accessed, such as image stabilizing binoculars or night vision goggles;

E. Manually-operated technological devices used primarily for internal municipal entity communications and are not designed to surreptitiously collect surveillance data, such as radios and email systems;

F. City databases that do not contain any data or other information collected, captured, recorded, retained, processed, intercepted, or analyzed by surveillance technology, including payroll, accounting, or other fiscal databases.

G. Medical equipment used to diagnose, treat, or prevent disease or injury.

H. Police department interview room cameras.

I. Police department case management and records management systems~~.~~, including computer aided dispatch systems, and field-based reporting systems.

J. Police department early warning systems.

K. Personal communication devices that have not been modified beyond stock manufacturer capabilities in a manner described above, provided that any bundled face recognition technology is only used for the sole purpose of user authentication in the regular course of conducting City business.

~~*L.* Forensic instrumentation, equipment, reagents and standards that are used by the Oakland Police Department Criminalistics Laboratory (Crime Lab) as of August 2020 to analyze evidence samples collected in the course of an investigation, that upon analysis by the Crime Lab, may result in the identification of individual persons. A list of specific items is in Appendix A.~~

~~i. Like for like substitutions necessitated by improvements to current methodology, instrumentation failures or maintaining compliance with Federal Law will also be excluded.~~

~~ii. Entirely new biometric methodology outside the current scope of accreditation of the laboratory would require the laboratory to seek permission from the accreditation agency. This would also precipitate involvement of the Privacy Commission.~~[BS3]

15. "Surveillance Impact Report" means a publicly-released written report including at a minimum the following:

A. Description: information describing the surveillance technology and how it works, including product descriptions and manuals ~~(as attachments, if publicly available and current)~~ from manufacturers;

B. Purpose: information on the proposed purposes(s) for the surveillance technology;

C. Location: the location(s) it may be deployed, using general descriptive terms, and crime statistics for any location(s);

D. Impact: an assessment of the technology's adopted use policy and whether it is adequate in protecting civil rights and liberties and whether the surveillance technology was used or deployed, intentionally or inadvertently, in a manner that is discriminatory, viewpoint-based, or biased via algorithm;

E. Mitigations: identify specific, affirmative technical and procedural measures that will be implemented to safeguard the public from each such impacts;

F. Data Types and Sources: a list of all types and sources of data to be collected, analyzed, or processed by the surveillance technology, including "open source" data, scores, reports, logic or algorithm used, and any additional information derived therefrom;

G. Data Security: information about the steps that will be taken to ensure that adequate security measures are used to safeguard the data collected or generated by the technology from unauthorized access or disclosure;

H. Fiscal Cost: the fiscal costs for the surveillance technology, including initial purchase, personnel and other ongoing costs, the operative or proposed contract ~~if available - or past contract if available~~, and any current or potential sources of funding;

I. Third Party Dependence: whether use or maintenance of the technology will require data gathered by the technology to be handled or stored by a third-party vendor on an ongoing basis;

J. Alternatives: a summary of all alternative methods (whether involving the use of a new technology or not) considered before deciding to use the proposed surveillance technology, including the costs and benefits associated with each alternative and an explanation of the reasons why each alternative is inadequate; and,

K. Track Record: a summary of the experience (if any) other entities, especially government entities, have had with the proposed technology, including, if available, quantitative information about the effectiveness of the proposed technology in achieving its stated purpose in other jurisdictions, and any known adverse information about the technology (such as unanticipated costs, failures, or civil rights and civil liberties abuses).

16. "Surveillance Use Policy" means a publicly-released and legally enforceable policy for use of the surveillance technology that at a minimum specifies the following:

A. Purpose: the specific purpose(s) that the surveillance technology is intended to advance;

B. Authorized Use: the specific uses that are authorized, and the rules and processes required prior to such use;

C. Data Collection: the information that can be collected by the surveillance technology. Where applicable, list any data sources the technology will rely upon, including "open source" data;

D. Data Access: the category of individuals who can access or use the collected information, and the rules and processes required prior to access or use of the information;

E. Data Protection: the safeguards that protect information from unauthorized access, including encryption and access control mechanisms;

F. Data Retention: the time period, if any, for which information collected by the surveillance technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s), the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond that period;

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

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

I. Training: the training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology, and the category of staff that will provide the training;[BS4]

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

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

~~L. Reporting: Any emendations to the Annual Surveillance Report.~~[BS5]

17. "~~Remote~~ Voice Recognition Technology" means the automated or semi-automated process that assists in identifying or verifying an individual based on the characteristics of an individual's voice.

(Ord. No. 13563, § 3, 9-17-2019; Ord. No. 13489, § 2, 5-15-2018)

9.64.020 - Privacy Advisory Commission (PAC) notification and review requirements.

1. PAC Notification Required Prior to City Solicitation of Funds and Proposals for Surveillance Technology.

A. City staff shall notify the Chair of the Privacy Advisory Commission prior to:

1. Seeking or soliciting funds for surveillance technology, including but not limited to applying for a grant; or,

2. Soliciting proposals with a non-city entity to acquire, share or otherwise use surveillance technology or the information it provides.

B. Upon notification by city staff, the Chair of the Privacy Advisory Commission shall place the item on the agenda at the next Privacy Advisory Commission meeting for discussion and possible action. At this meeting, city staff shall inform the Privacy Advisory Commission of the need for the funds or equipment, or shall otherwise justify the action city staff will seek Council approval for pursuant to 9.64.030. The Privacy Advisory Commission may make a recommendation to the City Council by voting its approval to proceed, object to the proposal, recommend that the city staff modify the proposal, or take no action.

C. Should the Privacy Advisory Commission not make a recommendation pursuant to 9.64.020 1.B., City staff may proceed and seek Council approval of the proposed surveillance technology initiative pursuant to the requirements of Section 9.64.030.

2. PAC Review Required for New Surveillance Technology Before City Council Approval.

A. Prior to seeking City Council approval under Section 9.64.030, city staff shall submit a surveillance impact report and a surveillance use policy for the proposed new surveillance technology initiative to the Privacy Advisory Commission for its review at a regularly noticed meeting. The surveillance impact report and surveillance use policy must address the specific subject matter specified for such reports as defined under 9.64.010.

B. The Privacy Advisory Commission shall recommend that the City Council adopt, modify, or reject the proposed surveillance use policy. If the Privacy Advisory Commission proposes that the Surveillance Use Policy be modified, the Privacy Advisory Commission shall propose such modifications to city staff. City staff shall present such modifications to City Council when seeking City Council approval under Section 9.64.030.

C. Failure by the Privacy Advisory Commission to make its recommendation on the item within ninety (90) days of submission shall enable the city entity to proceed to the City Council for approval of the item.

3. PAC Review Requirements for Existing Surveillance Technology Before City Council Approval.

A. Prior to seeking City Council approval for existing city surveillance technology under Section 9.64.030 city staff shall submit a surveillance impact report and surveillance use policy

to the Privacy Advisory Commission for its review at a regularly noticed meeting. The surveillance impact report and surveillance use policy must address the specific subject matter specified for such reports as defined under 9.64.010.

B. Prior to submitting the surveillance impact report and proposed surveillance use policy as described above, city staff shall present to the Privacy Advisory Commission a list of surveillance technology possessed and/or used by the city.

C. The Privacy Advisory Commission shall rank the items in order of potential impact to civil liberties.

D. Within sixty (60) days of the Privacy Advisory Commission's action in 9.64.020 1.C., city staff shall submit at least one (1) surveillance impact report and proposed surveillance use policy per month to the Privacy Advisory Commission for review, beginning with the highest-ranking items as determined by the Privacy Advisory Commission, and continuing thereafter each month until a policy has been submitted for each item on the list.

E. Failure by the Privacy Advisory Commission to make its recommendation on any item within ninety (90) days of submission shall enable city staff to proceed to the City Council for approval of the item pursuant to Section 9.64.030.

(Ord. No. 13489, § 2, 5-15-2018)

9.64.030. - City Council approval requirements for new and existing surveillance technology.

1. City staff must obtain City Council approval prior to any of the following:

A. Accepting state or federal funds or in-kind or other donations for surveillance technology;[BS6]

B. Acquiring new surveillance technology, or replacing existing surveillance technology that has not been previously approved by the City Council pursuant to the requirements of this Chapter, including but not limited to procuring such technology without the exchange of monies or consideration;

C. Using new surveillance technology, or using existing surveillance technology [BS7]or the information it provides for a purpose, in a manner, or in a location not previously approved by the City Council pursuant to the requirements of this Chapter, except that for surveillance technology that has been acquired or is in use prior to enactment of this ordinance, such use may continue until the City Council votes to approve or reject the surveillance technology's corresponding use policy; or

D. Entering into a continuing agreement or written agreement with a non-city entity to acquire, share or otherwise use surveillance technology or the information it provides, including data sharing agreements.

E. Notwithstanding any other provision of this Section, nothing herein shall be construed to prevent, restrict or interfere with any person providing evidence or information derived from surveillance technology to a law enforcement agency for the purposes of conducting a criminal investigation or the law enforcement agency from receiving such evidence or information.

2. City Council Approval Process.

A. After the PAC notification and review requirements in Section 9.64.020 have been met, city staff seeking City Council approval shall schedule for City Council consideration and approval of the proposed surveillance impact report and proposed surveillance use policy, and include Privacy Advisory Commission recommendations at least fifteen (15) days prior to a mandatory, properly-noticed, germane public hearing. Approval may only occur at a public hearing[BS8]. City staff shall not unreasonably delay scheduling any item for City Council consideration.

B. The City Council shall only approve any action as provided in this Article after first considering the recommendation of the Privacy Advisory Commission, and subsequently making a determination that the benefits to the community of the surveillance technology outweigh the costs; that the proposal will safeguard civil liberties and civil rights; and that, in the City Council's judgment, no alternative with a lesser economic cost or impact on civil rights or civil liberties would be as effective.

C. For approval of existing surveillance technology for which the Privacy Advisory Commission failed to make its recommendation within ninety (90) days of review as provided for under 9.64.020 3.E, if the City Council has not reviewed and approved such item within four (4) City Council meetings from when the item was initially scheduled for City Council consideration, the city shall cease its use of the surveillance technology until such review and approval occurs.

3. Surveillance Impact Reports and Surveillance Use Policies are Public Records. City staff shall make the Surveillance Impact Report and Surveillance Use Policy, as updated from time to time, available to the public as long as the city uses the surveillance technology in accordance with its request pursuant to Section 9.64.020 A.1.

(Ord. No. 13489, § 2, 5-15-2018)

9.64.035 - Use of unapproved technology during exigent circumstances or large-scale event.

1. City staff may temporarily acquire or use surveillance technology and the data derived from that use in a manner not expressly allowed by a surveillance use policy in two (2) types of

circumstances without following the provisions of Section 9.64.030: (A) exigent circumstances, and (B) a large-scale event.

2. If city staff acquires or uses a surveillance technology in the two (2) circumstances pursuant to subdivision 1., the city staff shall:

A. Use the surveillance technology to solely respond to the exigent circumstances or large-scale event.

B. Cease using the surveillance technology when the exigent circumstances or large scale event ends.

C. Only keep and maintain data related to the exigent circumstances and dispose of any data that is not relevant to an ongoing investigation.

D. Following the end of the exigent circumstances or large-scale event, report that acquisition or use to the PAC at their next respective meetings for discussion and/or possible recommendation to the City Council in accordance with the Sunshine Ordinance, the Brown Act, and City Administrator deadlines.

3. Any technology temporarily acquired in exigent circumstances or during a large-scale event shall be returned within seven (7) days following its acquisition, or when the exigent circumstances end, whichever is sooner, unless the technology is submitted to the City Council for approval pursuant to Section 9.64.030 and is approved. If the agency is unable to comply with the seven-day timeline, the agency shall notify the City Council, who may grant an extension.

(Ord. No. 13489, § 2, 5-15-2018)

9.64.040 - Oversight following City Council approval.

1. On March 15th of each year, or at the next closest regularly scheduled Privacy Advisory Commission meeting, city staff must present a written annual surveillance report for Privacy Advisory Commission review for each approved surveillance technology item. If city staff is unable to meet the deadline, city staff shall notify the Privacy Advisory Commission in writing of staff's request to extend this period, and the reasons for that request. The Privacy Advisory Commission may grant a single extension of up to sixty (60) days to comply with this provision.

A. After review by the Privacy Advisory Commission, city staff shall submit the annual surveillance report to the City Council.

B. The Privacy Advisory Commission 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.

C. Failure by the Privacy Advisory Commission to make its recommendation on the item within ninety (90) days of submission shall enable the city entity to proceed to the City Council for approval of the annual surveillance report.

2. Based upon information provided in city staff's Annual Surveillance Report and after considering the recommendation of the Privacy Advisory Commission, the City Council shall re-visit its "cost benefit" analysis as provided in Section 9.64.030 2.B. and either uphold or set aside the previous determination. Should the City Council set aside its previous determination, the city's use of the surveillance technology must cease. Alternatively, City Council may require modifications to the Surveillance Use Policy that will resolve any deficiencies.

(Ord. No. 13489, § 2, 5-15-2018)

9.64.045 - Prohibition on City's acquisition and/or use of (i) biometric surveillance technology, or (ii) predictive policing technology

A. Notwithstanding any other provision of this Chapter (9.64), it shall be unlawful for the City or any City staff to obtain, retain, request, access, or use:

1. Biometric surveillance technology; or

2. Predictive policing technology; or

3. Information obtained from either biometric surveillance technology or predictive policing technology.

B. City staff's inadvertent or unintentional receipt, access of, or use of any information obtained from biometric surveillance technology or predictive policing technology shall not be a violation of this Section 9.64.045 provided that:

1. City staff did not request or solicit the receipt, access of, or use of such information; and

2. City staff shall immediately destroy all copies of the information upon its discovery and shall not use the information for any purpose, unless retention or use of exculpatory evidence is required by law; and[BS9]

3. City staff logs such receipt, access, or use in a written report provided at the next closest regularly scheduled meeting after discovery of the use, to the Privacy Advisory Commission for discussion and possible recommendation to the City Council. Such a report shall not include any personally identifiable information or other information the release of which is prohibited by law. In its report, City staff shall identify specific measures taken by the City to prevent the

further transmission or use of any information inadvertently or unintentionally obtained through the use of such technologies; and

4. After review by the Privacy Advisory Commission, city staff shall submit the report to the City Council.

(Ord. No. 13563, § 3, 9-17-2019)

9.64.050 - Enforcement.

1. Violations of this Article are subject to the following remedies:

A. Any violation of this Article, or of a surveillance use policy promulgated under this Article, constitutes an injury and any person may institute proceedings for injunctive relief, declaratory relief, or writ of mandate in the Superior Court of the State of California to enforce this Article. An action instituted under this paragraph shall be brought against the respective city department, and the City of Oakland, and, if necessary to effectuate compliance with this Article or a surveillance use policy (including to expunge information unlawfully collected, retained, or shared thereunder), any other governmental agency with possession, custody, or control of data subject to this Article, to the extent permitted by law.

B. Any person who has been subjected to a surveillance technology in violation of this Article, or about whom information has been obtained, retained, accessed, shared, or used in violation of this Article or of a surveillance use policy promulgated under this Article, may institute proceedings in the Superior Court of the State of California against the City of Oakland and shall be entitled to recover actual damages (but not less than liquidated damages of one thousand dollars ($1,000.00) or one hundred dollars ($100.00) per day for each day of violation, whichever is greater).

C. A court shall award costs and reasonable attorneys' fees to the plaintiff who is the prevailing party in an action brought under paragraphs A. or B.

D. Violations of this Article by a city employee shall result in consequences that may include retraining, suspension, or termination, subject to due process requirements and in accordance with any memorandums of understanding with employee bargaining units.

(Ord. No. 13489, § 2, 5-15-2018)

9.64.060 - Secrecy of surveillance technology.

It shall be unlawful for the city to enter into any surveillance-related contract or other agreement that conflicts with the provisions of this Article, and any conflicting provisions in such future

contracts or agreements, including but not limited to non-disclosure agreements, shall be deemed void and legally unenforceable.

To the extent permitted by law, the city shall publicly disclose all of its surveillance-related contracts, including any and all related non-disclosure agreements, if any, regardless of any contract terms to the contrary.

(Ord. No. 13489, § 2, 5-15-2018)

9.64.070 - Whistleblower protections.

1. Neither the city nor anyone acting on behalf of the city may take or fail to take, or threaten to take or fail to take, a personnel action with respect to any employee or applicant for employment, including but not limited to discriminating with respect to compensation, terms and conditions of employment, access to information, restrictions on due process rights, or civil or criminal liability, because:

A. The employee or applicant was perceived to, about to, or assisted in any lawful disclosure of information concerning the funding, acquisition, or use of a surveillance technology or surveillance data based upon a good faith belief that the disclosure evidenced a violation of this Article; or

B. The employee or applicant was perceived to, about to, or assisted or participated in any proceeding or action to carry out the purposes of this Article.

2. It shall be grounds for disciplinary action for a city employee or anyone else acting on behalf of the city to retaliate against another city employee or applicant who makes a good-faith complaint that there has been a failure to comply with any surveillance use policy or administrative instruction promulgated under this Article.

3. Any employee or applicant who is injured by a violation of this Section may institute a proceeding for monetary damages and injunctive relief against the city in any court of competent jurisdiction.

(Ord. No. 13489, § 2, 5-15-2018)

Chapter 9.64 - REGULATIONS ON CITY'S ACQUISITION AND USE OF SURVEILLANCE TECHNOLOGY

Sections:

9.64.010 - Definitions.

The following definitions apply to this Chapter.

1. "Annual Surveillance Report" means a written report concerning a specific surveillance technology that includes all the following:

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

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

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;

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

E. A summary of community complaints or concerns about the surveillance technology, and an analysis of the technology's adopted use policy and whether it is adequate in protecting civil rights and civil liberties. The analysis shall identify the race of each person that was subject to the technology's use. The Privacy Advisory Commission may determine, on an individual policy basis, to waive the obligation to identify the race of each person if the probative value is outweighed by the administrative burden and 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.

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.

Commented [BS1]: Officers may legitimately share records with other local depts. Same with a TRAK flyer. OPD would need to institute new policies and systems to require tracking every time any officer shares any leads acquired through any technology with anyone from another department (e.g. OPD may share an ALPR jpeg that contains data such as car color…through an email – this could not be tracked per standard ways OPD works with other departments).

Commented [BS2]: OPD appreciates this revised version for considering the administrative burden and potential greater invasiveness.

Commented [JB3R2]: While OPD tracks formal citizen complaints, the PAC would be more likely to receive general "complaints or concerns" about surveillance technology. Doesn't the PAC hold itself out as the proper forum for such complaints and concerns? OPD believes that the PAC may well be better situated to provide this summary. Similarly, the PAC was set up in order to assess OPD's use policies and "whether [they are] adequate in protecting civil rights and civil liberties." Again, this seems like an assessment the PAC is better situated than OPD to provide to the general public.

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;

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

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

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; and

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

2. "Biometric Surveillance Technology" means any computer software that uses Face Recognition Technology or Other Remote Biometric Recognition in real time or on a recording or photograph.

3. "City" means any department, agency, bureau, and/or subordinate division of the City of Oakland as provided by Chapter 2.29 of the Oakland Municipal Code.

4. "City Staff" means City personnel authorized by the City Administrator or designee to seek City Council approval of surveillance technology in conformance with this Chapter.

5. "Continuing Agreement" means an agreement that automatically renews unless terminated by one (1) party.

6. "Exigent Circumstances" means a law enforcement agency's good faith belief that an emergency involving danger of, or imminent threat of the destruction of evidence regarding, death or serious physical injury to any person requires the use of surveillance technology or the information it provides.

7. "Face Recognition Technology" means (A) an automated or semi-automated process that assists in identifying or verifying an individual based on an individual's face; or (B) logs characteristics of an individual's face, head, or body to infer emotion, associations, expressions, or the location of an individual.

8. "Large-Scale Event" means an event attracting ten thousand (10,000) or more people with the potential to attract national media attention that provides a reasonable basis to anticipate that exigent circumstances may occur.

9. "Other Remote Biometric Recognition" means (A) an automated or semi-automated process that (i) assists in identifying an individual, capturing information about an individual, or otherwise generating or assisting in generating information about an individual based on

Commented [BS4]: Do all modifications to a Use Policy post-approval need to go to PAC and back to Council?

Commented [JB5]: This is confusing because it appears to be a definition of Biometric Surveillance Technology. But this definition does not include many technologies that the PAC deems biometric surveillance technology, such as equipment used by the Crime Lab for DNA analysis.

This should be removed or renamed. There is no need for the disjunction. The PAC can still ban "Other Remote Biometric Recognition Technology", which is defined in 9 below.

physiological, biological, or behavioral characteristics ascertained from a distance; (ii) uses voice recognition technology; or (iii) logs such characteristics to infer emotion, associations, activities, or the location of an individual, and (B) does not include identification based on fingerprints or palm prints that have been manually obtained during the course of a criminal investigation or detention.

10. "Personal Communication Device" means a mobile telephone, a personal digital assistant, a wireless capable tablet and a similar wireless two-way communications and/or portable internet accessing devices, whether procured or subsidized by a city entity or personally owned, that is used in the regular course of city business.

11. “Predictive Policing Technology” means computer algorithms that use preexisting data to forecast or predict places or times that have a high risk of crime, or individuals or groups who are likely to commit a crime. This definition does not include computer algorithms used solely to visualize, chart, or map past criminal activity (e.g. heat maps).

Commented [BS6]: OPD appreciates this revised definition. Changing to “predict specific places or specific times” may still offer a more focused definition.

12. "Police Area" refers to each of the geographic districts assigned to a police commander and as such districts are amended from time to time.

13. "Surveillance" or "Surveil" means to observe or analyze the movements, behavior, data, or actions of individuals. Individuals include those whose identity can be revealed by license plate data when combined with any other record.

14. "Surveillance Technology" means any software, electronic device, system utilizing an electronic device, or similar technological tool used, designed, or primarily intended to collect, retain, analyze, process, or share audio, electronic, visual, location, thermal, olfactory, biometric, or similar information specifically associated with, or capable of being associated with, any individual or group. Examples of surveillance technology include, but is not limited to the following: cell site simulators (Stingrays); automatic license plate readers; gunshot detectors (ShotSpotter); facial recognition software; thermal imaging systems; body-worn cameras; social media analytics software; gait analysis software; video cameras that record audio or video, and transmit or can be remotely accessed. It also includes software designed to monitor social media services or forecast criminal activity or criminality, biometric identification hardware or software.

"Surveillance technology" does not include the following devices or hardware, unless they have been equipped with, or are modified to become or include, a surveillance technology as defined above:

A. Routine office hardware, such as televisions, computers, credit card machines, badge readers, copy machines, and printers, that is in widespread use and will not be used for any surveillance or law enforcement functions;

B. Parking Ticket Devices (PTDs);

C. Manually-operated, non-wearable, handheld digital cameras, audio recorders, and video recorders that are not designed to be used surreptitiously and whose functionality is limited to manually capturing and manually downloading video and/or audio recordings;

D. Surveillance devices that cannot record or transmit audio or video or be remotely accessed, such as image stabilizing binoculars or night vision goggles;

E. Manually-operated technological devices used primarily for internal municipal entity communications and are not designed to surreptitiously collect surveillance data, such as radios and email systems;

F. City databases that do not contain any data or other information collected, captured, recorded, retained, processed, intercepted, or analyzed by surveillance technology, including payroll, accounting, or other fiscal databases.

G. Medical equipment used to diagnose, treat, or prevent disease or injury.

H. Police department interview room cameras.

I. Police department case management and records management ~~systems~~ systems, including computer aided dispatch systems, and field-based reporting systems.

J. Police department early warning systems.

K. Personal communication devices that have not been modified beyond stock manufacturer capabilities in a manner described above.

L. Forensic instrumentation, equipment, reagents and standards that are used by the Oakland Police Department Criminalistics Laboratory (Crime Lab) as of August 2020 to analyze evidence samples collected in the course of an investigation, that upon analysis by the Crime Lab, may result in the identification of individual persons. A list of specific items is in Appendix A.

i. Like for like substitutions necessitated by improvements to current methodology, instrumentation failures or maintaining compliance with Federal Law will also be excluded.

ii. Entirely new biometric methodology outside the current scope of accreditation of the laboratory would require the laboratory to seek permission from the accreditation agency. This would also precipitate involvement of the Privacy Commission.

M. Live Scan machines (owned by the Alameda County Sheriff's Department but operated by OPD personnel).

15. "Surveillance Impact Report" means a publicly-released written report including at a minimum the following:

Commented [7]: Need more info from OPD re their proposed amendment to include records management systems, CAD, and field based reporting systems. AB 953

Commented [BS8R7]: PAC – are we clear on reasons for this addition?

Commented [BS9]: This addition is requested by the OPD Crime Lab Manager. OPD is arguing that these specific tools can be considered "biometric" per definition above of "surveillance technology." But in this case not everything that is "biometric" is surveillance. Perhaps a different form of exemption could be for forensic technology that is NOT used in real time or in the immediate presence of an individual or person. Crime Lab perspective – the technology is always used with a nexus of an actual crime – no prospective use of this biometric technology. We are trying to draw a balance between what is "surveillance" and simply forensic analysis. Staff think that the administrative burden of collating data for 270+ types of equipment into one or more Use Policies and then annual reports far exceeds the informational value achieved.

Commented [BJJ10]: OPD personnel use these stationary machines to conduct sex registrant fingerprinting, court bookings, juvenile in-custody fingerprinting, and applicant fingerprinting.

A. Description: information describing the surveillance technology and how it works, including product descriptions and manuals (as attachments, if publicly available and current) from manufacturers;

B. Purpose: information on the proposed purposes(s) for the surveillance technology;

C. Location: the location(s) it may be deployed, using general descriptive terms, and crime statistics for any location(s);

D. Impact: an assessment of the technology's adopted use policy and whether it is adequate in protecting civil rights and liberties and whether the surveillance technology was used or deployed, intentionally or inadvertently, in a manner that is discriminatory, viewpoint-based, or biased via algorithm;

E. Mitigations: identify specific, affirmative technical and procedural measures that will be implemented to safeguard the public from each such impacts;

F. Data Types and Sources: a list of all types and sources of data to be collected, analyzed, or processed by the surveillance technology, including "open source" data, scores, reports, logic or algorithm used, and any additional information derived therefrom;

G. Data Security: information about the steps that will be taken to ensure that adequate security measures are used to safeguard the data collected or generated by the technology from unauthorized access or disclosure;

H. Fiscal Cost: the fiscal costs for the surveillance technology, including initial purchase, personnel and other ongoing costs, the operative or proposed contract if available - or past contract if available, and any current or potential sources of funding;

I. Third Party Dependence: whether use or maintenance of the technology will require data gathered by the technology to be handled or stored by a third-party vendor on an ongoing basis;

J. Alternatives: a summary of all alternative methods (whether involving the use of a new technology or not) considered before deciding to use the proposed surveillance technology, including the costs and benefits associated with each alternative and an explanation of the reasons why each alternative is inadequate; and,

K. Track Record: a summary of the experience (if any) other entities, especially government entities, have had with the proposed technology, including, if available, quantitative information about the effectiveness of the proposed technology in achieving its stated purpose in other jurisdictions, and any known adverse information about the technology (such as unanticipated costs, failures, or civil rights and civil liberties abuses).

16. "Surveillance Use Policy" means a publicly-released and legally enforceable policy for use of the surveillance technology that at a minimum specifies the following:

Commented [BS11]: As long as there IS a manual and it is not very outdated, staff can comply.

Commented [BS12]: Staff may pursue a Use Policy as in drone/UAS before even having a final plan to purchase, or a choice of vendor. Even a proposed contract may not be available.

A. Purpose: the specific purpose(s) that the surveillance technology is intended to advance;

B. Authorized Use: the specific uses that are authorized, and the rules and processes required prior to such use;

C. Data Collection: the information that can be collected by the surveillance technology. Where applicable, list any data sources the technology will rely upon, including "open source" data;

D. Data Access: the category of individuals who can access or use the collected information, and the rules and processes required prior to access or use of the information;

E. Data Protection: the safeguards that protect information from unauthorized access, including encryption and access control mechanisms;

F. Data Retention: the time period, if any, for which information collected by the surveillance technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s), the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond that period;

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

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

I. Training: the training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology, ~~and the category of staff that will provide the training;~~

Commented [BS13]: For PAC: OPD cannot commit to a permanent decision as to who or what type of staff will produce the training. OPD will ensure that the proper training occurs and that such training is required per Use Policy.

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

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

L. Reporting: Any modifications to the required elements of the Annual Surveillance Report for this particular technology.

Commented [BS14]: May not be necessary now given PAC change to 9.64.010.E

Commented [JB15R14]: This is still necessary to allow flexibility. "Not applicable" will occasionally suffice, but it is important to have the flexibility to exempt certain technologies from certain reporting requirements.

17. "Voice Recognition Technology" means the automated or semi-automated process that assists in identifying or verifying an individual based on the characteristics of an individual's voice.

(Ord. No. 13563, § 3, 9-17-2019; Ord. No. 13489, § 2, 5-15-2018)

9.64.020 - Privacy Advisory Commission (PAC) notification and review requirements.

1. PAC Notification Required Prior to City Solicitation of Funds and Proposals for Surveillance Technology.

A. City staff shall notify the Chair of the Privacy Advisory Commission prior to:

1. Seeking or soliciting funds for surveillance technology, including but not limited to applying for a grant; or,

2. Soliciting proposals with a non-city entity to acquire, share or otherwise use surveillance technology or the information it provides.

B. Upon notification by city staff, the Chair of the Privacy Advisory Commission shall place the item on the agenda at the next Privacy Advisory Commission meeting for discussion and possible action. At this meeting, city staff shall inform the Privacy Advisory Commission of the need for the funds or equipment, or shall otherwise justify the action city staff will seek Council approval for pursuant to 9.64.030. The Privacy Advisory Commission may make a recommendation to the City Council by voting its approval to proceed, object to the proposal, recommend that the city staff modify the proposal, or take no action.

C. Should the Privacy Advisory Commission not make a recommendation pursuant to 9.64.020 1.B., City staff may proceed and seek Council approval of the proposed surveillance technology initiative pursuant to the requirements of Section 9.64.030.

2. PAC Review Required for New Surveillance Technology Before City Council Approval.

A. Prior to seeking City Council approval under Section 9.64.030, city staff shall submit a surveillance impact report and a surveillance use policy for the proposed new surveillance technology initiative to the Privacy Advisory Commission for its review at a regularly noticed meeting. The surveillance impact report and surveillance use policy must address the specific subject matter specified for such reports as defined under 9.64.010.

B. The Privacy Advisory Commission shall recommend that the City Council adopt, modify, or reject the proposed surveillance use policy. If the Privacy Advisory Commission proposes that the Surveillance Use Policy be modified, the Privacy Advisory Commission shall propose such modifications to city staff. City staff shall present such modifications to City Council when seeking City Council approval under Section 9.64.030.

C. Failure by the Privacy Advisory Commission to make its recommendation on the item within ninety (90) days of submission shall enable the city entity to proceed to the City Council for approval of the item.

3. PAC Review Requirements for Existing Surveillance Technology Before City Council Approval.

A. Prior to seeking City Council approval for existing city surveillance technology under Section 9.64.030 city staff shall submit a surveillance impact report and surveillance use policy to the Privacy Advisory Commission for its review at a regularly noticed meeting. The surveillance impact report and surveillance use policy must address the specific subject matter specified for such reports as defined under 9.64.010.

B. Prior to submitting the surveillance impact report and proposed surveillance use policy as described above, city staff shall present to the Privacy Advisory Commission a list of surveillance technology possessed and/or used by the city.

C. The Privacy Advisory Commission shall rank the items in order of potential impact to civil liberties.

D. Within sixty (60) days of the Privacy Advisory Commission's action in 9.64.020 1.C., city staff shall submit at least one (1) surveillance impact report and proposed surveillance use policy per month, after the PAC completes a recommendation for a different surveillance technology, to the Privacy Advisory Commission for review, beginning with the highest-ranking items as determined by both the Privacy Advisory Commission and staff, and continuing thereafter each month until a policy has been submitted for each item on the list.

E. Failure by the Privacy Advisory Commission to make its recommendation on any item within ninety (90) days of submission shall enable city staff to proceed to the City Council for approval of the item pursuant to Section 9.64.030.

(Ord. No. 13489, § 2, 5-15-2018)

9.64.030. - City Council approval requirements for new and existing surveillance technology.

1. City staff must obtain City Council approval prior to any of the following:

A. Accepting state or federal funds or in-kind or other donations for surveillance technology;

B. Acquiring new surveillance technology, or replacing existing surveillance technology that has not been previously approved by the City Council pursuant to the requirements of this Chapter, including but not limited to procuring such technology without the exchange of monies or consideration;

C. Using new surveillance technology, or using Council-approved existing surveillance technology or the information it provides for a purpose, in a manner, or in a location not previously approved by the City Council pursuant to the requirements of this Chapter; or

Commented [BS16]: This one technology per-month pace is not realistic, given the nature of the scrutiny and review and related staff time – as well as PAC capacity. We need a different standard - see addition in track changes.

Commented [BS17]: Departments might accept without a fully developed spending plan, or may need to change plans

Commented [BS18]: This phrase looks good to solve issue in next comment.

Commented [BS19]: This phrase can be interpreted to mean that city departments are in violation of this section for every piece of “existing surveillance technology” until the surveillance use policy is approved – a process that already takes years for OPD

Commented [BS20]: This intent of this revision is to clarify that PAC/Council must approve use of all tech and the way it is used, but deal with problem in comment above.

E. Entering into a continuing agreement or written agreement with a non-city entity to acquire, share or otherwise use surveillance technology or the information it provides, including data sharing agreements.

F. Notwithstanding any other provision of this Section, nothing herein shall be construed to prevent, restrict or interfere with any person providing evidence or information derived from surveillance technology to a law enforcement agency for the purposes of conducting a criminal investigation or the law enforcement agency from receiving such evidence or information.

2. City Council Approval Process.

A. After the PAC notification and review requirements in Section 9.64.020 have been met, city staff seeking City Council approval shall schedule for City Council consideration and approval of the proposed surveillance impact report and proposed surveillance use policy, and include Privacy Advisory Commission recommendations at least fifteen (15) days prior to a mandatory, properly-noticed, germane public hearing. Approval may only occur at a public hearing. City staff shall not unreasonably delay scheduling any item for City Council consideration.

B. The City Council shall only approve any action as provided in this Article after first considering the recommendation of the Privacy Advisory Commission, and subsequently making a determination that the benefits to the community of the surveillance technology outweigh the costs; that the proposal will safeguard civil liberties and civil rights; and that, in the City Council's judgment, no alternative with a lesser economic cost or impact on civil rights or civil liberties would be as effective.

C. For approval of existing surveillance technology for which the Privacy Advisory Commission failed to make its recommendation within ninety (90) days of review as provided for under 9.64.020 3.E, if the City Council has not reviewed and approved such item within four (4) City Council meetings from when the item was initially scheduled for City Council consideration, the city shall cease its use of the surveillance technology until such review and approval occurs.

3. Surveillance Impact Reports and Surveillance Use Policies are Public Records. City staff shall make the Surveillance Impact Report and Surveillance Use Policy, as updated from time to time, available to the public as long as the city uses the surveillance technology in accordance with its request pursuant to Section 9.64.020 A.1.

(Ord. No. 13489, § 2, 5-15-2018)

9.64.035 - Use of unapproved technology during exigent circumstances or large-scale event.

1. City staff may temporarily acquire or use surveillance technology and the data derived from that use in a manner not expressly allowed by a surveillance use policy in two (2) types of

Commented [21]: Make sure OPD understands this does not pertain to prohibited tech in Section 9.64.045

Commented [JB22]: For City Attorney: Does this provision require all changes to a Use Policy to go back to the City Council for approval? And would this override those use policies (e.g., the BWC/PDRD policy) that are overseen by the IMT and the Police Commission?

Commented [BS23]: Public hearing? Goal is to not have on closed session, does not need to be "public hearing." Review with OCA.

circumstances without following the provisions of Section 9.64.030: (A) exigent circumstances, and (B) a large-scale event.

2. If city staff acquires or uses a surveillance technology in the two (2) circumstances pursuant to subdivision 1., the city staff shall:

A. Use the surveillance technology to solely respond to the exigent circumstances or large-scale event.

B. Cease using the surveillance technology when the exigent circumstances or large scale event ends.

C. Only keep and maintain data related to the exigent circumstances and dispose of any data that is not relevant to an ongoing investigation.

D. Following the end of the exigent circumstances or large-scale event, report that acquisition or use to the PAC at their next respective meetings for discussion and/or possible recommendation to the City Council in accordance with the Sunshine Ordinance, the Brown Act, and City Administrator deadlines.

3. Any technology temporarily acquired in exigent circumstances or during a large-scale event shall be returned within seven (7) days following its acquisition, or when the exigent circumstances end, whichever is sooner, unless the technology is submitted to the City Council for approval pursuant to Section 9.64.030 and is approved. If the agency is unable to comply with the seven-day timeline, the agency shall notify the City Council, who may grant an extension.

(Ord. No. 13489, § 2, 5-15-2018)

9.64.040 - Oversight following City Council approval.

1. For each approved surveillance technology item, city staff must present a written annual surveillance report for Privacy Advisory Commission review by April 30 of the following year ~~a year from the date that the corresponding use policy was approved by the City Council, and annually thereafter~~ as long as the technology is in use. If city staff is unable to meet the deadline, city staff shall notify the Privacy Advisory Commission in writing of staff's request to extend this period, and the reasons for that request. The Privacy Advisory Commission may grant a single extension of up to sixty (60) days to comply with this provision.

A. After review by the Privacy Advisory Commission, city staff shall submit the annual surveillance report to the City Council.

B. The Privacy Advisory Commission 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.

C. Failure by the Privacy Advisory Commission to make its recommendation on the item within ninety (90) days of submission shall enable the city entity to proceed to the City Council for approval of the annual surveillance report.

2. Based upon information provided in city staff's Annual Surveillance Report and after considering the recommendation of the Privacy Advisory Commission, the City Council shall re-visit its "cost benefit" analysis as provided in Section 9.64.030 2.B. and either uphold or set aside the previous determination. Should the City Council set aside its previous determination, the city's use of the surveillance technology must cease. Alternatively, City Council may require modifications to the Surveillance Use Policy that will resolve any deficiencies.

(Ord. No. 13489, § 2, 5-15-2018)

9.64.045 - Prohibition on City's acquisition and/or use of (i) biometric surveillance technology, or (ii) predictive policing technology

A. Notwithstanding any other provision of this Chapter (9.64), it shall be unlawful for the City or any City staff to obtain, retain, request, access, or use:

1. Biometric surveillance technology; or

2. Predictive policing technology; or

3. Information obtained from either biometric surveillance technology or predictive policing technology.

B. City staff's inadvertent or unintentional receipt, access of, or use of any information obtained from biometric surveillance technology or predictive policing technology shall not be a violation of this Section 9.64.045 provided that:

1. City staff did not request or solicit the receipt, access of, or use of such information; and

2. City staff shall immediately destroy all copies of the information upon its discovery and shall not use the information for any purpose, unless required by law; and

3. City staff logs such receipt, access, or use in a written report provided at the next closest regularly scheduled meeting after discovery of the use, to the Privacy Advisory Commission for discussion and possible recommendation to the City Council. Such a report shall not include any personally identifiable information or other information the release of which is prohibited by law. In its report, City staff shall identify specific measures taken by the City to prevent the

Commented [JB24]: See above comments about the definition.

Commented [BS25]: Should suffice staff need to keep exculpatory evidence.

further transmission or use of any information inadvertently or unintentionally obtained through the use of such technologies; and

4. After review by the Privacy Advisory Commission, city staff shall submit the report to the City Council.

(Ord. No. 13563, § 3, 9-17-2019)

9.64.050 - Enforcement.

1. Violations of this Article are subject to the following remedies:

A. Any violation of this Article, or of a surveillance use policy promulgated under this Article, constitutes an injury and any person may institute proceedings for injunctive relief, declaratory relief, or writ of mandate in the Superior Court of the State of California to enforce this Article. An action instituted under this paragraph shall be brought against the respective city department, and the City of Oakland, and, if necessary to effectuate compliance with this Article or a surveillance use policy (including to expunge information unlawfully collected, retained, or shared thereunder), any other governmental agency with possession, custody, or control of data subject to this Article, to the extent permitted by law.

B. Any person who has been subjected to a surveillance technology in violation of this Article, or about whom information has been obtained, retained, accessed, shared, or used in violation of this Article or of a surveillance use policy promulgated under this Article, may institute proceedings in the Superior Court of the State of California against the City of Oakland and shall be entitled to recover actual damages (but not less than liquidated damages of one thousand dollars ($1,000.00) or one hundred dollars ($100.00) per day for each day of violation, whichever is greater).

C. A court shall award costs and reasonable attorneys' fees to the plaintiff who is the prevailing party in an action brought under paragraphs A. or B.

D. Violations of this Article by a city employee shall result in consequences that may include retraining, suspension, or termination, subject to due process requirements and in accordance with any memorandums of understanding with employee bargaining units.

(Ord. No. 13489, § 2, 5-15-2018)

9.64.060 - Secrecy of surveillance technology.

It shall be unlawful for the city to enter into any surveillance-related contract or other agreement that conflicts with the provisions of this Article, and any conflicting provisions in such future

contracts or agreements, including but not limited to non-disclosure agreements, shall be deemed void and legally unenforceable.

To the extent permitted by law, the city shall publicly disclose all of its surveillance-related contracts, including any and all related non-disclosure agreements, if any, regardless of any contract terms to the contrary.

(Ord. No. 13489, § 2, 5-15-2018)

9.64.070 - Whistleblower protections.

1. Neither the city nor anyone acting on behalf of the city may take or fail to take, or threaten to take or fail to take, a personnel action with respect to any employee or applicant for employment, including but not limited to discriminating with respect to compensation, terms and conditions of employment, access to information, restrictions on due process rights, or civil or criminal liability, because:

A. The employee or applicant was perceived to, about to, or assisted in any lawful disclosure of information concerning the funding, acquisition, or use of a surveillance technology or surveillance data based upon a good faith belief that the disclosure evidenced a violation of this Article; or

B. The employee or applicant was perceived to, about to, or assisted or participated in any proceeding or action to carry out the purposes of this Article.

2. It shall be grounds for disciplinary action for a city employee or anyone else acting on behalf of the city to retaliate against another city employee or applicant who makes a good-faith complaint that there has been a failure to comply with any surveillance use policy or administrative instruction promulgated under this Article.

3. Any employee or applicant who is injured by a violation of this Section may institute a proceeding for monetary damages and injunctive relief against the city in any court of competent jurisdiction.

(Ord. No. 13489, § 2, 5-15-2018)

CERTIFICATE OF ACCREDITATION

ANSI National Accreditation Board
2000 Regency Parkway, Suite 430, Cary, NC 27518

This is to certify that

Oakland Police Department
Criminalistics Laboratory

has been assessed by ANAB
and meets the requirements of

ISO/IEC 17025:2017

ANAB 17025:2017 Forensic Science Testing and Calibration Laboratories Accreditation Requirements
FBI Quality Assurance Standards for Forensic DNA Testing Laboratories:2011

while demonstrating technical competence in the field of

FORENSIC TESTING

Refer to the accompanying Scope of Accreditation for information regarding the types of tests to which this accreditation applies

Certificate Number: FT-0057

Valid to: 10/31/2022

Pamela L. Sale
Vice President, Forensics

ANSI National Accreditation Board

SCOPE OF ACCREDITATION TO:
ISO/IEC 17025:2017

ANAB 17025:2017 Forensic Science Testing and Calibration Laboratories Accreditation Requirements

FBI Quality Assurance Standards for Forensic DNA Testing Laboratories:2011

Oakland Police Department Criminalistics Laboratory

455 7th Street, Room 608
Oakland, California 94607

FORENSIC TESTING

Valid to: October 31, 2022 Certificate Number: FT-0057

Discipline: Biology			
Component/Parameter or Characteristic Tested	**Test Method**	**Items Tested**	**Key Equipment or Technology**
Body Fluid Identification[2,3]	FBU SOP	Blood, Semen, Saliva, Tissue, Urine, Feces	Chemical, Visual
DNA-STR[1]	Flexible Scope	Blood, Saliva, Urine, Feces, Hair, Bone, Teeth, Semen	Robotic System, Extraction, Capillary Electrophoresis, Data Interpretation System
Individual Characteristic Database	FBU SOP	DNA Profiles	Combined DNA Index System (CODIS)

Discipline: Firearms and Toolmarks			
Component/Parameter or Characteristic Tested	**Test Method**	**Items Tested**	**Key Equipment or Technology**
Physical Comparison	Firearms SOP	Ammunition Components	Comparison Microscope
Determination of Functionality	Firearms SOP	Firearm	Refer to Method
Length Measurement	Firearms SOP	Firearm	Measuring Equipment
Trajectory Determination[2]	Firearms SOP	Location, Physical Item	Refer to Method
Individual Characteristic Database	Firearms SOP	Ammunition Components	National Integrated Ballistic Information Network (NIBIN)

2000 Regency Parkway, Suite 430, Cary, NC 27518
414-501-5494 www.anab.org

ilac-MRA ANAB

Discipline: Friction Ridge			
Component/Parameter or Characteristic Tested	**Test Method**	**Items Tested**	**Key Equipment or Technology**
Collection[2,3]	LPU Processing Manual	Physical Evidence	Adhesive Lift, Photography
Enhancement[2,3]	LPU Processing Manual	Latent, Patent, Plastic	Visual (Photoshop), Photography, Physical, Chemical
Physical Comparisons	LPU SOP	Latent, Patent, Plastic to Known, Known to Known, Unknown to Unknown	Refer to Method
Individual Characteristic Database	LPU SOP	Latent, Patent, Plastic or a Known	California Automated Fingerprint Identification System (AFIS), Next Generation Identification (NGI)

Discipline: Seized Drugs			
Component/Parameter or Characteristic Tested	**Test Method**	**Items Tested**	**Key Equipment or Technology**
Qualitative Identification[1,2,3]	Flexible Scope	Solid, Liquid, Botanical	Macroscopic and Microscopic Exam, Color Spot Test, Microcrystalline Test, Thin Layer Chromatography, Gas Chromatography, Mass Spectrometry, Infrared Spectroscopy, Fluorescence Spectroscopy
Weight Measurement	DAU SOP	Solid, Liquid, Botanical	Balance

Note 1: A flexible scope has been granted for this component/parameter or characteristic tested. ANAB has assessed the competence required to develop, validate, and perform quality assurance within this provided service. New or modified methods for the item(s) and equipment/technology(ies) listed in this row on the Scope of Accreditation may be introduced. New measurement principles, item(s), and technology(ies) will require evaluation by ANAB prior to granting a scope extension. Contact the forensic service provider for information on the specific test method in use at any point in time and utilized for accredited testing work.

Note 2: Field Testing: performance of testing task(s) at a location other than that listed on this scope of accreditation. Often, but not always, the location is not under the control of the forensic service provider.

Note 3: The forensic service provider performs these testing services both at the stated location and in the field.

Pamela L. Sale
Vice President, Forensics

2000 Regency Parkway, Suite 430, Cary, NC 27518
414-501-5494 www.anab.org

POSITION STATEMENT

The OPD Criminalistics Laboratory views the analysis of DNA at the loci approved by the FBI as an investigative tool for determining the presence, or absence, of individuals associated with evidence collected at a crime scene. After collection, the evidence is turned into property. After a request for analysis, a genetic profile may be developed. Use of a database may then be necessary. If a database match is determined and confirmed by a gatekeeper of the database, then and only then is a name released to the OPD Criminalistics Laboratory. Only after a reference sample is collected from this individual and run through the same DNA analysis as the evidence to develop a profile does an OPD criminalist analyze this data to determine an inclusion or find an exclusion. There is a separation in time and space and the role of a trained human interpreter is key; at no time does a machine make any identification.

This differs vastly from the use of DNA as a biometric which would be a rapid analysis in which a machine makes a determination as to a person's identity directly from a sample. There may be no separation in time or space, there is no gatekeeper to disclosing named individuals and there is no trained human—the machine makes the call.

Neither does the Criminalistics Laboratory view the current DNA analysis practices as surveillance. DNA analysis cannot be done on random samples with no possible nexus to a crime scene, nor can it be done in real time (at present). The regions of the DNA analyzed are non-coding regions where phenotypes are not present. Most important to privacy, this means that characteristics of the individual such as blue eyes or a proclivity to develop cancer, are not part of the developed profile. The profile may only be used to include an individual or, very importantly, exclude others.

Nonetheless, the laboratory takes confidentiality seriously. The Laboratory is happy to disclose the rigorous number of safeguards to confidentiality existing in current protocols. Indeed, not only does laboratory policy dictate proper regard for confidentiality, but professional ethics codes to which all staff adhere and the laboratory's accreditation agency also mandate it. Lastly, if there were to be lapses in the disclosure of this confidential information, eligibility to use CODIS would be suspended and criminal prosecutions against laboratory personnel could occur.

The Laboratory hopes to be able to provide the Privacy Commission, City Council and most importantly, the residents of Oakland confidence that they are not being surveilled, biometrically profiled or if their DNA is analyzed in the course of a criminal investigation that the laboratory shields that information from improper dissemination with robust confidentially measures.

Instruments and Equipment

LabUnit	Type	Manufacturer	Item	In-Service Date	Out-Service Date	alibrationRequire	Critical	General Terminology
FB		AB	7500 System Detection Software			FALSE	FALSE	Quantitation software
FB	CE	AB 3130 Genetic Analyzer HID	3130 Capillary Electrophoresis Unit	18-Jan-11		FALSE	TRUE	Genetic Analyzer
FB	CE	Applied Biosystems	3500 Capillary Electrophoresis Unit			FALSE	TRUE	Genetic Analyzer
FB	Centrifuge	Hermle MR-2	Centrifuge, table top			FALSE	FALSE	Centrifuge for DNA digestion
FB	Centrifuge	Hermle Z-180 HLA	Centrifuge, table top	17-May-00		FALSE	FALSE	Centrifuge for DNA digestion
FB	Centrifuge	Hermle Z-180 HLA	Centrifuge, table top	01-Jun-01		FALSE	FALSE	Centrifuge for DNA digestion
FB	Centrifuge	Hermle Z-180 HLA	Centrifuge, table top	01-Jun-04		FALSE	FALSE	Centrifuge for DNA digestion
FB	Centrifuge	Hermle Z-180 HLA	Centrifuge, table top	01-Jun-04		FALSE	FALSE	Centrifuge for DNA digestion
FB	Centrifuge	Hermle Z233 M-2	Centrifuge, table top	21-Jan-10		FALSE	FALSE	Centrifuge for DNA digestion
FB	Centrifuge	Hermle Z233 M-2	Centrifuge, table top	21-Jan-10		FALSE	FALSE	Centrifuge for DNA digestion
FB	Centrifuge	Hermle Z-323	Centrifuge, table top			FALSE	FALSE	Centrifuge for DNA digestion
FB	Centrifuge	Labnet	Spectrafuge			FALSE	FALSE	Centrifuge for DNA digestion
FB	Centrifuge	ThermoFisher Scientific	DNA SpeedVac System			FALSE	FALSE	DNA Concentrator
FB	Incubator	Eppendorf	Thermomixer R - A	09-Feb-12		FALSE	FALSE	Incubator for DNA digestion
FB	Incubator	Eppendorf	Thermomixer R - C	09-Feb-12		FALSE	FALSE	Incubator for DNA digestion
FB	Incubator	Thelco	Incubator Oven			FALSE	FALSE	
FB/LP	Light Source	CRIMESCOPE	Forensic Light Source	30-Jul-09		FALSE	FALSE	Alternate Light Source for screening
FB/LP	Light Source	Foster & Freeman	CrimeLite - Blue			FALSE	FALSE	Alternate Light Source for screening
FB/LP	Light Source	Foster & Freeman	CrimeLite - Blue Green			FALSE	FALSE	Alternate Light Source for screening
FB/LP	Light Source	Foster & Freeman	CrimeLite - Green			FALSE	FALSE	Alternate Light Source for screening
FB/LP	Light Source	Foster & Freeman	CrimeLite - UV			FALSE	FALSE	Alternate Light Source for screening
FB/LP	Light Source	Foster & Freeman	CrimeLite - Violet			FALSE	FALSE	Alternate Light Source for screening
FB/LP	Light Source	Foster & Freeman	CrimeLite - White			FALSE	FALSE	Alternate Light Source for screening
FB/LP	Microscope	Keyence	Keyence Microscope with camera and scale	05-Aug-20		FALSE	FALSE	Microscope
FB	Microscope	Zeiss (bought via CTK)	Zeiss AxioLab Microscope with HD Digital Camera	05-Aug-20		FALSE	FALSE	Microscope
FB	Peripheral	HP	Server hard disk for CODIS	16-Jul-10		FALSE	FALSE	CODIS Server
FB	Peripheral	HP	Server hard disk for CODIS	16-Jul-10		FALSE	FALSE	CODIS Server
FB	Peripheral	HP	Server hard disk for CODIS	16-Jul-10		FALSE	FALSE	CODIS Server
FB	Quantitation	Applied Biosystems	7500 Real Time PCR System	01-Sep-07		FALSE	TRUE	Real-time PCR Instrument
FB	Quantitation	Applied Biosystems	7500 Real Time PCR System	18-Jan-11		FALSE	TRUE	Real-time PCR Instrument
FB	Robot	Auroa Biomed	Versa 1100			FALSE	FALSE	Liquid Handling Robot
FB	Robot	Aurora Biomed	Versa 1100	26-Feb-13		FALSE	TRUE	Liquid Handling Robot
FB	Robot	Qiagen	BioRobot EZ1 XL	03-Jun-13		FALSE	TRUE	Liquid Handling Robot
FB	Robot	Qiagen	BioRobot EZ1 XL	21-Jan-11		FALSE	TRUE	Liquid Handling Robot
FB	Robot	Qiagen	BioRobot EZ1 XL	01-Apr-17		FALSE	TRUE	Liquid Handling Robot
FB	Robot	Qiagen	QIAgility Liquid Handling Robot	31-Mar-15		FALSE	TRUE	Liquid Handling Robot
FB	Robot	Qiagen	QIAgility Liquid Handling Robot	21-Jan-11		FALSE	TRUE	Liquid Handling Robot
FB	Robot	Qiagen	QIAgility Liquid Handling Robot	21-Jan-11		FALSE	TRUE	Liquid Handling Robot
FB	Software	AB	7500 System Detection Software	25-Jul-19		FALSE	FALSE	Quantitation software
FB	Software	AB	7500 System Detection Software	13-May-20		FALSE	FALSE	Quantitation software
FB	Software	AB	Data Collection v4 6-Dye	01-Apr-17		FALSE	FALSE	Typing software
FB	Software	AB	Data Collection v4 6-Dye	30-Mar-16		FALSE	FALSE	Typing software
FB	Software	AB	GMIDX Client			FALSE	FALSE	Typing software
FB	Software	ABI	GMID X Full Installation			FALSE	FALSE	Typing software
FB	Software	Aurora Biomed	VERSAware v 1.0.26			FALSE	FALSE	
FB	Software	NicheVision	ArmedXpert Analysis Software			FALSE	FALSE	Typing software
FB	Thermal Cycler	Life Technologies (aka AB)	Proflex PCR System D			FALSE	TRUE	Thermal Cycler
FB	Thermal Cycler	Life Technologies (aka AB)	Proflex PCR System E			FALSE	TRUE	Thermal Cycler
LP	ESDA	Foster + Freeman	ElectroStatic Detection Apparatus			FALSE	FALSE	
LP	Light Source	Foster + Freeman	Halogen Fiber Optic Light Source and Accessory Package	20-May-14		FALSE	FALSE	

LP	Measurement Standard	Applied Image Inc	Ultra High Resolution Target - T-90-N-CG	26-Apr-13		FALSE	FALSE
LP	Miscellaneous	Arrowhead Forensics	Arrowflow FDCS - Environmental Chamber	18-May-16		FALSE	FALSE
LP	Miscellaneous	Foster + Freeman	MVC 3000D - CA Fuming Chamber	18-May-16		FALSE	FALSE
LP	Miscellaneous	Polaroid	MP-4 Land Camera Copy Stand			FALSE	FALSE
LP	Monitor	ViewSonic	XG3220			FALSE	FALSE
LP	Monitor	ViewSonic	VP2770-LED/VS14703	18-Sep-14		FALSE	FALSE
LP	Peripheral	Wacom	Pen & Tablet - Intuos Pro M/PTH-651	18-Sep-14		FALSE	FALSE
LP	Peripheral	Western Digital	External Drive - My Passport Ultra	18-Sep-14		FALSE	FALSE
LP	Scanner	Epson	Scanner - V700 Photo	20-Jul-10		FALSE	FALSE
LP	Server	HP	HP proLiant ML350 G6 - ADAMS Server	03-Sep-10		FALSE	FALSE
LP	Vacuum Chamber	Sirchie	VAC100			FALSE	FALSE
LP	Vacuum Chamber	Sirchie	VAC200			FALSE	FALSE
LP	Software	Forensic Comparison Software	FCS				
LP	Software	Foray	ADAMS (software for images)				
LP	Lightsource	Coherent	TracER				
LP	Software	FBI	Universal Latent Workstation				
LP	Server	Foray	Backup server for system				
LP	Software	Adobe	Photoshop				

Reagents, Standards and equipment

LabUnit	Type	Description	Directions	UsedFor		QCNeeded	CriticalReagent
FB	EXT	EZ1 Robot Tissue Kit				TRUE	FALSE
FB	POP4	POP 4, 3130, 3.5ml				TRUE	TRUE
FB	310	Capillary				TRUE	FALSE
FB	3130	Capillary Array, 36cm				TRUE	TRUE
FB	CE	Analysis Buffer, 10X				TRUE	TRUE
FB	CE	5 Dye Matrix Standards				FALSE	FALSE
FB	Reagent	TE	Add Tris HCl and 0.5M EDTA to dH2O. Adjust pH to 8.0 with 1N HCl. Aliquot into bottles, mark the volume, and autoclave. After autoclaving, adjust volume back to mark with sterile dH2O.	Tris-EDTA buffer is used to dilute extracted DNA while using the Centricon-100 spin columns. TE-4 can be used instead of sterile dH2O to dilute DNA samples.		TRUE	TRUE
FB	Reagent	PBS (Reagent)	Add commercially prepared packets of phosphate buffered saline (PBS, pH 7.4) to dH2O. Dissolve the powder and mark the volume. After autoclaving, adjust to original volume with sterile dH2O. This reagent can be commercially prepared.	PBS pH 7.4 is used in the extraction of cellular material from substrates (i.e. epithelial cells, spermatozoa).		TRUE	TRUE

FB	Reagent	Dithiothreitol - Manual (Reagent)	Dissolve DTT in dH2O, then aliquot 220 µL into 0.5 mL microcentrifuge tubes. 1 unit = 1 mL	Dithiothreitol reagent is used in differential extraction of biological material potentially containing spermatozoa, digestion of hair, and digestion of bone.		TRUE	TRUE
FB	Reagent	Proteinase K - Manual (Reagent)	Add Proteinase K to dH2O. Dissolve, and aliquot 220 µL in 0.5 mL microcentrifuge tubes. 1 unit = 1 mL	Proteinase K is used to inactivate endogenous nucleases such as RNases and DNases, and to digest proteins. Pro K is a nonspecific serine protease.		TRUE	TRUE
FB	Reagent	123 bp Ladder	The ladder DNA is diluted in 6X loading buffer and TE-4 to yield final concentrations of 1 µg DNA / 6 µL and 1X loading buffer.	The 123 bp DNA ladder is used in the product gel to evaluate the size of double-stranded DNA. This ladder consists of 34 fragments ranging in length from 123 to 4182 bp.		TRUE	TRUE

FB	Chemical	EDTA, 0.5M	Commercially prepared.	0.5 M EDTA is used in many of the buffers as a preservative by chelating heavy metals which can act as cofactors for DNA damaging enzymes. This concentrated EDTA is added to other buffer preparations. Should be made at the start of the Chemical Batch pr		TRUE	TRUE
FB	Chemical	Dithiothreitol (Chemical)				FALSE	FALSE
FB	Chemical	Proteinase K (Chemical)				FALSE	FALSE
FB	AMP	Yfiler Kit				TRUE	TRUE
FB	EXT	EZ1 Investigator Kit				TRUE	TRUE
FB	Reagent	EZ1 Buffer MTL	no manufacturer expiration date. Per email conversation, they recommend ~ 1 year after receipt. Our expiration date will be at the end of the chemical batch year.			TRUE	TRUE
FB	CE	DS-33 Maxtrix Standards				FALSE	FALSE
FB	Reagent	Hydrogen Peroxide, 30%, 500mL				TRUE	FALSE
FB	Reagent	Xmas Tree Stains				TRUE	TRUE
FB	Chemical	Dnase I (Chemical)				FALSE	FALSE
FB	Chemical	Magnesium Chloride Solution	Keep container tightly closed in a dry and well-ventilated place.	making MgCl2/CaCl2 reagents for Dnase based selective degradation.		FALSE	FALSE
FB	Consumable	Seratec p30 Cartridges	QC 1 in lot # prior to use	Semen body fluid testing: detection of prostate specific antigen		TRUE	TRUE
FB	QUANT	7500 Spectral Calibration Kit II (CY3, CY5 and Texas Red Dyes)				FALSE	FALSE

FB	Reagent	Amylase Buffer (Reagent)	Dissolve NaH2PO4, Na2HPO4, and NaCl in dH2O. Mark the volume and autoclave. After autoclaving, adjust volume back to mark with sterile dH2O.	Amylase radial diffusion and mapping. This is the in-house preparation of this buffer. It has been replaced by using manufacturer prepared buffer mix.		TRUE	TRUE
FB	Chemical	AP Spot Test (Chemical)		NPFA rating: (dibasic sodium phosphate 1/0/1/2, maleic acid 3/0/0/0, alpha naphthyl acid phosphate 2/1/0/0, o-dianisidine-tetrazotized 1/0/0/0)		TRUE	TRUE
FB	Reagent	Carrier RNA (Aliquots)	Reconstitute the carrier RNA by adding 310uL TE to one tube of carrier RNA. Do not vortex! Prepare 15uL aliquotes into 200uL PCR tubes.	CH 41.7 23 Aug 11 HW		TRUE	TRUE
LP	Reagent	Crystal violet				TRUE	TRUE
FB	Unk	K562 DNA High Molecular Weight		Coffee Can		FALSE	FALSE
FB	Reagent	o-Tolidine (Reagent)	1% o-tolidine (w/v) dissolved in a 1:1 solution of ethanol and glacial acetic acid	Ortho-tolidine is used for presumptive blood tests.		TRUE	TRUE
FB	Chemical	o-Tolidine (Chemical)		Blood Presumptive Test		FALSE	FALSE
FB	Chemical	Phenolphthalin (Chemical)	Add ~5 mg of phenolphthalin into ~2mL of saturated sodium carbonate solution and mix.	Blood Presumptive Test		FALSE	FALSE
FB	Unk	PowerPlex Matrix Standards		Validation ONLY/Kit expired		FALSE	FALSE
FB	QUANT	7500 Spectral Calibration Kit I				FALSE	TRUE
FB	Reagent	Formamide (Reagent)	From the 25mL bottle, aliquot 25 1mL samples into a 1.7mL micro centrifuge tube.			TRUE	TRUE

FB	Reagent	Amylase Diffusion Buffer Mix (Reagent)	Dissolve 1 container of Amylase Buffer Mix (SERI B116) in 500mL water. Mark the volume and autoclave. After autoclaving, adjust volume back to mark with sterile dH2O.	Amylase radial diffusion and mapping.		FALSE	TRUE
FB	Reagent	AP Spot Test (Reagent)	Dissolve 0.26g SERI AP spot test reagent in 10mL water.	Presumptive semen testing		TRUE	TRUE
FB	Reagent	Phenolphthalin (Reagent)	Add ~5 mg of phenolphthalin into ~2mL of saturated sodium carbonate solution and mix.	Blood Presumptive Test		TRUE	TRUE
FB	Reagent	TWB (Reagent)	Add 20mM Tris HCl and 1 mM EDTA, pH 8.0 stock, and distilled water. Adjust pH to 8.0 with 1N HCl. Mark volume level, autoclave and bring to marked volume with sterile dH2O. Lastly, add 2% Tween 80.			TRUE	TRUE
FB	Reagent	Dnase I - Versa (Reagent)	Add Dnase I to DEPC treated water. Then add 40% glycerol to solution. Prepare 380uL aliquots into 2.0mL tubes. 1 unit = 1 mL ***This recipe is for 3363 Kunitz units/mg Dnase***	used in the differential digestion methods to remove residual free EC DNA from the sperm fraction prior to digestion of sperm.		TRUE	TRUE
FB	Reagent	EDTA - Versa (Reagent)	Prepare 440uL aliquots of 0.5M EDTA stock solution into 2.0mL sample tubes. 1 unit = 1 mL	used in the differential digestion methods to inactivate DNase prior to digestion of sperm.		TRUE	TRUE
FB	Reagent	MgCl2/CaCl2 - Versa (Reagent)	Add the MgCl2 and CaCl2 chemicals to DEPC treated water. Prepare 500uL aliquots in 2.0mL tubes. 1 unit = 1 mL	used in the differential digestion methods to activate Dnase to remove residual EC DNA prior to digestion of sperm.		TRUE	TRUE

FB	Reagent	Dithiothreitol - Versa (Reagent)	Dissolve DTT in dH2O in an appropriately sized container, then aliquot 440uL aliquots in 2.0mL tubes. 1 unit = 1 mL	Dithiothreitol reagent is used in differential extraction of biological material potentially containing spermatozoa, digestion of hair, and digestion of bone.		TRUE	TRUE
FB	Reagent	Proteinase K - Versa (Reagent)	Add Proteinase K to dH2O, dissolve and prepare 440uL aliquots in 2.0mL tubes. 1 unit = 1 mL	Proteinase K is used to inactivate endogenous nucleases such as RNases and DNases, and to digest proteins. Pro K is a nonspecific serine protease.		TRUE	TRUE
FB	AMP	PowerPlex Fusion				TRUE	TRUE
FB	Reagent	EDTA -Manual (Reagent)	Prepare 220uL aliquots of 0.5M EDTA stock solution into 0.5mL microcentrifuge tubes. 1 unit = 1 mL	used in the differential digestion methods to inactivate DNase prior to digestion of sperm.		TRUE	TRUE
FB	Reagent	MgCl2/CaCl2 Salt Solution - Manual (Reagent)	Add the MgCl2 and CaCl2 chemicals to DEPC treated water. Prepare 275uL aliquots in 0.5mL microcentrifuge tubes. 1 unit = 1 mL	used in the differential digestion methods to activate Dnase to remove residual EC DNA prior to digestion of sperm.		TRUE	TRUE

FB	Reagent	Dnase I - Manual (Reagent)	Add Dnase I to DEPC treated water. Then add 40% glycerol to solution. Prepare 165uL aliquots into 0.5mL microcentrifuge tubes. 1 unit = 1 mL ***This recipe is for 3363 Kunitz units/mg Dnase***	used in the differential digestion methods to remove residual free EC DNA from the sperm fraction prior to digestion of sperm.		TRUE	TRUE
FB	Consumable	Rapid Stain ID-Semen				FALSE	FALSE
FB	Consumable	Rapid Stain ID-Saliva				FALSE	FALSE
FB	Consumable	Rapid Stain ID-Blood				FALSE	FALSE
FB	Consumable	Rapid Stain ID-Urine				FALSE	FALSE
FB	Consumable	HemaTrace ABA card Human Blood				FALSE	FALSE
LP	Chemical	L-Alanine, 5 g bottle				FALSE	FALSE
LP	Chemical	Leuco Crystal Violet, 5 g bottle				FALSE	FALSE
LP	Chemical	Naphthol Blue Black, 25 g bottle				FALSE	FALSE
LP	Chemical	Ninhydrin 99%, 50 g bottle				FALSE	FALSE
LP	Chemical	Rhodamine 6G, 25 g bottle				FALSE	FALSE
LP	Solvent	Shandon (Xylene Substitute)				FALSE	FALSE
LP	Chemical	Sudan Black B, 25 g bottle				FALSE	FALSE
LP	Powder	Fingerprint Powder - Bi-Chromatic, 16 oz jar				FALSE	FALSE
LP	Powder	Fingerprint Powder - Print Glo, Fluorescent, Magnetic				FALSE	FALSE
LP	Reagent	Amido Black - Aqueous, Solution	Commercially purchased. Aqueous Amido Black has an indefinite shelf life [5]. Store in clear or dark bottles.	Non porous surface with blood		FALSE	FALSE
LP	Reagent	Crystal (Gentian) Violet - Working Solution	Combine the ingredients and allow crystals to dissolve using a stir plate if necessary. The shelf life of the working solution is indefinite.	Adhesive side of tape		FALSE	FALSE
LP	Reagent	Ninhydrin - Working Solution, Acetone	Dissolve Ninhydrin crystals in Methanol on a stirring device (a magnetic stirrer is recommended). Add 2-Propanol to Ninhydrin/Methanol solution, stir. Add Ninhydrin, Methanol, 2-Propanol solution to Acetone and stir.	Porous items containing amino acids		FALSE	FALSE
LP	Reagent	Ninhydrin - Working Solution, Pet Ether	Dissolve Ninhydrin crystals in Methanol on a stirring device (a magnetic stirrer is recommended). Add 2-Propanol to Ninhydrin/Methanol solution, stir. Add Ninhydrin, Methanol, 2-Propanol solution to Petroleum Ether and stir.	Porous items containing amino acids		FALSE	FALSE
LP	Chemical	Photo-Flo 600 Solution, 1 gal bottle				FALSE	FALSE

LP	Reagent	Rhodamine 6G - Working Solution, Methanol	Combine the ingredients and place on a stirring device until all the Rhodamine 6G is dissolved. The concentration of the fluorescent dye may be adjusted. Water may be used as an alternative carrier solvent.	Nonporous surface dye staining		FALSE	FALSE
LP	Reagent	Sudan Black - Working Solution				FALSE	FALSE
LP	Powder	Fingerprint Powder - Silver/Gray, 2 oz jar				FALSE	FALSE
LP	Powder	Fingerprint Powder - Black, Swedish, 60 ml jar				FALSE	FALSE
LP	Powder	Fingerprint Powder - Silver, Special, 60 ml jar				FALSE	FALSE
LP	Chemical	Ninhydrin - Monohydrate, ACS grade, 100 g bottle				FALSE	FALSE
LP	Other	ESDA - Cascade Beads, 1 kg bottle				FALSE	FALSE
LP	Reagent	CA - Liquid, Cyanobloom	See SOP	Fuming		FALSE	FALSE
LP	Powder	ESDA - Cascade Developer, 25 g bottle				FALSE	FALSE
LP	Powder	ESDA - Toner, 250 g bottle				FALSE	FALSE
LP	Powder	Fingerprint Powder - Green, Fluorescent, 2 oz				FALSE	FALSE
LP	Powder	Fingerprint Powder - Green, Fluorescent, 2 oz jar				FALSE	FALSE
LP	Powder	Fingerprint Powder - Green, Fluorescent, Magnetic, 1 oz jar				FALSE	FALSE
LP	Powder	Fingerprint Powder - Red, Fluorescent, 2 oz jar				FALSE	FALSE
LP	Powder	Fingerprint Powder - Red, Fluorescent, Magnetic, 1 oz jar				FALSE	FALSE
LP	Powder	Fingerprint Powder - Yellow, Fluorescent, 2 oz jar				FALSE	FALSE
LP	Powder	Fingerprint Powder - Yellow, Fluorescent, Magnetic, 2 oz jar				FALSE	FALSE
LP	Powder	Fingerprint Powder - Bi-Chromatic, Magnetic, 16 oz jar				FALSE	FALSE
LP	Chemical	Amido Black, 25 g bottle				FALSE	FALSE
LP	Chemical	Basic Yellow 40, 25 g bottle				FALSE	FALSE
LP	Chemical	Crystal Violet, 25 g bottle				FALSE	FALSE
LP	Chemical	Molybdenum Disulfide - SPR, 30 g jar				FALSE	FALSE
LP	Chemical	Sticky-Side Powder kit - Photo-Flo 200 Solution				FALSE	FALSE
LP	Other	CA - Fuming Wand kit with Butane				FALSE	FALSE
LP	Other	Mikrosil - Casting Putty (kit), white				FALSE	FALSE
LP	Other	Mikrosil - Hardener				FALSE	FALSE
LP	Powder	Fingerprint Powder - Black Ruby, Fluorescent, Magnetic, 1 oz jar				FALSE	FALSE
LP	Powder	Fingerprint Powder - Black, Magnetic, 16 oz jar				FALSE	FALSE

LP	Powder	Fingerprint Powder - White, 2 oz jar				FALSE	FALSE
LP	Powder	Sticky-Side Powder kit - Powder				TRUE	FALSE
LP	Other	CA - Fuming Wand kit, UV Fuming Cartridge				FALSE	FALSE
LP	Powder	Fingerprint Powder - Black, 16 oz jar				FALSE	FALSE
LP	Other	CA - Fuming Wand kit, CA Cartridges, Fuminator				FALSE	FALSE
LP	Chemical	DFO (1, 8-Diazafluoren-9-one), 1 g vial				FALSE	FALSE
LP	Reagent	CA - Gel Packet, The Finder	See SOP	Fuming		FALSE	FALSE
LP	Reagent	DFO (1, 8-Diazafluoren-9-one) - Working Solution, Spray	It is important that the DFO powder be ground with a mortar and pestle prior to solution preparation to ensure complete solubility. Grinding DFO powder should be performed in a hood, per laboratory safety guidelines. Combine the ingredients in the order	Porous items containing amino acids		FALSE	FALSE
LP	Reagent	Rhodamine 6G - Working Solution, Water	Combine the ingredients and place on a stirring device until all the Rhodamine 6G is dissolved. The concentration of the fluorescent dye may be adjusted. Methanol may be used as an alternative carrier solvent.	Nonporous surface dye staining		FALSE	FALSE
LP	Reagent	Sticky Side Powder - Working Solution	Place the sticky-side powder in a shallow jar. Fill the brown dropper-bottle half full of water and half full of Photo-Flo 200. Shake well. Using the dropper, add this solution to the powder in the shallow jar until a paste with the consistency of thin	Adhesive side of tape		FALSE	FALSE
LP	Reagent	DFO (1, 8-Diazafluoren-9-one) - Working Solution in Pet Ether	Combine the ingredients and place on a stirring device for approximately 20 minutes until the DFO is dissolved. Dilute the stock solution to 2L with petroleum ether. The working solution should be a clear gold color.	Porous items containing amino acids		TRUE	FALSE
LP	Chemical	Basic Yellow 40				FALSE	FALSE
FB	Chemical	PBS Buffer pH 7.4 with Tween 20 Powder Blend (5 packs/box)				FALSE	FALSE
FB	AMP	PowerPlex Fusion 6C, Custom				FALSE	FALSE
FB	Chemical	Proteinase K (1 g)				FALSE	FALSE
FB	Chemical	Xmas Tree Stain				FALSE	FALSE
LP	Positive Control	Control Strip with L-Alanine: 100 microgram dilution	Dip control strip in amino reactive solutions and follow post-treatment procedurs, if applicable.	amino reactive solutions		FALSE	FALSE
FB	Consumable	Reference Collection Kit				FALSE	FALSE

FB	Consumable	Sexual Assault Collection Kit (Female)				FALSE	FALSE
FB	Consumable	Sexual Assault Collection Kit (Male)				FALSE	FALSE
LP	Chemical	Black Wetwop	Pre-mixed solution to develop latent prints on non-porous, adhesive surfaces.			TRUE	FALSE
LP	Chemical	Sudan Black B, 25g bottle	Stain for use in latent print development on wet, non-porous & grease/sebaceous contaminated surfaces.			TRUE	FALSE
FB	Positive Control	DNA Std - NIST Traceable		Annual QC check of the FBU DNA analysis processes Genotypes attached to the MSDA		TRUE	TRUE
LP	Solvent	HFE-7100 3M NOVEC Engineering Fluid	Carrier solvent for Ninhydrin or DFO. Used on porous surfaces for latent print development.			TRUE	FALSE
LP	Chemical	1, 2 Indanedione	Dye-stain used on porous materials for development of latent prints.			TRUE	FALSE
LP	Chemical	Black Wetwop	Pre-mixed solution for use to develop latent prints on non-porous, adhesive surfaces.			TRUE	FALSE
LP	Chemical	White Wetwop	Pre-mixed solution for use to develop latent prints on non-porous, adhesive surfaces.			TRUE	FALSE
LP	Chemical	Formic Acid, Optima LCMS grade	Reagent for use in Amido Black Working Solution - detection & enhancement of blood prints on both porous and non-porous surfaces.			TRUE	FALSE
LP	Chemical	5-Sulfosalicylic Acid Dihydrate	Chemical for use in Amido Black solution.	Development of latent prints on blood stained non-porous surfaces.		TRUE	FALSE
LP	Chemical	L-Alanine, 99%, Molecular Formula: C3H7NO2	**30-Aug: Incomplete Master Item Inventory entry, pending receipt of chemical. DGF**	Amino Acid Control Strip		FALSE	FALSE
LP	Positive Control	L-Alanine Control Test Strip with two (2) dilutions	1.On the scale, place 0.5g of L-Alanine in a weigh boat 2.In a 25mL beaker: a.Dissolve 0.5g of L-Alanine in 5mL of Distilled Water. b.In a 200mL beaker, set aside 1mL of the 100 microgram L Alanine dilution to be used in the 1-microgram dilution below	Used for +/- control for DFO & Ninhydrin		FALSE	FALSE

LP	Consumable	L-Alanine Solution 1	1.Set the RL2 pipette to draw 1 microliter of solution in the pipette tip. 2. Dispense 1 microliter of solution as a concentrated drop in the 100-microgram location on the test strip.	+ Control for DFO & Ninhydrin		FALSE	FALSE
LP	Consumable	L-Alanine Solution 2	1. Set the RL2 pipette to draw 1 microliter of solution in the pipette tip. Always dial the pipette down to the desired volume. 2. Dispense 1 microliter of solution as a concentrated drop in the 1-microgram location on the test strip	+ Control for DFO & Ninhydrin		FALSE	FALSE
LP	Chemical	Acetonitrile	Rhodamine recipe, details to follow - used for print enhancement			TRUE	FALSE
FB	QUANT	PowerQuant System	store kit frozen. Reduce freeze-thaw cycles for all reagents. Prior to use, thaw 2XMM and 20XPrimer to RT, vortex each 10 seconds, don't spin down. Mix final master mix prior to use. Male gDNA standard should be thawed, aliquoted and stored refrigerated (	Human DNA quantitation: autosomal, male and degradation index.		TRUE	TRUE
FB	Other	PowerQuant Calibration Kit		calibration of the real-time PCR thermal cycler (7500) when using PowerQuant DNA Quantitation kit.		FALSE	TRUE
LP	Reagent	Amido Black-Working Solution	Combine all ingredients an mix using a stirring device until all Amido Black/Naphthol Blue Black is dissolved. This should take approximately 30min.	Dye which stains protein present in blood to give a blue-black product. It will not detect normal constituents of latent prints and therefore must be used in sequence with other techniques when blood-contaminated latent prints are examined.		FALSE	FALSE

LP	Reagent	Amido Black - Rinse Solution	Combine the ingredients.	Apply rinse following Amido Black - Working solution		FALSE	FALSE
LP	Reagent	Small Particle Reagent - Dark, Commercially Prepared	***NOT FOR USE IN CASEWORK UNTIL VALIDATED*** PROCEDURE 1 - DIPPING METHOD: Under a hood or well-ventilated area, using proper PPE (lab coat, gloves and safety glasses): 1. Thoroughly shake the commercially prepared bottle of SPR and pour the solution i	Light colored, non-porous or adhesive items that are or have been wet, items which have been soaked in liquid accelerants. Surfaces that need other forensic examinations such as biology, questioned document, or trace examinations should be carefully eval		TRUE	TRUE
FB	EXT	Casework Direct Kit				TRUE	TRUE
FB	Consumable	Seratec HemDirect Hemoglobin Assay	incubate cutting or portion of AqE from stain, add to cartridge, read results	Confirmatory test for blood using the detection of human hemoglobin in a immunoassay.		TRUE	TRUE
LP	Powder	Fingerprint Powder - Bi-Chromatic, 16 oz jar				FALSE	FALSE
LP	Powder	Fingerprint Powder - Black, 16oz jar	Apply to a non-porous surface for development of prints			FALSE	FALSE
FB	CE	Capillary Array (3500), 8 cap, 36cm	Install capillary array using the wizard in the 3500 software.	STR typing using the 3500 genetic analyzer		TRUE	TRUE

Oakland Police Department Criminalistics Laboratory
List of Biometric Instrumentation, Reagents, Standards and Equipment

Background

The Oakland Police Department Criminalistics Laboratory has a long and laudable history. In existence since July of 1944, the Laboratory celebrated our 75th anniversary last year. The first Laboratory Director, John Davis, was a towering figure in forensic science who took research and professional engagement seriously by publishing technical papers, founding journals and establishing professional organizations (California Association of Criminalists). Under the leadership of Jan Bashinski (the first female Laboratory Director in California), the Laboratory achieved accreditation in 1983, becoming the first in California and the fourth in the nation to achieve this status. The OPD Laboratory has maintained continuous accreditation since that time (see Attachment 1: Certificate and Scope of Accreditation). Accreditation requires and ensures that laboratories use appropriate methods and have policies on how to safeguard the proper treatment of sensitive information.

Confidentiality

The laboratory takes confidentiality seriously. There are a number of rigorous safeguards in current protocols to protect sensitive information including suspect and victim identification and to whom disclosures of such data can be made. Indeed, not only does laboratory policy dictate proper regard for confidentiality, but professional ethics codes to which all staff adhere and the laboratory's accreditation agency also mandate it. Lastly, if there were to be lapses in the disclosure of this confidential information, eligibility to use CODIS would be suspended and criminal prosecutions against laboratory personnel could occur.

Biometric Methods

The laboratory has four operational units: Drug Analysis, Firearms, Forensic Biology (DNA) and Latent Prints. Only the Forensic Biology and Latent Print Units employ biometric methods. Since the laboratory's inception, comparisons have been performed including latent print analysis. Early in the laboratory's history, serological methods were developed, published and used in casework. Jan Bashinski herself published methods before she went on to found the California Department of Justice's DNA Laboratory in Richmond. In the late 1990s with advancements in DNA sequencing, the OPD laboratory put PCR (Polymerase Chain Reaction) methods into use. Unless a suspect was known and a reference sample collected, the benefits DNA analysis provided investigators were limited. Only upon the introduction of the CODIS database in the mid-1990s did cases in which no suspect was developed become solvable. One example of this is a cold case of the brutal murder of Betty Elias in Oakland in 1979, recently showcased on the Paula Zahn show, in which OPDs work in 2015 led to a CODIS hit to a complete stranger to Ms. Elias. The suspect also left a bloody fingerprint which the OPD laboratory found to include the suspect. The power and importance of each of these biometric analyses are thus illustrated.

Exclusions to Surveillance Ordinance

Notwithstanding the long history of the use of biometrics by the OPD Criminalistics Laboratory, the laboratory has used biometric information properly and to good effect. As an accredited laboratory since 1983, use of appropriate methods in line with industry standards have been followed and sensitive information has been safeguarded. As such, it is the request of the Oakland Police Department Criminalistics Laboratory to have the Surveillance Ordinance specifically exclude instrumentation, reagents, standards and pieces of equipment currently in use by the laboratory for the current scope of methods. A primer on the methods currently in use follows and a specific list of exclusions is attached.

Developing A DNA Profile from Evidence Samples

1. Screening

Purpose: To find potential body fluids, we use visual and chemical screening methods.

Current Technologies:

Alternative light source to find potential bodily fluids: Crime-Scope, TracER Laser, Crime-Lite 2

Stereoscopic microscope to examine fingernails, hairs, etc.: Keyence microscope with camera and scale

Compound microscope to examine cells such as sperm: Zeiss AxioLab microscope with HD digital camera

Current Chemistries:

Detection or identification of semen or sperm: acid phosphatase spot test reagent, Christmas tree staining reagents, SERATEC p30 Semiquant Assay

Detection or identification of blood: Phenolphthalin reagent, ortho-tolidine reagent, hydrogen peroxide, SERATEC HemDirect

Detection or identification of saliva: Amylase radial diffusion assay

2. Digestion Cells and Extraction of DNA

Purpose: The digestion process break open cells and releases the DNA into solution. The extraction process purifies the DNA and removes all the extra cellular material.

Current Technologies:

Incubator to bring the sample to appropriate temperatures: Eppendorf Thermomixer

Centrifuge to spin samples down: Hermle

Multi-channel liquid handling robot for biological material digestion: Versa 1100 instrument

Multi-channel extraction robot that purifies the DNA: QIAgen EZ1 Advanced XL

Current Chemistries:

Reagents for Digestion process: Casework Direct, Qiagen MTL Buffer, Phosphate Buffered Saline, Tween Buffer, Qiagen G2 Buffer, Proteinase K, Dithiothreitol, DNase I, $CaCl_2$ and $MgCl_2$ solution, EDTA, TE

Reagents for Extraction process: Casework Direct, Qiagen EZ1 Investigator Kits

3. Quantitation of DNA

Purpose: To determine the amount of DNA recovered from a sample. If not enough DNA is present, the sample may stop at this point. If a low amount of DNA is present, the sample may be concentrated and subjected to DNA typing. If too much DNA is present, the sample may be diluted before being subjected to DNA typing.

Current Technologies:

DNA Concentrator to concentrate the DNA: SpeedVac Concentrator instrument

Liquid handling robot to prepare the quantitation plate: QIAgility instrument

Real-time PCR instrument and software for DNA quantitation: ABI 7500 instrument, 7500 SDS Analysis software, PowerQuant Analysis Tool (Excel workbook program)

Current Chemistries:

Quantitation chemistry kits for reaction: PowerQuant System, PowerQuant Calibration Kit

4. Amplification of DNA

Purpose: The Polymerase Chain Reaction (PCR) is used for the amplification of regions of DNA of forensic interest. These regions of interest (DNA fragments) are highly variable allowing us to be able to differential individuals.

Current Technologies:

Liquid handling robot to prepare the amplification plate: QIAgility instrument

PCR instrument to perform the amplification process: ABI ProFlex Thermal Cycler instrument

Current Chemistries:

Typing kit which contains reagents for amplification reaction: PowerPlex Fusion 6C system

5. DNA Typing

Purpose: The separation of PCR product (DNA typing) is performed to allow us to determine the quality and quantity of each DNA fragment. The DNA fragments are tagged with a fluorescent dye during the amplification process. The genetic analyzer separates the DNA fragments based on size, smaller fragments travel faster than larger fragments. As the DNA fragments passes through the detection window, a laser excites the fluorescent tags which gives off a signal captured by the software. This allows us to determine the fragment size and quantity of the fragment. The data is then analyzed with genotyping software and interpreted by the scientist.

Current Technologies:

Liquid handling robot to prepare the sample plate: QIAgility instrument

Genetic Analyzer instrument to perform the separation of DNA fragments: ABI 3130 Genetic Analyzer, ABI 3500 Genetic Analyzer

Analysis software: Genetic analyzer data collection software, GeneMapper ID-X software, ArmedXpert software

Current Chemistries:

Genetic Analyzer reagents used for the separation of DNA fragments: PowerPlex 6C Matrix Standards, POP-4 polymer, analysis buffer, capillary array

6. Entry into CODIS

Purpose: DNA profiles obtained from evidence items which meet the eligibility requirements may be entered into the Combined DNA Index System (CODIS). CODIS is a computer-based software system consisting of various indexes of qualified DNA profiles which can be searched against each other ultimately aiding investigations.

Current Technologies:

CODIS Server computer

CODIS Workstation computer

Developing Ridge Detail from Latent Print Evidence Samples

1. Screening

Purpose: To determine from potential areas of evidence whether prints with ridge detail are present. Both visual and chemical processing methods may be used. Latent Prints are not visible to the naked eye; Patent and Plastic Prints are those left in a medium observable with the naked eye.

Current Technologies:

Magnifier to enlarge potential images in areas of interest

Alternative light source to find potential prints: Crime-Scope, TracER Laser, Crime-Lite 2, Foster and Freeman halogen fiber optic

Stereoscopic microscope to examine evidence: Keyence microscope with camera and scale

Current Chemistries (representative, not exhaustive of methods used at crime scenes):

Black Powder
Bichromatic powder
Cyanoacrylate
Fluorescent / Magnetic Powder

2. Processing (not used for every case)

Purpose: To enhance aspects of Latent Prints to provide ridge detail to be used for comparisons. On occasion, a case will not have prints obvious to the human eye, which upon chemical treatment, develops ridge detail from the sweat, oils and chemicals left in the fingerprint.

Current Technologies:

ESDA equipment with reagents to develop indentations

Fuming Chamber to chemically develop prints on all surfaces in contact with the atmosphere

Copy Stand assists to manipulate surfaces to develop prints

Current Chemistries (representative, not exhaustive for development of prints on different surfaces in the laboratory):

Amido Black
Black Wetwop
DFO
Gentian Violet
Leuco Crystal Violet
Naphthol Blue Black
Ninhydrin
Rhodamine
Sudan Black

3. Comparison

Purpose: To assess whether an evidentiary print (questioned) can be included or excluded from a set of reference prints obtained from a specific individual (known). The act of comparison in this laboratory follows the ACE-V method (Analysis/Comparison/Evaluation – Verification) in which the questioned print is analyzed before comparison to the known and a separate verifier conducts an independent analysis all to reduce bias.

Current Technologies:

Measurement Standard to perform calibration check of scanned images

Monitor device used to assess and analyze prints for ridge detail

Pen and Tablet suitable way to mark prints for analysis

Scanner primary means to archive prints for analysis

ADAMS software for image analysis
Foray image storage, assessment and backup system
Image Software Adobe Photoshop for images

4. Entry into AFIS or other databases

Purpose: Latent Prints determined to be of sufficient quality to be suitable for comparison are obtained from evidence items. These prints may be entered into Automated Fingerprint Identification System (AFIS). AFIS is a computer-based software system consisting of Fingerprints from individuals which can be searched against each other to aid investigations.

Current Technologies:

AFIS Server computer
AFIS Workstation computer
Universal Latent Workstation
External Drives

Attachment 1: Certificate and Scope of Accreditation

To provide the Privacy Commission with an awareness of the exemptions being sought, the current scope of accreditation is provided in order to show the laboratory capabilities that are accredited.

Note: In June 2020 the laboratory underwent a successful assessment and new rules of the accreditation agency (ANAB) require a re-draft of the scope. The new document has not been issued but will be in the next few months. It will have a different look and feel, but the areas of accreditation will remain the same. All scopes of accreditation are published online and are publicly available. The Laboratory can supply the new scope upon request.

Attachment 2: List of Specific Items to be excluded from the Surveillance Ordinance

The laboratory maintains multiple lists of thousands of items that are procured in order to accomplish, maintain and support all forensic work in each of the four disciplines of Drug Analysis, Firearms, Forensic Biology and Latent Prints. These lists were narrowed down to only those items relevant to DNA and Latent Prints which are the only units working to develop biometric information. The list of all DNA and Latent Print items is 824. The list of items relevant to the development of biometric data requested to be excluded is 207.

The attached Excel Spreadsheet itemizes the specific current instrumentation, reagents, standards and equipment to be excluded in the Surveillance Ordinance.

The request by the Laboratory is also that when replacing like for like instrumentation, reagents, standards and equipment that support our current methodologies being improved, or due to changes necessitated to become compliant with Federal requirements, that these items also be excluded.

Were entirely new methodology to be put online, these would not automatically be excluded and a conversation with the Privacy Commission would ensue. The decision point for this conversation would be obvious to laboratory management since new methodology would require the laboratory to seek permission from the Accreditation agency to expand the current scope of accreditation. Were this to occur, the Privacy Commission would also be involved.

Reporting

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 is to solve crimes that have already occurred (retrospectively).

Annually, the number of cases that were analyzed using DNA analytical supplies, reagents, standards and instrumentation will be reported to the Privacy Commission. The report will also indicate like-for-like and federally-mandated improvements the laboratory made to existing technology. Any additional biometric capacities added by the laboratory in the reporting year will have been approved by the Privacy Commission in advance and will be restated in the Annual Report. An updated list of exempted items will be provided with the report.

CITY OF OAKLAND

AGENDA REPORT

TO:	Edward Reiskin City Administrator	**FROM:**	Susan E. Manheimer Interim Chief of Police
SUBJECT:	OPD 2020 DNA Backlog Reduction Program	**DATE**:	August 26, 2020

RECOMMENDATION

Staff Recommends That The City Council Adopt In Advance of Formal Award A Resolution Authorizing The City Administrator, Or Designee, To: 1) Accept And Appropriate Grant Funds In An Amount Not To Exceed $369,460 From The U.S. Department Of Justice (DOJ), Office of Justice Programs (OJP), Bureau of Justice Assistance (BJA) For Implementation Of The FY (Fiscal Year) 2020 DNA Capacity Enhancement For Backlog Reduction Program For The Oakland Police Department (OPD); And 2) Waive The City Advertising And Competitive Bidding Requirements For The Purchases Of DNA Typing Supplies and Instruments From (1) Qiagen For One Hundred Seventy-Five Thousand One Hundred Twenty Dollars ($175,120), (2) Promega For One Hundred Fifty-Seven Thousand and Forty Dollars ($157,040), And (3) Thermo Fisher/Life Technologies For Nineteen Thousand Ninety-Six Dollars ($19,096).

EXECUTIVE SUMMARY

Adoption of this resolution in advance of formal award will allow OPD to accept the BJA FY 2020 DNA Capacity Enhancement and Backlog Reduction (CEBR) grant of $369,460 in a timely manner thus expediting funds for staff training and DNA processing without potential delay of casework. The OPD Crime Laboratory (Crime Lab), with these grant funds, will be able to decrease the biological evidence analysis turnaround time and the backlog of cases. This resolution calls for waiving the City's Advertising and Competitive Bidding Requirements because of the need to buy specialized laboratory-validated DNA typing equipment, reagents, and supplies available only from specific vendors.

BACKGROUND AND LEGISLATIVE HISTORY

The DNA Capacity Enhancement for Backlog Reduction Program is a formula grant created by the U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance (DOJ/OJP/BJA) to assist laboratories that conduct DNA analysis. The aggregate amount of FY 2020 funds expected to be awarded to eligible applicants from each State was based on a determination by the Bureau of Justice Assistance (BJA) of a primary and a secondary amount, and then distributed among the eligible applicants within the State. The total (primary and secondary) amount available for California as indicated in the FY 2020 grant solicitation formula

is $9,828,035, of which $369,460 is allocated to Oakland Police Department. OPD is anticipating a formal award letter by December 2020.

The goal of the program is to improve DNA laboratory infrastructure and analysis capacity so that DNA samples can be processed efficiently and effectively. The program also provides continuing education courses and training associated with DNA analyses required by the Federal Bureau of Investigation (FBI) DNA Quality Assurance Standards (QAS) mandatory education and training requirements, as well as funds to analyze backlogged forensic DNA casework samples. Improvements are necessary and critical to reduce current DNA backlogs, prevent future increases and to help the criminal justice system reach its full potential in the utilization of DNA technology.

Backlogged case requests from homicides, sexual assaults, robberies, assaults, and property crime cases will be enrolled into the FY 2020 DNA Backlog Reduction Program. The eligible DNA profiles obtained from evidence in these cases will be entered into the Combined DNA Index System (CODIS). DNA profiles entered into CODIS has resulted in an approximately seventy-three percent hit rate.[1] This will assist not only Oakland Police Department investigators, but also the Alameda County District Attorney, and other law enforcement, prosecutorial, and judicial agencies in the surrounding area.

ANALYSIS AND POLICY ALTERNATIVES

The Crime Lab will focus on three goals with the implementation of the FY 2020 DNA Backlog Reduction Program grant initiative:

Goal #1: Reduce the Average Turnaround Time

The analysis of the backlogged cases will include case evaluation, biological evidence examination and screening, DNA typing, technical review, and data entry into CODIS. A minimum of 239 backlogged case requests will be analyzed using grant funds for DNA typing reagents and supplies. The supplies will include capillaries and associated polymer for the instruments, DNA extraction kits, quantitation kits, and typing kits. These readily available supplies will alleviate the time waiting for supplies to arrive at the Laboratory, thus reducing the turnaround time. Other laboratory funds will be used to purchase consumable supplies such as gloves, masks, scalpels, and plastic-ware.

Goal #2: Provide Required Continuing Education for Each Criminalist and Forensic DNA Technician

The Criminalistics Division must comply with several types of credentialing processes:

- ANSI-ASQ National Accreditation Board accreditation (ANAB)
- National DNA Index System (NDIS) requirements for CODIS data entry
- American Board of Criminalistics certification educational requirements

[1] "Hit rate" is defined as that portion of cases with DNA profiles submitted to CODIS in which an association to a named individual or case-to-case (either solved or unsolved) is made to a DNA profile(s) in the database during the last 18 months.

- Federal Bureau of Investigation (FBI) DNA Quality Assurance Standards (QAS) mandatory education and training requirements

To comply with and maintain the Criminalistics Division's required accreditations, scientific staff must obtain continuing education credits. The Criminalistics Division and Forensic Biology Unit do not have independent budgets for training. This federal grant will fund travel and tuition for various conferences and training opportunities. It is anticipated that case completion time would improve, because of conference attendance, and training of Forensic Biology Unit staff may result in implementation of new technologies learned. By the end of the award period, it is expected that the Forensic Biology Unit Criminalists will have fulfilled a portion of their required continuing education through this grant.

Goal #3: Increase Capacity of the Crime Lab for Forensic Casework

The Crime Laboratory will use the grant funds to purchase two EZ2 DNA purification instruments. These instruments will replace two older model, lower capacity, EZ1 DNA purification instruments. Our current model capacity is 14 samples per run, the newer replacement model capacity is 24 samples per run. Thus, replacing the older model EZ DNA purification instrument will increase the capacity of conducting DNA typing on case samples.

Waiver of the Advertising and Bidding Process

Section 2.04.050.1.5 (Bid Procedure) explains that the City can make exceptions to its competitive bidding process when City Council finds and determines that it is in the best interest of the City. Purchasing DNA supplies and typing instruments from vendors other than those who manufacture DNA kits and instruments used by the Crime Laboratory would not be acceptable for this federal grant. The Forensic Biology Unit has conducted extensive validation studies as part of the selection process in determining which typing kits and instruments to implement in our evidence processing scheme. The use of other products which have not been validated would hence violate the FBI DNA QAS; OPD therefore believes that waiving the competitive bidding process in this instance is in the best interest of the City. The Crime Lab must adhere to FBI DNA QAS standards to enter DNA profiles into CODIS for searching. The reagents to be purchased through this grant include: DNA extraction kits and DNA purification instruments (Qiagen), DNA quantitation kits (Promega), DNA typing kits (Promega), DNA typing supplies (Thermo Fisher/Life Technologies). These reagents and instruments from these specific vendors have undergone rigorous validation studies and no vendor substitutions are acceptable.

FISCAL IMPACT

The table below details how OPD will utilize the USDOJ/NIJ FY 2020 DNA Backlog Reduction Grant Program funds. The table lists the use of funding for staff travel and training, and technology and supply costs.

Budget Category	**Amount**
Instrument	
DNA Purification Instruments (Qiagen)	$112,000
Total Instruments	**$112,000**

Training and Travel	
Travel, Lodging, and Registration Costs	$18,204
Total Training and Travel	**$18,204**
Technology and Supplies	
DNA Typing Reagents and Supplies (Qiagen)	$63,120
DNA Typing Reagents and Supplies (Promega)	$157,040
DNA Typing Reagents and Supplies (Thermo Fisher/Life Technologies)	$19,096
Total Technology and Supplies	**$239,256**
TOTAL	**$369,460**

The $369,460 in grant funds from the USDOJ/NIJ for the implementation of the FY 2020 DNA Backlog Reduction Grant Program shall be appropriated in the Federal Grant Fund (2112), Criminalistics Division Organization (102610), Criminalistics Division Program (PS05), in a Project Number to be established.

Fiscal Year	Fund Source	Organization	Account	Project	Program	Amount
2020-2021	2112	102610	TBD	TBD	PS05	$369,460

PUBLIC OUTREACH / INTEREST

The public has a significant interest in ensuring that the OPD Crime Laboratory can effectively process DNA evidence; successfully processed DNA evidence helps OPD with investigations by either rejecting individuals excluded by the evidence or leads to effective criminal prosecutions.

COORDINATION

The Budget Bureau and the Office of the City Attorney were consulted by OPD on the production of this report as well as the accompanying resolution.

SUSTAINABLE OPPORTUNITIES

Economic*:* There are no economic opportunities associated with this report.

Environmental*:* There are no environmental opportunities associated with this report.

Race and Social Equity*:* Provisions for continuing education and supplies funded by this grant will enhance OPD's ability to analyze biological evidence in criminal cases in a timelier fashion. The public safety for all Oakland residents and visitors is enhanced through greater OPD investigative capacity, through the use of science-based methods which mitigates potential bias.

ACTION REQUESTED OF THE CITY COUNCIL

Staff Recommends That The City Council Adopt A Resolution Authorizing The City Administrator, Or Designee, To: 1) Accept And Appropriate Grant Funds In An Amount Not To Exceed $369,460 From The U.S. Department Of Justice, National Institute Of Justice (USDOJ/NIJ) For Implementation Of The FY (Fiscal Year) 2020 DNA (Deoxyribonucleic Acid) Capacity Enhancement For Backlog Reduction Program For The Oakland Police Department (OPD); And 2) Waive The City Advertising And Competitive Bidding Requirements For The Purchases Of DNA Typing Supplies and Instruments From (1) Qiagen For One Hundred Seventy-Five Thousand One Hundred Twenty Dollars ($175,120), (2) Promega For One Hundred Fifty-Seven Thousand and Forty Dollars ($157,040), And (3) Thermo Fisher/Life Technologies For Nineteen Thousand Ninety-Six Dollars ($19,096) For DNA Typing Supplies and Instruments.

For questions regarding this report, please contact Bonnie Cheng, Criminalist II, at (510) 238-3386.

Respectfully submitted,

Susan E. Manheimer
Interim Chief of Police
Oakland Police Department

Reviewed by:
Sandra Sachs, Crime Laboratory Manager,
OPD, Criminalistics Division

Prepared by:
Bonnie Cheng, Criminalist II
OPD, Criminalistics Division

Bruce Stoffmacher, Legislation Manager
OPD, Research and Planning, Office of the Chief

Approved as to Form and Legality

_____
City Attorney

OAKLAND CITY COUNCIL

RESOLUTION NO._____C.M.S.

Introduced by Councilmember _____

RESOLUTION: 1) AUTHORIZING THE CITY ADMINISTRATOR, OR DESIGNEE, TO ACCEPT IN ADVANCE OF FORMAL AWARD AND APPROPRIATE GRANT FUNDS IN AN AMOUNT NOT TO EXCEED THREE HUNDRED SIXTY-NINE THOUSAND FOUR HUNDRED SIXTY DOLLARS ($369,460) FROM THE U.S. DEPARTMENT OF JUSTICE (DOJ), OFFICE OF JUSTICE PROGRAMS (OJP), BUREAU OF JUSTICE ASSISTANCE (BIJ) FOR IMPLEMENTATION OF THE FISCAL YEAR 2020 DNA CAPACITY ENHANCEMENT FOR BACKLOG REDUCTION (CEBR) GRANT PROGRAM FOR THE OAKLAND POLICE DEPARTMENT; 2) WAIVE THE ADVERTISING AND COMPETITIVE BIDDING REQUIREMENTS FOR THE PURCHASE OF DNA TYPING SUPPLIES AND INSTRUMENTS FROM (1) QIAGEN FOR ONE HUNDRED SEVENTY-FIVE THOUSAND ONE HUNDRED TWENTY DOLLARS ($175,120), (2) PROMEGA FOR ONE HUNDRED FIFTY-SEVEN THOUSAND AND FORTY DOLLARS ($157,040), AND (3) THERMO FISHER/LIFE TECHNOLOGIES FOR NINETEEN THOUSAND NINETY-SIX DOLLARS ($19,096).

WHEREAS, the advent of Deoxyribonucleic Acid (DNA) technology and automation equipment has revolutionized law enforcement's ability to analyze biological evidence at a genetic level; and

WHEREAS, the DNA Capacity Enhancement for Backlog Reduction Program was created by the U.S. Department of Justice, Office of Justice Program, Bureau of Justice Assistance (DOJ/OJP/BIJ) to assist laboratories that conduct DNA analysis with a goal of improving DNA laboratory infrastructure and analysis capacity so that DNA samples can be processed efficiently and effectively; and

WHEREAS, grant funds in an amount not to exceed $369,460, when awarded by DOJ/OJP/BIJ to the Oakland Police Department (OPD) will be applied to Fiscal Year 2020 implementation of the DNA Capacity Enhancement for Backlog Reduction Program; and

WHEREAS, the DNA Capacity Enhancement for Backlog Reduction Program was created to assist laboratories in increasing DNA typing capacity and reducing the number of cases in their backlog in which DNA analyses may be conducted on

biological evidence; and

WHEREAS, the funds will be allocated to purchase DNA purification instruments, staff required training, and purchase laboratory-validated DNA typing reagents and supplies; and

WHEREAS, the OPD Criminalistics Division must use and maintain rigorously validated DNA typing reagents and instruments from specific vendors because purchasing DNA supplies from vendors other than those who manufacture DNA kits or instruments not currently used by the crime lab would not be acceptable as the OPD Forensic Biology Unit has not validated their use and hence would violate the Federal Bureau of Investigation (FBI) DNA Quality Assurance Standards (QAS); and

WHEREAS, Oakland Municipal Code (OMC) Section 2.04.050.1.5 authorizes the City Council to waive the advertising and competitive bidding requirements of OMC Section 2.04.050 after finding and determining that it is in the best interests of the City to do so; and

WHEREAS, the grant term for the proposed initiative is January 1, 2021 through December 31, 2022; and

WHEREAS, the City Council previously authorized acceptance of similar grant funds by Resolution No. 87996 C.M.S., dated January 21, 2020, Resolution No. 87429 C.M.S., dated November 1, 2018, Resolution No. 87428 C.M.S., dated September 27, 2018, Resolution No. 86982 C.M.S., dated November 2, 2017, Resolution No. 86532 C.M.S., dated November 22, 2016,Resolution No. 85899 C.M.S., dated November 17, 2015, Resolution No. 85223 C.M.S., dated October 21, 2014, Resolution No. 84686 C.M.S., dated November 5, 2013, Resolution No. 84041 C.M.S., dated October 2, 2012; Resolution No. 83672 C.M.S., dated December 15, 2011; Resolution No. 83030 C.M.S., dated October 19, 2010; Resolution No. 82291 C.M.S., dated September 22, 2009; Resolution No. 81624 C.M.S., dated October 21, 2008; Resolution No.80869 C.M.S., dated October 2, 2007; Resolution No. 80129 C.M.S., dated September 19, 2006; Resolution No. 79534 C.M.S., dated October 18, 2005 and Resolution No. 78909 C.M.S., dated November 16, 2004; and

WHEREAS, staff recommends that the City Council make a finding and a determination that it is in the best interests of the City to waive advertising and bidding processes because purchasing DNA supplies and instruments from vendors other than those who manufacture DNA kits and instruments currently used by the Crime Laboratory would not be effective as other DNA supplies and instruments from other vendors have not been validated for use; now, therefore be it

RESOLVED: That the City Council hereby authorizes the City Administrator, or designee, to accept and appropriate grant funds in an amount not to exceed $369,460 from the DOJ/OJP/BIJ and to increase revenues and appropriate said budget to OPD; and be it

FURTHER RESOLVED: That said grant funds, in an amount not to exceed $369,460, shall be appropriated in the Federal Grant Fund (2112), Criminalistics Division Org. (102610), Criminalistics Division Program (PS05), in a Project Number to be established; and be it

FURTHER RESOLVED: That said grant funds shall be used purchase two DNA purification instruments; and be it

FURTHER RESOLVED: That said grant funds shall be used to fund DNA training courses, and purchase laboratory-validated DNA typing reagents utilized in the examination of biological material; and be it

FURTHER RESOLVED: That the City Council finds and determines that pursuant to OMC Section 2.04.050.1.5 and based upon the reasons stated above and in the City Administrator's report accompanying this resolution, that it is in the best interests of the City to waive the advertising and competitive bidding requirements of the OMC for the purchases of DNA purification instruments for $112,000 from Qiagen, and DNA typing supplies from Qiagen for $63,120, Promega for $157,040; and Thermo Fisher/Life Technologies for $19,096, and be it

FURTHER RESOLVED: That the City Administrator, or designee, is hereby authorized to complete all required negotiations, certifications, assurances, agreements and documentation required to accept, modify, extend and/or amend the grant award; and be it

FURTHER RESOLVED: That any agreement authorized by this resolution shall be reviewed and approved by the Office of the City Attorney for form and legality prior to execution, and a copy shall be placed on file with the City Clerk.

IN COUNCIL, OAKLAND, CALIFORNIA, _____

PASSED BY THE FOLLOWING VOTE:

AYES – BAS, GALLO, GIBSON MCELHANEY, KALB, REID, TAYLOR, THAO, and PRESIDENT KAPLAN

NOES -

ABSENT -

ABSTENTION -

ATTEST: _____
LaTonda Simmons
City Clerk and Clerk of the Council
of the City of Oakland, California

CITY OF OAKLAND

AGENDA REPORT

TO:	Edward D. Reiskin City Administrator	**FROM:**	Susan E Manheimer Interim Chief of Police
SUBJECT:	CA DOJ Sexual Assault Evidence Testing Grant	**DATE:**	August 28, 2020

City Administrator Approval Date:

RECOMMENDATION

Staff Recommends That The City Council Adopt A Resolution Authorizing The City Administrator Or Designee To: 1) Enter Into A Memorandum Of Understanding (MOU) With The California Department Of Justice (CA DOJ) Bureau Of Forensic Services; 2) Accept And Appropriate One Hundred Fifty-Three Thousand Six Hundred Twenty-Seven Dollars ($153,627) In Untested Sexual Assault Evidence Grant Program Funds, To Process Untested Sexual Assault Evidence Kits In OPD's Inventory; and 3) Authorize the City's General Purpose Fund to Support the Associated Central Services Overhead Costs.

EXECUTIVE SUMMARY

Adoption of the resolution accompanying this report will allow OPD and CA DOJ to enter into a MOU and receive a grant in the amount of $153,627. The grant term is July 1, 2020 – June 30, 2022. Funding will be used to process approximately 97 untested sexual assault evidence kits in OPD's inventory that have been identified for testing. All funding will be spent on salary and overtime (Property and Evidence (PEU), Special Victim's Unit (SVU), and Criminalistics Laboratory (Lab) staff), and to purchase testing kits, reagents and supplies to complete the work.

BACKGROUND / LEGISLATIVE HISTORY

In 2018, the CA DOJ Bureau of Forensic Services Untested Sexual Assault Evidence Grant program (Audit Grant) was developed to assist county and city agencies to compile the number of untested sexual assault evidence kits statewide. The grant was supported by funds allocated with the passage of SB 862 (Cal. Stats. 2018, ch. 449), which appropriated $1 million to CA DOJ for grants to counties and cities, to count the number of untested sexual assault evidence kits in their possession. It was intended to support the requirements outlined in Assembly Bill 3118 (Chiu, 2018). These funds were available for Fiscal Year 2018-19, with a grant period beginning January 1, 2019 and ending June 30, 2019. The grant had an award formula, and

Alameda County was allocated $38,865.86. OPD applied for and received $38,088 of those funds to count untested sexual assault kits in its possession prior to October 1, 2018.

This year's testing grant is supported by funds allocated with the passage of the State of California Budget Act of 2019 (0820-101-0001), which appropriated $2 million to CA DOJ to award local law enforcement grants. These 2019-20 funds are available with a grant period ending June 30, 2022. Since agencies were encouraged to apply for amounts based on need, OPD applied for a total of $272,734 to purchase and process supplies to test 169 kits using overtime; a grant aware of $153,627 however was approved by CA DOJ - 45 percent less than anticipated. OPD hopes to test and process 97 evidence kits with these grant funds.

ANALYSIS AND POLICY ALTERNATIVES

To meet the June 30, 2022 grant project deadline, OPD needs to use current Property and Evidence (PEU), Special Victim's Unit (SVU), and Criminalistics Laboratory (LAB) staff to conduct the work. Each of these units is challenged by understaffing; staff will need to lengthen their shifts or add days of work to accommodate their current workload in addition this additional project. Funding will therefore be used to cover regular salary and overtime for Lab, PEU and SVU staff, as well as to purchase the 97 sexual assault evidence testing kits, reagents and supplies. OPD is also required to submit a final report to CA DOJ.

FISCAL IMPACT

The budget for this grant allocates funds across three units of the department: PEU, SVU, and Lab. Tables 1.1, 1.2, 1.3, and 1.4 below outline OPD personnel spending plan for the Untested Sexual Assault Evidence Grant Program Funds. Tables 2 and 3 outline the equipment purchases and summarize total grant spending plans.

Table 1.1: Use of CA DOJ Grant Funds for Crime Lab Personnel Costs

Salary Expense	**Amount**
Reg Salary for Forensic Tech (LAB) – 171.32 hours @ $39.43/hr	$6,755
Reg Salary for Criminalist I (LAB) – 171.32 hours at $48.77/hr	$8,355
Reg Salary for Criminalist II (LAB) – 342.66 hours at $54.45/hr	$18,658
Reg Salary for Criminalist III (LAB) – 57.11 hours at $60.69/hr	$3,466
OT for Forensic Tech (LAB) – 57.11 hours @ $59.15/hr	$3,378
OT for Criminalist I (LAB) – 57.11 hours at $71.00/hr	$4,055
OT for Criminalist II (LAB) – 114.22 hours at $78.68/hr	$8,987
OT for Criminalist III (LAB) – 28.56 hours at $91.04/hr	$2,600
Total Crime Lab Personnel Cost	**$56,254**

Table 1.2: Use of CA DOJ Grant Funds for Crime PEU Personnel Costs

OT for Police Property Specialist (PEU) – 45.70 hours at $47.42/hr	$2167
OT for Police Property Supervisor (PEU) – 22.85 hours at $61.62/hr	$1408
TOTAL	**$3,575**

Table 1.3: Use of CA DOJ Grant Funds for Crime SVU Personnel Costs

OT for Police Officer (SVU) – 34.27 hours at $91.43/hr	$3,133
OT for Police Sergeant (SVU) – 22.84 hours at $105.49/hr	$2,409
OT for Police Lieutenant (SVU) – 11.42 hours at $122.01/hr	$1,393
TOTAL	**$6,935**

Table 2: Use of CA DOJ Grant Funds for Crime Lab Equipment

Use of Funds	**Amount**
Sexual Assault Kits for DNA extraction, quantitation, and/or amplification – 97 kits @ $900/kit	**$86,863**

Commented [BS1]: This is $87,300 – are kits actually $895.50?

Total grant award:

Use of Funds	**Amount**
Personnel Costs: Salary and OT	$66,764
Supply Cost: Sexual Assault Evidence Kits	$86,863
TOTAL	**$153,627**

Funds will be allocated in the State of California Fund (2159); Criminalistics Organization (102610), Special Victims Organization (102130), and Property and Evidence Organization (102120); in the Project to be determined. Based on the City's Central Services Overhead (CSO) rates of 15.5%, overhead charges associated with the grant's personnel costs will be approximately $10,349. However, per the granting agency, indirect costs such as CSO charges are disallowed; staff therefore requests the City's General Purpose Fund contribute $10,349 to cover the CSO charges.

PUBLIC OUTREACH / INTEREST

Commented [GM2]: Do we include Privacy Commission here?

No public outreach was required beyond the standard City Council noticing requirements. This report was also presented to the City's Privacy Advisory Commission.

COORDINATION

This report and legislation have been reviewed by the Office of the City Attorney and the Budget Bureau.

SUSTAINABLE OPPORTUNITIES

Economic: There are no economic opportunities identified in this report

Environmental*:* There are no environmental opportunities identified in this report.

Race and Social Equity*:* The activities completed under this grant will position OPD to respond to a state mandate to test historical sexual assault exam kits which remain untested. It should be noted that the Lab's Contemporary Kit Program vets and analyzes all current Sexual Assault Kits well within the 120-day mandate set by the State of California – this timeline benefits current and future Oakland residents and visitors who are victims of sexual violence by giving potential investigative leads as quickly as possible. Examining historical kits may give closure to previous victims of sexual violence.

ACTION REQUESTED OF THE CITY COUNCIL

Staff Recommends That The City Council Adopt A Resolution Authorizing The City Administrator Or Designee To: 1) Enter Into A Memorandum Of Understanding (MOU) With The California Department Of Justice (CA DOJ) Bureau Of Forensic Services; 2) Accept And Appropriate One Hundred Fifty-Three Thousand Six Hundred Twenty-Seven Dollars ($153,627) In Untested Sexual Assault Evidence Grant Program Funds, To Process Untested Sexual Assault Evidence Kits In OPD's Inventory; and 3) Authorize the City's General Purpose Fund to Support the Associated Central Services Overhead Costs.

For questions concerning this report, please contact Dr. Sandra Sachs at 510-238-2108.

Respectfully submitted,

Susan E. Manheimer
Interim Chief of Police
Oakland Police Department

Reviewed by:
Shamika Shavies, Fiscal Services Manager
OPD, Fiscal Services Division

Bruce Stoffmacher, Management Assistant
OPD, Research and Planning, Training Division

Sandra Sachs, Criminalistics Laboratory Manager
OPD, Criminalistics Division

Prepared by:
Molly Giesen-Fields, Grants Coordinator
OPD, Fiscal Services Division

Approved as to Form and Legality

_____
City Attorney

OAKLAND CITY COUNCIL

RESOLUTION NO._____C.M.S.

RESOLUTION AUTHORIZING THE CITY ADMINISTRATOR OR DESIGNEE TO: 1) ENTER INTO A MEMORANDUM OF UNDERSTANDING (MOU) WITH THE CALIFORNIA DEPARTMENT OF JUSTICE (CA DOJ) BUREAU OF FORENSIC SERVICES; 2) ACCEPT AND APPROPRIATE ONE HUNDRED FIFTY-THREE THOUSAND SIX HUNDRED TWENTY-SEVEN DOLLARS ($153,627) IN UNTESTED SEXUAL ASSAULT EVIDENCE GRANT PROGRAM FUNDS, TO PROCESS UNTESTED SEXUAL ASSAULT EVIDENCE KITS IN OPD'S INVENTORY; AND 3) AUTHORIZE THE CITY'S GENERAL PURPOSE FUND TO SUPPORT THE ASSOCIATED CENTRAL SERVICES OVERHEAD COSTS.

WHEREAS, the CA DOJ Bureau of Forensic Services Untested Sexual Assault Evidence Grant program (Testing Grant) is designed to assist statewide county and city local law enforcement agencies to test sexual assault forensic evidence, to support the requirements outlined in Assembly Bill 3118 (Chiu, 2018); and

WHEREAS, grant funds totaling one hundred fifty-three thousand six hundred twenty-seven ($153,627) have been awarded by CA DOJ for OPD to cover salary and overtime for staff to complete the sexual assault kit processing work and sexual assault kit testing supplies for approximately 97 kit analyses; and

WHEREAS, the grant award period of performance is July 1, 2020 through June 30, 2022; therefore be it

WHEREAS, Article V, Section 504(l) of the Oakland City Charter requires that the City Council approve all inter-agency relationships such as between OPD and CA JOJ; therefore be it

RESOLVED: That the City Council does hereby authorize the City Administrator or designee to accept and appropriate a grant award in an amount totaling one hundred fifty-three thousand six hundred twenty-seven dollars ($153,627) from the State of California, Department of Justice; and be it

FURTHER RESOLVED: That the grant funds shall be maintained in the State of California Fund (2159); Criminalistics Organization (102610), Special Victims Organization (102130), and Property and Evidence Organization (102120); in the Project to be determined; and be it

FURTHER RESOLVED: That the City Council hereby authorizes the City Administrator or designee to act as an agent to conduct all negotiations and related actions and to sign all applications, agreements and memoranda of understanding that may be necessary for the completion of the aforementioned grant.

FURTHER RESOLVED: That all contracts issued hereunder shall be reviewed and approved by the City Attorney for form and legality and copies shall be placed on file in the City Clerk's Office; and be it

FURTHER RESOLVED: That the City Administrator, or designee, is hereby authorized to complete all required negotiations, certifications, assurances and documentation required to accept, modify, extend and/or amend the agreement.

IN COUNCIL, OAKLAND, CALIFORNIA,

PASSED BY THE FOLLOWING VOTE:

AYES - FORTUNATO BAS, GALLO, GIBSON MCELHANEY, KALB, REID, TAYLOR, THAO AND PRESIDENT KAPLAN

NOES –

ABSENT –

ABSTENTION –

ATTEST:_____
ASHA REED
Acting City Clerk and Acting Clerk of the Council
of the City of Oakland, California

Approved as to Form and Legality

City Attorney

OAKLAND CITY COUNCIL

RESOLUTION NO._____C.M.S.

Introduced by Councilmember _____

RESOLUTION WAIVING THE CITY'S ADVERTISING AND COMPETITIVE BIDDING REQUIREMENTS AND WAIVING THE REQUEST FOR PROPOSALS/QUALIFICATIONS (RFP/Q) PROCESS REQUIREMENTS FOR THE PURCHASE OF CERTIFIED AND ACCREDITED FORENSIC ANALYTICAL SUPPLIES, EQUIPMENT, INSTRUMENTATION, SOFTWARE, AND RELATED SERVICES ON AN AS-NEEDED BASIS WHEN LABORATORY FORENSIC SCIENCE SUBJECT MATTER EXPERTS DETERMINE SUCH SUPPLIES AND / OR SERVICES ARE REQUIRED BASED ON CASEWORK CONDITIONS, THE LABORATORY'S VALIDATION METHODS, OR ITS QUALITY ASSURANCE PROGRAM, OR NEEDED FOR THE TIMELY ANALYSIS OF EVIDENCE, OR WHEN THE MATERIALS OR SERVICES ARE AVAILABLE FROM ONLY ONE SOURCE, IN THE AMOUNT OF UP TO SIX HUNDRED THOUSAND DOLLARS ($600,000) PER FISCAL YEAR THROUGH JUNE 30, 2025, FOR A TOTAL COST NOT TO EXCEED THREE MILLION DOLLARS ($3,000,000)

WHEREAS, the Oakland Police Department's Criminalistics Laboratory (Crime Laboratory) brought to Council on July 28 a resolution for the terms listed above and it was modified to a shorter time period to expire Dec 31, 2020; and

WHEREAS, the Department having brought forth a list of all technology used by the Crime Lab to the Privacy Advisory Commission (PAC) in August 2020 (by the September 2020 deadline) in a list of items proposed to be excluded from the ordinance

OR

WHEREAS, a Use Policy for DNA Analytical supplies will be provided to Privacy by October which includes a template of data to be reported by the Laboratory to the Privacy Commission annually in order to allow the PAC to make a recommendation to the City Council to approve this bid waiver before the end of the calendar year, and

WHEREAS, the Crime Laboratory is a full service forensic science laboratory accredited to ISO/IEC 17025:2017 (ISO) by the American National Standards Institute National

Accreditation Board (ANAB); and

WHEREAS, the Crime Laboratory must adhere to all applicable accreditation standards and requirements to successfully maintain and renew accreditation every four years; and

WHEREAS, ANAB is the largest and most established accrediting body in the United States engaging in the accreditation of forensic science testing laboratories; and

WHEREAS, accreditation is a requirement for eligibility for receipt and use of state and federal grant funds and for access to the state and national databases; and

WHEREAS, the use of validation methods and proficiency testing by ISO 17043 approved providers are requirements of accreditation; and

WHEREAS, the Crime Laboratory has implemented validation methods across all its forensic disciplines; and

WHEREAS, those validated methods specify supplies, instrumentation, and other analytical conditions necessary to produce reliable results; and

WHEREAS, the Crime Laboratory's Forensic Biology Unit is required to adhere to the Federal Bureau of Investigation (FBI) DNA Quality Assurance Standards (QAS) in order to maintain access to the Combined DNA Index System (CODIS);

WHEREAS, the FBI QAS requires the Forensic Biology Unit to use rigorously validated DNA typing methods that use specific quality controlled reagents and instruments from specific vendors;

WHEREAS, ANAB requires the Crime Laboratory to use only suitable external providers of specific supplies, instruments, equipment, instrument service, equipment service, proficiency testing, and evidence collection kits to perform its casework using its validated methods; and

WHEREAS, the Crime Laboratory employs forensic subject matter experts who possess the requisite scientific knowledge to determine which supplies, instruments, and services are most suited to the Laboratory's needs or which are required to successfully analyze evidence in particular cases; and

WHEREAS, subject matter experts may determine that such supplies, instrumentation, instrument services, and related software are specifically required by forensic casework conditions, the laboratory's validated methods, or its quality assurance program, or that the materials are needed for the timely analysis of evidence, or that the materials or services are available from only one source, or that such materials or services cannot be substituted by products from another supplier; and

WHEREAS, subject matter experts anticipate entering agreements with vendors

such as, but not limited to the following: Adorama, Agilent Technologies, Airgas, American Society for Quality, ANSl National Accreditation Board LLC, Artic White LLC, Arrowhead Forensics, Aurora Biomed, Autodesk, Brownells, Cabella's, Cayman Chemicals, Cerilliant Corporation, Cheaper Than Dirt?, Coherent Inc., Collaborative Testing Services Inc., Covanta Inc., CSI Forensic Supply, Environmental Science Research, EVIDENT, Fisher Scientific, Foray Technologies, Forensic Comparison Software Company, Foster + Freeman Ltd, Full Spectrum, Grainger, Leeds Forensic Systems Inc., Leeds Precision Instruments Inc., Leica Geosystems, Life Technologies, Manthei Mess Systeme, Mettler-Toledo Rainin LLC, Midway USA, Perkin-Elmer, Promega Corporation, Qiagen, Niche Vision Forensic LLC, The REMI Group Inc., Rice Lake Weighing Systems Division, Ron Smith and Associates, Safariland, San Diego Police Equipment Co Inc., Security Envelope Company, Serological Research Institute, Sigma Aldrich, Sirchie, Steraloids Inc., Thermo-Fisher, Thomas Scientific, Tri-Tech Inc., Uline, Unity Lab Services, USA Scientific, and VWR; and

WHEREAS, Oakland Municipal Code (OMC) Section 2.04.010 defines formal and informal bidding to include competitive processes (advertising and bidding or solicitation) and for informal bidding to require a minimum of three quotes or responses; and

WHEREAS, OMC Section 2.04.040 D 2 the City Administrator shall institute informal contracting procedures for the purchase of supplies, services or combination; and

WHEREAS, OMC Section 2.04.050.1.5 allows the City Council to waive the advertising and competitive bidding requirements after a finding and determination that it is in the best interests of the City to do so; and

WHEREAS, the City Council waiving the advertising and competitive bidding requirements after a finding and determination that it is in the best interests of the City to do so does not supersede other, non-bidding related ordering requirements elsewhere in the OMC; and

WHEREAS, OMC Section 2.04.051.A allows the City Council to waive the request for proposals/qualifications (RFP/Q) process requirements upon a finding and determination that it is in the best interest of the City to do so; and

WHEREAS, OMC Section 2.04.060 stipulates that in addition to price, a number of other considerations shall be made to determine the lowest responsible bidder including: the quality and performance of the supplies, the ability of the bidder to provide the supplies in a timely manner, the reputation and experience of the bidder and the quality of the bidder's performance on previous purchases; and

WHEREAS, City staff recommends waiving the advertising and competitive bidding requirements, and request for proposals/qualifications requirements because: 1) specific validated laboratory methods often require specific chemicals and reagents from

specific providers, 2) casework situations require the rapid acquisition of specific supplies and materials which may be available from only one source, and 3) it is not possible to anticipate when such casework situations will arise and thus would be very difficult for the Crime Laboratory to seek "sole source" purchasing authority each time such situations occur; and

WHEREAS, the City Administrator has determined that a professional services agreement authorized by this resolution would be of a professional and temporary nature and shall not result in the loss of employment or salary by any person having permanent status in the competitive civil service; and

WHEREAS, the City Council previously authorized on multiple occasions the waiving of advertising and competitive bidding for the purchase of Crime Laboratory related supplies, instrumentation and software under Resolution No. 87996 C.M.S., dated January 21, 2020, Resolution No. 87429 C.M.S., dated November 1, 2018, Resolution No. 87428 C.M.S., dated September 27, 2018, Resolution No. 86982 C.M.S., dated November 2, 2017, Resolution No. 85943 C.M.S., dated January 5, 2016, Resolution No. 86532 C.M.S., dated November 22, 2016, Resolution No. 86529 C.M.S., dated December 13, 2016, Resolution No. 85899 C.M.S., dated November 17, 2015, Resolution No. 85223 C.M.S., dated October 21, 2014, Resolution No. 84686 C.M.S., dated November 5, 2013, Resolution No. 84041 C.M.S., dated October 2, 2012; Resolution No. 83672 C.M.S., dated December 15, 2011; Resolution No. 83030 C.M.S., dated October 19, 2010; Resolution No. 82291 C.M.S., dated September 22, 2009; Resolution No. 81624 C.M.S., dated October 21, 2008; Resolution No. 80869 C.M.S., dated October 2, 2007; Resolution No. 80129 C.M.S., dated September 19, 2006; Resolution No. 79534 C.M.S., dated October 18, 2005 and Resolution No. 78909 C.M.S., dated November 16, 2004; and,

WHEREAS, the Crime Laboratory anticipates the annual need to replenish supplies, instruments, and related services from the listed vendors or required from other sources based on casework needs as determined by forensic subject matter experts at a cost not to exceed $600,000 per fiscal year; and

WHEREAS, the Crime Laboratory anticipates that not extending this bid waiver beyond December 2020 will bring analysis of evidence that requires supplies, reagents, standards to an immediate halt; therefore, be it

RESOLVED: That the City Council finds and determines that pursuant to OMC Sections 2.04.050.1.5 and 2.04.051.B, and based upon the reasons stated above and in the report accompanying this resolution, that it is in the best interests of the City to waive the City's advertising and competitive bidding requirements for purchase of certified and accredited forensic laboratory analytical supplies, equipment, instrumentation, instrument services and software on an as-needed basis when crime laboratory subject matter experts determine such supplies and related services are required by forensic casework conditions, the laboratory's validated methods, or its quality assurance program, or needed for the timely

analysis of evidence, or when the materials or services are available from only one source at a cost not to exceed $600,000 per fiscal year through June 30, 2025, for a total cost not to exceed three million dollars ($3,000,000); and be it

FURTHER RESOLVED: That the City Council finds and determines that pursuant to OMC Section 2.04.050.1.5 and based upon the reasons stated above and in the City Administrator's report accompanying this resolution, that it is in the best interests of the City to waive the advertising and competitive bidding requirements for the following vendors: Adorama, Agilent Technologies, Airgas, American Society for Quality, ANSl National Accreditation Board LLC, Artic White LLC, Arrowhead Forensics, Aurora Biomed, Autodesk, Brownells, Cabella's, Cayman Chemicals, Cerilliant Corporation, Cheaper Than Dirt?, Coherent Inc., Collaborative Testing Services Inc., Covanta Inc., CSI Forensic Supply, Environmental Science Research, EVIDENT, Fisher Scientific, Foray Technologies, Forensic Comparison Software Company, Foster + Freeman Ltd, Full Spectrum, Grainger, Leeds Forensic Systems Inc., Leeds Precision Instruments Inc., Leica Geosystems, Life Technologies, Manthei Mess Systeme, Mettler-Toledo Rainin LLC, Midway USA, Perkin-Elmer, Promega Corporation, Qiagen, Niche Vision Forensic LLC, The REMI Group Inc., Rice Lake Weighing Systems Division, Ron Smith and Associates, Safariland, San Diego Police Equipment Co Inc., Security Envelope Company, Serological Research Institute, Sigma Aldrich, Sirchie, Steraloids Inc., Thermo-Fisher, Thomas Scientific, Tri-Tech Inc., Uline, Unity Lab Services, USA Scientific, and VWR; and be it

FURTHER RESOLVED: the Department prohibition from purchasing any new equipment or software that may be considered surveillance technology for use by the Crime Lab or that contains any new capabilities or features beyond the existing technology is lifted because the Laboratory had made a full and good faith effort to complete the above process and will comply with the language proposed to be added to OMC 9.64.010 14 as section L; and be it

FURTHER RESOLVED: That any agreement authorized by this resolution shall be reviewed and approved by the Office of the City Attorney for form and legality prior to execution, and a copy shall be placed on file with the City Clerk.

IN COUNCIL, OAKLAND, CALIFORNIA, _____

PASSED BY THE FOLLOWING VOTE:

AYES – BAS, GALLO, GIBSON MCELHANEY, KALB, REID, TAYLOR, THAO, and PRESIDENT KAPLAN

NOES -

ABSENT -

ABSTENTION -

ATTEST:

_____
ASHA REED
Acting City Clerk and Acting Clerk of the Council

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: September 3, 2020

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 the recent ICE activity, 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. The Schedule I allows the CCPO to review each Schedule for compliance. The Department of Workplace and Employment Standards to conduct a preliminary scan to identify immediate errors. All Schedule I's meeting preliminary scans for completeness are forwarded to the Chief Privacy Officer (CPO), Office of the City Administrator. Subsequent tracking monitoring and enforcement fall under the purview of the CPO.

Applying the new schedule to the City's existing Contracting Process
After final adoption of the ordinance in June, staff developed a mechanism to ensure compliance. The Chief Privacy Officer (CPO) met with the Department of Workplace and Employment Standards (DWES) Director. It was agreed that the Schedule I would be submitted during the competitive process for all potential service agreements conducted by the DWES. Therefore, it was agreed that DWES would add "Schedule I" **(See Attachment A)** to its list of schedules that all potential service contractors must submit in order to move to the next phase of contracting with the City; and as originator, the CPO will track, monitor, and report compliance with the new law.

CPO Compliance monitoring and enforcement
If a contractor self-Certifies that they have no contracts with ICE, CBP, or HHS/ORR on Schedule I, then they may continue with the contracting process. If they attest that they ***do*** have a contract with ICE or CBP , the Schedule I is forwarded to CPO and the process is stopped by the CPO and determine with the individual department seeking to use the contractor if they believe there is any reason to seek a waiver.

Clarifying Memo
A notice was provided by the CPO to the Contract and Compliance Staff **(Attachment B)** and was posted on the department's website along with Schedule I to allow for greater public awareness of the new law. Also, included on the website was the list of known contractors that already are prohibited from contracting with the City of Oakland **(Attachment C)**.

Disclosure of Compliance/Violations
By advertising the prohibition proactively to all potential contractors on the website and with Schedule I embedded in the standard contract packet, staff believe most enforcement will take place pre-emptively; contractors who are prohibited will self-select to not do business with the City. If they or the department that is seeking their services believes they deserve a waiver, it requires a review and recommendation by the PAC to be forwarded to the City Council.

Actions Taken to Cure Deficiencies
Although the Implementation Plan was underway by the late fall of 2019, the CPO and DWES Leadership met in the Summer of 2020 to further develop the process. *This is not due to any known compliance issue.* Starting in September 2020, the DCES will provide all Schedule I's to the CPO on a monthly basis for a further verification.

This will address any concern that a contractor may misrepresent themselves on Schedule I and especially if the contractor recently entered into an agreement with ICE/CBP/or DDS/ORR. An additional compliance piece that needs to be better developed is routine updating of the list of known prohibited contractors. There is not a built-in mechanism to update the list, but CPO staff are committed to developing an effective one.

The Department of Workplace and Employment Standards (DWES) pledges to forward all Schedule I documents received by way of the competitive process for which it is responsible. DEWS does not track and monitor compliance, investigate or address non-compliances. .

Investment Prohibitions
The CPO provided the same 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 and as of the end of 2019, no investments in the prohibited entities were noted. As noted above, a current compliance item that needs more development is the updating of the list of prohibited entities.

As of the end of 2019, no potential contractor has submitted a Schedule I indicating they have an active contract with ICE, CBP, or HHS/ORR, therefore the trigger of review and recommendation by the PAC has not been pulled.

Respectfully submitted,

Joe DeVries,
Chief Privacy Officer

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

Attachment A: City of Oakland Schedule I.
Attachment B: Memo from the CPO to Contracts and Compliance Staff
Attachment C: List of known prohibited entities.

CITY OF OAKLAND

Schedule I

"Sanctuary City Contracting and Investment Ordinance"

United States Immigration and Customs Enforcement (ICE), Customs and Border Protection (CBP), and Department of Health and Human Services Office of Refugee Resettlement (HHS/ORR) Prohibition.

This Schedule must be submitted with all proposals or bids by all contractors/Consultants and their sub-contractors/subconsultants, and all vendors seeking to do business with the City of Oakland. Compliance must be established prior to full contract execution.

I, (name)_____, the undersigned, _____ of
(Position/Title

_____
(Business Entity) - hereinafter referred to as Business Entity and duly authorized to attest on behalf of the business Entity), declare the following:

1. Neither this Business Entity nor any of its subsidiaries, affiliates or agents are under contract with the United States Immigration and Customs Enforcement (ICE), Customs and Border Protection (CBP), or the Department of Health and Human Services Office of Refugee Resettlement (HHS/ORR) to provide services or goods for data collection or immigration detention facilities. The term "data collection" includes the collection of information (such as personal information about consumers) for another purpose from that which it is ultimately used, datamining in large data bases for trends and information, threat-modeling to identify probable attackers to computer systems, predictive risk analysis to predict future events, and similar services. Additionally, this business entity does not anticipate a contract with ICE, CBP, or HHS/ORR for such work for the duration of a contract/contracts with the City of Oakland.
2. The appropriate individuals of authority are cognizant of their responsibility to notify the City's Project Manager and invoice reviewer or the City Administrator's Office, Chief Privacy Officer if any of this Business Entity's subsidiaries, affiliates, or agents are under contract with ICE, CBP, or HHS/ORR for the purposes listed above.
3. To maintain compliance, upon review and approval of invoices, the contractors/vendors hereby agree to submit a declaration on company stationery attached to each invoice that the company remains in compliance with the ICE, CBP, and HHS/ORR Prohibition and will not seek or secure a contract with ICE, CBP, or HHS/ORR.
4. Upon close out or completion of deliverables and prior to issuance of final payment (while honoring the Prompt Payment Ordinance), this business entity agrees to submit a statement attached to the final invoice, under penalty of perjury, declaring full compliance with the ICE, CBP, and HHS/ORR Prohibition. I understand that an invoice is not declared fully complete and accepted unless and until the declaration of compliance is accepted.
5. If this business entity fails to disclose a contract with ICE, CBP, or HSS/ORR to provide services for data collection or immigration detention facilities, the relevant persons may be guilty of a misdemeanor and up to a $1,000 fine. Additionally, the City Administrator may to the extent permissible by law, remedy any such violations and may use all legal measures available to rescind, terminate, or void contracts in violation.
6. I declare under penalty of perjury that the above will not, have not, and do not plan to contract with ICE, CBP, or HHS/ORR to provide services or goods for data collection or immigration detention facilities.

CITY OF
OAKLAND

PLEASE COMPLETE AND SIGN

☐ **I declare that I understand Ordinance #13540 C.MS. Based on my understanding the above is true and correct to the best of my knowledge.**

or

☐ **I declare that I understand Ordinance # 13540 C.MS. Based on my understanding all or a portion of the above is not true and correct to the best of my knowledge.**

(Printed Name and Signature of Business Owner) (Date)

(Name of Business Entity) (Street Address, City, State, and Zip Code)

(Name of Parent Company) (If applicable)

Contacts:
Office Phone: _____ Cell Phone:_____ email: _____

For Office Use Only:

Approved/Denied/Waived

(signed) _____ _____
Authorized Representative Date

SCHEDULE I DB/DM 2019

CITY OF OAKLAND
Office of the City Administrator

(510) 238-3301 • 1 Frank H. Ogawa Plaza, 11th Floor • Oakland, CA 94612

Memorandum

To: Contracts and Compliance Division Staff Members

From: Joe DeVries, Chief Privacy Officer

Re: The Sanctuary City Contracting and Investment Ordinance

Date: October 7, 2019

Ordinance N.O. 13540 CMS was adopted by the Oakland City Council on June 4th, 2019 and prohibits the City from contracting with any person or entity that provides the United States Immigration and Customs Enforcement (ICE) services or goods for data collection or with the United States Customs and Border Protection (CBP) Customs and Border Protection (CBP), or the Department of Health and Human Services Office of Refugee Resettlement (HHS/ORR) to support immigration detention facilities. These contractors are not to be used 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. The ordinance also requires that the City provide an annual report to the Privacy Advisory Commission on its enforcement.

Because this ordinance was sponsored by the Privacy Advisory Commission and is specifically related to protecting the privacy of people's personal data, I will provide oversight of this ordinance as the Chief Privacy Officer for the City. The goal is to prevent anyone from applying for an RFP, RFQ, or other contract before they get too far in the process so it will be important to let potential contractors know about this requirement as early in the process as possible. In most instances that should be enough, however, in the circumstance that a contractor (and the City Department they would be working with) feels that they can argue successfully for a waiver, they can continue in the process and I would have the Privacy Advisory Commission review this claim to make a recommendation to the City Council.

Attached is a list of known businesses that already do business with ICE or CBP for these services that would be excluded under the law. As this list is updated periodically, I will share it with you but will also review any ongoing requests your office receives. If you have any questions about the ordinance, please do not hesitate to contact me at 510-238-3083 or jdevries@oaklandca.gov