CITY OF OAKLAND

Privacy Advisory Commission

June 4, 2020
4:00 PM
Teleconference
Special 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/83424517084

Or iPhone one-tap :

US: +16699009128,,83424517084# or +12532158782,,83424517084#

Or Telephone:

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

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

Webinar ID: 834 2451 7084

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

Pursuant to the Governor's Executive Order N-29-20, members of the Privacy Advisory Commission, as well as City staff, will participate via phone/video conference, and no physical teleconference locations are required.

1. Call to Order, determination of quorum

2. Open Forum/Public Comment

3. Review and approval of the draft May meeting minutes

4. Federal Task Force Transparency Ordinance – OPD – FBI's Joint Terrorism Task Force 2019 Annual Report – review and take possible action.

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

CITY OF OAKLAND

Privacy Advisory Commission

May 14, 2020 5:30 PM
Oakland City Hall
Hearing Room 1
1 Frank H. Ogawa Plaza, 1st Floor
Special Meeting Minutes

***Commission Members**: **District 1 Representative**: Reem Suleiman, **District 2 Representative**: Chloe Brown, **District 3 Representative**: Brian Hofer, Chair, **District 4 Representative**: Lou Katz, **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.

1. Call to Order, determination of quorum

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

2. Open Forum/Public Comment

AC Transit At-Large Board Member Chris Peeples spoke about AC Transit's desire to develop a Use Policy for the cameras that are being installed on the Bus Rapid Transit Stations throughout Oakland before they go live. He asked if members of the PAC would want to provide technical assistance to the working group.

Jeffrey Wang and Javiera Jamil both spoke about the JTTF Annual Task Force Report being overdue and urged the PAC to hold OPD accountable and require the report be submitted.

Asada Olugbala asked about the PAC's authority to review Task Force Reports and Agreements. She noted that neither the Surveillance Tech Ordinance nor the enabling ordinance that created the PAC gives that authority and she wants to see where it originated. Chairperson Hofer identified that Ordinance Number 13457 gives the PAC that authority.

3. Review and approval of the draft March meeting minutes

The March Minutes were approved unanimously.

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

Chairperson Hofer opened up the conversation noting there were several portions of the Use Policy that are incomplete and would need to be finished. Member Oliver had questions about predictive policing and the potential impact on racial profiling. Member Katz asked about their data sharing agreements, noting their mention of not sharing with ICE but asked about other agencies.

Captain Bassett noted that the system does not have predictive abilities and Robert Batty with forensic Logic noted that they have prohibited any data sharing with ICE at OPD's request since 2009.

Member Suleiman asked about the contractor's relationship with CE and the city's ban on using such contractor's Captain Figueroa said that while there are some other contractors, they simply don't have the equipment, tools or algorithms that Forensic Logic has developed. Their long-standing work with Oakland makes separating even more challenging to select a different contractor.

Chair Hofer circled back to the missing items, noting that if the PAC has a better understanding of the contract and what Forensic Logic provides, it will be much easier to review and make a recommendation on a policy. An ad hoc group was created and the item will be brought back soon to give time for the contract to go to Council in a timely manner.

5. Surveillance Equipment Ordinance – OPD – UAS (Drone) Impact Report and proposed Use Policy – review and take possible action

The group reviewed the most recent Impact Statement and Use Policy and Member Tomlinson made a motion to approve both with two stipulations: first, that the City only acquire a drone with the capabilities allowed in the Use Policy (no added features that would require future modifications to the policy). Second, due to the economic fragility of the City during the downturn, that the City only use grant funds to purchase a drone and not general fund revenue.

The motion was adopted unanimously.

CITY OF OAKLAND

MEMORANDUM

TO: Privacy Advisory Commission

FROM: Roland Holmgren
Deputy Chief of Police

SUBJECT: OPD – FBI 2019 Joint Terrorism Taskforce (JTTF) Annual Report

DATE: May 20, 2020

EXECUTIVE SUMMARY

Ordinance No. 13457 C.M.S. approved by the City Council on October 3, 2017, adds Chapter 9.72.010 to the City of Oakland Municipal Code (OMC) concerning "Law Enforcement Surveillance Operations." OMC 9.72.010 requires that, among other requirements, that by January 31 of each year, the Chief of Police shall provide to the Privacy Advisory Commission (PAC) and City Council, a public report with appropriate public information on the Police Department's work with the Federal Bureau of Investigation (FBI) Joint Terrorism Task Force (JTTF) or other federal law enforcement agency task force in the prior calendar year.

STAFFING, EQUIPMENT AND FUNDING

As of January 1, 2019, one (1) employee (sworn OPD officer) was assigned to the FBI JTTF. The officer was assigned to work a standard regular work week of (40) forty hours per week. This officer is assigned to OPD's Intelligence Unit and has a joint duty of also participating and assisting with the FBI JTTF. The officer's duties and reporting responsibilities depend upon whether there is any active counter-terrorism investigation as well as the current needs and priorities of the OPD Intelligence Unit.

The position is compensated as a regular OPD officer; the FBI does not compensate OPD for this position's salary. The officer position works regular hours: 40 hours per week; 1,920 hours per year (approximately). Any overtime (OT) hours specific to taskforce operations are paid by the FBI - in 2019, the OPD JTTF Officer did not work any OT hours related to JTTF duties.

The JTTF-assigned officer was on special loan from the Intelligence Unit for most of 2019, assisting with upgrades to OPD's Bureau of Services Evidence Unit; the officer participated in monthly meetings with the JTTF during this time and actively assisted with investigations when requested. The upgrades to the OPD evidence unit are now complete enough that the officer can support both the OPD Intelligence Unit and JTTF information development (see ***Cases Assigned to the OPD JTTF Officer*** Section below), in addition to attending regular JTTF meetings.

OTHER RESOURCES PROVIDED

The FBI provided a vehicle, covered all fuel expenditures, and allowed access to the FBI JTTF office space and access to FBI data systems. OPD provides the mobile phone used by the Task Force (TF) Officer. The officer is not provided with any FBI surveillance equipment.

CASES ASSIGNED TO THE OPD JTTF OFFICER

The JTTF Officer assists the FBI on counter-terrorism cases. The OPD JTTF-assigned officer was assigned on special loan to OPD's Bureau of Services for the evidence unit for project support for most of 2019 as described above. Therefore, the officer was not assigned to any JTTF cases as a lead investigator; the JTTF Task Force Officer was assigned zero (0) cases as lead investigator in 2019. In 2019, there were five cases where the officer assisted the FBI as a secondary officer in a support role, primarily conducting research.

The following are two examples where the OPD JTTF-assigned officer assisted with investigations:

- In February 2019, the FBI requested OPD assistance in identifying a location and suspect related to homicide threat. The OPD JTTF Officer, who utilized certain FBI information, the FBI was able to eliminate several locations and connected individuals, and clearly identify the exact location as well as the key suspect. This information allowed the FBI to issue a search warrant on the residence, and a suspect was arrested. The victim, a mother of two children, was unharmed and safely relocated with her children. The FBI, with the assistance of the JTTF Officer, saved a mother and her children from murder.

- On June 27, 2019, suspects, armed with rifles, robbed a Loomis Armored Trunk in front of Wells Fargo in the City of Oakland, stealing approximately $500,000. The OPD JTTF Officer utilized OPD information to identify three suspects; Several search warrants were served, which led to the arrests of the suspects as well as significant evidence recovery.

The JTTF Officer participated in zero (0) duty to warn cases, where "Duty to Warn" is identified as the "requirement to warn U.S. and non - U.S persons of impending threats of intentional killing, serious bodily injury, or kidnapping".[1]

There were zero (0) cases in 2019 where OPD declined to participate after FBI request. The FBI knows that OPD task force officers must comply with all Oakland laws and policies. Furthermore, the FBI commonly works with different jurisdictions and understands that taskforces must collaborate with the particular polices and laws of those jurisdictions.

UNDERCOVER OPERATIONS AND INTERVIEWS

In 2019, the OPD JTTF Officer did not participate in any joint FBI-OPD undercover operations or interviews (JTTF interviews are normally conducted by FBI Agents); zero (0) undercover operations were conducted by the OPD JTTF-assigned officer. However, the officer did support informational gathering on behalf of JTTF investigations. The OPD officer only conducted information gathering, and did not work directly with FBI personnel on any actual operations.

In 2019, the OPD JTTF Officer did not take part in any interviews (voluntary or involuntary) - zero (0) were conducted.

In 2019, the OPD JTTF Officer did not conduct any assessments - zero (0) assessments conducted. Generally, unless someone were to come to the OPD to report a threat, all assessments begin with the FBI. Procedurally, FBI is notified, and an assessment is opened and FBI will then forward the assessment to specific agents.

[1] FBI Duty to Warn – Intelligence Community Directive 191: https://fas.org/irp/dni/icd/icd-191.pdf

The OPD JTTF Officer does not manage any informant relationships. In 2019, there were zero (0) informant's managed by OPD JTTF Officer. Furthermore, the Intelligence Unit Sergeant is the Informant Program Coordinator for all OPD informants. A file check was conducted on the JTTF Officer and there were zero (0) informant relationships related to the JTTF[2].

In 2019, there were no requests from outside agencies (e.g. Immigration and Customs Enforcement or "ICE") for records or data of OPD. There were no cases where the Task Force Officer was involved or aware of asking an individual's U.S. Person (residency) status. Furthermore, it is OPD Policy that OPD shall not inquire about a citizen's residency status.

The FBI is aware of requirements mandated of OPD and its protocols for undercover operations and interviews; the Task Force Officer was always held responsible for following all sworn officer policies and standards.

TRAINING AND COMPLIANCE

The OPD JTTF Officer follows all OPD policies and receives several police trainings, including but not limited to: continual professional training, procedural justice, and annual firearms training. The Officer has also reviewed all provisions of the JTTF MOU. The JTTF Officer as well as supervisor are held responsible by OPD for compliance with all applicable Oakland and California laws. The most recent list of trainings attended are as follows:

Date	**Training Type**
September 16, 2019	Criminal Investigations and Constitutional Law Update
September 17, 2019	Racial Profiling Update
September 18, 2019	Annual Firearms / Force Options Training
Ongoing	Virtual FBI training

The OPD JTTF Officer supervisor (Intel Sergeant) conducts mandatory bi-weekly meetings with the officer. Daily and weekly meetings are also held when critical incidents occur. Furthermore, the Intel Sergeant regularly works with the JTTF Officer in the same building/office located at the Police Administration Building (PAB). Additionally, the Sergeant supervising the officer in 2019 had U.S. Secret Service clearance and could review the work of the OPD JTTF Officer.

ACTUAL AND POTENTIAL VIOLATIONS OF LOCAL/STATE LAW

The JTTF OPD Officer had no violations of local, California, or Federal law. OPD Command consults with the Office of the City Attorney to ensure that all polices conform with State and Federal laws. Furthermore, a file check was conducted on the OPD JTTF Officer's complaint history in 2019 and there were zero (0) zero complaints against the Officer.

[2] Identities of any informant would never be released to the public as such information is may be dangerous for the life of the informant.

SUSPICIOUS ACTIVITY REPORTING (SARs) and NORTHERN CALIFORNIA REGIONAL INTELLIGENCE CENTER (NCRIC)

OPD submits Suspicious Activity Reports (SARs) to the Northern California Regional Intelligence Center (NCRIC). These reports contain information regarding activity, such as, but not limited to: narcotics, cyber-attacks, sabotage, terrorism threats, officer safety, and human trafficking. NCRIC provides a secure online portal where police agencies can provide this information. NCRIC has shared with OPD that providing false or misleading information to NCRIC is a violation of Federal Law and may be subject to prosecution under Title 18 USC 1001. The JTTF is a recipient of SAR information. The OPD JTTF Officer submitted zero (0) SARs to NCRIC during the 2019 calendar year. It is unknown how many SAR's OPD Officers received during 2019 as there is no current tracking system.

COMMAND STRUCTURE FOR OPD JTTF OFFICER

The OPD JTTF Officer works under the command structure of OPD; the OPD JTTF Officer reports directly to the OPD Intelligence Unit Supervisor (Sergeant). The Officer also coordinates with the FBI Supervisor, who is also serves as a Counterterrorism Assistant Agent.

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) Universal 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 ***Appendix B*** "Forensic Logic Product Modules" 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, rank results based on serious of the offense, proximity to a user's location and time of event, and extract entities and relationships from the data. 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 regional agencies empowers those agencies to

better investigate crimes that may be from other cities but still connected to Oakland crime as well.

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.

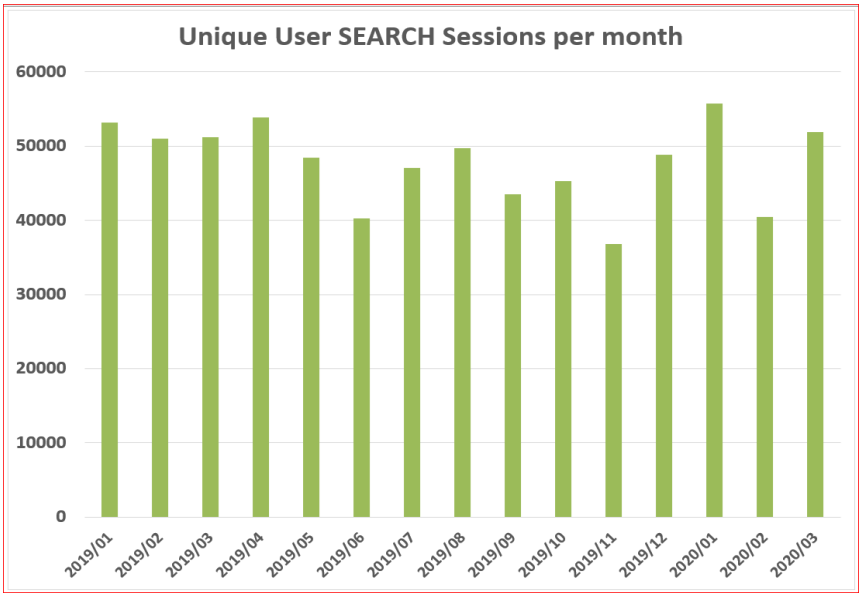
B. Proposed Purpose

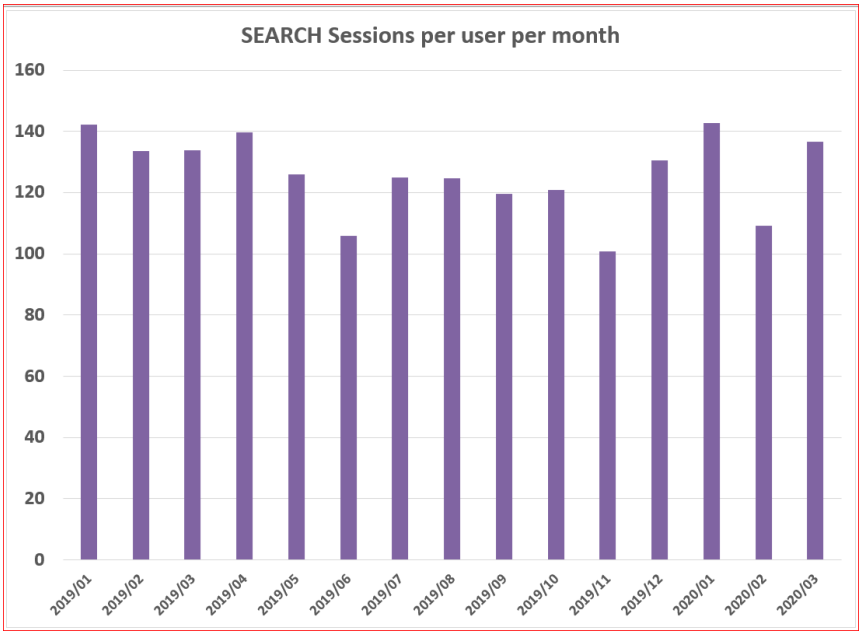
Forensic Logic provides three core services for OPD: a) crime analysis report production; b) search; and c) technical assistance**.**

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 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 to a legal name of a suspect of in a recent homicide, now

[1] https://www.oaklandca.gov/topics/oaklands-ceasefire-strategy

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.

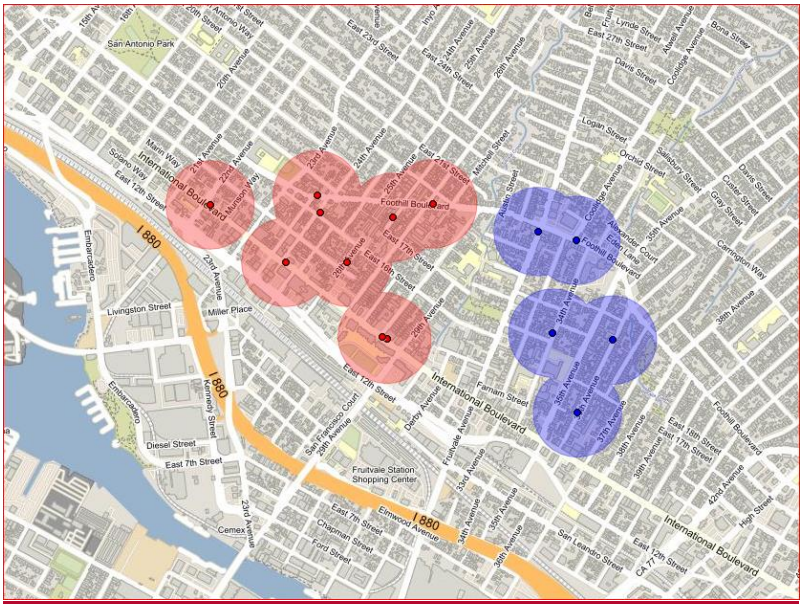
- A CopLink search on an auto burglary suspect vehicle, revealed that the suspect vehicle was connected to several other auto burglaries. Officers located and towed the suspect vehicle. The vehicle is now being analyzed by OPD evidence technicians for more clues.

- 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.

CopLink is not a predictive policing system. The system is an aggregation of law enforcement data previously collected from existing law enforcement information systems such as CAD and RMS by law enforcement agencies into a data warehouse; the system connects data based on common variables (e.g., location, name, vehicle) using a ranking system. Data connected to more serious and violent crimes are ranked higher. Data connected to entered query data with a closer geographic proximity will be ranked higher and thus presented near the top of search results (similar to a standard search engine query). However, the system ranking does not provide any type of analytics to predict future activity. There is a "hotblocks" feature in CopLink Analytics (see LEAP User Guide ***Appendix C***) that illustrates incident clusters (see Figure 1 below). However, the hotblocks feature is a mathematical geospatial tool for plotting similar incidents on a map given incident locations. The 'math' looks at latitude/longitude - and then calculates how near some dots on the map are to all other dots on the map. Investigators can use the visualization – along with other data and evidence to help identify leads. This type of work is integral to intelligence-led policing. This tool does not actually make any predictions but rather helps personnel with their analysis of where crimes are occurring.

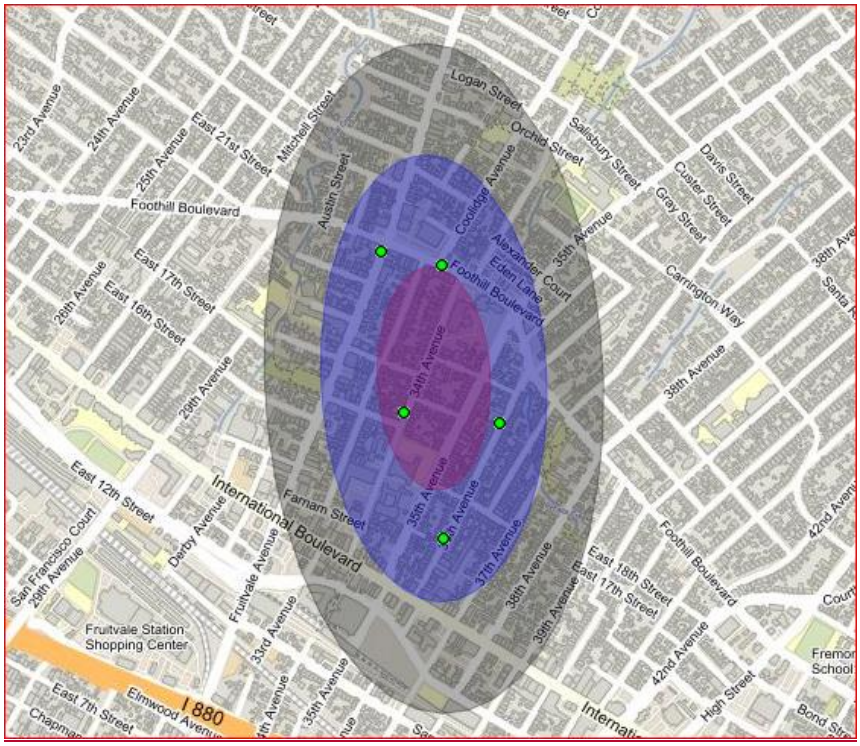
Formatted: Heading 1, Indent: Left: 0.38", Right: 0.7", Space Before: 11.55 pt, After: 6 pt, Tab stops: 0.38", Left

Figure 1: CopLink HotBlocks Feature of Penal Code PC 245(a)(2) shootings in Oakland between January 1, 2020 and May 31, 2020



The LEAP User Guide (***Appendix C***) also speaks about the "Next Crime Location (NCL)" feature. NCL is similar to HotBlocks in that it also displays on a map the relationship of incident locations (X-Y grid) and their relationship to the center of mass of those X-Y points and one, two and three standard deviation distribution from that center of mass. ***Figure 2*** below shows that NCL takes geographic incident data and calculates mathematical spaces around the center of gravity of the dot. This tool similarly allows personnel to see crime density on a map so that personel can make more informed decisions about where crime is more likely to occur in the future.

Figure 2: CopLink Next Crime Location (NCL) Feature of Penal Code PC 245(a)(2) shootings in Oakland between January 1, 2020 and May 31, 2020



OPD uses Forensic Logic CopLink to search through past law enforcement information to piece together information related to crimes that have occurred.

3. Technical Assistance

   OPD occasionally solicits Forensic Logic 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 Monitors 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 product 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 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. However, data housed in the Forensic CopLink system is limited to criminal incidents, arrest and jail booking records. Data is already collected, stored and shareable (in limited cases) with other law enforcement agencies by OPD.

Oakland residents who may not have a legal immigration status also have a right to privacy. Indeed, Oakland Municipal Code (OMC) 2.23.030[2] prohibits the City from contracting with vendors who provide services or goods for data collection or immigration detention facilities to the United States Immigrations and Customs Enforcement (ICE), Customs and Border Protection (CBP), or the Department of Health and Human Services, Office of Refugee Resettlement (DHS/ORR). Additionally, the California Values Act (SB 543) is enacted to ensure that 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.

[2]Prohibition on contracting with contractors that provide services or goods for data collection or immigration detention facilities to the United States Immigrations and Customs Enforcement, Customs and Border Protection, or the Department of Health and Human Services, Office of Refugee Resettlement.

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

The Forensic Logic CopLink system does not share any OPD information with any of the above-mentioned federal organizations.

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, state and local laws and ordinances 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 employ several strategies to mitigate against the potential for system abuse and/or data breach. In accordance with CJIS Security Policy (CSP) 5.8, 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.

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.

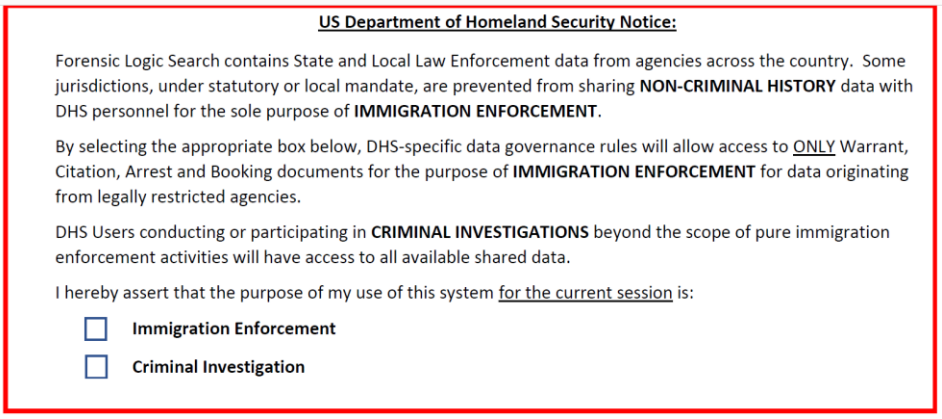
Section G below (Data Security) provides an in-depth explanation of the many ways the Forensic Logic CopLink system itself is secure to data breaches. Data that is deleted from OPD CAD/RMS or other systems is automatically deleted from the Forensic Logic CopLink system. OPD can also request that OPD data be expunged from Forensic Logic CopLink where appropriate based on changes to incident files.

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 (which focuses on expressly criminal investigations).

Forensic Logic partners with a number of 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)[4] 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:



US Department of Homeland Security Notice:

Forensic Logic Search contains State and Local Law Enforcement data from agencies across the country. Some jurisdictions, under statutory or local mandate, are prevented from sharing **NON-CRIMINAL HISTORY** data with DHS personnel for the sole purpose of **IMMIGRATION ENFORCEMENT**.

By selecting the appropriate box below, DHS-specific data governance rules will allow access to ONLY Warrant, Citation, Arrest and Booking documents for the purpose of **IMMIGRATION ENFORCEMENT** for data originating from legally restricted agencies.

DHS Users conducting or participating in **CRIMINAL INVESTIGATIONS** beyond the scope of pure immigration enforcement activities will have access to all available shared data.

I hereby assert that the purpose of my use of this system for the current session is:

☐ **Immigration Enforcement**

☐ **Criminal Investigation**

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 specify.

OPD data additionally cannot be accessed by ICE nor other non-authorized agencies via the National Law Enforcement Telecommunications System (NLETS)[5]. 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 Departments of Motor Vehicles (DMV) and the FBI National Crime Information Center (NCIC) where 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

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

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

virtual machines (computer servers) in a CJIS environment.

For the most part, NLETS does not store or collect data, 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; ~~T~~therefore, neither ICE nor other agencies can utilize CopLink and NLETS to access OPD data.

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 (e.g. name or address without actual names or addresses), 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.

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, ShotSpotter, and property data that could be used to populate an ATF eTrace[6] 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

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

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 protection of the law enforcement officers encountering the individuals described in the system.

There are many types of OPD data that, by policy and process, will not be sent to Forensic Logic CopLink for accessibility to OPD personnel 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[7] capabilities

[7] Forensic Logic Product Modules (see ***Appendix B***) shows that the older "Legacy" previously owned by IBM offered a feature called "FaceMatch" facial recognition. This system was used to provide five other

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

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

The Forensic Logic CopLink enterprise service is broken down into a number of components. The two primary components are: 1) Analytics; and 2) Search.

There are several elements to the Analysis component – 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 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 analytics modules above are included with the subscription to the CopLink Analytics service in the Forensic Logic CopLink network and are not provided independently. OPD has successfully negotiated an enterprise subscription to the Forensic Logic CopLink Analytics product at no additional charge so all OPD sworn officers and civilians under the auspices of the Chief of Police will have access to all Analytics capabilities at no additional fee.

There are several elements to the Search component – all of which are

---

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.

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 Analytics services as a Named User subscription available to selected sworn staff and professional staff operating under the auspices of the Chief of Police.

In addition, Forensic Logic oftentimes is called upon by OPD 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[8]. 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)[9], CJIS). One strategy is that Azure Government

[8] https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center
[9] https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final

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[10] certificates and 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 at NLETS 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

.

Commented [BS1]: OPD is currently negotiating the cost of a 2-3 year new contract with Forensic. Prior, OPD paid approximately 185k/yr for services. OPD anticipates a new annual cost at a slightly higher rate.

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

[10] RSA is a public key encryption algorithm that cannot be broken in a timely manner by even the largest computer networks: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf
https://en.wikipedia.org/wiki/FIPS_140-2

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. They have built a customized crime report system 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 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. 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. 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.

Appendix A

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.

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/or use of force investigations).

Rules and Processes Prior to use

- Only sworn law enforcement personnel or 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 criminal 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

In addition, for those law enforcement agencies that subscribe directly to the Thomson Reuters CLEAR public records database, the Forensic Logic CopLink network has indexed abstracts (summary information lacking details) of certain public records available in the Thomson Reuters CLEAR service so that a single search in the Forensic Logic CopLink search service will reveal that the CLEAR service has more information about the topic. A user is then able to select the item and will be transported to the Thomson Reuters CLEAR system directly where user authentication is required by Thomson Reuters and the user, depending on the data requested, must satisfy all the requirements as stipulated by the Gramm-Leach-Bliley Act (also known as the Financial Services Modernization Act of 1999) and the Federal Credit Reporting Act. Forensic Logic CopLink is not involved in the administration of this process and only provides a link to Thomson Reuters based on an abstract of the record being found in its search service. Moreover, if a user is

not a subscriber to the Thomson Reuters CLEAR service, no mention will be found by a user query to the Forensic Logic CopLInk network.

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.

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.

Law enforcement agencies in the following CA counties currently either have access and/or contribute or plan to contribute data to the Forensic Logic CopLink network.

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.

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: