# 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.

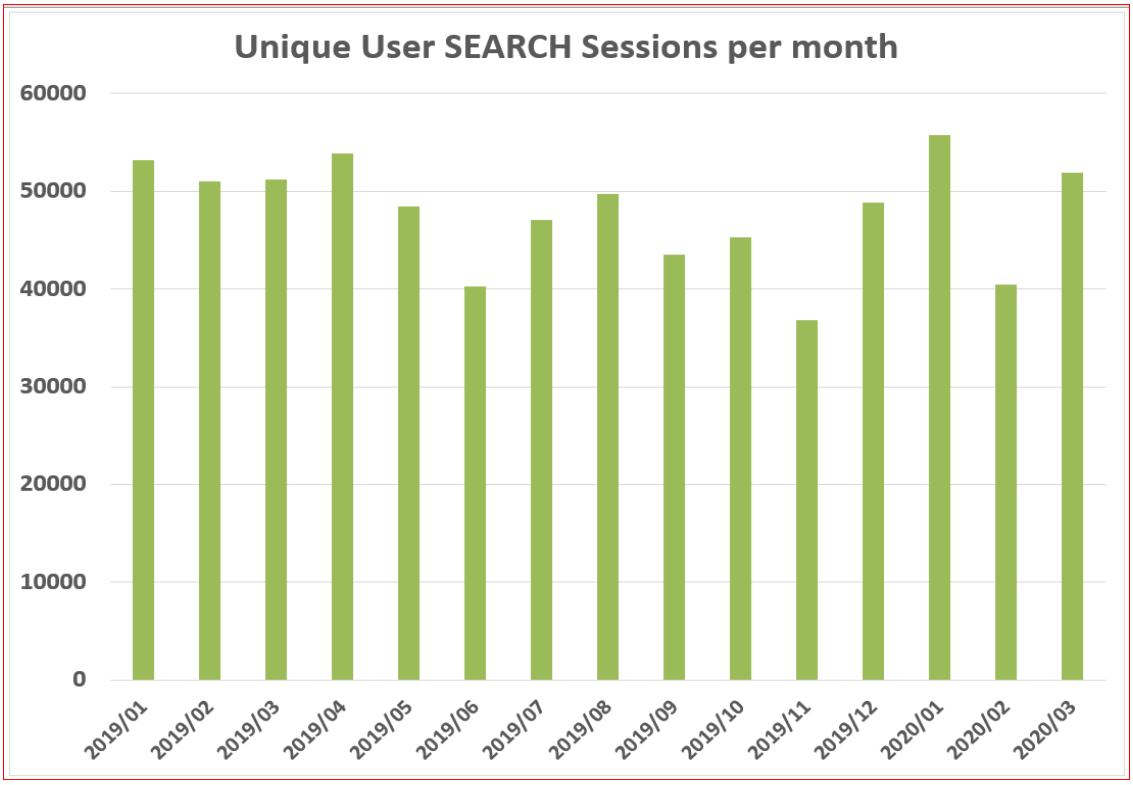
## B. Proposed Purpose

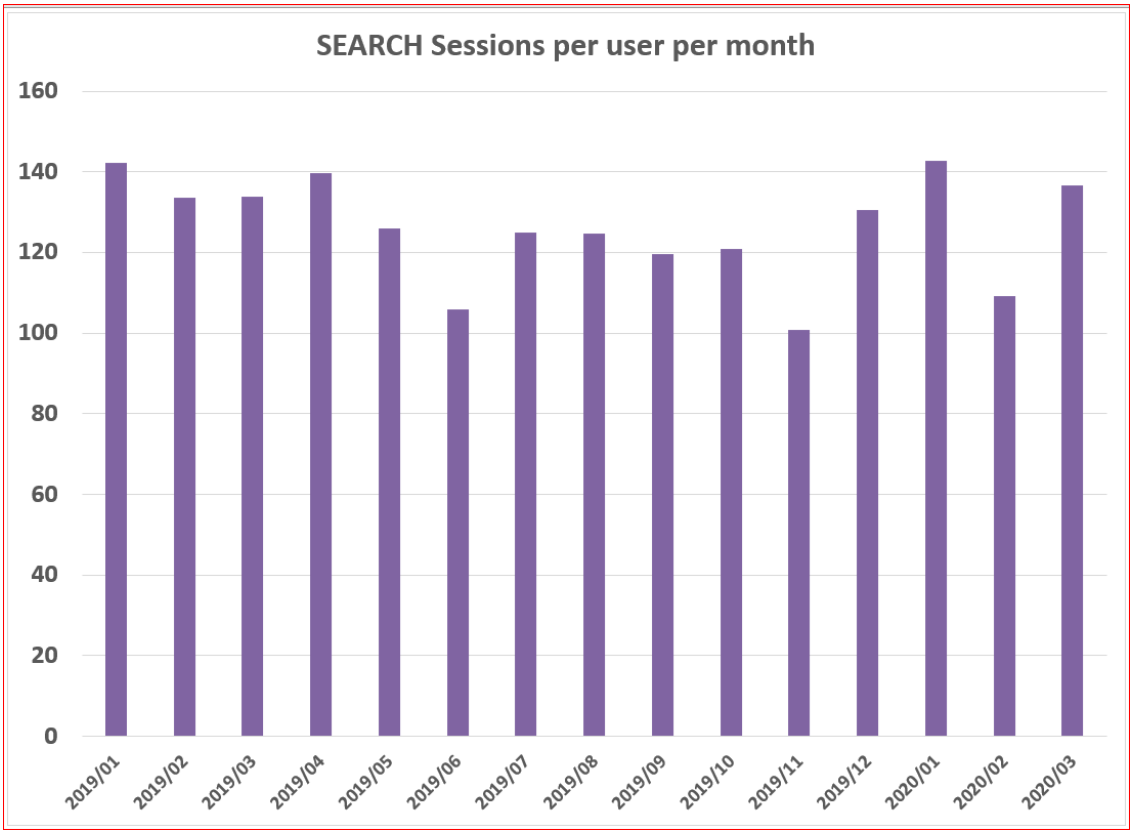
Forensic Logic provides three core services for OPD: a) crime analysis report production; b) search; and c) technical assistance**.**

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***

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

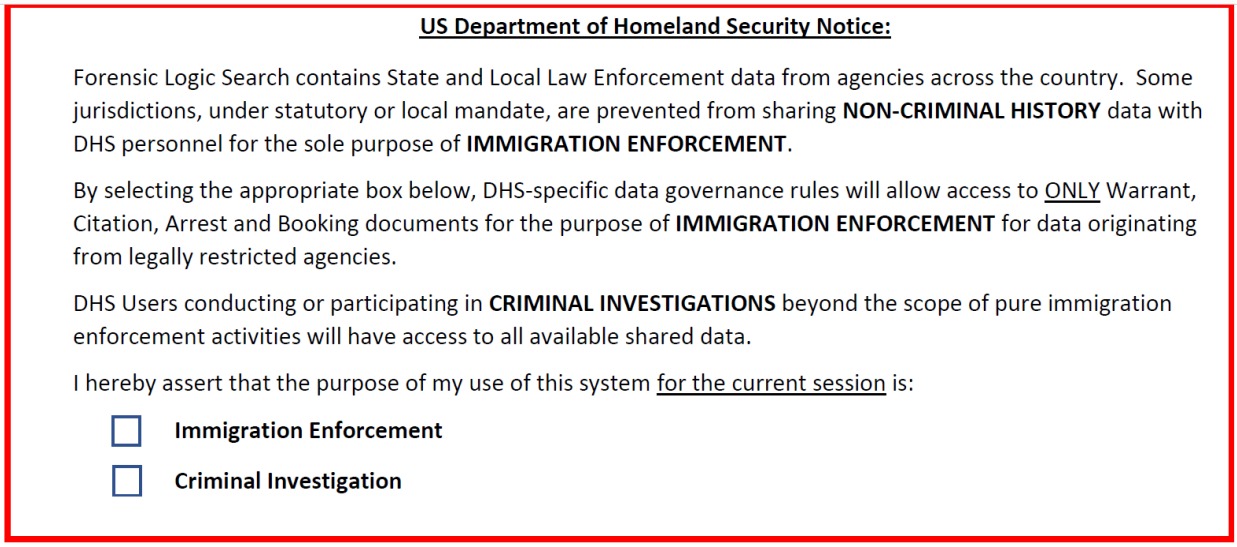
the Forensic Logic CopLink system.

*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:



**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

[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.

*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.*