CITY OF OAKLAND

Privacy Advisory Commission

May 14, 2020 5:30 PM
Via 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*

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.

Agenda

1. Call to Order, determination of quorum
2. Open Forum/Public Comment
3. Review and approval of the draft March meeting minutes
4. Surveillance Equipment Ordinance – OPD – Forensic Logic Impact Report and proposed Use Policy - review and take possible action.
5. Surveillance Equipment Ordinance – OPD – UAS (Drone) Impact Report and proposed Use Policy – review and take possible action

PUBLIC PARTICIPATION

The Privacy Advisory Commission encourages public participation in the online board meetings. The public may observe and/or participate in this meeting in several ways.

OBSERVE:

• To observe the meeting by video conference, please click on this link:

https://us02web.zoom.us/j/88574901972 at the noticed meeting time. Instructions on how to join a meeting by video conference are available at: https://support.zoom.us/hc/en-us/articles/201362193, which is a webpage entitled "Joining a Meeting"

• To listen to the meeting by phone, please call the numbers below at the noticed meeting time: Dial (for higher quality, dial a number based on your current location):

iPhone one-tap :
US: +16699009128,,88574901972# or +12532158782,,88574901972#
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 +1 301 715 8592 or +1 312 626 6799 or +1 646 558 8656

For each number, please be patient and when requested, dial the following Webinar ID: 885 7490 1972

After calling any of these phone numbers, if you are asked for a participant ID or code, press #. Instructions on how to join a meeting by phone are available at: https://support.zoom.us/hc/en-us/articles/201362663, which is a webpage entitled "Joining a Meeting By Phone."

PROVIDE PUBLIC COMMENT: There are three ways to make public comment within the time allotted for public comment on an eligible Agenda item.

• Comment in advance. To send your comment directly to the Selection Panel and staff BEFORE the meeting starts, please send your comment, along with your full name and agenda item number you are commenting on, to Joe DeVries at jdevries@oaklandca.gov. Please note that eComment submissions close thirty (30) minutes before posted meeting time. All submitted public comment will be provided to the Selection Panel prior to the meeting.

• By Video Conference. To comment by Zoom video conference, click the "Raise Your Hand" button to request to speak when Public Comment is being taken on an eligible agenda item at the beginning of the meeting. You will then be unmuted, during your turn, and allowed to participate in public comment. After the allotted time, you will then be re-muted. Instructions on how to "Raise Your Hand" are available at: https://support.zoom.us/hc/en-us/articles/205566129, which is a webpage entitled "Raise Hand In Webinar."

• By Phone. To comment by phone, please call on one of the above listed phone numbers. You will be prompted to "Raise Your Hand" by pressing STAR-NINE ("*9") to request to speak when Public Comment is being taken on a eligible agenda item at the beginning of the meeting. Once it is your turn, you will be unmuted and allowed to make your comment. After the allotted time, you will be re-muted. Instructions of how to raise your hand by phone are available at:
https://support.zoom.us/hc/en-us/articles/201362663, which is a webpage entitled "Joining a Meeting by Phone."

If you have any questions about these protocols, please e-mail Joe DeVries at jdevries@oaklandca.gov

CITY OF OAKLAND

Privacy Advisory Commission

March 5, 2020 5:00 PM
Oakland City Hall
Hearing Room 1
1 Frank H. Ogawa Plaza, 1st Floor
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, **Mayoral Representative**: Heather Patterson, Co-Chair*

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

2. Open Forum/Public Comment

There was one speaker under Open Forum, Rick de Silva speaking in favor of item 6. He wanted to be on the record but needed to leave early.

3. Review and approval of the draft February meeting minutes

The February Minutes were approved unanimously.

4. Election of Vice Chair

Chairperson Hofer nominated Member Gage as the Vice-Chair, and he was approved unanimously.

5. Federal Task Force Transparency Ordinance – OPD – Presentation of Annual Reports for US Marshals, DEA, ATF – review and take possible action

Bruce Stoffmacher gave an overview of the reports and noted the following: There was no work with ICE, no personal information was shared with ICE or other agencies. Officers are trained to adhere to OPD

Policy not Federal Policy and that with only one officer on the task force, OPD is not reporting any violations because this would be a personnel issue under P.C. 832.7, identifying the officer for a violation that otherwise would not be publicly reported/would be protected.
Chairperson Hofer asked about PC832.7 and argued that the Skinner Bill allows for the release of this type of information and asked for a legal opinion about this conflict. Both Joe DeVries and DC Holmgren agreed they would submit a request for a legal opinion on this topic. Member Reem asked what the threshold number of task force members there would need to be to release data on violations. Member Gage noted his concern for blanket confidentiality, he moved that the item be forwarded for approval with the caveat that the PAC has a real concern about the department citing P.C. 832.7 and the impact on the task force reporting.

There was one public speaker, Asada Olugbala who stated that she did not believe this should be the purview of the PAC but instead should be reviewed by the Police Commission.

6. Surveillance Equipment Ordinance – DOT – Chinatown Chamber of Commerce Camera Grant Program Impact Report and proposed Use Policy – review and take possible action

Chairperson Hofer explained why this program is required to be presented first to the PAC and DOT Assistant Director Wlad Wlasowsky explained how the program was allocated funding during the budget process and placed into DOT (it was originally under a street light improvement program). He also explained that the proposal was an addition to an earlier camera project from 2012.

There were 6 public speakers on the issue as summarized below:
Asada Olugbala argued that Chinatown should pay for the cameras themselves as there is crime all over the City and its not equitable for one neighborhood to receive this help.
Jessica Chen from the Chinatown Chamber of Commerce described the plan to install and monitor the cameras and the need that her group has identified.
Carl Chan of the Chamber stated his support and discussed the crime stories he hears at the NCPC Meetings.
Juan-Gong also aired their support, citing his wife's experience of being assaulted last year.
Michael Katz-Lacabe argued this proposal is public funding of private surveillance and is flawed. It provides for little oversight and transparency and needs stronger reporting requirements.

The PAC Members raised significant concerns about this program being anathema to the goals of transparency and public oversight of surveillance technology. Chairperson Hofer noted the need for better reporting requirements, auditing, and performance evaluation. Member Katz asked if there was any data to suggest these cameras actually reduce crime. DC Holmgren was asked about and discussed Chinatown Crime trends in general and explained that OPD is using video footage to solve a lot of crimes so it can be very useful even if not well measured. He also offered to help with a more thorough oversight plan if the proposal moves forward. The item was tabled to a later date to allow DOT. OPD, and the CAO to work on a more developed oversight plan.

7. Surveillance Equipment Ordinance – OPD – Live Stream Cameras – review and take possible action

Joe DeVries reviewed the Emergency Operations Center activation standards that were provided for discussion and DC Holmgren discussed the Reasonable Suspicion language concerns. The Chair noted that the lack of clarity on the department's proposed uses is around the EOC activation standards. He wants to see a set of activation standards that are transparent and clear to better support the use of these cameras when there is an activation. However, he proposed supporting the Use Policy if there is a clause requiring a written notification any time the department activates the cameras and uses them to observe Protected Activity.

There was one public speaker, Asada Olugbala who raised serious concern about OPD being under a long-term consent decree and having a history of racial profiling. She believes these cameras will be used disproportionately on African Americans.

With several proposed edits, the PAC unanimously approved forwarding the policy to the City Council.

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

There was minor discussion about some of the uses listed in the Use Policy but the item was continued to a later meeting due to the time.

OAKLAND POLICE DEPARTMENT

Surveillance Impact Report:

Forensic Logic, Inc. CopLink Search and Crime Report System

---

1. 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 complex algorithm that allows OPD crime analysts to produce various crime reports such as point in time year-to-date and year-to-year comparisons. The algorithm takes thousands of penal code types and organizes the data 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) / record management system (RMS) crime incident data, as well as from county arrest, booking, and jail records.

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 and extract entities and relationships from the data. The original LEAP search system allowed for 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 CopLink.

2. Proposed Purpose

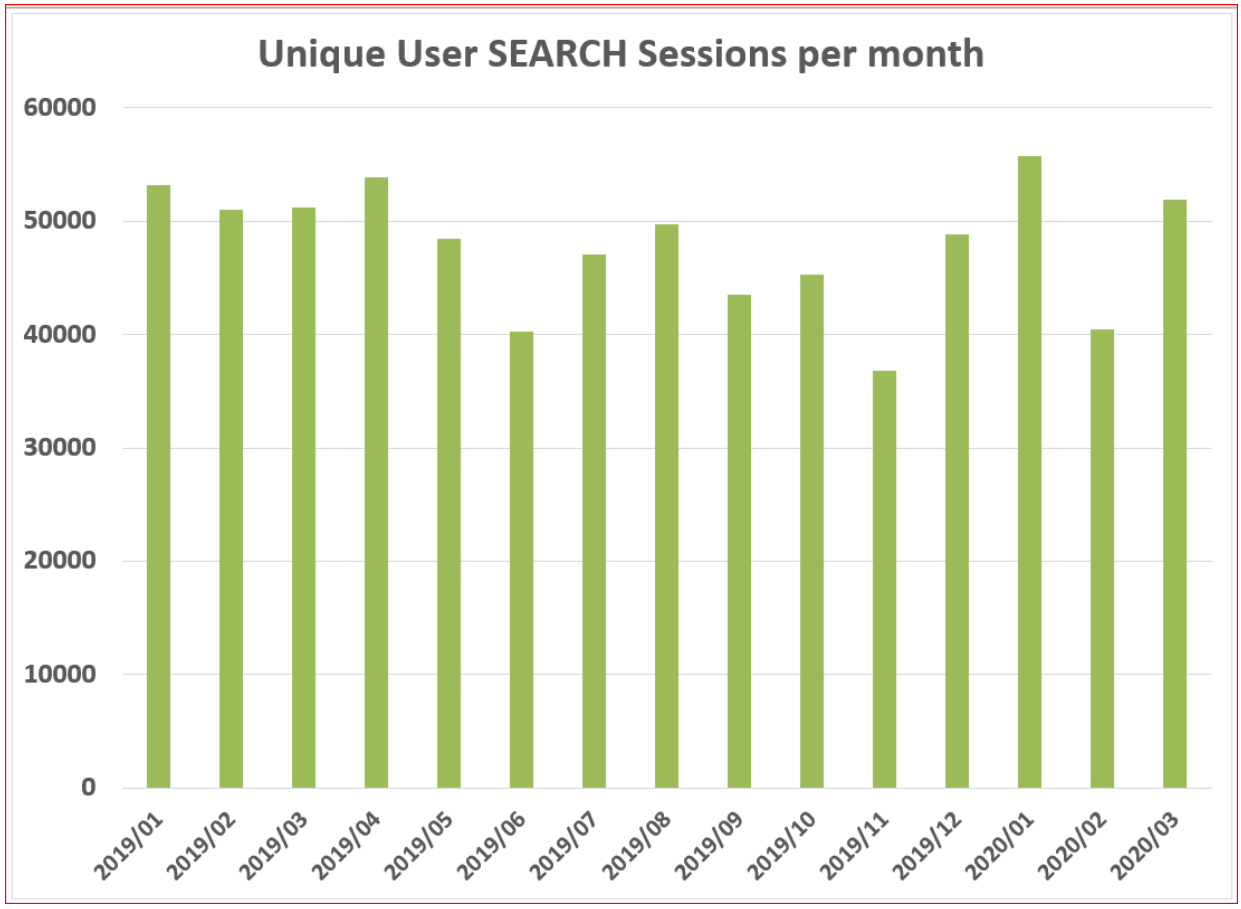
Forensic Logic provides three core services for OPD: a) crime analysis report production; b) search; and c) technical assistance**.**

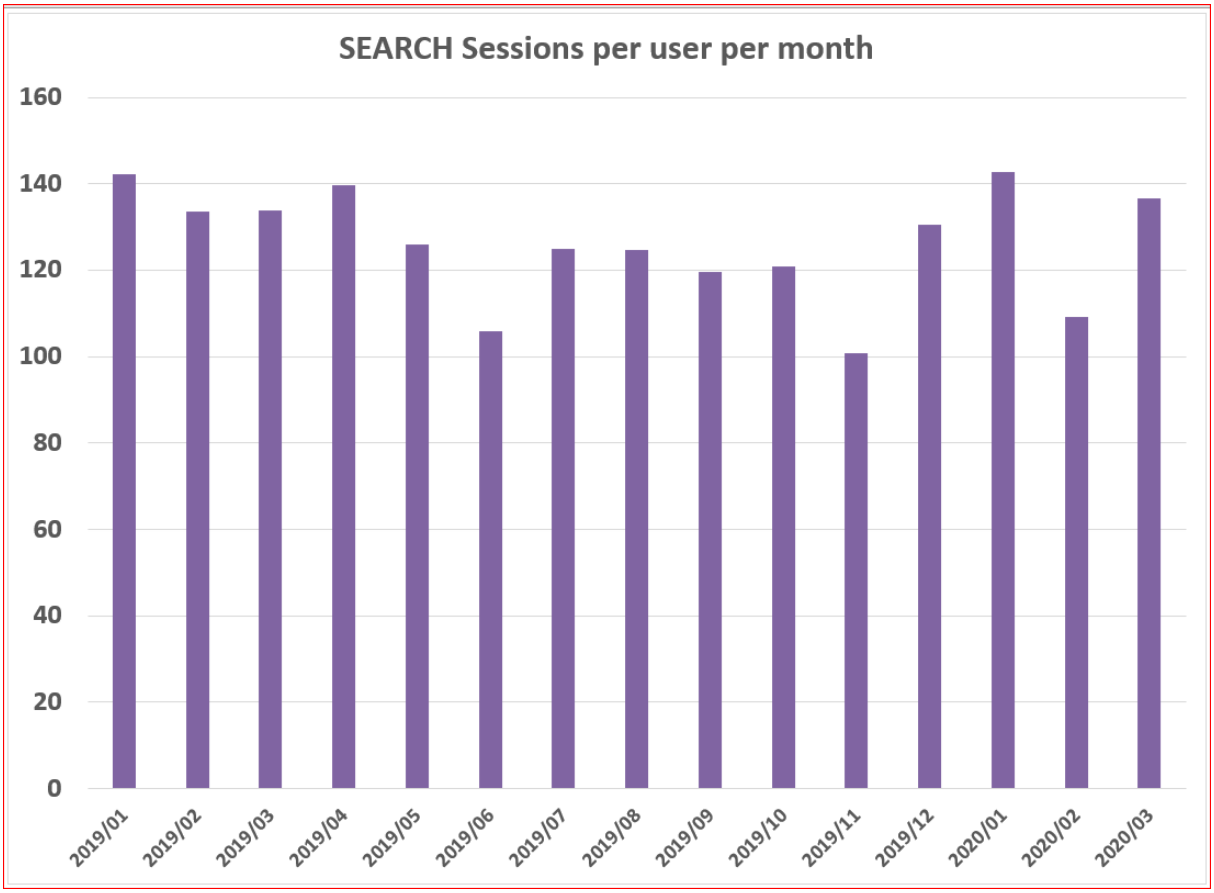
a. Crime Analysis Report Production – Forensic Logic has built a complex algorithm that allows OPD crime analysts to better

access OPD's own data - the algorithm 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.

b. 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 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



CopLink: Critical Tool for Crime Investigations

Criminal Investigation Division (CID) investigators use LEAP/CopLink 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**.**

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

- 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 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.

c. 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.

3. 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 algorithm 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.

4. 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 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, Customs and Border Protection, or

the Department of Health and Human Services, Office of Refugee Resettlement. Additionally, the California Values Act (SB 54[2]) 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 potential 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, OPD has never allowed its ALPR data to be entered into Forensic LEAP Search or CopLink – even though many other participating agencies share ALPR data, and OPD can benefit from these data commingled in the CopLink system.

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, OPD has never allowed its ALPR data to be entered into Forensic LEAP Search or CopLink – even though many other participating agencies share ALPR data, and OPD can benefit from these data commingled in the CopLink system.

5. 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. 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 7 below (data security) provides an in-depth explanation of the many ways the CopLink system itself is secure to data breaches. Data that is deleted from OPD CAD/RMS or other systems is automatically deleted from CopLink. OPD can also request that OPD data be expunged from CopLink where appropriate based on changes to incident files.

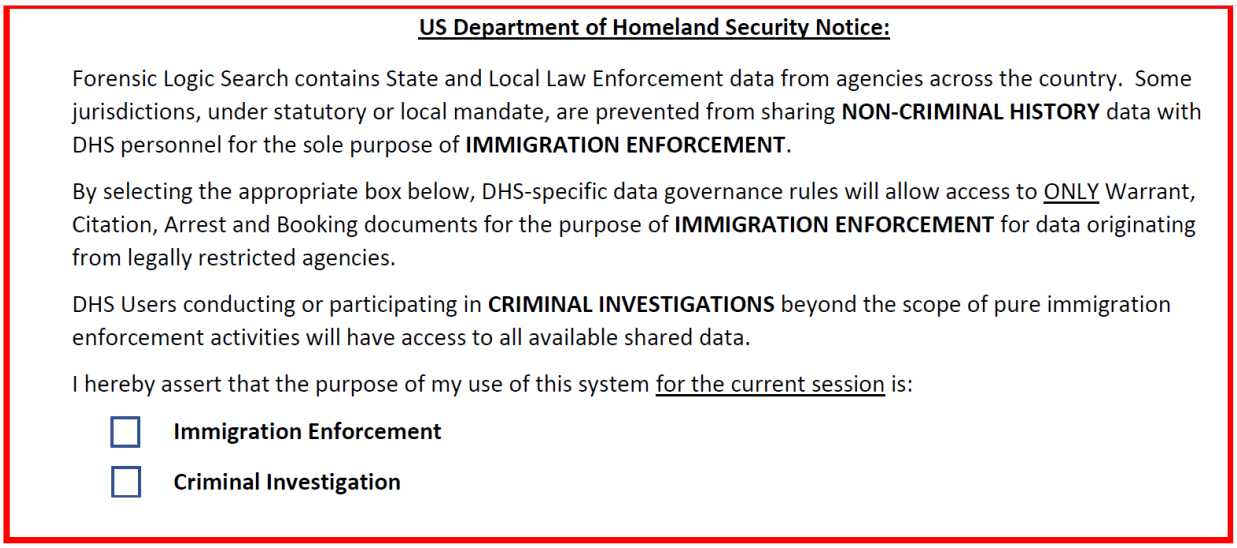
Forensic Logic partners with federal agencies: the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), the FBI, and the U.S. Marshals Service (two of the 94 U.S. Attorney Districts). Forensic Logic did have one contract with Immigrations, Customs and Enforcement (ICE) that expires on May 22, 2020, and there is the possibility of future Forensic Logic-ICE agreements.

Forensic Logic has created technical mitigations to ensure that cities in California and elsewhere can use 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 CopLink system

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

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 United States Homeland Security Investigations (HSI) and Immigrations and Customs Enforcement (ICE).

Police agencies using CopLink can also require that federal agencies that are involved in a criminal investigation utilizing CopLink have access to the data they need to protect communities - but be restricted from such data if such use is for immigration enforcement purposes.. CopLink uses 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**

6. 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 eTrace[3] data. Additionally, OPD is discussing the possibility of incorporating National Integrated Ballistic Information Network (NIBIN) firearm shell casing data into the system.

7. 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[4]. Forensic Logic, along with their partner at Microsoft Azure

[3] https://www.atf.gov/resource-center/fact-sheet/fact-sheet-etrace-internet-based-firearms-tracing-and-analysis
[4] https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center

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. Legacy 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.

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)[5], 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[6] certificates and FIPS 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. 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 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,

---

[5] https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final

[6] 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

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.

8. Costs

.

9. 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 and CopLink system create a unique product with national scope.

10. Alternatives Considered

No other product or company can provide the local, regional and national law enforcement data needed by OPD to assist in criminal investigations. In the case investigators actually know which agency may useful information, they can contact that agency (e.g., BART Police), and ask that 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.

OPD would also 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 until that process in complete later in 2020 or 2021, OPD needs 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.

11. Track Record of Other Entities

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

Counties of San Francisco, San Diego, Los Angeles. Santa Barbara, and the Spokane WA area are underway.

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

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

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

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

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

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

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

DEPARTMENTAL GENERAL ORDER

I-24: FORENSIC LOGIC COPLINK

Effective Date:

Coordinator: Electronic Services Unit and Special Operations Division

---

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

I. VALUE STATEMENT

The purpose of this policy is to establish guidelines for the use of the Forensic Logic, Inc. 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.

II. DESCRIPTION OF THE TECHNOLOGY

A. Forensic CopLink Components

Forensic Logic, Inc. ("Forensic Logic") is a technology company that incorporates law enforcement digital data into a secure cloud-hosted computer server environment. The company integrates data such as from computer-assisted dispatch (CAD) and Records Management Systems (RMS) from different law enforcement agencies. The company has built an intuitive search system (formerly known as LEAP, now as Forensic CopLink) to access law enforcement data. The search can connect data such as criminal suspect name and/or known locations, motor vehicles, recovered crime scene firearms or shell casings. The cloud-based search system is accessible via internet web browser from vehicle mobile data terminal (MDT), web-enabled computers on the OPD computer network, or via OPD-issued and managed mobile devices.

B. Purpose – Forensic Logic CopLink

Forensic Logic provides two core services for OPD: 1) crime analysis reports; and 2) data search

1. Crime Analysis Report Production – Forensic Logic has built a complex algorithm that allows OPD crime analysts to produce crime analysis reports such as point in time year-to-date and year-

to-year comparisons. The algorithm 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 integrated with other agency law enforcement data. Personnel can use the system to search for data (e.g. names of individual (suspect or victim, or vehicle license plates).

III. GENERAL GUIDELINES

A. Authorized Use

All sworn personnel as well as authorized auditors, crime analysists, evidence technicians and certain other assigned other staff may access the system. Personnel authorized to use Forensic CopLink shall be instructed on its use by their supervisor designee.

B. Restricted Use

Department members 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, or for crime analysts to produce crime reports.

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 an investigation.

IV. FORENSIC COPLINK DATA

A. Data Collection

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 eTrace data. Additionally, OPD is discussing the possibility of incorporating National Integrated Ballistic Information Network (NIBIN) firearm shell casing data into the system.

B. Data Retention

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 CopLink. OPD can also request that OPD data be expunged from CopLink where appropriate based on changes to incident files.

C. Data Access

1. OPD data in the CopLink system is owned by OPD and not Forensic Logic and is drawn from OPD underlying systems. The CopLink System and Forensic Logic Crime Report systems are designed for law enforcement. The system contains OPD data (and data of other agencies) that originate in other OPD technologies (e.g., CAD/RMS, or Field Based Reporting modules). OPD personnel shall follow the public access policies set forth in the policies and protocols 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.

D. Data Protection and 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. 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.

V. COPLINK ADMINISTRATION

A. System Coordinator / Administrator

1. OPD's IT Unit will appoint assign personnel to be responsible for ensuring system access and coordinate with Forensic Logic.

2. Legacy 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.

3. 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 CopLink and Crime Reporting modules during the previous year. The report shall include all report components compliant with Ordinance No. 13489 C.M.S.

B. Maintenance

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

C. Training

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

D. Auditing and Oversight

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

By Order of

Susan E. Manheimer

Chief of Police Date Signed:

DEPARTMENTAL GENERAL ORDER

I-25: UNMANNED AERIAL SYSTEM (UAS)

Effective Date:

Coordinator: Electronic Services Unit, Special Operations Division

---

UNMANNED AERIAL SYSTEMS (UAS)

The purpose of this order is to establish Departmental policy and procedures for the use of Unmanned Aerial Systems.

I. VALUE STATEMENT

The purpose of this policy is to establish guidelines for the use of unmanned aerial systems (UAS) and for the storage, retrieval, and dissemination of images and data captured by UAS.

II. DESCRIPTION OF THE TECHNOLOGY

A. UAS Components

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

- A UAV, composed of:
  - Chassis with several propellers for flight
  - Control propellers and other flight stabilization technology (e.g. accelerometer, a gyroscope),
  - Radio frequency and antenna equipment to communicate with a remote-control unit;
  - A computer chip for technology control;
  - A camera; and

- A digital image/video storage system for recording onto a digital data memory card;
- A remote-control unit; and
- Battery charging equipment for the aircraft and remote control.

B. Purpose

UAS have been used to save lives and protect property and can detect possible dangers that cannot otherwise be seen. UAS can support first responders in hazardous incidents that would benefit from an aerial perspective. In addition to hazardous situations, UAS have applications in locating and apprehending subjects, missing persons, and search and rescue operations as well as task(s) that can best be accomplished from the air in an efficient and effective manner. Any use of a UAS will be in strict accordance with constitutional and privacy rights and Federal Aviation Administration (FAA) regulations.

C. How the System Works

1. The FAA Modernization and Reform Act of 2012 provides for the integration of civil unmanned aircraft systems into national airspace by September 1, 2015.
2. UAS are controlled from a remote-control unit. Drones can be controlled remotely, often from a smartphone or tablet. Wireless connectivity lets pilots view the drone and its surroundings from a birds-eye perspective. Users can also leverage apps to pre-program specific GPS coordinates and create an automated flight path for the drone. Another wirelessly-enabled feature is the ability to track battery charge in real time, an important consideration since drones use smaller batteries to keep their weight low.
3. UAS have cameras so the UAS pilot can view the aerial perspective.
4. UAS use secure digital (SD) memory cards to record image and video data; SD cards can be removed from UAS after flights to input into a computer for evidence.

III. GENERAL GUIDELINES

A. Authorized Use

1. Any use of a UAS will be in strict accordance with constitutional and privacy rights and Federal Aviation Administration (FAA) regulations. UAS operations should be conducted in accordance with FAA approval.
2. Only authorized operators who have completed the required training shall be permitted to operate the UAS.

3. UAS may only be used for the following specified situations:
    a. Mass casualty incidents (e.g. large structure fires with numerous casualties, mass shootings involving multiple deaths or injuries);
    b. Disaster management;
    c. Missing or lost persons;
    d. Hazardous material releases;
    ~~d.~~e. Sideshow events where many vehicles and reckless driving is present;[CB1]
    ~~e.~~f. Rescue operations;
    ~~Large or sSpecial events;~~
        ~~i. Such as, large gatherings of people on city streets, sporting events, or large parades or festivals (see authorization for "large or special events under Deployment Authorization below).~~
    ~~f.~~g. Training;
    ~~g.~~h. Hazardous situations which present a high risk to officer and/or public safety, to include:
        i. Barricaded suspects;
        ii. Hostage situations;
        iii. Armed suicidal persons;
        iv. Arrest of armed and/or dangerous persons (as defined in OPD DGO J-04 "Pursuit Driving" Appendix A, H "Violent Forcible Crime");
        v. Scene documentation for evidentiary or investigation value (e.g. crime, collision, or use of force scenes);
        vi. Operational pre-planning (planning (prior planning for services of search and arrest warrants. This is would provide up-to-date intelligence (e.g. terrain, building layout) so that personnel allocate appropriate resources and minimize last minute chance encounters and uses of force); and
        vii. Service of high risk search and arrest warrants involving armed and/or dangerous persons (as defined in OPD DGO J-04 "Pursuit Driving" Appendix A, H "Violent Forcible Crime"; and
        viii. Exigent circumstances
        ix. A monitoring commander (Lieutenant or above) may authorize a UAS deployment under exigent

circumstances. A report shall be completed and forwarded to the Chief of Police and the OPD UAS Coordinator for all UAS deployments authorized under exigent circumstances, for a full review to determine policy compliance.

~~vii. Service of search and arrest warrants.~~

4. **Deployment Authorization**

a. Deployment of OPD UAS

i. Deployment of an OPD UAS shall require the authorization of the incident commander, who shall be of the rank of Lieutenant of Police or above.

ii. Incident commanders of a lower rank may authorize the use of a UAS during exigent circumstances. In these cases, authorization from a command-level officer shall be sought as soon as is reasonably practical.

~~**Deployment Authorization for Large or Special Events**~~

~~Upon notification, the Special Operations Division Commander or designee (Incident Commander) shall develop a written operations plan. The Incident Commander shall be responsible for the overall coordination of the event as well as for crowd control and management.~~

~~Operations plans for large events requiring the use of UAS and / or the redeployment of personnel from regular assignments shall be approved by the Deputy Chief of Field Operations.~~

~~The following factors shall be considered and addressed in developing the operations plan for a large crowd event, including but not limited to:~~

~~What type of event is to occur?~~

~~Who are the organizers? What is their past record of conduct (peaceful, violent, cooperative, etc.)?~~

~~Will outsiders visibly and/or physically oppose the planned event?~~

~~Will the event involve the use or abuse of alcohol or other substances?~~

- ~~Where is the event to occur? The Incident Commander shall consider the size, location, and ingress and egress points.~~
- ~~What is the optimal site for a command post as well as staging areas?~~
- ~~Have the appropriate event permits been issued?~~
- ~~Have other agencies, bureaus, and divisions been notified and included in the planning process (paramedics, fire department, Communications, Intel, etc.)?~~
- ~~Will the EOC be needed? Is Mutual Aid needed?~~
- ~~Will off-duty personnel be involved? Has the commander of any off-duty personnel been made part of the planning process?~~

ii. ~~Is it possible and appropriate to coordinate with group organizers and explain the Department's mission, preparation, and potential responses?~~

5. Deployment Logs

a. ESU shall record details from each UAS deployment onto a flight log which shall be submitted to ESU, and kept on file for FFA records purposes.

b. Flight logs will provide all mission deployment details for each flight.

6. Privacy Considerations

a. O~~Absent a warrant or exigent circumstances, o~~perators and observers shall adhere to FAA altitude regulations.

b. Operators and observers shall not intentionally record or transmit images of any location where a person would have a reasonable expectation of privacy (e.g. residence, yard, enclosure). When the UAS is being flown, operators will take steps to ensure the camera is focused on the areas necessary to the mission and to minimize the inadvertent collection of data about uninvolved persons or places. Operators and observers shall take reasonable precautions, such as turning imaging devices away, to avoid inadvertently recording or transmitting images of areas where there is a reasonable expectation of privacy.

B. Restricted Use

1. UAS shall not be equipped with any weapon systems or analytics capable of identifying groups or individuals, including but not limited to facial recognition or gait analysis.

2. UAS and remote control units shall not transmit any data except to each other. Data shall only be recorded onto removable SD cards.

3. UAS shall not be used for the following activities:

    a. For any activity not defined by "Authorized Use" Part 3 above.

    b. Conducting ~~random~~ surveillance not related to an authorized operation;

    c. Targeting a person based on their individual characteristics, such as but not limited to race, ethnicity, national origin, religion, disability, gender, clothing, tattoos, and/or sexual orientation when not connected to actual information about specific individuals related to criminal investigations.

    d. For the ~~sole~~ purpose of harassing, intimidating, or discriminating against any individual or group.

    e. To conduct personal business of any type.

C. Communications

Notifications will be made to the Communications Section [2][SB3]for notifying patrol personnel, when UAS operations are authorized by a Commander.

IV. UAS DATA

A. Data Collection

The video recording only function of the UAS shall be activated whenever the UAS is deployed, and deactivated whenever the UAS deployment is completed. The UAS operator will rely on SD Cards for video recordings.[SB4][SB5]

B. Data Retention

Video recording collected by OPD UAS shall be deleted from the ~~device within~~device within five (5) days unless:

1. The recording is needed for a criminal investigation;
2. The recording is related to an administrative[BH6] investigation; or;
3. Retention of data is necessary for another organizational or public need.
    a. The program coordinator shall develop procedures to ensure that data are retained and purged in accordance with applicable record retention schedules.[BH7]

C. Data Access

OPD's Electronic Services Unit (ESU) shall be responsible for the maintenance and storage of UAS equipment. Members approved to access UAS equipment under these guidelines are permitted to only access the data for administrative or criminal investigation purposes.

UAS image and video data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law, using the following procedures:

1. The agency makes a written request for the OPD data that includes:
    a. The name of the requesting agency.
    b. The name of the individual making the request.
    c. The basis of their need for and right to the information.
        i. 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 an investigation.
2. The request is reviewed by the Chief of Police, Assistant Chief of Police, or Deputy Chief/ Deputy Director or designee and approved before the request is fulfilled.
3. The approved request is retained on file, and incorporated into the annual report pursuant to Oakland Municipal Code Section 9.64.010 1.B.

D. Data storage, access, and security

The program coordinator shall develop procedures to ensure that all UAS SD card data intended to be used as evidence are accessed, maintained, stored and retrieved in a manner that ensures its integrity as evidence. These procedures include strict adherence to chain of custody requirements.

Electronic trails, including encryption, authenticity certificates, and date and time stamping shall be used as appropriate to preserve individual rights and to ensure the authenticity and maintenance of a secure evidentiary chain of custody.

E. Data Sharing

UAS systems deployed by OPD shall not share any data with any external organizations via integrated technology. T~~;~~ ~~t~~he UAS only sends data to the flight controller via encrypted radio signals – there is no internet connection for external data sharing.

UAS data which is collected and not retained under subsection B of this section is considered a "law enforcement investigatory file" pursuant to Government Code § 6254, and shall be exempt from public disclosure. UAS data which is retained pursuant to subsection B [BH8]shall be available via public records request pursuant to applicable law regarding Public Records Requests.[SB9][SB10]

F. Data Protection and Security

All UAS SD card data will be will be secured in a manner (e.g. lockbox) only accessible to ESU personnel. All evidence from UAS SD cards shall be submitted to the OPD Evidence Unit for safe storage.

V. UAS ADMINISTRATION

A. System Coordinator / Administrator

1. The ESU will appoint a program coordinator who will be responsible for the management of the UAS program. The program coordinator will ensure that policies and procedures conform to current laws, regulations and best practices. The program coordinator shall be responsible for the following program administration responsibilities.
2. The ESU Unit Supervisor, or other designated OPD personnel shall provide the Chief of Police, Privacy Advisory Commission, and City Council with an annual report that covers all use of the UAS technology during the previous year. The report shall include all report components compliant with Ordinance No.

13489 C.M.S.

3. **FAA Certificate of Waiver or Authorization (COA)**

COA (Certificate of Authorization) given by the FAA which grants permission to fly within specific boundaries and perimeters. The UAS Coordinator ~~ACSO~~ will maintain current COA's consistent with FAA regulations. The ESU Unit Supervisor, or other designated OPD personnel, shall coordinate the application process and ensure that the COA is current.

4. **Submission and evaluation of requests for UAS use**

The ESU Unit Supervisor, or other designated OPD personnel, shall develop a uniform protocol for submission and evaluation of requests to deploy a UAS, including urgent requests made during ongoing or emerging incidents.

B. Facilitating law enforcement requests

The ESU Unit Supervisor, or other designated OPD personnel, shall facilitate law enforcement [CB11]access to images and data captured by UAS.

C. Program improvements

The ESU Unit Supervisor, or other designated OPD personnel, shall recommend and accept program improvement suggestions, particularly those involving safety and information security.

D. Maintenance

The ESU Unit Supervisor, or other designated OPD personnel, shall develop a UAS inspection, maintenance and record-keeping protocol to ensure continuing airworthiness of a UAS, and include this protocol in the UAS procedure manual.

E. Training

The ESU Unit Supervisor, or other designated OPD personnel, shall ensure that all authorized operators and required observers have completed all required FAA and department-approved training in the operation, applicable laws, policies and procedures regarding use of the UAS.

F. Auditing and Oversight

The ESU Unit Supervisor, or other designated OPD personnel, shall develop a protocol for documenting all UAS uses in accordance to this policy with specific regards to safeguarding the privacy rights of the community and include this in the UAS procedure manual~~.~~ and the annual UAS report. The UAS supervisor will develop an electronic record of time, location, equipment, purpose of deployment, and number of UAS

personal involved. Whenever a deployment occurs the operator will send notification/submit (either electronically or hard copy) to the UAS Supervisor to include the topics listed above. This protocol will allow the UAS supervisor to have a running log of all deployments and assist in the annual report.

G. Reporting

The ESU Unit Supervisor, or other designated OPD personnel, shall monitor the adherence of personnel to the established procedures and shall provide periodic reports on the program to the Chief of Police.

The ESU Unit Supervisor, or other designated OPD personnel, shall provide the Chief of Police, Privacy Advisory Commission, and City Council with an annual report that contains a summary of authorized access and use.

H. Training

The ESU Unit Supervisor, or other designated OPD personnel, shall develop an operational procedure manual governing the deployment and operation of a UAS including, but not limited to, safety oversight, use of visual observers, establishment of lost link procedures and secure communication with air traffic control facilities.

By Order of

~~Anne E. Kirkpatrick~~….

Chief of Police Date Signed:

OAKLAND POLICE DEPARTMENT
Surveillance Impact Report:
Unmanned Aerial Systems (UAS)

---

1. Information Describing Unmanned Aerial Systems (UAS) and How They Work

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

- A UAV which consists of the chassis with several propellers for flight, radio frequency and antenna equipment to communicate with a remote-control unit, control propellers and other flight stabilization technology (e.g. accelerometer, a gyroscope), a computer chip for technology control, a camera for recording, and a digital image/video storage system for recording onto a secure digital card (SD card);
- A remote-control unit that communicates with the UAV via radio frequency; and
- A battery charging equipment for the aircraft and remote control.

UAS are controlled from a remote-control unit (similar to a tablet computer). Wireless connectivity lets pilots view the UAS and its surroundings from a bird's-eye perspective.

UAS have cameras so the UAS pilot can view the aerial perspective. UAS record image and video data onto a secure digital (SD) memory cards. SD cards can be removed from UAS after flights to input into a computer for evidence.

2. Proposed Purpose

UAS offer to significantly improve the capacity of law enforcement (LE) to provide a variety of foundational police services. This technology has already been used with many law enforcement agencies to save lives and help

capture dangerous criminal suspects. UAS can support first responders in hazardous incidents that would benefit from an aerial perspective. Responding to violent crime in Oakland often requires officers to face risks to their safety – in addition to the clear risks faced by members of the public when violent crime is present. In 2019 Oakland saw 75 homicides, 3,334 aggravated assaults (284 with firearms), 189 rapes, and 2,789 robberies. OPD relies on policies and procedures to mitigate the possibility that attempts to arrest crime suspects will not lead to the injury of bystanders or officers. Technology such as UAS can play a vital role in further mitigating these omnipresent dangers, by providing a greater view into the immediate surroundings of crime scenes and active pursuits.

~~Better situational awareness also mitigates against conditions that lead to bodily injury of suspects and LE personnel.~~ Searches for armed and dangerous suspects are more effective and controlled with UAS support; an armed suspect can be hiding in a tree or on a roof. LE can respond accordingly and more safely when provided with this critical information (see Section #10 below "Alternatives Considered" for more information on how UAS compares to alternatives for situational awareness). More informed responses also lead to less injury and less uses of force.

LE agencies have successfully used UAS to locate missing persons, especially in more remote areas – as well as for rescue missions. UAS is also being used during disasters and during any hazardous material releases The situational awareness UAS provides has also become an important tool for large events (e.g. sport events, parades, and festivals); the aerial view provides information that would otherwise require a much larger deployment of LE personnel to maintain the same level of public safety support. ~~LE agencies have successfully used UAS to locate missing persons, especially in more remote areas – as well as for rescue missions. UAS is also being used during disasters and during any hazardous material releases~~ Additionally, UAS offer LE a more efficient system for documenting vehicular collision as well as crime scenes. Furthermore, smaller UAS can be equipped with a loud speaker to communicate (e.g. hostage situations/providing verbal commands and directions to the subject).

As Bryan Smith, APSA[1] Safety Program Manager explains in "Working Together: Deploying Manned and Unmanned Aircraft Safely and Successfully" in Air Beat[2]-July-August 2019 Issue, "What if we (LE) had the ability to coordinate tasking, splitting the airborne support responsibilities between manned (helicopter) and unmanned crews so one could watch the perimeter while another searches below treetop level in the courtyards and windows and a third went head of the entry team?" In the same AirBeat Issue, Charles L. Werner, Chairman, National Council on Public Safety U.S. explains in "Public Safety Drones: The Past, Present, and Future," "Virginia's

[1] APSA = Airborne Public Safety Association

[2] The Official Journal of the Airborne Public Safety Association

public safety UAS team in York County used one of its drones to fly into a hostage situation to determine when police could safely enter." The article also details how the Alameda County Sheriff's Office (ACSO) is using its drones for traffic incidents, tactical operations, and search and rescue.

OPD does have access to ACSO UAS. However, OPD must make a formal request for each use. This approval process takes several hours when situations require immediate action. Circumstances may proceed without any time for advance planning and conditions may involve individuals believed to be armed and dangerous. OPD can better respond to such dangerous situations where UAS offers useful intelligence and mitigates officer danger – by having a separate UAS program; a standalone OPD UAS program will allow for much quicker deployment options.

3. Locations Where, and Situations in which UAS may be deployed or utilized.

OPD proposes to use UAS as outlined in OPD Department General Order (DGO) I-25 "UNMANNED AERIAL SYSTEM (UAS)," Section III "General Guidelines" A "Authorized Use" only for the following situations:

a. Mass casualty incidents (e.g. large structure fires with numerous casualties, mass shootings involving multiple deaths or injuries);
b. Disaster management;
c. Missing or lost persons;
d. Hazardous material releases;
e. Sideshow events where many vehicles and reckless driving is present;
f. Rescue operations;
g. Special events;
    i. Such as large gatherings of people on city streets, sporting events, or large parades or festivals; (see authorization for "large or special events under Deployment Authorization below);
h. Training;
i. Hazardous situations which present a high risk to officer and/or public safety, limited to:
    i. Barricaded suspects;
    ii. Hostage situations;
    iii. Armed suicidal persons;
    iv. Arrest of armed and/or dangerous persons (as defined in OPD DGO J-04 "Pursuit Driving" Appendix A, H "Violent Forcible Crime";

Commented [CB1]: Does this belong under Hazardous situations?

v. Scene documentation for evidentiary or investigation value (e.g. crime, collision, or use of force scenes);

vi. Operational pre-planning (prior planning for services of search and arrest warrants. This is would provide up-to-date intelligence (e.g. terrain, building layout) so that personnel allocate appropriate resources and minimize last minute chance encounters and uses of force);

vii. Service of high risk search and arrest warrants involving armed and/or dangerous persons (as defined in OPD DGO J-04 "Pursuit Driving" Appendix A, H "Violent Forcible Crime"; and

viii. Exigent circumstances

i. A monitoring commander (Lieutenant or above) may authorize a UAS deployment under exigent circumstances. A report shall be completed and forwarded to the Chief of Police and the OPD ~~Department~~ UAS Coordinator for all UAS deployments authorized under exigent circumstances, for a full review to determine policy compliance. ~~At the direction of a command officer.~~

Potentially, UAS could be deployed in any location in the City of Oakland where one or more of the above situations occur and where the proper authorizations are provided. Fortunately, several of these situations rarely occur – but some do occur regularly, as such arresting armed/dangerous person, and crime scene documentation. OPD regularly needs to document crime, use of force, and/or vehicular collision scenes for evidentiary and/or investigation value. UAS can greatly aid in this documentary process, to memorialize a scene from an aerial or overview perspective. In 2018, OPD made 8,239 arrests that included either a felony charge, a misdemeanor charge that required an arrest (warrant, domestic violence, firearms violation), or both. In 2018 there were 70 homicides, 2,624 robberies, and 2,338 reported cases of aggravated assault. Additionally, OPD continues to authorize the use of armored vehicles several times each month where personnel attempt to safely locate individuals suspected in homicides and other violent crimes – UAS can provide situational awareness in many of these cases to provide a greater level of safety for officers as well as for nearby bystanders. ~~Furthermore, smaller UAS such as the DJI Mavic that OPD may purchase, are equipped with a loud speaker; such UAS can be used for one-way communication during several of the use-cases described in this section above (e.g. hostage situations/providing verbal commands and directions to the subject).~~

Formatted: Highlight

Commented [SB2]: Moved to Sec 2

4. Privacy Impact

OPD recognizes that the use of UAS raises privacy concerns. UAS are becoming ubiquitous in the United States, and there is a growing concern that people can

be surveilled without notice or reason. There is concern that UAS can be utilized to observe people in places, public or private, where there is an expectation of privacy. The level of potential privacy impact depends upon factors such as flight elevation and camera zoom magnitude, as well as where the UAS is flown.

The results of the research study titled, "Mission-based citizen views on UAV usage and privacy: an affective perspective[3]," published in February 2016 found that people's perceptions of how UAS impacts privacy relate to use type. The researchers from College of Aeronautics, Florida Institute of Technology, and the Aeronautical Science at Embry-Riddle Aeronautical University (ERAU), College of Aviation UAS Lab found that people tend to be less concerned about police UAS use when the technology is only used for specific uses - "concerns for privacy were less in the condition where the UAV was only used for a specific mission than when it was operated continuously." DGO I-25.III.A "General Guidelines, Authorized Use" explains that OPD personnel can only use UAS for specific missions, detailed above in Section 3 "Locations Where, and Situations in which UAS may be deployed or utilized."

OPD cannot, for the most part, control how private individuals use these systems as the technology available to anyone continues to improve. The Federal Aviation Administration (FAA), however, does set strict flight regulations for all UAS users, including for law enforcement. The FAA provides two law enforcement options for creating acceptable UAS programs (see ***Attachment A: "Drones in Public Safety: A Guide to Starting Operations***"), under 14 Code of Federal Regulation (CFR) part 107, subpart E, Special Rule for Model Aircraft; the agency can designate individual members to earn FAA drone pilot certificates and fly under the rules for small UAS, or receive a FAA certificate to function as a "public aircraft operator" to self-certify agency drone pilots and drones. Either way, these options allow for OPD to use systems under 55 pounds, for flying at or below 400 feet above ground level[4]. Absent an emergency situation warranting a FAA COA/Part 107 waiver-permitted law enforcement response, law enforcement is also restricted from using UAS to fly over or near the following locations:

- Stadiums and Sporting Events;
- Near Airports; and
- Emergency and Rescue Operations (wildfires and hurricanes).

Commented [CB3]: This is not a privacy concern, and most of it isn't relevant to privacy. Suggest moving relevant cite (re: height) to Mitigations section below, and deleting rest.

5. Mitigations

OPD's DGO I-25 restricts OPD's use of UAS in several ways to promote greater privacy protections.

OPD will only use UAS for specific missions rather than operating

[3] https://www.nrcresearchpress.com/doi/abs/10.1139/juvs-2015-0031#.XkHEAWhKiUl

[4] Under FAA guidelines, in the case of emergency where a law enforcement agency cannot fully comply with existing regulations under their Certificate of Authorization (COA) or part 107, a law enforcement agency can request an emergency, temporary amendment to an existing COA, or, if without a COA, obtain a temporary, emergency airspace authorization for a limited period of time at specified locations.

continuously, mitigating concerns raised in the February 2016 study cited above.

DGO I-25.III "General Guidelines," A."Authorized Use" Part 3 lists the only allowable uses of UAS (e.g. mass casualty incidents, Arrest of armed and/or dangerous persons (as defined in OPD DGO J-04 "Pursuit Driving" Appendix A, H "Violent Forcible Crime")). DGO I-25.III.A.4 "Deployment Authorization" articulates that an Incident Commander must approve all uses of UAS. DGO I-25.III.A.4 "Deployment Authorization for Large or Special Events" lists the additional requirements for using UAS during these situations; this additional deployment list is required so that OPD considers the need for situational awareness in the context of not restricting the rights of Oakland residents and visitors to freedom of expression in the public domain.

DGO I-25.III.A."Authorized Use," Part 7 "Privacy Considerations," outlines several protocols for mitigating against privacy abuse:

- OPD UAS personnel must adhere to FAA altitude guidelines – flying below 400 feet helps to ensure that UAS is not used for surveilling overly large geographic areas; OPD will use UAS to focus specifically on specific areas.
- OPD UAS operators shall not intentionally record or transmit images of any location where a person would have a reasonable expectation of privacy (e.g. residence, yard, enclosure, place of worship, medical provider's office).
- Operators and observers shall take reasonable precautions, such as turning imaging devices away, to avoid inadvertently recording or transmitting images of areas where there is a reasonable expectation of privacy.

DGO I-25.III.B "Restricted Use" explains that:

- UAS and remote control units shall not transmit any data except to each other.
- Data shall only be recorded onto removable SD cards.
- UAS shall not be used for the following activities:
    - Targeting a person based on their individual characteristics, such as but not limited to race, ethnicity, national origin, religion, disability, gender, clothing, tattoos, and/or sexual orientation when not connected to actual information about specific individuals related to criminal investigations;
    - For the purpose of harassing, intimidating, or discriminating against any individual or group; or
    - To conduct personal business of any type.

The technology itself also provides privacy mitigations through information security. The DJI Matrice 210 and DJI Mavic 2 Enterprise systems both use DJI's "OcuSync 2.0" protocol and are encrypted using the leading AES-256 standard as well as password login protection. DJI[5] uses this encrypted software to turn off the radio transmission to all devices except the paired unit controller. However, there is no guarantee that these drone-to-controller radio transmissions cannot be potentially hacked by bad actors (higher grade military level encryption would be cost-prohibitive for OPD). ~~These protocols help to ensure that drone to controller transmissions cannot be intercepted by 3rd parties, and that the systems themselves cannot be used without authorized permission~~. DJI has produced a "Commitment to Data Security" document (see ***Attachment B***). The document explains protocols undertaken to ensure that flight data is not transmitted back to DJI or other sources (e.g. storing data on a U.S.-based AWS server). DJI's "Implementing Mitigation Measures Recommended By The DHS" (see ***Attachment C***) recommends mitigations that mirror OPD UAS mitigations:

- Deactivate Internet Connection from Device Used to Operate the UAS
- Take Precautionary Steps Prior to Installing Updated Software or Firmware
- Remove Secure Digital Card from the Main Flight Controller/aircraft
- If SD Card is Required to Fly the Aircraft, Remove All Data from the Card After Every Flight

OPD will also commit to using UAS such as from DJI that do not directly connect to the internet; rather, the controllers will use a separate mobile device for possible remote transmission. The UAS have local data built into the controller firmware for flight control.

6. Data Types and Sources

UAS will record using industry standard file types such as (e.g. jpeg, mov, mp4, wav or RAW). Such files may contain standard color photograph, standard color video, or other imaging technology such as thermal. Although UAS can transmit one-way audio from OPD, the UAS technology available today does not currently record sound[6].

[5] The lead UAS manufacturer for equipment used by police agencies throughout the U.S.

[6] Microphones could be installed, but the sound of the propellers would make sound indecipherable in current models available to OPD.

7. Data Security

OPD takes data security seriously and safeguards UAS data by both procedural and technological means. The video recording function of the UAS shall be activated whenever the UAS is deployed. Video data will be recorded onto Secure Digital (SD) Cards. OPD DGO I.25.4.B "Data Retention" states video recording collected by OPD UAS shall be deleted from the device within five (5) days unless:

- The recording is needed for a criminal investigation;
- The recording is related to an administrative investigation; or
- Retention of data is necessary for another organizational or public need when OPD is requested for outside agency criminal investigations, administrative investigations, and/or aiding in natural disasters; the program coordinator shall develop procedures to ensure that data are retained and purged in accordance with applicable record retention schedules (in accordance with DGO I.25.4.B "Data Retention."). Outside agency assist would only be conducted if it is within OPD policies.

The program coordinator shall develop procedures to ensure that all UAS SD card data intended to be used as evidence are accessed, maintained, stored and retrieved in a manner that ensures its integrity as evidence, including strict adherence to chain of custody requirements.

Electronic trails, including encryption, authenticity certificates, and date and time stamping shall be used as appropriate to preserve individual rights and to ensure the authenticity and maintenance of a secure evidentiary chain of custody.

OPD's Electronic Services Unit (ESU) shall be responsible for the maintenance and storage of UAS equipment. Members approved to access UAS equipment under these guidelines are permitted to access the data for administrative or criminal investigation purposes.

UAS image and video data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes, using the following procedures:

- The agency first makes a written request for the OPD data that includes:
    - The name of the requesting agency.
    - The name of the individual making the request.
    - The basis of their need for and right to the information.
        - 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 an

Commented [BH4]: Does this refer to an internal admin investigation, perhaps an internal affairs complaint? Also – no mention of civil discovery or public record requests.

Commented [BH5]: There is no DGO I.25. What is the correct citation?

Commented [BH6]: Per OPD, this is likely DGO I.15 IV B. https://powerdms.com/public/OAKLAND/tree/documents/663735 but this needs some work.

investigation.

- The request is reviewed by the Chief of Police, Assistant Chief of Police, or Deputy Chief/ Deputy Director or designee and must be approved before the request is fulfilled.
- The approved request is retained on file, and incorporated into the annual report pursuant to Oakland Municipal Code Section 9.64.010 1.B.
-

Formatted: Outline numbered + Level: 1 + Numbering Style: Bullet + Aligned at: 0.74" + Indent at: 0.99"

8. Costs

Costs for a UAS program can vary from thousands to hundreds of thousands and beyond. Different types of systems exist that would support police services, and technology continues to evolve. However, OPD personnel have procured some initial bids to start an OPD UAS program. UAS technology updates at a fast pace and we do not want to commit to a current model. The following costs ($46,800 total), provided here as an example, are based on an actual bid for one large UAS and four smaller UAS for different types of missions:

UAS System	Components	Cost
DJI Matrice 210 V2 (one system) – large drone for standard use	Rugged commercial enterprise drone that carry a payload of 5.07 pounds (enough for the powerful zoom camera and infrared camera). System comes with drone body, landing gear, monitor, propellers, battery packs and chargers, cables.	$9,600
	Powerful Zoom lens Camera: Zenmuse Z30 (30x Optical Zoom)	**$2,999**
	Infrared Camera: DJI Zenmuse FLIR XT2 Dual Sensor 640x512 30Hz 13mm Radiometric	$13,200.00
	Six extra batteries: DJI TB55 Intelligent Flight Battery (Extended); $369 x 6	$2,214
	Matrice 200 Series Case	$739
DJI Mavic 2 (four systems) – smaller	Drone body with protection kit, controller, batteries, battery chargers, propellers, cables, other related accessories such as spotlights and one-way speakers;	$11,796

drone for lighter use as well as for indoor use	$2,949 x 4	
	Additional batteries; $169x24	$4,056
	DJI Smart Controller; $549x4	$2,196
		$46,800

OPD will utilize one-time General Purpose Funds and/or look to grant funding such as from the United States Department of Homeland Security Urban Area Security Initiative (UASI).

9. Third Party Dependence

OPD is currently reliant upon the Alameda County Sheriff's Office (ACSO) when exigent circumstances occur that warrant UAS requests. OPD has requested and received UAS support from ACSO four times in 2019. "Use of Unapproved Surveillance Technology Under Exigent Circumstances – January 28, 2019" (see Attachment B) explains the use of ACSO UAS on January 18, 2019 in connection with an OPD observed murder suspect. "Use of Unapproved Surveillance Technology-December 17, 2019" (see Attachment C) December 17, 2018 explains the use of ACSO UAS on December 15, 2018 in connection with a residential (home invasion) robbery in progress with a suspected armed suspect.

OPD values its relationship with ACSO and the UAS support provided in 2019; However, OPD now hopes to join the growing list of municipal police agencies developing their own UAS programs. The "Proposed Purpose" Section 2 above explains the benefit and local need for such situational awareness. There are several vendors currently manufacturing law enforcement enterprise quality systems. Section 8 "Cost" above details a possible purchase from DJI – a leading manufacturer. However, OPD will solicit competitive bids and reevaluate vendors if and this Surveillance Impact Report and connected DGO I.25 Use Policy are approved by the City Council.

Commented [7]: From the Ordinance 12. (I) Third Party Dependence: whether use or maintenance of the technology will require data gathered by the technology to be handled or stored by a third-party vendor on an ongoing basis;

Commented [SB8R7]: If ACSO provides a drone (and pilot) to OPD operations, they will have that data so seems relevant.

10. Alternatives Considered

OPD could continue the status quo by relying on its partnership with ACSO UAS; however, OPD will be able to more efficiently deploy UASs when needed in priority situations, by having its own UAS program. OPD currently relies on ACSO for UAS access, as noted in Section 2 "Proposed Purpose" above. OPD must make a request to ACSO in each time a situation arises that would benefit from UAS use and meets all requirements outlined in the OPD UAS Policy. These requests can take several hours in which case OPD's ability to respond is greatly diminished. In cases such hostage

situations, missing persons, or pursuit of homicide investigation suspects, a two or more-hour request period can lead to negative outcomes.

Helicopters also offer sky-view situational awareness during some of the situations described in the Purpose and Impact sections above, but UAS costs are lower and UAS can be used in more situations. Helicopters cost several million dollars as well as $200-$400 per hour for manned flight. Currently OPD only has one functional helicopter because the high cost to maintain them. There are situations where UAS do not offer an alternative - UAS can never replace the helicopter for missions such as active vehicle pursuits, sustained flight, active observations and communications from the helicopter. UAS can only be compared in terms of some situations where a local above-ground perspective is needed.

The much lower costs of UAS however means that they can potentially be deployed in more situations where the cost of maintaining helicopters is too prohibitive. UAS can also provide utility in ways beyond the capabilities of much more expensive helicopters:

- Support during fire and emergency operations – UAS can be flown in lower elevation positions such as near fires to locate possible trapped people where helicopters cannot fly; infrared cameras on UAS can also be used to identify heat spots for fire department attention.
- Finding suspects – UAS can be used to find dangerous violent crime suspects, by being flown in locations such as to view roof tops, in trees, or between buildings.
- Crime and vehicle collision scene investigation – UAS can be used to collect evidence that may be difficult to reach from the ground; UAS can easily be used to provide maps and 3D images within minutes using 3rd party software specifically designed to produce such maps and 3D images using photographic data captured by the UAS; this data is also valuable during court testimony.
- Finding and/or seizing illegal drones - police UAS can be flown to identify unregistered UAS that may be hazardous to the surrounding environment.

Another alternative to the use of UAS or helicopters would be to deploy many officers to events described in DGO I-25. Section III "General Guidelines" A. "Authorized Use." However, a greater deployment of sworn personnel would at times be less effective; A missing persons' event would require many more officers to provide the same information as UAS. Additionally, the use of UAS can also allow OPD to minimize its physical presence in situations where more officers may actually be perceived as unnecessary and even threatening, during large or special events. Furthermore, large officer deployments can cause a greater use of overtime funding and cause negative impacts to OPD's general fund budget.

Commented [BH9]: This isn't a proposed use. Why is it here?

11. Track Record of Other Entities

Many cities and counties in California and nationwide have begun to implement UAS programs due to the numerous uses cases for law enforcement. The Alameda County Sheriff's Office (ACSO) and Sacramento County Sheriff's Office have developed programs with several types of UAVs and full time deputy positions, and Stanislaus County is beginning to develop their program. Cities such as Citrus Heights, Fremont, Pittsburg, and Torrance all now have UAS programs as well.

Interviews with Citrus Heights PD, Pittsburg PD and the Sacramento County Sheriff's Office all testify to the high use value of developing a UAS program for law enforcement. These agencies have all used UAS for search and rescue missions, emergency situations (e.g. natural gas explosions and fires), and to search for suspects considered armed and dangerous. UAS are also being used by these agencies on a regular basis to document fatal vehicle collision scenes as well as for gunshot scenes to develop 3D models that provide great value for investigations – such capabilities were only possible prior to UAS technology with much more human staff time as well as expensive 3D camera technology.

Citrus Heights PD reported that initially they experienced community concerns around privacy. However, the department was able to explain their plan to community groups, to show how the program is used and the safety and privacy mitigations they employ. The department reports that this approach has led to greater community support. Pittsburg PD also reported that their community did not express any privacy concerns about their UAS program - but that they ensured transparency through proactive UAS Program communications.