CITY OF OAKLAND

Privacy Advisory Commission

February 6, 2020 5:00 PM
Oakland City Hall
Hearing Room 1
1 Frank H. Ogawa Plaza, 1st Floor
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**: vacant **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

2. Open Forum/Public Comment

3. Review and approval of the draft January special meeting minutes

4. Census Team – Presentation on 2020 Census – Informational report only

   Richard J. Luna, Assistant to the City Administrator, will give a presentation regarding the 2020 Census. The 2020 Census will be conducted primarily online and made available in only 13 languages, which makes it a challenge in ensuring a complete count for Oakland. According to the State of California, 57% of Oakland's population lives in hard-to-count Census tracts. Factors that lead to hard-to-count areas in Oakland include: crowded units, renters, multiple families living at a residence, people living below the poverty level, among others. The City of Oakland and County of Alameda have partnered in outreach efforts to ensure everyone is counted during the 2020 Census. Commissioners are encouraged to make a pledge to take the Census, register as a Census Ambassador, and to discuss the importance of the Census with family and friends.

5. Chair report – Informational report only
   a. PAC Annual Report
   b. 2020 Planning and Agenda Management
   c. OPD Tech Priority List
   d. Goldman School of Public Policy – Citizen Data Project

6. Surveillance Equipment Ordinance – OPD – Cell Site Simulator Annual Report (2019) – review and take possible action

7. Surveillance Equipment Ordinance – OPD UAS (Drone) Exigent Use Report – review and take possible action.

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

9. Surveillance Equipment Ordinance – OPD – Mobile ID Impact Report and proposed Use Policy – review and take possible action

10. Adjournment at 7:00pm

CITY OF OAKLAND

Privacy Advisory Commission

January 8, 2020 5:00 PM
Oakland City Hall
Hearing Room 1
1 Frank H. Ogawa Plaza, 1st Floor
Special Meeting Minutes

***Commission Members**: **District 1 Representative**: Reem Suleiman, **District 2 Representative**: Chloe Brown, **District 3 Representative**: Brian M. Hofer, Chair **District 4 Representative**: Lou Katz, **District 5 Representative**: Vacant, **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: Hofer, Suleiman, Brown, Katz, Tomlinson, Oliver, Gage, Patterson.

2. Open Forum/Public Comment

There no Open Forum Speakers.

3. Review and approval of the draft December meeting minutes

The Minutes were approved unanimously.

4. Chief Privacy Officer report - Privacy Principles status update and implementation

Joe DeVries reported that the administration is proposing to bring forward the Privacy Principals to the Public Safety Committee on February 25th which could mean a full Council vote by March 3. He will also be presenting the Principals and the Draft Implementation Roadmap to the Department Directors in early February. There was discussion about Member Suleiman's Implementation Roadmap. Member Patterson had some suggested revisions for the sake of timing early wins that can be implemented without new staff or funding.

5. Chair/Vice Chair report – 2020 planning, PAC annual report, report tracking, agenda management

Chairperson Hofer reviewed the priority list and noted that new priorities came up and there is a need to revisit and reorder the list. The group reached agreement on reprioritizing the list. He also noted changes to the ordinance to allow staggered annual reports to come forward instead of them all coming at the same time each year.

6. Surveillance Equipment Ordinance – OPD – Live Stream Camera Impact Report and proposed Use Policy – review and take possible action

The Live Stream Use Policy was reviewed again with the emphasis on the Emergency Operations Center (EOC) activation process and restrictions on its use to surveille protected activity. Chairperson Hofer raised concern about whether language was added that had been discussed by the ad hoc group. First, he asked about EOC activation standards. DC Holmgren explained it would include any event that requires multiple department such as the PSPS Power Shutoffs. Neither he nor Joe DeVries were aware of a specific protocol for EOC activation but instead noted that there is a list of events that warrant activation. Joe DeVries agreed to follow-up with more information on activation procedures with OFD and the City Administrator to be able to provide a written list or protocol.

Second, Chairperson Hofer recommended that sections from the DAC Policy covering Allowable Uses, Protected Activity, and reporting requirements when the cameras are used to monitor and transmit protected activity be added to this policy. He cited the number of activations that were associated with Protected Activity in the past five years gives him concern about just allowing the use during an activation without further restriction on monitoring Protected Activity. He wants to see an auditing function such as after-the-fact reporting when the cameras are used to monitor Protected Activity (section VIII B of the DAC Policy). Although, he suggested the reporting be annual, not immediately following the use.

Member Oliver noted the PSPS Shut-offs give him concern that even more of those would occur and they would activate the EOC. Member Brown had additional questions about using the cameras to monitor Protected Activity and saw some inconsistencies in the policy regarding hand-held cameras, versus affixing them permanently to a stationary object; she was unclear if additional restrictions were in place when monitoring protected activity. Bruce Stoffmacher noted that the cameras will not be affixed to stationary objects for any use (not just protected activity).

Member Gage added a substantive edit under the authorized use section of the policy (3A), noting that the cameras can be used in certain circumstances AND when authorized by the City Administrator (it currently states OR). He believes both circumstances need to exist. Joe DeVries noted that in an exigent circumstance, that authority would not be needed, instead there would be a report back at the next PAC Meeting. There was a detailed conversation about the meaning of exigency and its unpredictability. Ultimately Member Gage suggested changing both the Impact Statement and Use Policy to say "OR."

Chairperson Hofer proposed amending the Use Policy to include the definition of Protected Activity under Restricted Use and also use section VIIIB and section VII of the DAC Use Policy in the same section but with the reporting taking place annually. This motion passed unanimously.

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

Sgt. Daza-Quiroz presented the overview of this technology and how the department would like to use it. He noted that drones greatly impact officer safety in certain critical incidents such as armed suspects barricaded inside a property. OPD has been looking at developing a policy for 8 months and have closely studied Alameda County's Use Policy for drones. Currently OPD uses Alameda County's drones and the department contemplates purchasing their own for similar uses.

Chair Hofer noted that the PAC has heard and approved four Exigent Use incidents where OPD used the County's drone so this request is no surprise. OPD is looking to purchase 5 devices and has identified funding they can use (through May) to purchase. Bruce Stoffmacher reviewed the Impact Statement and Use Policy noting that there are a lot of incidents these could be used to avoid use of force situations. Some drones have microphones and two way speakers (although the quality is not good due to the noise of the drones).

Chairperson Hofer noted that two-way communication needs to be included in the Use Policy. Member Patterson asked some clarifying questions such as whether they would fly at night since the FAA has restrictions at night. Member Katz asked about the microphone sensitivity, infrared devices (FLIR), and/or other devices that would enhance the drones. Sgt. Michael Chun spoke to this and noted the microphones are only one-way—they allow OPD to speak to the subject but not vice versa. They do not have FLIR or Cell Site Simulator capabilities.

There was dialogue about FAA Regulations and how they may overlap the City's as well as questions about private space versus areas within the right-of-way. Member Brown suggested some additions to the Impact Statement. Member Patterson suggested some Public Education about the use of drones so as to inform the public about how they are used and what data they do (and don't) collect. Sgt. Daza-Quiroz noted that the OPD PIOs can help with this.

The Use Policy was continued to the February meeting so staff can return with the recommendations incorporated into a new draft.

8. Surveillance Equipment Ordinance – OPD – Biometric Data Analysis (DNA Crime Lab) funding request – review and take possible action

DC Holmgren presented this topic as the department is prepared to go to Council to accept funds that will help address its DNA Backlog and the ability to process important evidence in a timely manner with up-to-date equipment. This is an ongoing grant OPD has received for many years but its renewal triggers the approval process built into the Surveillance Technology Ordinance since the department is accepting grant money for technology that is used in surveilling or storing people's personal data (DNA).

This item was not on the original list of existing technologies the department identified when the ordinance was passed so the PAC has evaluated the use. OPD is only seeking support to accept the grant funding and will return with an Impact Statement and Use Policy before anything is purchased.

Dr. Sandra Sachs with the OPD Crime Lab was present and discussed how the equipment is used to analyze DNA Samples that have already been collected. The equipment is 20 years old and needs updating to allow for much faster processing. She answered some questions about typing, individualization and matching processes that are performed both by computers and human analysis.

There was also discussion with Nancy Chang, the City's CODIS Administrator who oversees how samples are shared with the State and the variety of different CODIS Databases the State maintains.

Dr. Sachs raised concern about the approval process impinging on the acceptance of the grant funding. Chairperson Hofer explained that the approval to accept funds will happen this week so as not to delay. The Use Policy process can follow as soon as OPD submits it. DC Holmgren confirmed the department can bring back a policy in the next two months giving the department time to still use the that money in a timely manner.

The PAC voted unanimously to recommend to the City Council that OPD be authorized to accept the funds.

9. The meeting adjourned at 7:30pm

CITY OF OAKLAND

MEMORANDUM

TO:	Anne E. Kirkpatrick, Chief of Police	**FROM:**	Kathryn Jones, Sergeant OPD, Intel Unit; Bruce Stoffmacher, Mgt. Assistant, OPD, Research and Planning
SUBJECT:	Cellular Site Simulator – 2019 Annual Report	**DATE:**	January 24, 2020

Background

Oakland Police Department (OPD) Department General Order (DGO) I-11: Cellular Site Simulator (CSS) Usage and Privacy, requires that OPD provide an annual report to the Chief of Police, the Privacy Advisory Commission (PAC), and Public Safety Committee. The information provided below is compliant with the annual report policy requirements of Resolution 86585 C.M.S. (Sergeant Kathryn Jones is currently the CSS Program Coordinator).

2019 Data Points

(a) The number of times cellular site simulator technology was requested: (1) One. One request was made and permission was granted, however, an outside agency, Sacramento Police Department (PD), advised they would conduct the entire investigation. The suspect was located prior to them using their technology.

(b) The number of times cellular site simulator technology was used: (0) Zero – the 'request' was to locate a homicide suspect, but the suspect was located by other means prior to any official notifications or required search warrants.

(c) The number of times that agencies other than the Oakland Police Department received information from use of the equipment by the Oakland Police Department: (0) Zero. DGO I-11 does provide that OPD may share CSS data with other law enforcement agencies that have a right to know and a need to know[1], such as an inspector with the District Attorney's Office. However, no CSS data would be downloaded, retained, or shared.

(d) The number of times the Oakland Police Department received information from use of this equipment by other agencies: (0) Zero. OPD did not receive any data from use of this equipment by other agencies.

(e) Information concerning any violation of this policy including any alleged violations of policy. (0) Zero. There were no policy violations.

[1] DGO I-11 explains that a right to know is the legal authority to receive information pursuant to a court order, statutory law, or case law.

(f) Total costs for maintenance, licensing and training, if any. ($0.00) Zero. OPD did not incur any maintenance, licensing, or training costs.

(g) The results of any internal audits and if any corrective action was taken, subject to laws governing confidentiality of employment actions and personnel rules. (0) Zero. No audits were conducted due to no usage in 2019. In 2018, there was also no usage. No corrective action was needed.

(h) The number of times the equipment was deployed: (0) Zero.

OPD is committed to providing the best services to our community while being transparent and instilling procedural justice through daily police activity. This report is compliance with these OPD commitments as well as the reporting requirements of Resolution 86585 C.M.S. OPD hopes that this report helps to strengthen our trust within the Oakland community.

Respectfully submitted,

Kathryn Jones, Sergeant, OPD, Intelligence Unit

Bruce Stoffmacher, OPD, Training Division

CITY OF OAKLAND

MEMORANDUM

TO:	Privacy Advisory Commission	**FROM:**	Anne E. Kirkpatrick
SUBJECT:	Use of Unapproved Surveillance Technology Under Exigent Circumstances – January 6 and 7, 2020	**DATE:**	February 3, 2020

RECOMMENDATION

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

EXECUTIVE SUMMARY

In accordance with OMC 9.64.035, the Oakland Police Department (OPD) used surveillance technology under exigent circumstances (home invasion robbery). The technology is Unmanned Aerial System (UAS), commonly known as a drone.

BASIS FOR EXIGENCY

January 6, 2020
RD #20-000897
Incident #LOP200106000070

On January 6, 2020, at about 3:52am, OPD Officers responded to 2722 Adeline Street on a report of a burglary in progress at a warehouse. Upon their arrival OPD officers located one (1) suspect, armed with a pistol, in the parking lot; officers were able to arrest this suspect. The suspect then advised that two (2) additional suspects were still inside the warehouse. Through their preliminary investigation, it was discovered that the warehouse was an illegal marijuana grow house. The security company, who was streaming live video from outside mounted cameras on the warehouse, advised that the suspects were armed with firearms. OPD elected to use UAS to gain an aerial view of the warehouse and location without compromising officer safety. The UAS aerial reconnaissance assisted in determining the overview outlook. The onsite commander requested the Tactical Operations Team from OPD's Special Operations Division; the warehouse was fortified, and the tactical operators breached through the skylights and used the UAS to gain a view of the interior of the warehouse. The operation finished at 4:00pm. The suspects were not located in the warehouse and it was determined the suspects had fled prior to OPD arrival.

January 7, 2020
RD #20-000450

On January 7, 2020, at about 5:00am, OPD Tactical Operations Team officers responded to 2646 62nd Ave to execute a pre-planned search warrant search stemming from a Ceasefire investigation.

The suspects had outstanding arrest warrants; they were known gang members (based on a variety of data from past criminal activity). These individuals were also known to carry firearms and known to conduct burglaries and robbery takeovers.

The Tactical Operations Team surrounded the residence and contacted the occupants. The UAS assisted in using a light to light up a side of the residence where it was difficult for officers to gain safe views to ensure officer security. The suspects were ordered outside, detained without incident, and taken into custody.

DEVICE USE INFORMATION

The UAS detection equipment was provided by, and operated by the Alameda County Sheriff's Office (ACSO) – both for the January 6, 2020 and January 7, 2020 incidents.

Video Recorded

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

Retention of Recordings

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

Usefulness in Arresting Suspect/s

The UAS was not used in connection with the one arrest on January 6, 2020 near the marijuana grow house burglary; the UAS was used to find additional suspects believed to be inside a building. UAS helped OPD safety determine that there were no other suspects at the location.

UAS was utilized in connection with the January 7, 2020 pre-planned search warrant search and arrest. The UAS provided much-needed real-time intelligence.

COMPLIANT USE

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

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

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

Respectfully submitted,

Anne E. Kirkpatrick
Chief of Police
Oakland Police Department

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

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

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

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

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[1][2]

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.

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.

The situational awareness UAS provides has 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.

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 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 ACSO is using its drones for traffic incidents, tactical operations, and search and rescue.

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;

b. Disaster management;

[1] APSA = Airborne Public Safety Association

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

c. Missing or lost persons;

d. Hazardous material releases;

e. Rescue operations;

f. Special events**[3][4][5][6]**;

   a. Such as, large gatherings of people on city streets, sporting events, or large parades or festivals, etc.[7]

g. Training;

h. Hazardous situations which present a high risk to officer and/or public safety, limited to:**[8]**

i. Barricaded suspects;

j. Hostage situations;

k. Armed suicidal persons;

l. Arrest of armed and/or dangerous**[9][10]** persons;**[11][12]**

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

n. Operational planning**[13][14][15]**;

o. Service of high risk search and arrest warrants**[16][17]** involving armed and/or dangerous persons; and**[18]**

p. At the direction of a command officer.**[19]**

   i. A monitoring commander may authorize a UAS deployment under exigent circumstances. A report shall be completed and forwarded to the Chief of Police and the Department UAS Coordinator for all UAS deployments authorized under exigent circumstances for a full review to determine policy compliance.

[20]

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**[21][22].[23]** 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. ~~Although OPD does not track which of these arrests relate to "armed and/or dangerous persons" -(one of the allowed uses for UAS) as a separate category, the number is likely significan~~**[24][25][26]**t. 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,**[27][28][29][30][31]** 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). **[32][33][34]**

3. 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. 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. **[35][36]**

Law enforcement is also restricted from using UAS to fly over or near the following locations including:

- Stadiums and Sporting Events
- Near Airports
- Emergency and Rescue Operations (wildfires and hurricanes).**[37][38][39]**

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

[3] https://www.nrcresearchpress.com/doi/abs/10.1139/juvs-2015-0031?src=recsys&mobileUi=0&journalCode=juvs#.XemT1-hKiUl

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."

4. 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 continuously, mitigating concerns raised in the February 2016 study cited above. Further, Section III.B. "Deployment Authorization" explains that "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; lower rank personnel may authorize UAS use only during exigent circumstances (e.g. hostage situation) but must still seek commander-level authorization as soon as possible."

Section III.C "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:
    - Conducting random surveillance;
    - 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.

OPD DGO I25 Section III.D "Privacy Considerations," outlines several protocols for mitigating against privacy abuse:

- OPD UAS personnel must adhere to FAA altitude guidelines absent a search warrant exigent circumstances[40][41][42].[43]
- 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).

- 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. [44][45]

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. 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~~, a leading brand of small UAS and flight control software for LE,~~[46] 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.

5. 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. [47][48]

6. 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[49][50] 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.[51] 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[52][53][54] 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 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.

7. 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. 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[55], controller, batteries, battery chargers, propellers, cables, other related accessories such as spotlights and one-	$11,796

drone for lighter use as well as for indoor use	way speakers; $2,949 x 4[56]	
	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).

8. 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. [57][58][59]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.

9. 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[60], by having its own UAS program.

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[61]. 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.

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;[62] this data is also valuable during court testimony.
- Finding and/or seizing illegal drones - police UAS can be flown to identify unregistered UAS[63] that may be hazardous to the surrounding environment.

10. 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 for requiring dual FAA certifications (COA & 107) as well as ways that a UAS program will enhance officer safety[64][65]. The department continues to make presentations to community groups to show how the program is used and the safety and privacy mitigations[66] 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.

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;
    b. Disaster management;
    c. Missing or lost persons;
    d. Hazardous material releases;
    e. Rescue operations;
    f. Special events;[1][2]
        i. Such as, large gatherings of people on city streets, sporting events, or large parades or festivals, etc.
    ~~f.~~g. Training;
    ~~g.~~h. Hazardous situations which present a high risk to officer and/or public safety, to include:
        i. Barricaded suspects[3];
        ii. Hostage situations;
        iii. Armed suicidal persons;
        iv. Arrest of armed and/or dangerous persons[4][5];
        v. Scene[6] documentation for evidentiary or investigation value; (can you explain further on how this is categorized as a hazardous situation)[7]
        vi. Operational planning[8][9]; and
        vii. Service of search and arrest warrants.[10][11]

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.

5. Deployment Authorization for Special Events

a. There are additional special event situations that can occur in the City of Oakland which will justify the use of UASs. Large events with numerous people pose challenges to public safety. UASs are authorized, by an OPD commander (captain or above) when exigent circumstances exist – or when the City Administrator has authorized a partial or full activation of the City's Emergency Operations Center (EOC) and a police Commander (captain or above) approves the use of the UASs. The following use cases are examples where EOC full or partial activation may occur and where a commander may authorize the use of live-stream transmitters:

- Large gatherings[12] of people on city streets;
- Sporting events;
- Large parades or festivals; and
- Natural disasters.

OPD commanders need real-time situational awareness to ensure public safety in public spaces. Real-time information regarding events (e.g. crowd management facilitation, coordinated response to catastrophic unplanned events) provides critical information for OPD commanders when making resource deployment decisions. Authorized personnel utilizing UASs with live-streaming transmitters can provide important situational awareness to OPD without the need to deploy many officers. UASs shall only be deployed with authorizations from an incident commander.

~~5.~~6.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.~~7.Privacy Considerations

a. Absent a warrant or exigent circumstances, operators and observers shall adhere to FAA altitude regulations. [13][14]

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.

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[15].[16][17]

   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 [18][19]for notifying patrol personnel, when UAS operations are authorized by a Commander.

IV. UAS DATA

There should be a section that describes the data transmission process. Over 4G or 5G network? What carrier? Is it a dedicated line? Can it leverage the First Net public safety broadband?

A. Data Collection

The video recording[20] only function of the UAS shall be activated whenever the UAS is deployed, and deactivated whenever the UAS [lands][21][22].

B. Data Retention

Video recording collected by OPD UAS shall be deleted[23] from the device within five (5) days unless:

1. The recording is needed for a criminal investigation;
2. The recording is related to an administrative investigation; or;
3. Retention[24] of data is necessary for another organizational or public need.[25]
    a. The program coordinator shall develop procedures to ensure that data are retained and purged in accordance with applicable record retention schedules[26].

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 access the data for administrative or criminal investigation purposes.[27]

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.[28][29]
        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; the UAS only sends data to the flight controller via encrypted radio signals – there is no internet connection for external data sharing.

OPD will consider sharing information from UAS operations with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law and/ or Department policies, using the following procedures:

1. The agency makes a request for UAS data and/or usage, which includes:
   a. The name of the requesting agency.
   b. The name of the individual making the request.
   c. The intended purpose of obtaining the information.
2. The request is reviewed by the Chief of Police or designee and approved before the request is fulfilled.

3. The approved request is retained on file.[30][31][32][33]

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 shall be available via public records request pursuant to applicable law regarding Public Records Requests.

Is this data available for view upon public request via the Freedom of Information Act for all public institutions?[34]

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 [35]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 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 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.[36][37][38] and the annual UAS 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[39][40][41]

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

For

Mobile Identification Devices

---

1. Mobile Identification Devices (MID) and How they Work

Mobile Identification Devices (MID) are small enough to be handheld, and contains an optical sensor to scan fingerprints and transmit them to look for matches within local databases MIDs are not investigative tools – they only allow personnel to attempt to match fingerprints of individuals who are to be arrested with possible matches from past arrests in Alameda and Contra Costa Counties.

The MID uses the Bluetooth radio standard to send a scanned image of a fingerprint to a police vehicle mobile data terminal (MDT), which can connect with special software. The software accesses a regional fingerprint database shared by Alameda and Contra Costa Sheriff's Offices called Cogent Automated Fingerprint Identification System (CAFIS).

The MDT software sends the fingerprint digital image to CAFIS where the Almeda and Contra County CAL-ID Mobile Web ID system runs the fingerprint against the Alameda County Consolidated Records Information Management System (CRIMS) and the Contra Costa County Automated Regional Information Exchange System (**ARIES**) Systems to cross reference the scanned image to look for matches. The software match process uses a graphic representation of the print as a mathematical model of the relationships between the ridges of the fingerprint image. This mathematical measuring of friction ridges allows the image to be transmitted as a string of numbers the Automated Fingerprint Identification System (AFIS) databases can use.

Search results are sent back to MDTs. If a search result ends in a match with CAFIS, a fingerprint record will appear in the MID with the following:

- Transaction Number;
- Main Number,
- Name on Record;
- Date of Birth (DOB);
- Sex;

- Person File Number (PFN) / Juvenile File Number (JFN); and
- Arrest Booking Photo (if one is on file).

The hit will only return with the record hit (not a list of possible matches); a hit means a 100 percent match. No hits return with the display, "No hit." A "No Hit" means only that the subject's fingerprints are not in the CAFIS database.

2. Proposed Purpose

The sole purpose of the MID is to allow police to identify individuals who do not possess acceptable forms of identification (e.g. driver's license or passport) in cases where they otherwise do not need to be booked in the Alameda County Jail. State law requires police to identify individuals to be cited for an infraction or misdemeanor; arrest and booking into jail is legally required when an acceptable form of ID cannot be obtained. Police need to know who you are when a citation is appropriate.

For situations where an individual must face custodial arrest, OPD currently transports individuals to the Alameda County Sheriff's Office (ACSO) Santa Rita Jail in Dublin, CA, where they are turned over to ACSO deputies for intake and identification.

In 2018, there were eight arrests where California Vehicle Code section 40302(a) or (b)[1] was one of the listed offenses (one case as for 2019 as of October 17, 2019). These are instances where the initial stop and/or citation was merely for a traffic violation but adequate identification could not be made. However, the arrests involving 40302 VC are not the only instances of subjects being booked on citable misdemeanors due to a lack of identification. There are countless situations where individuals faced custodial arrest at Santa Rita Jail where a citation would have been an appropriate remedy. For 2018, OPD made 8,239 custodial arrests for 16,853 charges. 6,940 of these arrests (84 percent) included either a felony charge, a misdemeanor charge that required an arrest (warrant, domestic violence, firearms violation), or both. The remaining 1,299 arrests involved over 100 different charges; Table 1 below lists the top categories (>30 arrests each). In many of these cases, custodial arrest would be the best option even when the arrestee could provide identification. For example, individuals who are highly inebriated may need to be arrested for their own safety so they can recover in a safe place and not be susceptive to outdoor exposure and/or victimization. There are cases of prostitution where arrest is part of a larger process to connect human trafficking victims with support services. However, there are cases such as the 58 battery custodial arrests where identification could have afforded the officers the ability to issue a simple citation.

[1] CVC 40302: Whenever any person is arrested for any violation of this code, not declared to be a felony, the arrested person shall be taken without unnecessary delay before a magistrate within the county in which the offense charged is alleged to have been committed and who has jurisdiction of the offense and is nearest or most accessible with reference to the place where the arrest is made in any of the following cases: (a) When the person arrested fails to present both his or her driver's license or other satisfactory evidence of his or her identity and an unobstructed view of his or her full face for examination; (b) When the person arrested refuses to give his or her written promise to appear in court.

T***able 1: OPD 2018 Non-Required Custodial Arrests Top Categories***

Statute Code	**Description**	**Charge Count**
PC647 (F)	DISORDERLY CONDUCT: ALCOHOL	203
PC647 (B)	DISORDERLY CONDUCT: PROSTITUTION	200
VC23152 (A)	DUI* ALCOHOL/DRUGS	158
PC166 (A)(4)	CONTEMPT OF COURT: DISOBEY COURT ORDER/ETC	101
PC653.22(A)	LOITER: INTENT: PROSTITUTION	89
PC242	BATTERY	58
PC 166(C)(1)	CONTEMPT OF COURT: VIOLATE PROTECTIVE ORDER/ETC	32

*__DUI__ = driving a vehicle under the influence of alcohol or other intoxicant

Officers are not allowed to transport subjects to Santa Rita Jail alone. Each arrest requires hours of time of at least two officers and wastes significant time for the arrested individuals who need to return to Oakland or elsewhere upon release. Officers can more efficiently utilize patrol service time in the community. OPD would rather cite people for low-level crimes when appropriate, and allow individuals to not face the hassles and burdens of being temporarily removed from society and going to jail some 26 miles from Oakland. Individuals who could be cited for an infraction or misdemeanor but cannot provide ID will be saved the burden of transportation back to Oakland after the full arrest and booking process.

Additionally, the arrest can cause varying levels of stress for individuals and lead to escalations of anger, noncompliance, and even use of force. Furthermore, if an individual who must face custodial arrest has a vehicle at the arrest location, their vehicle may face parking fees and even towing – causing an additional burden.

By providing rapid ID when records exist, MIDs can mitigate these challenges as well as offer other benefits.

3. Locations Where, and Situations in which the MID System may be deployed or utilized.

Where - The technology would be provided to patrol officers throughout the five police areas of the City.

Situations - Any misdemeanor that does not require a custodial arrest by statute or circumstance (inebriation, crime likely to continue, etc.).

4. Impact

Public Privacy Impact

The privacy risks associated with MID are:

1) personnel could abuse the device to ascertain a person's identify when not justified; or
2) the person's data, associated with fingerprints, could be shared intentionally or unintentionally in ways that violate the person's right to privacy.

To address the first concern, OPD Department General Order (DGO) I-21 "MOBILE IDENTIFICATION DEVICES" explicitly requires that MID may only be used when the individual provides knowing and voluntary[2] consent (captured via Body-Worn Camera (BWC) video or on a signed consent form[3], and one of the following circumstances exist:

1. Probable causes exists for the subject's arrest; or
2. The subject is to be cited for an infraction or misdemeanor and cannot provide satisfactory evidence of identity.

Furthermore, DGO I.21 C.2. "Use Procedure" explains that MIDs will be stored at Bureau of Field Operations Offices and that patrol officers must contact their supervising sergeant to request a MID for identification purposes.

In terms of a person's data being shared in ways that violate their expectation and / or right to privacy, the MID technology does not store any data – it only searches data that already exists. Fingerprint data is not transferred or stored from existing databases onto MDTs or other OPD data systems.

5. Mitigations

MIDs are designed to not store data but to only access the fingerprint database shared between Alameda and Contra Costa County to compare the fingerprint itself. Since data is not retained by the MID or police computer, personally identifiable data cannot be shared inappropriately. DGO I-21 C.3 provides another layer of privacy impact mitigation – in the event that an officer uses the MID with a person's voluntary consent, the officer will use personal a BWC to record the encounter and ensure an evidentiary record. As previously mentioned, the absence of a BWC will require a signed consent form (TF-2018).

6. Data Types and Sources

The MID is used to scan an individual's fingerprint. The scan is connected via the MID, via Bluetooth to the in-car computer, with a fingerprint database maintained

[2] In accordance with OPD Training Bulletin I-Q – *Consent Searches* (see Appendix A), officers seeking consent shall tell the subject that they have the right to refuse being identified via MID..
[3] As of the effective date of this order, the form number is TF-2018 (see Appendix B).

by ACSO and the Contra Costa Sheriff's Office. The fingerprint images are scanned using algorithms to compare different points on the image of the fingerprint. This system can also connect to arrest records if the algorithm matching software sees a match between a MID-scanned fingerprint image and a fingerprint on file. In this case, the MID will access the arrest record and personal file number from the prior arrest with associated name on file. Alameda County Mobile ID devices use the CAL-ID Mobile WEB ID system to run fingerprint searches against the fingerprint database. MID users must log into the Mobile ID WEB ID systems to use the Mobile ID device and receive search results. The arrest record is not actually visible on the handheld MID, it merely lets one know the record exists. An officer would be required to use the personal file number to see the arrest record in CRIMS.

7. Data Security

ACSO's Central Identification Bureau (CIB) manages Alameda County's CAL-ID System infrastructure consisting of an infrastructure of CAL-ID systems, sub-systems and network. The main CAL-ID system is an Automated Fingerprint Identification System (AFIS). CAL-ID includes several supporting systems also referred to as 'sub-systems' that provide additional information and tools to law enforcement. Supporting systems include mugshot and mobile ID systems. Management includes all CAL-ID databases, equipment, system and equipment maintenance, equipment deployment, training and system access. All systems are Criminal Justice Information Service (CJIS)-compliant, meaning that ACSO maintains security controls aimed at ensuring only authorized individuals have access to the fingerprint information. Furthermore, this system is maintained behind a firewall and is housed separate from other ACSO systems and Alameda County internet and data systems.

All users must first complete the Mobile ID User Agreement and receive hands-on training. The agreement is signed by their supervisor and sent to ACSO's CIB for final approval and user account access. When the user signs the Mobile Identification User Agreement, they certify that they have received training, and will abide by all policies.

Any maintenance required of the MID will done by ACSO staff, and requests will be directed to ACSO through the OPD Information Technology Unit.

8. Costs

ACSO will accept all costs to furnish OPD with MID technology. ACSO will also maintain responsibility for maintenance costs.

9. Third Party Dependence

ACSO will provide MID devices to OPD and will accept all costs to furnish OPD with MID devices. The MID devices themselves are made by Cogent

(owned by 3M).

10. Alternatives Considered

The alternative to using MIDs for persons that cannot be identified in conditions outlined in DGO I-21.C.1 will be to continue to arrest people who otherwise would not need to be arrested and taken to jail in Dublin, CA for the purpose of identification. In these cases, people will continue to assume the burden of arrest and transport a long distance from Oakland, and police time will continue to be used ineffectively. OPD is not aware of another system for legally identifying persons without acceptable identification.

11. Track Record of Other Entities

MID devices are used by many California city police agencies and county sheriff departments. Cities include:

- Fresno;
- Los Angles;
- San Francisco;
- San Jose;
- Modesto; and
- Pasadena;

Counties include:

- Fresno;
- Kern;
- Los Angeles'
- Marin;
- Santa Clara;
- San Francisco; and
- Stanislaus

Several cities and counties are beginning to conduct MID studies. Other locations are using similar technologies. The Brentwood Police Department has installed BlueCheck mobile ID systems – a similar type of fingerprint reader, in some police vehicles. These handheld devices also match prints to files maintained by Contra Costa and Alameda counties. The San Jose Police Department, in partnership with Santa Clara County, is using BlueCheck, a mobile fingerprinting device from 3M Corporation. The L.A.

County Sheriff's Office and several L.A. County police departments are also using BlueCheck devices for fingerprint ID. Several Alameda County police departments are using the Cogent 3M MIDs, including Berkeley, Hayward, and San Leandro.

Appendix A

TRAINING BULLETIN

Effective Date
13 Dec 11

Index Number: I-Q
Alpha Index: Consent Searches

Evaluation Coordinator: Training Section Commander
Automatic Revision Cycle: 3 Years

"Department Training Bulletins shall be used to advise members of current police techniques and procedures and shall constitute official policy."

CONSENT SEARCHES

Introduction

Law enforcement officers have a variety of methods available to enforce and prevent crime. One such method that is often overlooked is the consent search.

If an officer obtains valid consent, the officer may conduct a search without a warrant, probable cause, exigent circumstances, or parole/probation conditions.

With valid consent, the officer is entitled to seize contraband and the fruits or instrumentalities of a crime as well as any other item the officer reasonably believes will aid in a suspect's apprehension or conviction.

Consent to search not only applies to suspects, but also to victims who similarly retain a reasonable expectation of privacy.

When seeking consent to search, the officer must explicitly ask the suspect or victim for their consent and advise they have the right to refuse pursuant to DGO M-19.

Officers shall document in their respective reports that they explicitly asked the suspect/victim for consent, state whether consent was implied or expressed, and that they were advised they had the right to refuse consent.

In addition to explicitly asking a suspect or victim consent to search, consent will be valid if all of the following apply:

- The consent is voluntary and a product of the subject's free will.
- It is not coerced by force, threats, tricks, promises, or the exertion of an officer's authority.
- The person providing the consent has the authority or apparent authority to provide the consent.
- The search does not exceed the scope or limits of the consent given.

This Training Bulletin examines each of these criteria.

Consent is Voluntary

A person may give either express or implied consent.

Express consent is verbal consent given with words, such as "Yeah," Go ahead," or "Do what you want."

Implied consent is consent given through physical gestures or acts, such as pointing or waving.

Because a subject has the right to remain silent and refuse consent, silence in response to an officer's request for consent **does not** constitute implied consent. (*Pavao v. Pagay* (9th Cir. 2002) 307 F3 915, 919)

Factors that may impair a subject's decision making capability-such as medication, age, intoxication, and mental condition-are considered by the court, and the court may rule such factors make a subject's consent unknowing and less than voluntary. A suspect's consent, for example, was ruled involuntary when he was in critical condition and in pain in a hospital emergency room. (George (9th Cir. 1993) 987 F.2d 1428, 1431)

An Officer's Display of Intimidating Conduct or Force can Affect the Validity of a Consent Search

By exhibiting force while seeking consent, an officer takes a risk that the consent will be ruled involuntary. The courts also consider whether weapons have been drawn. In order for consent to be valid, it must be uncontaminated by duress, intimidating conduct, or other pressure tactics, whether direct or indirect. (*People v. Challoner* (1982) 136 CA3 743,758)

An Officer's Words can Affect the Validity of a Consent Search

The words an officer uses in seeking consent are often decisive in determining if consent is voluntary.

An officer must avoid commanding a subject to perform an act that permits the officer's search or facilitates the officer's access. Instead, an officer must ask the subject for permission to perform the search.

For example, an officer does not command a subject to "open the door." Instead, the officer asks, "Would you mind opening the door?" An officer does not command a subject to "open a car trunk." Instead, the officer asks, "Would you mind if I looked in the trunk?"

If a subject aids an officer in a search by obtaining evidence or by opening a door, trunk, or purse, it is more likely the consent will be ruled voluntary. An officer, however, must not command a person to perform these acts.

The court will ask if the officer made the subject feel he or she had a choice or if the officer made the subject feel he or she had to give consent. By asking for and receiving permission, the officer obtains a valuable indication that the subject's consent was voluntary.

While not mandatory, an officer obtaining a subject's written waiver of Fourth Amendment rights in order to establish consent can help shows that the consent was voluntary.

An Officer's Misrepresentation can Affect the Validity of a Consent Search

An officer shall not misrepresent his/her identify or purpose for seeking consent. An officer may not misrepresent his/her authority by stating he/she has a warrant when he/she does not. (*Bumper v. North Carolina* (USSC 1968) 391 US543, 550). Additionally, an officer may not state he/she wants to enter for one reason and then enter for another. (*US v. Harrison* (10C 2011) 639 F3 1273, 1280).

An undercover officer may legally misrepresent his/her identity and purpose for obtaining consent. This only applies when the undercover officer enters a residence for the purpose of buying or selling contraband or engages in other illegal conduct. (*U.S. v. Lopez* (USSC 1963) 373 US 427, 438)

The Person Providing the Consent has the Authority

A person may consent to the search of property he/she owns or occupies.

A joint or co-occupant of a premises may consent only to the search of his/her exclusively owned property, shared property, or common areas. Before searching questionable areas, an officer needs to ask if the person giving consent has free access to the object or area in question.

One spouse may consent to the search of the other spouse's property only if the spouse giving consent has joint access or joint control over that property AND the other spouse does not object. Officers do not have to seek consent from the other spouse and the objecting spouse must be on scene to object. (*Georgia v. Randolph* (USSC 2006) 547 US 103, 120)

Parents may consent to the search of areas or property that has not been "staked out" by a child as his/her own. For example, an officer may search a juvenile's room with parental consent if a parent cleans the room and the juvenile does not pay rent. However, a parent cannot give consent for an officer to search a juvenile's personal effects, such as a suitcase or toolbox, if the parent makes no claim or right of control over the object even if the object is in the parent's bedroom.

In some circumstances, a teenager may possess sufficient authority to allow an officer to enter and look about common areas. As children advance in age, they acquire greater discretion to admit visitors on their own authority. (*People v. Jacobs* (1987) 43 C3 472, 483)

An owner of property may give authorization to a third party to give consent to a search.

A host may consent to the search of a room where a non-paying guest is staying; however, the host does not have authority to consent to the search of the guest's personal property.

A property owner may not consent to the search of premises rented by a tenant.

A motel owner or employee may not consent to the search of a guest's room. Although motel employees may enter a rented room to clean, an officer may not send an employee in as the officer's agent to look for crime related evidence.

An employer or employee may consent to the search of areas and items, such as file cabinets, over which he/she has common authority or control.

A real estate agent may not consent to the entry of listed houses by persons whom the agent knows to be police officers looking for evidence.

Under the rule of "apparent authority," courts will uphold a search as valid if an officer had a reasonable, good-faith belief, based on all the circumstances, that the consenter had the authority to give consent. (*U.S. v. Matlock* (USSC 1974) 415 US 164, 171)

If an officer has questions about authority, the officer must ask questions to determine whether the person giving consent shares the use of and has joint control over the area or object to be searched.

The Search Does Not Exceed the Scope of Consent Given

The places where an officer may search are limited entirely by the scope of the consent given.

It is the officer's responsibility to ensure the consenter has given consent for the officer to search the areas where he/she is looking.

Consent to look for a person is not consent to look in a place where a person could not be located. Consent to search a house is not consent to answer the telephone. Consent to search a suitcase, however, includes consent to look inside the suitcase compartments and containers.

As long as an officer remains within the scope given, the officer may seize any crime related evidence in plain view.

Additional Information about Consent Searches

- Custody tends to show a suspect's consent is not voluntary. However, custody alone does not necessarily destroy an otherwise valid consent search.

  It is possible to get a valid consent from someone who is arrested and handcuffed.

- Miranda warnings are not required prior to requesting consent to search.

  A voluntary consent may be obtained even after a person has asserted his/her Miranda right to remain silent or his/her right to an attorney.

- A subject may withdraw his/her consent at any time during a search.

  When a subject withdraws consent, an officer must immediately stop the search.

  Actions inconsistent with consent may act as withdrawal of consent. For example, if a suspect gives consent and then attempts to hamper or thwart the search, by throwing away a car's keys, for example, the consent may be ruled involuntary.

- After formal charges have been filed against a suspect and an attorney has been appointed or retained, it is improper for an officer to conduct a search without also obtaining the consent of the suspect's counsel or a search warrant. An officer shall not contact the suspect without first contacting the suspect's attorney.

- All factors of consent are scrutinized at many different levels in the court system and, in some cases, by multiple judges.

  The preferred method for an officer to document consent is on an audio/video device or in writing.

Appendix B

CONSENT TO SEARCH
搜查同意書
CONSENTIMIENTO DE BÚSQUEDA O REGISTRO

RD No.
街道號碼：
No. de RD _____

I consent to the search of: (Describe Person, Vehicle, Premises, etc.)
我同意搜： (明個人、車輛、房宅等)
Otorgo mi consentimiento para la búsqueda o re gistro de: (Describa a la persona, vehículo, lugar, etc.)

_____

_____

_____

I have been told that I ha ve a right to refuse to allow the police to search my person or my proper ty. I have given my consent voluntarily without threats or promises.

我已被告知有權拒絕警察搜查我個人或我的物業。我自願同意被搜查，沒有人威脅我或答應我任何事

Se me ha comunicado que tengo el derecho de negar me a permitirle a la poli cía que realice una búsqueda o registro en mi persona o en mi propiedad. He otorgado mi consenti miento voluntariamente sin amenazas ni promesas.

Witnessed By:
證人：
Atestiguado por

_____
(Signature of Consenting Party) (同意人簽名)
(Firma de la parte que otor ga su consenti miento)

_____

_____

_____

Date/Time
日期 / 時間
Fecha/Hora

_____

TF-2018 (3/03) Consent to Search – English, Spanish, Chinese

DEPARTMENTAL GENERAL ORDER

I-21: MOBILE IDENTIFICATION DEVICES

Effective Date: DD MMM 19
Coordinator: Information Technology Unit; Bureau of Field Operations Division (BFO)

PURPOSE

This order sets forth Department policy and procedure for the use of Mobile Identification Devices (MID). MID allow law enforcement personnel to temporarily cross reference specific biometric data with a handheld device in the field and then wirelessly compare the data to a biometric database for comparison and identification. Identification can be made in near real time without having to take a subject to a detention facility for the identification process.

A. DEFINITIONS

A - 1. Authorized User

A member trained in the use of the MID and accompanying software. Only authorized users may use the MID.

A - 2. Mobile Identification Devices (MID) Currently Used by the Department

As of the effective date of this order, the Department uses wireless Bluetooth-enabled fingerprint scanners which pair with software on a Mobile Data Terminal (MDT) to compare fingerprints obtained from a person with fingerprints in the CAFIS fingerprint database.

A - 3. Cogent Automated Fingerprint Identification System (CAFIS)

A regional fingerprint database shared by Alameda and Contra Costa Counties.

B. DESCRIPTION OF THE TECHNOLOGY

B - 1. The MID System

Mobile Identification Devices (MID) are handheld devices with an optical sensor that scans fingerprints and match them with fingerprint databases. The MID uses the Bluetooth wireless radio standard to send a scanned image of a fingerprint to a police vehicle mobile data terminal (MDT) with special software. The software accesses a regional fingerprint database shared by Alameda and Contra Costa Sheriff's Offices – Cogent Automated Fingerprint Identification System (CAFIS).

B - 2. How MID Works

The MDT software sends the fingerprint digital image to CAFIS where the Almeda and Contra County CAL-ID Mobile Web ID system runs the fingerprint against the CAFIS system to look for matches; the software match process uses a graphic representation of the print as a mathematical model of

the relationships between the ridges of the fingerprint image. This mathematical measuring of ridge lines allows the image to be transmitted as a string of numbers the Automated Fingerprint Identification System (AFIS) databases can use.

Search results are sent back to MDTs. If a search result ends with a 'hit' to a fingerprint record in CAFIS, a return with limited data (Transaction number (of the search), name on record, date of birth (DOB), Sex, Person File Number (PFN)/Juvenile File Number (JFN) and booking photo (if there is a previous arrest booking number) will be displayed. The hit will only return with the record hit (not a list of possible matches). No hits return with the display, "No hit."

C. AUTHORIZED USE POLICY

C - 1. Identification of Detained and Arrested Subjects

Prior to using MID, members shall use available databases (e.g. CRIMS, DMV, CalPhoto) as the primary means of identifying persons. If available databases are not sufficient to positively identify a subject who must be identified on scene, the MID may be used to identify the subject. A MID may only be used when the individual provides knowing and voluntary[1] consent (captured via Body-Worn Camera (BWC) video or on a signed consent form[2], and one of the following circumstances exist:

1. Probable causes exists for the subject's arrest; or
2. The subject is to be cited for an infraction or misdemeanor and cannot provide satisfactory evidence of identity.

C - 2. Use Procedure

MID devices will be stored with BFO; patrol officers requesting to use a MID shall contact their supervising sergeant. The sergeant will direct the officer to retrieve the MID from BFO offices or to have another personnel member deliver the MID in the field for identification purposes.

C - 3. Assistance to Other Agencies

Providing MID assistance to other agencies shall be approved by a supervisor or command officer. All instances of such outside assistance shall be documented, at minimum, by a notation on the Computer-Aided Dispatch (CAD) incident. Mobile identification assistance provided to other law enforcement agencies must be carried out in accordance with all sections of this use policy including section D "Prohibited Uses and Actions," Section D

[1] Officers seeking consent shall tell the subject that they have the right to refuse being identified via MID.
[2] As of the effective date of this order, the form number is TF-2018.

"Data Collection, Access, Protection, Retention, Sharing, and Maintenance," and Section F "Data

C - 4. Other Uses of MID

Any use of the MID for reasons other than set forth in B-1 and B-2 shall be approved by a supervisor or command officer prior to use.

C - 5. Documentation of MID Use

All instances of MID use, other than training, shall be documented in the appropriate report (or CAD incident for outside agency assistance). Documentation shall include the basis for use of the MID and, if directed by a supervisor or commander, the name and serial number of that member.

D. PROHIBITED USES / ACTIONS

D - 1. Tampering with or Modifying the MID

Members shall not tamper with or modify the MID. All loss or damage of MID shall be reported in accordance with DGO N-05, *Lost, Stolen, Damaged City Property*, with a copy of the memo routed to the Information Technology Unit.

D - 2. General Investigative Purposes or Intelligence Gathering

MID shall not be used for general investigative purposes or intelligence gathering absent an authorized use as prescribed in section B.

D - 3. Physical Force or Coercion

Members shall not use physical force or coercion to force a subject to submit to use of an MID.

E. DATA COLLECTION, ACCESS, PROTECTION, RETENTION, SHARING, AND MAINTENANCE

E - 1. Data Collection

The MID operate by collecting specific fingerprint data through electronic scanning technology.

E - 2. Data Access

The Alameda County Sheriff's Office (ACSO) Central Identification Bureau (CIB) maintains all data access. MID user access is limited to the results of a fingerprint search through the Mobile WEB ID system.

Public and defendant access to the database shall follow the same rules as currently established for public access to CAFIS.

E - 3. Public Access

Requests for MID data by non-law enforcement or non-prosecutorial agencies will be processed as provided in Departmental General Order M-09.1, Public Records Access (Civil Code § 1798.90.55).

~~E - 3.~~**E - 4. Data Protection**

Data is transmitted from the MID to the MDT by secure Bluetooth connection, and then from the MDT to the CAFIS database and back via encrypted wireless connection.

~~E - 4.~~**E - 5. Data Retention**

The MID will hold up to 10 searches (in case out of range of the MDT) until they are 'sent' to search against the Alameda /Contra Costa fingerprint database. ACSO CIB logs and maintains transaction information. Data is purged from the MID after being sent to the MDT; data is not stored in the MDT.

F. TECHNOLOGY ADMINISTRATION

F - 1. System Coordinator / Administrator

The OPD Information Technology Unit (ITU) shall administer the MID program. ITU shall be responsible for collaborating with the Training Division to ensure that personnel with access to the system are properly trained. ITU or other designated personnel shall also be responsible for any required audits in support of the annual report to the City's Privacy Advisory Commission and City Council.

~~F - 1.~~**F - 2. Maintenance**

ITU will also collaborate as necessary with ACSO / CIB to maintain system operations.

Third-Party Data Sharing

OPD assistance to outside agencies is governed by B-2. Outside agencies requesting MID use shall be responsible for possessing the appropriate basis for requesting the data.

~~F - 2.~~**F - 3. Data and Equipment Maintenance**

ACSO's CIB manages Alameda County's CAL-ID System infrastructure consisting of an infrastructure of CAL-ID systems, sub-systems and network. The main CAL-ID system is an Automated Fingerprint Identification System (AFIS). CAL-ID includes several supporting systems also referred to as 'sub-systems' that provide additional information and tools to law enforcement. Supporting systems include mugshot and mobile ID systems. Management includes all CAL-ID databases, equipment, system and equipment maintenance, equipment deployment, training and system access.

Alameda County Mobile ID devices use the CAL-ID Mobile WEB ID system to run fingerprint searches against the fingerprint database. MID users must log into the Mobile ID WEB ID systems to use the Mobile ID device and receive search results. Only the Alameda/Contra Costa County fingerprint database is searched.

All mobile ID results return to laptops in the patrol vehicles (MDT). If a search results ends with a 'hit' to a fingerprint record in the Alameda/Contra Costa County database, a return with limited data [Transaction number, Name on record, DOB, Sex, Person File Number (PFN)/Juvenile File Number (JFN) and booking photo] will be displayed. The hit will only return with the record hit (not a list of possible matches).

~~F - 3.~~F - 4. Training

All users must first complete the Mobile ID User Agreement and receive hands-on training. The agreement is signed by their supervisor and sent to ACSO's CIB for final approval and user account access. When the user signs the Mobile Identification User Agreement, they certify that they have read and will comply with the Mobile Identification Policy, have received all required training documents, and will abide by all policies. Any maintenance required of the MID will done by ACSO staff, and requests will be directed to ACSO through the OPD ITU.

Any maintenance required of the MID will done by ACSO staff, and requests will be directed to ACSO through the OPD ITU.

F - 5. Auditing and Oversight

The System Coordinator will be responsible for coordinating audits every year to assess system use. The System Coordinator will collaborate with ACSO to produce a report detailing use of each device. A summary of user access and use will be made part of an annual report to the City's Privacy Advisory Commission and City Council.

By order of

Anne E. Kirkpatrick
Chief of Police

Date Signed: _____

TO:	Public Safety Committee, City Administrator Sabrina Landreth	**FROM:**	Privacy Advisory Commission (PAC)
SUBJECT:	PAC 2018-2019 Annual Reports	**DATE:**	February 25, 2020

The following pages contain the PAC 2018 & 2019 Annual Reports. It is formatted in the Council Agenda Report template to make it easier to read and follow.

EXECUTIVE SUMMARY

The objective of this report is to provide City stakeholders with an update on the activities of the Privacy Advisory Commission (PAC), including making recommendations on:

1. **Sanctuary City Ordinance** (Council approved)
2. **Surveillance Equipment Ordinance** (Council approved)
3. **Annual Reports To Date** (Council approved)
4. **Exigent Circumstances Reports** (Council approved)
5. **Sanctuary Contracting Ordinance** (Council approved)
6. **U.S. Department of State – International Visitors** (N/A)
7. **Bay Area Roundtable** (N/A)
8. **Facial Recognition Ban** (Council approved)
9. **Privacy Principles** (Pending)

BACKGROUND / LEGISLATIVE HISTORY

In March 2014, the City Council established an Ad Hoc Advisory Committee to develop a Privacy and Data Retention Policy for the Domain Awareness Center (DAC), a City-Port security project located at the Emergency Operations Center.

This Committee developed a Policy for the DAC and proposed a set of additional recommendations for the City Council to consider. One of the key recommendations that the City Council considered and adopted was the Creation of a Permanent Standing Privacy Advisory Commission to develop and advise on citywide privacy concerns.

On January 19, 2016, the City Council adopted Ordinance No. 13349 C.M.S., which created and defined the duties of the Privacy Advisory Commission. Those duties broadly stated are:

- Provide advice and technical assistance to the City of Oakland on best practices to protect citizen privacy rights in connection with the City's purchase and use of surveillance equipment and other technology that collects or stores citizen data.
- Draft for City Council consideration, model legislation relevant to privacy and data protection, including a Surveillance Equipment Usage Ordinance.
- Submit annual reports and recommendations to the City Council regarding: (1) the City's use of surveillance equipment, and (2) whether new City surveillance equipment privacy and data retention policies should be developed or such existing policies be amended.

- Provide analyses to the City Council of pending federal, state and local legislation relevant to the City's purchase and/or use of technology that collects, stores, transmits, handles or processes citizen data.
- Conduct public hearings, make reports, findings and recommendations either to the City Administrator or the City Council, as appropriate including an annual report to be presented in writing to the City Council.
- Review and make recommendations to the City Council regarding any proposed changes to the operations of the Domain Awareness Center ("DAC") and/or proposed changes to the City's Policy for Privacy and Data Retention for the Port Domain Awareness Center ("DAC Policy") as specified in Resolution 85638 C.M.S.

Excerpt From Enabling Ordinance 13349:

Section 2. Duties And Functions

e. Submit annual reports and recommendations to the City Council regarding: (1) the City's use of surveillance equipment, and (2) whether new City surveillance equipment privacy and data retention policies should be developed or such existing policies be amended.

…

g. The Privacy Commission shall make reports, findings and recommendations either to the City Administrator or the City Council, as appropriate. An annual report will be presented in writing to the City Council…

RECENT ACHIEVEMENTS

1. **Surveillance Equipment Ordinance**: After two years of deliberations with staff, community stakeholders, outside subject matter experts, and motivated by the Domain Awareness Center discussion, the PAC forwarded a ground-breaking draft of legislation to govern the city's procurement and use of surveillance technology, the first such ordinance to involve a citizens commission in the vetting and policy crafting, and the first to prohibit non-disclosure agreements, and add enhanced whistleblower protections. Ordinance No. 13489 was unanimously adopted on May 15, 2018.

2. **Surveillance Equipment Ordinance Policies** – Pursuant to the Surveillance Equipment Ordinance, staff must propose a Use Policy, and the policy must receive City Council approval, to continue (for pre-existing equipment) or begin use (for new acquisitions) of surveillance technology. In 2018-2019, the following policies were approved by the City Council: DOT Automated License Plate Readers, Dockless Mobility Data Sharing, StarChaser GPS, and ShotSpotter. The following policies have been recommended for approval by the PAC, and await a decision by the City Council: DOT Drone, and OFD Data Collection For Fire Inspections.

3. **Surveillance Equipment Annual Reports** – Due to the mid 2018 approval date of the Ordinance, most annual reports will be reviewed and presented to the Council and public in this coming year. The City Council has received two annual reports pertaining to the Cell-Site Simulator (cell phone tracker) after the PAC reviewed and recommended that they be accepted. The annual reports revealed no disparate impact or civil liberties violations, and that the equipment was used appropriately to pursue homicide suspects.

4. **Facial Recognition Ban** – Following the ground-breaking lead of San Francisco in prohibiting city staff's use of facial recognition technology, Oakland became the third city in the nation to ban the technology. At least seven cities across the country have done so to date, and two states (CA, MA) have imposed moratoriums on the technology.

5. **Sanctuary City Ordinance/Sanctuary Contracting Ordinance** – Following an ICE raid that occurred in 2017 in West Oakland, a large community coalition successfully advocated for a true non-cooperation Sanctuary City Ordinance, giving our sanctuary city proclamation the weight of law. As the data mining practices of ICE became more exposed, and as Trump's policy of family separation dominated the headlines, the PAC recommended a contracting ordinance that followed similar ordinances such as the Border Wall Contractors prohibition, and the Anti-Nuclear Weapons Ordinance, prohibiting the city from entering into contracts with entities that supply federal immigration agencies with data, extreme vetting analytics, or detention facility support.

6. **Hosting Special Guests** – PAC Chair Brian Hofer and CPO Joe DeVries met with two groups of international visitors, facilitated by the U.S. Department of State. The visitors were comprised of law enforcement and government policy officials, cybersecurity and cybercrime investigators, journalists, and human rights advocates. On February 28, 2019, PAC Co-Chair Heather Patterson and UC Berkeley's Center for Long-Term Security researcher Steve Trush and team co-hosted a roundtable for local municipal professionals with a direct involvement in policy making pertaining to surveillance technology, data collection and retention, and community outreach. The roundtable was joined by Kelsey Finch, policy council at the Future of Privacy Forum, and PAC members participate in a monthly "Municipal Privacy Professionals" conference call hosted by Ms. Finch, where PAC members and other municipal staff discuss best practices and share and review work product.

UPCOMING PROJECTS

9. **Surveillance Equipment Policies** – The PAC will continue to work with staff on Use Policies for existing surveillance technology used by the City, and on new proposals to come.

10. **Privacy Principles Rollout** – Conditioned upon City Council approval of the PAC's recommended Privacy Principles, the PAC and relevant city staff will undertake an estimated 2-3-year rollout across all city departments, to review existing data collection and retention practices, create boilerplate language to be used with the public, vendors, permits and contracts, and to conduct community outreach.

SPECIAL RECOGNITION

The PAC would like to specially recognize those listed below for their past and present assistance in policy writing, legal research, and technical expertise.

11. Clint Johnson (former Commissioner, co-chair)
12. Raymundo Jacquez, III (former Commissioner, co-chair)
13. UC Berkeley Law, School of Information's Prof. Deirdre Mulligan (former Commissioner)

14. Saied Karamooz (former Commissioner)
15. Tim Birch (former OPD Office of the Chief staff liaison to the PAC)
16. Deputy Chief Roland Holmgren (OPD Office of the Chief; primary policy writer)
17. Bruce Stoffmacher (OPD Office of the Chief staff liaison to the PAC; primary policy writer)
18. UC Berkeley Law's Prof. Catherine Crump (advisor and guest speaker)
19. UC Davis Law's Prof. Elizabeth Joh (guest speaker)
20. Mike Sena, Executive Director of NCRIC (guest speaker)
21. Darlene Flynn, Director of Race & Equity
22. Chloe Brown – U.S. House Oversight Committee Detailee (current PAC Commissioner)
23. UC Berkeley's Samuelson Law, Technology, and Public Policy Clinic (students Courtney Reed, Amisha Gandhi, Nomi Conway; supervising attorneys Erik Stallman, Megan Graham)
24. UC Berkeley's School of Information (Steve Trush, Daniel Griffin, Peter Rowland, Amy Turner)
25. Timandra Harkness "Big Data: Does Size Really Matter?" (featuring DAC ad hoc commission)
26. Cyrus Farivar "Habeas Data: Privacy vs. The Rise of Surveillance Tech" (featuring PAC)
27. Policing Project/Latham & Watkins (formal study of the PAC)

For questions regarding this report, please contact Brian Hofer, PAC Chair, at 510-303-2871.

Respectfully submitted,

Brian Hofer
Privacy Advisory Commission, Chair

Reviewed by:
Privacy Advisory Commission
Joe DeVries, Assistant to the City Administrator

Prepared by:
Brian Hofer
PAC Chair

Oakland Privacy Advisory Commission Workplan 2020-21							Last update 1-28-20							
Feb '20	Mar '20	Apr '20	May '20	Jun '20	Jul '20	Aug '20	Sep '20	Oct '20	Nov '20	Dec '20	Jan '21	Feb '21	Mar '21
OPD Remote Pole Camera Policy	OPD Automated License Plate Reader Policy	OPD FLIR Observation Tower Policy	OPD FLIR Helicopter Policy (conversion only)	OPD Body Worn Camera Policy	OPD Pen-Link Policy	OPD Starchaser Annual Report	OPD FLIR Boat Policy	OPD ShotSpotter Annual Report	OPD Cellebrite Policy		OPD Hostage Throw Phone Policy	OPD Robot - Land Policy	OPD Cellsite Simulator Policy (conversion only)
OPD Unmanned Aerial Device Policy		OPD Crime Lab Biometric Equipment Policy						OPD FLIR Helicopter Annual Report			OPD Live Stream Camera Annual Report	OPD Robot - Water Policy	
OPD Cell-site Simulator Annual Report												OPD Cell-Site Simulator Annual Report	
PAC Agenda Management	PAC Annual Report	PAC Privacy Principles					PAC Privacy Principles				PAC Privacy Principles		PAC Annual Report
				DOT Automated License Plate Reader Annual Report			DOT Dockless Data Sharing Annual Report						
			City Mgr Sanctuary Contracting Annual Report										

Department	Color
OPD	
DOT	
PAC	
OFD	
DPW	
City Manager/CPO	
IT	

OPD Surveillance Technologies with Priority List for Review by Oakland Privacy Advisory Commission (PAC)

Item	Description	Use Policy and Impact Report	Priority for bringing to PAC	Estimated Date to Bring Use Policy / Impact Report to PAC	Annual Report
Automated License Plate Recognition (ALPR)	Cameras photograph all seen license plates and use optical recognition software to structure text of license, and populate into license database for tracking	Draft to PAC; needed legal review of data retention schedule	3	Mar-20	n/a
Body Worn Camera (BWC)	Officer BWC manually used to record videos. Officers use docking system to upload to city-maintained server system, w/ plans to upgrade to cloud-storage system.	Draft to PAC; needed legal review of data retention schedule	5	Jun-20	n/a
Cell Site Simulator (Cell Phone Locator)	Machine to mimic cell phone tower signals and determine location of cell phones with predetermined identifiers for specific cell phones or in rescue mode to locate cell phones with unknown identifiers.	Pre-Surveillance Technology ordinance, OPD to revise policy into DGO format	11	Mar-21	Need to bring 2019 annual report to PAC Feb - 2020
Cellphone Data Extraction Equipment	Technology is used to manually download data from seized cell phones.	no	8	Nov-20	n/a
DNA Typing Technology (Crime Lab)	Various technologies used by OPD's crime lab to analyze DNA systems	no	4	Apr-20	n/a
FLIR Camera / Boat	Thermal and video camera in boat	no	7	Sep-20	n/a
FLIR Camera / Helicopter	Thermal and video camera in helicopter.	no	7	Sep-20	n/a
FLIR Camera / Portable Observation Tower	Thermal and video camera in portable manned observation tower.	no		Apr-20	n/a

Item	Description	Use Policy and Impact Report	Priority for bringing to PAC	Estimated Date to Bring Use Policy / Impact Report to PAC	Annual Report
GPS Tracker	Technology is used to track vehicles in relation to an investigation.	OPD brought policy and report to PAC; PAC recommended both to Council.	n/a	n/a	OPD to bring 2019 Annual Report to PAC by Aug-2020
Gunshot Locater Technology	OPD uses gunshot locater technology (ShotSpotter) to determine time and place as well as other data concerning gunshots.	PAC recommended the Use Policy and Impact Report; approved by City Council	n/a	n/a	Need to bring 2019 annual report to PAC by Oct 2020
Hostage Negotiation Throw Phone	The phone that OPD uses to throw into structures with hostage takers include communication capabilities.	no	9	Jan-21	n/a
Live-Stream Transmitter	Transmitter attached to a video camera to live-stream (not record) to the EOC.	Yes	n/a	n/a	Bring 2020 report in Jan 2021
Remote Mobile (Utility Pole) Camera	Video camera mounted to utility pole that can be moved to different locations, reviewed remotely.	As part of pre-combined policy with live-stream transmitter introduce to PAC in 2019	2	Feb-20	n/a
Remote Audio Telecommunications Monitoring (Pen-Link)	Technology is used to monitor private phone calls.	no	6	Jul-20	n/a
Robot (Land)	The OPD (land) robot for critical incident use includes remote access video capability, to the operator.	no	10	Feb-21	n/a
Robot (Water)	The OPD aquatic robot includes remote access video capability to the operator via cabled connection.	no	10	Feb-21	n/a

Item	Description	Use Policy and Impact Report	Priority for bringing to PAC	Estimated Date to Bring Use Policy / Impact Report to PAC	Annual Report
Thermal Imaging /VIDEO ATTIC Camera	Thermal and Infrared camera on mobile pole	PAC to review if falls under Surveillance Ordinance	n/a	TBD	n/a
Unmanned Aerial Devices (UAV) *	Remote operated aerial device to which video cameras can be mounted	Introduced Jan-20 to PAC	1	Jan-20	Bring 2019 Annual Report to PAC
*** = recently added to list**					