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 Agenda

***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**: Raymundo Jacquez III, **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 December meeting minutes
4. Chief Privacy Officer report - Privacy Principles status update and implementation
5. Chair/Vice Chair report – 2020 planning, PAC annual report, report tracking, agenda management
6. Surveillance Equipment Ordinance – OPD – Live Stream Camera Impact Report and proposed Use Policy – review and take possible action
7. Surveillance Equipment Ordinance – OPD – UAS (Drone) Impact Report and proposed Use Policy – review and take possible action
8. Surveillance Equipment Ordinance – OPD – Biometric Data Analysis (DNA Crime Lab) funding request – review and take possible action
9. Adjournment at 7:00pm

CITY OF OAKLAND

Privacy Advisory Commission

December 5, 2019 5:00 PM
Oakland City Hall
Hearing Room 1
1 Frank H. Ogawa Plaza, 1st Floor
Regular Meeting Agenda

***Commission Members**: **District 1 Representative**: Reem Suleiman, **District 2 Representative**: Chloe Brown, **District 3 Representative**: Brian M. Hofer, **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*

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

Present: Brown, Suleiman, Tomlinson, Hofer, Katz, Gage, Patterson, Oliver

2. Open Forum/Public Comment

There were no Open Forum Speakers.

3. Review and approval of the draft November meeting minutes

The November Minutes were approved unanimously.

4. Surveillance Equipment Ordinance – OFD – Data Collection for Wildfire District and Fire Safety Inspections Impact Statement and proposed Use Policy – review and take possible action

Chairperson Hofer noted this is the second review of the Policy and Impact Statement and that there were some outstanding questions last month. OFD Captain Sanders explained that the impact statement changed, but the Use Policy is essentially the same as last month. Member Oliver raised the concern about what portion of California Code allows OFD to photograph private property and Chairperson Hofer noted where it is now highlighted in the Impact Statement.

Member Katz had questions about how OFD avoids photographing the outside of a building and also access to the photographs. Captain Sanders clarified that only the property owner can have access to the photos—not the general public. Member Katz suggested some clarifying language in the Impact Statement that was accepted.

Chairperson Hofer asked for clarifying language under 3rd party data sharing noting that it should clarify which city (City of Oakland) and (registered) owners have access to the photos.

There were some additional questions about access to the photos for owners without internet access and Captain Sanders responded that owners can visit the bureau and view them in person. There were also questions about old data being transferred to the new Accela system but Captain Sanders noted that the photos are only part of the new system.

Member Brown asked about clarification as to when OFD would take phots inside a property and Chairperson Hofer proposed some clarifying language about consent and/or court ordered access.

With the suggested edits, the PAC voted unanimously to approve the Impact Statement and Use Policy and forward it to the City Council.

5. Federal Task Force Transparency Ordinance – OPD – FBI's Joint Terrorism Task Force MOU – review and take possible action

Chairperson Hofer opened the conversation noting that this is 3rd or 4th time the PAC has reviewed this document this year and had an ad hoc committee work directly with OPD staff to try to offer amendments that align with the PAC's mission. Unfortunately, the ad hoc committee felt that it was not possible to get this accomplished and is proposing an alternate resolution concluding that the Coty of Oakland not participate in the JTTF. He articulated that it is not about OPD, but is about the parts of the agreement that are outside of their control; specifically, the federal guidelines.

Bruce Stoffmacher articulated that he felt OPD could monitor whether the FBI would ask them to violate a the policy and that the PAC should support and forward OPD's resolution to Council. He distinguished between OPD and the polices being considered and the recently published "white paper" that highlighted problems with the JTTF and local control versus federal overstep. He also stated that the FBI said they were willing to meet with the PAC ad hoc committee annually. Finally, he noted that this is a 3 year MOU not permanent and that OPS was trying to strike a compromise.

There were three public speakers on this item:

Ali Talib with the Asian law caucus urged voting in support of the alternative resolution, and against the OPD one. He noted that the Federal government has a recent track record of separating families and religious discrimination.

Jeff Wang, also with the caucus noted that the white paper showed FBI officials allowed and directed local officers to violate the local policies that has been put in place and discriminated against the Muslim community on numerous occasions.

Javeria Jamil, also with Asian Law Caucus noted that the FBI surveils and targets vulnerable communities.

Member Katz asked if the FBI reached out to OPD to enter into the JTTF or did Oakland reach out to FBI?

-Bruce stated that he was not sure of the history but at this point in time, it's mutual, both departments see the value in collaborating.

Member Suleiman pointed out that the City is already working with the FBI on the homicide task force and the PAC supports that relationship but sees little benefit to joining this terrorism task force based on its track record. She does not understand the possible added benefits in this MOU which is written on the FBI's terms.

Member Tomlinson asked how the JTTF is working for other cities and Bruce pointed out that SF had thoughts of revisiting their removal from task force after the Pier 39 incident. He explained that the main benefit is an OPD officer can go into FBI buildings and get access to their meetings, can get alerts, and share intelligence.

Vice Chair Patterson asked about whether the OPD officer assigned previously was active, pointing out that the lack of activity in 2018 caused her to struggle to understand the benefits as well. Chairperson Hofer stated that Federal agencies will still notify OPD if there's a real threat and collaborate with them. He pointed out that the FBI's definition of terrorism is just challenging the status quo and first amendment protected activity and that the City and Feds already have a violent crime task force.

Chairperson Hofer made a motion to adopt the alternative resolution, Member Oliver seconded the motion and it passed unanimously.

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

Lt. Mark Rhoden presented the Impact Statement, Policy, and gave an overview of the technology. He explained that it is only used when OPD has already decided person is arrestable before it can be used and the purpose is to avoid the arrest. There is no cost to OPD since Alameda County pays and maintains the database and no information is saved or stored. The only data is data already in the CRIMS database.

This technology will eliminate the time of taking someone to jail just because the officer cannot ID them and there is no 5th amendment issue because it's by consent. Member Oliver asked if this has this been submitted to the Monitor, Bruce said it had not. There were some other clarifying questions about the purpose and use of the equipment and the item was continued to the January Meeting.

7. Election of PAC Vice Chair

Chairperson Hofer nominated Member Heather Patterson to be the new Vice Chair, this was seconded by Reem Suleiman and approved unanimously.

TO: Oakland Privacy Advisory Commission,
Joe Devries, Chief Privacy Officer

From: Commissioner Reem Suleiman

RE: Implementation Roadmap for Newly Adopted "Privacy Principles"

I. **Purpose:** The purpose of this document is to serve as a roadmap to implement the "Privacy Principles," also known as the "Principles," designed by the Samuelson Law, Technology & Public Policy Clinic at Berkeley Law. The roadmap is divided into three major phases that detail concrete and pragmatic steps the City of Oakland can take to integrate and institutionalize the "Principles" into various City department workflows. The recommendations provided are based on the guidance and examples provided to us by the Samuelson clinic, paying particular attention to departments that 1) operate surveillance technologies and/or 2) collect PII to provide services. The progression of each phase is predicated on budgetary approval and staff resourcing. Thus I have included additional sections on budgetary opportunities and proposed timelines for each phase outlined below.

II. **Background**: Over the course of several months, fellows at the Samuelson Law, Technology & Public Policy Clinic at Berkeley Law conducted privacy research for the Commission alongside a series of interviews with members of the PAC, City Department heads, and community stakeholders. They developed the following set of seven "Privacy Principles" for the City of Oakland, which was adopted by the Privacy Advisory Commission officially on [insert date]:
    A. Principle I: Design and use equitable privacy practices
    B. Principle II: Limit collection and retention of personal information
    C. Principle III: Manage personal information with diligence
    D. Principle IV: Extend Privacy Protections to our relationships with third parties
    E. Principle V: Safeguard individual privacy in public records disclosures
    F. Principle VI: Be transparent and open
    G. Principle VII: Be accountable to Oaklanders

III. **Implementation, Phase I:**
    A. **Update retention schedules: [**Principle II, limit collection and retention of personal information] Work with the City Clerk's Office to revisit the retention schedules for all applicable data collected by surveillance technologies and City departments. Work with the City Clerk to create a timeframe for these to be updated according to the retention schedules outlined in their respective and approved Impact and Use reports.
    B. **Conduct a survey/ sweep for "sleeping data" [**Principle II, limit collection and retention of personal information; Principle III]: Manage personal information with diligence] In collaboration with the City Clerk's Office and CPO, survey all

databases from Tier I and Tier II City departments in search for obsolete or dormant data. Once that sweep has been conducted, seek guidance from PAC to determine whether sets should be destroyed, protected, or set on a new retention schedule.

C. **Request impact assessments from various departments (ongoing):** [Principle I: Design and use equitable privacy practices] WIth the direction and coordination of the CPO, continue to encourage city agencies to be proactive in preparing impact and use policies for all surveillance technologies or data collection practices as required by law, and to approach the PAC for guidance if unsure as to whether a particular item falls under the purview of the Ordinance. Already, several City departments (including the Department of Transportation, the Port Authority, and the IT Department) have been proactive in reaching out to the PAC for conversations around safeguarding Oaklanders right to privacy in its data collection practices.

D. **Create boilerplate language for forms and surveys that collect Oaklanders personal information** [Principle VI: Be transparent and open] Create boilerplate privacy language that City Departments can use on public-facing documents, service forms, and surveys --particularly those that request Oaklanders' PII. Ask each Department to customize language to include what types of information the City will collect and store from the document (and preferably for how long, if applicable).

E. **Create boilerplate data sharing and privacy agreements for third-party contractors and vendors [**Principle IV: Extend Privacy Protections to our relationships with third parties] Similarly, the PAC can create some guidance and best practices for City departments to assist them in creating contracts, agreements, and MOUs with third party contractors and vendors that put Oaklanders privacy front and center and safeguard against misuse of any data or PII visible to the third-party.

IV. Implementation, Phase II:

A. **Develop an accessible website to host privacy information, policies and resources**: [Principle VI: Be transparent and open; Principle VII: Be accountable to Oaklanders] The City of Seattle hosts on its website a page dedicated to "Privacy initiatives." The interface includes the option to comment on a surveillance technology, read a description of its privacy program, review the City's list of surveillance technologies (and related use policies), search "Privacy Impact Assessments" for particular projects and programs, and view all the personally identifiable information (PII) collected by the City of Seattle. With limited resources dedicated to the PAC and CPO, the City of Oakland is not in an immediate position to replicate the scale of Seattle's microsite without additional sources of budgetary funding. However, I have outlined the following

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

Item	Description	OPD Policy?	Impact Use Stmnt to PAC?	Priority for bringing to PAC	Estimated Date - Impact Stmt and Policy to PAC
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.	no	no	2	Dec-18
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.	no	no	3	Jan-19
Cell Site Simulator	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	no	1	Nov-18
Cellphone Data Extraction Equipment	Technology is used to manually download data from seized cell phones.	no	no	10	Aug-19
FLIR Camera / Boat	Thermal and video camera in boat	no	no	5	Mar-19
FLIR Camera / Helicopter	Thermal and video camera in helicopter.	no	no	5	Mar-19
FLIR Camera / Portable Observation Tower	Thermal and video camera in portable manned observation tower.	no	no	5	Mar-19
GPS Tracker	Technology is used to track vehicles in relation to an investigation.	no	no	6	Apr-19

Gunshot Locater Technology	OPD uses gunshot locater technology (ShotSpotter) to determine time and place as well as other data concerning gunshots.	no	no	4	Feb-19
Hostage Negotiation Throw Phone	The phone that OPD uses to throw into structures with hostage takers include communication capabilities.	no	no	12	Oct-19
IP Addresses of live-streamed privately-owned video cameras voluntarily provided by business owners	Business owners voluntarily provide IP addresses of private video cameras to OPD personnel.	no	no	9	Jul-19
Pole-mounted Video Camera	Video camera on a pole that can be moved to different locations and powered by utility. Reviewed remotely.	no	no	8	Jun-19
Remote Audio Telecommunications Monitoring	Technology is used to monitor private phone calls.	no	no	11	Sep-19
Robot (Land)	The OPD (land) robot for critical incident use includes remote access video capability, to the operator.	no	no	13	Nov-19
Robot (Water)	The OPD aquatic robot includes remote access video capability to the operator via cabled connection.	no	no	13	Nov-19
Thermal Imaging /VIDEO ATTIC Camera	Thermal and Infrared camera on mobile pole	no	no	12	Oct-19
Unmanned Aerial Devices (UAV)*	Remote operated aerial device to which video cameras can be mounted	no	no	7	May-19
* = recently added to list					

OAKLAND POLICE DEPARTMENT

Surveillance Impact Report for Live Stream Transmitter

1. Information Describing Live-Stream Transmitters and How They Work

OPD utilizes different types of cameras to capture single image and video data. Cameras that are strictly manually operated are not considered "surveillance technology" under the Oakland Surveillance Ordinance No. 13489 C.M.S. Handheld Live stream transmitters are affixed to handheld video cameras are manually operating cameras connected to a transmitter to allow the live stream transmission to a different location such as OPD and the City of Oakland have Emergency Operations Centers (EOC). The camera and transmitter are operated by a team of two or more uniformed officers, referred to as Video Teams. OPD and the City of Oakland have Emergency Operations Centers (EOC). Cameras attached to handheld live stream transmitters "handheld live stream cameras" allow an officer to transmit a live view of what they see to the EOC.

2. Proposed Purpose

Live stream camera transmitters allow OPD to deploy a minimal level of police presence while providing critical situational awareness to OPD commanders. A small number of officers can monitor events and provide real-time footage to Command. This information helps OPD Command to make efficient deployment decisions. OPD at times must otherwise deploy ten or more officers and sergeants to events where crowds or large events are occurring – so that officers can adequately convey local information to remote-stationed commanders. At times people in crowds and large events might not appreciate or understand the need for a large police presence – the transmitters allow OPD to maintain needed information with a minimal police footprint.

3. Locations Where, and Situations in which Live Stream Transmitters May be Deployed or Utilized.

Live stream transmitters may be used anywhere in the public right of way within the City of Oakland – under conditions outlined in Department General Order (DGO) I-23 Live Stream Transmitter Use Policy, III.A 'Authorized Use': "Live stream transmitters are authorized by OPD…when such exigent circumstances exist – and when a city commander (captain or above) has authorized a partial

or full activation of the City's Emergency Operations Center (EOC) as well as the use of the live-stream transmitters." Personnel may use transmitters within in the public right of way within the City of Oakland; however, these cameras are generally only used for mass-person events to as to provide situational awareness during events where public safety must be monitored (e.g. large gatherings of people and/or parades. ***OPD's 2018 4th Quarter Crowd Control Report is provided as an attachment*** to this report to provide relevant data on events where OPD may use live stream transmitters for crowd situational awareness.

4. Privacy Impact

OPD recognizes that the use of live stream transmitters in the public right of way raises civil liberties concerns. There is concern that the use of this technology can be utilized to identify the activity, behavior, and/or travel patterns of random individuals, and that this usage may have a chilling effect on protected activity; however, OPD only proposes to use live stream transmitters under specific conditions – DGO I-23 III: "General Guidelines, A. Authorized Use" explains that a critical use restriction as: "Large events with numerous people pose challenges to public safety. Live stream transmitters are authorized, by an OPD commander (captain or above) when exigent circumstances exist – and 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) has approved the use of the live-stream transmitters.

OPD does not randomly employ this technology throughout the City. Rather, these transmitters are only used during events where public safety has a greater likelihood of being negatively impacted, or where there is a need to provide an Incident Commander real time information to manage resources for a given situation.

Live stream transmitters offer situational awareness in numerous ways that challenge measurement. 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; OPD needs to see where people present in order to adjust resources in real-time to better ensure public safety is maximized.

5. Mitigations

"Protected Activity" means all rights including without limitation: speech, associations, conduct, and privacy rights including but not limited to expression, advocacy, association, or participation in expressive conduct to further any political or social opinion or religious belief as protected by the

United States Constitution and/or the California Constitution and/or applicable statutes and regulations. The First Amendment does not permit government "to forbid or proscribe advocacy of the use of force or of law violation except where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action." *White v. Lee* (9th Cir. 2000) 227 F.3d 1214, 1227; *Brandenburg v. Ohio* (1969) 395 U.S.

In respect to honoring protected activity, OPD's DGO I-23: Live Stream Transmitter Use Policy restricts the use of the technology as follows:

1. Department members shall not use or allow others to use handheld live-stream cameras, software or data for any unauthorized purpose.
2. Personnel shall not affix a live-stream camera to any fixed structure and not remain present at the same location; livestream cameras shall not be used for any remote surveillance.
3. Live stream transmitters shall not be except when authorized by the Chief of Police or designated commander.

All live-stream transmitters shall be housed and secured within the Police Administration Building only accessible to authorized personnel. Regular camera data, if the camera attached to a live stream transmitter is recording data, shall be uploaded onto a secure computer at the with user and email password protection, stored with OPD's IT Unit within the Police Administration Building (PAB). For data that is captured and used as evidence, such data shall be turned in and stored as evidence pursuant to existing policy. Otherwise, camera data will be destroyed after 30 days.

OPD will monitor its use of live stream transmitters to ensure the accuracy of the information collected and compliance with all applicable laws. The IT Unit Coordinator and/or designated staff shall provide the Chief of Police, Privacy Advisory Commission, and Public Safety Committee with an annual report that contains activity usage information for the following for the previous 12-month period. This report shall be compliant with reporting aspects outlined in Ordinance No. 13489 C.M.S.

6. Data Types and Sources

Live stream transmitters attached to cameras that record directly onto an internal memory device (e.g. secure digital (SD) card) and operate similar to consumer digital video cameras. These types of cameras contain an internal storage device for storing audio and video data – an integrated element that can be connected to a computer for data downloads, or a removable device (e.g. SD card) which can be connected to a computer for digital downloads.

Live stream transmitters can use different technologies (e.g. cellular 3G/4G/5G, LTE, WiFi, Ethernet, and Microwave) to transmit the video stream. Transmitters allow the live-stream images or video to be viewed on a screen with the appropriate data connection and reception technology. The

transmitters specifically transmit the data to a receiver where the data can then be viewed (OPD only has receivers at the EOC).

7. Data Security

Live stream transmitters shall be housed and secured within the Police Administration Building and not accessible with to the public or to personnel without permission to use such equipment. Regular camera data shall be uploaded onto secure computer with user and email password protection, stored with OPD's IT Unit within the Police Administration Building. For data that is captured and used as evidence, such data shall be turned in and stored as evidence pursuant to existing policy. Otherwise, camera data will be destroyed after 30 days.

8. Costs

OPD currently has four transmitters from TVU networks that allow standard single shot or video cameras to live-stream data to OPD's Administration Building or the City's Emergency Operations Center (this data is not recorded). These transmitters are approximately eight years old. OPD does not currently pay for ongoing maintenance service; the cost to upgrade the unsupported system would cost about $120,000 for a two-year maintenance contract and then $12,000 for additional years. OPD is planning to use approximately $130,000 from the Justice Assistance Grant (JAG) Program[1] to pay four new modern TVU Networks transmitters.

9. Third Party Dependence

OPD uses TVU Networks-brand transmitter and receiver equipment for live-stream video transmission. This is an encrypted point-to-point data stream, only accessible via the receiver.

10. Alternatives Considered

OPD officers and personnel rely primarily on traditional policing techniques to monitor large events and to gather evidence related to criminal investigations. For decades evidence gathering also includes the use of cameras, sometimes with live-stream transmitters, to record images, video and audio. Police personnel must maintain some level of situational awareness when hundreds and thousands of people gather on public streets and threats to public safety increase. Alternatives to live-stream cameras would include having more officers and personnel deployed during every mass-event. Such a deployment extends beyond OPD budget capacity.

[1] https://www.bja.gov/jag/

11. Track Record of Other Entities

OPD has not yet found others agencies using live stream transmitters with mobile cameras to live stream crowd-control events. However, OPD will continue to research the use of the technology by other agencies.

DEPARTMENTAL GENERAL ORDER

I-23: LIVE STREAM TRANSMITTER USE POLICY

Effective Date:
Coordinator: Information Technology Unit, Bureau of Services Division

---

HANDHELD LIVESTREAM CAMERA

The purpose of this order is to establish Departmental policy and procedures for the use of Live Stream Transmitters.

I. VALUE STATEMENT

The protection of human life and the general safety of the public shall be the primary consideration when deciding to use handheld live stream cameras.

II. DESCRIPTION OF THE TECHNOLOGY

A. Live Stream Transmitter Components

Transmitters can send a wireless signal to a specific location such as the City's Emergency Operation Center (EOC).

B. Purpose

Live stream camera transmitters allow OPD to deploy a minimal level of police presence while providing critical situational awareness to OPD commanders. A small number of officers can monitor events and provide real-time footage to Command. This information helps OPD Command to make efficient deployment decisions.

C. How the System Works

Live stream transmitters support real-time transmission and remote live-stream viewing. Transmitters can use different formats (e.g. cellular 3G/4G LTE, WiFi, Ethernet, and Microwave). Transmitters can be connected to static single image digital video cameras. Transmitters allow the live-stream video to be viewed on a screen with the appropriate data connection and reception technology (receiver). The transmitters specifically transmit the stream to a receiver where the video can then be viewed.

III. GENERAL GUIDELINES

A. Authorized Use

There are different situations that can occur in the City of Oakland which will justify the use of live-stream transmitters. Large events with numerous people pose challenges to public safety. Live stream transmitters 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 live-stream transmitters. 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 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 cameras with live-streaming transmitters can provide important situational awareness to OPD without the need to deploy many officers. Live stream transmitters shall only be deployed with authorizations from an incident commander.

Personnel authorized to use live-stream cameras or access information collected through the use of such equipment shall be specifically trained in such technology and authorized by the Chief of Police or designee. Any sworn officer may utilize hand-held live-stream cameras with the approval of OPD's Information Technology (IT) Unit Coordinator.

B. Restricted Use

1. Department members shall not use or allow others to use handheld live-stream transmitters, software or data for any uses not enumerated above in III.A.

2. Personnel shall not affix a handheld live-stream camera to any fixed structure and not remain present at the same location;

livestream cameras shall not be used for any remote surveillance.

3. The Handheld Live Stream Camera (Captain or higher rank) shall not be used to except when approved by a police commander

C. Communications

For clarity of communications, radio traffic should identify the units using such device as a "Video Team." Video Teams are made up of two to three uniformed officers. An equipment officer (videographer) and security officers.

IV. LIVE STREAM CAMERA DATA

A. Data Collection

Live stream transmitters do not store data. Regular camera data, if the camera attached to a live stream transmitter is recording data, shall be uploaded onto a secure computer at the with user and email password protection, stored with OPD's IT Unit within the Police Administration Building (PAB).

B. Retention

Handheld live stream cameras can send the digital stream wirelessly. The EOC does not record this data; data recorded by the handheld cameras is maintained by the OPD IT Unit within in the Bureau of Services (BOS). Personnel using live-stream cameras shall return them at the end of their shift to the IT Unit.

For data that is captured and used as evidence, such data shall be turned in and stored as evidence pursuant to existing policy. Otherwise, camera data will be destroyed after 30 days.

C. Data Access

OPD's IT unit shall be responsible for the maintenance and storage of live-stream cameras. Members approved to access live-stream camera data under these guidelines are permitted to access the data for administrative (force investigation or citizen complaints) or criminal investigation purposes.

Live-stream camera 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:

4. The agency makes a written request for the 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.

5. The request is reviewed by the Bureau of Services Deputy Chief/ Deputy Director or designee and approved before the request is fulfilled.
6. 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. A request from the public to access handheld camera data shall follow standard public records request protocols. The EOC does not record livestream camera footage.

D. Third Party Data Sharing

OPD currently uses TVU Networks-brand transmitters; however, no data is shared with TVU networks. Data is only transmitted from OPD equipment to the City's and/or OPD's EOC.

E. Data Protection and Security

All live-stream transmitters shall be housed and secured within the Police Administration Building only accessible to authorized personnel.

Live-stream camera data will be closely safeguarded and protected by both procedural and technological means. All live-stream cameras shall be housed and secured at the Police Administration Building only accessible by authorized personnel within IT Unit or lockers.

V. LIVE STREAM TRANSMITTER ADMINISTRATION

A. System Coordinator / Administrator

The Oakland Police Department will monitor its use of the live stream cameras to ensure the accuracy of the information collected and compliance with all applicable laws, including laws providing for process, and time period system audits.

The IT Coordinator, or other designated OPD personnel shall provide the Chief of Police, Privacy Advisory Commission, and City Council with an annual report that covers use of the technology during the previous year. The report shall include all report components compliant with Ordinance No. 13489 C.M.S.

The IT Unit Coordinator is responsible for ensuring systems and processes are in place for the proper collection, accuracy and retention of live-stream camera system data.

B. Maintenance

There is no data created by use of live stream camera transmission. The cameras transmitters encrypt data during transit to ensure the security and integrity of the data feed.

C. Training

The Training Section shall ensure that members receive department-approved training for those authorized to use or access live-stream cameras.

D. Auditing and Oversight

The Project Coordinator will be responsible for coordinating audits every year to assess system use. 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

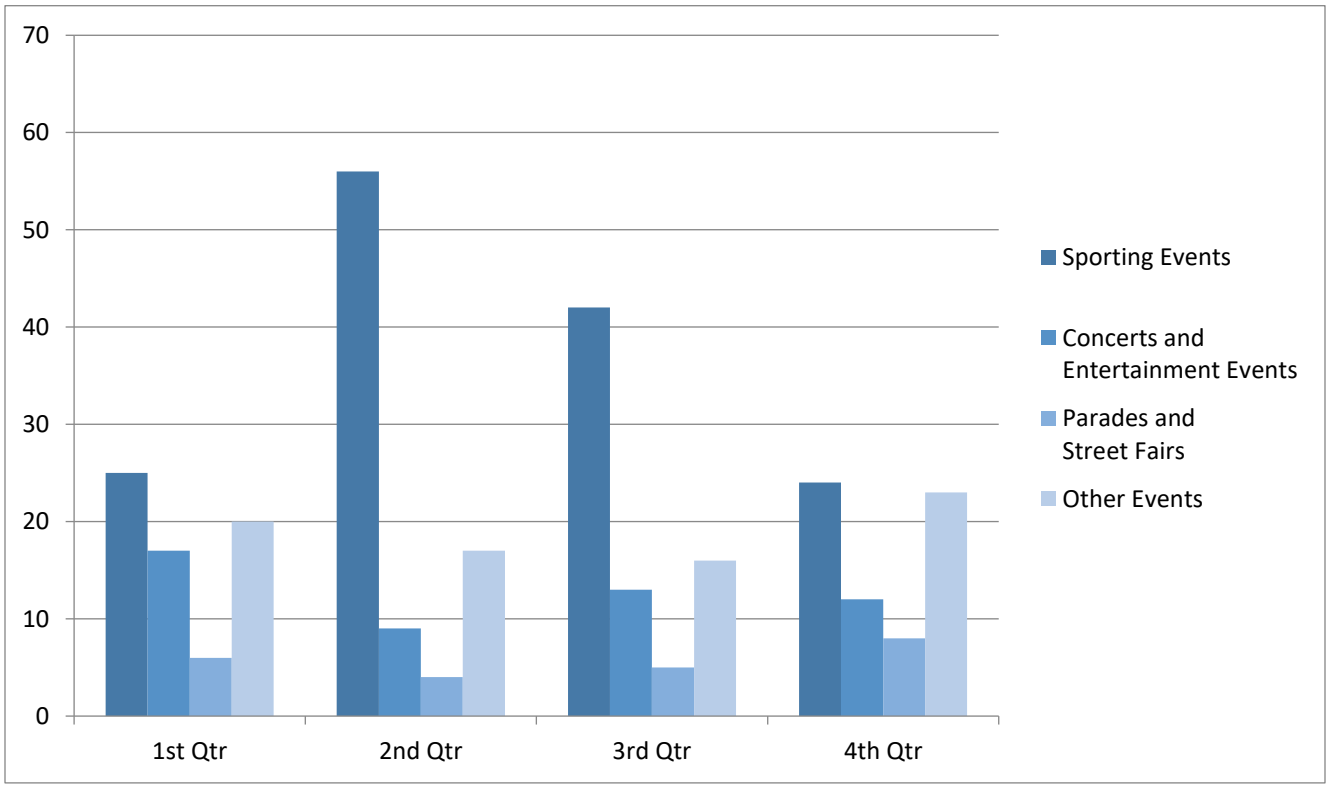
Anne E. Kirkpatrick
Chief of Police Date Signed:

Oakland Police Department

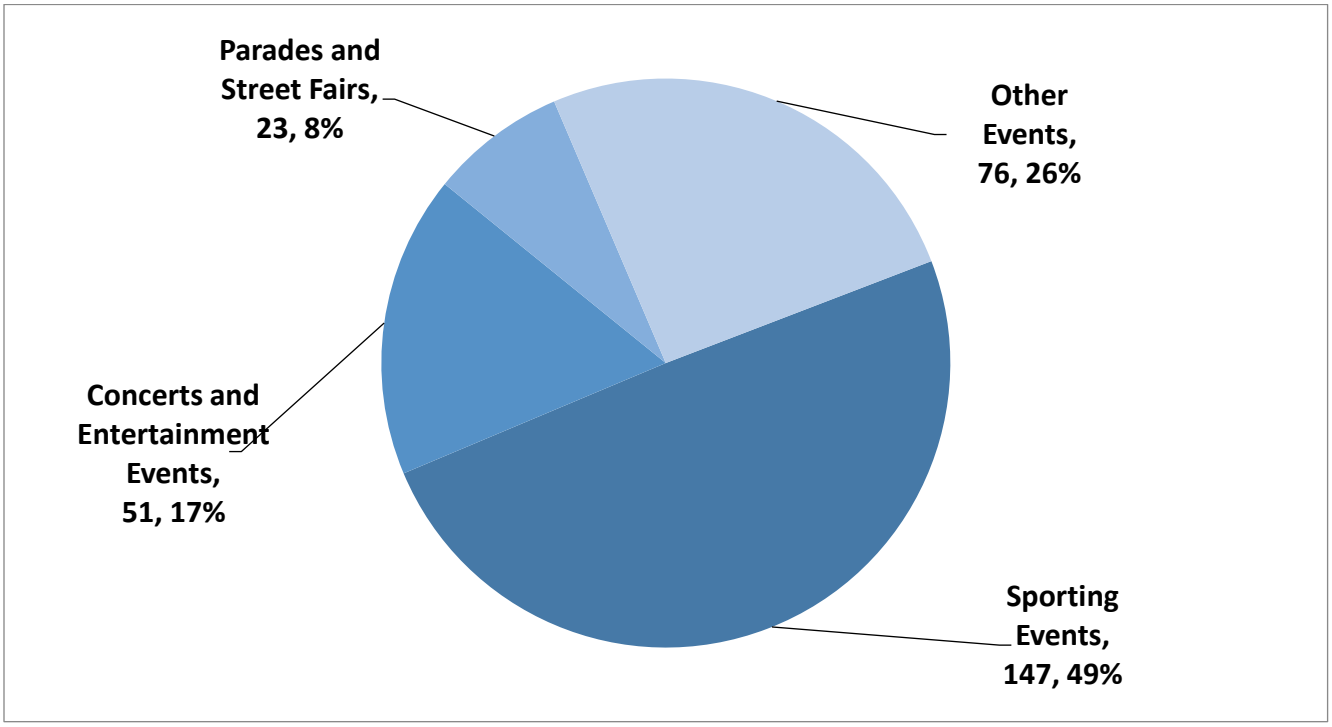
2018 4th Quarterly Crowd Control Report **Reporting Period: 01 Oct 18 – 31 Dec 18**

This document is the Annual and 4th Quarterly report for all City of Oakland crowd control/management events of 2018.

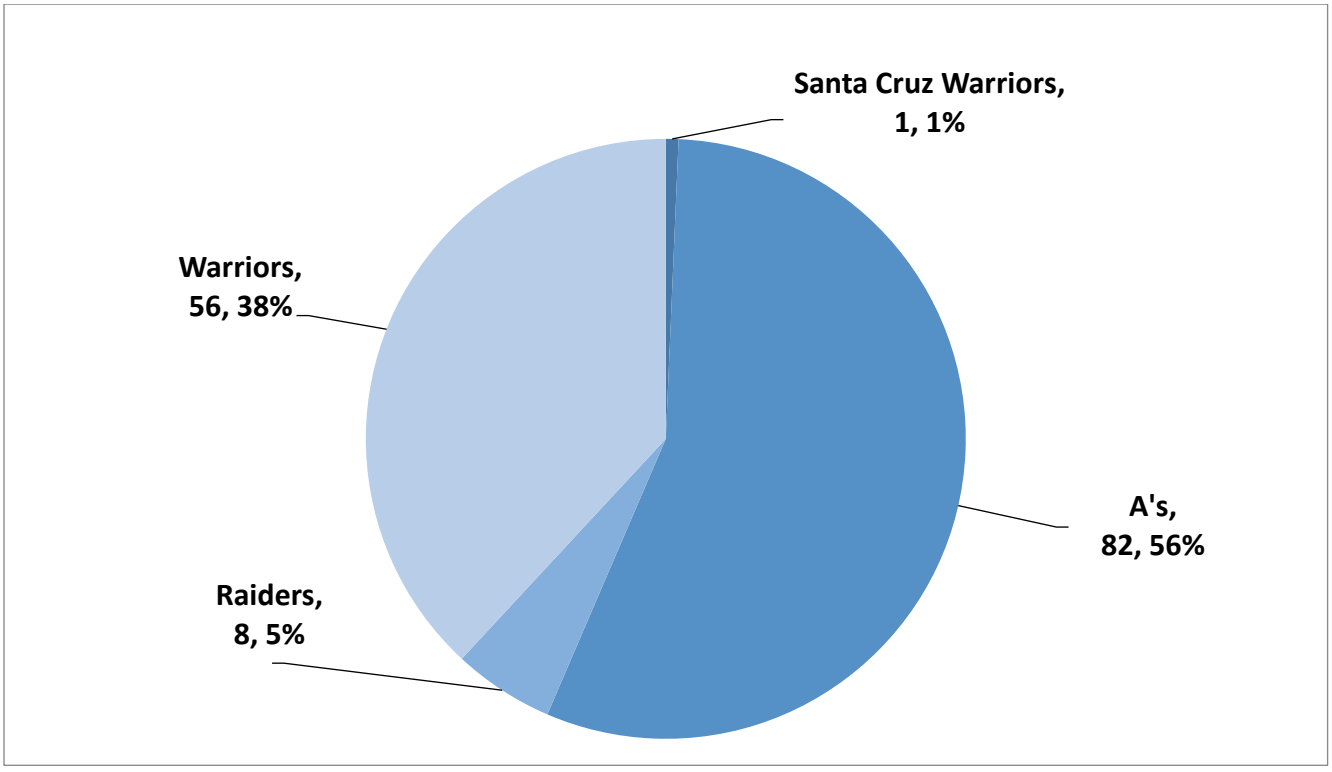
2018					
Event Type	**1st QTR**	**2nd QTR**	**3rd QTR**	**4th QTR**	**TOTAL**
Sporting Events (Raiders/Warriors/A's)	25	56	42	24	**147**
Concerts and Entertainment Events	17	9	13	12	**51**
Parades and Street Fairs	6	4	5	8	**23**
Other Events (Protests, Marches, etc.)	20	17	16	23	**76**
TOTAL EVENTS	**68**	**86**	**76**	**67**	**297**



2018 EVENT TYPE TOTALS



2018 SPORTING EVENT TOTALS

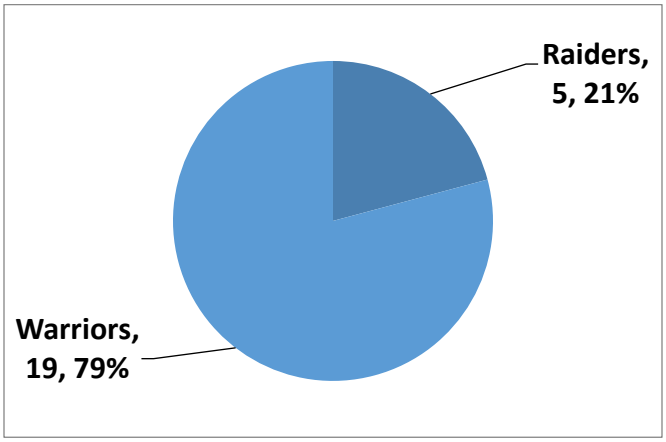


TOTAL PERFORMANCE DATA: 2018 Year in Review								
Event Type	**Events**	**Attended**	**OPD**	**Complaints**	**Arrests**	**Citations**	**Ejections**	**Uses of Force**
Sporting Events	147	2,834,284	5,984	4	50	70	177	4
Concerts and Entertainment Events	51	657,297	1,444	3	26	65	39	2
Parades and Street Fairs	23	1,280,900	1,331	1	15	202	1	0
Other Events	76	83,202	1,386	3	2	13	0	8
TOTALS	**297**	**4,855,683**	**10,145**	**11**	**93**	**350**	**217**	**14**

2017					
Event Type	**1st QTR**	**2nd QTR**	**3rd QTR**	**4th QTR**	**TOTAL**
Sporting Events (Raiders/Warriors/A's)	21	60	44	27	**152**
Concerts & Entertainment Events	18	10	24	20	**72**
Parades & Street Fairs	3	6	21	5	**35**
Other Events (Protests, Marches, etc.)	22	11	25	18	**76**
TOTAL EVENTS	**64**	**87**	**114**	**70**	**335**

TOTAL PERFORMANCE DATA: 2017								
Event Type	**Events**	**Attended**	**OPD**	**Complaints**	**Arrests**	**Citations**	**Ejections**	**Uses of Force**
Sporting Events	152	2,621,971	5,702	4	72	96	223	**5**
Concerts and Entertainment Events	72	641,642	1,081	3	35	31	15	**0**
Parades and Street Fairs	35	1,384,550	1,112	1	7	14	7	**1**
Other Events	76	137,747	4,353	0	12	126	0	**5**
TOTALS	**335**	**4,785,910**	**12,248**	**8**	**126**	**267**	**245**	**11**

SPORTING EVENTS: RAIDERS/WARRIORS/A'S



Date	Event Type	Attended	OPD	Complaints	Arrests	Citations	Ejections	Uses of Force
16-Oct-18	**Warriors vs Thunder**	19,052	36	0	1	0	1	0
22-Oct-18	**Warriors vs Suns**	19,000	36	0	0	0	0	0
24-Oct-18	**Warriors vs Wizards**	18,000	36	0	0	0	4	0
28-Oct-18	**Raiders vs Colts**	43,776	140	0	5	11	12	0
31-Oct-18	**Warriors vs Pelicans**	17,400	36	0	0	0	1	0
05-Nov-18	**Warriors vs Grizzlies**	16,893	36	0	0	0	2	0
08-Nov-18	**Warriors vs Bucks**	18,000	36	0	0	0	0	0
10-Nov-18	**Warriors vs Nets**	18,000	36	0	0	0	0	0
11-Nov-18	**Raiders vs Chargers**	40,245	140	0	3	5	8	0
13-Nov-18	**Warriors vs Hawks**	18,000	36	0	0	0	0	0
21-Nov-18	**Warriors vs Thunder**	18,000	36	0	0	0	0	0
23-Nov-18	**Warriors vs Trail Blazers**	17,931	36	0	0	0	0	0
24-Nov-18	**Warriors vs Kings**	18,000	36	0	0	0	0	0
26-Nov-18	**Warriors vs Magic**	18,000	36	0	1	0	0	0
02-Dec-18	**Raiders vs Chiefs**	42,412	140	0	0	4	11	0
09-Dec-18	**Raiders vs Steelers**	48,424	154	0	3	1	28	0
10-Dec-18	**Warriors vs Timberwolves**	17,500	36	0	0	0	0	0
12-Dec-18	**Warriors vs Raptors**	18,000	36	0	0	0	0	0
17-Dec-18	**Warriors vs Grizzlies**	17,817	35	0	0	0	0	0
22-Dec-18	**Warriors vs Mavericks**	18,400	35	0	1	0	0	0
23-Dec-18	**Warriors vs Clippers**	18,000	35	0	0	0	0	0
24-Dec-18	**Raiders vs Broncos**	48,000	160	0	0	2	18	2
25-Dec-18	**Warriors vs Lakers**	18,000	35	0	1	0	0	0
27-Dec-18	**Warriors vs Trail Blazers**	18,000	35	0	0	0	0	0
SPORTING EVENTS TOTALS		**Attended**	**OPD**	**Complaints**	**Arrests**	**Citations**	**Ejections**	**Uses of Force**
		564,850	**1413**	**0**	**15**	**23**	**85**	**2**

CONCERTS AND ENTERTAINMENT EVENTS

Date	Event Type	Attended	OPD	Complaints	Arrests	Citations	Ejections	Uses of Force
26-Oct-18	**Aubrey & the Three Migos Tour**	17,000	27	0	0	0	0	0
27-Oct-18	**Aubrey & the Three Migos Tour**	13,000	28	0	0	0	2	0
29-Oct-18	**Aubrey & the Three Migos Tour**	16,156	35	0	2	0	7	0
31-Oct-18	**Halloween Takeover Sideshow**	0	23	0	0	0	0	0
11-Nov-18	**Twenty One Pilots Concert**	14,000	29	0	0	0	0	0
17-Nov-18	**Kevin Hart Irresponsible Tour**	10,000	22	0	2	0	0	0
25-Nov-18	**Fleetwood Mac Concert**	13,000	23	0	0	0	0	0
28-Nov-18	**Trans-Siberian Orchestra**	5,972	23	0	0	0	0	0
11-Dec-18	**Childish Gambino**	11,000	27	0	1	1	2	0
15-Dec-18	**WWE Live Holiday Tour**	7,000	9	0	0	0	0	0
16-Dec-18	**Travis Scott: Astroworld Tour**	12,000	32	0	0	0	5	0
31-Dec-18	**New Year's Eve Deployment**	20,000	50	0	2	0	0	1
CONCERTS AND ENTERTAINMENT EVENTS TOTALS		**Attended**	**OPD**	**Complaints**	**Arrests**	**Citations**	**Ejections**	**Uses of Force**
		139,128	**328**	**0**	**7**	**1**	**16**	**1**

PARADES AND STREET FAIRS

Date	Event Type	Attended	OPD	Complaints	Arrests	Citations	Ejections	Uses of Force
05-Oct-18	**First Friday**	15,000	41	0	3	5	0	0
13-Oct-18	**DC Wonder Woman Running Series 5K and 10K**	1,500	52	0	0	0	0	0
13-Oct-18	**Treasure Island Music Festival**	6,000	18	0	0	0	0	0
14-Oct-18	**Treasure Island Music Festival**	7,000	18	0	0	0	0	0
02-Nov-18	**Postponed First Friday**	1,000	23	0	1	87	0	0
04-Nov-18	**Día De Los Muertos**	80,000	38	0	0	0	0	0
22-Nov-18	**Oakland Turkey Trot**	3,000	17	0	0	0	0	0
07-Dec-18	**First Friday**	10,000	51	0	3	28	0	0
PARADES AND STREET FAIRS TOTALS		**Attended**	**OPD**	**Complaints**	**Arrests**	**Citations**	**Ejections**	**Uses of Force**
		123,500	**258**	**0**	**7**	**120**	**0**	**0**

OTHER EVENTS: PROTESTS, MARCHES, ETC.

Date	Event Type	Attended	OPD	Complaints	Arrests	Citations	Ejections	Uses of Force
02-Oct-18	**All Eyes on the Sheriff**	75	4	0	0	0	0	0
06-Oct-18	**Anti-Confirmation: Judge Kavanaugh "Oakland Does Not Consent"**	100	8	0	0	0	0	0
07-Oct-18	**Sonny's 80th Birthday Party – Hell's Angels**	Unknown	0	0	0	0	0	0
08-Oct-18	**Oakland Marriott City Center**	50	1	0	0	0	0	0
09-Oct-18	**Oakland Marriott City Center**	50	4	0	0	0	0	0
10-Oct-18	**Oakland Marriott City Center**	50	8	0	0	0	0	0
11-Oct-18	**Oakland Marriott City Center**	50	6	0	0	0	0	0
12-Oct-18	**Oakland Marriott City Center**	50	6	0	0	0	0	0
13-Oct-18	**Oakland Marriott City Center**	50	5	0	0	0	0	0
14-Oct-18	**Oakland Marriott City Center**	50	6	0	0	0	0	0
15-Oct-18	**Oakland Marriott City Center**	50	9	0	0	0	0	0
16-Oct-18	**Oakland Marriott City Center**	50	6	0	0	0	0	0
17-Oct-18	**Oakland Marriott City Center**	50	6	0	0	0	0	0
18-Oct-18	**Oakland Marriott City Center**	50	6	0	0	0	0	0
20-Oct-18	**Oakland Marriott Protest**	100	6	0	0	0	0	0
23-Oct-18	**Pack the Courtroom for Whole Foods Suit**	30	2	0	0	0	0	0
08-Nov-18	**Nobody Is Above the Law – Mueller Protection Rapid Response**	200	6	0	0	0	0	0
03-Dec-18	**Stop the Tows, We Won't Go! Protest at Oakland City Hall Against Mass Towing of RVs**	12	3	0	0	0	0	0

04-Dec-18	**End Criminal Justice Fines and Fees in Alameda County**	10	2	0	0	0	0	0
05-Dec-18	**Edes Ave Encampment Operation**	75	29	0	0	0	0	0
06-Dec-18	**Edes Ave Encampment Operation**	30	33	0	0	0	0	0
10-Dec-18	**Oakland High School Teacher Walkout**	100	5	0	0	0	0	0
11-Dec-18	**School Protest**	100	2	0	0	0	0	0
OTHER EVENTS TOTALS		**Attended**	**OPD**	**Complaints**	**Arrests**	**Citations**	**Ejections**	**Uses of Force**
		1,382	**163**	**0**	**0**	**0**	**0**	**0**

TOTAL PERFORMANCE DATA: 2018 4th Quarter	**Attended**	**OPD**	**Complaints**	**Arrests**	**Citations**	**Ejections**	**Uses of Force**
	828,860	**2,162**	**0**	**29**	**144**	**101**	**3**

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 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 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 UAV its surroundings from a birds-eye perspective.

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

2. Proposed Purpose

UAS offer to significantly improve the capacity of law enforcement (LE) to provide a variety of foundational police services. This technology has already been used with many law enforcement agencies to save lives and help capture dangerous criminal suspects. UAS can support first responders in

hazardous incidents that would benefit from an aerial perspective. 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 – the sky view provided by UAS is incredibly useful in providing more information about conditions officers must face. Some UAS also have lamps that can be used to illuminate areas where armed and dangerous suspects may be present. 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.

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

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

a. Mass casualty incidents;
b. Disaster management;
c. Missing or lost persons;
d. Hazardous material releases;
e. Rescue operations;
f. Special events;
g. Training;
h. Hazardous situations which present a high risk to officer and/or public safety, to include:
i. Barricaded suspects;
j. Hostage situations;
k. Armed suicidal persons;
l. Arrest of armed and/or dangerous persons;

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

n. Operational planning;

o. Service of search and arrest warrants; and

p. At the direction of a command officer.

Potentially, UAS could be deployed in any location in the City of Oakland where one or more of the above situations occur and where the proper authorizations are provided. Fortunately, several of these situations rarely occur – but some do occur regularly. 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. In 2018, OPD made 8,239 custodial arrests for 16,853 charges – 6,940 arrests, or 84 percent, of these 8,239 arrests included either a felony charge, a misdemeanor charge that required an arrest (warrant, domestic violence, firearms violation), or both. Only some of these arrests relate to "armed and/or dangerous persons" as one of the allowed uses for UAS; However, 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 2 that OPD will consider purchasing, contain both a speaker and microphone; such UAS can be used for two-way communications during several of the use-cases described in this section above (e.g. hostage situations).

4. Privacy Impact

OPD recognizes that the use of UAS in public right of way raises privacy concerns. UAS are becoming ubiquitous in the United States, and there is a growing concern that people can be surveilled upon without notice or reason from this new sky-bound technology. There is concern that the use of this technology 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. 14 CFR 107 includes the following stipulations[1] for law enforcement agencies:

- Each aircraft over 55 pounds must be individually registered;
- The agency must fly only in uncontrolled airspace;
- The aircraft must be kept in sight (visual line-of-sight);
- The UAS must be flown under 400 feet;
- The UAS must be flown only during daylight;
- The UAS must fly at or below 100 mph;
- The UAS must yield right of way to manned aircraft;
- The UAS must not fly over people (OPD will position UAS over buildings to avoid flying over people); and
- The UAS must not be operated from a moving vehicle.

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

- Stadiums and Sporting Events
- Near Airports
- Security Sensitive Airspace Restrictions
- Restricted or Special Use Airspace
- Washington, DC
- Emergency and Rescue Operations (wildfires and hurricanes).

The results of the research study titled, "Mission-based citizen views on UAV usage and privacy: an affective perspective[2]," published in February 2016 found that people's perceptions of how UAS impacts privacy relate to use type. The researchers from College of Aeronautics, Florida Institute of Technology and the Aeronautical Science at Embry-Riddle Aeronautical University (ERAU), College of Aviation UAS Lab found that people tend to be less concerned about police UAS use when the technology is only used for specific uses - "concerns for privacy were less in the condition where the UAV was only used for a specific mission than when it was operated continuously." DGO I-25.III.A "General Guidelines, Authorized Use" explains that OPD personnel can only use UAS for specific missions, detailed above in Section 3 "Locations Where, and Situations in which UAS may be deployed or utilized."

[1] https://www.faa.gov/about/office_org/headquarters_offices/avs/offices/afx/afs/afs800/afs820/part107_oper/

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

5. Mitigations

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

- OPD UAS shall not be equipped with any weapon systems;
- 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 solely on their individual characteristics, such as but not limited to race, ethnicity, national origin, religion, disability, gender, and/or sexual orientation;
    - For the sole purpose of harassing, intimidating, or discriminating against any individual or group;
    - To conduct personal business of any type; and

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 or exigent circumstances.
- 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).
- 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.

The technology itself also provides privacy mitigations. The types of UAS OPD will consider using provide integrated protections. 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, has produced a "Commitment to Data Security" document (see Attachment B). The document explains protocols undertaken to ensure that flight data is not transmitted back to DJI or other sources (e.g. storing data on a U.S.-based AWS server). DJI's "Implementing Mitigation Measures Recommended By The DHS" (see Attachment C) recommends mitigations that mirror OPD UAS mitigations:

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

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

6. Data Types and Sources

UAS record using standard digital cameras file types (e.g. jpeg, mov, mp4, wav or RAW).

7. Data Security

OPD takes data security seriously and safeguards UAS data by both procedural and technological means. The video recording function of the UAS shall be activated whenever the UAS is deployed. Video data will be recorded onto Secure Digital (SD) Cards. OPD DGO I.25.4.B "Data Retention" states video recording collected by OPDUAS 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; the program coordinator shall develop procedures to ensure that data are retained and purged in accordance with applicable record retention schedules.

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 or as otherwise permitted by law, using the following procedures:

- The agency makes a written request for the data that includes:
    - The name of the requesting agency.
    - The name of the individual making the request.
    - The basis of their need for and right to the information.
- 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.
- The approved request is retained on file, and incorporated into the annual report pursuant to Oakland Municipal Code Section 9.64.010 1.B.

8. Costs

Costs for a UAS program can vary from thousands to hundreds of thousands and beyond. Different types of systems exist that would support police services, and technology continues to evolve. However, OPD personnel have procured some initial bids to start an OPD UAS program. 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	**R**ugged 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, other accessories.	$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 for lighter use as well as for indoor use	Drone body with protection kit, controller, batteries, battery chargers, propellers, cables, other related accessories; $2,949 x 4	$11,796
	Additional batteries; $169x24	$4,056
	DJI Smart Controller; $549x4	$2,196
Total		**$46,800**

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

9. Third Party Dependence

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

in progress with a suspected armed suspect.

OPD values its relationship with ACSO and the UAS support provided in 2019; However, OPD now hopes to join the growing list of municipal police agencies developing their own UAS programs. The “Proposed Purpose” Section 2 above explains the benefit and local need for such situational awareness. There are several vendors currently manufacturing law enforcement enterprise quality systems. Section 8 “Cost” above details a possible purchase from DJI – a leading manufacturer. However, OPD will solicit competitive bids and reevaluate vendors if and this Surveillance Impact Report and connected DGO I.25 Use Policy are approved by the City Council; the City Council will also have to approve UAS purchases over $50,000.

10. Alternatives Considered

There is no perfect alternative to the combination of sky-view situational awareness as well as cost effectiveness provided by UAS. Helicopters also offer sky-view situational awareness. Helicopters however 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.

Both helicopters and UAS can be used to provide a sky-view during all of the situations described in the Purpose and Impact sections above; both technologies can be used for search and rescue operations and to search for missing persons. 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 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 provide maps and 3D images within minutes; this data is also valuable during court testimony.
- Finding and/or seizing illegal drones - police UAS can be flown to identify unregistered UAD that may be hazardous to the surrounding environment (some operators do not have the proper training and licensing necessary to fly, especially in environments with large crowds).
- Assist Department of Transportation (DOT) – DOT can utilize UAS for

a variety of transportation mapping situations.

As Bryan Smith, APSA[3] Safety Program Manager explains in "Working Together: Deploying Manned and Unmanned Aircraft Safely and Successfully" in Air Beat[4]-July-August 2019 Issue, "What if we (LE) had the ability coordinate tasking, splitting the airborne support responsibilities between manned 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.

11. Track Record of Other Entities

Many cities and counties in California and nationwide have begun to implement UAS programs due to the numerous uses cases for law enforcement. The Alameda County Sheriff's Office (ACSO) as well as Sacramento County Sheriff's Office have developed programs with several types of drones and full time deputy positions; Stanislaus County is beginning to develop their program currently. 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 many much more human staff time as well as expensive 3D camera technology.

[3] APSA = Airborne Public Safety Association

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

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 an unmanned aerial system (UAS) and for the storage, retrieval, and dissemination of images and data captured by the 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 handy 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. 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;

g. Training;

h. Hazardous situations which present a high risk to officer and/or public safety, to include:

i. Barricaded suspects;

ii. Hostage situations;

iii. Armed suicidal persons;

iv. Arrest of armed and/or dangerous persons;

v. Scene documentation for evidentiary or investigation value;

vi. Operational planning; and

vii. Service of search and arrest warrants.

4. **Deployment Authorization**

a. Deployment of OPD UAS

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

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

5. Deployment Logs

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

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

6. Privacy Considerations

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

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

B. Restricted Use

1. UAS shall not be equipped with any weapon systems.

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. Conducting random surveillance;

   b. Targeting a person based solely on their individual characteristics, such as but not limited to race, ethnicity, national origin, religion, disability, gender, and/or sexual orientation.

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

   d. To conduct personal business of any type.

C. Communications

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

IV. UAS DATA

A. Data Collection

The video recording function of the UAS shall be activated whenever the UAS is deployed.

B. Data Retention

Video recording collected by OPDUAS shall be deleted 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 of data is necessary for another organizational or public need.
    a. The program coordinator shall develop procedures to ensure that data are retained and purged in accordance with applicable record retention schedules.

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.

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 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.
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.

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.

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 use of the 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 and include this in the UAS procedure manual.

G. Reporting

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

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

H. Training

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

By Order of

Anne E. Kirkpatrick

Chief of Police Date Signed:

IMPLEMENTING MITIGATION MEASURES RECOMMENDED BY THE DHS

DJI values the trust our customers place in us to improve their businesses with drone technology, to make their operations safer and more efficient, and to help empower them to safeguard the data generated using our products. Safety and security are at the core of everything we do, because greater confidence in our technology will help unlock the full promise of drones. As technology has advanced, we have worked collaboratively with industry and government agencies to ensure the safe and secure use of our technology.

We would like to address the recent concerns driven by the **U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency Industry Alert** that was issued this week. In this Alert, four specific mitigating measures are referenced. Below are some guidelines on how to implement these mitigating measures when using DJI drones.

1. DHS Recommendation: Deactivate Internet Connection from Device Used to Operate the UAS

- Background: DJI aircraft are not directly connected to the internet, but instead use your mobile device, or a hotspot enabled controller with a built-in screen, to connect to the internet for updating apps, firmware and handle other basic functions.

- Solution: DJI's Pilot app for commercial operators offers 'Local Data Mode', a software feature that disables all external activity by the flight control app. The app supports DJI's enterprise aircraft including Matrice 200 Series, Mavic 2 Enterprise series and others. If you are using consumer aircraft compatible with DJI Go 4 only, you can easily disconnect your DJI UAS from the internet by enabling airplane mode on the mobile device.

2. DHS Recommendation: Take Precautionary Steps Prior to Installing Updated Software or Firmware

- Background: DJI releases a variety of different software, from flight control and fleet management to photogrammetry, across mobile, PC and cloud platforms. As with all software, there are regular updates that improve core functionality and stability. All updates go through DJI's software QA process to ensure they are secure prior to publication.

- Solution: For users concerned about updates to their existing flight control software on their mobile device, users can choose to disconnect their flight control applications from connecting to the internet as referenced above. This will prevent any software updates to the aircraft and flight control software.

- Solution: DJI's FlightHub Enterprise and FlightHub Government fleet management software provide your organizations IT team full control over release of all software and firmware updates to your UAS fleet, meaning that no software or firmware updates are pushed out unless mandated by your IT administrator. For users concerned about updates to their existing fleet management and other cloud or desktop-based software, please contact your organization's IT team to review the software before implementing it.

- Note: DJI's cloud and PC-based software are not critical for operating DJI drones and there are 3rd party options available from DJI's US-based partners.

3. DHS Recommendation: Remove Secure Digital Card from the Main Flight Controller/aircraft

- Background: SD cards are removable storage used to store images and videos the UAS captures. In most cases they are removable; the data is always accessible only to the user. DJI aircraft are not directly connected to the internet, and no DJI drone or controller is built with a cellular modem installed. Users may choose to connect a 4G dongle to the controller or connect to internet on their mobile phone to enable workflow-specific capabilities.

- Solution: SD cards would fall under each organization's data management policy, which would typically be administered and monitored by the IT Team. DJI encourages all organizations to manage their data in accordance with the policies they set, including the removal and storage of SD cards.

4. DHS Recommendation: If SD Card is Required to Fly the Aircraft, Remove All Data from the Card After Every Flight

- Background: To store footage users choose to capture during flight, each DJI aircraft can hold a single removable SD card and the newer Mavic 2 series also has in-built memory for storing image data.

- Solution for removable SD cards: Remove your SD card after each flight, retrieve data required, and clear contents of SD card prior to next flight.

- Solution for in-built storage: Download all footage captured then delete data stored on internal storage after each flight.

We will continue to directly address concerns about our products, and have invested significant resources in bolstering our security infrastructure so enterprise and government customers can securely integrate DJI hardware and software into their workflows.

DJI is committed to our partners and providing the best, safest, and most secure aerial platform for their work. We will continue to be available to discuss these issues further.

DJI's COMMITMENT TO DATA SECURITY

DJI values the trust our customers place in us to improve their businesses with drone technology, to make their operations safer and more efficient, and to help empower them to safeguard the data generated using our products. Safety and security are at the core of everything we do, because greater confidence in our technology will help unlock the full promise of drones. As technology has advanced, we have worked collaboratively with industry and government agencies to ensure the safe and secure use of our technology.

We would like to address the recent concerns driven by the **U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency Industry Alert** that was issued this week. Our official public statement is below followed by a recap of the features and tools that DJI has designed into our products to give our customers complete control over how their data is collected, stored, and transmitted.

Official DJI Statement:

"At DJI, safety is at the core of everything we do, and the security of our technology has been independently verified by the U.S. government and leading U.S. businesses. DJI is leading the industry on this topic and our technology platform has enabled businesses and government agencies to establish best practices for managing their drone data. We give all customers full and complete control over how their data is collected, stored, and transmitted. For government and critical infrastructure customers that require additional assurances, we provide drones that do not transfer data to DJI or via the internet, and our customers can enable all the precautions DHS recommends. Every day, American businesses, first responders, and U.S. government agencies trust DJI drones to help save lives, promote worker safety, and support vital operations, and we take that responsibility very seriously. We are committed to continuously working with our customers and industry and government stakeholders to ensure our technology adheres to all of their requirements."

DJI has led the drone industry in giving our customers access to best in class features and tools to give them complete control over their data. DJI has gone to great lengths to work with government and commercial customers, especially on critical infrastructure, to deliver on this promise, as outlined by the initiatives we have implemented:

- **FlightHub Software** – DJI introduced drone fleet management solutions to meet the stringent data custody and security needs for our enterprise and government customers who have additional security requirements. FlightHub Basic and Advanced are hosted on a secure, US-based AWS server, while the new FlightHub Enterprise includes options such as private cloud or on-premise hosting and non-internet connected systems to safeguard no data is shared back to DJI or with third party apps.

- **Government Edition** – DJI has collaborated with key partners across the United States to offer a new Government Edition solution that directly addresses the security requirements of United States Government entities. The solution is being vetted by a U.S. Federal entity, with over 3,000 flights using Government Edition.

- **Independent Security Audit** – DJI commissioned an independent cybersecurity firm, Kivu Consulting, to review and evaluate our customer data protection protocols. Kivu validated that no malware exists within our products; that our customers have control over how their data is collected, stored and transmitted; and that DJI does not have access to customer data unless customers choose to share it.

- **Secure Data Storage** – DJI follows industry best-practices by storing any data shared with us by international users on secure cloud servers located in the United States. DJI is committed to helping our customers protect their data. Wherever possible, we design our products to give customers control over their data, including if, when, and how that information is collected, transmitted, or shared.

- **Local Data Mode** – Built into the DJI Pilot flight control app, this feature allows users to stop any connectivity to the internet.

- **Bug Bounty Program** – DJI offers Bug Bounty rewards to encourage security researchers to discover and responsibly report potential vulnerabilities in our systems, helping to ensure that data stored by DJI stays secure.

We will continue to directly address concerns about our products, and have invested significant resources in bolstering our security infrastructure so enterprise and government customers can securely integrate DJI hardware and software into their workflows.

DJI is committed to our partners and providing the best, safest, and most secure aerial platform for their work. We will continue to be available to discuss these issues further.

DRONES IN PUBLIC SAFETY: A GUIDE TO STARTING OPERATIONS

Law enforcement and public safety agencies are realizing the potential of using drones to enhance their missions. Some agencies choose to hire drone pilots certified by the Federal Aviation Administration to conduct operations for them. But if your agency wants to conduct its own drone operations or create a program with multiple pilots and drones, this primer will help get you started.

Your agency has two options to operate drones:

- **Designate** individual members of your team to earn FAA drone pilot certificates and fly under the rules for small unmanned aircraft systems (sUAS).
- **Receive** an FAA certificate of authorization (COA) to function as a "public aircraft operator" that can self-certify its drone pilots and drones.

The sUAS Rule

Most drone pilots operate under the sUAS rule, which is commonly known as Part 107 after the designated section of the federal code. Part 107 defines requirements for drone pilots and drones, and it sets operational limits for drone usage.

Pilot certification and responsibilities

- Members of your team may choose to take the FAA Airman Knowledge Test to become drone pilots. Those who pass the test receive remote pilot airman certificates, giving them the right to operate qualified sUAS.

Operational limitations

- Drones flown by remote pilots must weigh less than 55 lbs. This limitation includes any attached equipment or cargo, such as emergency aid in search-and-rescue operations.
- Remote pilots cannot fly their drones more than 400 feet above ground level (or more than 400 feet above the top of structures like communications towers).
- Remote pilots must receive FAA authorization to fly in airspace near airports. They may use an automated system called Low Altitude Authorization and Notification Capability (LAANC).
- Other limitations include not flying over people or at night. Your agency may apply for waivers to certain rules. To request a waiver, visit faa.gov/uas/request_waiver.

Aircraft requirements

- No FAA airworthiness certificate is required to fly sUAS under Part 107, but your team must register each aircraft with the FAA. The remote pilot must confirm that an aircraft is in condition for safe operation before each flight.

– February 2019 –

Federal Aviation Administration

DRONES IN PUBLIC SAFETY: A GUIDE TO STARTING OPERATIONS

Public Aircraft Operator

Rather than certify pilots and register aircraft under Part 107, your agency may choose instead to request a COA from the FAA to become a public aircraft operator. This would allow your agency to self-certify your drone pilots and drones for flights to perform governmental functions.

The first step is to ask your legal department to draft a Public Declaration Letter that certifies your agency as a governmental entity and send it to the FAA. The FAA will send you a user ID and password to the UAS COA Online Application System, where you can complete your application. This process can take up to 60 days.

For more information about the COA process, please visit **www.faa.gov/go/COA**

Emergency Authorizations and Operations

To support emergency responders and other entities affiliated with them, the FAA can quickly issue authorizations for responses to natural disasters and other emergencies. For more information, please visit: **www.faa.gov/go/EmergencyWaiver**

Learn more at faa.gov/uas

Download the B4UFLY app

FAA B4UFLY

CITY OF OAKLAND

AGENDA REPORT

TO:	Sabrina B. Landreth CITY ADMINISTRATOR	**FROM:**	Anne E. Kirkpatrick Chief of Police
SUBJECT:	Use of Unapproved Surveillance Technology Under Exigent Circumstances – January 28, 2019	**DATE:**	February 25, 2019

City Administrator Approval | Date

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 Surveillance (UAS or drone). OMC 9.64.035 requires that

BACKGROUND AND LEGISLATIVE HISTORY

Oakland' Surveillance Technology Ordinance requires that city departments bring employed surveillance technologies to the Privacy Advisory Commission (PAC); the PAC can then choose whether to forward their recommendation to the City Council. The Ordinance creates OMC 9.64.035 "Use of unapproved technology during exigent circumstances or large-scale event." The OMC allows OPD to use unapproved technologies during these two types of events. The OMC requires that staff shall:

a. Use the surveillance technology to solely respond to the exigent circumstances or large-scale event.
b. Cease using the surveillance technology when the exigent circumstances or large scale event ends.
c. Only keep and maintain data related to the exigent circumstances and dispose of any data that is not relevant to an ongoing investigation.
d. Following the end of the exigent circumstances or large-scale event, report that acquisition or use to the PAC at their next respective meetings for discussion and/or possible recommendation to the City Council in accordance with the Sunshine Ordinance, the Brown Act, and City Administrator deadlines.

ANALYSIS AND POLICY ALTERNATIVES

On January 18, 2019, at 11:06 am, OPD Officers observed a vehicle containing a murder suspect, who had an active warrant for his arrest in connection to a triple murder which had occurred in West Oakland. The suspect was seated in the right front passenger seat and the driver was unknown to officers. OPD officers attempted to conduct a vehicle enforcement stop to arrest the suspect. The driver fled and OPD officers engaged in a vehicle pursuit. The suspect vehicle crashed when exiting from the freeway. Both suspects fled the scene, in opposing directions. The triple murder suspect ran onto the Mills College campus[1]. The school was placed on lockdown and the suspect was apprehended hiding inside a building. The second suspect ran into an area with bushes and trees near the school, and hid from officers. OPD personnel as well as UAS and CHP[2] helicopters were used to gain an aerial view of the area. The area is heavily populated with trees, bushes and brush. The UAS allowed OPD officers to remain at a safe distance from where the second suspect was believed to be hiding while still obtaining real time information. This situation was deemed an immediate and serious threat to the public (schools and residences) as well as to officer safety. The UAS assisted officers in locating the suspect as well as the clothing the suspect discarded.

Device Use Information

The UAS detection equipment was provided by and operated by the Alameda County Sheriff's Office (ACSO). The UAS was used to assist uniformed officers during a search of a heavily wooded area.

Deployment Timeline

The below times are for January 18, 2019.

January 18, 2019

- 11:11 am: OPD Officers observe a triple murder suspect in the passenger seat of a vehicle;
- 11:12 am: OPD Officers attempt to conduct vehicle enforcement stop and the driver of the vehicle sped off;
- 11:13 am: OPD helicopter advises not available until noon;
- 11:15 am: Suspect vehicle exits freeway and crashes. Suspects exit and runs in opposing directions;
- 11:16 am: Initial perimeter set to contain suspect(s);
- 11:19 am: CHP helicopter advises in-route;
- 11:12 am: Mills College is advised that one suspect jumped over fence and ran into school property. Mills College is locked down and students/teachers advised to shelter in place;
- 11:30 am: Triple murder suspect apprehended inside of Mills College;
- 11:34 am: OPD officers obtain information that the driver of the suspect vehicle is hiding in the wooded area;

[1] Mills College 5000 MacArthur Blvd., Oakland)
[2] CHP = California Highway Patrol

- 11:37 am: OPD officers observe suspect hiding in wooded area and lose sight;
- 11:37 am: ALCO Sheriff's Department is requested to respond to scene with UAS;
- 11:37 am: CHP helicopter arrives on scene and observes "no movements;"
- 12:01 pm: Unity High School[3] is locked down and students and teachers advised to shelter in place;
- 12:17 pm: CHP helicopter advised searched entire area with negative results
- 12:28 pm: CHP helicopter advised still unable to locate the second suspect and CHP helicopter leaves
- 1:24 pm: ALCO UAS goes up and locates subject in area
- 2:26 pm: OPD helicopter arrived on scene
- 2:37 pm: OPD helicopter leaves scene;
- 2:40 pm: Subject located in heavily wooded area
- 2:50 pm: ALCO UAS used search for any firearms

The UASs were used during the wooded area search for approximately one and a half hour. The UASs were used concurrently with a helicopter[4] because of the heavily wooded area and the UAS's were only allowed to fly at a limited height. The UASs flew lower and into the trees and brush area, which were considered danger spots for officers. The helicopters flew overhead and much higher to gain the overview of the area. The use of the UASs proved successful for real time information to officers, which ultimately assisted in locating the suspect. The UAS's were then utilized to search for any discarded firearms. A later search of the vehicle resulted in the recovery of a rifle and a pistol.

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

ALCO successfully utilized the UAS to discover where the suspect was hiding; ALCO directed OPD Officers to where the suspect was hiding because of the UAS-obtained locational information. The UAS as well as the helicopter was useful in providing increased officer safety during the search.

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.

[3] Unity High School (Independent Charter High School, 6038 Brann St, Oakland)
[4] One helicopter was used at a time.

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. The Alameda County Sheriff's Office maintained possession of the equipment during the entire equipment usage period.

PUBLIC OUTREACH / INTEREST

This report was presented to the City's Privacy Advisory Commission on February 7, 2019.

COORDINATION

The Office of the City Attorney reviewed this report.

SUSTAINABLE OPPORTUNITIES

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

Environmental: There are no environmental issues associated with this report.

Social Equity: This report provides transparency around OPD's use of surveillance technology in conjunction with police services.

ACTION REQUESTED OF THE PUBLIC SAFETY COMMITTEE

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.

For questions regarding this report, please contact Bruce Stoffmacher, Management Assistant, at (510) 238-6976.

Respectfully submitted,

Anne E. Kirkpatrick
Chief of Police
Oakland Police Department

Reviewed by:
Timothy Birch, Police Services Manager
OPD, Research and Planning, Training Division

Prepared by:
Bruce Stoffmacher, Management Assistant
OPD, Research and Planning, Training Division

recommendations to move us incrementally towards this goal for an accessible, comprehensive privacy website:

1. Organize a spreadsheet of active surveillance technologies in use by the City of Oakland, linking to its impact report and use policy (when applicable)
2. Translate the "Privacy Principles" in languages representative of Oakland's diverse landscape in line with the "Equal Access to Services," SEC.2.30.050 of the Oakland Municipal Code. Oakland census data reveals the most common spoken languages other than English are (in the following order) Spanish, Mandarin, Cantonese, and Vietnamese.[1]
3. Write the "About" section: Archive the developing history of Oakland's privacy leadership, preserve institutional memory around the "Domain Awareness Center," and provide a history to the creation of the Privacy Advisory Commission and its guiding Surveillance Technology Ordinance.
4. Take inventory of the PII collected by various departments to make data collection explicit and transparent on the City's website. (This could be done in collaboration with the City's IT department, which is streamlining data collection onto OakApps and has created a corresponding Online Privacy Security Policy--approved by PAC July 8, 2019--that could be listed also on our site)

B. Privacy training for relevant City staff:

1. Introduction to the Privacy Principles, Ordinance, and City's privacy record
2. Data security hygiene: In collaboration with the City's IT Department that includes best practices on all issues related to data protection (from spotting phishing attempts and using proper encryption software to preparing for a data breach or DOS attack)
3. How to respond to CPRA requests while protecting privacy

C. Create "onboarding" packet for new Commissioners:

1. Provide history information to the City's privacy initiatives from the DAC and FLIR to creation of PAC
2. Include "Surveillance Technology Assessment Questionnaire", developed by former Commissioner Karamooz
3. Offer any of aforementioned trainings given to City staff

V. <u>Implementation, Phase III:</u>

A. Create online portal for residents to submit complaints, concerns, and questions to the PAC, CPO, or other relevant City staff.

B. Polling/surveying Oaklanders on privacy concerns

[1] https://datausa.io/profile/geo/oakland-ca/#demographics

C. **Public workshops for Oaklanders on privacy issues based on survey results**
D. **Work with the Department of Race & Equity and IT Department to develop internal privacy audit [**Principle I: Design and use equitable privacy practices; Principle III: Manage personal information with diligence]

VI. **Budgetary opportunities:** The budgetary cycle for this year has passed. However, the Commission can request funding in the interim from the City Administrator's discretionary funds. Even modest, short-term funding can lay the groundwork for initial phases of implementation. In preparation for the next budgetary cycle in 2021, below are specific line item suggestions to request funding for, reflective of the various projects and initiatives outlined in Phases I- III:

A. Web services to build out the functions listed in Phase II, A and Phase IIII, C.
B. Project manager to oversee website development project
C. Additional staffing to support the CPO in implementation plan
D. Translation services, especially for the "Principles" into multiple languages
E. Community outreach and polling, as outlined in Phase III, B and C
F. Privacy consultants to develop and execute departmental trainings, Phase II B
G. Independent audit to determine data security vulnerability that can be adapted and executed regularly and internally

VII. **Proposed Timeline**:

A. Phase I (now- April 2019) The items in this phase are less predicated on budgetary funding, albeit a significant portion of City staff time.
    1. Work with the City Administrator and Council in the immediate to see what funds we can gather in lieu of the passed budget cycle deadline
B. Phase II: (April 2019- Dec 2022)
    1. February 2021-- PAC to send budgetary line items in proposal to The Budget Office, City Administrator, and City Council
    2. If the budget is approved and funds are allocated, July 2021 proceed to hiring Project Manager to work under the direction of the CPO and begin:
        a) RFP process for a third-party contractor to build out website
        b) Commissioning translation materials for "Principles" and other relevant materials
        c) Collecting history, information and copy for website
C. Phase III: (July 2021- Dec 2022) Items in this phase will likely require budgetary funding, so the timeline has been pushed to begin for late summer when funds have been appropriated.

CITY OF OAKLAND

AGENDA REPORT

TO: Sabrina B. Landreth
City Administrator

FROM: Anne Kirkpatrick
Chief of Police

SUBJECT: OPD 2019 DNA Backlog Reduction Program

DATE: November 6, 2019

City Administrator Approval Date: 1/24/2020

RECOMMENDATION

Staff Recommends That The City Council Adopt A Resolution: 1) Authorizing The City Administrator Or Designee To Accept And Appropriate Grant Funds In An Amount Not To Exceed Three Hundred Twenty-Five Thousand, Seven Hundred Fifty Dollars ($325,750) From The U.S. Department Of Justice, National Institute Of Justice (USDOJ/NIC) For Implementation Of The Fiscal Year 2019 DNA (Deoxyribonucleic Acid) Backlog Reduction Grant Program For The Oakland Police Department; 2) Waive The Advertising And Competitive Bidding Requirements For The Purchase Of DNA Typing Supplies From (A) Promega For One Hundred And Six Thousand Dollars ($106,000), (B) Qiagen For Thirty-Four Thousand Three Hundred Dollars ($34,300), (C) Thermo Fisher/Life Technologies For One Hundred Twenty-Eight Thousand Eight Hundred Dollars ($128,800), And (D) Thermo Fisher/Life Technologies, Aurora Biomed, Qiagen, And/Or Remi For Thirty-Two Thousand Six Hundred Seventy-Four Dollars ($32,674) For DNA Typing Supplies, Instruments, And Service Maintenance.

EXECUTIVE SUMMARY

Adoption of this resolution will allow OPD to accept the USDOJ/NIJ Fiscal Year (FY) 2019 DNA Capacity Enhancement and Backlog Reduction grant of $325,750, which will fund the continuation of staff training and technology costs. The OPD Crime Laboratory (Crime Lab), with these grant funds, will be able to decrease the biological evidence analysis turnaround time and the backlog of cases. This resolution calls for waiving the City's Advertising and Competitive Bidding Requirements because of the need to buy specialized laboratory validated DNA typing equipment and supplies available only from specific vendors.

BACKGROUND AND LEGISLATIVE HISTORY

The DNA Capacity Enhancement for Backlog Reduction Program was created by the U.S. Department of Justice, National Institute of Justice (USDOJ/NIJ) to assist laboratories that conduct DNA analysis. The goal of the program is to improve DNA laboratory infrastructure and

analysis capacity so that DNA samples can be processed efficiently and effectively. The program also provides continuing education courses and training associated with DNA analyses, as well as funds to analyze backlogged forensic DNA casework samples. Improvements are necessary and critical to reduce current and prevent future DNA backlogs and to help the criminal justice system reach its full potential in the utilization of DNA technology.

Backlogged case requests from homicides, sexual assaults, robberies, assaults, and property crime cases will be enrolled into the FY 2019 DNA Backlog Reduction Program. The eligible DNA profiles obtained from evidence in these cases will be entered into the Combined DNA Index System (CODIS). DNA profiles entered into CODIS has resulted in an approximately forty-five percent hit rate.[1] This will assist not only Oakland Police Department investigators, but also the Alameda County District Attorney, and other law enforcement, prosecutorial, and judicial agencies in the surrounding area.

OPD has previously received several 2019 DNA Backlog Reduction Program grants. The Oakland City Council has previously authorized acceptance of the following grant-authorizing resolutions:

- Resolution No. 87429 C.M.S., dated November 27, 2018;
- Resolution No. 87428 C.M.S., dated November 27, 2018;
- Resolution No. 86982 C.M.S., dated November 28, 2017;
- Resolution No. 86532 C.M.S., dated December 13, 2016;
- Resolution No. 85899 C.M.S., dated November 17, 2015;
- Resolution No. 85223 C.M.S., dated November 21, 2014;
- Resolution No. 84686 C.M.S., dated November 5, 2013;
- Resolution No. 84041 C.M.S., dated October 2, 2012;
- Resolution No. 83672 C.M.S., dated December 20, 2011;
- Resolution No. 83030 C.M.S., dated October 19, 2010;
- Resolution No. 82291 C.M.S., dated September 22, 2009;
- Resolution No. 81624 C.M.S., dated October 21, 2008;
- Resolution No.80869 C.M.S., dated October 2, 2007;
- Resolution No. 80129 C.M.S., dated September 19, 2006;
- Resolution Nos. 79534 and 79535 C.M.S., both dated October 18, 2005; and
- Resolution Nos. 78909 and 78910 C.M.S., both dated November 16, 2004.

[1] "Hit rate" is defined as that portion of cases with DNA profiles submitted to CODIS in which at least one association (named individual) is made to a DNA profile(s) in the database. Multiple suspects may be identified in some portion of the cases examined.

ANALYSIS AND POLICY ALTERNATIVES

The Crime Lab will focus on three goals with the implementation of the FY 2019 DNA Backlog Reduction Program grant initiative:

Goal #1: Reduce the Forensic DNA Case Backlog

Between July 2018 to June 2019, the Forensic Biology Unit has completed the analyses on 426 requests in an average of 97 business days[2]. The goal of the proposed grant is to decrease the Forensic Biology Unit's backlog by in-part reducing turnaround time. Turnaround time will be reduced through specialized training and the purchase of instruments and supplies for Forensic Biology Unit Criminalists to analyze 155 backlogged cases. Case evaluation, biological evidence examination and screening, DNA typing, technical review, and data entry into CODIS will be conducted during normal business hours. Forensic DNA typing kits and reagents will be purchased to analyze these 155 backlog cases.

Goal #2: Increase Capacity of the Crime Lab for Forensic Casework

The Crime Laboratory will use the grant to purchase two real-time polymerase chain reaction (PCR) DNA typing instruments. These instruments will replace two antiquated real-time PCR DNA typing instruments and increase the capacity of conducting DNA typing on case samples.

Goal #3: Provide Required Continuing Education for Each Criminalist and Forensic DNA Technician

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

- ANSI-ASQ National Accreditation Board accreditation (ANAB)[3]
- Certification of individual scientists
- National DNA Index System (NDIS) requirements for CODIS data entry
- American Board of Criminalistics educational requirements
- Federal Bureau of Investigation (FBI) DNA Quality Assurance Standards (QAS) mandatory education and training requirements

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

[2] The Crime Lab counts business days as from the date of receipt of request to report authorization.
[3] ANSI = American National Standards Institute; ASQ = American Society for Quality

Waiver of the Advertising and Bidding Process

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

FISCAL IMPACT

The table below details how OPD will utilize the USDOJ/NIJ FY 2019 DNA Backlog Reduction Grant Program funds. The table lists the use of funding for staff travel and training, and technology and supply costs.

Budget Category	**Amount**
Instrument	
DNA Typing Instruments (Thermo Fisher/Life Technologies)	$114,000
Total Instruments	**$114,000**
Training and Travel	
Travel and Lodging Costs	$18,876
(16) Forensic Biology Unit Training Registrations	$5,100
Total Training and Travel	**$23,976**
Technology and Supplies	
DNA Typing Supplies (Thermo Fisher/Life Technologies)	$14,800
DNA Typing Supplies (Promega)	$106,000
DNA Typing Supplies (Qiagen)	$34,300
Total Technology and Supplies	**$155,100**
Service Instrument Maintenance	
Annual Maintenance (Aurora Biomed)	$32,674
Annual Maintenance (Qiagen)	
Annual Maintenance (Thermo Fisher/Life Technologies)	
Annual Maintenance (REMI)	
Total Service Instrument Maintenance	**$32,674**
TOTAL	**$325,750**

The $325,750 in grant funds from the USDOJ/NIJ for the implementation of the FY 2019 DNA Backlog Reduction Grant Program shall be appropriated in the Federal Grant Fund (2112), Criminalistics Division Organization (102610), Criminalistics Division Program (PS05), in a Project Number to be established.

Fiscal Year	Fund Source	Organization	Project	Program	Amount
2019-2020	2112	102610	TBD	PS05	$325,750

PUBLIC OUTREACH / INTEREST

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

COORDINATION

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

SUSTAINABLE OPPORTUNITIES

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

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

Social Equity: Provisions for continuing education and supplies funded by this grant will enhance OPD's ability to analyze biological evidence in criminal cases in a timelier fashion. The public safety for all Oakland residents and visitors is enhanced through greater OPD investigative capacity.

ACTION REQUESTED OF THE CITY COUNCIL

Staff Recommends That The City Council Adopt A Resolution: 1) Authorizing The City Administrator Or Designee To Accept And Appropriate Grant Funds In An Amount Not To Exceed Three Hundred Twenty-Five Thousand, Seven Hundred Fifty Dollars ($325,750) From The U.S. Department Of Justice, National Institute Of Justice (USDOJ/NIC) For Implementation Of The Fiscal Year 2019 DNA (Deoxyribonucleic Acid) Backlog Reduction Grant Program For The Oakland Police Department; 2) Waive The Advertising And Competitive Bidding Requirements For The Purchase Of DNA Typing Supplies From (1) Promega For One Hundred And Six Thousand Dollars ($106,000), (2) Qiagen For Thirty-Four Thousand Three Hundred Dollars ($34,300), (3) Thermo Fisher/Life Technologies For One Hundred Twenty-Eight Thousand Eight Hundred Dollars ($128,800), And (4) Thermo Fisher/Life Technologies, Aurora Biomed, Qiagen, And/Or Remi For Thirty-Two Thousand Six Hundred Seventy-Four Dollars ($32,674) For DNA Typing Supplies, Instruments, And Service Maintenance.

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

Respectfully submitted,

Anne Kirkpatrick
Chief of Police
Oakland Police Department

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

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

Bruce Stoffmacher, Legislation Manager
OPD, Research and Planning, Training Section

Approved as to Form and Legality

DRAFT
City Attorney

OAKLAND CITY COUNCIL

RESOLUTION NO._____C.M.S.

Introduced by Councilmember _____

RESOLUTION: 1) AUTHORIZING THE CITY ADMINISTRATOR OR DESIGNEE TO ACCEPT AND APPROPRIATE GRANT FUNDS IN AN AMOUNT NOT TO EXCEED THREE HUNDRED TWENTY-FIVE THOUSAND, SEVEN HUNDRED FIFTY DOLLARS ($325,750) FROM THE U.S. DEPARTMENT OF JUSTICE, NATIONAL INSTITUTE OF JUSTICE (USDOJ/NIJ) FOR IMPLEMENTATION OF THE FISCAL YEAR 2019 DNA (DEOXYRIBONUCLEIC ACID) BACKLOG REDUCTION GRANT PROGRAM FOR THE OAKLAND POLICE DEPARTMENT; 2) WAIVE THE ADVERTISING AND COMPETITIVE BIDDING REQUIREMENTS FOR THE PURCHASE OF DNA TYPING SUPPLIES FROM (1) PROMEGA FOR ONE HUNDRED AND SIX THOUSAND DOLLARS ($106,000), (2) QIAGEN FOR THIRTY-FOUR THOUSAND THREE HUNDRED DOLLARS ($34,300), (3) THERMO FISHER/LIFE TECHNOLOGIES FOR ONE HUNDRED TWENTY-EIGHT THOUSAND EIGHT HUNDRED DOLLARS ($128,800), AND (4) THERMO FISHER/LIFE TECHNOLOGIES, AURORA BIOMED, QIAGEN, AND/OR REMI FOR THIRTY-TWO THOUSAND SIX HUNDRED SEVENTY-FOUR DOLLARS ($32,674) FOR DNA TYPING SUPPLIES, INSTRUMENTS, AND SERVICE MAINTENANCE.

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

WHEREAS, the DNA Forensic Capacity Enhancement and Casework Backlog Program was created by the U.S. Department of Justice, National Institute of Justice (USDOJ/NIJ) to assist laboratories that conduct DNA analysis with a goal of improving DNA laboratory infrastructure and analysis capacity so that DNA samples can be processed efficiently and effectively; and

WHEREAS, grant funds in an amount not to exceed $325,750 were awarded by USDOJ/NIJ to the Oakland Police Department (OPD) to its Fiscal Year 2019 implementation of the DNA Backlog Reduction Program; and

WHEREAS, the DNA Backlog Reduction Program was created to assist laboratories in increasing DNA typing capacity and reducing the number of cases in

their backlog in which DNA analyses may be conducted on biological evidence; and

WHEREAS, the funds will be allocated to continue to purchase real-time polymerase chain reaction (PCR) typing instruments, staff required training, and purchase laboratory validated DNA typing reagents; and

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

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

WHEREAS, the grant term for the proposed initiative is January 1, 2020 through December 31, 2021; and

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

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

RESOLVED: That the City Council hereby authorizes the City Administrator, or designee, to accept and appropriate grant funds in an amount not to exceed $325,750 from the USDOJ/NIJ and to increase revenues and appropriate said budget to OPD; and be it

FURTHER RESOLVED: That said grant funds, in an amount not to exceed $325,750, shall be appropriated in the Federal Grant Fund (2112), Criminalistics Division Org. (102610), Criminalistics Division Program (PS05), in a Project Number to be established; and be it

FURTHER RESOLVED: That said grant funds shall be used purchase two real-time DNA typing instruments; and be it

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

FURTHER RESOLVED: That the City Council finds and determines that pursuant to OMC Section 2.04.050.1.5 and based upon the reasons stated above and in the City Administrator's report accompanying this resolution, that it is in the best interests of the City to waive the advertising and competitive bidding requirements of the OMC for the purchases of DNA typing instruments for $114,000 from Thermo Fisher/Life Technologies, DNA typing supplies from Thermo Fisher/Life Technologies for $14,800, Promega for $106,000; and Qiagen for $34,300, and DNA typing instrument service maintenance from Thermo Fisher/Life Technologies, Aurora Biomed, Qiagen, and/or REMI for $32,674, and be it

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

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

IN COUNCIL, OAKLAND, CALIFORNIA, _____

PASSED BY THE FOLLOWING VOTE:

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

NOES -

ABSENT -

ABSTENTION -

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