CITY OF OAKLAND

Privacy Advisory Commission

February 7, 2019 5:00 PM
Oakland City Hall
Hearing Room 1
1 Frank H. Ogawa Plaza, 1st Floor
Meeting Agenda

***Commission Members**: **District 1 Representative**: Reem Suleiman, **District 2 Representative**: Chloe Brown, **District 3 Representative**: Brian M. Hofer, **District 4 Representative**: Lou Katz, **District 5 Representative**: Raymundo Jacquez III, **District 6 Representative**: Vacant, **District 7 Representative**: Robert Oliver, **Council At-Large Representative**: Saied R. Karamooz, **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. 5:00pm: Call to Order, determination of quorum

2. 5:05pm: Review and approval of January 3 meeting minutes

3. 5:10pm: Open Forum

4. 5:15pm: UC Berkeley's Samuelson Law, Technology & Public Policy Clinic – introduction and discussion of scope of work, including drafting of Privacy Principles.

5. 5:20pm: Surveillance Equipment Ordinance – OPD – Exigent Use of Surveillance Technology report, and take possible action.

6. 5:30pm: Surveillance Equipment Ordinance – OPD – Automated License Plate Reader Anticipated Impact Report – review and take possible action.

7. 6:00pm: Federal Task Force Transparency Ordinance – OPD – presentation of inaugural annual reports (FBI/JTTF, ATF, DEA task forces), and take possible action.

8. 6:30pm: Surveillance Equipment Ordinance – OPD – Body Worn Camera Anticipated Impact Report – review and take possible action.

9. 7:00pm: Adjournment

CITY OF OAKLAND

Privacy Advisory Commission

January 3, 2019 5:00 PM
Oakland City Hall
Hearing Room 1
1 Frank H. Ogawa Plaza, 1st Floor
Meeting Minutes

***Commission Members**: **District 1 Representative**: Reem Suleiman, **District 2 Representative**: Chloe Brown, **District 3 Representative**: Brian M. Hofer, **District 4 Representative**: Lou Katz, **District 5 Representative**: Raymundo Jacquez III, **District 6 Representative**: Vacant, **District 7 Representative**: Robert Oliver, **Council At-Large Representative**: Saied R. Karamooz, **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. 5:00pm: Call to Order, determination of quorum

Members Present: Suleiman, Brown, Hofer, Katz, Oliver, Karamooz, Patterson.

2. 5:05pm: Review and approval of December 6 meeting minutes

Approved unanimously.

3. 5:10pm: Open Forum

There were no Open Forum Speakers.

4. 5:15pm: Surveillance Equipment Ordinance – OFD – Discuss with staff existing equipment capabilities, report and policy drafting sequence

Deputy Chief Nick Luby spoke on behalf of OPD regarding the list provided. The first two technologies: the hand-held Thermal Imaging Camera and the Forward Looking Thermal Camera attached to the airport apparatus do not qualify under the ordinance and therefore do not need a policy adopted.

The third device, OFD Communications Van Cameras would qualify but are currently non-operational. If funding is identified to operationalize them, OFD would need to return to the PAC to develop a policy.

5. 5:25pm: Surveillance Equipment Ordinance – OPD – Body Worn Camera Anticipated Impact Report and draft Use Policy – (continued from December 6) review and take possible action

OPD presented an updated Impact Report and the Commission provided additional feedback but continued the item to February.

6. 6:00pm: Surveillance Equipment Ordinance – OPD – Automated License Plate Reader Anticipated Impact Report and draft Use Policy – review and take possible action

OPD presented an updated Impact Report and the Commission provided additional feedback but continued the item to February.

7. 6:25: Unapproved Use of Surveillance Technology Report—OPD-take action on Report.

OPD presented the Report and it was accepted and forwarded to the City Council.

8. 7:00pm: Adjournment

CITY OF OAKLAND

MEMORANDUM

TO:	Privacy Advisory Commission	**FROM:**	Anne E. Kirkpatrick
SUBJECT:	Use of Unapproved Surveillance Technology Under Exigent Circumstances – January 28, 2019	**DATE:**	January 22, 2019

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).

BASIS FOR EXIGENCY

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.

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

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;
- 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.

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

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.
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.

Respectfully submitted,

Anne E. Kirkpatrick
Chief of Police
Oakland Police Department

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

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

Prepared by:
Sergeant Omar Daza-Quiroz
Intelligence Unit
OPD

OAKLAND POLICE DEPARTMENT

Surveillance Impact Use Report for the Automated License Plate Reader

1. Information Describing the Automated License Plate Reader (ALPR) and How It Works

ALPR technology consists of cameras that can automatically scan license plates on vehicles that are publicly visible (in the public right of way and/or on public streets). The Oakland Police Department (OPD) uses only ALPR cameras mounted to patrol vehicles so that license plates can be photographed during routine police patrol operations. Each camera housing (two housings per vehicle) consists of a regular color photograph camera as well as an infrared camera (for better photography during darkness). ALPR reads these license plates with a lens and charge-coupled device (CCD) that sense and records the image as well and connects the image to an optical character recognition (OCR) system that can connect the image to that actual license plate characters.

The ALPR system in a patrol vehicle is turned on manually by authorized personnel in a police patrol vehicle. Once initiated, the system runs continuously and photographs vehicles during until turned off manually. The system compares license plate characters against specific databases, and stores the characters along with the date, time, and location of the license plate in a database. Authorized personnel within OPD can also enter specific license plate numbers into the system so that active vehicle ALPR systems will alert the officer in the vehicle if there is a real-time match between the entered license plate and the observed and photographed license plate. The system in vehicles uploads all photographs to the OPD-maintained database when authorized personnel turn off the system. The platform software allows authorized personnel to query the system to see if a certain license plate (and associated vehicle) have been photographed. The system will show the geographic location within Oakland for license plates that have been photographed, as well as time and date. Authorized personnel can see the actual photographs that match a particular license plate query – the OCR system can incorrectly match letter and digit characters so the actual photographs are vital for ensuring the accuracy of the license plate query.

2. Proposed Purpose

OPD uses ALPR for two purposes:

1. The immediate (real time) comparison of the license plate characters

against specific databases such as those provided by the California Department of Justice listing vehicles that are stolen or sought in connection with a crime or missing persons; and

2. Storage of the license plate characters – along with the date, time, and location of the license plate – in a database that is accessible by law enforcement (LEA) agencies for investigative purposes.

3. Locations Where, and Situations in which ALPR Camera Technology may be deployed or utilized.

OPD owns 35 sets (left and right) of ALPR vehicle-mounted cameras. Authorized personnel (as described in the Mitigations Section below) may operate ALPR camera technology on public streets in the City of Oakland.

4. Impact

ALPR technology helps OPD personnel to leverage their street presence and to more effectively use their limited time for more critical activity. The technology can alert officers to vehicles that are stolen or connected to a serious felony crime (e.g. aggravated assault, homicide, robbery, sexual assault) immediately (by automatically connected to criminal databases). Officers can then use the information to notify OPD personnel and/or stop the vehicle as justified by the information. The automatic process can free officers from laborious data entry processes allowing more time for observing public activity and speaking with members of the public.

ALPR also provides an important tool for criminal investigations. The information collected by analysists and investigators can locate locations where a plate has been in the past, which can help to confirm whether or not a vehicle has been at the scene of a crime. Such information may help personnel to find new leads in a felony crime investigation.

OPD has not historically tracked ALPR usage for vehicle stops, nor for later criminal investigations[1] in a way that easily allows for impact analysis. However, OPD's Criminal Investigations Division, in preparation for this report, has found cases where ALPR license plate locational data was instrumental in the ultimate arrest and arraignment of at least two homicide suspects, and with the conviction of at least one of them. There are also documented cases where other LEA contact OPD to make specific queries regarding serious crimes which have occurred in their jurisdictions. OPD personnel believe that ALPR has provided critical information for many other felony cases but cannot currently document them.

OPD recognizes that the use of ALPR technology raises significant privacy concerns. There is concern that the use of ALPR technology can be utilized

[1] Current policies mandate documenting reasons for vehicle stops and reported race and gender persons stopped. OPD is reviewing how to ensure that investigators note when ALPR was instrumental in criminal investigations for documenting ALPR impact.

to ascertain vehicle travel patterns over periods of time. OPD can use the ALPR technology to see if a particular license plate (and thus the associated vehicle) was photographed in particular places during particular times; however OPD can only develop such by manually querying the system based upon a right to know (see Mitigation Section 5 below. OPD also recognizes that ALPR cameras may photograph extraneous data such as images of the vehicle, the vehicle driver and/or bumper stickers or other details that affiliate the vehicle or driver with particular groups. As explained in the Description Section (1) above and the Mitigation (5) section below, authorized personnel can only manually query the ALPR system for particular license plates and only for particular reasons as outlined in OPD policy. Therefore, technology cannot be used to query data based upon vehicle drivers, type of vehicle, or based on any type of article (e.g. bumper sticker) affixed to a vehicle. Additionally, OPD has instituted many protocols (see Mitigation section below) to safeguard against the unauthorized access to any ALPR data.

There is concern that ALPR camera use may cause disparate impacts if used more intensely in certain areas such as areas with higher crime and greater clusters of less-advantaged communities. Firstly, OPD does not affix ALPR cameras to fixed infrastructure. OPD deploys ALPR camera-affixed vehicles through every area of Oakland[2], even though there may be times when OPD Commanders request that ALPR cameras be used in particular areas for short periods of time to address crime patterns. Therefore, there is little possibility that vehicles travelling within certain neighborhoods, or by certain streets will more likely have their license plates recorded over an extended period of time. Lastly, ALPR usage does not lead to greater police stops; ALPR use only directly impacts the public in the case where a real-time photographed license plate matches a stop warrant for a stolen vehicle or serious crime in a criminal database.

Commented [BS1]: What about TOS trailer?

5. Mitigations

OPD ALPR policy provides several mitigations which limit the use real-time and aggregated ALPR data. OPD's Direct General Order (DGO) "I-12: Automated License Plate Readers" Policy Section "B-2 Restrictions on Use," provides a number of internal safeguards, including:

1. Accessing data collected by ALPR requires a right to know and a need to know. A right to know is the legal authority to receive information pursuant to a court order, statutory law, or case law. A need to know is a compelling reason to request information such as direct involvement in an investigation.
2. Department members shall not use, or allow others to use the equipment or database records for any unauthorized purpose (Civil Code § 1798.90.51; Civil Code § 1798.90.53);

[2] OPD often must use ALPR camera-equipped vehicles for standard patrol activity regardless of location because of limited fleet reserves.

3. Personnel must complete equipment-specific training prior to use;
4. No ALPR operator may access department, state or federal data unless otherwise authorized to do so;
5. Consideration should be given to using ALPR-equipped cars to canvass areas around homicides, shootings and other major incidents;
6. ALPR shall only be used for official LEA business; and
7. If practicable, agency personnel should verify ALPR response through the California Law Enforcement Telecommunications System (CLETS) before taking enforcement action that is based solely on an ALPR alert.

OPD requires ALPR training of all personnel authorized to access the ALPR system. This training includes subjects such as:

- Applicable federal and state law
- Applicable policy
- Memoranda of understanding with other
- Functionality of equipment
- Accessing data
- Safeguarding password information and data
- Sharing of data
- Reporting breaches
- Implementing post-breach procedures

ALPR policy also requires that personnel input the reason for each system query. The database software also creates a log of activity including which personnel member used the system and which license plates were queried.

6. Data Types and Sources

ALPR data is composed of photographs of license plates, which can be linked through OCR software to identify license plate letter and digit characters. License plate photographs, as detailed in Section One above, may contain images of the vehicle with particular visual details of the vehicle (such as bumper stickers). Photographs may also contain images of the vehicle driver. However, the ALPR system only annotates photographs based on license plate characters; therefore, authorized personnel can only query license plate numbers – there is no way to query the system based on type of vehicle, vehicle details (such as bumper stickers) or individuals associated with a vehicle.

OPD is currently seeking legal guidance regarding State of California law which relates to ALPR and other data retention requirements. OPD shall permanently maintain ALPR data when connected to one of the following situations:

1. A criminal investigation;
2. An administrative investigation;
3. Research;

4. Civil litigation;
5. Training; and/or
6. Other Departmental need.

7. Data Security

OPD takes data security seriously and safeguards ALPR data by both procedural and technological means. OPD will observe the following safeguards regarding access to and use of stored data (Civil Code § 1798.90.51; Civil Code § 1798.90.53):

1. All ALPR data downloaded to the mobile workstation and in storage shall be accessible only through a login/password-protected system capable of documenting all access of information by username, license number or other data elements used in the search, name, date, time and purpose (Civil Code § 1798.90.52).
2. Members approved to access ALPR data under these guidelines are permitted to access the data for legitimate LEA purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action.

OPD also conducts regular ALPR system audits to ensure the accuracy of ALPR data.

8. Costs

OPD spent $293,500 in 2014 to purchase the ALPR system from 3M. Neology later purchased the ALPR product line from 3M. OPD however does not have a maintenance contract with Neology and therefore relies on EVO for ALPR maintenance. Currently spends approximately $50,000 annually with EVO-Emergency Vehicle Outfitters Inc. for ALPR vehicle camera maintenance. OPD relies on EVO to outfit police vehicles with many standard police technology upgrades (e.g. vehicle computers) as well as ALPR camera maintenance.

9. Alternatives Considered

OPD officers and investigators rely primarily on traditional policing techniques to gather evidence related to criminal investigations such as speaking to witnesses and suspects, gathering information from observations, and using standard data aggregation systems. These methods will continue to be employed as primary investigative tools that will be supplemented by use of BWCs to document police activity.

ALPR technology provides LEA personnel with a fast and efficient way to connect vehicles to violent and felonious criminal activity. This tool helps

OPD's authorized personnel increase their ability to find wanted suspects and help solve crimes in a way that is unique – by creating a time map of vehicle locational activity. OPD recognizes the privacy concerns inherent in such a technology but has in place the numerous mitigations and data security protocols described in sections five and seven above respectively. However, OPD believes that the alternative to ALPR usage would be to forgo its observational and investigatory benefits. OPD LEA personnel, without access to ALPR data, would rely patrol officer observations and other basic investigatory processes. OPD data suggest that some future violent felonies would remain unsolved if only for the inability to use ALRP technology.

10. Track Record of Other Entities

Numerous local and state government entities have researched and evaluated the use of ALPR cameras. The International Association of Chiefs of Police (IACP) documents many recent reports[3]. The AICP report, "News Stories about Law Enforcement ALPR Successes September 2017 - September, 2018"[4] presents scores of cases from different national LEA jurisdictions where ALPR data helped lead to the capture of violent criminals. A July 2014 study[5] from the Rand Corporation research organization found that ALPR cameras have proven useful for crime investigations in numerous cities and states, and that systems with the most database access and longest retention policies provide the greatest use in terms of providing real-time information as well as useful investigation data. This report also find that privacy mitigations are critical to ensuring legal use of ALPR and public privacy protections.

[3] https://www.theiacp.org/projects/automated-license-plate-recognition
[4] https://www.theiacp.org/sites/default/files/ALPR%20Success%20News%20Stories%202018.pdf
[5] https://www.rand.org/pubs/research_reports/RR467.html

OPD - Federal Bureau of Investigation (FBI)
Joint Terrorism Taskforce (JTTF) 2018 Annual Report

Staffing

1. **Number of full and part time OPD officers assigned to JTTF:** One officer.
2. **Number of hours worked as JTTF officer**: Regular 40 hours per week. However, the current task force officer is often assigned to other OPD operations based on OPD needs and priorities and whether or not there is any active counter-terrorism investigation.
3. **Funding source for OPD JTTF officer salary**: Regular OPD general personnel funding.

Other Resources Provided

1. **Communication equipment:** City of Oakland Cellular Telephone
2. **Surveillance equipment:** None
3. **Clerical/administrative staff hours:** None
4. **Funding sources for all the above:** Regular OPD general equipment funding.

Cases

1. **Number of cases OPD JTTF officer was assigned to:**
2. **Number of "duty to warn" cases:** none
3. **General types of cases:** counter-terrorism
4. **Number of times the FBI asked OPD to perform/OPD declined to perform:** None – the FBI knows that OPD task force officers must comply with all Oakland laws and policies. Furthermore, the FBI commonly works with different jurisdictions and understands that taskforces must collaborate with the particular polices and laws of those jurisdictions.
   a. **Reason for OPD declination (e.g. insufficient resources, local/state law):** N/A

Commented [BS1]: Checking w/ OPD Intel

Operations

1. **Number of Assessments opened:**
2. **Number of Voluntary Interviews opened:** The FBI cannot disclose this information; a Freedom of Information Act (FOIA) request would have to be made and the information would be redacted before release.
3. **Number of Assessments closed without becoming preliminary or full investigations:** Same answer as above.
4. **Number of Voluntary Interviews closed without becoming preliminary or full investigations:** Same answer as above.
5. **Number of times use of undercover officers were approved** Same answer as above.
6. **Number of instances where OPD JTTF officer managed informants:** Same answer as above.
7. **Number of cases involving informants that OPD JTTF officer worked on:** Same answer as above.
8. **Number of requests from outside agencies (e.g. ICE) for records or data of OPD:**

Commented [BS2]: Checking w/ OPD Intel

a. **Number of such requests that were denied:** Same answer as above.
b. **Reason for denial:** Same answer as above.

9. **Whether OPD JTTF officer was involved in any cases where USPER (U.S. person status) information was collected:** Same answer as above.
10. **Number of cases:** Same answer as above.

Training and Compliance

1. **Description of training given to OPD JTTF officer by OPD to ensure compliance with Oakland and California law:** The OPD officer assigned to the JTTF follows all OPD policies and has received several police trainings, including but not limited to: continual professional training, Procedural Justice Training and annual firearms training. The officer has also reviewed all provisions of the JTTF MOU.
2. **Date of last training update, and last training audit:**
3. **Frequency with which OPD JTTF officer briefs OPD supervisor on cases:** Weekly and daily if and when a critical incident occurs.

Commented [BS3]: Checking w/ OPD Intel

Actual and Potential Violations of Local/State Law

1. **Number of actual violations:** Release of any of this information would violate California law (832.7), as there is only one OPD officer per task force.
2. **Number of potential violations:** Same answer as above.
3. **Actions taken to address actual or potential violations:** The officer follows OPD polices. OPD leadership consult with the Office of the City Attorney to ensure that all polices conform with State and Federal laws.
4. **Recommendations by OPD to address prevention of future violations:** OPD will continue to consult with the Office of the City Attorney and the Privacy Advisory Commission to ensure that personnel continue to follow federal, state, and local laws and policies.

SARs and NCRIC

1. **Whether OPD JTTF officer submits SARs to NCRIC:**
2. **Whether OPD officer receives SAR information:**

Commented [BS4]: Checking w/ OPD Intel

Command Structure for OPD JTTF Officer

1. **Reports to whom at FBI?** Counterterrorism Assistant Agent in Charge
2. **Reports to whom at OPD?** Sergeant Omar Daza-Quiroz in OPD Intelligence Unit

OPD – Alcohol Tobacco and Firearms (ATF) Taskforce 2018 Annual Report

Staffing

1. **Number of full and part time OPD officers assigned to ATF Taskforce:** Two officers.
2. **Number of hours worked as ATF Taskforce Officer**: Regular 40 hours per week. However, one of the current task force officers is often assigned to other OPD operations. The work assignment of this officer is based on OPD needs and priorities and whether or not there active investigations.
3. **Funding source for ATF Taskforce Officer salary**: City of Oakland General Purpose Fund and ATF overtime reimbursement.

Other Resources Provided

1. **Communication equipment:** OPD and ATF radios.
2. **Surveillance equipment:** ATF funded rental vehicle
3. **Clerical/administrative staff hours:** N/A
4. **Funding sources for all the above:** City of Oakland General Purpose Fund and ATF funds.

Cases

1. **Number of cases ATF Taskforce Officer was assigned to:** Seven.
2. **Number of "duty to warn" cases:** N/A
3. **General types of cases:** Firearms and narcotics.
4. **Number of times ATF asked OPD to perform/OPD declined to perform:** None
   a. **Reason for OPD declination (e.g. insufficient resources, local/state law):** N/A

Operations

1. **Number of Assessments opened:** Seven.
2. **Number of Voluntary Interviews opened:** Six
3. **Number of Assessments closed without becoming preliminary or full investigations:** Two.
4. **Number of Voluntary Interviews closed without becoming preliminary or full investigations:** Two.
5. **Number of times use of undercover officers were approved:** Three.
6. **Number of instances where OPD Taskforce officer managed informants:** Zero.
7. **Number of cases involving informants that ATF Taskforce Officer worked on:** All cases except adopted cases.
8. **Number of requests from outside agencies (e.g. ICE) for records or data of OPD**
   a. **Number of such requests that were denied:** None.
   b. **Reason for denial:** None.
9. **Whether ATF Taskforce Officer was involved in any cases where USPER (U.S. person status) information was collected:** None.

Training and Compliance

1. **Description of training given to ATF Taskforce Officer by OPD to ensure compliance with Oakland and California law:** The OPD officers assigned to the ATF Taskforce follow all OPD policies and has received several police trainings, including but not limited to: continual professional training, Procedural Justice Training and annual firearms training. The officers have also reviewed all provisions of the ATF Taskforce MOU.
2. **Date of last training update, and last training audit:** June 2018.
3. **Frequency with which ATF Taskforce Officer briefs OPD supervisor on cases:** Monthly.

Actual and Potential Violations of Local/State Law

1. **Number of actual violations:** Release of any of this information would violate California law (832.7), as there is only two OPD officer assigned to this task force.
2. **Number of potential violations:** Same answer as above.
3. **Actions taken to address actual or potential violations:** The officers follow OPD polices. OPD leadership consult with the Office of the City Attorney to ensure that all polices conform with State and Federal laws.
4. **Recommendations by OPD to address prevention of future violations:** OPD will continue to consult with the Office of the City Attorney and the Privacy Advisory Commission to ensure that personnel continue to follow federal, state, and local laws and policies.

SARs and NCRIC

1. **Whether OPD Taskforce Officer submits SARs to NCRIC:** None.
2. **Whether OPD officer receives SAR information:** None.

Command Structure for OPD Taskforce Officer

1. **Reports to whom at ATF?** Supervisory Agent in Charge Tom Cleary.
2. **Reports to whom at OPD?** Sergeant Robert Muniz and Lieutenant James Beere.

OPD – Drug Enforcement Agency (DEA) Taskforce
2018 Annual Report

Staffing

1. **Number of full and part time OPD officers assigned to DEA Taskforce:** One
2. **Number of hours worked as DEA Taskforce Officer**: 1,865 hours.
3. **Funding source for DEA Taskforce Officer salary**: N/A

Other Resources Provided

1. **Communication equipment:** None
2. **Surveillance equipment:** None
3. **Clerical/administrative staff hours:** None
4. **Funding sources for all the above:** None

Cases

1. **Number of cases DEA Taskforce Officer was assigned to:** None
2. **Number of "duty to warn" cases:** N/A
3. **General types of cases:** Drugs and money laundering investigations
4. **Number of times the DEA asked OPD to perform/OPD declined to perform:** None
   a. **Reason for OPD declination (e.g. insufficient resources, local/state law):** N/A

Operations

1. **Number of Assessments opened:** N/A
2. **Number of Voluntary Interviews opened:** N/A
3. **Number of Assessments closed without becoming preliminary or full investigations:** N/A
4. **Number of Voluntary Interviews closed without becoming preliminary or full investigations:** N/A
5. **Number of times use of undercover officers were approved:** zero
6. **Number of instances where OPD Taskforce officer managed informants:** Zero
7. **Number of cases involving informants that DEA Taskforce Officer worked on:** One
8. **Number of requests from outside agencies (e.g. ICE) for records or data of OPD**
   a. **Number of such requests that were denied:** None
   b. **Reason for denial:** None
9. **Whether DEA Taskforce Officer was involved in any cases where USPER (U.S. person status) information was collected:** none

Training and Compliance

1. **Description of training given to DEA Taskforce Officer by OPD to ensure compliance with Oakland and California law:** The OPD officer assigned to the DEA Taskforce follows all OPD policies and has received several police trainings, including but not limited to: continual professional training, Procedural Justice Training and annual firearms training. The officer has also reviewed all provisions of the DEA Taskforce MOU.
2. **Date of last training update, and last training audit:** April 19, 2018.
3. **Frequency with which DEA Taskforce Officer briefs OPD supervisor on cases:** Weekly.

Actual and Potential Violations of Local/State Law

1. **Number of actual violations:** Release of any of this information would violate California law (832.7), as there is only one OPD officer per task force.
2. **Number of potential violations:** Same answer as above.
3. **Actions taken to address actual or potential violations:** The officer follows OPD polices. OPD leadership consult with the Office of the City Attorney to ensure that all polices conform with State and Federal laws.
4. **Recommendations by OPD to address prevention of future violations:** OPD will continue to consult with the Office of the City Attorney and the Privacy Advisory Commission to ensure that personnel continue to follow federal, state, and local laws and policies.

SARs and NCRIC

1. **Whether OPD Taskforce Officer submits SARs to NCRIC:** None.
2. **Whether OPD officer receives SAR information:** None.

Command Structure for OPD Taskforce Officer

1. **Reports to whom at DEA?** Special Agent in Charge Brian Cole.
2. **Reports to whom at OPD?** Sergeant Robert Muniz.

OAKLAND POLICE DEPARTMENT

Surveillance Impact Use Report for the Body Worn Camera

1. Information Describing the Body Worn Camera and How It Works

The Body Worn Camera (BWC) is a durable video camera meant to attach to a police officer's uniform. The BWC has an "on" and "off" switch to allow personnel to record only during authorized and required uses. The on/off switch also opens and closes the lens cover so as to protect the lens when not in use. OPD BWC policy dictates that officers are to wear the BWCs on the front of their uniform or uniform equipment, as the primary recording location, to facilitate recording. The BWC may be temporarily moved from the primary location to facilitate recording in furtherance of a police objective. Upon completion of the objective, the BWC shall be returned to the primary recording location as soon as practical.

The BWC records video footage directly onto the solid-state internal storage unit when in recording "on" function. The BWC contains a solid-state computer storage unit capable of storing digital video files.

The Portable Video Management System (PVMS) is a computer server and/or internet cloud-based video archival, storage, and playback system. OPD in 2018 entered into a contract with VIEVU to purchase new LE5 generation BWCs as well as a BWC-docking and internet cloud-based storage and archival system.

2. Proposed Purpose

The authorized and required purposes for the PVMS including the BWC and for collecting information using that technology to:

a. Citizen contacts to confirm or dispel a suspicion that the citizen may be involved, as a suspect, in criminal activity;

b. Detentions and Arrests; Assessment or evaluation for a psychiatric detention;

c. Involved personnel during a vehicle pursuit;

d. Serving a search or arrest warrant;

e. Conducting any of the following searches of a person and/or property;

- Incident to arrest;
- Cursory* (i.e., patdown or limited weapons search);

- Probable Cause; Probation/Parole; Consent; or Inventory[1]
- Transporting any detained or arrested citizen (excluding prisoner wagon transports); or
- Upon the order of a higher-ranking member.

OPD BWC policy dictates that personnel shall de-activate their BWCs during the following situations:

a. Their involvement in the citizen contact, arrest or detention has concluded or becomes a hospital guard.

b. They receive an order from a higher-ranking member;

c. They are discussing administrative, tactical or law enforcement sensitive information away from the citizen;

d. They are at a location where they are not likely to have interaction or a chance encounter with the suspect (e.g. outer perimeter post, traffic control post, etc.);

e. The search requiring activation has concluded, and the officer believes they will have no further interaction with the person;

f. The officer reasonably believe the recording at a hospital may compromise patient confidentiality;

g. A pursuit[2] has been terminated;

h. The officer is interviewing an informant for the purpose of gathering intelligence. At the conclusion of the interview, the BWC shall be re-activated until no longer required by policy; or

i. The officer is meeting with an undercover officer. At the conclusion of the meeting, the BWC shall be re-activated until no longer required by policy;

j. Taking a statement from a victim or witness in lieu of taking a written statement (shall not be used to record statements from child abuse or sexual assault victims); Personnel shall advise or obtain consent from victims or witnesses when taking a BWC recorded statement;

k. Officers, when not prohibited from or required to activate their BWC, may use their own discretion when deciding to activate and de-activate the BWC.

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

[1] "Inventory" refers to a check of a vehicle or structure for contents. Officers are required to conduct an inventory of vehicles that are towed.

[2] Pursuits can be terminated for a variety of reasons. Pursuit termination refers to the end of the entire police activity; personnel continue to utilize BWCs following pursuits that lead to further actions such as arrests and/or speaking with potential victims or witnesses. Personnel are not required to utilize BWCs after pursuits that end by no longer attempting to pursue a person(s) or vehicle(s).

utilized.

Officers may use BWCs anywhere where officers have jurisdiction to operate as sworn officers. Officers shall not use BWCs during certain proscribed situations described above in Section 2.

4. Impact

BWC technology provides video and audio documentation of policing activity in addition to the oral and written statements of officers, victims, and witnesses. BWCs provide OPD with an important tool to promote personnel accountability as well as policing transparency. A recent Police Foundation report explains that BWC "benefits may include reductions in police use-of-force incidents, fewer complaints against officers, improvements in citizens' satisfaction with the police, and increased public perceptions of the legitimacy of police agencies.[3]"

Between 2012 and 2017, officer use of force (UOF) has decreased each year[4] - from 1,46 incidents to 317 (a 75% decline over five years). OPD cannot definitely prove a causal relationship between use of BWCs and declining UOF rates. However, some studies have directly linked use of BWCs with declines in UOF rates – a Mesa, AZ internal 2013 study also reported a 75% UOF decline due to BWC usage[5].

Complaints against OPD and OPD officers have increased somewhat since 2016 (482 between July and December 2015; 685 between January and June 2018), although OPD cannot draw a correlation between this complaint increase and ongoing BWC usage. The greatest type of complaint between January 1 and June 30, 2018 shows that the largest number (42 percent) fall under the "Other" category; duplicates are the same complaints are the same complaint received more than once, and service complaints are not actionable because they did not involve allegations of misconduct against specific employees. Performance of Duty[6] was the second most common (32%) type of complaint.

Police misconduct legal claims have steadily declined on average from a high between January-June 2012 (76) to January to June 2018 (22). OPD cannot make a direct connection between misconduct complaint declines and BWC usage. However, OPD leadership expect the ongoing implementation of policy and procedural justice trainings will foster better police-community trust.

OPD recognizes that the use of BWC technology raises significant privacy

---

[3] Cost and Benefits Of Body-Worn Camera Deployments, Final Report, April, 2018, Police Foundation Executive Forum, page 17 - https://www.policeforum.org/assets/BWCCostBenefit.pdf

[4] UOF data on Oakland Open Data Portal: https://data.oaklandnet.com/dataset/OPD-Use-of-Force-all-levels-2012-2017/y4uh-vs2v

[5] Cost and Benefits Of Body-Worn Camera Deployments, Final Report, April, 2018, page 47

[6] This category includes: intentional illegal search, seizure, or arrest; unintentional or improper search, seizure, or arrest; failure to perform duties as required or directed by law, Departmental rule, policy, or order; improper care of the property of persons; and; changing a work assignment without authority

concerns. There is concern that the use of ALPR technology can be utilized to record people peacefully gathering to assemble and/or legally protest political activity. OPD Department General Order (DGO) I-15: Body Worn Camera, as explained in the Mitigation (Section 5 below) details how authorized personnel may only use BWC technology during certain conditions. DGO 1-15 also describes how BWCs will not be used during certain conditions so as to support the privacy of individuals during certain conditions (e.g. taking testimony from sexual assault victims). Furthermore, OPD policy requires that officers annotate each video file at the end of their work shift, so officers must justify their activity in which a video file was generated. Additionally, a log file is created whenever authorized personnel log into the BWC PVMS. The need to know access requirement for viewing files, the required video annotations, and the log files generated by viewing BWC files creates a multi-layered system to guard against the unauthorized access to video evidence.

5. Mitigations

OPD BWC policy provides several mitigations which limit the use of this audio and video technology. Firstly, OPD Department General Order (DGO) I-15: Body Worn Camera Program Section A "Purpose of the Technology" provides clarity and direction for when BWCs can or cannot be used, or for when officer discretion is allowed. For example, BWC usage is required per policy during detentions and arrests; policy requires that BWCs be deactivated during used to record statements from child abuse or sexual assault victims.

BWC policy provides numerous internal protocols which limit access to video footage and help to ensure greater privacy controls. Other mitigations provide public access to video content to promote greater police transparency.

DGO I-15 explains that all BWC files are the property of the Oakland Police Department, and that the unauthorized use, duplication, editing, and/or distribution of BWC files is prohibited. Officers are assigned particular BWCs that each have serial numbers and upload video files that are automatically tagged to the assigned officer. The OPD Information Technology Unit is designated as the Custodian of Record for all BWC data files. Officers do not have access to video footage recorded from their BWCs once they are docked (at the end of a shift) and uploaded to the video management system. Video footage is only accessible on a need to know basis per OPD policy. Personnel are not allowed to remove, dismantle or tamper with any hardware/software component or part of the BWC. OPD's BWC platform always requires double-layer authentication login (authorized personnel receive an email or text message code which must be entered as part of the login). Additionally, the BWC platform utilizes software that creates cryptographic files which would leave an evidence trail of any type of alteration of the video file.

OPD BWC Policy requires that all sergeants audit BWC videos involving certain arrests and incidents involving Use of Force. Sergeants are required to view video

footage from beginning of the incident to the arrest, and sergeants are required to annotate their view of the BWC footage in the comment area of the system.

DGO I-15 D-1 articulates that members of OPD are not allowed to intentionally use the BWC recording functions to record any personal conversation of, or between another member without the recorded member's knowledge. This section also explains that personnel may not intentionally use the BWC to record at Department facilities where a reasonable expectation of privacy exists (e.g., bathrooms, locker rooms, showers) unless there is a legal right to record and a Departmental requirement to record. These rules serve to support the privacy of OPD members.

DGO I-15 Section H-2 explains that OPD will produce an annual report for the PAC and the Public Safety Committee. The annual report will provide numerous metrics related to the use of BWCs:

Protocols for the use of BWCs during certain interviews with victims and witnesses provides another policy mitigation to ensure public privacy. DGO 15 provides that officers shall not use BWCs during contact with victims and witnesses to possible sexual assault, domestic violence and/or child abuse.

OPD's BWC data retention policy also helps to ensure public privacy from BWC usage. OPD's current data retention policy provides that OPD will delete all BWC video footage unless a particular video has been identified for permanent keeping as a part of an investigation.

Commented [BS1]: Need to define policy….

Commented [BS2]: We need to talk about why the retention policy is just / useful based on where we land

OPD mitigates against improper public release of video footage with protocols outlined in DGO 15; BWC files are reviewed and released in accordance with federal, state, local statutes, and Departmental General Order M-9.1 (PUBLIC RECORDS ACCESS. However, OPD will also comply with the newly enacted Assembly Bill 749 (signed by Governor Edmund G. Brown, Jr. on September 30, 2018. This new law mandates that audio and visual recordings of "critical incidents" resulting in either the discharge of a firearm by law enforcement or in death or great bodily injury to a person from the UOF by a police officer to be made publicly available under the Public Records Act within 45 days of the incident, with certain exceptions.

6. Data Types and Sources

BWC data is composed of recordings of live video and sound footage of incidents where personnel activate there BWCs.

BWCs record digital video files. BWC video may contain images and voice recordings of members of the public who have been stopped by officers during regular police operations; videos may also contain images and voice recordings of individuals such as witnesses, victims of crimes and/or individuals being asked to provide information to officers related to criminal activity or suspected criminal activity. Videos may also contain information and voice recordings related to any activity where OPD personnel are required to activate BWCs as described above in Section #2 "Proposed

Purpose."

7. Data Security

The PVMS employed by OPD features BWC docking stations and an internet web interface for controlling how files are uploaded and archived. The interface allows for Internet Protocol restriction features to control the locations where the system can be accessed. These restrictions limit BWC video file access to only authorized OPD personnel. Videos that are tagged for any reason as part of an investigation are moved to separate folders where they cannot be deleted. OPD currently employs an "on-premises" server back-up system to maintain all BWC video files. Historically, OPD has not deleted any video files archived to the older PVMS. Once OPD fully transitions to the new VIEVU cloud archive environment, videos not tagged for investigations shall be maintained for three years. The VIEVU cloud-based archive system has built-in redundancy with multiple servers to ensure the data integrity.

OPD's BWC policy helps to ensure data security through numerous protocols (see mitigations above).These policies help to ensure that OPD BWC video footage remains well secured on BWCs and OPD and/or VIEVU servers; all video footage is the property of OPD and OPD does not share video footage with other organizations. VIEVU BWCs encrypt video data both within the BWC as well as in the cloud-based storage system for data security.

8. Costs

In November 2017, the Oakland City Council approved a resolution authorizing a contract between OPD and VIEVU LLC. VIEVU was chosen after a competitive Request for Proposal (RFP) process. The new contract which will not exceed $1.271 million dollars, allows OPD to buy new BWCs and to have VIEVU provide a complete fully hosted digital evidence management solution. The new contract will serve OPD from 2018 through 2022.

9. Third Party Dependence

The Oakland Police Department uses VIEVU brand BWCs and is reliant upon VIEVU for BWC maintenance. The new OPD VIEVU contract allows for OPD to begin using the VIEVU PVMS for video file back-up, search, storage and security.

10. Alternatives Considered

OPD officers and investigators rely primarily on traditional policing techniques to gather evidence related to criminal investigations such as

speaking to witnesses and suspects, gathering information from observations, and using standard data aggregation systems. These methods will continue to be employed as primary investigative tools that will be supplemented by use of BWCs to document police activity.

PRDR technology provides video and audio documentation of policing activity in addition to the oral and written statements of officers, victims, and witnesses. Alternatives to the use of BWCs would be vehicle-based cameras and/or not utilizing BWCs. However, OPD sees the use of BWCs as an integral strategy to ensuring that officers use procedurally just strategies and to ensure compliance with how officers interact with members of the public. The video and audio files generated using BWCs provide an important record of police encounters which can be reviewed against statements made by officers and members of the public. OPD's BWC usage provides a layer of accountability and transparency for OPD as well as for all Oakland residents and visitors.

11. Track Record of Other Entities

Scores of police agencies have now adopted BWCs as a tool to promote officer accountability. Many departments have developed their own usage policies which may include standards for required officer use, supervisory review, storage and data retention standards, and internal and public access.

A report for the U.S. Bureau of Justice Administration[7] cites a 2013 Rialto, CA study that showed that the use of BWCs led to a 59 percent decrease in UOF and an 87.5 percent decrease in citizen complaints. Likewise, the Mesa, AZ report noted in "Impact" Section above also points to large decreases in UOF and citizen complaints.

The 2017 Police Body Worn Cameras: A Policy Scorecard[8] provides an analysis of how scores of different police agencies have employed BWCs through the following metrics:

- Is the policy available for the public?
- Limits on officer discretion for when to record;
- Does the policy address personal privacy concerns?
- Are there prohibitions on officer pre-report viewing?
- Is there a specific data-retention policy?
- Policies for tampering with video footage;
- Is footage available to individuals filing complaints?; and
- Are there limits against biometric data analysis?

[7] https://www.bja.gov/bwc/pdfs/14-005_Report_BODY_WORN_CAMERAS.pdf - pages 6-8
[8] https://www.bwcscorecard.org/