CITY OF OAKLAND

Privacy Advisory Commission

January 3, 2019 5:00 PM
Oakland City Hall
Hearing Room 1
1 Frank H. Ogawa Plaza, 3rd 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 December 6 meeting minutes

3. 5:10pm: Open Forum

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

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

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

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

8. 7:00pm: Adjournment

CITY OF OAKLAND

Privacy Advisory Commission

December 6, 2018 5:00 PM
Oakland City Hall
Hearing Room 1
1 Frank H. Ogawa Plaza, 3rd 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: Jaquez, Hofer, Katz, Suleiman, Oliver.

2. 5:05pm: Review and approval of November 26 special meeting minutes

The minutes were approved unanimously.

3. 5:10pm: Open Forum

There were no Open Forum Speakers.

4. 5:15pm: Surveillance Equipment Ordinance – DOT – Unmanned Aerial Vehicle Anticipated Impact Report and draft Use Policy – review and take possible action

Staff from the Department of Transportation presented the Anticipated Impact Statement and Proposed Use Policy and the PAC made some minor edits and then recommended approval and forwarding to the City Council unanimously.

5. 5:35pm: Surveillance Equipment Ordinance – OFD – Discuss with staff existing equipment capabilities, report and policy drafting sequence

This item was tables until January.

6. 5:50pm: Federal Task Force Transparency Ordinance – Discuss with OPD annual reporting metrics

The attached JTTF Annual Compliance Report Template was reviewed and discussed. Bruce Stoffmacher with OPD noted that he was using the template to gather the requested information internally and was already about one third of the way done. There were no concerns with the data being requested and the template was adopted unanimously for use moving forward.

7. 6:20pm: Surveillance Equipment Ordinance – OPD – Body Worn Camera Anticipated Impact Report and draft Use Policy – review and take possible action

Sgt. Taylor gave a brief presentation on how the Body Worn Cameras are used and was available to answer questions. No action was taken and the item will come back to the PAC in January.

8. 7:00pm: Adjournment

JTTF Annual Compliance Report Template (adopted by PAC 12/06/18)

Staffing

1. Number of full and part time OPD officers assigned to JTTF
2. Number of hours worked as JTTF officer
3. Funding source for OPD JTTF officer salary

Other Resources Provided

1. Communication equipment
2. Surveillance equipment
3. Clerical/administrative staff hours
4. Funding sources for all the above

Cases

1. Number of cases OPD JTTF officer was assigned to
2. Number of "duty to warn" cases
3. General types of cases
4. Number of times FBI asked OPD to perform/OPD declined to perform
    a. Reason for OPD declination (e.g. insufficient resources, local/state law)

Operations

1. Number of Assessments opened
2. Number of Voluntary Interviews opened
3. Number of Assessments closed without becoming preliminary or full investigations
4. Number of Voluntary Interviews closed without becoming preliminary or full investigations
5. Number of times use of undercover officers were approved
6. Number of instances where OPD JTTF officer managed informants
7. Number of cases involving informants that OPD JTTF officer worked on
8. Number of requests from outside agencies (e.g. ICE) for records or data of OPD JTTF activities
    a. Number of such requests that were denied
    b. Reason for denial
9. Whether OPD JTTF officer was involved in any cases where USPER (U.S. person status) information was collected
    a. Number of cases

Training and Compliance

1. Description of training given to OPD JTTF officer by OPD to ensure compliance with Oakland and California law
2. Date of last training update, and last training audit
3. Frequency with which OPD JTTF officer briefs OPD supervisor on cases

Actual and Potential Violations of Local/State Law

1. Number of actual violations
2. Number of potential violations
3. Actions taken to address actual or potential violations
4. Recommendations by OPD to address prevention of future violations

SARs and NCRIC

1. Whether OPD JTTF officer submits SARs to NCRIC; number submitted
2. Whether OPD officer receives SAR information; number received

Command Structure for OPD JTTF Officer

1. Reports to whom at FBI?
2. Reports to whom at OPD?

Oakland Fire Department Surveillance Equipment List

1. **Thermal Imaging Cameras (TICs):** These are used by truck company personnel to check for heat signatures while inspecting for heat in emergency responses. OFD's TIC cameras do not have Gait Analysis Technology capability. They are hand held cameras utilized in a burning structure (smoke and fire environment) by responding crews to locate trapped victims, they do not record.

2. **Forward Looking Infra-Red Camera Systems (FLIRS):** 2 Aircraft Rescue Firefighting apparatus have forward looking infra-red camera systems which are also designed to detect heat signatures. These are cameras mounted on the crash rescue apparatus owned and maintained by the Oakland Airport. The cameras assist OFD personal operating the apparatus during a downed aircraft event to navigate through the smoke. It allows for the apparatus to reach the aircraft without running over passengers evacuating the aircraft. All five of the apparatus at the airport have or will have these cameras in the near future. Rescue 3,5,6 cameras activate when the code 3 lights come on. Rescue 17 and 18 (delivered in December as new apparatus) will have cameras that operate when the vehicle is started.

3. **OFD Communications Van Cameras:** The apparatus does have cameras that can be recorded using a DVR on the vehicle. It is seldom used and it's likely the DVR function has never been used. The video feed does provide situational awareness on an internal monitor to personnel inside the vehicle due to the fact it has limited windows to the outside. Currently this camera is non-operational with no funds identified to repair/replace it.

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). 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 recognition system that can connect the image to that actual license plate characters. The ALPR system then compares the license plate characters against specific databases, and stores the characters along with the date, time, and location of the license plate in a database.

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 approximately 35 pairs of ALPR cameras which are mounted to police patrol vehicles (five are in disrepair). Authorized personnel (as described in the Mitigations Section below) may per policy use ALPR 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 person 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 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.

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);
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

[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.

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

6. Data Types and Sources

ALPR data is composed of photographs of license plates, which can be linked through optical recognition software to identify license plate letter and digit characters. 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 approximately $50,000 with EVO-EMERGENCY VEHICLE OUTFITTERS INC, one of the largest California-based up-fitter of LEA vehicles.

9. Third Party Dependence

Commented [BS1]: This section to be completed

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.

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.

11. 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[2]. The AICP report, "News Stories about Law Enforcement ALPR Successes September 2017 - September, 2018"[3] presents scores of cases from different national LEA

[2] https://www.theiacp.org/projects/automated-license-plate-recognition
[3] https://www.theiacp.org/sites/default/files/ALPR%20Success%20News%20Stories%202018.pdf

jurisdictions where ALPR data helped lead to the capture of violent criminals. A July 2014 study[4] 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.

[4] https://www.rand.org/pubs/research_reports/RR467.html

DEPARTMENTAL GENERAL ORDER

I-12: AUTOMATED LICENSE PLATE READERS

Effective Date: XX Mar 19
Coordinator: Information Technology Unit

The Oakland Police Department (OPD) strives to use technology that promotes accountability and transparency. This policy provides guidance for the capture, storage and use of digital data obtained through the use of ALPR technology while recognizing the established privacy rights of the public.

All data and images gathered by the ALPR are for the official use of this department. Because such data may contain confidential information, it is not open to public review.

A. Description of the Technology

OPD uses Automated License Plate Reader (ALPR) technology to capture and store digital license plate data and images.

A – 1. How ALPR Works

ALPR technology works by automatically scanning license plates on vehicles that are publicly visible. ALPR reads these license plates, compares the license plate characters against specific databases, and stores the characters along with the date, time, and location of the license plate in a database. This process allows for two functions by ALPR:

1. 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.
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 agencies for investigative purposes.

Commented [TB1]: 9.64.010 7 C Data Collection: The information that can be collected by the surveillance technology. Where applicable, list any data sources the technology will rely upon, including "open source" data;

Commented [TB2]: 9.64.010 7 A Purpose: The specific purpose that the surveillance technology is intended to advance.

A – 2. The ALPR System

There are two components to the ALPR system:

1. Automated License Plate Readers: These devices include cameras attached to vehicles, trailers, or poles and a corresponding device that transmits collected data to various state databases for comparison and a central repository for storage and later retrieval.

2. ALPR Database: This central repository stores data collected and transmitted by the Automated License Plate Readers.

B. General Guidelines

B – 1. Authorized Users

Personnel authorized to use ALPR equipment 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. Such personnel shall be limited to designated sergeants, officers, police service technicians, and parking enforcement personnel unless otherwise authorized.

Commented [TB3]: 9.64.010 7 D Data Access: The category of individuals who can access or use the collected information, and the rules and processes required prior to access or use of the information;

B – 2. Restrictions on Use

1. 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. No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.

3. No ALPR operator may access department, state or federal data unless otherwise authorized to do so.

4. While ALPR may be used to canvass license plates around any crime scene, particular consideration should be given to using ALPR-equipped cars to canvass areas around homicides, shootings and other major incidents. Partial license plates reported during major crimes should be entered into the ALPR system in an attempt to identify suspect vehicles.

5. ALPR shall only be used for official law enforcement business.

6. ALPR may be used in conjunction with any routine patrol operation or criminal investigation. Reasonable suspicion or probable cause is not required before using an ALPR to scan license plates or collect data.

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.

8. 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.

C. ALPR Data

C – 1. Data Collection and Retention

1. Transfer of Data

   Data will be transferred from vehicles to the designated storage in

accordance with department procedures.

2. Data Retention

All ALPR data downloaded to the server shall be stored for six months, unless required for:

a. A criminal investigation;
b. An administrative investigation;
c. Research;
d. Civil litigation;
e. Training; and/or
f. Other Departmental need.

C – 2. Data Security

All data will be closely safeguarded and protected 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 law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action.

3. ALPR system audits shall be conducted on a regular basis by the Bureau of Services. The purpose of these audits is to ensure the accuracy of ALPR Information and correct data errors.

C – 3. Releasing or Sharing ALPR Data

ALPR 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 ALPR data that 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 Bureau of Services Deputy Chief/ Deputy

Commented [TB4]: 9.64.010 7 F Data Retention: The time period, if any, for which information collected by the surveillance technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s), the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond that period;

Commented [TB5]: 9.64.010 7 E Data Protection: The safeguards that protect information from unauthorized access, including encryption and access control mechanisms;

9.64.010 7 K Maintenance: The mechanisms and procedures to ensure that the security and integrity of the surveillance technology and collected information will be maintained.

Director or designee and approved before the request is fulfilled.

3. The approved request is retained on file.

Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed as provided in Departmental General Order M-9.1, Public Records Access (Civil Code § 1798.90.55) and per any interagency agreements.

D. ALPR Administration

All installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the Bureau of Services.

D – 1. ALPR Administrator

The Bureau of Services Deputy Chief or Deputy Director shall be the administrator of the ALPR program, and shall be responsible for developing guidelines and procedures to comply with the requirements of Civil Code § 1798.90.5 et seq. The Bureau of Services Deputy Chief is responsible for ensuring systems and processes are in place for the proper collection, accuracy and retention of ALPR data.

D – 2. ALPR Coordinator

The title of the official custodian of the ALPR system is the ALPR Coordinator.

D – 3. Monitoring and Reporting

The Oakland Police Department will monitor its use of ALPR technology 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 ALPR Coordinator shall provide the Chief of Police, Privacy Advisory Commission, and Public Safety Committee with an annual report that contains following for the previous 12-month period:

1. The number of times the ALPR technology was used.
2. A list of agencies other than the Oakland Police Department that were authorized to use the equipment.
3. A list of agencies other than the Oakland Police Department that received information from use of the equipment.
4. Information concerning any violation of this policy.
5. Total costs for maintenance, licensing and training, if any.
6. The results of any internal audits and if any corrective action was taken.

The above information and reporting procedures will assist in evaluating the efficacy of this policy and equipment.

D – 4. Training

Commented [TB6]: 9.64.010 7 H Third Party Data Sharing: If and how other City departments, bureaus, divisions, or non-City entities can access or use the information, including any required justification or legal standard necessary to do so and any obligations imposed on the recipient of the information;

Commented [TB7]: 9.64.010 7 G Public Access: How collected information can be accessed or used by members of the public, including criminal defendants;

Commented [TB8]: 9.64.010 J Auditing and Oversight: The mechanisms to ensure that the Surveillance Use Policy is followed, including internal personnel assigned to ensure compliance with the policy, internal recordkeeping of the use of the technology or access to information collected by the technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the legally enforceable sanctions for violations of the policy;

9.64.010 7 K Maintenance: The mechanisms and procedures to ensure that the security and integrity of the surveillance technology and collected information will be maintained.

The Training Section shall ensure that members receive department-approved training for those authorized to use or access the ALPR system and shall maintain a record of all completed trainings. (Civil Code § 1798.90.51; Civil Code §1798.90.53).

Training requirements for employees authorized in ALPR Users Section include completion of training by the ALPR Coordinator or appropriate subject matter experts as designated by OPD. Such training shall include:

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

Training updates are required annually.

Commented [TB9]: 9.64.010 I Training: The training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology;

By Order of

Anne E. Kirkpatrick
Chief of Police

Date Signed:

CITY OF OAKLAND

MEMORANDUM

TO:	Privacy Advisory Commission	**FROM:**	Anne E. Kirkpatrick
SUBJECT:	Use of Unapproved Surveillance Technology Under Exigent Circumstances	**DATE:**	December 26, 2018

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 December 15, 2018, at 12:15 pm, OPD Officers were dispatched to 1815 13th Avenue to investigate the report of a residential (home invasion) robbery in progress. One of the suspects was reported to be armed with a rifle. OPD Officers arrived and met with one of the victims, who said a suspect had broken into the residence and was armed with a long rifle similar to an AK-47. A suspect exited the residence and was detained. Through further investigation it was discovered additional suspect(s) and victim(s) might be in the residence, creating a potential hostage situation. Although the suspect(s) was inside of the residence, the UAS and helicopters (CHP[1] and EBRPD[2] PD) were still utilized for two reasons; first, to gain an aerial view of the residence/property/area and, second, in anticipation that additional suspects might flee from the residence. The usage also allowed OPD officers to remain a safe distance from the residence and still obtain real time information. This situation was deemed an immediate and serious threat to public and officer safety.

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 the course of several yard searches for the wanted subject.

[1] CHP = California Highway Patrol
[2] EBRPD PD = East Bay Regional Park District Police Department

Deployment Timeline

The below times are for December 15 to 16, 2018.

December 15, 2018

- 12:15 pm: OPD Officers were dispatched to 1815 13th Avenue on the report of home invasion robbery.
- 12:16 pm: OPD Officers arrived on scene
- 12:19 pm: Initial perimeter set to contain suspect(s) inside of residence
- 12:33 pm: First suspect exited residence and was detained
- 12:45 pm: ACSO deployed UAS overhead
- 12:51 pm: CHP helicopter arrived and used Forward Looking InfraRed (FLIR) technology[3] to attempt to locate additional suspect(s). No heat sources were located in the backyard or adjacent backyard.
- 2:08 pm: CHP advised that their helicopter was running low on fuel and they left.
- 3:40 pm: EBRPD PD (helicopter arrived and used FLIR technology to attempt to locate additional suspect(s). They found and then lost heat sources.
- 3:45 pm: SWAT (Special Weapons and Tactics) Team callout initiated to locate additional suspect(s).
- 4:29 pm: ACSO used drones to see through windows and was unable to locate anything.
- 5:00 pm: ACSO sent a drone inside the residence. They were unable to locate anything on the first floor of the two-story residence.
- 7:11 pm: The first suspect (who had been detained) stated there were three additional suspects hiding in the residence.
- 11:08 pm: The second suspect surrendered and exited through a window.

December 16, 2018

- 12:28 am: The residence was searched and no additional suspects located.

The UASs were used during the yard search/aerial building views for approximately eight to nine hours. The UASs were used concurrently with a helicopter[4] because of the layout of the residence/property/land. The UASs flew lower and into blind spots 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.

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

[3] FLIR technology governed by FLIR Privacy and Data Retention Policy (Resolution No. 85807 C.M.S., passed October 6, 2015).
[4] One helicopter was used at a time.

The suspect was apprehended when he surrendered and exited from the residence. The UAS and helicopters FLIR were useful in providing increased officer safety during the search for an individual who had committed a home invasion robbery and was suspected of being armed with a rifle.

COMPLIANT USE

The following information on both technologies is required by OMC 9.64.035 and shows that they were 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