CITY OF OAKLAND

Privacy Advisory Commission

September 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**: Raymundo Jacquez III, **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

2. Open Forum/Public Comment

3. Review and approval of the draft August 1 meeting minutes

4. Port of Oakland presentation – GoPort Program – Freight Intelligent Transportation System (FITS)

5. Surveillance Equipment Ordinance – OPD – StarChase GPS Impact Report and proposed Use Policy – review and take possible action

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

7. Surveillance Equipment Ordinance – OPD – Remote Camera Impact Report and proposed Use Policy – review and take possible action.

8. Adjournment at 7:00pm

CITY OF OAKLAND

Privacy Advisory Commission

August 1, 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**: 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

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

2. Open Forum/Public Comment

There were no Open Forum Speakers.

3. Review and approval of the draft July 8 special meeting minutes

The minutes were approved unanimously.

4. Guest Presentation by UC Davis Law Professor Elizabeth Joh – "Policing the Smart City"

Professor Joh provided an overview of her work and the emerging issue of Smart Cities and their potential impact on Privacy. As cities acquire more sensors to track things such as smart meters, traffic sensors, devices to monitor waste production, they essentially are expanding a city's capacity to surveille people. Also, this surveillance is far less visible as it is in a small sensor as opposed to a police vehicle monitoring an intersection.

As surveillance opportunities expand and become invisible, Cities have a responsibility to establish standards for these uses, including determining who has access to the data, how the data can be used, reused, and kept. This expansion is further complicated as these technologies will be implemented by both the public and private sector (for very different reasons) and with the private sector can have the ability to effect consumers en masse.

The PAC discussed preparing for this by building a framework to address these items now, in anticipation of this expansion. Ideas such as regulating private companies' collection of data, using licensing to regulate the collection, and reviewing data storage subscriptions for law enforcement agencies were all discussed as possible solutions.

This was an informational report and no action was taken.

5. Surveillance Equipment Ordinance – OPD – 2018 Annual Cell Cite Simulator Report

Deputy Chief Roland Holmgren presented the annual report which indicated the cell site simulator was not used during the past year and the report was approved unanimously.

6. Surveillance Equipment Ordinance – OPD – StarChase GPS Impact Report and proposed Use Policy – review and take possible action.

Deputy Chief Roland Holmgren presented this new technology that OPD is considering that allows officers to deploy a small tracking device that sticks to a vehicle when a suspect flees so they can be pursued from a safe distance. These devices have the potential to dramatically reduce the tension and danger involved in pursuits which is a huge concern, especially in densely populated areas where suspects will often travel at excessive speeds and injure innocent bystanders. The device collects no Personally Identifiable Information and is only used in these limited instances of pursuit which narrows the potential civil liberties impact on the general public.

The PAC discussed several issues including: the length of a pursuit (hot versus cold), the cost of deployment, how to measure success (such as a reduction in pursuit related traffic accidents), the system capabilities, and data retention periods. A small ad hoc group committed to meeting with OPD to work on these details and bring the item back in September.

7. Surveillance Equipment Ordinance – OPD – Remote Camera Impact Report and proposed Use Policy – review and take possible action.

The PAC briefly discussed additions to the draft use policy including adding sections that mirror the DAC Allowable Use Section as a guide, adding language regarding plain clothes versus uniformed officers, and a better clarification as to when and why these devices would be used. The item will be brought back in September.

GoPort Freight Intelligent Transportation System Project

JULY 2019

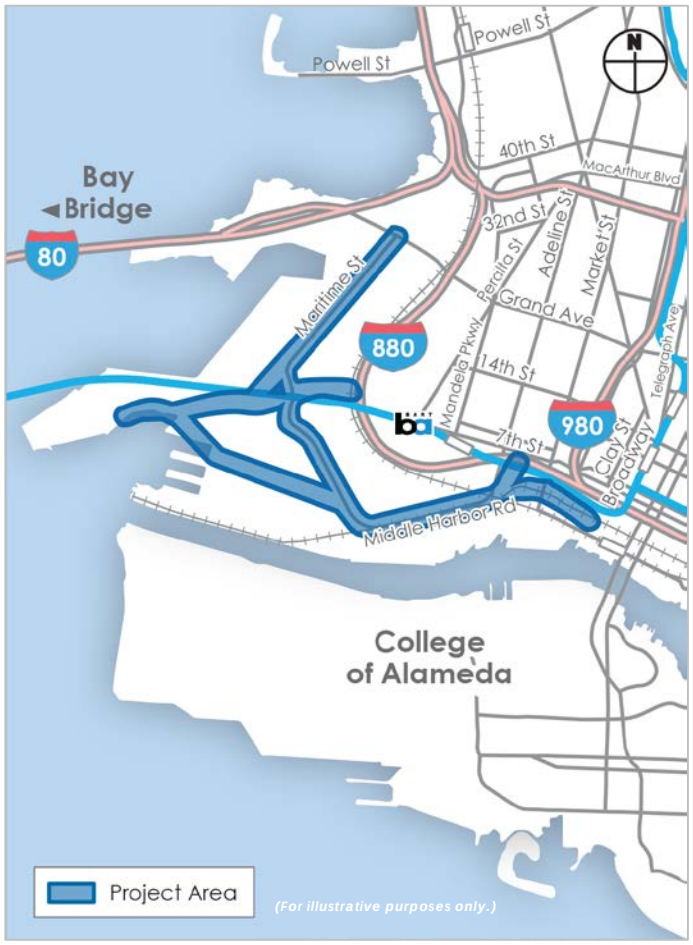
PROJECT OVERVIEW

The Alameda County Transportation Commission (Alameda CTC), in partnership with the City of Oakland and the Port of Oakland (Port), proposes to implement the Global Opportunities at the Port of Oakland (GoPort) Program, a package of landside transportation improvements within and near the Port. The Freight Intelligent Transportation System (FITS) project is a suite of demonstration information technology projects along West Grand Avenue, Maritime Street, 7th Street, Middle Harbor Road, Adeline Street, and Embarcadero West, that are intended to improve truck traffic flows, increase the efficiency of goods movement operations, and enhance the safety and incident response capabilities throughout the seaport.

The purpose of this project is aimed at traffic management and operations of arterial roadways in the Port environment and disseminating traveler information and data to users and stakeholders.

PROJECT NEED

- Support regional economic development and Port growth potential.
- Provide common platform to receive critical information on Port conditions, queue lengths, and incident alerts.
- Develop an ITS communication network that serves future needs
- Reduce truck idling that causes negative impacts to neighboring communities

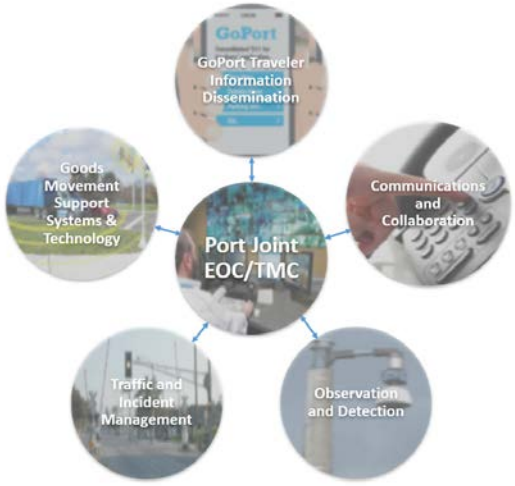


PROJECT BENEFITS

- Improves safety, efficiency and reliability of truck and rail access to the Oakland Port Complex
- Provides real-time traveler information to users
- Improves traffic and incident management within the Port, its terminals and access routes
- Reduces congestion, truck idling and related emissions
- Improves Port competitiveness

Congestion, bottlenecks, and trucks queuing at the Port of Oakland.

GoPort mobile application.



Freight ITS operations overview.

COST ESTIMATE BY PHASE ($ X 1,000)

PE/Environmental	$2,500
Final Design (PS&E)	$4,100
Construction	$24,000
Total Expenditures	**$30,600**

FUNDING SOURCES ($ X 1,000)

Measure BB	$6,600
Federal (ATCMTD)[1]	$9,720
Federal (PSGP)[2]	$1,824
State (SB 1 TCEP)[3]	$12,456
Total Revenues	**$30,600**

[1] Advanced Transportation and Congestion Management Technologies Deployment (ATCMTD).

[2] Port Security Grant Program (PSGP).

[3] Senate Bill 1 Trade Corridor Enhancement Program (TCEP).

STATUS

Implementing Agency: Alameda CTC

Current Phase: Construction

- California Environmental Quality Act (CEQA) clearance through the 2002 Oakland Army Base Environmental Impact Report (EIR) and the 2012 addendum.
- National Environmental Policy Act (NEPA) clearance through a Categorical Exclusion (CE) was completed on August 31, 2018.
- State and federal construction funds fully authorized in June 2019.

PARTNERS AND STAKEHOLDERS

City of Oakland, Port of Oakland, Federal Highway Administration, California Transportation Commission, California Department of Transportation, U.S. Department of Homeland Security and the Metropolitan Transportation Commission

SCHEDULE BY PHASE

	Begin	End
PE/Environmental	Fall 2016	Summer 2018
Final Design	Fall 2018	Early 2019
Right-of-Way	Fall 2018	Early 2019
Construction	Fall 2019	Late 2021

Note: Information on this fact sheet is subject to periodic updates.

OAKLAND POLICE DEPARTMENT

Pursuit Mitigation System Impact Use Report

1. Information Describing the Pursuit Mitigation System and How It Works

The Pursuit Mitigation System provided by StarChase, Inc., comprised of "StarChase GPS[1] System," "StarChase Tag," and "Track System" is together a less-than lethal GPS tracking system. The StarChase system is a pursuit management technology that contains a miniature GPS tag and a launcher mounted in a police vehicle. A compressed-air launcher, mounted behind the grille of a police cruiser, uses a laser to target the fleeing vehicle. It deploys a GPS tag. Dispatch views location and movements of the tagged vehicle in real-time on a secure web-based mapping portal. Through the efficient use of technology, a high-speed chase is replaced with a safer interdiction technology.

The Pursuit Mitigation GPS Tag and Track Launcher System is comprised of a less-than-lethal, dual barrel GPS launcher which contains two GPS Tags (1 per barrel) mounted in the vehicle grille or on a push bumper. The launcher is equipped with compressed air and an eye-safe laser for assisting with targeting prior to launching the GPS Tag.

The system can be deployed both from the inside of the vehicle using the control panel as well as remotely outside the vehicle using a small key fob. Once the GPS Tag is launched, Dispatch, Line Supervisors and other personnel can view the location and movements of the "hot pursuit" vehicle in real-time on a secure, web-based mapping portal. In addition to accurate mapping, critical information including travel direction, speed and traffic activity is transmitted every 5 seconds allowing for visibility of suspect vehicle movements. StarChase integrates with existing CAD and AVL systems and is designed to allow credentialed user access to critical mapping for dispatch, 911 centers or patrol vehicle terminals.

2. Proposed Purpose

The proposed purpose of the Pursuit Mitigation System is to track and ultimately capture a suspect vehicle (and occupant) when a vehicle pursuit event occurs. California Vehicle Code (CVC) 2800 states that it "is unlawful to willfully fail or refuse to comply with a lawful order, signal, or direction of a peace officer." CVC 2800.1 explains it's illegal to flee or attempt to elude a

[1] GPS = global positioning satellite system, used to pinpoint the location of an object on a map

pursuing peace officer. CVC 2800.2 explains that such attempts to elude an officer can be a felony crime when the pursued vehicle is "driven in a willful or wanton disregard for the safety of persons or property."

Oakland Police Department (OPD) Departmental General Order (DGO) J-4 "Pursuit Driving" defines a vehicle pursuit as "an event involving one or more law enforcement officers attempting to apprehend a suspected or actual violator of the law in a motor vehicle while the driver is using evasive tactics, such as high speed driving, driving off a highway or turning suddenly and failing to yield to the officer's signal to stop[2]." OPD policy reflects the understanding that vehicle pursuits are dangerous; therefore OPD J-4 only allows for vehicle pursuits under limited circumstances. J4 II.B. explains that, "Vehicle pursuits may only be initiated when there is reasonable suspicion to believe the suspect committed a violent forcible crime and/or a crime involving the use of a firearm, or probable cause that the suspect is in possession of a firearm." The specific list of "violent forcible crimes" from J-4 include:

- Murder;
- Manslaughter;
- Mayhem
- Kidnapping;
- Robbery;
- Carjacking;
- Arson to an inhabited structure, inhabited property or that causes GBI;
- Explode or ignite a destructive device or any explosive causing GBI or death;
- Use or possession of a weapon of mass destruction;
- Use of a firearm in the commission of a felony;
- Assault with a deadly weapon, firearm;
- Assault with a deadly weapon, other than a firearm (e.g. clearly using a vehicle as a weapon);
- Aggravated Battery with severe or great bodily injury; and
- Sexual Assault

Citizens sometimes become victims to pursuit-related events. High speed vehicle evasions and pursuits can lead accidents and physical injuries and/or death of the fleeing motorist and/or innocent bystanders. There is no way to justify an injury and / or loss of life; however, the costs associated with pursuit-related litigation and settlements is in the millions, and the financial

[2] OPD policy reflects the understanding that vehicle pursuits are dangerous; therefore OPD J-4 only allows for vehicle pursuits under limited circumstances. J4 II.B. explains that,
"Vehicle pursuits may only be initiated when there is reasonable suspicion to believe the suspect committed a violent forcible crime and/or a crime involving the use of a firearm, or probable cause that the suspect is in possession of a firearm."

costs from damaged property, both in the city and for a police department can be extremely expensive.

OPD's Office of the Inspector General (OIG) undertook a review of OPD's pursuit policy[3], which was revised in August 2014, to limit the types of crimes for which officers could pursue a suspect(s) (so as to mitigate the significant risk to OPD and the public). The review found a significant drop in the number of pursuits[4] after the policy change, but little change in the rate of property damage and injuries - about a third of all pursuits result in property damage. The OIG report also finds that the percentage of injuries resulting from a vehicle pursuit have not fluctuated more than 3% from 2013 to 2017 - roughly 10% of all pursuits continue to result in injury. Additionally, the Office of the Oakland City Attorney's Fiscal Year 2017-18 Annual Report shows that the City has paid an average of over $3 million dollars per year over five fiscal years between 2013 and 2018. OPD cannot currently determine the extent these vehicle accident payouts are connected to OPD pursuits. In terms of overall pursuit data, for 2017 there were a total of 65 vehicle pursuits; 105 in 2018; and 54 in 2019 as of August 16, 2019 (date of this Impact Use Report).

Vehicles pursuits that result in vehicular collisions can also erode police-community relationships. StarChase can help OPD accomplish the goal of tracking individuals in vehicles who choose to evade law enforcement - without dangerous vehicle pursuits.

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

The technology would be installed onto various patrol vehicles and would thus be deployed throughout the city. The technology is affixed to patrol vehicles but can be removed and re-affixed to new vehicles as patrol vehicles become decommissioned through extended use.

[3] http://www2.oaklandnet.com/oakca1/groups/police/documents/agenda/oak072028.pdf

[4] The greatest decline in vehicle pursuits was for Level 3 pursuits, "a vehicle pursuit which does not result in injury or property damage, unless a pursuit intervention maneuver technique was utilized."

The following table presents Part 1 Crime Data for January 1-May 31 Year to Date (YTD).

Part 1 Crimes	YTD 2015	YTD 2016	YTD 2017	YTD 2018	YTD 2019	YTD % Change 2018 vs. 2019	5-Year YTD Average	YTD 2019 vs. 5-Year Average
Homicide 187(a)PC	35	19	25	22	31	41%	26	17%
Aggravated Assault	1,150	1,061	1,160	1,188	1,347	13%	1,181	14%
Rape	80	93	96	88	71	-19%	86	-17%
Robbery	1,388	1,180	1,161	1,021	1,053	3%	1,161	-9%
Burglary	5,330	3,979	5,363	3,749	4,616	23%	4,607	0%
Vehicle Theft	3,200	3,359	3,144	2,633	2,551	-3%	2,977	-14%
Larceny	2,618	2,424	2,466	2,622	2,438	-7%	2,514	-3%
Arson	66	53	38	71	48	-32%	55	-13%

4. Impact

Impacts to public privacy would result if the Pursuit Mitigation System was used indiscriminately to monitor vehicles disconnected from actual crime or suspected criminal activity. OPD is only proposing to use the system in the event where an actual motorist chooses to evade lawful attempts to stop the motorist, as defined in #2 “Proposed Purpose” above. Furthermore, the system only captures longitude and latitude data of the GPS tag – no data is captured pertaining to the actual vehicle or motorist.

5. Mitigations

The Pursuit Mitigation System mapping portal uses encryption to prevent unauthorized users from accessing the system. The GPS data from the

StarChase GPS is securely transported to a secure StarChase server environment. The entire platform is FedRAMP[5] ready and access to systems are restricted by secure login and all connections are encrypted using 2048bit SSL encryption. In addition, the system is protected and monitored 24/365 by multiple layers of firewalls and security protocols. The system uses multi-factor authentication, whitelisted IPs and secure firewalls.

6. Data Types and Sources

Data is collected from the GPS tag used in the Pursuit Mitigation System – latitude and longitude data. The data is collected and processed in its pure form without changes. Data processing is only utilized in the retrieval of information from the system's database used to store the raw data collected from the GPS assets. Captured data includes electronic signatures (radio frequencies, cellphone signals, network activity) as well as GPS location (latitude, longitude) data, vehicle speed, and battery life. These data sources are used only for capturing the tag location; cellphone signals are not monitored, and the contents cannot be determined.

7. Data Security

The Pursuit Mitigation System data server environment serves as an encrypted host for all agency tracking data. Designated users have variable levels of direct access to data and event histories which are downloadable and can be stored on a secure server; only a limited number of StarChase employees within IT and Support as well as OPD personnel with system access.

The StarChase data trail provides historical evidence for any pursuit, interdiction event or chain of custody requirement. GPS information is stored in a secure and restricted environment in a secure Amazon Web Services (AWS) cloud platform. StarChase only shares data with the contract police agency (OPD) – there is no sharing with any outside entities.

StarChase uses both automated and human staff authentication. StarChase uses a third-party to conduct a security audit of the system and its data.

8. Costs

StarChase will cost $57,500 in one-time costs for 10 launcher systems ($152,850 for 30 systems), each of which includes the interior console, two remove key fobs, and unlimited projectile GPS tags. This cost also includes 12 months of data mapping and access to secure web-based tag data

[5] The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

connectivity and mapping. OPD hopes to purchase 30 systems initially as a pilot program. The ongoing support cost is approximately $1,000 per system per year. Therfore, OPD expects an estimated cost of $30,000 per year after the initial $152,850 year one cost.

9. Third Party

ODP will be dependent upon StarChase LLC for the equipment and data platform associated with this tracking technology. StarChase as a private company uses a third-party to conduct a security audit of the system and its data.

10. Alternatives Considered

OPD does not currently have any GPS tracking system to use in conjunction with vehicle pursuits. Currently OPD must use officer-driven patrol vehicles to pursue motorists who chose not to stop during legally permissible police stops. The challenges of vehicle pursuits is outlined #2 “Proposed Purpose” above. Helicopter pursuits perform a similar role to vehicle pursuits. In fact, OPD uses helicopters when feasible in conjunction with vehicle pursuits. Helicopter use is integrated into OPD DGO J-4 for this reason – OPD ground units involved in vehicle pursuits must disengage from active pursuits upon notification by the helicopter unit of visual contact with a fleeing vehicle. However, OPD only possesses one functional helicopter. Additionally, the helicopter at times is non-operable. Therefore, OPD views helicopter usage as complimentary to ground vehicle pursuits – helicopters do not offer a realistic alternative to ground vehicle pursuits when the conditions warrant their usage. Therefore, the other “alternative” from acquiring this pursuit mitigation system would be to continue to use vehicles for pursuits according to current practices.

11. Track Record of Other Entities

StarChase is utilized by hundreds of law enforcement agencies. Cities in California include Bakersfield, Benicia, Brentwood, Fremont, Modesto, Tustin, Lafayette, Contra Costa County, Pittsburg, San Pablo, Martinez, Pinole, and Walnut Creek as well as the California Highway Patrol. Cites outside of California include Albuquerque, Austin, Denver, Kansas City, Houston, Orlando, and Spokane. Many agencies have reported that StarChase has allowed for the successful detection and arrest of suspects without dangerous high-speed vehicle pursuits. Examples include:

- California Highway Patrol (CHP) - Pittsburg police tried to stop a motorist in a truck that fled officers at high speed on June 4, 2019. The vehicle occupants did not stop after being asked to stop. Officers were deploy the GPS tag, which allowed a Contra Costa Sheriff’s helicopter and a CHP

Commented [BS1]: We need to know some specifics about changes to collisions from pursuits, successful pursutis. Also any problems. Would help to have contacts to talk to some of these agencies.

airplane to follow from above at a distance; CHP was able to later make an arrest.

- Greene County Sheriff (MO) - August 6, 2019, were able to use StarChase to apprehend a motorist driving the wrong way on a highway and causing two vehicle collisions.
- The Florida Highway Patrol used StarChase successfully on a chase in Pasco County, Florida. Officers were pursuing an aggravated assault suspect after determining that pursuit and other methods to stop the vehicle were too dangerous.
- Springfield, MO – Springfield, MO PD state that the StarChase tags have stuck to vehicles 93 percent of times used, and recovery rate 1s 100 percent when the tag is successfully stuck to a suspect vehicle. They also say that the tracker is less useful during rain and inclement weather.

DEPARTMENTAL GENERAL ORDER

I-22: PURSUIT MITIGATION SYSTEM~~TRACKERS~~

Effective Date: XX XX 19
Coordinator: Bureau of Field Operations

The protection of human life is the primary consideration when deciding to engage in a vehicle pursuit. Vehicle pursuits may be necessary to apprehend dangerous criminals who evade police in an attempt to escape. However, vehicle pursuits are inherently dangerous, and OPD policy balances these interests by stating that pursuits "shall be terminated whenever the totality of circumstances known or which should be known to involved personnel during the pursuit indicate that the risks in continuing the pursuit reasonably appear to outweigh the risks resulting from terminating the pursuit."

Pursuit Mitigation Trackers, using Global Positioning Satellite (GPS) Tracking technology, offer officers a technology alternative to vehicle pursuits. Pursuit Mitigation trackers provide solutions for apprehending individuals who are involved in serious crimes or who purposely evade lawful commands to stop, while mitigating many of the risks inherent to police vehicle pursuits.

A. DESCRIPTION OF THE TECHNOLOGY

A - 1. ~~Pursuit Mitigation Tracker System~~Pursuit Mitigation System and Components

"StarChase", a private company, manufactures and supports its Pursuit Mitigation GPS Tag Tracking System. The "StarChase" system is a pursuit management technology that contains a miniature GPS tag and a launcher mounted in a police vehicle.

The GPS Tag and Track Launcher System are comprised of a less-than-lethal, dual barrel GPS launcher which contains two GPS Tags (1 per barrel) mounted in the vehicle grille or on a push bumper. The launcher is equipped with compressed air and an eye-safe laser for assisting with targeting before launching the GPS Tag.

A - 2. How the GPS Tag Works

The StarChase system allows an officer to remotely affix a GPS tag to a pursued (or about to be pursued) vehicle using an air pressure system to discharge the tag from the front of the StarChase equipped patrol car to the vehicle in front of it. Once the tracker is affixed, its location can be monitored by personnel using a computer with an internet connection (the battery of each tag lasts approximately eight hours).

The system can be deployed both from the inside of the vehicle using the control panel as well as remotely outside the vehicle using a small key fob. Once the GPS tag is launched, dispatch personnel, field supervisors, and other personnel can view the location and movements of the tagged vehicle in real-time on a secure, web-based mapping portal. In addition to accurate mapping, critical information including travel direction, speed, and traffic activity is

Commented [BS1]: Deleted "tracker" but maybe we leave in "tag?"

transmitted every 3-5 seconds allowing for visibility of suspect vehicle movements in near real- time.

B. GENERAL GUIDELINES

B - 1. Communications

For clarity of communications, radio traffic should identify the device as "StarChase".

B - 2. Authorized Users

StarChase equipment in the patrol vehicle will only be operated by officers who have been trained in its use. StarChase equipped vehicles will not be assigned to officers who are not trained on its use unless required by exigent circumstances.

B - 3. Authorized Uses

The StarChase system may be utilized during the following situations:

1. To tag a vehicle which officers are pursuing as part of an authorized vehicle pursuit under DGO J-4;
2. If there is reasonable suspicion to believe the suspect committed a violent forcible crime and/or a crime involving the use of a firearm, or probable cause that the suspect is in possession of a firearm (pursuant OPD DGO J4 "Pursuit Driving" Section II "Engaging in a Vehicle Pursuit");
3. If there is reasonable suspicion to believe the suspect in the vehicle committed any Part 1 felony[1];
4. If the vehicle is operated by an individual believed to be driving under intoxication (DUI) pursuant to CVC **23152(a);** or
5. A monitoring commander may authorize the deployment under exigent circumstances other than what is authorized in 1-4 above.

B - 4. Safety Considerations

The StarChase operator shall evaluate all safety decisions related to the discharge of a StarChase tag before deployment. While supervisors may direct or approve the deployment of a StarChase equipped patrol car in pursuit and the discharge of a tag, safety decisions related to passing other involved vehicles and the actual deployment of the device will be evaluated by the operator before deployment. The safety of uninvolved persons, persons inside the pursued vehicle, and pursuing officers shall be considered. The following considerations are specifically included:

[1] As defined by the FBI's Uniform Crime Reporting (UCR) Program; The seven Part I offense classifications included the violent crimes of murder and nonnegligent manslaughter, rape (legacy & revised), robbery, and aggravated assault, and the property crimes of burglary, larceny-theft, and motor vehicle theft. By congressional mandate, arson was added as the eighth Part I offense category in 1979.

Formatted: Indent: Left: 0", First line: 0"

1. Whether the officer can safely maneuver close enough to the suspect vehicle to come within targeting range;
2. Whether the officer can safely pass other vehicles to get to the subject vehicle; and
3. Whether any circumstances would indicate the device would not work (e.g., weather conditions, suspect vehicle weaving, et cetera).

B - 5. Deploying the StarChase During an Active Pursuit

StarChase equipped patrol cars, with approval of a supervisor, are authorized to respond to authorized vehicle pursuits in progress for potential use of the device. When so doing, officers driving these cars shall obey the following directives:

1. Unless directed otherwise, the StarChase equipped vehicle will join the pursuit at the rear of authorized pursuing vehicles until cleared to pass;
2. Once a StarChase equipped vehicle joins a pursuit, it becomes an authorized unit as it relates to the number of authorized pursuing vehicles;
3. StarChase equipped vehicles may pass other pursuing vehicles only when deemed safe and only with specific permission from the unit to be passed. Permission is to be sought and acknowledged one vehicle at a time. Officers driving the StarChase equipped vehicle will identify which side of the overtaken vehicle they will pass;
4. StarChase tags will be deployed in accordance with training;
5. Once the StarChase tag has been successfully deployed, pursuing vehicles shall disengage from the pursuit of the vehicle by deactivating the emergency lights and siren and obeying all speed and traffic laws. After disengaging from the pursuit, members may trail the fleeing vehicle by responding to the direction of the StarChase monitor, with the intent of not being seen by the suspect and to facilitate the arrest or detention of the driver and/or occupants of the vehicle;
6. One member shall be designated as the StarChase Monitor, who will relay speed, direction, and location updates on the suspect vehicle via the radio. While ideally dispatch personnel, this can be any member with access to the StarChase system;
7. Officers will maintain constant communication with the StarChase Monitor for speed/direction/location updates of the suspect vehicle.
8. The Supervisor will coordinate with the StarChase Monitor to direct resources and officers to appropriate locations to apprehend the suspect.
9. No officer who is driving a moving patrol car will access the StarChase Monitor data as this creates an unnecessary hazard.

10. Vehicles equipped with StarChase should not be used to perform a Pursuit Intervention Technique (PIT).

B - 6. Deploying the StarChase Prior to or to Mitigate a Possible Pursuit

Officers may deploy the StarChase on a vehicle, when authorized under section B-3, before attempting to stop the vehicle. If the tag is properly affixed and transmitting, officers **shall not** pursue the car, but instead follow the steps outlined in B-5, 5-10, in order to safely detain the vehicle and its occupants.

Absent authorization to pursue a vehicle pursuant to DGO J-04, officers **shall not** engage in vehicle pursuits simply to get close enough to affix the StarChase GPS tag.

B - 7. Restricted Uses

The StarChase tag will not be deployed in the following situations unless the suspect poses a substantial risk to the public:

1. Situations that do not comply with Section B-3, **Authorized Uses,** above;
2. During heavy rain;
3. While driving on exceptionally rough terrain;
4. When the subject is on a motorcycle, trike, quad, saddled off-road vehicle, bicycle, or is a pedestrian; or
5. When pedestrians are between or very near the suspect vehicle and the StarChase equipped vehicle.

B - 8. Reporting Requirements

In addition to the normal pursuit reporting procedures, officers who use the StarChase system will report all tag deployments in the appropriate report.

C. DATA MANAGEMENT

C - 1. Data Collection and Retention

The StarChase system collects latitude, longitude, and – by inference over time – speed data of the GPS tag. StarChase does not collect any data related to the vehicle onto which the tag is affixed. StarChase will maintain OPD-specific data for two years; OPD will maintain in perpetuity GPS tag tracker data related to actual criminal investigations.

C - 2. Data Access

OPD personnel with a right and need to know will have access to log into the StarChase portal. OPD Internal Affairs will have access to system data to review compliance with policy in Internal Affairs investigations. The StarChase System Coordinator will be responsible for assigning specific login user and password credentials to those personnel with a need to access

Commented [BS2]: Pre-tagging covered here

Commented [JT3]: Here's my stab at the "no catching up" thing. Can be cut and left out.

Commented [JT4]: Lol but seriously. People will at least think about tagging people fleeing on bicycles. Tried to cover sideshow-type vehicles as well (quads, dirt bikes, etc.) while not exempting off-road vehicles like Jeeps.

At the same time, I'm totally down for us tagging a ped in an exigency (think North Hollywood Bank Robbers).

Commented [BS5R4]: We agree to these restrictions?

Commented [JT6]: What's this mean? I foresee a question on this one such as, does that mean if you tag my car thinking it's a 211 vehicle and it's the wrong one, you keep the track of me going to the house of worship / pawn shop / other secret place indefinitely?

Maybe for felony arrests? All arrests / cites?

Commented [BS7R6]: Seems like if it's an investigation OPD has to keep the data

StarChase data.

C - 3. Data Security

The StarChase data server environment serves as an encrypted host for all agency tracking data. Designated users have variable levels of direct access to data and event histories which are downloadable and can be stored on a secure server; only a limited number of StarChase employees within IT and Support as well as OPD personnel have system access.

The StarChase data trail provides historical evidence for any pursuit, interdiction event, or chain of custody requirement. The GPS information is stored in a secure and restricted environment in a secure cloud platform. StarChase only shares data with the contract police agency (OPD) and does not share OPD's data with any outside entities.

StarChase uses both automated and human staff authentication. StarChase uses an independent third-party company to conduct a security audit of the system and its data.

C - 4. Data Protection

StarChase will maintain all data on cloud servers with standard encryption technology. StarChase will only have access to the latitude and longitude (and associated vehicle speed) of GPS tag trackers. Only OPD will have data to connect tracked tags to vehicles and criminal cases. Additionally, all used tags shall be retained as evidence by OPD's system coordinator and Evidence Unit. Additionally, officers shall either photograph with a camera or their body-worn camera (BWC) the damage or lack of damage to the vehicle when recovering the tag.

Formatted: List Paragraph, Space After: 0 pt

C - 5. Releasing or Sharing StarChase System Data

StarChase does not share data with any outside agencies or companies.

OPD will consider sharing StarChase latitude and longitude data with other law enforcement or prosecutorial agencies for 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 written request for GPS tag tracker 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 Chief of Police or designee and approved before the request is fulfilled.

3. The approved request is retained on file.

D. PURSUIT MITIGATION SYSTEM ADMINISTRATION

D - 1. System Coordinator / Administrator

The StarChase system coordinator will be responsible for collaborating with the Training Division to ensure that personnel with access to the system are properly trained. The system coordinator is responsible for ensuring that appropriate personnel have individual login and password credentials. The system coordinator is also responsible for annual system audits.

D - 2. Training

The Training Division shall ensure that members receive department-approved training for those authorized to use or access the StarChase System and shall maintain a record of all completed training.

Training requirements for employees authorized to use the StarChase System include completion of training by the System Coordinator or appropriate subject matter experts as designated by OPD. Such training shall include:

1. System design and functionality
2. Situations that affect system functionality
3. Applicable federal and state law
4. Applicable policy
5. Accessing data
6. Safeguarding password information and data
7. Sharing of data
8. Reporting breaches
9. Implementing post-breach procedures

Training updates are required annually.

D - 3. Auditing and Oversight

The System Coordinator will be responsible for coordinating audits every year to assess system use. A summary of user accesaccess 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: _____

FOR OFFICIAL USE ONLY

JOINT TERRORISM TASK FORCE

STANDARD MEMORANDUM OF UNDERSTANDING

BETWEEN

THE FEDERAL BUREAU OF INVESTIGATIONI

AND

THE OAKLAND POLICE DEPARTMENT

PREAMBLE

The policy of the United States with regard to domestic and international terrorism is to deter, defeat and respond vigorously to all terrorist attacks on out territory and against our citizens, or facilities. Within the United States, the Department of Justice, acting through the Federal Bureau of Investigation (FBI), is the lead agency domestically for the counterterrorism effort.

In order to ensure that there is a robust capability to deter, defeat and respond vigorously to terrorism in the U.S. interest, the FBI recognizes the need for all federal, state, local and tribal agencies that are involved in fighting terrorism to coordinate and share information and resources. To that end, the FBI believes that the creation of the FBI National Joint Terrorism Task Force (NJTTF) and Joint Terrorism Task Forces (JTTFs) embodies the objectives of the U.S. policy on counterterrorism as set forth in Presidential Directives.

FBI policy for the NJTTF and JTTFs is to provide a vehicle to facilitate sharing FBI information with the intelligence and law enforcement communities to protect the United States against threats to our national security, including international terrorism, and thereby improve the effectiveness of law enforcement, consistent with the protection of classified or otherwise sensitive intelligence and law enforcement information, including sources and methods. All NJTTF and JTTF operational and investigative activity, including the collection, retention and dissemination of personal information, will be conducted in a manner that protects and preserves the constitutional rights and civil liberties of all persons in the United States.

This Memorandum of Understanding (MOU) shall serve to establish the parameters for the detail of employees (Detailees or members) from the Participating Agency to the FBI-led JTTF's in selected locations around the United States.

I. PURPOSE

A. The purpose of this MOU is to outline the mission of the JTTF, and to formalize the relationship between the FBI and the Participating Agency; in order to maximize cooperation and to create a cohesive unit cable of addressing the most complex terrorism investigations.

B. The MOU specifically represents the agreement between the FBI and the Participating Agency, which will govern the process by which employees of the Participating Agency are detailed to work with the FBI as part of the JTTF.

C. The MOU is not intended, and should not be construed, to create any right or benefit, substantive or procedural, enforceable at law of otherwise by any third party against the parties, their parent agencies, the U.S., or the officers employees, agents or other associated personnel thereof.

II. MISSION

The mission of the JTTF is to leverage the collective resources of the member agencies for the prevention, preemption, deterrence and investigation of terrorist acts that affect United States interests and to disrupt and prevent terrorist acts and apprehend individuals who may commit or plain to commit such acts. To further this mission, the JTTF shall serve as a means to facilitate information sharing amount JTTF members.

III. AUTHORITY

Pursuant to 28U.S.C. §533, 28 C.F.R. §0.85. Executive Order 12333, Presidential Decision Directive (PDD) 39, PDD 62 and pending approval of National Security Presidential Decision Directive (NSPD) 46 and Homeland Security Presidential Directive (HSPD) 15, the FBI is authorized to coordinate an intelligence, investigative and operational response to terrorism. By virtue of that same authority, the FBI formed the JTTFs composed of other federal, state, local and tribal law enforcement agencies acting in support of the above listed statutory and regulatory provisions.

[Participating agencies may include applicable authority for entering into this MOU.]

IV. CONTROLLING DOCUMENTS

A. Since the JTTF operates under the authority of the Attorney General of the United States, all JTTF participants must adhere to applicable Attorney General's Guidelines and directives, to include the following; as amended or supplemented;

1. Attorney General's Guidelines on General Crimes, Racketeering enterprise and Terrorism Enterprise Investigations;

2. Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection;

3. Attorney General's Guidelines on Federal Bureau of Investigation Undercover Operations;

4. Attorney General's Guidelines Regarding Prompt Handling of Reports of Possible Criminal Activity Involving Foreign Intelligence Sources;

5. Attorney General's Memorandum dated march 6, 2002, titled "Intelligence Sharing Procedures for Foreign Intelligence and Foreign Counterintelligence Investigations Conducted by the FBI;

6. Attorney General's Guidelines Regarding the Use of Confidential Informants;

7. Attorney General's Guidelines on the Development and Operation of FBI Criminal Formants and Cooperative Witnesses in Extraterritorial Jurisdictions;

8. Attorney General's Guidelines Regarding Disclosure to the Director of Central Intelligence and Homeland Security Officials of Foreign Intelligence Acquired in the Court of a Criminal Investigation; and

9. Memorandum of the Deputy attorney General and the FBI Director re: Field Guidance on Intelligence Sharing Procedures for [Foreign Intelligence] and [Foreign Counterintelligence] Investigations (December 24, 2002).

B. All guidance on investigative matters handled by the JTTF will be issued by the Attorney General and the FBI. The FBI will provide copies of the above-listed guidelines and any other applicable policies for referenced and review to all JTTF members. Notwithstanding the above, this MOU does not alter or abrogate existing directives or policies regarding the conduct of investigations or the use of special investigative techniques or controlled informants. The FBI agrees to conduct periodic briefings of the member agencies of the JTTF subsequent to execution of this agreement.

V. STRUCTURE AND MANAGEMENT OF THE TASK FORCE

A. MEMBERS

1. Each JTTF shall consist of a combined body of sworn and non-sworn personnel from the FBI and each Participating Agency. This MOU shall apply to Participating Agencies that join the JTTF subsequent to execution of this agreement.

B. PROGRAM MANAGEMENT, DIRECTION AND SUPERVISION

1. In order to comply with Presidential Directives, the policy and program management of the JTTFs is the responsibility of FBI Headquarters (FBIHQ). The overall commander of each individual JTTF will be the Special Agent in Charge (SAC) or Assistant Director in Charge (ADIC), if assigned, of the FBI's local Field Division The operational chain of command beginning at the highest level, in each FBI Field Division will be as follows" ADIC if assigned, SAC, Assistant Special Agent in Charge (ASAC), and Supervisory Special Agent [JTTF Supervisor].

2. Each FBI ADIC/SAC, through his or her chain-of-command, is responsible for administrative and operational matters directly associated with the Division's JTTF(s). Operational activities will be supervised by FBI JTTF Supervisors. Staffing issues are the responsibility of the FBI chain of command.

3. All investigations opened and conducted by the JTTF must be conducted in conformance with FBI policy, to include the above stated Controlling Documents. Each FBI ADIC/SAC, through his or her chain-of-command, will ensure that all investigations are properly documented on FBI form in accordance with FBI rules and regulations. Any operational problems will be resolved at the field office level. Any problems not resolved at the field office level will be submitted to each agency's headquarters for resolution.

4. Each Participating Agency representative will report to his or her respective agency for personnel administrative matters. Each Participating Agency shall be responsible for the pay, overtime, leave, performance appraisals, and other personnel matters relating to its employees detailed to JTTFs. As discussed later herein a Paragraph XI, the FBI and Participating Agency may provide for overtime reimbursement by the FBI by separate written agreement.

5. Each JTTF member will be subject to the personnel rules, regulations, laws and policies applicable to employees of his or her respective agency and also will adhere to the FBI's ethical standards and will be subject to the Supplemental Standards of Ethical Conduct for employees of the Department of justice. Where there is a conflict between the standards or requirements of the greatest organizational protection of benefit will apply, unless the organizations jointly resolve the conflict otherwise.

6. JTTF members are subject to removal from the JTTF by the FBI for violation of any provision of this MOU, the FBI's ethical standards, the Supplemental Standards of Ethical Conduct for employees of the Department of Justice, or other applicable agreements, rules and regulations.

7. The FBI maintains oversight and review responsibility of the JTTFs. In the event of any FBI inquiry into JTTF activities by an investigative or administrative body, including but not limited to, the FBI's Office of Professional Responsibility or the FBI's Inspection Division, each Participating Agency representative to the JTTF, may be subject to interview by the FBI.

C. PHYSICAL LOCATION AND SUPPORT

1. The FBI will provide office space for all JTTF members and support staff. In addition, the FBI will provide all necessary secretarial, clerical, automation and technical support for the JTTF in accordance with FBI guidelines and procedures. The FBI will provide all furniture and office equipment. Participating agencies may bring office equipment furniture into FBI space with the approval of the FBI JTTF Supervisor and in compliance with FBI regulations.

2. The introduction of office equipment and furniture into FBI space by participating agencies is discouraged, as any such material is subject to examination for technical compromise, which may result in its being damaged or destroyed

VI. SECURITY PROGRAM

A. CLEARANCES

1. State, local and tribal members of the JTTFs, as well as appropriate supervisory personnel responsible for these individuals, must apply for and receive a Top Secret/Sensitive Compartmental Information (TS/SCI) Security Clearance granted by the FBI. JTTF members from other federal agencies must obtain a Top Secret/SCI clearance from their agency and have this information passed to the FBI. No one will have access to sensitive or classified documents or material or FBI space without a valid security clearance and the necessary "need-to-know." Pursuant to the provision of Section 1.2 of the Executive Order 12968, Detailees are required to have signed a non-disclosure agreement approved by the FBI's Security Division. Pursuant to federal law, JTTF members are strictly for bidden from disclosing any classified information to individuals who do not possess the appropriate security clearance and the need to know.

2. All JTTF management personnel must ensure that each participating JTTF officer or agent undertakes all necessary steps to obtain a TS/SCI clearance. Conversion of FBI counterterrorism and JTTF spaces to Sensitive Compartmented Information Facilities (SCIFs) is underway. This will require that all JTTF task force officers enhance their clearances to TS/SCI (SI,TK, Gamma, HCS-P).

3. Federal agency task force officers should contact their Security Officers and request and obtain the following SCI Clearances; SI, TK, Gamma and HCS-P. If the parent agency refuses or is unable to provide the appropriate clearances, the FBI will request the task force officer's security file. If provided, the FBI will adjudicate the SCI clearances. This action may not involve a prohibitively long process and should be avoided.

4. Each Participating Agency fully understands that its personnel detailed to the JTTF' are not permitted to discuss official JTTF business with supervisors who are not members of the JTTF unless the supervisor possesses the appropriate security

clearance and the dissemination or discussion is specifically approved the FBI JTTF Supervisor. Participating Agency heads will be briefed regarding JTTF matters by the SAC or ADIC, as appropriate through established JTTF executive Board meeting.

5. In accordance with the Director of Central Intelligence Directive (DCID) 6/4, entitled Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information (SCI), the FBI will implement protocols to ensure Special Agent (SA) and Task Force Officers (TFO) assigned to Joint Terrorism task Forces (JTTF) in the field and the National Joint Terrorism Task Force (NJTTF) at FBI Headquarters – Liberty Crossing 1, are in compliance with stated directive. In order to comply with DCID 6/4, all JTTF personnel, including FBI and non FBI JTTF members and contractors who perform functions requiring access to FBI classified data networks and space, will be given counter-intelligence focused on polygraphs. The FBI will recognize polygraph examination meets the PSPP requirements.

6. All JTTF members must agree to submit to counter-intelligence focused polygraphs as part of the process for obtaining and retaining a Top Secret Security Clearance.

B. RESTRICTIONS ON ELECTRONIC EQUIPTMENT

Personally owned Portable Electronic Devices (PEDs) including, but not limited to, personal digital assistance, Blackberry devices, cellular telephones and two-way pagers are prohibited in FBI space unless properly approved. No personally owned electronic devices are permitted to operate within SCIF's as outlined in DCI Directive 6/9 and existing Bureau policy. All other non-FBI owned information technology and systems (such as computers, printers, fax machines, copers, PEDs, cameras and medical including diskettes, CDs, tapes) require FBI approval prior to introduction, operation, connection or removal from FBI spaces to include SCIFs' Additionally, if approved by the FBI Security Officer, these systems must operate in compliance with the FBI's policies, guidelines and procedures.

VII. DEPUTATION

Non-federal members of the JTTF who are subject to a background inquiry and are sworn law enforcement officers will be federally deputized while detailed to the JTTF. The FBI will secure the required authorization for the deputation. Deputation of these individuals will ensure that they are able to assist fully in investigations in compliance with applicable federal statutes. On occasion, investigations may be conducted outside

of the JTTF's assigned territory. Deputation will allow non-federal members of the JTTF to exercise federal law enforcement authority throughout the United States.

Under the terms of this MOU, all Participating Agencies agree that non-sworn detailed to the JTTF will not: (1) participate in law enforcement activities, (2) carry a weapon or (3) participate in the execution of search/arrest warrants.

VII. STAFFING COMMITMENT

A. In view of the need for security clearances and continuity of investigations, all personnel detained to the JTTF should be expected to be detained for the period of at least two (2) years. This MOU imposes no maximum limit as to the time that any individual may remain a member of the JTTF. All non-FBI members of the JTTF must adhere to the same rules and regulations as FBI employees with regard to conduct and activities while in FBI space, while operating FBI vehicles, and while conducting JTTF business. All Task Force members detained from other federal agencies are responsible for maintaining an appropriate case load, as directed by JTTF management.

B. All investigators detailed to the JTTF will be designed either full-time or part-time. The operational needs of the JTTF require that any assignments to special details, or duties outside of the JTTF to full time JTTF members be coordinated with the FBI JTTF Supervisor. Though each JTTF member will report to his or her respective Participating Agency for personnel matters, he or she will coordinate leave with the JTTF's FBI JTTF Supervisor.

C. During periods of heightened threats and emergencies, the JTTFs may be expected to operate 24 hours a day, seven days per week, for extended periods of time. To function properly, the JTTF depends upon the unique contributions of each Participating Agency. Accordingly, during these periods, each Participating Agency member will be expected to be available to support JTTF activities

IX. RECORDS, REPORTS AND INFORMATION SHARING

A. All JTTF materials and investigative records, including any Memorandum of Understanding, originate with, belong to, and will be maintained by the FBI. All investigative reports will be prepared by JTTF personnel solely by the FBI and may not be removed from FBI space with the approval of the JTTF Supervisor. Dissemination, access or other use of JTTF records will be in accordance with Federal law, Executive Orders, and Department of Justice and FBI regulations and policy, including the dissemination and information sharing provisions of the FBI Intelligence Policy Manual. As FBI records, they may be disclosed only with FBI permission and only in conformance with the provisions of federal laws and regulations, including the Freedom of Information Act, 5 U.S.C. Section 552, and the Privacy Action of 1974, 5 U.S.C. Section 552a, as well as applicable civil and

criminal discovery privileges. This policy includes any disclosure of FBI information, including JTTF materials and investigative records, to employees and officials of a Participating Agency who are not members of a JTTF which must be approved by the JTTF supervisor. All electronic records and information, including, but not limited to, systems, databases and media, are also regulated by FBI policy. JTTF members may request approval to disseminate FBI information from the JTTF Supervisor.

B. Each Participating Agency agrees to have its Detailees to the JTTF execute an FD-868, or a similar form approved by the FBI. This action obligates the Detailee, who is accepting a position of special trust in being granted access to classified and otherwise sensitive information as part of the JTTF, to be bound by prepublication review to protect against the unauthorized disclosure of such information,

C. The participation of other federal, state, local and tribal partners on the JTTF us critical to the long term success of the endeavor. Articulating the level of effort for these partnership is a key measure of the JTTF's performance. According, all task force members will be required to record their workload in the Time Utilization Recordkeeping (TURK) system used by the FBI.

X. COORDINATION

A. The Participating Agency agrees to not knowingly act unilaterally on any matter affecting the JTTF without first coordinating with the FBI. The parties agree that matters designated to be handled by the JTTF shall not knowingly be subject to non-JTTF or non-FBI intelligence, law enforcement and operation actions will be coordinated and cooperatively carried out within the JTTFs.

B. JTTF criminal investigative procedures will conform to the requirements for federal prosecution. It is expected that the appropriate United States Attorney in consultation with the FBI and affected JTTF partners, will determine on a case-by-case basis whether the prosecution of cases will be at the federal or state level, based upon which would better advance the interests of justice.

XI. FUNDING

This MOU is not an obligation or commitment of funds, not a basis for transfer of funds. Even where one party has agreed (or later does agree) to assume a particular financial responsibility, written agreement must be obtained before incurring an expense expected to be assumed by another party. All obligations of an expenditures by the parties are subject to their respective budgetary and fiscal processes and availability of funds pursuant to all laws, regulations and policies applicable thereto. The parties acknowledge that there is no intimation, promise or guarantee that funds will be available in future years. The FBI and

the Participating Agency may enter into a separate agreement to reimburse the Participating Agency' for approved overtime expenses.

XII. TRAVEL

All JTTF-related travel of non-FBI personnel requires the approval of the appropriate JTTF Supervisor and Participating Agency authorization prior to travel. In order to avoid delay in operation travel, the Participating Agency will provide general travel authority to all of its participating employees for the duration of the employee's membership in the JTTFs. For domestic travel, each agency member will be responsible for appropriate notifications within his or her own agency, as well as standard FBI travel approvals and notification. The FBI will obtain FBIHQ authorization and country clearances for all JTTF members who are required to travel outside the United States. As noted above, the appropriate security clearance must be obtained prior to any international travel. The FBI will pay costs for travel of all members of the JTTFs to conduct investigations outside of the JTTF's assigned territory.

XIII. VEHICLES AND EQUIPMENT

A. In furtherance of this MOU, employees of the Participating Agency may be permitted to drive FBI owned or leased vehicles for surveillance, case management and investigation in connection with any JTTF investigation. FBI vehicles must only be used for official JTTF business and only in accordance with applicable FBI rules and regulations.

B. *[non-Federal entities only]* Any civil liability arising from the use of any FBI owned or leased vehicle by a Participating Agency task force member while engaged in any conduct other than his or her official duties and assignments under this MOU shall be the responsibility of the Participating Agency. The Participating Agency will indemnity and hold harmless the FBI and the United State for any claim for property damage or personal injury arising from any use of any FBI owned or leased vehicle by a Participating Agency JTTF member which is outside of the scope of his or her official duties and assignments under this MOU.

C. For official inventory purpose, all JTTF equipment including badges, credentials and other form of JTTF identification subject to FBI property inventory requirements will be produced by each JTTF member upon request. At the completion of the member's assignment on the JTTF, or upon withdrawal or termination of the Participating Agency from the JTTF, all equipment will be returned to the supplying agency.

XIV. FORFEITURE

The FBI shall be responsible for the processing of assets seized for federal forfeiture in conjunction with JTTF operations, as provided by these rules and regulations. Asset

forfeitures will be conducted in accordance with federal law and the rules and regulations set forth by the U.S. Department of Justice and the FBI. Forfeitures attributable to JTTF investigations may be distributed among the Participating Agency in JTTF-related operations at the discretion of the FBI.

XV. HUMAN SOURCES

A. All human sources developed through the JTTF will be handled in accordance with the Attorney General and the FBI's Guidelines, policies and procedures.

B. All human sources developed through the JTTF investigation shall be operated with all appropriate FBI suitability paperwork completed prior to use. All source debriefings or written products of information obtained from any human source will use FBI document format and handling procedures.

C. The FBI, as permitted by federal law, agrees to pay reasonable and necessary human source expenses incurred by the JTTF. All expenses must be approved by the FBI before they are incurred. No payments may be made to JTTF human sources without prior FBI approval.

XVI. MEDICAL

A. All Participating Agencies will ensure that detailed JTTF members are medically qualified according to their agencies' standards to perform law enforcement duties, functions and responsibilities.

B. To ensure protection for purposes of the Federal Employees' Compensation Act (FECA), JTTF members should be detailed to the FBI consistent with the provisions of the Intergovernmental Personnel Act (IPA), 5 U.S.C. § 337(d). This Act stipulates that "[a] State of local government employee who is given an appointment in a Federal agency for the period of the assignment or who is on detail to a Federal agency and who suffers disability or dies as a result of a personal injury sustained while in the performance of his duty during the assignment shall be treated . . . as though he were an employee as defined by section 8101 of this title who has sustained the injury in the performance of duty." Other provisions of federal law may extend FECA benefits in more limited circumstances. The Department of Labor's Office of Workers' Compensation Program is charged with making FECA coverage determinations and is available to provide guidance concerning specific circumstances.

XVII. TRAINING

All JTTF members are required to attend FBI legal training in compliance with FBI regulations and any other training deemed necessary by the FBI chain of command. The FBI is responsible for the costs of such training. The Participating Agency will bear

the costs of any training required of its own employees detailed to the JTTF.

XVIII. DEADLY FORCE AND SHOOTING INCIDENT POLICIES

Members of the JTTF will follow their own agency's policy concerning use of deadly force.

XIX. DEPARTMENT OF DEFENSE COMPONENTS

The Posse Comitatus Act, 18 U.S.C. § 1385, prohibits the Army and Air Force (Department of Defense regulations now restrict the activities of all branches or components of the Armed Services under this Act) from being used as a posse comitatus or otherwise to execute the laws entrusted to civilian law enforcement authorities. The restrictions of the Act do not apply to civilian employees of the Department of Defense who are not acting under the direct command and control of a military officer. Other statutory provisions specifically authorize certain indirect and direct assistance and participation by the military in specified law enforcement functions and activities. All Department of Defense components (except strictly civilian components not acting under direct command and control of a military officer) who enter into this agreement, shall comply with all Department of Defense regulations and statutory authorities (describing restrictions, authorizations and conditions in support of law enforcement) including but not limited to Department of Defense Directives 5525.5, and 3025.15, Chapter 18 of Title 10 of the United States Code dealing with military support for civilian law enforcement agencies and any other or subsequent rules, regulations and laws that any address this topic or that may amend, or modify any of the above provisions. This MOU shall not be construed to authorize any additional or greater authority (than already described) for Department of defense components to act in support of law enforcement activities.

XX. MEDIA

All media releases will be mutually agreed upon and jointly handled by the member Participating Agencies of the appropriate JTTF. Press releases will confirm to DOJ Guidelines regarding press releases. No press release will be issued without prior FBI approval.

XXI. LIABILITY

The Participating Agency acknowledges that financial and civil liability, if any and in accordance with applicable law, for the acts and omissions of each employee detailed to the JTTF remains vested with his or her employing agency. However, the Department of Justice (DOJ) may, in its discretion determine on a case-by-case basis that an individual should be afforded legal representation, legal defense or indemnification of a civil judgment, pursuant to federal law and DOJ policy and regulations.

A. COMMON LAW TORT CLAIMS

1. Congress has provided that the exclusive remedy for the negligent or wrongful act or omission of any employee of the U.S Government, acting within the scope of his or her employment, shall be an action against the United States under FTCA, 28 U.S.C. § 1346(b) and §§ 2671 – 2680.

2. Nothwithstanding the provisions contained in Article XIII of this MOU, for the limited purpose of defending civil claims arising out of JTTF activity, a state, local or tribal law enforcement officer who has been federally deputized and who is acting within the course and scope of his or her official duties and assignments pursuant to the MOU may be considered an "employee" of the U.S. government, as defined at 28 U.S.C. § 2671. See 5 U.S.C. § 3374(c)(2).

3. Under the Federal employee Liability reform and Tort Compensation Act of 1998 (commonly known as the Westfall Act), 28 U.S.C. § 2679(b)(1), if an employee of the United States is named as a defendant in a civil action, the Attorney General or his or her designee may certify that the defendant acted within the scope of his or her employment at the time of the incident giving rise to the suit. 28 U.S.C. § 2679(d)(2). The United States can then be substituted for the employee as the sole defendant with respect to any tort claims alleged in the action. 28 U.S.C. § 2679(d)(2). If the United States is substituted as defendant, the individual employee is thereby protected from suit on any tor claim arising out of the incident.

4. If the Attorney General declines to certify that an employee was acting within the scope of employment, "the employee may at any time before trial petition the court to find and certify that the employee was acting with the scope of his office or employment." 28 U.SC. § 269(d)(3).

5. Liability for any negligent or willful acts of JTTF members undertaken outside the terms of this MOU will be the sole responsibility of the respective employee and agency involved.

B. CONSTITUTIONAL CLAIMS

1. Liability for violations of federal constitutional law may rest with the individual federal agent of officer pursuant to Bivens v. Six Unknown Names Agents of the Federal Bureau of Narcotics, 403 U.S. 388 (1971) or pursuant to 42 U.S.C. § 1983 for state officers.

2. Federal, state, local and tribal officers enjoy qualified immunity from suit for constitutional torts, "insofar as their conduct does not violate clearly established statutory or constitutional rights of which a reasonable person would have known." Harlow v. Fitzgerald 457 U.S. 800 (9182).

3. If a Participating Agency JTTF officer is named as a defendant in his or her individual capacity in a civil action alleging constitutional damages as a result of conduct taken within the course of the JTTF, the officer may request representation by DOJ. 28 C.F.R. §§ 50.15, 50.16.

4. An employee may be provided representation "when the actions for which representation is requested reasonably appears to have performed within the scope of the employee's employment and the Attorney General, or his or her designee, determines that providing representation would otherwise be in the interest of the United States." 28 C.F.R. §50.15(a).

5. A JTTF member's written request for representation should be directed to the Attorney General and provided to the Chief Division Counsel (CDC) of the FBI division coordinating the JTTF. The CDC will forward the representation request to the FBI's Office of the General Counsel (OGC) together with a letterhead memorandum concerning the factual basis of the lawsuit. FBI's OGC will then forward the request to the Civil Division of DOJ together with an agency recommendation concerning scope of employment and DOJ representation. 28 C.F.R. §50.15(a)(3).

6. If a JTTF member is found to be liable for a constitutional tort, he or she may request indemnification from DOJ to satisfy and adverse judgment rendered against the employee in his or her individual capacity. 28 C.F.R. § 50.15(c)(4). The criteria for payment are substantially similar to those used to determine whether a federal employee is entitled to DOJ representation under 28 C.F.R. §(a).

7. Determination concerning legal representation and indemnification by the United States are discretionary and are made by DOJ on a case by case basis. The FBI cannot guarantee that the United States will provide legal representation, legal defense, or indemnification to any federal or state employee detailed to the JTTF, and nothing in this Article shall be deemed to create any legal right on the part of any JTTF personnel.

C. EXPRESS RESERVATIONS

1. Nothing in this Article shall be deemed to create an employment relationship between the FBI or the United States and any Participating Agency JTTF member other than for exclusive purposes of the FTCA as outlined herein.

2. The participating agencies do not waive any available defenses and/or limitations on liability. No Participating Agency shall be considered to be an agent of any other Participating Agency.

XXII. DURATION

A. The term of the MOU shall be an indefinite period. The MOU may be terminated at will by any party, provided written notice is provided to the other parties of not less than sixty (60) days. Upon termination of the MOU, all equipment will be returned to the supplying agency(ies). It is understood that the termination of this agreement by any one of the Participating Agencies will have no effect on the agreement between the FBI and all other participating agencies.

B. Notwithstanding this provision, the provisions of Paragraph IX, entitled RECORDS, REPORTS AND INFORMATION SHARING, and Paragraph XXI, entitled LIABILITY, will continue until all potential liabilities have lapsed. Similarly, the inherent disclaimer limitation contained in the EXPRESS RESERVATION provision will survive any termination.

XXIII. AMENDMENTS

This agreement in no manner affects any existing MOUs or agreements with the FBI or any other agency. This agreement may be amended only by mutual written consent of the parties. The modification shall have no force and effect unless such modifications are reduced to writing and signed by an authorized representative of the FBI and the Participating Agency.

CITY OF OAKLAND

AGENDA REPORT

TO:	Sabrina B. Landreth City Administrator	**FROM:**	Anne E. Kirkpatrick Chief of Police
SUBJECT:	OPD JTTF MOU	**DATE:**	December 27, 2017

City Administrator Approval | Date

RECOMMENDATION

Staff Recommends That The City Council Approve A Resolution Authorizing The City Administrator Or Designee To Enter Into A Memorandum Of Understanding (MOU) With The United States Department Of Justice, Federal Bureau Of Investigation (FBI) To Authorize The Oakland Police Department (OPD) To Participate In The Bay Area FBI Joint Terrorism Task Force (JTTF) To Fight Terrorism And Terrorism Planning Activity Which May Occur In, Or Relate To, The City Of Oakland, From January 1, 2018 Through December 31, 2019.

EXECUTIVE SUMMARY

The JTTF serves as an information hub for JTTF members and other agencies that have a right to know and need to know about sensitive information that could save lives. All JTTF operational and investigative activity, including the collection, retention and dissemination of personal information, is conducted in a manner that protects and preserves the constitutional rights and civil liberties of all persons in the United States. The resolution allows OPD personnel with FBI Top Secret/Sensitive Compartmented Information Security Clearance to participate in the JTTF to support anti-terrorism investigations related to the City of Oakland. The MOU has been reviewed by the City's Privacy Advisory Commission (PAC), as the City's Transparency and Accountability for City Participation in Federal Surveillance Operations Ordinance (13457 C.M.S.) requires the initial PAC review.

BACKGROUND AND LEGISLATIVE HISTORY

The FBI[1] defines international terrorism as "perpetrated by individuals and/or groups inspired by or associated with designated foreign terrorist organizations or nations (state-sponsored)." The FBI defines domestic terrorism as "perpetrated by individuals and/or groups inspired by or associated with primarily United States (U.S.)-based movements that espouse extremist ideologies of a political, religious, social, racial, or environmental nature." The New York Times[2],

[1] https://www.fbi.gov/investigate/terrorism
[2] https://www.nytimes.com/2017/11/01/reader-center/readers-debate-what-is-or-isnt-terrorism.html

after the October 1, 2017 Las Vegas mass shooting, wrote that terrorism generally "requires that the violence have a political, ideological or religious motive.

The FBI has created multiple regional JTTFs to embody the objectives of U.S. counterterrorism efforts. According to the FBI[3], the designated mission for each JTTF is to leverage the collective resources of the member agencies for the prevention, preemption, deterrence and investigation of terrorist acts that affect the United States interests, and to disrupt and prevent terrorist acts and apprehend individual who may commit or plan to commit such acts. The JTTF serves as an information hub for JTTF members. All JTTF operational and investigative activity, including the collection, retention and dissemination of personal information, will be conducted in a manner that protects and preserves the constitutional rights and civil liberties of all person in the United States (see "Transparency and Accountability for City Participation in Federal Surveillance Operations Ordinance" Section below). The FBI is authorized to coordinate an intelligence, investigative, and operation response to terrorism, and by virtue of that same authority pursuant to numerous federal statutes[4]. The FBI formed JTTFs composed of other federal, state, local, and tribal law enforcement agencies acting in support of the above listed statutory and regulatory provisions.

Formatted: Font: Not Bold, Not Italic

Formatted: Font: Bold, Italic

Rationale for S.F. Bay Area JTTF

The San Francisco Bay Area is an internationally famous area, and thus, unfortunately, an attractive terrorist target. The Bay Area contains iconic landmarks like the Golden Gate Bridge and the San Francisco-Oakland Bay Bridge. The area also contains numerous professional sports teams and venues, such as the Oakland Coliseum and Oracle Arena, which may realistically be attractive targets for terrorist attacks. Silicon Valley, with its many famous companies, may also be a location for a terrorist attack.

Several large business and government organizations are in Oakland (e.g. Bay Area Rapid Transit (BART), Clorox, Kaiser, Pandora, Southwest Air, University of California Office of the President). Oakland is also home to the fifth busiest container port in the United States. All these sites are potential high-profile targets. Additionally, as high-profile targets became hardened or more secure, terrorist actors may change their tactics and aim for softer targets such as event spaces, museums, theatres and restaurants. Oakland is also home to several gay bars and clubs, as well as houses of religious worship[5]. Oakland has many such spaces in different neighborhoods (e.g. Acorn, Castlemont, Downtown, Dimond, Elmhurst, Fruitvale, Mosswood, Piedmont Avenue, Uptown, Rockridge, Sobrante Park, Temescal…) and any of these physical spaces can become the target of a future terrorist attack plan.

Formatted: No underline

Mass transit has been a target of terrorism throughout the world. Oakland houses an international airport in addition to the Port of Oakland. The City also has BART and Amtrak

[3] https://www.fbi.gov/investigate/terrorism/joint-terrorism-task-forces
[4] 28 U.S.C. § 533, 28 C.F.R. § 0.85, Executive Order 12333, Presidential Decision Directives (PDD) 39, PDD 62, National Security Presidential Directive (NSPD) 46, and Homeland Security Presidential Directive (HSPD) 15
[5] Temple Sinai was recently vandalized although fortunately the damage was minor and there is no known connection to actual terrorism

which passes through all parts of our city. In other words, the Oakland has a significant number of potential targets. OPD does not have enough resources to address the threat of terrorism to these numerous potential sites. Therefore, the residents and visitors of Oakland are best served when Oakland can collaborate with local, state, and federal partners to proactively try to prevent terrorism. The JTTF provides OPD with critical additional resources, knowledge, and experience to protect all our residents, employees and visitors against the threats of terrorism.

Recent Cases of U.S. Domestic Terrorism

The following list highlights recent national examples of domestic terrorism:

1. Boston Marathon Bombing[6] - On April 15, 2013, Tamerlan Tsarnaev and younger brother Dzhokhar Tsarnaev both Russian immigrants of Chechen ethnicity, detonated bombs near the finish line of the Boston Marathon, killing 3 and injuring more than 180 people. Dzhokhar stated that he and his brother were motivated by opposition to the U.S. involvement in Iraq and Afghanistan.
2. 2013 Los Angeles International Airport shooting[7] - On November 1, 2013, Paul Anthony Ciancia entered the checkpoint at the Los Angeles International Airport and killed a Transportation Security Administration (TSA) Officer and injured six others with a rifle. Mr. Ciancia later expressed to authorities his hatred towards TSA officers.
3. Charleston Church Shooting[8] - On June 17, 2015, 21-year old Dylann Roof entered Emanuel African Methodist Episcopal Church in downtown Charleston, South Carolina, shot 10 people and killing nine of them. Mr. Roof claimed he committed the shooting to initiate a race war.
4. Orlando Nightclub Shooting[9] - On June 12, 2016, Omar Mateen, a 29-year-old security guard, killed 49 people and wounded 58 others at Pulse, a gay nightclub in Orlando, Florida. Mateen swore allegiance to the leader of the Islamic State of Iraq and the Levant (ISIL) during the shooting in a 9-1-1 call. During the stand-off in which he was later killed by local Special Weapons And Tactics (SWAT) officers, he claimed the shooting was in retaliation for the U.S. involvement in Iraq and Syria.
5. 2017 Las Vegas Shooting[10] **-** On October 1, 2017, 64-year-old Stephen Paddock of Mesquite, Nevada, fired more than 1,100 rounds from a hotel into a crowd of 22,000 people, killing 58 people and injuring 546 people. He was found dead in his room from a self-inflicted gunshot wound, and his motives are unknown.

ANALYSIS AND POLICY ALTERNATIVES

[6] http://edition.cnn.com/2013/04/18/us/boston-marathon-things-we-know
[7] http://www.latimes.com/local/lanow/la-me-ln-lax-shooting-slain-tsa-agent-identified-as-gerardo-i-hernandez-20131101-story.html#axzz2jQAO3Gla
[8] https://www.nytimes.com/2015/06/18/us/the-charleston-shooting-what-happened.html
[9] http://www.cnn.com/2016/06/12/us/orlando-nightclub-shooting/index.html
[10] https://www.washingtonpost.com/news/morning-mix/wp/2017/10/02/police-shut-down-part-of-las-vegas-strip-due-to-shooting/?utm_term=.67853d8ec043

JTTFs cannot possibly deter all acts of terrorism. The United States is a free and open society; the public only supports limited amounts and types of surveillance and investigations. However, these cases below, a small fraction of the many different terrorist attacks which have occurred in the U.S. over that last several years, point to the need for the FBI to work with local partners to maintain investigative capacities while the public's right to privacy and due process remain unfettered.

The JTTF is comprised of numerous agencies partnering with the FBI to fight terrorism. Local JTTF cells work together to assess threats, investigate leads, gather evidence, and make arrests. JTTFs gather and share intelligence and conduct outreach and training. JTTFs are organized to deploy resources at a moment's notice for threats or major incidents; the JTTF also can provide resources for security at special events. The JTTF establishes a relationship and familiarity between investigators and managers of numerous agencies before a crisis occurs. JTTFs pool talents, skills, and knowledge from across the law enforcement and intelligence communities into a single team that responds together

The San Francisco-based JTTF is comprised of numerous agencies throughout the Bay Area:

- United States Secret Service (USSS);
- United States Department of Home Security (DHS);
- United States Marshalls (USM);
- Alameda County Sheriff's Office (ACSO);
- California Highway Patrol (CHP)
- Fremont Police Department (FPD);
- Bay Area Rapid Transit Police Department (BART PD);
- San Jose Police Department (SJPD);
- San Mateo County Sheriff's Office (SMCSO); and
- Santa Clara County Sheriff's Office (SCCSO);

These agencies partners are committed to work with the FBI to fight terrorism. OPD believes in working with these local, state, and federal agencies and the FBI to assess threats, investigate leads, gather evidence, and where warranted – to make arrests. In addition, the JTTF gathers and shares intelligence, and conducts outreach to both law enforcement and local community organizations. The FBI provides procedural and tactical training to local police department SWAT teams and officers. The civil rights program also provides extensive training and briefings to police departments about proper legal and use of force procedures. The FBI communicates with schools, rail service providers (such as BART PD) and religious institutions (regardless of denomination) and provides training on homegrown violent extremists (HVE), active shooters and other issues of concern. In addition, programs like the human trafficking program also provide direct outreach to the private sector (as well as law enforcement officers) to educate and provide an increased awareness about human trafficking. The FBI is striving to engage the private sector in a broader way through the office of Private Sector Engagement. The FBI is always striving to strengthen its relationships with the communities in the Bay Area through these programs.

Through the JTTF, local agencies can combine different skills and capacities (i.e. SWAT units and different intelligence gathering efforts) across the law enforcement and intelligence communities and blends them into a single team that can respond as one unit. The JTTF agencies, through mutual collaboration, can deploy resources more quickly to respond to threats or during major critical incidents. The JTTF can provide essential security resources at special events. Through mutual collaboration, agencies like OPD are prepared - before a crisis occurs.

Commented [BS1]: Say more here about the value to OPD of having a TF officer assigned

JTTF Anti-Terrorism Investigation Examples

The following examples illustrate recent examples of terrorist plots which occurred in the San Francisco Bay Area.

1. Pipe Bomb Investigation - There was October 2018 pipe bomb investigation in which Bay Area politicians and members of the media received pipe bombs in the mail. OPD was concerned that local figures in Oakland were also targeted. The OPD JTTF Officer coordinated with the Task Force on investigations (the Task Force determined that no Oakland based officials were targeted, and this information was relayed to City officials)[11]
2. Oakland ISIS Sympathizer[12] - Berkeley High School graduate Amer Sinan Alhaggagi, 22, was indicted in July 2017, for attempting to provide support to the terrorist group ISIS. Federal prosecutors say that Alhaggagi planned to kill thousands of people by bombing gay night clubs, planting bombs on UC Berkeley's campus, and selling drugs laced with poison. He applied for a job as a police officer with OPD, and exchanged bomb-making materials with undercover FBI agents. The FBI and JTTF investigations led to his arrest.
3. FBI thwarts Oakland bank bombing[13] - A mentally disturbed man who said he believed in violent jihad and hoped to start a civil war in the United States was arrested in the process of trying to detonate a bomb at a bank in Oakland. Matthew Aaron Llaneza, 28, of San Jose believed he was triggering a cell phone-activated bomb at a crowded Bank of America branch. An undercover FBI agent posed as a go-between with the Taliban in Afghanistan. The FBI created a faux-bomb for Mr. LLaneza after repeated declarations of wanting to kill Americans, and after past arrest on weapons charges.
4. Pier 39 Christmas Plot[14] - Everitt Aaron Jameson, a 26-year old former U.S. Marine from Northern California was arrested December 22, 2017 for allegedly offering to carry out a terrorist attack on Christmas Day in San Francisco at the Pier 39. He is charged with attempting to provide material support to a foreign terrorist organization (ISIS). He had been investigated by the FBI, according to the unsealed criminal complaint, for

[11] This case occurred before 2018 (the year of this annual report). OPD is including this past information because 2018 is the first reporting year; past information is provided for context as to relevant work related to the JTTF TF.
[12] https://www.nbcbayarea.com/news/local/Feds-Oakland-ISIS-Sympathizer-Wanted-to-Kill-Thousands-in-String-of-Bay-Area-Terror-Attacks-436633853.html
[13] http://www.sfgate.com/crime/article/FBI-thwarts-Oakland-bank-bombing-4263660.php
[14] http://sanfrancisco.cbslocal.com/2017/12/22/fbi-pier-39-christmas-day-terror-plot-arrest/

espousing "radical jihadi beliefs, including authoring social media posts that are supportive of terrorism, communicating with people he believes share his jihadi views and offering to provide services to such people …" Jameson had allegedly shared plans for a terrorist attack (involving use of firearms and explosives) with undercover FBI agents.

Transparency and Accountability for City Participation in Federal Surveillance Operations Ordinance

The City Council passed Ordinance no. 13457 C.M.S. (Transparency and Accountability for City Participation in Federal Surveillance Operations) on October 3, 2017. This ordinance added Chapter 9.72.010 to Chapter 9 of the Oakland Municipal Code (OMC) to ensure greater transparency and establish a protocol for city participation in federal law enforcement surveillance operations. OMC 9.72.010 reads as follows:

1. The City of Oakland, including but not limited to the Oakland Police Department, may assist federal agencies, including but not limited to, the Federal Bureau of Investigation ("FBI") through its Joint Terrorism Task Force, or any successor task force, joint operation, assignment, or enforcement activity (collectively, "JTTF") in preventing and investigating possible acts of terrorism and other criminal activity only in a manner that is fully consistent with the laws of the State of California, including but not limited to the inalienable right to privacy guaranteed by Article 1, Section 1 of the California Constitution, as well as the laws and policies of the City of Oakland, including but not limited to Police Department policies, procedures, and orders.
2. Before execution of any Memorandum of Understanding or other written agreement, contract or arrangement (collectively, "MOU") between the Oakland Police Department and the FBI, or other federal law enforcement agency, regarding the Police Department's participation on the JTTF or other federal law enforcement agency task force, or any amendment to any such existing MOU, the Chief of Police shall submit the proposed MOU and any orders, policies, and procedures relevant to the subject matter of the MOU for discussion and public comment at an open meeting of the PAC.
3. By January 31 of each year, the Chief of Police shall provide to the PAC and City Council, a public report with appropriate public information on the Police Department's work with the JTTF or other federal law enforcement agency task force in the prior calendar year, including any issues related to compliance with this Section – The PAC unanimously accepted OPD's 2018 Annual JTTF report after on July 8, 2019. OPD first presented the annual report earlier in 2019; the acceptance of the annual report on July 8, 2019 was the result of significant collaboration between OPD, the PAC, and numerous privacy advocacy organizations.~~.~~

In accordance with Ordinance No. 13457 C.M.S, OPD plans to provide to the PAC and City Council each year a public report with appropriate public information on OPD's work with the JTTF in the prior calendar year. Ordinance No. 13457 C.M.S. also requires that OPD bring this MOU and resolution first to the PAC before the City Council can approve the resolution which authorizes the City Administrator to negotiate and execute the MOU. The PAC reviewed this MOU and resolution on….

OPD FBI JTTF Participation Protocols

The supervisor of the San Francisco-based JTTF is the FBI Special Agent in Charge (SAIC) or Assistant Director in Charge (ADIC) from the FBI San Francisco Division. OPD personnel participating in the JTTF are subject to all OPD policies and procedures and agree to adhere to the FBI's ethical standards. OPD personnel assigned to the JTTF are subject to the Supplemental Standards of Ethical Conduct for employees of the United States Department of Justice. Whichever standard or requirement that provides the greatest restrictions as well as organizational protection or benefit will apply where this is a conflict between the standards or requirements of OPD and the FBI.

Participating OPD personnel remain OPD employees and all other JTTF participating personnel remain employees of their respective agencies. Any~~l~~ OPD personnel participating in the JTTF shall be held responsible for adhering to all OPD policies including Use of Force and City of Oakland and State of California immigration-specific policies. OPD personnel participating in the JTTF shall also adhere to ~~undergo~~ the FBI Top Secret/Sensitive Compartmented Information Security Clearance process.

Both OPD and the FBI will maintain responsibility for all costs related to normal staffing and operation costs. There is no promise or guarantee of funding for participation in the JTTF, except that the FBI may pay for travel costs for OPD personnel participating in the JTTF when investigations require travel outside of Oakland. OPD personnel participating in the JTTF may be permitted to drive FBI-owned or leased vehicles for official JTTF use and in accordance with applicable FBI rules and regulations. Any civil liability arising from the use of an FBI owned or leased vehicle by OPD personnel, other than for official duties related to the JTTF, shall be the responsibly of OPD.

~~In accordance with Ordinance No. 13457 C.M.S, OPD plans to provide to the PAC and City Council each year a public report with appropriate public information on OPD's work with the JTTF in the prior calendar year. Ordinance No. 13457 C.M.S. also requires that OPD bring this MOU and resolution first to the PAC before the City Council can approve the resolution which authorizes the City Administrator to negotiate and execute the MOU. The PAC reviewed this MOU and resolution on….~~

~~City of San Francisco JTTF Participation~~

~~The San Francisco Police Department announced on February 1, 2017[15], that they would cancel their collaboration with the Bay Area JTTF, first signed in 2007, after the City received letters from the Asian Law Caucus, the Council on American-Islamic Relations' San Francisco Bay Area office and the American Civil Liberties Union of Northern California. However, after the recent Pier 39 Christmas Plot (see Page 5 below), then-acting Mayor (and current Supervisor) London Breed is now asking[16] the city should re-join the Task Force.~~

~~[15] http://sanfrancisco.cbslocal.com/2017/02/01/san-francisco-police-department-suspends-participation-with-fbi-joint-terrorism-task-force/~~
~~[16] http://sanfrancisco.cbslocal.com/2017/12/26/pier-39-terror-plot-breed-cooperation-feds/~~

Formatted: Font: Bold, Italic
Formatted: Font: Bold, Italic
Formatted: Font: Bold, Italic

Commented [BS2]: Do we have an update on this?

Commented [BS3]: We don't know where things stand with SF JTTF, so thinking it's best to leave out this entire section.

PUBLIC OUTEACH / INTEREST

The PAC reviewed the FBI JTTF MOU on…. During publicly noticed meetings….

COORDINATION

OPD consulted the Office of the City Attorney in the development of this report and accompanying resolution.

FISCAL IMPACT

There are no personnel or other costs to OPD associated with membership in the FBI JTTF. OPD will designate one or more officers already employed through OPD's operating budget. OPD is responsible for providing the salary, benefits and overtime payments for its assigned personnel.

Asset forfeitures attributable to the JTTF investigations may be distributed among participating JTTF agencies at the discretion of the FBI. Any reimbursements for overtime expenses made by the FBI to OPD shall be deposited into Fund 2999, Org 102310, Account 46129, Project 1001413, and Program PS03.

SUSTAINABLE OPPORTUNITIES

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

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

Social Equity: OPD's collaboration with the DEA helps OPD to target not only illegal drug and narcotics trafficking but violent crime connected to illegal drug trafficking and associated networks. All residents and visitors benefit from these efforts to investigate and prosecute individuals involved in this illegal and dangerous activity.

ACTION REQUESTED OF THE PUBLIC SAFETY COMMITTEE

Staff Recommends That The City Council Approve A Resolution Authorizing The City Administrator Or Designee To Enter Into A Memorandum Of Understanding (MOU) With The United States Department Of Justice, Federal Bureau Of Investigation (FBI) To Authorize The Oakland Police Department (OPD) To Participate In The Bay Area FBI Joint Terrorism Task Force (JTTF) To Fight Terrorism And Terrorism Planning Activity Which May Occur In, Or Relate To, The City Of Oakland, From January 1, 2018 Through December 31, 2019.

For questions regarding this report, please contact Sergeant Serge Babka, Intelligence Unit, Office of the Chief of Police, at (510) 238-3753.

Respectfully submitted,

Anne E. Kirkpatrick
Chief of Police
Oakland Police Department

Reviewed by:
Serge Babka, Sergeant
Office of the Chief of Police, Intelligence Unit

Prepared by:
Bruce Stoffmacher, Legislation Manager
Training Division, Research and Planning

OAKLAND POLICE DEPARTMENT

Surveillance Impact Use Report for Handheld Lives Stream Cameras

1. Information Describing Manual Live-Stream Cameras 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 cameras are manually operating cameras connected to a transmitter to allow the live stream transmission to a different location. OPD and the City of Oakland have Emergency Operations Centers (EOC). Cameras attached to transmitters "handheld live stream cameras" allow an officer to transmit a live view of what they see to the EOC.

2. Proposed Purpose

Handheld live stream cameras are used by OPD authorized personnel to provide situational awareness during large events where there is a greater probability that criminal activity may occur and public safety is more likely to be impacted; the City's Surveillance Technology Ordinance[1] defines "large-scale event(s)" as events "attract(ing) ten thousand (10,000) or more people with the potential to attract national media attention that provides a reasonable basis to anticipate that exigent circumstances may occur." OPD may also use live stream cameras on poles held by officers to observe smaller events in the scores or hundreds of people where the same conditions exist. This technology provides the opportunity to deploy a minimal level of police presence while providing critical situational awareness to OPD commanders.

3. Locations Where, and Situations in which Handheld Live Stream Cameras may be deployed or utilized.

These cameras may be used anywhere in the public right of way within the City of Oakland. Personnel may use handheld cameras with live-viewing capabilities 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 protests or parades.

[1] Ordinance No. 13489C.M.S. passed by the City Council on May 15, 2018

The following table presents Part 1 Crime Data for January 1-May 31 Year to Date (YTD).

Part 1 Crimes	YTD 2015	YTD 2016	YTD 2017	YTD 2018	YTD 2019	YTD % Change 2018 vs. 2019	5-Year YTD Average	YTD 2019 vs. 5-Year Average
All Crimes	2,653	2,353	2,442	2,319	2,502	8%	2,454	2%
Homicide 187(a)PC	35	19	25	22	31	41%	26	17%
Aggravated Assault	1,150	1,061	1,160	1,188	1,347	13%	1,181	14%
Rape	80	93	96	88	71	-19%	86	-17%
Robbery	1,388	1,180	1,161	1,021	1,053	3%	1,161	-9%
Burglary	5,330	3,979	5,363	3,749	4,616	23%	4,607	0%
Vehicle Theft	3,200	3,359	3,144	2,633	2,551	-3%	2,977	-14%
Larceny	2,618	2,424	2,466	2,622	2,438	-7%	2,514	-3%
Arson	66	53	38	71	48	-32%	55	-13%

Commented [BH1]: Curious as to why this table is used. Almost none of these crimes occur at mass events or undercover investigations, which are the suggested uses for this equipment.

Commented [BS2R1]: It's difficult to provide crime data specific on only times where these cameras have been utilized. The PAC is requiring that crime data be provided for this section. Citywide multi-year crime data provides context for which OPD uses different types of surveillance technology.

4. Impact

OPD recognizes that any use of cameras to record activity which occurs 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 it may have a chilling effect. TO mitigation section below provides explains the restricted use as specified in OPD Department General Order (DGO) >>>>> "Handheld Live Stream Camera" Policy.

Formatted: Highlight

However, OPD does not randomly employ this technology throughout the City. Rather, these cameras are only used during mass-events where public safety has a greater likelihood of being negatively impacted.

Commented [BH3]: Above, it always says "undercover operations." Which is it?

Commented [BS4R3]: That was deleted

Handheld live stream cameras offer evidentiary and situational awareness in numerous ways that challenge measurement. Mass events where thousands of people gather require that police personnel see where people are moving in real-time to better ensure that resources are provided as needed to ensure public safety.

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) >>>>> "Handheld Live Stream Camera" Policy restricts the use of handheld live stream cameras in section III.B 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. The Handheld Live Stream Camera shall not be used to infringe, monitor, or intrude upon Protected Activity except where all of the following conditions are met:
    a. There is a Reasonable Suspicion of criminal wrongdoing; and
    b. OPD articulates the facts and circumstances surrounding the use and basis for Reasonable Suspicion in a written statement filed with the Chief Privacy Officer no later than 48 hours after activation of the RLSC. These facts and circumstances shall be incorporated into the annual report pursuant to Oakland Municipal Code Section 9.64.010 1.A.

All live-stream cameras shall be housed and secured within OPD's IT Unit lockers and not accessible with to the public or to personnel without permission to use such equipment. Regular camera data, if the cameras are recording data, from live stream cameras shall be uploaded onto a 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

Formatted: Highlight

Commented [BS5]: change from 8 hrs to 48 hrs

Commented [BH6]: Where? Owned and used by who?

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 handheld ~~manual~~ live -stream cameras 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

Cameras that record directly onto an internal memory device (e.g. secure digital (SD) card) 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.

Cameras can be mounted to telescoping monopods to simply extend the range of the unit. In these instances, the pole merely extends the reach of the camera.

TV Transmitters can use different formats (e.g. cellular 3G/4G LTE, WiFi, Ethernet, and Microwave). Transmitters can be connected to static single image digital cameras or video cameras. 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.

7. Data Security

All cameras and TV transmitters shall be housed and secured within IT Unit or Intel Unit lockers 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.

Commented [BH7]: Where? Owned and used by who?

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[2] to pay four new modern TVU Networks transmitters.

9. Third Party Dependence

OPD uses TVU Networks-brand transmitter for live-stream video camera monitoring.

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.

11. Track Record of Other Entities

Many police departments rely on live-stream cameras to maintain situational awareness.

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

DEPARTMENTAL GENERAL ORDER

##: HANDHELD LIVE STREAM CAMERA

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 Cameras.

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. Handheld Live Stream Camera "Live Stream Camera" Components

Live-stream cameras consist of a standard camera with video capabilities and a TV transmitter. The TV transmitter can send a digital signal to a specific location such as OPD's Police Administration Building and/or the City of Oakland Emergency Operation Center (EOC).

~~Cameras that record directly onto an internal memory device (e.g. secure digital (SD) card) 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.~~

Commented [BS1]: If we are focusing policy just on live stream then maybe delete and not focus on whether the camera also records, as we do not need a policy for a simple camera that records – surveillance ordinance is specific on that.

B. How the System Works

Cameras become "live-stream" cameras when connected to a transmitter which allows for 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 cameras or video cameras. 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.

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 cameras. Large events with numerous people pose challenges to public safety. Protests, sporting events, parades, and large festivals can attract individuals seeking to engage in violent criminal behavior and/or large-scale property destruction. OPD needs situational awareness to ensure that at such events police personnel are

efficiently and properly deployed. Authorized personnel utilizing cameras with live-streaming transmitters can provide important situational awareness to OPD without the need to deploy many officers. At the direction of an incident commander, and when the OPD or City of Oakland EOC has been activated.

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 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. The Handheld Live Stream Camera shall not be used to infringe, monitor, or intrude upon Protected Activity except where all of the following conditions are met:

a. There is a Reasonable Suspicion[1] of criminal wrongdoing; and

[1] For purposes of determining whether sufficient grounds exist for any of the allowable uses authorized under this policy under the Section "Authorized Uses", "Reasonable Suspicion"

Commented [BH2]: You're abandoning undercover use then?

Commented [BS3R2]:

Commented [BS4R2]: yes

Commented [BH5]: The ordinance requires that they must be enumerated.

Commented [BS6R5]: Ordinance requires: The specific purpose(s) that the surveillance technology is intended to advance;

b. OPD articulates the facts and circumstances surrounding the use and basis for Reasonable Suspicion in a written statement filed with the Chief Privacy Officer no later than 48 hours after activation of the RLSC. These facts and circumstances shall be incorporated into the annual report pursuant to Oakland Municipal Code Section 9.64.010 1.A.

Commented [BS7]: change from 8 hrs to 48 hrs

C. Communications

For clarity of communications, radio traffic should identify the device as "live stream camera."

IV. LIVE STREAM CAMERA DATA

A. **Data Collection and Retention**

Handheld live stream cameras can send the digital image files (e.g. jpeg, gif) and video files (e.g. .mp4, .wav) 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. ~~The IT Unit Coordinator shall download the data onto secure IT Unit computer within 24 hours of receiving returned RLSC equipment.~~

~~The IT Unit shall maintain all camera data for 30 days unless notified by the Chief of Police or designee (e.g. Internal Affairs Captain or Criminal Investigations personnel) that the image and video data is needed for an investigation. The IT Unit Coordinator is responsible for recovering the data from the camera data storage unit.~~

~~Data that is part of an investigation shall be provided to the appropriate personnel as a separate digital data file, kept permanently as part of the official investigation record.~~

~~The IT Unit shall delete all live-stream camera data left on installed on IT Unit computers after 30 days unless otherwise notified to maintain the data as part of an investigation as detailed above.~~

Commented [BH8]: What can be collected? Per Ordinance: 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 [BS9R8]: See addition here on digital formats

Commented [BS10]: Recommend delete as this policy is about use of the livestream, not about the recording of a standard handheld camera.

---

means specific and articulable facts which, taken together with rational inferences from those facts, evince more than an inchoate and unparticularized suspicion or hunch that an individual or organization is involved in a definable criminal activity or enterprise. Reasonable Suspicion shall not be based on Protected Activity. A suspect's actual or perceived race, national origin, color, creed, age, alienage or citizenship status, gender, sexual orientation, disability, or housing status, shall not be considered as a factor that creates suspicion, and may only be used as identifying information in the description of a criminal suspect.

B. 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 legitimate law enforcement purposes only, such as when the data related to an administrative or criminal investigation, or for training 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 ~~intended purpose of obtaining 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.

~~6.~~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.

C. Data Security

Live-stream camera data will be closely safeguarded and protected by both procedural and technological means:

1. All live-stream cameras -shall be housed and secured within IT Unit or lockers. All data downloaded from camera shall be uploaded onto secure user and email password protected IT Unit computers and / or Intel Unit computers.
2. For data that is captured and used as evidence, such data shall be turned in and stored as evidence.

V. LIVE STREAM TRACKER SYSTEM ADMINISTRATION

A. System Coordinator / Administrator

Commented [BH11]: Missing category, from the Ordinance: G.
Public Access: how collected information can be accessed or used by members of the public, including criminal defendants;

Commented [BS12R11]: See B.4 below

Commented [BH13]: What administrative purposes?

Commented [BS14R13]: Could be internal affairs or training

Commented [BH15]: Definition of "Need to Know": "Need To Know" means even if one has all the necessary official approvals (such as a security clearance), one shall not be given access to the data unless one has a specific need to access the system or data in order to conduct one's official duties in connection with one of the Authorized Uses of this Policy.
Furthermore, the "need" shall be established prior to access being granted by the designated City official or their designee and shall be recorded in accordance with Oakland Municipal Code 9.64.010 1.B.

Commented [BS16R15]: Addressed w/ change of language on 4.B.C

Commented [BH17]: Needs discussion. "A need to know and a right to know" is our standard threshold and requires a direct involvement in the investigation. This language is too broad.

Commented [BS18R17]: Addressed w/ change of language on 4.B.C

Commented [BH19]: Missing category, from the Ordinance: K.
Maintenance: The mechanisms and procedures to ensure that the security and integrity of the surveillance technology and collected information will be maintained

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.

~~B.~~C. **Training**

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

~~C.~~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: