CITY OF OAKLAND

**Privacy Advisory Commission**
**Special Meeting Agenda**

**Oakland City Hall, Hearing Room 1**
**1 Frank H. Ogawa Plaza**

**Thursday October 1, 2026**
**5:00 PM**

## PUBLIC PARTICIPATION

The Privacy Advisory Commission encourages public participation in its meetings. Members of the public may observe and/or provide public comment in the following ways:

### OBSERVE THE MEETING

**By Zoom:**
To observe the meeting via video conference, please click the following link at the noticed meeting time:
https://oaklandca-gov.zoom.us/j/82683698612

**By Phone:**
Call he number below:

+1 669 444 9171

Instructions for joining by phone are available at:
https://support.zoom.us/hc/en-us/articles/201362663

### PROVIDE PUBLIC COMMENT

Public comment may be submitted in the following ways, within the time allotted for each eligible agenda item:

• Submit written comment in advance:
Email your comment, full name, and the agenda item number to Michelle NewRingeisen at MNewRingeisen@oaklandca.gov no later than one (1) hour before the posted meeting time. All timely submissions will be shared with the Selection Panel prior to the meeting.

• Complete a speaker card during the meeting.

• Raise your hand on Zoom during public comment or open forum and staff will call on you to speak for the time allotted by the Chair.

For questions regarding these procedures, please contact Michelle NewRingeisen at MNewRingeisen@oaklandca.gov

CITY OF OAKLAND

**Privacy Advisory Commission**
**Special Meeting Agenda**

**Oakland City Hall, Hearing Room 1**
**1 Frank H. Ogawa Plaza**

**Thursday October 1, 2026**
**5:00 PM**

## I. CALL TO ORDER
The Chair opens the meeting and officially begins proceedings.

## II. ROLL CALL
The Clerk Calls roll to confirm member attendance to determine if there is a quorum (5 members) to conduct business.

Commissioners: Byron White, Issac Cheng, Gina Tomlinson, Vice Chair Henry Gage III, Chair Jessica Leavitt, Ray Sudip

## III. PUBLIC COMMENT
During Public Comment, members of the public may comment on any a**gendized items** within the Commission's jurisdiction when called.

## IV. APPROVAL OF MINUTES
The Panel reviews the draft minutes from a prior meeting and may take action to approve them as presented or with revisions.

1. July 2nd Meeting Minutes

## V. PRIVACY ADVISOR COMMISSION VOTE FOR A CHAIR
The Commission may receive nominations from the body and take action to appoint a Chair of the Privacy Advisory Commission

## VI. PRIVACY ADVISOR COMMISSION VOTE FOR A VICE CHAIR
The Commission may receive nominations from the body and may take action to appoint a Vice Chair of the Privacy Advisory Commission

## VII. TASKFORCE BUREAU OF ALCOHOL, TOBACCO, FIREARMS AND EXPLOSIVES (ATF) MOU
Review and receive public comment on the Memorandum of Understanding governing the Oakland Police Department's participation in the ATF Joint Law Enforcement Task Force, including provisions related to investigative authority, information sharing, and operational responsibilities.

## VIII. BODY WORN CAMERA MOU
Review and receive public comment on the Body-Worn Camera Addendum establishing requirements for the use, handling, retention, and disclosure of body-worn camera recordings during ATF Joint Law Enforcement Task Force operations.

CITY OF OAKLAND

**Privacy Advisory Commission**
**Special Meeting Agenda**

**Oakland City Hall, Hearing Room 1**
**1 Frank H. Ogawa Plaza**

**Thursday October 1, 2026**
**5:00 PM**

**IX. DRUG ENFORCEMENT ADMINISTRATION (DEA) MOU**
Review and receive public comment on the Memorandum of Understanding governing the Oakland Police Department's participation in the DEA Joint Law Enforcement Task Force, including provisions related to investigative authority, information sharing, and operational responsibilities.

**X. I-34 VEHICLE DIGITAL FORENSIC TECHNOLOGY**
Receive public comment and make a recommendation whether City Council should adopt, modify, or reject Oakland the Police Department's Surveillance Use Policy on vehicle digital forensic technology.

**XI. DRONE USE POLICY**
Review and receive public comment on the Oakland Police Department's Drone Use Policy, including provisions related to authorized uses, deployment procedures, data collection and retention, privacy protections, and oversight requirements.

**XII. Oakland Fire Department Unmanned Aircraft System (UAS)**
Review and receive public comment on the Oakland Fire Department's proposed UAS Program and Policy to support firefighter safety, situational awareness, emergency response, and incident management, including authorized uses, deployment procedures, data retention, privacy protections, and oversight requirements.

**XIII. OPEN FORUM**
Members of the public may speak on **non-agendized** items within the Panel's jurisdiction.

**ADJOURNMENT**

Do you need an ASL, Cantonese, Mandarin or Spanish interpreter or other assistance to participate? Please email Michelle NewRingeisen at MNewRingeisen@oaklandca.gov or call (510) 238- or (510) 238-2007 for TDD/TTY five days in advance.

¿Necesita un intérprete en español, cantonés o mandarín, u otra ayuda para participar? Por favor envíe un correo electrónico a Felicia Michelle NewRingeisen at MNewRingeisen@oaklandca.govo llame al (510) 238-7857 o al (510) 238-2007 para TDD/TTY por lo menos cinco días antes de la reunión. Gracias.

你需要手語,西班牙語,粵語或國語翻譯服務嗎?請在會議前五個工作天電郵
Michelle NewRingeisen at MNewRingeisen@oaklandca.gov 或 致電 (510) 238-7857

CITY OF OAKLAND

**Privacy Advisory Commission**
**Draft Meeting Minutes**

**Oakland City Hall, Hearing Room 1**
**1 Frank H. Ogawa Plaza**

**July 2, 2026**
**5:00 PM**

## I. Called To order

## II. Roll Call

Byron White - Excused
Gina Tomlinson - Present
Chair Jessica Leavitt – Present
Issac Cheng – Present
Vice Chair Henry Gage III - Present
Sudip Ray - Present

## III. Public Comment

## IV. Approval of Meeting Minutes

June 4, 2026 Meeting Minutes

**Discussion:** No Discussion

**Motion:** to Approve the June 4, 2026 meeting minutes as listed on the agenda with a correction identified by Commissioner Cheng to remove Vice Chair Gage from the ad-hoc committee established during the June 4, 2026 meeting, by Chair Leavitt

**Seconded by:** Commissioner Cheng

**Vote:**
Issac Cheng Y Gina Tomlinson Y Byron White Ex
Vice Chair Henry Gage III Y Ch Jessica Leavitt Y Sudip Ray Y

**Result:** Motion passes 5 Y's and 1 Excused

## V. NCRIC / WISN ACCESSING FLOCK IN VIOLATION OF SB 34

**Discussion:** OPD provided an in-person informational report detailing the City's interaction and decision to revoke Northern California Regional Information Center (NCRIC) access to Oakland's FLOCK data.

NCRIC originally met the qualification to access OPD's Flock database in 2024, meaning at that time, the City determined that NCRIC met the standards to access the database. Upon a subsequent internal audit of system data searches in 2025, however, OPD raised questions about some of those searches.

During the period of October 2024through November 2025, NCRIC performed 374 searches with 226 of those searches determined to be related to ATF. OPD learned that NCRIC provided access to the Western States Intelligence Network (WSIN), a 3rd party, to run searches on NCRIC's behalf. A portion of those searches were deemed by OPD to violate SB 34. OPD determined that NCRIC did not have sufficient protocols in place to access Oakland's data and proactively revoked access to the system in November of 2025. NCRIC has subsequently requested reinstatement and was denied.

Discussion focused on process, reporting, how OPD audits information and implications for requested data by PAC for the next annual report. OPD shared information on the process by which the department performs/refines searches.

PAC will provide advocacy to the department as needed for resources and will request additional information to be brought forward in the next annual report; OPD confirmed.

**Motion:** Receive the informational report provided by OPD and request that OPD provide additional information on this issue in their 2026 annual report by Chair Leavitt.

**Seconded by:** Vice Chair Gage

**Vote:**

Issac Cheng Y Gina Tomlinson Y Byron White Ex
Vice Chair Henry Gage III Y Ch Jessica Leavitt Y Sudip Ray Y

**Result:** Motion passed 5 Y and 1 Excused

**ADJOURNMENT**

**MEMORANDUM OF UNDERSTANDING**

**BETWEEN**

**THE BUREAU OF ALCOHOL, TOBACCO, FIREARMS AND EXPLOSIVES,**

And

**THE OAKLAND POLICE DEPARTMENT (OPD)**

This Memorandum of Understanding ("MOU") is entered into by and between the Bureau of Alcohol, Tobacco, Firearms and Explosives ("ATF") and the Oakland Police Department ("participating agency") as it relates to the ATF Task Force (herein referred to as the "Task Force").

## AUTHORITIES

The authority to investigate and enforce offenses under the provisions of this MOU is found at 28 U.S.C. § 599A, 28 C.F.R. §§ 0.130, 0.131, and 18 U.S.C. § 3051.

## PURPOSE

The Task Force will perform the activities and duties described below:

a. Investigate firearms trafficking
b. Investigate firearms-related violent crime
c. Gather and report intelligence data relating to trafficking in firearms
d. Conduct undercover operations where appropriate and engage in other traditional methods of investigation in order that the Task Force's activities will result in effective prosecution before the courts of the United States and the State of California.
e. Identify and apprehend wanted offenders who are involved in firearms violence or other firearms crimes.

## MEASUREMENT OF SUCCESS

The ability to measure the success of this initiative will depend on the participating agencies' willingness to share certain information (i.e., crime statistics).

Core Functions:

- Firearm Criminal Possession and Use
- Criminal Groups and Gangs
- Illegal Firearms Trafficking

Performance Goal Statement:

- Reduce the risk to public safety caused by criminal possession and use of firearms.
- Reduce the risk to public safety caused by criminal organizations and gangs.
- Reduce the risk to public safety caused by illegal firearm trafficking.

Strategic Objectives:

- Interdict and prevent the criminal use of firearms.
- Identify, disrupt, and dismantle violent gangs and criminal organizations emphasizing the use of state and local intelligence to identify problematic offenders.
- Interdict and prevent illegal firearms trafficking.
- Share technology such as NIBIN and E Trace.

Share intelligence with state and local law enforcement.

## PHYSICAL LOCATION

Officers/troopers/agents assigned to this Task Force by their employer shall be referred to as task force officers (TFOs). TFOs will be assigned to the ATF Oakland Field Office at 1301 Clay Street, 670s, Oakland, CA.

## SUPERVISION AND CONTROL

The day-to-day supervision and administrative control of TFOs will be the mutual responsibility of the participants, with the ATF Special Agent in Charge or his/her designee having operational control over all operations related to this Task Force.

TFOs shall remain subject to their respective agencies' policies and shall report to their respective agencies regarding matters unrelated to this agreement/Task Force. With regard to matters related to the Task Force, TFOs will be subject to federal law and Department of Justice and ATF orders, regulations and policies, including those related to standards of conduct, sexual harassment, equal opportunity issues, and federal disclosure laws.

Failure to comply with this section could result in a TFO's dismissal from the Task Force.

## PERSONNEL, RESOURCES AND SUPERVISION

To accomplish the objectives of the Task Force, ATF will assign five (5) Special Agents to the Task Force. ATF will also, subject to the availability of funds, provide necessary funds and equipment to support the activities of the ATF Special Agents and TFOs assigned to the Task Force. This support may include office space, office supplies, travel funds, funds for the purchase of evidence and information, investigative equipment, training, and other support items.

Each participating agency agrees to make available to its assigned task members any equipment ordinarily assigned for use by that agency. In the event ATF supplies equipment (which may include vehicles, weapons, or radios), TFOs must abide by any applicable ATF property orders and policy and may be required to enter into a separate agreement for their use.

To accomplish the objectives of the Task Force, the Oakland Police Department agrees to detail a minimum of two (2) up to six (6) full-time TFOs and/or part-time TFOs to the Task Force for a period of not less than two (2) years.

All full-time TFOs shall qualify with their respective firearms by complying with ATF's Firearms and Weapons Policy.

## SECURITY CLEARANCES

All TFOs will undergo a security clearance and background investigation, and ATF shall bear the costs associated with those investigations. TFOs must not be the subject of any ongoing investigation by their department or any other law enforcement agency, and past behavior or punishment, disciplinary, punitive, or otherwise, may disqualify one from eligibility to join the Task Force. ATF has final authority as to the suitability of TFOs for inclusion on the Task Force.

## DEPUTATIONS

ATF, as the sponsoring federal law enforcement agency, will require that the participating agency's TFOs be deputized by the U.S. Marshals Service to extend their jurisdiction, to include applying for and executing federal search and arrest warrants, and requesting and executing federal grand jury subpoenas for records and evidence involving violations of federal laws.

A TFO will not be considered for Department of Justice legal representation if named as a defendant in an individual-capacity lawsuit alleging constitutional violations unless all deputation paperwork has been completed and approved prior to the event(s) at issue in the lawsuit.

The participating agencies agree that any federal authority that may be conferred by a deputation is limited only to activities supervised by ATF and will terminate when this MOU is terminated or when the deputized TFOs leave the Task Force, or at the discretion of ATF.

## ASSIGNMENTS, REPORTS, AND INFORMATION SHARING

An ATF supervisor or designee will be empowered with designated oversight for investigative and personnel matters related to the Task Force and will be responsible for opening, monitoring, directing, and closing Task Force investigations in accordance with ATF policy and the applicable United States Attorney General's Guidelines.

Assignments will be based on, but not limited to, experience, training, and performance, in addition to the discretion of the ATF supervisor.

All investigative reports will be prepared utilizing ATF's investigative case management system (N-Force or Spartan, as appropriate) utilizing ATF case report numbers. The participating agency will share investigative reports, findings, intelligence, etc., in furtherance of the mission of this agreement, to the fullest extent allowed by law. For the purposes of uniformity, there will be no duplication of reports, but rather a single report prepared by a designated individual which can be duplicated as necessary. Every effort should be made to document investigative activity on ATF Reports of Investigation (ROI), unless otherwise agreed to by ATF and the participating agency(ies). This section does not preclude the necessity of individual TFOs to complete forms required by their employing agency.

Information will be freely shared among the TFOs and ATF personnel with the understanding that all investigative information will be kept strictly confidential and will only be used in furtherance of criminal investigations. No information gathered during the course of the Task Force, to include informal communications between TFOs and ATF personnel, may be disseminated to any third party, non-Task Force member, by any Task Force member without the express permission of the ATF Special Agent in Charge or his/her designee.

Any public requests for access to the records or any disclosures of information obtained by Task Force members during Task Force investigations will be handled in accordance with applicable federal statutes, regulations, and policies pursuant to the Freedom of Information Act and the Privacy Act, and other applicable federal and/or state statutes and regulations.

## BODY WORN CAMERAS AND TASK FORCE OFFICERS

In accordance with ATF Order 3020.4, dated June 2, 2022, and incorporated herein, Body Worn Cameras (BWCs) may be worn by TFOs operating on a federal Task Force when their parent agency mandates their use by personnel assigned to the Task Force. In such cases, the TFO and parent agency shall comply with all DOJ and ATF policies and the required procedures, documentation, and reporting while participating in the Task Force.

## USE OF FORCE

TFOs shall remain subject to their respective agencies' policies and shall report to their respective agencies regarding matters unrelated to this agreement/Task Force.

All TFOs will comply with ATF and the Department of Justice's (DOJ's) Use of Force orders and policies. TFOs must be briefed on ATF's and DOJ's Use of Force policy by an ATF official and will be provided with a copy of such policy.

## INVESTIGATIVE METHODS AND ELECTRONIC SURVEILLANCE

The parties agree that all investigative methods (including search warrants), evidence handling, and electronic surveillance (including wiretaps or consensual electronic monitoring) conducted by the Task Force will be consistent with and reviewed in accordance with applicable federal laws and regulations, as well as ATF and Department of Justice policy and guidelines. However, in situations where state or local consensual electronic monitoring laws are more restrictive than

comparable federal law, consensual electronic monitoring methods and procedures employed by state and local law enforcement agencies may conform to those requirements, pending a decision as to a venue for prosecution.

None of the parties to this MOU will knowingly seek investigations under this MOU that would cause a conflict with any ongoing investigation of an agency not party to this MOU. It is incumbent upon each participating agency to notify its personnel regarding the Task Force's areas of concern and jurisdiction. All law enforcement actions will be coordinated and cooperatively carried out by all parties to this MOU.

## EVIDENCE

Evidence will be maintained by the lead agency having jurisdiction in the court system intended for prosecution. Evidence generated from investigations initiated by a TFO or ATF special agent intended for federal prosecution will be placed in the ATF-designated vault, using the procedures set forth in ATF orders.

All firearms seized by a TFO must be submitted for fingerprint analysis and for a National Integrated Ballistic Information Network (NIBIN) examination. Once all analyses are completed, all firearms seized under federal law shall be placed into the ATF designated vault for proper storage. All firearms information/descriptions taken into ATF custody must be submitted to ATF's National Tracing Center.

## INFORMANTS

ATF guidelines and policy regarding the operation of informants and cooperating witnesses will apply to all informants and cooperating witnesses directed by TFOs.

Informants developed by TFOs may be registered as informants of their respective agencies for administrative purposes and handling. The policies and procedures of the participating agency for handling informants will apply to all informants that the participating agency registers. In addition, it will be incumbent upon the registering participating agency to maintain a file with respect to the performance of all informants or witnesses it registers. All information obtained from an informant and relevant to matters within the jurisdiction of this MOU will be shared with all parties to this MOU. The registering agency will pay all reasonable and necessary informant expenses for each informant that a participating agency registers.

## DECONFLICTION

Each participating agency agrees that the deconfliction process requires the sharing of certain operational information with the Task Force, which, if disclosed to unauthorized persons, could endanger law enforcement personnel and the public. As a result of this concern, each participating agency agrees to adopt security measures set forth herein:

a. Each participating agency will assign primary and secondary points of contact.
b. Each participating agency agrees to keep its points of contact list updated.

The points of contact for this Task Force are:

ATF: Resident Agent in Charge Nathan Sanchez, Oakland Field Office

Participating Agency: Lt. Gabriel Urquiza-Leibin

## JURISDICTION/PROSECUTIONS

Cases will be reviewed by the ATF Special Agent in Charge or his/her designee in consultation with the participating agency and the United States Attorney's Office and appropriate state's attorney offices, to determine whether cases will be referred for prosecution to the U.S. Attorney's Office or to the relevant state's attorney's office. This determination will be based upon which level of prosecution will best serve the interests of justice and the greatest overall benefit to the public. Any question that arises pertaining to prosecution will be resolved through discussion among the investigative agencies and prosecuting entities having an interest in the matter.

In the event that a state or local matter is developed that is outside the jurisdiction of ATF or it is decided that a case will be prosecuted on the state or local level, ATF will provide all relevant information to state and local authorities, subject to federal law. Whether to continue investigation of state and local crimes is at the sole discretion of the state or local participating agency.

## MEDIA

Media relations will be handled by ATF and the U.S. Attorney's Office's public information officers in coordination with each participating agency. Information for press releases will be reviewed and mutually agreed upon by all participating agencies, who will take part in press conferences. Assigned personnel will be informed not to give statements to the media concerning any ongoing investigation or prosecution under this MOU without the concurrence of the other participants and, when appropriate, the relevant prosecutor's office.

All personnel from the participating agencies shall strictly adhere to the requirements of Title 26, United States Code, § 6103. Disclosure of tax return information and tax information acquired during the course of investigations involving National Firearms Act (NFA) firearms as defined in 26 U.S.C., Chapter 53 shall not be made except as provided by law.

## SALARY/OVERTIME COMPENSATION

During the period of the MOU, participating agencies will provide for the salary and employment benefits of their respective employees. All participating agencies will retain control over their employees' work hours, including the approval of overtime.

ATF may have funds available to reimburse overtime to the state and local TFO's agency, subject to the guidelines of the Department of Justice Asset Forfeiture Fund. This funding would be available under the terms of a memorandum of agreement (MOA) established pursuant to the

provisions of 28 U.S.C. § 524. The participating agency agrees to abide by the applicable federal law and policy with regard to the payment of overtime from the Department of Justice Asset Forfeiture Fund. The participating agency must be recognized under state law as a law enforcement agency and their officers/troopers/investigators as sworn law enforcement officers. If required or requested, the participating agency shall be responsible for demonstrating to the Department of Justice that its personnel are law enforcement officers for the purpose of overtime payment from the Department of Justice Asset Forfeiture Fund. **This MOU is not a funding document.**

In accordance with these provisions and any MOA on asset forfeiture, the ATF Special Agent in Charge or designee shall be responsible for certifying reimbursement requests for overtime expenses incurred as a result of this agreement.

## AUDIT INFORMATION

Operations under this MOU are subject to audit by ATF, the Department of Justice's Office of the Inspector General, the Government Accountability Office, and other Government-designated auditors. Participating agencies agree to permit such audits and to maintain all records relating to Department of Justice Asset Forfeiture Fund payments for expenses either incurred during the course of this Task Force or for a period of not less than three (3) years and, if an audit is being conducted, until such time that the audit is officially completed, whichever is greater.

## SEIZURES/FORFEITURES/EQUITABLE SHARING

All assets seized for federal administrative forfeiture will be seized and forfeited in compliance with federal law and U.S. Department of Justice policy as set forth in the Asset Forfeiture Policy Manual. When the size or composition of the item(s) seized makes it impossible for ATF to store the property, in coordination with the U.S. Marshals Service, any of the participating agencies having the storage facilities to handle the seized property agree to store the property at no charge land to maintain the property in the same condition as when it was first taken into custody. The agency storing said seized property agrees not to dispose of the property until authorized to do so by ATF.

Federal law authorizes the Attorney General to share federally forfeited property with participating state, local, or tribal law enforcement agencies. The Attorney General's equitable sharing authority is discretionary. Any sharing of the net proceeds from forfeitures will be shared, with sharing percentages based upon the U.S. Department of Justice equitable sharing policies as set forth in the *Guide to Equitable Sharing for State, Local, and Tribal Law Enforcement Agencies* (March 2024) (the "*Guide*").

For additional information on equitable sharing, participating agencies should refer to the *Guide.*

## DISPUTE RESOLUTION

In cases of overlapping jurisdiction, the participating agencies agree to work in concert to achieve the Task Force's goals and objectives. The parties to this MOU agree to attempt to

resolve any disputes regarding jurisdiction, case assignments, and workload at the lowest level possible.

## LIABILITY

ATF acknowledges that the United States is liable for the wrongful or negligent acts or omissions of its officers and employees, including TFOs, while on duty and acting within the scope of their federal employment, to the extent permitted by the Federal Tort Claims Act, 28 U.S.C. §§ 1346(b), 2671-2680.

Claims against the United States for injury or loss of property, personal injury, or death arising or resulting from the negligent or wrongful act or omission of any federal employee while acting within the scope of his or her office or employment are governed by the Federal Tort Claims Act, (unless the claim arises from a violation of the Constitution of the United States, or a violation of a statute of the United States under which other recovery is authorized).

Except as otherwise provided, the parties agree to be solely responsible for the negligent or wrongful acts or omissions of their respective employees and will not seek financial contributions from the other for such acts or omissions. Legal representation by the United States for individual capacity claims is determined by the United States Department of Justice on a case-by-case basis. ATF cannot guarantee the United States will provide legal representation to any state or local law enforcement officer.

Liability for any negligent or willful acts of any agent or officer undertaken outside the terms of this MOU will be the sole responsibility of the respective agent or officer and agency involved.

## DURATION

This MOU is effective for five years from the date of the final signature.

This MOU supersedes previously signed MOUs and shall remain in effect until the aforementioned expiration date or until it is terminated in writing (to include electronic mail and facsimile), whichever comes first. All participating agencies agree that no agency shall withdraw from the Task Force without providing ninety (90) days' written notice to the other participating agencies. If any participating agency withdraws from the Task Force prior to its termination, the remaining participating agencies shall determine the distributive share of assets for the withdrawing agency, in accordance with Department of Justice guidelines and directives.

This MOU shall be deemed terminated at the time all participating agencies withdraw, and ATF elects not to replace such members, or in the event ATF unilaterally terminates the MOU upon 90 days' written notice to all the remaining participating agencies.

## MODIFICATIONS

This agreement may be modified at any time by written consent of all participating agencies. Modifications shall have no force and effect unless such modifications are reduced to writing and signed by an authorized representative of each participating agency.

## SIGNATURES

James P. Beere / 7/31/2025

James P. Beere Date
Chief of Police
Oakland Police Department

_____ /_____

John Wester Date
Special Agent in Charge, ATF
San Francisco Field Division

ATF and the partner agency agree to the provisions set forth in this agreement.

| Printed Name of Special Agent in Charge | Signature of Special Agent in Charge | Date |
|---|---|---|

| Printed Name of Partner Agency Representative and Name of Partner Agency | Signature of Partner Agency Representative | Date |
|---|---|---|

**OR**

Due to state and/or local law(s) requiring recording outside the parameters of this agreement, ATF and the partner agency agree to the provisions set forth in this agreement along with the revised language detailed in, *ATF TFO BWC MOU Addendum-Appendix A*.

| Printed Name of Special Agent in Charge | Signature of Special Agent in Charge | Date |
|---|---|---|
| JAMES P. BEERE | James P. Beere | 7/31/2026 |

Printed Name of Partner Agency Representative and Name of Partner Agency

Signature of Partner Agency Representative Date

Attachment: ATF TFO BWC MOU Addendum-Appendix A

## Addendum to Task Force Agreements Pertaining to Body Worn Cameras

This addendum supplements the agreement between the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) and the partner agency establishing an ATF sponsored Task Force. Pursuant to the Bureau of Alcohol, Tobacco, Firearms and Explosives Task Force Officer Use of Body-Worn Camera (BWC) Policy, the partner agency has advised ATF that it will require its deputized officers participating in the Task Force to use Body Worn Cameras (BWCs). This addendum governs that use.

The parties hereby agree to the following:

I. TFOs will adhere to ATF's Standard Operating Procedures for Task Force Officer Body Camera Program, and other applicable ATF policies and procedures.

II. The partner agency confirms that prior to executing this agreement it has provided to ATF details regarding the BWC system and cameras, including the details of any system protections, and any state or local policies or laws applicable to the TFO's use of BWCs, including any retention policies as detailed in Attachment 1 – Agency Checklist.

III. Use of BWCs During ATF Federal Task Force Operations:

A. Deputized Task Force Officers (TFO) through the Joint Law Enforcement Operations (JLEO) Program will be allowed to wear and activate their recording equipment with BWCs for the purposes of recording their actions only during:

1. A planned attempt to serve an arrest warrant or other planned arrest; or
2. The execution of a search warrant.

B. TFOs are authorized to activate their BWCs upon approaching a premises or a subject, and must deactivate their BWCs when the scene is secured as determined by the federal supervisor on the scene as designated by the ATF.

1. For purposes of this agreement, the term "secured" means that the scene is safe and under law enforcement control.
2. In the event circumstances arise requiring additional law enforcement assistance to secure the scene, the TFO will end BWC recording when relieved from the scene by another law enforcement agency.
3. If there are unanticipated interactions with the public or other exigent circumstances, such as contentious or violent interactions that could lead to the use of force, TFO's will, if and when it is safe to do so, reactivate their BWC either before, during, or after a planned arrest or execution of a search or seizure warrant or order.
4. For the execution of a search warrant, BWCs should not be used for searches of property lawfully in government custody or control, or a search to obtain digital or electronic records executed by a third party, such as an electronic service provider or custodian of electronic records.

C. TFOs will follow the provisions set forth in this agreement for use of BWCs, and the provisions of this agreement will supersede any conflicting provision in the agency's policy for TFOs while serving on the ATF Federal Task Force.

D. TFOs may use BWCs in accordance with this policy anywhere they are authorized to act as a police or peace officer under state, local, territorial or tribal law.

E. TFOs may use only agency-issued and agency-owned BWCs. TFOs will not be allowed to use any privately owned BWC or other recording device of any kind.

F. In the event a TFO's BWC is not working or inoperable due to a technical problem or cannot be used due to physical damage, and, in the judgement of the Task Force supervisor, delaying the operation to repair or obtain a replacement BWC is not practical or would impair the operation, the TFO may participate in the operation without using a BWC.

G. Even when BWC use would be permissible in the circumstances set forth in Section III A above, TFOs are prohibited from recording:

1. Undercover personnel;
2. Confidential informants or confidential sources;
3. On-scene witness interviews prior to or after the operation;
4. Personnel using specialized investigative techniques or equipment; or
5. Actions by any non-law enforcement persons at the scene who are assisting law enforcement personnel prior to or after the operation.

H. Even when BWC use would be permissible in the circumstances set forth in Section III A above, TFOs are prohibited from activating their BWC if in the judgment of the ATF the cases involve:

1. National security (including international and domestic terrorism investigations or cases involving classified information);
2. Public corruption;
3. Medical facilities; or
5. Other sensitive investigations as determined by ATF.

I. Even when BWC use would be permissible in the circumstances set forth in Section III A above, TFOs shall not use BWCs to record any activities related to:

1. Specialized or sensitive investigative techniques;
2. In a sensitive area; or
3. An undercover or covert status on behalf of the ATF Federal Task Force.

IV. Partner Agency Internal Controls:

A. Partner Agency Chief/Sheriff or a Departmental Designee will serve as a point-of- contact (POC) for ATF on BWC matters.

B. The partner agency will notify ATF of any change in state or local law that will modify how ATF TFOs must use BWCs or will affect release or redaction of BWC recordings from TFO BWCs made while working under federal authority on behalf of ATF ("TFO BWC recordings"), see Appendix A.

C. The partner agency will notify ATF of any change in agency policy that will affect the storage, release, or redaction of TFO BWC recordings.

D. The partner agency will familiarize ATF Task Force personnel on the BWCs, specifically concerning their capabilities and operation during task force activities.

V. Handling of BWC Recordings Made During Task Force Operations:

A. For purposes of this agreement, the term "TFO BWC recordings" refers to audio and video recordings, and associated metadata, from TFO BWCs made while the TFO is working under federal authority.

B. In accordance with current agency policy and practice, the partner agency will provide full, un-redacted copies of TFO BWC recordings to ATF within 72 hours unless approved in writing by the ATF SAC.

C. TFOs will document BWC use and the existence of BWC recordings in the Report of Investigation (ROI). The TFO will include in the ATF ROI a statement attesting that the data provided is a fair and accurate copy of the data recorded by the BWC.

D. All TFO BWC recordings made during ATF Federal Task Force operations, including such recordings retained by the the partner agency and/or in the possession of any third party engaged by the partner agency to store or process BWC recordings, shall be deemed federal records of the United States Department of Justice, Bureau of Alcohol, Tobacco, Firearms and Explosives (DOJ/ ATF) pursuant to the Federal Records Act.

E. Internal Dissemination:
The TFO's partner agency is authorized to use TFO BWC recordings for internal investigations of its personnel consistent with the partner agency's policies and procedures, not involving dissemination outside the partner agency or public release. The parent agency shall provide written notification to ATF prior to any internal review.

F. Expedited Public Release:
All TFO BWC recordings made during ATF Federal Task Force operations are federal records and shall be retained and disseminated in accordance with all applicable federal laws, policies and procedures including the Federal Records Act, Freedom of Information Act, and/or the Privacy Act. All TFO BWC recordings made during ATF Federal Task Force operations will be provided to ATF. The Department will work to expedite the public release of BWC recordings depicting conduct resulting in serious bodily injury or death of another consistent with DOJ policies and subject to any redactions as appropriate. If a TFO partner agency plans to release TFO BWC recording(s) from a BWC issued by the partner agency that depict conduct committed solely by a TFO resulting in serious bodily injury or death of another, the TFO's partner agency shall notify ATF, providing as much advance notice as possible as to the time and manner of its release. Following the notification, the TFO's partner agency may release such recording(s), subject to any redactions as appropriate.
If a TFO partner agency plans to release TFO BWC recording(s) from a BWC issued by the partner agency that depict conduct committed solely by an ATF agent resulting in serious bodily injury or death of another, the TFO's partner agency shall notify and coordinate the release with ATF, providing as much advance notice as possible as to the time and manner of its release. Following the notification, the TFO's partner agency may release such recording(s), subject to any redactions as appropriate.

G. In all circumstances, TFO BWC recordings shall be treated as law enforcement sensitive information, the premature disclosure of which could reasonably be expected to interfere with enforcement proceedings, and as potential evidence in a federal investigation, subject to applicable federal laws, rules, and policy concerning

disclosure or dissemination (including but not limited to 28 C.F.R. Ch. 1, Pt. 16, Subpart B, "Touhy", absent appropriate redaction prior to disclosure or dissemination). Accordingly, these recordings are deemed privileged absent appropriate redaction prior to disclosure and may be entirely exempt from public release under federal laws, rules and policies.

H. If a TFO BWC recording involves a use of force incident to include: a shooting incident, any incident involving serious bodily injury or death, or where any enforcement action by ATF resulted in the use of force or deadly force; physical assault or attempted physical assault on a Law Enforcement Officer; intentional damage to any facility, conveyance or any property owned by ATF, or involves another time-sensitive or urgent situation, the partner agency will provide ATF copies on an expedited basis, including during non-business hours. For purposes of this provision, use of force incidents include, but are not limited to, incidents utilizing intermediate weapons, i.e., TASERs, expandable batons, kinetic energy projectiles, emergency/improvised intermediate impact weapons, such as, a flashlight or radio; any use of force resulting in serious injury or death; canine bites resulting in penetration of human skin; and all shooting incidents.

I. The partner agency will provide witnesses as needed to authenticate TFO recordings in ATF cases.

J. The partner agency will inform ATF of the length of time TFO BWC recordings will be retained by the agency before deletion. The partner agency will honor any request by ATF to retain the TFO BWC recordings for a longer period of time.

K. The partner agency will notify ATF immediately of any unauthorized access to TFO recordings discovered by the agency.

L. The partner agency will cooperate fully with ATF in the investigation of any unauthorized access to or disclosure of TFO recordings, including providing ATF the name(s) of any agency personnel determined by the agency to be involved in unauthorized access, copying, or disclosure.

M. The partner agency's failure to comply with any part of this addendum may result in immediate termination of the Task Force Memorandum of Understanding.

N. The partner agency will notify ATF as soon as possible regarding any request or demand for release or disclosure of TFO recordings, including but not limited to subpoenas, discovery demands or motions, open record/freedom of information requests, media requests, or union or other professional association requests.

**Bureau of Alcohol, Tobacco, Firearms and Explosives**

**Body Worn Camera Program**

# TFO BWC MOU ADDENDUM
## Appendix A

The following is controlling guidance for situations that may affect a Task Force (TF) partner agency regarding the TFO (Task Force Officer) BWC (Body Worn Camera) MOU (Memorandum of Understanding) Addendum. This guidance is issued by the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) Body Worn Camera Program (BWCP) and ATF Office of Chief Counsel (CC):

- **Review Boards/Other Public Dissemination:** If an agency is under a consent decree or otherwise required by statute, law, or agreement to disclose BWC footage to a review board, that entity and their access to the agency BWC and the qualifying events or incidents that are the subject of the agreement will be described in a letterhead memo that the ATF will keep in the BWC MOU tracking system. The memo should include the timeline for that board to receive the footage, if their access to an agency BWC Video Retention System is direct or indirect, and whether the review board has independent/unilateral public disclosure authority. This information will assist the ATF Chief Counsel in determining what timeline they may be under to perform agency review if a qualifying incident occurs where TFO and/or ATF BWC footage has been recorded.

- **State/Local Law(s):** If state law or statute requires recording outside the parameters of ATF TFO BWC MOU Addendum, the agency will provide that information and a copy of the legal justification to the ATF BWCP. Any recording of events outside of the TFO enforcement action (i.e., medical facilities, prisoner transport) should be separated if possible. This separation can be achieved by deactivating the recording of the TFO BWC prior to re-activation of recording upon the start of an ATF enforcement action, and/or deactivating the recording of the TFO BWC when a scene is concluded and secure. The TFO can then reactivate recording when the officer is operating under their agency policy alone for a non-TFO agency responsibility. When separate recording(s) are possible, ATF will receive only the enforcement BWC recording. If deactivation and reactivation of recording are not feasible or are not permitted by state law, the entire recording will be shared with ATF with the understanding that ATF will, if necessary, redact the entire portion of any recording that shows the TFO performing an agency duty where they are not operating under the ATF Task Force (TF) MOU parameters for enforcement actions. If a partner agency TFO BWC has the technical capability to apply a marker during a recording, the TFO will apply the marker at the beginning and end of the enforcement action, if feasible.

- **Short term operations:** Any TF partner agency not covered by an existing executed ATF TFO BWC MOU Addendum and any non-partner state, local, federal, or tribal agency are authorized to utilize their BWC during an ATF short term operation or ATF led national initiative after agreeing to share any BWC footage obtained during the operation with the ATF upon request. Any BWC footage of a critical incident such as an Officer Involved Shooting or other use of force leading to death will be shared as soon as possible after the incident. Other footage will only be requested if the ATF has a mission-related requirement that can only be supported by receipt of the BWC recording from the BWC agency.

DEPARTMENTAL GENERAL ORDER

**I-34: Vehicle Digital Forensic Technology**

Effective Date: DD MMM 26

Coordinator: Vehicle Digital Forensic Coordinator, Criminal Investigations Division

---

The purpose of this policy is to establish guidelines for the Oakland Police Department's use of vehicle digital forensic technology, for the purpose of furthering the Department's public safety mission through successful criminal investigation and apprehension.

## A. PURPOSE OF TECHNOLOGY

Vehicle digital forensic technology supports Oakland Police Department investigations by allowing investigators to extract and analyze data stored in vehicle electronic systems, such as infotainment and telematics systems. An infotainment system is the user-facing interface in a vehicle that provides navigation, media, hands-free calling, and device connectivity features. A telematics system is the embedded hardware and software that collects and transmits vehicle operational data, such as location, speed, and diagnostic information. All modern vehicles contain a telematics system. Infotainment systems are present in many but not all vehicles, depending on the make, model, and trim level. When authorized, this technology allows investigators to recover evidence of vehicle use, identify devices that were connected to the vehicle and associated user data, reconstruct where a vehicle has been, and establish timelines of events related to criminal activity. The use of this technology is intended to further legitimate law enforcement objectives while complying with applicable department, legal, and constitutional requirements.

## B. DESCRIPTION OF THE TECHNOLOGY

Vehicle digital forensic technology is a combination of hardware and software tools used to extract and analyze data stored in a vehicle's infotainment and telematics systems. The technology connects to vehicle systems through the vehicle's diagnostic port, by direct connection to internal components, or by removing and examining system modules. Extracted data is processed using forensic software on a computer operated by authorized OPD personnel.

The data that can be recovered includes historical data such as GPS and navigation history, travel routes, saved and recent locations, known or prior devices connected to the vehicle through Bluetooth, Wi-Fi, or USB, contact lists, call logs, text messages, media files, and vehicle event data such as door openings, ignition activity, and seatbelt use, along with associated dates and times. The types and amount of data available will vary based on the vehicle's make, model, year, and what systems are installed. The data extracted is only from the onboard system(s) on the vehicle.

This technology does not provide real-time monitoring or tracking of a vehicle. It recovers data already stored by the vehicle's own systems. Regardless of the vendor or platform used, all vehicle digital forensic examinations by OPD are governed by the same legal standards, authorization requirements, departmental policies, and city ordinances applicable to surveillance technologies.

## C. AUTHORIZED USE

Vehicle digital forensic technology may be used only as part of an active criminal investigation and only when authorized by a search warrant compliant with the California Electronic Communications Privacy Act (CalECPA), codified at California Penal Code section 1546 et seq. Any extraction and retention of data from a vehicle's electronic systems requires a search warrant that specifies the vehicle and systems to be examined and the types of data to be extracted.

Only OPD personnel assigned to, or directly assisting with, the specific investigation for which the vehicle digital forensic examination is authorized may access or utilize the technology. Access to extracted data shall be limited to personnel with a legitimate right to know and a need to know based on their assigned investigative role. Extracting, retaining, or reviewing data by personnel not assigned to or assisting with the investigation, or outside the scope of the authorized purpose, is prohibited.

Exigent use of vehicle digital forensic technology may occur only when exigent circumstances are present as defined by the California Electronic Communications Privacy Act (CalECPA). Exigent circumstances are situations where there is an immediate danger of death or serious bodily injury to any person, or where delay in obtaining a warrant would result in the loss of critical evidence related to such danger, consistent with Penal Code section 1546.1(c)(6).

Exigent use requires approval from an OPD commander at the rank of lieutenant or above.

If a vehicle digital forensic examination is conducted under exigent circumstances, a post hoc search warrant must be sought as soon as practicable and no longer than within three court days after obtaining the electronic information, and must document the facts establishing probable cause and the exigent circumstances justifying the examination and any data obtained, pursuant to Penal Code section 1546.1(h). The Vehicle Digital Forensic Coordinator is to be notified of any exigent examinations.

After an exigent use of vehicle digital forensic technology, if OPD is not able to obtain a post hoc search warrant, the Vehicle Digital Forensic Coordinator shall provide a report of the circumstance to the Privacy Advisory Commission at the next scheduled meeting.

## D. DATA COLLECTION

Vehicle digital forensic technology collects data stored in a vehicle's infotainment and telematics systems, including historical GPS and navigation history, travel routes, saved and recent locations, connected devices, contact lists, call logs, text messages, media files, vehicle event data, and associated dates and times. Data is extracted by connecting forensic hardware to the vehicle's systems and processed using forensic software operated by authorized OPD personnel.

The data collected is limited to what is stored by the vehicle's own electronic systems. The technology does not intercept communications in real time, does not enable live monitoring or tracking, and does not access data from external sources such as cloud accounts or cellular networks.

## E. DATA ACCESS

Access to vehicle digital forensic data is limited to OPD investigators or OPD personnel assisting with ongoing criminal investigations. Extracted data may be accessed only for legitimate law enforcement purposes and in a manner consistent with the scope of the applicable search warrant.

Data extracted during an authorized examination may be accessed by OPD investigators or OPD personnel assisting with ongoing criminal investigations for review and analysis. Data is made available through the forensic software used to conduct the examination or through a Department approved evidence management system such as Axon Evidence.com.

Vehicle digital forensic data is not accessed, reviewed, or shared for purposes unrelated to lawful law enforcement activities. Any access or disclosure of extracted data must comply with applicable law, court orders, and Department policy. Unauthorized access or use of vehicle digital forensic data is prohibited.

## F. DATA PROTECTION

Vehicle digital forensic data is stored on the computer used to conduct the examination and within the forensic software platform during the period of active use. The coordinator shall ensure that the computer and its contents are properly protected according to best practices for cybersecurity. Access to the forensic software and extracted data is limited to authorized OPD personnel for investigative purposes related to an active criminal investigation.

At the conclusion of the extraction, the investigator reviews the data and identifies information relevant to the authorized scope of the investigation. Vehicle digital forensic data is either deleted from the forensic software platform or preserved by exporting the data into a Department approved law enforcement evidence management system, such as Axon Evidence.com, when the data is needed for a criminal prosecution or other lawful purpose. When necessary, data may also be stored on a physical medium protected by a password to limit access. Data that is not needed for evidentiary or investigative

purposes is deleted and not retained. The deletion of non-evidentiary data is the primary safeguard against the retention of information that falls outside the scope of the authorized investigation.

## G. DATA RETENTION

Vehicle digital forensic data that is not identified as relevant to a lawful criminal investigation is retained for no longer than thirty days from the date of extraction and is deleted thereafter. This retention period applies to data stored on the forensic examination computer or within the forensic software platform and is intended to limit the retention of data that does not have an investigative or evidentiary purpose.

If vehicle digital forensic data is determined to be relevant to a lawful criminal investigation, prosecution, or court proceeding, the data may be retained for the duration of the legal process. Such data is retained only while the associated criminal matter is pending and is deleted after full adjudication of the court proceeding, including any right to appeal. Data is not retained beyond this period unless otherwise required by law or court order.

## H. PUBLIC ACCESS

Data that is collected and retained under this policy is considered a "law enforcement investigatory file" pursuant to Government Code § 7923.600(a) and shall be exempt from public disclosure. Members of the public may request data via public records request pursuant to applicable law regarding Public Records Requests as soon as the criminal or administrative investigation has concluded and/or been adjudicated.

## I. THIRD PARTY DATA SHARING

Vehicle digital forensic data is not shared outside the Oakland Police Department absent proper legal authority. Any sharing of vehicle digital forensic data with another law enforcement agency or prosecuting authority requires a CalECPA compliant search warrant, a court authorized sharing order, or a discovery requirement arising from a criminal prosecution. Informal requests or requests made without supporting legal documentation are not sufficient.

Any outside agency requesting vehicle digital forensic data must submit a written request to OPD identifying the legal authority for the request and the investigative or prosecutorial need for the data. The request and OPD's response shall be documented and retained in accordance with Department policy. When legally authorized, data is shared only to the extent permitted by the applicable warrant, court order, or discovery obligation and remains subject to the handling, retention, and protection requirements set forth in this policy.

## J. TRAINING

The Vehicle Digital Forensic Coordinator shall be certified in vehicle digital forensics by the vendor or an equivalent accredited training provider prior to conducting examinations. The coordinator shall maintain current certification and complete any continuing education requirements associated with the certification.

The coordinator is responsible for training other OPD personnel authorized to use the technology. Training shall cover this policy, the legal requirements governing its use including the California Electronic Communications Privacy Act (CalECPA) and related case law, the operation of the hardware and software, proper evidence handling procedures, and data retention obligations.

OPD personnel shall not conduct vehicle digital forensic examinations until they have been trained by the coordinator. Supervisory personnel involved in approving or overseeing the use of vehicle digital forensic technology should receive training sufficient to ensure compliance with this policy and applicable law.

The coordinator is responsible for tracking training completion and maintaining associated training records.

## K. AUDITING AND OVERSIGHT

The vehicle digital forensic coordinator is appointed by the Captain of the Criminal Investigation Division (CID). The coordinator is responsible for tracking all uses of vehicle digital forensic technology by OPD. This includes maintaining a record of each examination, the associated investigation, the legal authority authorizing the use, and the scope of data extracted. The coordinator ensures that each use of the technology is connected to a CalECPA compliant search warrant or a documented exigency, followed by a post hoc search warrant.

An annual use report shall be submitted in accordance with Oakland Municipal Code. This report may include aggregate usage information, audit results, and demographic data such as race information when required for reporting purposes. Public reportable information is limited to non-investigative data and does not include case specific or personally identifiable information.

## L. MAINTENANCE

The vehicle digital forensic coordinator is responsible for ensuring that vehicle digital forensic data is managed in accordance with the Data Protection and Data Retention sections of this policy. This includes ensuring that data stored on forensic examination computers, physical media, or Department approved evidence management systems is handled consistently with policy requirements.

The coordinator is also responsible for coordinating with the vendor, when necessary, to address technical issues related to the hardware or software. Maintenance of the technology is limited to vendor supported processes and does not include modification of the technology by OPD personnel.

By Order of

James Beere

Interim Chief of Police

Date Signed:

# Drug Enforcement Administration

# State and Local Law Enforcement Agency

# Memorandum of Agreement

This agreement is made this 29 day of July, 20 26, between the United States Department of Justice, Drug Enforcement Administration (hereinafter "DEA"), and the Oakland Police Department (hereinafter "parent agency"), ORI# CA0010900; Unique Entity Identifier (UEI#) GBDMTM5J75R6. The DEA is authorized to enter into this cooperative agreement concerning the use and abuse of controlled substances under the provisions of 21 U.S.C. § 873.

WHEREAS there is evidence that trafficking in narcotics, dangerous drugs, controlled-substance pharmaceuticals, and/or listed chemicals exists in the Greater East Bay Area of California area and that such illegal activity has a substantial and detrimental effect on the health and general welfare of the people of Greater East Bay Area of California, the parties hereto agree to the following:

1. The San Francisco Field (DEA Division) will perform the activities and duties described below:
   a. Disrupt the illicit drug traffic in the Greater East Bay Area of California area by immobilizing targeted violators and trafficking organizations;
   b. Investigate, gather and report intelligence data relating to trafficking in narcotics and dangerous drugs, trafficking of controlled pharmaceuticals and/or listed chemicals; and
   c. Conduct undercover operations where appropriate and engage in other traditional methods of investigation in order that the DEA Division's activities will result in effective prosecution before the courts of the United States and the State, Commonwealth, or Territory of California.
   d. Investigate, disrupt and dismantle individuals and/or organizations involved in diversion schemes (e.g., "doctor shopping," prescription forgery, and prevalent retail-level violators) of controlled pharmaceuticals and/or listed chemicals in the Greater East Bay Area of California area; if applicable.
2. To accomplish the objectives of the DEA Division, the parent agency agrees to detail experienced officer(s) to the DEA Division for a period of not less than

two years.[1] During this period of assignment, the parent agency officer(s) will be under the direct supervision of DEA supervisory personnel assigned to the DEA Division.

3. The parent agency officer(s) assigned to the DEA Division shall adhere to all DEA policies and procedures. Failure to adhere to DEA policies and procedures shall be grounds for dismissal from the DEA Division. Failure to complete mandatory DEA training within the required timeframe shall be grounds for dismissal from the DEA Division.

4. In instances where parent agency policy or state/local law imposes a requirement that is not addressed in DEA policy, the parent agency will promptly notify DEA and provide DEA with written copies of the applicable law and/or policy. Whether the parent agency officer will comply with parent agency policy in such instances will be at the discretion of DEA.

5. The parent agency officers assigned to the DEA Division shall be deputized as Task Force Officers pursuant to 21 U.S.C. § 878.

6. To accomplish the objectives of the DEA Division, DEA will assign Special Agent(s) and/or Diversion Investigator(s), if applicable, to the DEA Division. Other support to DEA office(s), including any overtime reimbursement, is funded on the basis of whether the group is DEA Program Funded, Fee Funded (SPEAR), or HIDTA Funded.

    a) **DEA Program Funded** - To accomplish the objectives of the DEA Division, DEA will assign DEA Special Agent(s) to the DEA Division and up to One (1) Task Force Officer(s). The parent agency agrees to provide and maintain a vehicle for use for each of its assigned Task Force Officers. DEA will also, subject to the availability of annually appropriated funds or any continuing resolution thereof, provide necessary funds and equipment to support the activities of the DEA Special Agent(s) and parent agency officer(s) assigned to the DEA Division. This support will include: office space; office supplies; travel funds; funds for the purchase of evidence and information; investigative equipment; training; and other investigative support items.

    b) **Synthetics Precursors Enforcement and Regulations (SPEAR) (Fee Funded)** - DEA will, subject to the availability of annual Diversion Control Fee Account (DCFA) funds, provide necessary funds, vehicles, and equipment to support the activities of the DEA Special Agent(s) and up to Zero (0) Task Force Officer(s) assigned to the DEA Division. This support will include: vehicles; office space; office supplies; travel funds; funds

[1] The number of officers assigned cannot exceed the number of positions allocated by the Division's Table of Organization.

for the purchase of evidence and information; investigative equipment; training; and other investigative support items, as available DCFA funds permit. While on duty and acting on DEA's business, the parent agency officer(s) assigned shall be subject to all DEA and federal government rules, regulations and procedures governing the use of Official Government Vehicles (OGVs) and home to work transportation when authorized. Accidents involving vehicles while in use for DEA Division purposes shall be reported and investigated in accordance with the procedures of DEA and the parent agency.

c) **High Intensity Drug Trafficking Areas (HIDTA) (HIDTA Funded)** - Subject to the availability of funding, and HIDTA planning and budgeting guidance, HIDTA will provide funding to support the activities of Federal Special Agents, and up to Zero (0) Task Force Officer(s), and other specified employees (if any). This support will include: office space; office supplies; travel funds; funds for the purchase of evidence and information; investigative equipment; training; and other investigative support items. The parties to this agreement understand that financial reimbursement to participating organizations is subject to the budgeting, administrative and managerial decisions of the HIDTA Executive Board, as well as the availability of HIDTA funding (from whatever source).

Vehicles may be provided by the parent agency or furnished by DEA subject to the availability and approval of HIDTA funding for vehicle leases. DEA may request that HIDTA fund installation and removal of mobile radios in DEA Division vehicles and reimburse the parent agency for fuel, maintenance, and repair attributable to use of the vehicles for DEA Division purposes. Accidents involving vehicles while in use for DEA Division purposes shall be reported and investigated in accordance with the procedures of DEA and the parent agency.

While on duty and acting on DEA's business, the parent agency officer(s) assigned to the HIDTA group shall be subject to all DEA and federal government rules, regulations and procedures governing the use of OGV and home to work transportation when authorized.

d) **DEA Provisional -** DEA will also, subject to the availability of annually appropriated funds or any continuing resolution thereof, provide necessary funds and equipment to support the activities of the DEA Special Agent(s) and up to Zero (0) Task Force Officer(s) assigned to the DEA Division. This support will include: office space; office supplies; travel funds; funds for the purchase of evidence and information; investigative equipment; training; and other investigative support items. DEA does not reimburse for Provisional TFO overtime, and vehicles must be provided by the parent agency. Although DEA does not normally reimburse for Provisional

TFO overtime, TFOs may be eligible to receive overtime from eligible funding sources, subject to the availability of funds.

7. During the period of assignment to the DEA Division, the parent agency will remain responsible for establishing the salary and benefits, including overtime, of the officer(s) assigned to the DEA Division, and for making all payments due to them. DEA will, subject to availability of funds, reimburse the parent agency for overtime payments. Annual overtime for each state and local law enforcement officer is capped at the equivalent to 25% of the salary of a GS-12, step 1, of the general pay scale for the rest of the United States. Reimbursement for all types of qualified expenses shall be contingent upon availability of funds and submission of a proper request for reimbursement, which shall be submitted monthly on a fiscal year basis, and which provides the name of each officer(s) who incurred overtime in support of DEA investigations during invoiced period to include the number of overtime hours incurred, the hourly regular and overtime rates in effect for each officer, and the total cost for the invoiced period. If HIDTA funded, HIDTA will, subject to availability of annually appropriated funds, reimburse the parent agency for overtime payments incurred by its Task Force Officers. Each invoice submitted must include an **invoice number** and **invoice date**. The parent agency will bill overtime as it is performed, and no later than **30 days** after the end of each month in which the overtime is performed. The parent agency will submit invoices to San Francisco (DEA Division) process coordinator email box (Invoice.Sanfrancisco@dea.gov). ***Note: Task Force Officer's overtime "shall not include any costs for benefits, such as retirement, FICA, and other expenses including taxes."***

8. In no event will the parent agency charge any indirect cost rate to DEA for the administration or implementation of this agreement.

9. The parent agency shall maintain on a current basis complete and accurate records and accounts of all obligations and expenditures of funds under this agreement in accordance with generally accepted accounting principles and instructions provided by DEA to facilitate on-site inspection and auditing of such records and accounts.

10. The parent agency shall permit and have readily available for examination and auditing by DEA, the United States Department of Justice, the Comptroller General of the United States and any of their duly authorized agents and representatives, any and all records, documents, accounts, invoices, receipts, or expenditures relating to this agreement. The parent agency shall maintain all such reports and records until all audits and examinations are completed and resolved, or for a period of six (6) years after termination of this agreement, whichever is later.

11. The parties acknowledge and understand that the United States of America is liable for the wrongful actions or inactions of Federal employees, including those Federal employees deputized as Task Force Officers, who are acting within the scope of their employment under the Federal Torts Claim Act (2 8 U.S.C §§ 2671 – 2680). This may extend to representation of the covered employee if in the best interests of the United States (28 C.F.R. § 50.15(a)(2)). A state or local employee participating in the DEA group may concurrently or separately be covered for the purposes of liability by their employer.

12. The parent agency shall comply with Title VI of the Civil Rights Act of 1964, Section 504 of the Rehabilitation Act of 1973, the Age Discrimination Act of 1975, as amended, and all requirements imposed by or pursuant to the regulations of the United States Department of Justice implementing those laws, 28 C.F.R. Part 42, Subparts C, F, G, H and I.

13. The Parent Agency's signature to this agreement certifies the Parent Agency's compliance with the certifications required under 2 C.F.R. Part 2867 (Nonprocurement Debarment and Suspension); 28 C.F.R. Part 69 (New Restrictions on Lobbying); and 28 C.F.R. Part 83 (Government-Wide Requirements for Drug-Free Workplace). DEA awards Federal funds under this cooperative agreement in reliance upon the Parent Agency's certification of compliance with these requirements. The Parent Agency has accordingly reviewed these regulations.

14. When issuing statements, press releases requests for proposals, bid solicitations, and other documents describing projects or programs funded in whole or part with federal money, the parent agency shall clearly state: (1) percentage of the total cost of the program or project which will be financed with federal money; and (2) the dollar amount of federal funds for the program or project.

15. The term of this agreement shall be effective from the date in paragraph number one until September 30, 2031. This agreement may be terminated by either party on thirty (30) days' advance written notice. DEA's support to the DEA Division, including reimbursement of overtime, is subject to the availability of funds on a fiscal year basis (October 1 through September 30 of the next year). Billing for all outstanding obligations must be received by DEA within 30 days of the end of the fiscal year or within 30 days of the date of termination of this agreement. DEA will be responsible only for obligations incurred by parent agency during the term of this agreement on a fiscal year basis, subject to the availability of funds.

**For the Drug Enforcement Administration:**

| | |
|---|---|
| | San Francisco |
| Special Agent in Charge | Division |
| Bob P. Beris | |
| Printed Name | Date |

**For the Parent Agency:**

| | |
|---|---|
| | |
| Agency Head | Date |
| | |
| Printed Name and Title | |

[END OF DOCUMENT]

DEPARTMENTAL GENERAL ORDER

**I-25: Unmanned Aerial System (UAS) — Field-Based and Drone as First Responder (DFR)**

Effective Date: Day Month Year
Coordinator: Program Coordinator, Special Operations Division (SOD); Electronic Services Unit

---

The Oakland Police Department believes in protecting and serving its diverse community and city through fair, equitable, and constitutional policing. OPD believes in the usage of technology to aid in this mission and in the investment in Unmanned Aerial Systems (UAS), or better known as "Drones," to help improve public safety while still protecting community members' privacy rights. This includes a multipronged approach related to tactics, methodology, and technology that allows for de-escalation in often rapidly evolving situations. These fleets will never replace the police officers who have sworn to protect the community, but will assist in mitigating use of force, bring safe resolutions to critical incidents, and help save lives. OPD is committed to safeguarding and respecting the privacy of the community and has brought measures and policies in place to ensure none are violated. Regardless of deployment — whether Field-Based or Drone as First Responder (DFR) — UAS will be utilized in accordance with OPD Core Values and our Mission.

This policy provides guidance for the deployment, capture, storage, and use of digital data obtained through the use of Unmanned Aerial System (UAS) technology, including both the Department's Field-Based UAS program and its Drone as First Responder (DFR) program, while recognizing the established privacy rights of the public.

**Program Overview: Field-Based UAS and DFR**

This policy governs two distinct UAS deployment models used by the Department. Except where this policy specifically distinguishes between the two programs (see Sections D, F, and N), all provisions apply equally to both.

- **Field-Based UAS:** A trained member of the police department transports a UAS in a department vehicle, responds to the location where deployment is needed, and deploys the UAS on scene. Field-based deployment requires case-by-case authorization from an Incident Commander, as described in Section D-1 (Field-Based).
- **Drone as First Responder (DFR):** DFR Systems are stationed at fixed Launch Sites throughout the city and are dispatched automatically to qualifying calls for service via CAD. The DFR RPIC operates from a static location at the Real-Time Operations Center (RTOC) and does not travel to the scene, as described in Section D-1 (DFR). When technologically capable, control of a field-deployed UAS may be transferred to RTOC for continued remote piloting.

**A. Definitions**

This section defines the technical terms, personnel roles, and key concepts used throughout this policy.

For the purposes of this DGO, refer to Appendix A for definitions.

**B. Description**

This section describes the Unmanned Aerial System (UAS) technology, including its core components and how it operates.

An Unmanned Aerial System (UAS) is an unmanned aircraft of any type that is capable of sustaining directed flight, whether preprogrammed or remotely controlled (commonly referred to as a "Drone"), and all of the supporting or attached components designed for gathering information through imaging, recording, or any other means. Generally, a UAS consists of:

**B-1. UAS Components**

- A UAV, composed of:
  - Chassis with several propellers for flight
  - Control propellers and other flight stabilization technology (e.g. accelerometer, a gyroscope)
  - Radio frequency and antenna equipment to communicate with a remote-control unit
  - A computer chip for technology control
  - A camera, with thermal imaging capabilities
  - A digital image/video storage system for recording onto a digital data memory card or, where equipped, directly to a Flight Management Platform (FMP)
  - A removable speaker (Field-Based UAS)
  - A remote-control unit (Field-Based UAS)
  - Battery charging equipment for the aircraft and remote control
- A Docking Station (Drone-in-a-Box), for DFR-equipped systems, composed of:
  - Automated docks positioned at fixed locations across the city that keep the UAS charged and ready 24/7
  - Remote launch and recovery systems enabling instant launch upon a 9-1-1 call, call for service, or request, without a pilot being physically present at the site

**B-2. How the System Works**

1. The FAA Modernization and Reform Act of 2012 provides for the integration of civil unmanned aircraft systems into national airspace by September 1, 2015.

2. Field-Based UAS are controlled from a remote-control unit on scene. Drones can be controlled remotely, often from a smartphone or tablet. Wireless connectivity lets pilots view

the drone and its surroundings from a birds-eye perspective. Users can also leverage apps to pre-program specific GPS coordinates and create an automated flight path for the drone. Another wirelessly enabled feature is the ability to track battery charge in real time, an important consideration since drones use smaller batteries to keep their weight low.

3. DFR UAS are launched from a Docking Station and controlled remotely by an RPIC from the Real-Time Operations Center (RTOC). Unlike field-deployed UAS, the DFR RPIC is not physically present at the launch site; a Visual Observer (or ADS-B technology, per Section A) supports situational awareness at the launch site itself. RTOC monitors Computer-Aided Dispatch (CAD) and can direct a UAS to a call for service, often arriving in advance of ground units, using CAD-linked coordinates to pre-program an automated flight path to the incident location. The Docking Station tracks the UAS's battery charge in real time, ensuring the aircraft remains charged and ready for immediate launch.

4. UAS have cameras so the pilot can view the aerial perspective in real time, and, where equipped, may live-stream that view to authorized Department members as described in Section G.

5. UAS use secure digital (SD) memory cards to record image and video data, or, where equipped with a Flight Management Platform (FMP), data will be recorded and stored through the FMP. Data stored via SD card can be removed from the UAS after flights to input into a computer for evidence. Data stored via FMP may only be accessed by authorized personnel using an individual username and password. Integration with OPD's digital evidence management system preserves chain of custody and simplifies secure evidence management, backed by CJIS-compliant infrastructure trusted across public safety.

**B-3. Human Oversight of Automated Features**

While a UAS may incorporate some level of autonomous flight-assistance features (similar to the autopilot on conventional aircraft) designed to assist in the flight and management of the system, decision-making related to the deployment or dispatch of a UAS shall always be dictated and directed by human operators.

**C. Purpose**

The specific purpose(s) that the surveillance technology is intended to advance (OMC § 9.64.010.16.A).

UAS will been used to save lives and protect property and can detect possible dangers that cannot otherwise be seen, providing critical context related to rapidly evolving situations. UAS can support first responders in hazardous incidents that would benefit from an aerial perspective, and have applications in locating and apprehending subjects, missing persons, and search and rescue operations, as well as task(s) that can best be accomplished from the air in an efficient and effective manner. This makes UAS a key component of de-escalation, as a UAS Operator has the capacity to facilitate elements of time, distance, and cover for responding resources, while maintaining the ability to make observations that continuously inform teams on the ground. Because DFR Systems are strategically stationed at established locations throughout the city, they are also uniquely positioned to assist with mitigating vehicle pursuits and conducting high-risk area searches. The primary role of DFR is to provide aerial assistance with City-wide Patrol

Operations while the primary role of the Field Based UAS is to provide additional real time intelligence and officer safety during critical incidents.

The Department also recognizes that UAS have the capability of assisting with community safety efforts beyond the role of law enforcement and intends to facilitate the use of UAS to assist the Oakland Fire Department and other partnering emergency services in their public safety functions.

UAS may not always be ideal for deployment and alternatives should always be considered prior to deployment.

**D. Authorized Use**

The specific uses that are authorized, and the rules and processes required prior to such use (OMC § 9.64.010.16.B).

**D-1. Authorized Use**

1. Any use of a UAS will be in strict accordance with constitutional and privacy rights and Federal Aviation Administration (FAA) regulations. UAS operations should be conducted in accordance with FAA approval.

2. Only authorized operators who have completed the required training shall be permitted to operate a UAS.

**Field-Based UAS**

Field-Based UAS may only be used for the following specified situations:

a. Mass casualty incidents (e.g. large structure fires with numerous casualties, mass shootings involving multiple deaths or injuries);

b. Disaster management;

c. Missing or lost persons;

d. Hazardous material releases;

e. Sideshow events where many vehicles and reckless driving is present;

f. Rescue operations;

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

h. Training;

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

i. Barricaded suspects;

ii. Hostage situations;

iii. Armed suicidal persons;

iv. Arrest of armed and/or dangerous persons (as defined in OPD DGO J-04 “Pursuit Driving” Appendix B, H “Violent Forcible Crime”);

v. Operational pre-planning [prior planning for services of search and arrest warrants. This would provide up-to-date intelligence (e.g. terrain, building layout) so that personnel allocate appropriate resources and minimize last minute chance encounters and uses of force]; and

vi. Service of high-risk search and arrest warrants involving armed and/or dangerous persons (as defined in OPD DGO J-04 "Pursuit Driving" Appendix B, H "Violent Forcible Crime"); and

vii. Exigent circumstances — A monitoring commander (Lieutenant or above) may authorize a UAS deployment under exigent circumstances as defined in OPD DGO K-03 "Exigent Circumstances." A report shall be completed and forwarded to the Chief of Police and the Field-Based UAS Coordinator for all deployments authorized under exigent circumstances, for a full review to determine policy compliance.

**Drone as First Responder (DFR)**

DFR Systems are intended to assist with field operations by responding quickly to calls for service, critical incidents, active investigations, and public safety emergencies. The primary role of the DFR System is to provide aerial assistance with City-wide Patrol Operations".

DFR are only used to:

a. Respond to calls for service, including critical incidents and public safety emergencies, to provide real-time information on scene conditions.

b. Assess lower-priority calls for service to determine whether a law enforcement response is required.

c. Assist field units conducting preliminary investigations or engaged in enforcement actions

d. Support an active investigation, when approved in advance by a supervisor and consistent with any applicable warrant requirement.

The DFR System shall give precedence to Priority 1 calls for service. As later defined, a call for service is classified as Priority 1 when it is determined to be life-threatening.

**D-2. Deployment Authorization**

**Field-Based UAS**

a. Deployment of a Field-Based UAS shall only be for the authorized uses above and require the authorization of the incident commander, who shall be of the rank of Lieutenant of Police or above.

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

ESU Operators are encouraged to advise a supervisor or incident commanders when they believe they are incapable of operating a UAS in a safe manner.

**Drone as First Responder (DFR)**

Unlike Field-Based UAS, DFR System deployment does not require case-by-case authorization from an incident commander. DFR Systems are dispatched by the RPIC in response to qualifying calls for service via CAD, consistent with the priority framework described in Section D-1. RPICs are encouraged to advise a supervisor or RTOC when they believe they are incapable of operating a DFR System in a safe manner.

**D-3. Deployment Logs**

**Field-Based UAS**

a. A commander authorizing deployment of a UAS shall send notification of the deployment via the military equipment deployment notification process.u

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

c. Flight logs will provide all mission deployment details for each flight and may be made available via the Department's public transparency portal, if maintained, as described in Section J (Public Access).

**Drone as First Responder (DFR)**

a. Each DFR System deployment shall be automatically logged by the Flight Management Platform (FMP) upon launch.

b. The Flight Log shall be maintained by RTOC and ESU and kept on file for FAA record-keeping purposes, consistent with Section A.

c. Flight logs will provide all mission deployment details for each flight and may be made available via the Department's public transparency portal, if maintained, as described in Section J (Public Access).

**D-4. Privacy Considerations**

a. Operators and observers shall adhere to FAA altitude regulations.

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

**D-5. Communications**

Notifications will be made to the Communications Section for notifying patrol personnel when UAS operations are authorized by a Commander (Field-Based), or when a DFR System is dispatched to their area via CAD (DFR).

**E. Restrictions on Use**

This section identifies uses of UAS technology that are expressly prohibited, in addition to the authorized uses described in Section D.

**E-1. Permitted/Impermissible Uses**

Department personnel may only access and use the UAS consistent with this Policy. Accessing data collected by the UAS requires a right to know and a need to know. A right to know is the legal authority to receive information pursuant to a state or federal statute, applicable case law, or a court order. A need to know is a compelling reason to request information such as involvement in an active investigation.

Recordings retained by the Department related to criminal investigations are the property of the Oakland Police Department. The following uses of the UAS are specifically prohibited:

- **Invasion of Privacy:** See Section D-4 (Privacy Considerations).
- **Harassment or Intimidation:** It is a violation of this Policy to use the UAS with the intent to harass and/or intimidate any individual or group.
- **Use Based on a Protected Characteristic:** It is a violation of this policy to use a UAS to target a person or group solely because of a person's, or group's, race, gender, religion, political affiliation, nationality, ethnicity, sexual orientation, disability, or other classification protected by law.
- **Facial Recognition:** It is a violation of this policy for Department members to use UAS in conjunction with Facial Recognition technology.
- **Analytics and Object Tracking:** It is a violation of this policy for Department members to use a UAS in conjunction with any analytics or tracking technology capable of identifying or selectively tracking specific groups or individuals, including but not limited to gait analysis or motion-activated object tracking technology.
- **Weapons Platform:** It is a violation of this Policy to equip a UAS with a weapons system.
- **Personal Use:** It is a violation of this Policy to use the UAS or associated data for any personal purpose.
- **First Amendment Rights:** It is a violation of this policy to use the UAS or associated data for the intended purpose of infringing upon First Amendment rights.
- **Conducting Surveillance:** It is a violation of this Policy to use the UAS to conduct surveillance outside the scope of an authorized use under this Policy.
- **Immigration Enforcement:** In accordance with OPD/City of Oakland Policy and California State Law, OPD shall not use UAS to assist with immigration enforcement.

**F. 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 (OMC § 9.64.010.16.C).

UAS may live-stream and record photographic and videographic data utilizing mounted camera systems, together with associated flight and image metadata (e.g., location, altitude, and timestamp information), as further described in Section A. The UAS operator will rely on SD cards for video recordings, or, where the UAS is equipped with a Flight Management Platform (FMP), data will be recorded and stored through the FMP. Data stored via FMP may only be

accessed by authorized personnel using an individual username and password. Following the designated retention period, any data determined to be evidence related to an investigation shall be stored separately through the Department's Evidence.com storage platform.

UAS technology does not rely on open source data or external data feeds; all data collected under this section originates directly from the UAS itself.

**Field-Based UAS**

The video recording function of a Field-Based UAS shall be activated immediately upon deployment (take off) and deactivated upon completion of the UAS deployment (landing) and subject to the requirements of D-4 b. Privacy Considerations.

*Note: Unlike DFR System deployments, which involve transit from a fixed launch site to the operational area, Field-Based UAS are launched at or near the scene of deployment. Because there is no comparable transit phase over uninvolved areas, the horizon-orientation requirement applicable to DFR System transit (see below) does not apply to Field-Based UAS operations.*

**Drone as First Responder (DFR)**

The video recording function of a DFR System shall be activated upon arrival at the operational area and repositioning of the camera from the horizon-oriented transit position described below and deactivated upon completion of the mission at the operational area, prior to the DFR System's return transit to the Docking Station.

To mitigate potential invasions of privacy, DFR UAS cameras, if possible, shall be oriented toward the horizon while the UAS is in transit to and from the operational area. Camera repositioning or deviation from this requirement is permitted under exigent circumstances, including but not limited to situations where immediate observation is necessary to support active law enforcement operations, such as when a suspect is actively fleeing in the direction of the UAS.

**G. Data Access**

The category of individuals who can access or use the collected information, and the rules and processes required prior to access or use of the information (OMC § 9.64.010.16.D.).

**General Data Access Guidelines**

Department sworn personnel, police service technicians, crime analysts, or other authorized/designated Department personnel may use the data captured by UAS technology related to investigations. Authorized/designated users other than sworn personnel, crime analysts, or PSTs must be designated by the Chief of Police or designee.

Data stored on a Flight Management Platform (FMP) may only be accessed by authorized personnel using an individual username and password, and all such access shall be logged by username, date, and time.

**Real-Time Live Feed Access**

UAS access is controlled within the Department to provide robust community safety capabilities while also ensuring privacy safeguards are present. By assigning access based on roles and

responsibilities, sensitive footage can be restricted to authorized personnel, reducing the risk of misuse or breaches. This approach balances transparency, accountability, and privacy protection.

Authorized Department members may live-stream real-time video to any member of the Department (with a need-to-know, right-to-know) when such access may assist in operational awareness, decision-making, or response coordination. This includes, but is not limited to, incidents where the real-time (live) video can support establishing time and distance from subjects to lessen the potential for uses of force, maximizing the use of available cover, facilitating de-escalation efforts, or enhancing situational awareness during critical incidents, emergencies, or large-scale events such as natural disasters, mass casualty incidents, or search and rescue operations.

During critical incidents where an Emergency Operations Center (EOC) activation is required, members of the City assigned to duties within the EOC may have access to the live feeds of DFR to assist in their duties. The EOC acts as the central hub for coordinating emergency preparedness, response, and recovery activities across the city during critical incidents and live feeds of the DFR may assist personnel to accomplish such missions. **H. Data Protection**

The safeguards that protect information from unauthorized access, including encryption and access control mechanisms (OMC § 9.64.010.16.F).

All data shall be safeguarded and protected by both procedural and technological means. OPD shall observe the following safeguards regarding access to and use of stored data:

- For Field-Based UAS: all UAS video data recorded via SD card shall be uploaded to the Department's Flight Management Platform (FMP) as soon as practicable following the deployment; where equipped, a UAS may record directly to the FMP in lieu of an SD card.
- All evidence from UAS deployments — whether originally recorded via SD card or directly via FMP — shall ultimately be maintained on the FMP preserving chain of custody through the platform's CJIS-compliant infrastructure.
- All FMP server data shall be accessible only through a login/password-protected system capable of documenting all access to, review of, copying of, and deletion of UAS data by username, date, and time. Audit logs of access, review, copying, and deletion of UAS data shall be retained permanently.
- All data shall be accessed via a Department-approved, securely connected device.

The Program Coordinator shall develop procedures to ensure that all UAS data — whether originally recorded via SD card or FMP — intended to be used as evidence is accessed, maintained, stored, and retrieved in a manner that ensures its integrity as evidence. These procedures include strict adherence to chain of custody requirements.

Electronic trails, including encryption, authenticity certificates, and date and time stamping, are inherent to the FMP's evidentiary management system and shall be maintained to preserve individual rights and to ensure the authenticity and maintenance of a secure evidentiary chain of custody.

DRAFT

**I. Data Retention**

The time period, if any, for which information collected by the surveillance technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s), the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond that period (OMC § 9.64.010).

Video recording and associated metadata collected by OPD UAS — whether stored via SD card or Flight Management Platform (FMP) — shall be retained thirty (30) days and deleted on the thirtieth day unless:

1. The recording is needed for a criminal investigation;
2. The recording is related to a City of Oakland Police department administrative investigation (Internal Affairs Investigation).

A thirty (30) day retention period is appropriate to further the purposes described in Section C, as it provides sufficient time for a supervisor, investigator, or the RPIC to identify and flag footage of evidentiary or investigative value, while limiting the length of time that footage of uninvolved persons or non-evidentiary incidents is retained. Upon expiration of the thirty (30) day period, video recordings and associated metadata not flagged for retention under subsections 1 or 2 above will be purged from the Flight Management Platform (FMP), or, for SD card data not uploaded to FMP, deleted by the Program Coordinator or designee.

The Program Coordinator shall develop procedures to ensure that data are retained and purged in accordance with applicable record retention schedules. See Appendix B for the Department's category-specific data retention schedule.

**J. Public Access**

How collected information can be accessed or used by members of the public, including criminal defendants (OMC § 9.64.010).

UAS data which is collected and retained under Section I of this policy is considered a "law enforcement investigatory file" pursuant to Government Code § 7923.600, and shall be exempt from public disclosure while the related investigation remains active. Non-investigatory and otherwise non-exempt UAS records shall be disclosed in response to a public records request. UAS data retained for investigatory purposes shall become available via public records request as soon as the related criminal or administrative investigation has concluded and/or been adjudicated. Requests for information by non-law enforcement or non-prosecutorial agencies will be processed in accordance with Government Code § 7920 et seq., this policy, and applicable case law and court orders.

Criminal defendants may obtain access to UAS data through the criminal discovery process set forth in Penal Code § 1054 et seq. See Section K for the specific channels through which such access is provided.

**Public Records Requests for UAS Data Copies**

Public records requests for UAS data shall be accepted and processed in accordance with the provisions of federal, state, and local statutes and DGO M-09.1, Public Records Access, and forwarded to the Program Coordinator. Copies of UAS data released pursuant to a public records

request, or as authorized by the Chief of Police or designee, shall be redacted as required by prevailing law and Department procedure prior to release. Redaction for release shall not alter the original UAS data maintained by the Department for evidentiary or investigatory purposes.

The Department may maintain a publicly accessible transparency portal through which UAS flight logs are published to promote accountability and public awareness. Such flight logs shall be made available no sooner than thirty (30) days following the date of the recorded operation. The Department reserves the right to withhold or delay publication of any flight log that is determined to be associated with an active or ongoing investigation, or where disclosure would otherwise be restricted pursuant to applicable law or this policy.

**K. Third Party Data Sharing**

If and how other city departments, bureaus, divisions, or non-city entities can access or use the information, including any required justification or legal standard necessary to do so and any obligations imposed on the recipient of the information (OMC § 9.64.010.16.H).

UAS recorded data is not shared outside the Oakland Police Department absent proper legal authority or exigent circumstances. Routine sharing of UAS recorded data with another law enforcement agency or prosecuting authority requires a search warrant, a court order, or a discovery requirement arising from a criminal prosecution, including requests from a Public Defender's Office or criminal defense attorney made via the District Attorney's Office in accordance with applicable California criminal discovery laws. See Section J for a description of how criminal defendants may access UAS data through this process. Informal requests or requests made without supporting legal documentation are not sufficient.

In the routine course, any outside agency requesting UAS recorded data must submit a written request to OPD identifying the legal authority for the request and the investigative or prosecutorial need for the data. The request and OPD's response shall be documented and retained in accordance with Department policy. When legally authorized, data is shared only to the extent permitted by the applicable warrant, court order, or discovery obligation and remains subject to the handling, retention, and protection requirements set forth in this policy.

Nothing in this section prevents the release of UAS recorded data when disclosure is required by the California Public Records Act.

The Oakland Police Department does not permit the sharing of UAS data gathered by the city or its contractors/subcontractors for the purpose of federal immigration enforcement, pursuant to the California Values Act (Government Code § 7282.5; Government Code § 7284.2 et seq.) — these federal immigration agencies include Immigration and Customs Enforcement (ICE) and Customs and Border Protection (CBP).

**L. Training**

The training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology (OMC § 9.64.010.16.I).

The Special Operations Commander, ESU Unit Supervisor, or (for DFR) RTOC Commander, or other designated OPD personnel, under the direction of the Program Coordinator, shall ensure

that all authorized operators and required observers have completed all required FAA and department-approved training in the operation, applicable laws, policies and procedures regarding use of the UAS.

The Special Operations Commander, ESU Unit Supervisor, or (for DFR) RTOC Commander, or other designated OPD personnel, under the direction of the Program Coordinator, shall develop an operational procedure manual governing the deployment and operation of a UAS including, but not limited to, safety oversight, use of visual observers, establishment of lost link procedures, and secure communication with air traffic control facilities.

**M. Auditing and Oversight**

The mechanisms to ensure that the Surveillance Use Policy is followed, including internal personnel assigned to ensure compliance with the policy, internal recordkeeping of the use of the technology or access to information collected by the technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the legally enforceable sanctions for violations of the policy (OMC § 9.64.010.16.J).

**M-1. Auditing and Oversight**

The Special Operations Commander, ESU Unit Supervisor, or (for DFR) RTOC Commander, or other designated OPD personnel, under the direction of the Program Coordinator, shall develop a protocol for documenting all UAS uses in accordance with this policy with specific regard to safeguarding the privacy rights of the community, and shall include this protocol in the UAS procedure manual and the annual UAS report. The Special Operations Commander, ESU Unit Supervisor, or RTOC Commander will develop an electronic record of time, location, equipment, purpose of deployment, and number of UAS personnel involved. Whenever a deployment occurs, the operator will send notification/submit (either electronically or in hard copy) to the Special Operations Commander, ESU Unit Supervisor, or RTOC Commander to include the topics listed above. This protocol will allow the Special Operations Commander, ESU Unit Supervisor, or RTOC Commander to maintain a running log of all deployments and assist in the annual report.

Login/Log-Out Procedure. To ensure proper operation and facilitate oversight of the UAS program, all users accessing the Flight Management Platform (FMP) or other UAS data systems shall be required to have individual credentials for access to and use of such systems and/or data, consistent with the access-logging requirements of Section H (Data Protection). This requirement does not apply to Field-Based UAS deployments that rely solely on SD card recording without FMP use. It is the responsibility of the Department to actively pursue software and hardware upgrades needed to maintain full compliance with this section.

The records of the number of UAS deployments, Third Party Data Sharing related to Section K, item 2, and any exigent use of UAS shall be incorporated into the annual report required by O.M.C. § 9.64 et seq.

UAS system audits shall be conducted annually to ensure proper system functionality and that designated personnel are using the system according to policy rules.

**M-2. Reporting**

The Special Operations Commander, ESU Unit Supervisor, or (for DFR) RTOC Commander, or other designated OPD personnel, under the direction of the Program Coordinator, shall monitor the adherence of personnel to established procedures and shall provide an annual report on the program to the Chief of Police. The Special Operations Commander, ESU Unit Supervisor, or RTOC Commander, or other designated OPD personnel, shall provide the Chief of Police, Privacy Advisory Commission, Public Safety Committee, and City Council with an annual report that contains a summary of authorized access and use.

**M-3. Inquiry and Complaint Process**

*(Government Code § 7070(d)(7)) For a law enforcement agency, the procedures by which members of the public may register complaints or concerns or submit questions about the use of each specific type of military equipment, and how the law enforcement agency will ensure that each complaint, concern, or question receives a response in a timely manner.*

DGO M-3 informs all employees and the public of procedures for accepting, processing, and investigating complaints concerning allegations of employee misconduct. Refer to DGO K-7 for additional information.

**N. Maintenance and Administration**

The mechanisms and procedures to ensure that the security and integrity of the surveillance technology and collected information will be maintained (OMC § 9.64.010.16.K).

**N-1. System Coordinator / Administrator**

The Field-Based UAS program and the DFR System program both fall under the Special Operations Division (SOD). The Special Operations Commander, and/or ESU Unit Supervisor, will appoint a Program Coordinator, who holds overall responsibility for both the Field-Based UAS and DFR System programs and ensures that policies and procedures conform to current laws, regulations, and best practices across both.

The Program Coordinator will appoint a Field-Based UAS Coordinator and a DFR System Coordinator, each of whom reports to the Program Coordinator and is responsible for the day-to-day management of their respective program.

**Field-Based UAS**

The Field-Based UAS program is commanded by the ESU Unit Supervisor. The Field-Based UAS Coordinator manages day-to-day Field-Based UAS operations.

**Drone as First Responder (DFR)**

The DFR System program is housed within the Real-Time Operations Center (RTOC) and supervised by the RTOC Commander. The DFR System Coordinator manages day-to-day DFR operations, with the assistance of the RTOC Commander, including ensuring systems and processes are in place for the proper collection and retention of DFR System data.

DRAFT

**N-2. FAA Certificate of Waiver or Authorization (COA)**

COA (Certificate of Authorization) given by the FAA which grants permission to fly within specific boundaries and perimeters. The Program Coordinator will maintain current COA's consistent with FAA regulations. The Special Operations Commander, ESU Unit Supervisor, or (for DFR) RTOC Commander shall coordinate the application process and ensure that the COA is current.

If a UAS mission requires flying beyond visual line of sight (BVLOS), a Part 91 BVLOS Certificate of Waiver (CoW) must also be obtained. The Program Coordinator shall maintain current BVLOS waivers consistent with FAA regulations, and the Special Operations Commander, ESU Unit Supervisor, or (for DFR) RTOC Commander shall coordinate the application process to ensure the waiver remains current.

**N-3. Program Improvements**

The Special Operations Commander, ESU Unit Supervisor, or (for DFR) RTOC Commander, or other designated OPD personnel, shall recommend and accept program improvement suggestions, particularly those involving safety and information security.

**N-4. Maintenance**

The Special Operations Commander, ESU Unit Supervisor, or (for DFR) RTOC Commander, or other designated OPD personnel, shall develop a UAS inspection, maintenance, and record-keeping protocol to ensure continuing airworthiness of a UAS — including, for DFR, operational readiness of Docking Station infrastructure — and include this protocol in the UAS procedure manual. Maintenance and record-keeping should also include expenditures such as purchase of new equipment and mechanical repairs.

**N-5. Cost Analysis**

The Special Operations Commander, ESU Unit Supervisor, or (for DFR) RTOC Commander, or designated OPD personnel, shall develop a protocol for developing and documenting data for a cost-benefit analysis. This cost-benefit analysis will include the amount of UAS personnel involved (operators/RPICs and visual observers), UAS equipment utilized, suspect(s) located (e.g., gender, race, and age), and the recovery of evidentiary items (e.g., firearms, clothing, vehicles, etc.).

By Order of

**James P. Beere**

Chief of Police Date Signed: XXXXXX

DRAFT

**Appendix A — Definitions**

For the purposes of this DGO, the following definitions apply:

**A-1. Unmanned Aerial System (UAS) —** An unmanned aircraft of any type that is capable of sustaining directed flight, whether preprogrammed or remotely controlled, together with all of the supporting or attached components designed for gathering information through imaging, recording, or any other means. A UAS is commonly referred to as a "drone."

**A-2. Drone as First Responder (DFR) —** A deployment model in which UAS are stationed at fixed Launch Sites throughout the city and dispatched, often automatically, to calls for service, arriving before traditional emergency responders to provide real-time aerial situational awareness. DFR technology is intended to assist Department members [and other critical Emergency Medical Services (EMS responders] by allowing select trained Department members to respond to an incident to assess conditions, identify potential hazards, provide potential opportunities for de-escalation, support decision-making, and improve the safe and efficient deployment of resources in relation to an investigation or critical incident.

**A-3. Remote Pilot in Command (RPIC) —** The RPIC, a FAA-certified remote pilot, is the member of the Department who has completed the required training and is designated to have final authority over a UAS flight. This includes the power to initiate, continue, or terminate a flight based on real-time safety conditions. For Field-Based UAS, the RPIC controls the UAS from the remote-control unit on scene and is responsible for its safe operation; RPICs are assigned to the Electronic Services Unit are also referred to as ESU Operators. For DFR, the RPIC operates the UAS remotely from the Real-Time Operations Center (RTOC), providing real-time updates to field resources and command personnel.

**A-4. Visual Observer —** A trained member who assists the operator by maintaining visual awareness of the UAS and the surrounding airspace during flight and who supports safe operation and compliance with FAA requirements. A Visual Observer (VO) is not required when the UAS is equipped with Automatic Dependent Surveillance-Broadcast (ADS-B) technology providing equivalent airspace awareness.

**A-5. Electronic Services Unit (ESU) —** The unit within the Special Operations Division responsible for the UAS program, including the maintenance, storage, and security of UAS equipment and data, and for coordinating authorized law-enforcement access to UAS data.

**A-6. Program Coordinator —** The member responsible for managing the agency's UAS program and ensuring that policies and procedures conform to current laws, regulations, and best practices. The Field-Based UAS Coordinator and the DFR System Coordinator report to the Program Coordinator.

**A-7. Field-Based UAS Coordinator —** The member responsible to the Program Coordinator for managing Field-Based UAS operations.

**A-8. DFR System Coordinator —** The member responsible to the Program Coordinator for managing the Drone First Responder system.

**A-9. Incident Commander —** The command-level officer who authorizes the deployment of a Field-Based UAS for an authorized use. Rank requirements and the exigent-circumstances exception are set out in Section D-2 (Field-Based).

**A-10. Real-Time Operations Center (RTOC) —** The designated facility within OPD from which teleoperators conduct DFR operations, monitor Computer-Aided Dispatch (CAD), and coordinate with Communications. Also referred to as the DFR Operations Center.

**A-11. Exigent Circumstances —** Those circumstances that would cause a reasonable person to believe that a particular action is necessary to prevent physical harm to an individual, the destruction of relevant evidence, or the escape of a suspect, as defined in OPD DGO K-03.

**A-12. FAA Certificate of Waiver or Authorization (COA) —** An authorization issued by the Federal Aviation Administration (FAA) granting permission to operate a UAS within specific boundaries and parameters. The Program Coordinator maintains current COAs consistent with FAA regulations.

**A-13. Secure Digital (SD) Memory Card —** The removable digital memory card on which UAS image and video data are recorded. SD cards may be removed from the UAS after a flight for use as evidence. SD cards are used for Field-Based UAS; DFR Systems record directly to the Flight Management Platform (FMP).

**A-14. Flight Log —** The record of details from each UAS deployment, maintained by ESU and kept on file for FAA record-keeping purposes, that provides the deployment details for each flight.

**A-15. Flight Management Platform (FMP) —** A software platform designed to facilitate the ability of an RPIC to manage the flight of a UAS, visualize its trajectory, and provide obstacle/aircraft avoidance. FMPs also facilitate the requisite data streams related to the use of the camera, live stream video feed, flight path information, and other diagnostic data relevant to the operation of the UAS.

**A-16. BVLOS (Beyond Visual Line of Sight) —** UAS operations conducted beyond the unaided visual range of the remote pilot or visual observer, as authorized under an FAA Certificate of Waiver (CoW) or Certificate of Authorization (COA), as applicable.

**A-17. CoW (Certificate of Waiver) —** A Part 91 Certificate of Waiver (CoW), issued by the FAA under 14 C.F.R. § 91.113, is a distinct FAA approval authorizing beyond visual line of sight (BVLOS) UAS operations. A CoW is processed separately from, and is not interchangeable with, a Certificate of Authorization (COA).

**A-18. Mounted Camera System —** UAS utilize a mounted camera system to allow an RPIC to observe, document, and relay the events occurring on the ground to responding Department members, partnering first responders, supervisory and command members, and other relevant stakeholders for the purpose of providing enhanced public safety.

**A-19. Automatic Dependent Surveillance-Broadcast (ADS-B) —** An advanced aviation surveillance technology that allows aircraft to determine their position using satellite navigation or other sensors and periodically broadcast this information. This data includes the aircraft's position, velocity, and other relevant information, which can be received by air traffic control (ATC) ground-based or satellite-based receivers. ADS-B consists of two main functions: ADS-B Out and ADS-B In.

- ADS-B Out: This function periodically broadcasts information about the aircraft, such as identification, current position, altitude, and velocity. This data is transmitted through an

onboard transmitter and provides real-time aircraft position information to air traffic controllers.

- ADS-B In: This function involves the reception and processing of ADS-B information transmitted by other aircraft. It allows pilots to view traffic information about surrounding aircraft, including altitude, heading, speed, and distance.

**A-20. Metadata —** Data describing other data collected by the UAS, including but not limited to image and video metadata (e.g., location, altitude, exposure time, resolution) and flight metadata (e.g., GPS coordinates, camera orientation, speed, battery status).

**A-21. DFR Launch Site —** A fixed, Department-authorized location equipped with drone-in-a-box infrastructure from which DFR drones are remotely launched and recovered.

**A-22. Drone-in-a-Box (DIB) —** An automated UAS housing and charging system that enables remote launch, operation, and recovery of a drone without a pilot physically present at the launch site.

**A-23. Mission —** Any DFR flight operation from launch to landing, regardless of whether the drone arrives on scene before ground units.

**A-24. Priority Call —** A call for service classified as Priority 1 (life-threatening) or Priority 2 (in-progress crime or urgent hazard) in OPD's CAD system.

DRAFT

**Appendix B — Data Retention Schedule**

| Category Name | Retention Period | Legal Retention Requirements |
|---|---|---|
| Violent Felony / DOA | Indefinite | Statute of Limitations (SOL) |
| Misdemeanor Case (including report, statements, cite, or arrest) | 2 yrs | SOL |
| Felony Case (including report, statements, cite, or arrest — no violent felonies or sex crimes) | 3 yrs | SOL |
| Missing Person / Runaway | Indefinite | SOL (Possible homicide) |
| Sex Crimes | Indefinite | SOL |
| Vehicle Pursuit | 5 yrs | Administrative SOL |
| Sergeants / Commanders Admin | 2 yrs | Possible IA/DLI — intake/Sergeant/etc. to update category if so |
| IA/DLI | Indefinite | Administrative SOL |
| Use of Force — Levels 1 and 2 | Indefinite | Administrative SOL |
| Use of Force — Levels 3 and 4 | Indefinite | Administrative SOL |
| Felony — Filed by DA | 20 yrs | SOL plus appeals |
| Homicide | Indefinite | SOL |
| Misdemeanor — Filed by DA | 10 yrs | SOL plus appeals |
| Legal — OCA/Records/Authorized Users Only | Indefinite | City Attorney's Office (CAO) Order |
| Collision — 901C | Indefinite | CAO Order |
| Collision — Major Injury / Fatal | Indefinite | SOL |

DRAFT

# Surveillance Impact Report
# Unmanned Aircraft Systems (UAS)
# Oakland Fire Department

---

## A. Description

An Unmanned Aircraft System (UAS), commonly referred to as a drone, consists of an unmanned aircraft and the associated equipment necessary for its operation. A UAS generally includes the aircraft, remote controller or ground control station, communications equipment, flight-control systems, cameras or other approved sensors, batteries, software, and supporting equipment.

UAS are remotely operated by trained Department personnel and provide an aerial perspective that can assist emergency responders in assessing conditions that may be difficult, dangerous, or impossible to observe from ground level.

Depending upon the equipment utilized, OFD UAS may be capable of providing still photography, digital video, thermal imagery, mapping imagery, and three-dimensional imagery. These capabilities can provide Incident Commanders and emergency responders with real-time or recorded information to assist with emergency operations, incident management, investigations, planning, and other authorized Department functions.

UAS manufacturer/model and specific sensor package: To be determined through the Department's equipment evaluation and procurement process.

## B. Purpose

OFD proposes to use UAS to enhance firefighter and public safety, improve situational awareness, support emergency response and incident management, assist in protecting life and property, and provide aerial documentation associated with authorized Department operations.

Emergency incidents may expose firefighters and other responders to fire, structural instability, hazardous materials, difficult terrain, water hazards, and other dangerous environments. UAS may allow personnel to obtain information about these conditions without unnecessarily placing responders into hazardous areas solely to obtain visual information.

UAS may be utilized for authorized Department purposes including:

- Structure fires
- Vegetation and wildland fires
- Hazardous materials incidents
- Technical rescue operations
- Urban Search and Rescue incidents
- Water rescue operations
- Missing or lost person searches

- Disaster response and recovery
- Damage assessment
- Fire investigations and post-fire origin and cause documentation
- Scene documentation
- Incident command support
- Pre-incident planning
- Infrastructure inspections conducted for Department purposes
- Emergency management
- Fire code inspections
- Public safety training and emergency preparedness exercises
- Community risk reduction activities
- Other incidents or events where aerial observation improves responder safety or incident management

The purpose of the OFD UAS program is not to conduct general surveillance. UAS will be deployed for specific, authorized Department missions consistent with the OFD UAS Policy.

**C. Location**

OFD UAS may be deployed throughout the City of Oakland when necessary to support an authorized Department mission.

UAS may also be deployed outside the City when OFD is providing mutual aid, participating in regional, state, or federal emergency response, supporting California Urban Search and Rescue Task Force 4 (CA-TF4), participating in authorized training or exercises, or otherwise performing an authorized Department function.

UAS deployment will be based upon a specific operational need and will not be used for routine monitoring of a particular neighborhood, population, group, or geographic area.

All UAS operations will be conducted in accordance with applicable Federal Aviation Administration requirements and other applicable federal, state, and local laws.

**D. Impact**

The Department recognizes that UAS equipped with cameras and other sensors have the potential to impact individual privacy and civil liberties.

UAS operations may incidentally capture images of individuals, residences, vehicles, private property, or activities unrelated to the authorized Department mission. The degree of potential privacy impact may vary depending upon factors including the location of the operation, aircraft altitude, camera or sensor capabilities, duration of the flight, and type of imagery collected.

OFD's UAS program is intended to support specific emergency response, public safety, training, inspection, investigation, and Department operational purposes and is not intended for general surveillance.

The OFD UAS Policy establishes restrictions governing authorized and prohibited uses, deployment authorization, privacy protections, data collection, access, protection, retention, and sharing to minimize potential impacts upon individual privacy and civil liberties.

**E. Mitigations**

OFD will employ operational, administrative, and technological measures to minimize potential impacts upon privacy and civil liberties.

UAS may be deployed only for legitimate and authorized Department purposes. General surveillance unrelated to a legitimate Department mission is prohibited.

Department personnel shall collect only information reasonably necessary to accomplish the authorized mission and shall make reasonable efforts to minimize the collection of information concerning uninvolved persons or locations.

Personnel shall avoid intentionally recording areas where individuals have a reasonable expectation of privacy unless recording is necessary to accomplish a lawful emergency response, rescue, investigation, or other authorized Department mission.

UAS shall not be used to monitor individuals or groups solely because of race, ethnicity, religion, national origin, gender, sexual orientation, disability, political beliefs, or constitutionally protected activities.

UAS shall not be used to conduct facial recognition, biometric identification, gait analysis, or other biometric surveillance prohibited by Oakland Municipal Code Chapter 9.64.

OFD UAS shall not carry or deploy weapons.

Access to live or stored UAS data shall be limited to authorized personnel with a legitimate Department business need.

UAS deployments and program operations shall be documented and subject to Department review and oversight as provided by the UAS Policy.

**F. Data Types and Sources**

Depending upon the UAS and approved sensor package utilized by OFD, UAS may collect:

- Still photographs
- Digital video
- Thermal imagery
- Mapping and orthomosaic imagery
- Three-dimensional imagery
- Flight telemetry and information concerning the operation of the aircraft

- Other sensor data approved as part of the Department's UAS program

The primary source of image and sensor data will be the cameras and sensors installed on or utilized by Department UAS.

UAS cameras and sensors shall be activated and utilized only in connection with authorized Department missions or training.

OFD does not propose to use UAS to collect biometric information or to conduct facial recognition, gait analysis, or predictive policing.

**G. Data Security**

Only authorized personnel with a legitimate Department business need shall have access to UAS data.

UAS data shall be stored and maintained using City-approved systems and appropriate administrative, physical, and technological safeguards designed to protect information from unauthorized access, disclosure, alteration, or loss.

Data associated with investigations or other matters requiring evidentiary preservation shall be maintained in a manner that protects the integrity of the information and preserves applicable chain-of-custody requirements.

UAS data shall not be disseminated except as authorized by Department policy and applicable law.

Data storage platform and security protocols: To be determined based upon the UAS equipment and data-management solution ultimately selected. Any system selected shall comply with applicable City information-security and privacy requirements.

Data Retention

UAS imagery, video, and associated data that have no identified evidentiary, investigative, operational, training, administrative, legal, or other official Department purpose shall be deleted within 30 days of collection.

UAS data determined to have evidentiary, investigative, operational, training, administrative, legal, or other official Department value shall be retained in accordance with the applicable City records retention schedule, Department policy, and applicable law.

This approach provides the Department a limited period to determine whether collected UAS data have a legitimate continuing Department purpose while ensuring that routine or incidental data without continuing value are not retained indefinitely.

## H. Fiscal Cost

The fiscal cost of establishing and maintaining the OFD UAS program will depend upon the equipment and supporting systems ultimately selected.

Potential costs include aircraft, cameras and thermal imaging equipment, batteries and charging equipment, controllers, software and licensing, data storage, training and certification, maintenance and repair, and related equipment.

Initial acquisition cost and anticipated annual operating cost: To be determined based upon the equipment, software, data-storage, training, maintenance, and supporting services ultimately selected through the Department's evaluation and procurement process.

Funding source: To be determined as part of the Department's procurement and budget process.

Any applicable contracts, ongoing subscription or licensing costs, and anticipated personnel costs will be identified as the UAS program and equipment selection are finalized.

## I. Third Party Dependence

OFD's dependence upon third parties will depend upon the aircraft, software, data-storage platform, and supporting services ultimately selected.

Potential third-party dependencies may include the UAS manufacturer, flight-control software provider, mapping or imagery-processing provider, data-storage provider, equipment maintenance or repair provider, and training providers.

UAS manufacturer/vendor, software provider, and data-storage provider: To be determined through the Department's equipment evaluation and procurement process. Prior to implementation, OFD will identify any third party that will receive, process, store, maintain, or otherwise have access to UAS data and ensure applicable privacy, security, contractual, and City requirements are addressed.

Before implementation, OFD will determine whether any third party will receive, process, store, maintain, or otherwise have access to information collected through the UAS program.

Any third-party access to or sharing of UAS data shall comply with the OFD UAS Policy, applicable City requirements, contractual privacy and security requirements, and applicable law.

## J. Alternatives

Alternatives to Department-operated UAS include ground-based observation, elevated observation from Department apparatus or structures, manned aircraft, fixed-camera systems, and requesting UAS assistance from other public safety agencies.

These alternatives remain available and may be appropriate depending upon the circumstances of an incident. However, they may not provide the same combination of rapid deployment, aerial perspective, thermal imaging capability, accessibility, and ability to gather information without unnecessarily exposing personnel to hazardous conditions.

Ground-based observation may be limited by terrain, buildings, smoke, fire conditions, structural instability, hazardous materials, water, distance, or other hazards. Elevated observation from aerial apparatus or structures may similarly be limited by location, access, or operational conditions.

Manned aircraft can provide valuable aerial situational awareness but may not always be immediately available or able to operate at the lower altitudes or locations where a small UAS may safely provide useful information.

OFD may also request UAS resources from another public safety agency. Reliance solely upon outside resources, however, may result in delays or lack of availability, particularly during regional emergencies.

Continuing existing operations without UAS would avoid the privacy considerations associated with the technology but would not provide the same ability to obtain rapidly deployable aerial imagery while keeping responders away from hazardous conditions.

UAS are intended to supplement, not replace, existing Department resources, incident size-up, reconnaissance practices, or manned aviation resources.

**K. Track Record**

UAS technology has been used by public safety agencies for many years to support emergency response, search and rescue, fire operations, hazardous materials incidents, disaster assessment, incident documentation, and other public safety functions.

Locally, the Fremont Fire Department has operated a UAS program since 2017 and has utilized the technology to support fire and emergency operations. Fremont has subsequently expanded its use of UAS through a joint public safety Drone as First Responder program involving its Fire and Police Departments.

The Alameda County Sheriff's Office also operates an established UAS program and has utilized UAS technology to support public safety and emergency operations throughout Alameda County.

OFD has direct operational experience working with both the Fremont Fire Department and Alameda County Sheriff's Office UAS programs. OFD has partnered with these agencies during large-scale incidents within the City of Oakland where their UAS resources provided aerial support and situational awareness to incident operations. This experience has provided OFD personnel an opportunity to observe the operational value of UAS technology during actual emergency incidents.

OFD will continue to evaluate the experience of other public safety and fire service UAS programs, including operational effectiveness, safety, privacy considerations, technological limitations, and identified adverse impacts as the Department develops and evaluates its UAS program.

# OAKLAND FIRE DEPARTMENT
## POLICY AND PROCEDURES

APPROVED:

REFERENCE: Field Operations Bureau
NUMBER: XXX.XXX
EFFECTIVE: October 1, 2026
REVISED:

# UNMANNED AIRCRAFT SYSTEMS (UAS)

## I. PURPOSE:

The purpose of this policy is to establish standards governing the operation of Unmanned Aircraft Systems (UAS) by the Oakland Fire Department (OFD). UAS enhance firefighter safety, improve situational awareness, support emergency response and incident management, assist in protecting life and property, and provide aerial reconnaissance for emergency operations.

This policy establishes operational requirements, privacy protections, training standards, data management practices, and program oversight to ensure UAS are operated safely, effectively, and in compliance with all applicable federal, state, and local laws.

The Oakland Fire Department is committed to operating UAS in accordance with:

- Federal Aviation Administration (FAA) regulations;
- California law;
- Oakland Municipal Code governing surveillance technology;
- City of Oakland Surveillance Impact Report requirements;
- National Incident Management System (NIMS) and the Incident Command System (ICS); and Department policies and procedures.

## II. DEFINITIONS:

A. AUTHORIZED OPERATOR: A Department member who has successfully completed all required FAA and Department training and has been approved to operate a Department UAS.

B. INCIDENT COMMANDER (IC): The individual responsible for overall management of an incident under the Incident Command System.

C. SURVEILLANCE IMPACT REPORT (SIR): The document approved by the Oakland City Council describing the Department's authorized use, management, privacy protections, reporting requirements, and oversight of surveillance technology.

D. UAS PROGRAM COORDINATOR: A Department member designated by the Fire Chief to oversee the Department's UAS program, including training, maintenance, regulatory compliance, data management, and program administration.

E. UNMANNED AIRCRAFT SYSTEM (UAS): An unmanned aircraft and all associated components including aircraft, remote controller, communications equipment, software, payloads, batteries, sensors, and supporting equipment.

F. VISUAL OBSERVER (VO): A trained Department member assigned to assist the Remote Pilot in maintaining visual line of sight, identifying hazards, and monitoring surrounding airspace.

## III. POLICY:

The Oakland Fire Department may utilize Unmanned Aircraft Systems (UAS) to enhance firefighter safety, improve situational awareness, support emergency response, and protect life and property. UAS shall be operated in accordance with all applicable Federal Aviation Administration regulations, California law, the City of Oakland's Surveillance Technology Ordinance, the approved Surveillance Impact Report, and this policy. All UAS operations shall respect individual privacy and civil liberties and be conducted only for legitimate governmental purposes.

## IV. PROCEDURES:

### A. AUTHORIZED USES

Department UAS may be deployed for the following purposes:

1. Structure fires
2. Vegetation and wildland fires
3. Hazardous materials incidents
4. Technical rescue operations
5. Urban Search and Rescue incidents
6. Water rescue operations
7. Missing or lost person searches
8. Disaster response and recovery
9. Damage assessment
10. Fire investigations
11. Scene documentation
12. Incident command support
13. Pre-incident planning
14. Incident planning and post-incident analysis.

15. Infrastructure inspections conducted for Department purposes

16. Emergency management operations

17. Fire code inspections

18. Public safety training

19. Emergency preparedness exercises

20. Community risk reduction activities

21. Post-fire origin and cause documentation

22. Department-approved exercises

23. Any incident or event where aerial observation improves responder safety or incident management.

B. PROHIBITED USES

Department UAS shall not be used:

1. For personal use.

2. For general surveillance unrelated to a legitimate Department mission.

3. To monitor individuals or groups solely because of their race, ethnicity, religion, national origin, gender, sexual orientation, disability, political beliefs, or participation in activities protected by the United States or California Constitutions.

4. To collect information unrelated to the authorized mission.

5. To carry or deploy weapons.

6. To conduct facial recognition, biometric identification, gait analysis, or similar analytic technologies unless specifically authorized by law and approved by the City.

7. In any manner inconsistent with Department policy or applicable law.

C. AUTHORIZATION

1. The deployment of a Department UAS shall be authorized by the Incident Commander or other Department supervisor responsible for the operation.

2. Planned operations, training exercises, and non-emergency missions shall be approved by the UAS Program Coordinator or the appropriate Division Chief.

3. Emergency deployments necessary to protect life or property may occur immediately under the direction of the Incident Commander.

D. OPERATIONAL REQUIREMENTS

1. Prior to flight, the Remote Pilot shall:

   a. Conduct a pre-flight inspection.

   b. Verify aircraft airworthiness.

   c. Confirm battery status.

   d. Assess weather conditions.

   e. Verify required FAA airspace authorization.

   f. Conduct a crew briefing.

   g. Coordinate with the Incident Commander.

2. During flight, the Remote Pilot shall:

   a. Maintain compliance with FAA regulations.

   b. Yield to all manned aircraft.

   c. Maintain visual line of sight unless operating under an FAA approved waiver.

   d. Continuously evaluate operational risks.

   e. Immediately terminate flight whenever safety is compromised.

E. PRIVACY PROTECTION

1. The Department recognizes the importance of protecting individual privacy while utilizing UAS technology.

2. The Department shall make reasonable efforts to avoid collecting or retaining information unrelated to the authorized mission.

3. Personnel shall:

   a. Collect only information reasonably necessary to accomplish the authorized mission.

b. Avoid intentionally recording areas where individuals have a reasonable expectation of privacy unless necessary to accomplish a lawful emergency response, rescue, investigation, or other authorized Department mission.

c. Minimize the collection of information concerning uninvolved persons.

d. Restrict access to collected information to authorized personnel.

e. Comply with all applicable privacy laws and City of Oakland surveillance technology requirements.

F. DATA COLLECTION

1. Department UAS may collect:

a. Still photographs;

b. Digital video;

c. Thermal imagery;

d. Mapping and orthomosaic imagery;

e. Three-dimensional (3D) imagery; and

f. Other sensor data approved as part of the Department's UAS program.

2. UAS sensors shall be activated only during authorized Department missions or training exercises.

3. The Department shall collect only the information reasonably necessary to accomplish the authorized mission.

G. DATA ACCESS

1. Access to live video, imagery, and other data collected by Department UAS shall be limited to personnel with a legitimate business need.

2. Authorized personnel may include:

a. Remote Pilots in Command (RPIC);

b. Visual Observers;

c. Incident Command personnel;

d. Fire Investigators;

e. UAS Program Coordinator; and

f. Other Department personnel authorized by the Fire Chief or designee.

3. Access to stored data shall be limited to personnel authorized to perform operational, investigative, training, administrative, or legal functions.

H. DATA PROTECTION

1. All images, video recordings, and digital data collected by Department UAS are official Department records.

2. The Department shall establish procedures governing:

a. Data collection

b. Storage

c. Access

d. Chain of custody

e. Evidence preservation

f. Release of records

g. Information security

3. Only authorized personnel shall access UAS data.

4. Data shall not be disseminated except as authorized by law or Department policy.

I. DATA RETENTION

1. UAS data shall be retained only for the period authorized by the approved Surveillance Impact Report, the City's records retention schedule, and applicable law.

2. Data that has no evidentiary, investigative, training, legal, administrative, or operational value shall be deleted in accordance with the approved retention schedule.

3. Data associated with emergency incidents, investigations, claims, litigation, training, or other official Department purposes shall be retained in accordance with applicable records retention requirements.

J. PUBLIC ACCESS

1. UAS data and records shall be made available to the public only in accordance with the California Public Records Act, applicable exemptions, court orders, and other applicable laws governing the release of public records.

K. THIRD-PARTY DATA SHARING

1. UAS data may be shared only when authorized by law and consistent with the approved Surveillance Impact Report, including:

   a. Other City departments;

   b. Mutual aid agencies;

   c. Law enforcement when related to a criminal investigation;

   d. Insurance investigators when authorized;

   e. Courts pursuant to lawful process;

   f. Public records requests as required by law.

   g. Contractors or vendors providing support for the Department's UAS program when authorized by contract and applicable law.

L. SURVEILLANCE IMPACT REPORT COMPLIANCE

1. The Department shall operate all UAS in accordance with the City of Oakland's approved Surveillance Impact Report and Oakland Municipal Code governing surveillance technology.

2. The UAS Program Coordinator shall ensure compliance with all reporting, auditing, privacy, security, and oversight requirements established by the City.

3. No material changes to the UAS program shall occur without compliance with applicable City approval requirements.

M. PRIVACY ADVISORY COMMISSION REPORTING

1. The UAS Program Coordinator shall prepare an annual report consistent with the requirements of the City's Surveillance Technology Ordinance and approved Surveillance Impact Report.

2. The annual report shall include, at a minimum:

   a. Number of UAS deployments;

   b. General categories of incidents;

   c. Training flights;

   d. Equipment inventory and maintenance;

   e. Program expenditures;

f. Data retention practices;

g. Data sharing activities;

h. Complaints or alleged policy violations;

i. Corrective actions taken;

j. Recommendations for program improvements; and

k. Any additional information required by the Privacy Advisory Commission or City Council.

N. PROGRAM ADMINISTRATION

1. The Fire Chief shall designate a UAS Program Coordinator responsible for:

a. Program oversight;

b. FAA compliance;

c. Fleet management;

d. Equipment inventory;

e. Flight records;

f. Maintenance;

g. Policy compliance;

h. Operator qualifications;

i. Annual program review;

j. Privacy compliance; and

k. Coordination of required City reporting.

l. FAA waivers and airspace authorizations.

O. TRAINING

1. Only Department-authorized operators may operate Department UAS.

2. Authorized operators shall maintain:

a. FAA Remote Pilot Certification as required;

b. Department operational qualification;

c. Initial qualification, recurrent flight proficiency, and currency requirements established by the Department.;

d. Annual refresher training; and

e. Mission-specific training as determined by the UAS Program Coordinator.

3. Training records shall be maintained by the Training Division.

P. AUDITING AND OVERSIGHT

1. The UAS Program Coordinator shall:

a. Maintain deployment logs.

b. Conduct periodic reviews of UAS operations.

c. Audit access to stored data.

d. Review complaints.

e. Investigate policy violations.

f. Report significant violations through the chain of command.

g. Ensure compliance with the approved Surveillance Impact Report.

Q. MAINTENANCE

1. The UAS Program Coordinator shall establish procedures for:

a. Pre-flight inspections;

b. Scheduled maintenance;

c. Firmware updates;

d. Battery management;

e. Flight logs;

f. Equipment inventory;

g. Repair documentation.

h. Software and firmware updates.

2. Aircraft determined to be unsafe shall be removed from service until repaired.

R. SAFETY

1. Safety shall be the highest priority during all UAS operations.

2. The Remote Pilot shall immediately terminate flight operations whenever:

   a. Aircraft control becomes unsafe;

   b. Weather conditions deteriorate;

   c. Airspace conflicts exist;

   d. Equipment malfunctions occur;

   e. Directed by Air Operations or the Incident Commander; or

   f. Continued operation presents an unacceptable risk to responders or the public.

3. UAS operations shall not interfere with emergency operations or the safe operation of manned aircraft.