5-09/590.00 - Counter - Unmanned Aircraft Systems (C-UAS) Program

The Department's Counter-Unmanned Aircraft Systems (C-UAS) Program supports the protection of life, property, and critical infrastructure through the detection, tracking, identification, and, when legally authorized, mitigation of unmanned aircraft systems.

The program is intended to support pre-planned events, spontaneous incidents, emergency operations, and other authorized Department missions. Public notification regarding the potential use of C-UAS authority is hereby provided through this policy.

The C-UAS Program is assigned to the Emergency Operations Bureau (EOB). All Department C-UAS operations shall be managed, coordinated, and overseen by EOB. EOB shall be responsible for program administration, personnel assignments, training and qualification requirements, equipment management, operational planning, and coordination with federal, state, and local partners.

Definitions

Agency Approving Official – Senior official designated to authorize C-UAS operations on behalf of the Department. The Agency Approving Official may not serve as a mitigation operator for an operation that official has approved.

Authorized Technologies List – A list of authorized technology categories for C-UAS operations by State, Local, Tribal, and Territorial (SLTT) law enforcement and correctional agencies, maintained jointly by the Department of Justice, the Department of Homeland Security, the Department of Defense, the Department of Transportation and Federal Aviation Administration, the Federal Communications Commission, and the National Telecommunications and Information Administration.

Authorized Systems List – A subset of the Authorized Technologies List that identifies specific systems—including make, model, and hardware version—that have been authorized for operational use within one or more technology categories on the Authorized Technologies List.

C-UAS Authority and Operational Requirements

C-UAS authority may only be exercised to protect against credible threats posed by UAS, as defined by the Code of Federal Regulations (C.F.R.) title 6 C.F.R. section 124.2, and not for the sole purpose of collecting evidence for criminal prosecution or as a substitute for the authority of chapter 119 or 206 of title 18, United States Code.

Before any C-UAS mitigation action, certified EOB personnel must determine, under the totality of the circumstances, that a credible threat exists, and that any mitigation is proportionate and uses the least disruptive effective means available.

All C-UAS operations must comply with and be conducted in accordance with the First and Fourth Amendments to the United States Constitution, applicable law, and Department policy.

Only EOB personnel who have completed the applicable training, hold the legally required certifications and

obtain the required authorizations shall operate C-UAS equipment or perform designated C-UAS functions. Mitigation activities shall only be conducted after obtaining the required operational approvals.

Only systems within technology categories on the Authorized Technologies List and, where that list is populated, only specific systems on the Authorized Systems List, may be deployed pursuant to 6 C.F.R. section 124.7.

Designated EOB personnel must complete the required federal coordination, notification, and reporting for each C-UAS operation.

All C-UAS operations and post-operating procedures shall be conducted in a manner that protects privacy and civil liberties and minimizes the incidental collection of material captured. C-UAS data shall be handled, retained and disseminated in accordance with established C-UAS procedures on data handling, retention and dissemination and applicable legal authorities.

Procedures

EOB shall establish and maintain C-UAS implementation policy and program requirements and procedures, including, but not limited to:

- Operation plan requirements and tactical procedures
- Equipment use protocols
- Deployment approval requirements and procedures
- Engagement protocols that account for the risk to persons and property on the surface and in the air before engagement as well as use of force considerations
- Escalation procedures
- Ground intercept team procedures
- Safety protocols including render safe procedures
- Evidence collection and chain of custody procedures
- Communications procedures
- System operating procedures
- Data handling, retention, dissemination and purge requirements, verifications and procedures
- Pattern data identification requirements
- Documentation and reporting requirements

- Post-operation procedures

All personnel participating in C-UAS operations shall comply with the requirements, procedures, and operational protocols established by EOB.

Requests for C-UAS Deployment

Requests for C-UAS deployment during a pre-planned event shall be made by contacting the C-UAS Program Manager designated by the EOB Unit Commander.

Requests for C-UAS deployment during a spontaneous incident shall be made through the 24 Hour Operations Center, which shall contact the EOB Duty Sergeant.

Authorizations for C-UAS deployment shall be approved by the EOB Unit Commander or C-UAS Program Manager who are designated as the Department's Agency Approving Officials.

Military Equipment Reporting

Any C-UAS device that is considered military equipment under California Government Code section 7070 et seq., requires annual public reporting on the funding, acquisition, and use of such equipment. It also requires information on any such equipment the Department intends to acquire in the coming year. EOB is responsible for collecting all inventory, procurement, recording costs, managing respective military training requirements, and ensuring accurate reporting in the Department's annual military equipment report.