*Date Revised: 12/10/2020*

# UAS Reporting Form Instructions

Please refer to this form when filling out a reporting form to operate a Commercial Off-the-Shelf Unmanned Aircraft System (UAS). Do not submit requests for UAS operations that do not qualify for eligible purposes as defined below or when all necessary information is not available and provided. **Reporting forms** need to be submitted within twenty-four (24) hours after Emergency Operations have concluded and no later than forty-eight (48) hours after Emergency Operations have commenced.

- **Block 1** - UAS Reporting Forms can only be completed by employees of the Department of the Interior. Non-DOI entities or contractors should operate pursuant to the terms of their existing agreement with the Department.

- **Block 2 -** An "Emergency Operation" is defined as a UAS operation initiated for the following purposes: 1) Fighting an existing or imminent Wildland Fire; 2) Taking measures that are reasonably tailored to prevent an anticipated Wildland Fire; 3) Monitoring for or responding to a potential/declared national or state Emergency involving human safety or to prevent imminent damage to human life and property; and 4) Conducting a human search and rescue effort that involves the preservation or safety of human life or physical property as a core component of the mission. **Each Operation should have a clear connection to one of the health and safety purposes identified above.** Block 2 of the form should indicate which type of emergency your pilots have responded to/are conducting training to respond to.

- ***Block 2 - Fuels Management projects**—including prescribed fire treatments—limits the risk and negative impacts of wildfire to people, communities, and natural/cultural resources by reducing the accumulation of vegetation that contribute to the intensity, severity, or negative effects of wildfire. Waivers are required for fuels management projects. Please submit a waiver, and not a report, for these projects.

- **Block 3** - Be precise when describing the location, including GPS coordinates where possible.

- **Block 4** - Operation dates should include hours of operation when the UAS-approved activity is expected or has occurred. Forms must provide specific dates to the extent possible. The duration requested for a waiver should not exceed one month per waiver submission. If necessary, extensions should be sought in anticipation of an expired duration.

- **Block 5 -** When describing UAS hardware/software, please provide all available brand and manufacturer information for all UAS available and expected to be operated.

- **Block 6 -** Payload details should describe all UAS components that have the capacity to upload, store, transmit, or otherwise capture information of any nature.

- **Block 7 -** Identify all DOI-related offices, bureaus, or other entities that will have or had access to any data collected or captured at any point in the operation of the UAS. Describe the system used to store and keep secure acquired data.

- **Block 8** - Is the data that was or would potentially be obtained likely to involve sensitive information such as personally identifiable information or information relevant for law enforcement purposes?

    - Data collected by a UAS may be considered a Federal Record and thereby subject to retention in accordance with the relevant Records Schedule. Classification and treatment of such records should be coordinated with the Departmental Records Officer or relevant Bureau Records Officer, as appropriate, and the Division of General Law. Data must not be stored on the drone itself. All data must be immediately removed, and the UAS memory sanitized, at the conclusion of each flight.

- **Block 9 -** the Department of Defense's Defense Innovation Unit recently finalized its small UAS initiative, called Blue sUAS. This capability provides secure and trusted sUAS for Federal government operations: https://www.diu.mil/autonomy-blue-suas. Use of Blue sUAS is exempt from the Waiver and Reporting procedures. Please indicate whether 1) Blue sUAS would have been appropriate for this mission, and 2) what efforts have been made, if any, to acquire Blue sUAS.

- **Block 10 -** What tactics were or will be employed prior to operation of a UAS during an approved mission (e.g., detach/block camera, cover sensors, compliance validation plan, etc.)?

- **Block 11 -** Describe cybersecurity measures taken to protect, restrict, or limit potential threats to UAS operations or data loss (e.g., Airgap, Rizer, etc.).

- **Block 12 (additional comments)** - This should contain the names of all pilots who will conduct the operation. If data will be transferred in any capacity to a third party, that third party's information must be listed, as well as the information of the Incident Commander or Authorizing Official that approved the transfer. The Authorizing Official will be responsible for ensuring compliance with all stated mitigation measures by all pilots or individuals identified in the form.

# United States Department of the Interior

## Commercial Off-the-Shelf Unmanned Aircraft System (UAS) Emergency Operation Reporting Form

*Please complete the following form within **twenty-four (24) hours** after operations have concluded OR within **forty-eight (48) hours** after operations have commenced and email to uas@ios.doi.gov.*

1. Agency Bureau/Office:
2. Describe the search and rescue / emergency operation:
3. Location:
4. Operation dates:
5. UAS hardware / software:
6. Payload details - identify camera, Internet sensor, link info:
7. Who maintained the data and how will it be controlled?
8. Data security environment:
   a. Controlled (Not publicly releasable): ☐
      i. Sensitive mission? (If yes, please explain): Yes: ☐ No: ☐
      ii. Sensitive data? (If yes, please explain): Yes: ☐ No: ☐
      iii. Was the video encrypted? Yes: ☐ No: ☐
      iv. What was the DL Range?
      v. Was a map attached of area usage? Yes: ☐ No: ☐
   b. Uncontrolled ☐
   c. Benign (publicly releasable): ☐
10. Would "Blue sUAS" have been appropriate for use in the mission? Describe attempts to acquire, if any:
11. Describe pre-mission tactics:
12. Describe cyber-mitigation plan:
13. Additional comments:
14. Authorizing Official name, phone, & email: Date: