Date Revised: 12/10/2020

UAS Waiver Form Instructions

Please refer to this form when filling out a waiver request 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. **Waiver forms** for Emergency Readiness must be submitted at least thirty (30) days prior to the proposed date of operation.

- **Block 1** - UAS Waiver 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 -** "Emergency Readiness" is defined as DOI Remote Pilot training required under OPM-11 and described in the Interagency Aviation Training Guide (Approved Jan. 28, 2020) that is undertaken in furtherance of one of the health and safety purposes identified above. This training includes:
    - A-100 (3) Basic Aviation Safety
    - A-110 Aviation Transportation of Hazardous Materials (if applicable)
    - A-200 (3) Mishap Review
    - A-202 Interagency Aviation Organizations
    - A-203* Basic Airspace
    - A-450* Small Unmanned Aircraft System (sUAS) Basic Remote Pilot Course
    - A-452R* (2) Small Unmanned Aircraft System (sUAS) Remote Pilot Refresher Training

  Approvals for Emergency Readiness training will be limited to meeting these minimum requirements under OPM-11 and only where a health and safety purpose can be identified.

- **Block 2 - "**Emergency Readiness" also includes **fuels management projects**. 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 indicate if the operation is for fuels management in Block 2.

- **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 be 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 be doing training (in addition to certification requirements to be obtained through approval of this waiver) *or* the names of the 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 Readiness Waiver Form

*Please complete the following form at least **thirty (30) days** in advance of the emergency readiness operation and email to uas@ios.doi.gov.*

1. Agency Bureau/Office:
2. Describe the emergency readiness operation:
3. Location:
4. Operation dates:
5. UAS hardware/software:
6. Payload details - identify camera, Internet sensor, link info:
7. Who will maintain 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. Is the video encrypted? Yes: ☐ No: ☐
      iv. What is the DL Range?
      v. Is a map attached of area usage? Yes: ☐ No: ☐
   b. Uncontrolled ☐ Benign (publicly releasable): ☐
9. Would "Blue sUAS" be appropriate for use in current mission? Describe attempts to acquire, if any:
10. Describe pre-mission tactics:
11. Describe cyber-mitigation plan:
12. Additional comments:
    (If **urgent** request, please explain)
    (If **training**, explain certification needs)
13. Submitter name, phone, and email: Date:
13. Authorizing Official: Approved: ☐ Denied: ☐ Date: