United States Army Corps of Engineers
HQ Aviation

Implementation Guidance for Exception to Policy

Commercial Off-the-Shelf Small Unmanned Aircraft Systems Field Operations

Approved 25 January 2023

Valid through 24 January 2024

CONTENTS

USACE SUAS ETP Waiver

The Army Cyber waiver authorities (Army Acquisition Executive with the Army CIO/G6) issued the U.S. Army Corps of Engineers (USACE) a waiver to allow operation of Commercial Off -the-Shelf (COTS) Small Unmanned Aircraft Systems (SUAS). This waiver is valid through **24 January 2024.**

Who does this waiver and implementation guidance apply to?

All USACE SUAS operators who will be flying non-tactical missions.

(**NOTE**: This does not cover any other agencies at this time.)

For the purpose of this guidance, contractors fall into two categories: Support Contractors or Service Contractors

- Support Contractors are those contractors working for USACE directly. Several members of the USACE Aviation team are support contractors. Support contractors are required to obtain Small Unmanned Aircraft System Qualification Course (SQC) certification and are only then authorized to fly USACE SUAS under the USACE ETP waiver. As a general guideline, if the contractor has a USACE email account, they are a Support Contractor.

- Service Contractors are contractors working for companies that have agreements/contracts with USACE for services. HQ Aviation provides oversight provisions for Service Contractor's UAS operations per APL 95-1-1. Service Contractors may NOT operate any SUAS unless approved on the USACE ETP Waiver or on the DIU Blue Cleared List. **Service Contractor operations must adhere to APL 95-1-1, Section 14 requirements**.

SUAS Platforms and Missions

The list of COTS SUAS in the waiver and detailed in **Appendix A (controlled environments)** and **Appendix B (benign environments ONLY)** are the approved SUAS for USACE missions**. Appendix C** specifies DIU Blue Cleared-List Aircraft.

Appendix A is the list of SUAS that are approved to fly missions over DoD installations (controlled environment), Federal lands, or missions funded by military funding (for example, OMA funds).
__NOTE: All aircraft utilizing the Pixhawk Black Cube must upgrade to the Pixhawk Blue Cube to be used in controlled environments.__
***NOTE: All Futaba Controllers must be confirmed compliant before use.**

The DIU Blue Cleared-List Aircraft are located in Appendix C and at:
https://www.diu.mil/blue-uas-cleared-list

The DIU Blue Cleared-List identifies the SUAS authorized for USACE operations:

- These SUAS will not be listed on the USACE ETP waiver.
- These SUAS are required to be in the MARS Inventory following MARS mission planning, approvals, standards, operations, and execution.

The following requirements are critically important to all USACE SUAS operators:

1. Never connect to the internet or any other network.
2. Ensure all mitigation strategies are implemented prior to use. Treat all data collected as sensitive.
3. Never operate over people, sensitive facilities/equipment/activities unless specifically approved to do so IAW USACE APL 95-1-1.
4. Maintain a lateral clear zone from your flight path equal to your altitude above ground level. Only mission personnel are authorized inside the lateral clear zone.
5. Conduct thorough crew briefing prior to each mission day.
6. Utilize and adhere to the USACE UAS Operator's Checklist.

The SUAS must also adhere to the following rules when operating over DoD Installations:

1. All C2 links are encrypted to a minimum of AES 128.
2. There must be a prevention of unencrypted camera feeds.
3. Cover camera when not in use.
4. All operations are limited to Sanitized locations (do not expose TTPs- tactics, techniques & procedures).
5. Use only configurations approved on waiver and in the AWR. Contact the HQ Aviation if you have questions about the approved configurations.

HQAviation@usace.army.mil is available for any questions you may have.

DO NOT contact OSD, ARMY, G-3/5/7, or other external organizations regarding the USACE waiver. HQ Aviation is your voice to these organizations.

The attached USACE ETP waiver and this implementation guidance are provided for your use. USACE SUAS operations have an excellent reputation in the government both in DoD and beyond. This is due to the excellent operations conducted by you in the field. Please continue your diligent efforts to comply with the often-difficult guidance involved in these waivers.

KIRKPATRICK.JAS
ON.R.1109565845
2023.01.27
16:57:41 -06'00'

Jason Kirkpatrick
Aviation Program Manager

USACE SUAS Waiver Implementation Guidance

Introduction

This USACE ETP waiver pertains to non-tactical SUAS operations only. The USACE Commander recognizes the potential cyber- and information-security vulnerabilities associated with using COTS SUAS products. **The FY2020 National Defense Authorization Act (NDAA) 848 and EO 13981 intends to prohibit the procurement and use of People's Republic of China (PRC) SUAS except for counter SUAS testing, therefore, USACE has transitioned away from Chinese produced SUAS operational exemption requests. SUAS that utilize Manufactured in or Assembled in China transmitting components, firmware, logic boards, or software have been removed from USACE operational inventory and set aside for counter SUAS testing, disaster relief missions, and Engineering Research and Development Center (ERDC) laboratory test flights**. USACE adheres to HQDA EXORD 178-21 CONSOLIDATED DEPARTMENT OF DEFENSE (DOD)-ARMY, dated 23 June 2021 and the MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP – *Guidance for Procedures for the Operation and Procurement of Unmanned Aircraft to Implement Section 848 of the NDAA for Fiscal Year 2020, 8 September 2021*.

USACE SUAS Cyber-Security Risk Mitigation

USACE uses a cyber-security risk mitigation strategy designed by the USACE HQ Aviation Program and approved by the USACE Cyber Approving Official (AO) to prevent potentially malicious code from being introduced into USACE networks. Stand-alone laptop/tablet computers typically provided by USACE or the SUAS vendor are used as GCS.

USACE GCS computers have the following procedural constraints:

- Encryption for all **Controlled Environment** Missions
- Frequency Hopping Spread Spectrum (FHSS) for **Benign Environment** Missions
- Not permitted to connect to the internet
- Not permitted to be connected to any Information Technology (IT) Network (NETCOM CRN III Standard)
- Not used for any other purpose

Flight data collected during the SUAS mission is recorded on a removable memory medium; scanned for malicious code using an ACE-IT provided Air Gap Process before being brought into USACE networks. The Air Gap Process includes an Air Gap computer segregated from USACE and open networks while providing an up-to-date anti-virus solution that scans for malicious code. An Air Gap computer can only be operated by individuals who have completed Information Assurance (IA) fundamentals Training. Further air-gap training and assurance is conducted as part of the USACE Aviation Program's SUAS Qualifications Course.

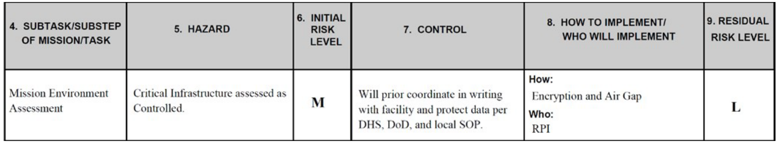
Radio modem links between GCS and the AV use FHSS technology on transmitted signals, protecting the command and data links. Backup RC radios also use FHSS and are uniquely paired to each aircraft. Pairing a different RC with the AV requires physical possession of the AV effectively preventing malicious backup RC intervention of the AV flight.

USACE SUAS Information Protection Risk Mitigation

USACE uses an information risk mitigation strategy for SUAS operations focused on preventing data obtained by SUAS operations from leaving USACE's control. SUAS data is only collected over USACE facilities or with the concurrence of USACE's Federal or state partners. Data collected on behalf of USACE partners is not distributed without explicit need and approval from the appropriate authority. The following are procedural controls implemented by USACE for all SUAS operations to mitigate information protection risks: (see APL 95-1-1, Section 3.1, *Management Information System for Aviation and Remote Systems (MARS)* and Section 7, *Safeguarding Data*.)

- All SUAS missions require an Aviation Mission Plan submitted in MARS; approved from a trained, Command-/Director-designated Aviation Mission Approval Authority.

  - The Mission Plan must include a Critical Infrastructure analysis. The analysis assesses all activities within a 5-mile radius of the planned SUAS operation. Criticality is defined and assessed in a three-tiered index based on Department of Homeland Security (DHS) or other Federal agency definitions.



4. SUBTASK/SUBSTEP OF MISSION/TASK	5. HAZARD	6. INITIAL RISK LEVEL	7. CONTROL	8. HOW TO IMPLEMENT/ WHO WILL IMPLEMENT	9. RESIDUAL RISK LEVEL
Mission Environment Assessment	Critical Infrastructure assessed as Controlled.	M	Will prior coordinate in writing with facility and protect data per DHS, DoD, and local SOP.	How: Encryption and Air Gap Who: RPI	L

- UAS hardware (aircraft and GCS) is not permitted to connect to ANY computer networks.

- Autopilot and payload data storage is cleared (IAW NIST 800-88) before and after each SUAS mission.

- If operated on a military bases, a fully encrypted C2 link and physical prevention of camera feeds being transmitted shall be employed.

- The SUAS will never be operated over sensitive facilities or equipment, or connected to a network.

- SUAS cameras and payloads shall be covered when not in use. The intent for storing systems in shipping containers or wall lockers is to ensure all sensors are covered. All data storage is removed when not in use.

- Batteries are removed when aircraft are not in use. The entire SUAS is stored in a closed container- normally the SUAS Shipping container or Wall Locker- in a secure facility with restricted access.

  - Battery Storage: Follow manufacture guidance and applicable USACE regulations. Refer to APL 95-1-1, Section 3.12 and the Battery Storage guidance located on the USACE SUAS SharePoint at**:** **https://usace.dps.mil/sites/KMP-UAS**.

- UAS hardware is only procured and disposed through approved USACE methods. Wireless communication modems must use the highest available security measures. Default usernames and passwords are changed and comply with department complexity regulations. SSIDs are hidden or changed from default if possible, and WPA2/PSK or WPA2 Enterprise, security levels are enabled and WPS disabled if available.

- Access to SUAS and associated hardware is limited to those who have been properly trained in risk mitigation procedures.

Appendix A

USACE SUAS Controlled Environments*

MANUFACTURER	MODEL	Type	Encryption	Configuration Notes
CENSYS	Sentaero	Multirotor	AES 128	
ERDC EL	ELX-Series	Multirotor	AES 256	**Must have Pixhawk Blue Cube (USA)***
ERDC EL	ELX-Tethered	Multirotor	AES 256	**Must have Pixhawk Blue Cube (USA)***
EXYN/ASYLON	EXYN Scout/Asylon ASY02E Custom	Multirotor	AES 128	
FiXAR	007	VTOL	AES 128	
FlightWave	Edge 130	VTOL	AES 128	
FLIR	SkyRaider R80D	Multirotor	AES 256	
FreeFly Systems	Alta 8 Pro	Multirotor	AES 128	**Must have Pixhawk Blue Cube (USA) & Compliant Futaba Controller***
Harris Aerial	Carrier HX8	Multirotor	AES 128	
Lockheed Martin	Indago 2	Multirotor	AES 256	
MicroDrones	MD4-1000	Multirotor	AES 256	Operated with MdRCXb
MicroDrones	MD4-3000	Multirotor	AES 256	Operated with MdRCXb
NRL Custom	Eagle v6	Multirotor	AES 256	
AeroVironment [Pulse AeroSpace]	Vapor 55	Helicopter	AES 256	
Riegl	RiCopter	Multirotor	AES 256	
SkyFish	M4 UAV	Multirotor	AES 128	
SkyFish	M6 UAV	Multirotor	AES 128	
Solute	CONDOR Hugin Gen 2	Multirotor	AES 256	

*** Any System with the Pixhawk Black Cube MUST be replaced with the Pixhawk Blue Cube (USA) to ensure NDAA 848 compliance.**

*** Any System with the Futaba T14SG Controller MUST be replaced with a compliant Futaba FMT-02 or T161Z or NDAA approved controller.**

*** VTOL (Vertical Takeoff & Land)**

Appendix B

USACE SUAS Benign Environments Inventory*

MANUFACTURER	MODEL	Type	Encryption	Configuration Notes
Wingtra	Wingtra One Gen I	VTOL	FHSS	

***VTOL (Vertical Takeoff & Land)**

Appendix C

DIU BLUE CLEARED-LIST AIRCRAFT*

MANUFACTURER	MODEL	Type	Encryption	Configuration Notes
Ascent AeroSystems	Spirit	Multirotor	AES 128	
BlueHalo	Intense Eye V2	Multirotor	AES 128	
Easy Aerial	Osprey	Multirotor	AES 256	
FlightWave	Edge 130	Fixed Wing	AES 128	
FreeFly Systems	AltaX	Multirotor	AES 256	
Harris Aerial	H6	Multirotor	AES 128	
Harris Aerial	H6 HE+	Multirotor	AES 128	
Harris Aerial	H6 Hydrone	Multirotor	AES 128	
Inspired Flight	IF750	Multirotor	AES 128	
Inspired Flight	IF1200	Multirotor	AES 256	
Parrot	ANAFI USA GOV	Multirotor	AES 128	
Parrot	ANAFI USA MIL	Multirotor	AES 128	
SenseFly/AgEagle	eBee TAC	Fixed Wing	AES 256	
Skydio	X2D [New Configuration]	Multirotor	AES 256	
Teal	Golden Eagle	Multirotor	AES 256	
Vantage Robotics	Vesper	Multirotor	AES 256	
Wingtra	WingtraOne Gen II [2022]	VTOL	AES 128	

***For current DIU Blue Cleared-List Aircraft, see https://www.diu.mil/blue-uas-cleared-list**

DEPARTMENT OF THE ARMY
OFFICE OF THE ASSISTANT SECRETARY OF THE ARMY
ACQUISITION LOGISTICS AND TECHNOLOGY
103 ARMY PENTAGON
WASHINGTON, DC 20310-0103

SAAL-ZS   25 January 2023

MEMORANDUM FOR: Headquarters (HQ), U.S. Army Corps of Engineers (USACE), 441 G Street NW, Washington, DC 20314

SUBJECT: Commercial Off-The-Shelf Unmanned Aircraft System Exception to Policy Request (22.118)

1. References:

a. HQ USACE memorandum (Request for Exception to Policy (ETP)), 5 December 2022

b. Office of the Assistant Secretary of the Army (Acquisition, Logistics and Technology) Memorandum (Army Delegation of Approval Authority for Unmanned Aircraft Systems Implementation Guidance), 11 February 2022.

2. Per reference 1a, HQ USACE requests ETP for use of Commercial Off-The-Shelf (COTS) Unmanned Aircraft System (UAS) AeroVironment Vapor 55 (1), CENSYS Tech CENSYS Sentaero (1), ERDC-EL ELX-Series (2), ERDC-EL ELX-Tethered (1), EXYN/ASYLON SCOUT/ASY02E (Pending), FiXAR OO7 (Pending), FlightWave Edge 130 (Pending), FLIR SkyRaider R80D (8), FreeFly Alta8 Pro (3), Harris Aerial Carrier HX8 (1), Lockheed Martin Indago 2 (1), MicroDrones MD4-1000 (3), MicroDrones MD4-3000 (Pending), NRL/PA State University Eagle v6 (1), Riegl RiCopter (2), SkyFish M4 (Pending), SkyFish M6 (1), solute CONDOR Hugin Gen 2 (1), Wintra WingtraOne Gen 1 (1) in support of Installation Support and Civil Support at various uncontrolled locations.

3. Per reference 1b, paragraph 4, I have reviewed and approve the request subject to the mitigation requirements set forth herein. The UAS and ground control station will never be connected to a network or operated near WiFi access. The UAS shall not be flown over people, sensitive facilities or equipment. The UAS shall be operated in accordance with (IAW) the approved Radio Frequency Authorization and the site spectrum manager's directions. All removable media will be cyber scanned prior to download to government computers. On-board storage will be sanitized IAW Department of Commerce National Institute of Standards and Technology Special Publication 800-88 Revision 1, "Guidelines for Media Sanitization," 17 December 2014. Cameras will remain covered when not in use. Please ensure all mitigation strategies are implemented reducing cyber vulnerability risks prior to use.

Controlled by: Army ASA(ALT)
CUI Category: Controlled Technical Info
Distribution/Limited Dissemination Control: FEDCON
POC: Mr. Ronald Crevecoeur, 703-614-3062

4. This exception approval is limited to twelve (12) months. Additional exception request(s) are required for operations beyond twelve months from this approval. In addition, if the UAS configuration or operational employment is changed, an additional exception request is required. You must notify the point of contact of this memorandum at the conclusion of the event that all COTS UAS use has been suspended and certify that all mitigation strategies were employed.

5. All government owned COTS UAS equipment will be placed on an Accountable Property System of Record in accordance with Department of Defense Instruction (DoDI) 5000.64, "Accountability and Management of DoD Equipment and Other Accountable Property," Change 3, 10 June 2019 and Army Regulation 735-5, "Property Accountability Policies," 9 November 2016 within 45 days of this memorandum.

6. Point of contact for this memorandum Mr. Ronald Crevecoeur, (703) 614-3062, DSN 224-3062, or email ronald.crevecoeur.civ@army.mil.

Young J. Bang
Principal Deputy Assistant Secretary of the Army
(Acquisition, Logistics and Technology)