2025

UNMANNED AIRCRAFT SYSTEMS (UAS) RESPONSE PLAYBOOK

FOR RESPONDING TO UAS INCIDENTS IN THE HOMELAND

FEDERAL BUREAU OF INVESTIGATION

NATIONAL COUNTERINTELLIGENCE TASK FORCE | NATIONAL JOINT TERRORISM TASK FORCE | CRITICAL INCIDENT RESPONSE GROUP

Acknowledgments

This Playbook was prepared by the National Counterintelligence Task Force (NCITF) and the National Joint Terrorism Task Force (NJTTF), with heavy involvement from the Critical Incident Response Group (CIRG), Weapons of Mass Destruction Branch (WMD), the Office of General Counsel (OGC) National Security & Cyber Law Branch (NSCLB), and OGC Investigative and Administrative law Branch (IALB) of the Federal Bureau of Investigation (FBI). This document has been reviewed in draft form by individuals chosen for their diverse perspectives and subject matter and technical expertise including members of partner agencies from across the federal government and US intelligence community.

UAS RESPONSE PLAYBOOK FOR ALL RESPONDERS TO UAS INCIDENTS IN THE HOMELAND

In an age defined by rapid technological advancement, Unmanned Systems (UxS) have emerged as a transformative force, bringing both innovation and significant challenges. These systems are reshaping the operational landscape across civilian, military, and national security domains.

The most immediate and visible threats have come from Unmanned Aircraft Systems (UAS), commonly referred to as drones. These systems are disruptive technologies, which are often exploited, endangering public safety, compromising the security of critical infrastructure, and challenging the operational integrity of military installations. From unauthorized drone incursions to sophisticated adversarial applications, UAS have demonstrated their capacity to operate with impunity, underscoring the urgency of addressing this evolving threat (see Appendix A-B).

Per Presidential Executive Order (EO) 14307, “Unleashing American Drone Dominance”, and EO 14305, “Restoring American Airspace Sovereignty”, as well as by direction of the FBI Executive Management, defines and prioritizes the threat landscape and evolution of UAS in the United States.

While our focus remains on countering the persistent dangers posed by UAS, we must not lose sight of the broader spectrum of UxS threats on the horizon. Unmanned Ground Systems (UGS) are poised to present unique challenges, with the potential for autonomous ground vehicles to disrupt transportation networks, deliver hazardous payloads, or support adversarial ground operations. Similarly, Unmanned Maritime Systems (UMS) offer adversaries new opportunities to exploit vulnerabilities in our coastal waters and beyond, enabling stealth operations, underwater surveillance, and even logistical support for hybrid warfare.

In this dynamic environment, our mission is twofold: to mitigate the current threats posed by UAS while proactively anticipating and preparing for the potential dangers associated with UGS and UMS. By maintaining vigilance, fostering innovation, and embracing a comprehensive

approach to UxS security, we can ensure that we are not only responding to today's challenges but also safeguarding against the threats of tomorrow.

This document serves as a call to action—a reminder that the evolving nature of UxS demands a proactive and unified response. Together, we can confront these challenges head-on and secure our future against the risks posed by unmanned threats.

To this end, the FBI and Department of Defense (DoD) have collectively convened subject matter experts to share information, knowledge, and best practices. This united front was the driving force behind the creation of the *Unmanned Aircraft Systems (UAS) Response Playbook – For Responding to UAS Incidents in The Homeland.*

Table of Contents

Introduction

UxS are autonomous or remotely piloted vehicles which are designed to fly, navigate on the surface or sub-surface of water, or move along the ground terrain. UxS pose both an urgent and enduring threat to U.S. personnel, facilities, and assets in the homeland and abroad. UAS—commonly referred to as drones—pose the most significant threat at this time and this threat is increasing in the homeland. Focusing on the near-term problem is not enough; we must acknowledge the rapid evolution of UxS capabilities such as UMS and UGS. The threat continues to evolve, creating a need for innovative strategies ranging from intelligence gathering and surveillance, to offensive operations. Their presence in air, maritime, and ground environments challenges traditional defensive mechanisms.

This initiative was spearheaded by the National Counterintelligence Task Force (NCITF) and the National Joint Terrorism Task Force (NJTTF) to address the UxS threat effectively, emphasizing the need to raise awareness, coalesce UxS incursion reporting, and encourage seamless partnerships among federal agencies, local and state law enforcement, private sector entities, and international allies to share intelligence, best practices, and technological solutions. Furthermore, Congress has expressed concerns about the threats posed by UAS to U.S. critical infrastructure at home and abroad. The need for this initiative was reinforced with the recent Executive Orders, “Unleashing American Drone Dominance” and "Restoring American Airspace Sovereignty", and the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2025 which includes a required strategy for countering drone technologies, referring drone offenses for investigation and prosecution, and assessing resources and authorities necessary for drone incursion response.

The UAS Response Playbook for First Responders is part of a broader effort to defend our homeland from hostile adversaries and an ongoing commitment to better protect the facilities that are critical to the United States of America.

This playbook should be used for UAS/UxS specific incidents in conjunction with standard operating and investigative procedures, as established by your home agency.

To enable later investigative and court processes the responding officer(s) should produce clear, concise, documented information encompassing their observations and actions.

1. UAS Initial Response Guidelines

UAS present a range of criminal concerns and threats to the homeland, including military installations, critical infrastructure, threats to life, mass gatherings, and border protection operations. It is particularly important to determine the nature of a UAS which has entered a restricted area. Determining whether the UAS presents an actual threat, a nuisance, or if it was a legitimate activity is critical to determining the intent of the UAS operator. Even legitimate UAS

activity can congest the airspace—obscuring the presence of malevolent threats—or cause unintentional harm.

Each FBI field office is required to have a dedicated Counter-UAS (C-UAS) Coordinator, led by CIRG and CTD. Please reach out to your local FBI field office.

Due to this expanding and evolving threat, developing a C-UAS awareness and sensing capability is therefore an important strategic need. Coordination between federal, state, local, tribal, and territorial (FSLTT) authorities will enable more effective investigative results and safer incorporation of UAS devices into the homeland operating environment. Additional UAS detection, mitigation, and response training for installation protection and response personnel will also be required (see Appendix C-E).

1.1 Immediate Identification and Threat Assessment

1) Detection of UAS and Anomalous Activity:

a) Unusual Activity: Human/Sensor indication of unusual and/or increased UAS activity near critical infrastructure, a restricted area, base, ship, etc.

- What was the date/start and end time of the UAS sighting?
- Where was the UAS sighting in relation to the location of the reporting party and where, exactly was the observer standing? Mark this location using geo-coordinates or a map application, if possible.
- Can the reporting party mark their location using a map application?
- What were the weather conditions during the UAS sighting?
- Was the UAS visually, audibly, and/or otherwise observed?
- Was the UAS operator observed?
- If the UAS was visually observed, what direction and bearing was it flying? (For example, north or south?)
- What was the total number of UAS observed? If more than one, did the UAS fly in formation (synchronized) or appear scattered/random?

b) UAS Types/Features

- Upon visual recognition, what type was the UAS? (see Appendix F)?
- Did the UAS resemble a type of airplane (i.e. fixed-wing), a helicopter, a quadcopter (i.e. rotary-wing), a hybrid, or something else?
- What were the features of the UAS?
- What was the color or color pattern of the UAS?
- Were any visible lights observed on the UAS? If so, what where the color of the lights, pattern, total number, notable blinking repetitions, location on the UAS, and any other relevant details of the lights?

- Did the UAS make any sounds? If so, please describe them. Document personal information from the witnesses, victims, suspects, and any statements or comments made.

c) Trajectories, movements, flight patterns etc.
- Did the UAS move, hover, or fly continuously in one direction?
- Was take-off or landing observed? If so, what was the location (for example, address, landmark, intersection, MGRS etc.)?
- What was the flight path and flight behavior observed?
- What direction was the UAS traveling (for example, North to South, East to West)?
- What was the approximate altitude of the UAS when it was flying? Try to use immobile objects as a frame of reference (i.e. trees, structures, light poles, etc.) as this can be subjective, especially via visual observation at night.
- Approximately at what speeds was the UAS flying?
- What was the UAS location as it relates to the angle off the horizon?

d) UAS Attachments/Payloads
- Was anything observed/detected having been attached to the UAS (see Appendix G)?
- What did the attachment look like? For example, did it resemble a package, payload, camera, sprayer/nozzle, small rocket, box, or something else?
- Did anything release, launch, and/or fall off of the UAS and if so, what was released?
- At what altitude and where in the flight path of movement was the item released?
- Was the released item recovered?
- If the released item was recovered, what are its characteristics and which agency currently possesses it, if known?

e) UAS Detection/Mitigation System(s)
- Does the facility/base have any UAS detection system(s) or were any other systems elsewhere present during the UAS incursion that may have detected the UAS?
- What type of UAS detection system(s) exists at your site and/or elsewhere, if any (if classified, report at the proper classification)?
- Did the UAS detection system(s) detect the UAS? Provide any information that was provided by the detection system including any .xml files or flight paths. Unsuccessful detection is also relevant investigative information.
- If a UAS mitigation system was used, what was the system name, time/duration used, and outcome? Unsuccessful mitigation is also relevant investigative information (if classified, report at the proper classification).
- Where was the UAS operator located when the UAS detection/mitigation system(s) was used?
- In what direction was the UAS detection/mitigation system(s) pointed during use?

- Did a UAS detection/mitigation system(s) work, while others did not? Please list the success of any and all detection/mitigation systems including facility security camera footage of the UAS.
- Were any other photos or videos of the UAS captured (i.e. witness, surveillance systems, closed-circuit television (CCTV))?
- Did the detection/mitigation system(s) corroborate a visual sighting?

2) **Probing Activity:**
   a) This activity may be a test of defensive responses or countermeasures or may be pre-operational activity.

   b) Was there indication of the UAS probing the facility and/or surveillance of personnel on or off the facility?

3) **Monitor and Verify:**
   a) Determine position/location/platform/domain/operating frequency of UAS.
      - If possible, the targeted location should turn on surveillance systems, such as radar/sonar and cameras/CCTV and preserve original footage.
      - Make best efforts to identify the operator as soon as the UAS is identified.
      - If applicable, obtain description of any vehicle(s) or platform(s) (i.e. shipping vessels) deploying the UAS.

   b) Assess UAS capabilities (e.g. camera, payload, speed).
      - In the event of an attack, immediately shelter and clear the area.
      - Be mindful of modifications i.e. attachments, payloads, hardware, software etc. (see Appendix G).

4) **Notify Federal, State, Local, and Tribal and Territorial Partners:**
   a) Observe UAS behaviors and track domain, communications information, and real time updates to support joint consolidated efforts via secure communication channels.

   b) Contact appropriate federal, state, local, and tribal and territorial partners, including appropriate DoD law enforcement/partners, and relay status of UAS intrusion.
      - Early coordination is imperative to identifying and—in some cases, when applicable—prosecuting UAS operators.

1.2 Attempt to Locate Operator

1) **Scan Area of Operation for launch location and/or human operator:**
   a) Attempt to locate individual(s) who are holding a controller or device that appears to be operating a UAS.

- The operator may be somewhere within direct line of sight of where the drone is operating. (Note: Drone operators do not *need* direct line of sight; however, it does allow the drone to operate more effectively.)
- Operators could be wearing First Person View goggles.
- Look at windows, balconies, rooftops, docks, piers, vessels, hilltops, and any possible observation or landing points nearby.

b) Identify drone operator location information and relay to appropriate law enforcement partners.

c) Capture available personally identifiable information (PII) and identification of UAS operator and relay info to appropriate law enforcement partners.
- Note: Flying a UAS in a restricted area is a violation of federal law (see Appendix A).

1.3 Coordinate Response and Attempt to Recover the UAS (reference section 2.2)

1) If UAS is recoverable, immediately contact your local FBI field office for the dedicated C-UAS Coordinator as well as your agencies' explosives ordinance disposal (EOD) units, and/or the FBI WMD Coordinator to render the device safe and secure the scene.

2) Coordinate combined external patrol response to prevent UAS from fleeing the area:

a) Share tracking data (e.g., direction of departure, video feeds, etc.) to assist in tracking the UAS and identifying the operator.

b) Alert nearby installations and critical infrastructure facilities in case the UAS attempts to target other sensitive areas.

3) If authorized under 124n and/or 130i legal frameworks, employ RF jamming.

a) Some federal agencies are authorized to use RF jamming countermeasures domestically. However, currently neither state nor local law enforcement are authorized to interfere with a drone in flight (see Appendix A).

4) Turn off the device, if recovered. Otherwise, conduct as little tampering as possible.

a) Do NOT handle the device without proper personal protective equipment (PPE) i.e. masks/face coverings, gloves, and/or Explosive Ordinance Disposal (EOD) suits. UAS may have the capability to record and/or capture facial recognition and biometrics.

b) See additional guidance on evidence handling procedures, (reference section 2.2).

5) Place the device in a faraday bag, if possible. This should prevent an external controller from communicating with the device, which could remotely wipe digital evidence.

6) Contact your local FBI Field Office for further technical exploitation (see Appendix H-I).

2. UAS Investigations Guide

This guidance has been created to maximize potential investigative avenues, and ensure the safety of the first responders, investigators and the general public.

2.1 Document Actions and Observations

Guidance: All activities conducted and observations made at the scene must be documented as soon as possible to preserve information. Visual observations of UAS activity— especially at night—***must*** be deconflicted with local manned or legitimate air traffic, as legitimate air activity is frequently mistakenly identified as drone activity.

The responding officer(s) should document observations of the scene, including the location of persons and items and the appearance and condition of the scene upon arrival.

Things to consider:

Questions to identify whether observed UAS activity represents a threat to public safety, national security, or involves federal criminal violations (see Appendix C-D).

- Was the UAS attempting to crash into manned aircraft?
- Was the UAS flying adjacent to, near, or over any part of an airport?
- Was the UAS flying over critical infrastructure such as a dam, nuclear plant, power substation, or government building?
- Was the UAS flying over or near a prison/correctional facility?
- Was the UAS flying over a military installation or facility associated with the defense industrial base (for example, US Navy submarine contractor)?
- Was the UAS flying over a mass gathering (for example, parade, sporting event, concert)?
- Was the UAS operating in a manner to harass people, livestock, or wildlife?
- Was the UAS flying over a wildfire or near emergency response aircraft?
- Were there any temporary (or permanent) flight restrictions in place in the area of the UAS flights at the time of the activity?
- Was there another reason the UAS warranted law enforcement notification or response?
- Does the facility/base have any UAS detection system(s) or were any other systems elsewhere present during the UAS incursion that may have detected the UAS?
- What type of UAS detection system(s) exists at your site and/or elsewhere, if any (if classified, report at the proper classification)?
- Did the UAS detection system(s) detect the UAS? Provide any information that was provided by the detection system including any .xml files or flight paths. Unsuccessful detection is also relevant investigative information.

- If a UAS mitigation system was used, what was the system name, time/duration used, and outcome? Unsuccessful mitigation is also relevant investigative information (if classified, report at the proper classification).
- Where was the UAS operator located when the UAS detection/mitigation system(s) was used?
- In what direction was the UAS detection/mitigation system(s) pointed during use?
- Did a UAS detection/mitigation system(s) work, while others did not? Please list the success of any and all detection/mitigation systems including facility security camera footage of the UAS.
- Were any other photos or videos of the UAS captured (i.e. witness, surveillance systems, closed-circuit television (CCTV))?
- Did the detection/mitigation system(s) corroborate a visual sighting?

If possible, attempt to identify whether or not Remote ID was being broadcast. Remote ID technology is either built into the UAS or retrofitted for legacy UAS and became mandatory as of March 16, 2024. A standard Remote ID drone broadcasts identification and location information of the drone and control station, via wi-fi or Bluetooth.

Remote ID Considerations (for UAS Only):

Was Remote ID being broadcast? (Dronehone via the AppStore, Google Play, or ATAk; other available apps are Drone Scanner and AirSentinel)

Exceptions for Remote ID of drones:

- Any drone NOT requiring FAA registration (i.e. weighing .55 lbs (250 gr.) or less AND being flown recreationally (14 CFR 89.101)) (see Appendix A and J); OR
- When operating within an FAA-recognized identification area (FRIA) (14 CFR 89.110(b) (see Appendix A)

These rules are subject to change by FAA. Review FAA website regularly for any updates and contact your FAA LEAP with any follow up questions.

Questions regarding the UAS Operator:

- Was the operator(s) of the UAS observed? How many? Provide a description of the person(s) and identification if possible.
- Were there suspicious vehicles nearby? Did the operator get into a vehicle? Vehicle description(s)? License plate(s)?
- How was the drone being controlled? Were they holding a controller or using any sort of electronics (including cell phones, which could be a controller)? ***All electronics—***

including cell phones, tablets, controllers, etc.—should be considered part of the UAS.

- Were photos or videos of the operator or vehicle captured (i.e. witness, surveillance systems, CCTV)?

Potential Operator Interview Questions:

- Ask for and make record of identification.
- Who was operating the drone?
- Why are you flying here?
- Did anyone direct you to fly here? Who? How did/do they communicate with you?
- Did you maintain line-of-sight with the drone at all times?
- How high did you fly the drone? Where did you fly it?
- What are you going to do with the video or photographs?
- How often do you fly the drone?
- Where did you purchase the drone?
- Did you receive any training on flying drones?
- Are you aware of FAA guidelines regarding drone operations?
- Did you check for any airspace restrictions? If so, what resources did you check?

Determine Pilot License/Certification:

- Drone operators must provide federal or state issued ID (think "license and registration", like a traffic stop) (see Appendix K).
- All drone operators are required to show proof of competency to operate; commercial pilots should possess a 14 CFR Part 107 Certificate; recreational operators are required to take the FAA TRUST Exam and show proof of TRUST certificate (refer to 49 USC 44809 or 14 CFR 107.7) (see Appendix B).
- The Part 107 Certificate, and/or TRUST Exam Certificate, and if applicable, a Certificate of Waiver/ Authorization must be provided to law enforcement (LE) upon request (see Appendix B).

Registration Considerations:

- Drone operators should show proof of registration in cases where:
  - the drone is required to be registered by virtue of the drone itself (i.e. if it weighs over 250 grams/0.55 lbs); or
  - the drone is, regardless of weight, being operated in a capacity wherein it requires registration (i.e. outside of the recreational exception)
- Recreational operators are required to register the drone if the drone weighs more than 0.55 pounds (see Appendix J).
- 107 Operations: a drone MUST be registered when being operated under Part 107 rather than under the exception for recreational. However, a PILOT who has a 107

certificate absolutely can operate an unregistered drone, as long as it is in accordance with the exception for recreational operations in 49 US Code 44809 (see Appendix I).

- Failure to register is a felony [49 USC § 46306(b)(5) and (6)] (see Appendix B).
- Registration numbers should be clearly labeled on the exterior of the UAS.

2.2 UAS Seizure

Guidance: If the determination has been made to seize the UAS, once it is rendered safe by local EOD or the FBI WMD Coordinator, the following guidance is provided to ensure that UAS seizures are conducted following recognized best practices (see Appendix H).

Drone Seizure Process:

1. Refer to CIRG's Drone Identification Guide to assist in the identification of the make and model of the UAS and complete research so that you are informed of the capability of the device that you have encountered and the respective data storage locations and digital intelligence or evidential opportunities available. Prior to any interaction with the user or the UAS device, consider how to obtain and handle evidence for the offense that you have witnessed or to which you have been called to respond.

Follow legal processes applicable to the FBI's Domestic Investigations and Operations Guide (DIOG) for proper searches and evidence collection.

2. Consider wet forensic (DNA and Fingerprint) evidence prior to any physical interaction with the UAS and remote control (RC). Ensure all handling of the device(s) is(are) mindful of the preservation of such evidence when considering seizure and packaging options. For example, wear gloves, consider wet forensic hot spots (power buttons, cable areas, joysticks, etc), and package carefully (in breathable material such as a faraday bag or cardboard box or bag, not plastic).

3. Rapidly consider the proximity of connected or associated devices that the UAS may be connected with or from which it is controlled. Most UASs have a short control range and so controllers/antennae are usually within close proximity. Attempt to locate the operator.

4. If possible, wear a mask or cover your face, approach the UAS from behind and obscure any cameras to avoid alerting the operator that the UAS may have been captured or compromised and/or prevent the UAS from recording facial recognition of any personnel when attempting to safely capture it. Assess whether the device is on (usually indicated by lights or noise on the unit) or off. Document the power state of the device and whether or not you have witnessed it powered on or off since arrival. If the device is on, review and record any information instantly available on any of its screens. Disable the flying ability of the device (using a non-tampering measure, such as putting a coat or net over the device, or tipping it over) until confident on how to safely shut down the specific drone make/model without causing data corruption.

5. Record key identifiers of the UAS, including the make, model, and serial number of the device. Identifiers may appear in different locations depending on the model being handled. Some UAS have QR codes which can be scanned to facilitate identification (although these can also be added by the pilot and introduce malware or corrupt/erase the data, so be careful before scanning).

6. If the UAS has a removable battery, remove this from the device. If there is a non-removable battery, power down the device by pressing the power button once, then pressing again and holding for two seconds (for DJI models) or switch to 'off' (depending on the model). Record the time at which any one of these steps is completed. CAUTION – If the battery has any signs of damage or leakage, do not remove or tamper as the battery could cause injury or explosion.

7. Record any readily identifiable modifications to the UAS or additional solutions and payloads, which may offer additional functionality, located on the device/in the proximity of the device.

8. Package the UAS and RC independently in separate faraday enclosures/bags to prevent over the air contamination and remote wiping. Package additional connected/associated devices in separate faraday bags, but record that they were found in proximity. Devices linked but located separately/a distance from the device should be treated as independent exhibits and packaged accordingly.

9. In the event a search warrant is required, please contact your local field office C-UAS Coordinator for search warrant examples from past cases. Please also refer to FBI-HQ existing resources for additional UAS search warrant and affidavit examples.

3. UAS Reporting Instructions

The effectiveness of our defense against UAS threats is only as strong as our commitment to detailed and consistent reporting. By working together and sharing timely information, we strengthen not just our individual installations but the entire defense framework of our nation.

3.1 Where to Report (eGuardian)

The FBI has requested all partners—including DoD, cleared defense contractors (CDC), critical infrastructure entities, state, local, tribal, and territorial law enforcement (SLTT), and others—to report all incidents of UAS incursions on critical infrastructure, threats to life, or mass gatherings to the FBI through the eGuardian platform. CDC's are further required to report suspicious incidents to the Defense Counterintelligence and Security Agency (DCSA) as required in 32 CFR Part 117 (National Industrial Security Program Operating Manual). DCSA FBI Counterintelligence Task Force, Task Force Members will ensure all respective reporting will be

entered into eGuardian or coordinate eGuardian reporting through the FBI or the Military Department Counterintelligence Organization (see Appendix B).

eGuardian Reporting Guidelines for UAS Incursions:

- All law enforcement partners are encouraged to tag any UAS incidents at DoD facilities, DCI facilities, and Defense Industrial Base (DIB) into eGuardian with the tag #UXSINCURSION (see Appendix L).
    - The FBI's eGuardian system is used to document, share, and track potential threats, suspicious activity, and cyber, counterterrorism, counterintelligence, and criminal incidents (collectively, "incidents") among the FBI and partners, as required by DoD Instruction (DoDI) 2000.26.
    - Law Enforcement or intelligence community partners can request an eGuardian account through the FBI's Law Enforcement Enterprise Portal (LEEP) at https://www.cjis.gov/ (see Appendix L).
- All other UAS incidents involving critical infrastructure, threats to life, or mass gatherings should be reported into eGuardian with the tag #REPORTEDUASSIGHTINGS (see Appendix B).
- All other private sector entities can report incidents via https://tips.fbi.gov (see Appendix M) using the reporting guidelines on the following page or they can reach out to their FBI Office of Private Sector Coordinator at their local FBI Field Office.

3.2 What to Include in Your Report

Please include any answers to questions from Section 2.1 with as much detail as possible. Should any answers rise above the classification capabilities of eGuardian, please only include appropriate information and work with your local FBI Field Office Joint Terrorism Task Force or Counterintelligence Task Force.

***** Reminder, if the answer to any of the above questions (i.e. counter UAS systems and their effectiveness) raises the classification of your report. eGuardian is only authorized to handle information up to U//FOUO//LES. *****

Appendices

Appendix A: Statutes/Potential Federal Violations Involving UxS/UAS Activity

6 USC §124n: Protection of certain facilities and assets from unmanned aircraft

10 U.S. Code § 130i: Protection of certain facilities and assets from unmanned aircraft

18 USC § 32(5): Endangering Operator of an Aircraft – Felony

18 USC § 39B(a)(1)-(2): Unsafe Operation of a UAS – Misdemeanor

18 USC § 39B(b)(1): Runway Exclusion Zone – Misdemeanor

18 USC § 40A: Operation of UAS over Wildfires – Felony

18 USC § 175-178 Biological Weapons

18 USC § 229 et sec. Chemical Weapons

18 USC § 792 Harboring or Concealing Persons

18 USC § 793 Gathering, transmitting or losing defense information

18 USC § 794 et sec. Espionage

18 USC § 795: Photographing Defense Installations – Misdemeanor

18 USC § 796: Use of Aircraft for photographing Defense Installations – Misdemeanor

18 USC § 831 et sec. Nuclear Material and Explosives

18 USC § 2332a et sec. Terrorism

18 USC § 31752(a)(5): Restricted buildings and grounds

49 USC § 44801: Definitions

49 USC § 46306(b)(5) & (6): Failure to Register – Felony

49 USC § 46306(b)(7) & (8): Operation without Certificate – Felony

49 USC § 46307: Violation of National Defense Airspace and Tactical Flight Restrictions (TFRs) – Misdemeanor

49 USC § 46320: Interference with Wildfire

14 CFR § 89.110: Remote ID requirements

14 CFR § 107.12(b): Certificate Required

14 CFR § 107.23(a): Hazardous Operation 14 CFR § 107.13: UAS not registered

14 CFR § 107.39: Flying over people (exception: 4 categories allowed)

14 CFR § 107.41: Operation in Certain Airspace 14 CFR § 107.29(a): Flying at night without required equipment

Appendix B: Critical Infrastructure

There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience advances a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure. This directive supersedes Homeland Security Presidential Directive 7.

Critical Infrastructure Sectors Include:

- Chemical Sector
- Commercial Facilities Sector
- Communications Sector
- Critical Manufacturing Sector
- Dams Sector
- Defense Industrial Base Sector
- Emergency Services Sector
- Energy Sector
- Financial Services Sector
- Food and Agriculture Sector
- Government Services and Facilities Sector
- Healthcare and Public Health Sector
- Information Technology Sector
- Nuclear Reactors, Materials, and Waste Sector
- Transportation Systems Sector
- Water and Wastewater Systems

Appendix C: eGuardian Reporting Questionnaire (Printable Copy Available on SharePoint) - Can be used as outreach document

UXS Incident Report Questionnaire Aerial – Ground – Maritime (Surface/Sub Surface) Systems			
*** Take Pictures of Items if Possible ***			
Reporting Agency's Name:			
Reporting Agency's Telephone Number:			
Reporting Officer's Name and ID Number:			
Reporting Officer's Telephone and Email:	Telephone Number:		Email Address:
Associated Report/Incident Numbers:			
Incident Date & Time:	Date:		Time:
Approximate Location of Incident:			
UXS / UAS Operator Information			
Operator's Name:	Last:	First:	Middle:
Date of Birth (Month/Day/Year):			
Current Address:			
	State:		Zip:
If address on ID is not Current Address, include ID Address here:			
	State:		Zip:
Phone: Mobile Home Work			
Email: Personal Work			
UAS Remote Pilot Certificate:	*Yes	No	#:
Recreational Operator TRUST Completion Certificate:	**Yes	No	#:
* If yes, the remote pilot shall have in their physical possession their Remote Pilot Certificate and Identification (Contains a photo, signature, date of birth, and permanent mailing address) and is made available to the FAA, NTSB, TSA, and any Federal State or Local Law Enforcement Officer. ** If yes, operator maintains TRUST Completion Certificate (electronic copy OK) and is made available to the FAA or Law Enforcement Officer upon request.			
UXS / UAS Information			
* Please provide information regarding associated individuals on the back of this form			
Make:			
Model:			
Registration (Reg) #:	Yes	No	#:
Is Reg # visible on exterior of UAS?	Yes	No	
UAS Serial #:			
Information on Operation of UAS			
Did the reporting officer witness the individual operating the UAS?	Yes	No	
Was there a witness to the individual operating the UAS?	Yes	No	Contact Information:
What was the purpose of the flight? (Operator & Witness version)			
Who was the remote Pilot-In-Command or Operator?			
Was an airspace authorization or waiver obtained?	*Yes	No	How?

Appendix D: National Threat Operations Center UAS Intake Questionnaire

Unmanned Aircraft Systems (UAS), aka Drones

Define the specific threat or possible federal criminal activity:

1. **What UAS/drone activity are you reporting to the FBI?** (see if response aligns to any of the options below)

   Possible threats to public safety or national security, or federal criminal violations are below:

   a. UAS is attempting/attempted to crash into manned aircraft
   b. UAS is flying adjacent to, near, or over an airport runway/tarmac
   c. UAS is flying over or near a prison/correctional facility
   d. UAS is flying over a military installation or facility associated with the defense industrial base (i.e., US Navy submarine contractor)
   e. UAS is flying over critical infrastructure such as a dam, nuclear plant, power sub-station, government building
   f. UAS is flying over a mass gathering (i.e., parade, sporting event, concert)
   g. UAS is flying over a wildfire
   h. UAS is flying near people, houses, cars, or buildings (i.e., possible unsafe operation of a UAS)
   i. UAS is transporting observable payload (i.e., something is attached to the underside of the UAS)
   j. Other reason complainant feels UAS activity warrants law enforcement notification or response

Obtain Details of Activity Observed:

1. **Where is/was the UAS flying?**

   a. Location of UAS sighting (City, County/Parish, State, or landmark nearby)
   b. Date/Time of UAS sighting

2. **Gather UAS/Drone Information:**

   a. What direction was the UAS travelling (i.e., North to South; East to West; etc.)?
   b. Did it hover like a helicopter or remain in constant flight like an airplane?
   c. Did you observe it take off or land? If so, provide the location (i.e., address, landmark, intersection)
   d. Did it look like an airplane (fixed-wing) or a helicopter/quadcopter (rotary-wing) or something else?

Appendix D: National Threat Operations Center UAS Intake Questionnaire Cont.

e. Any visible lights? If so, what was their color, pattern, total number, location on drone?
    i. Were the lights constantly on, or did they turn on and off?
    ii. What were the light repetition details (rapid red blinking, normal navigational blinking white, green, and/or red lights etc.).
f. Any attachments on the UAS such as a camera or other payload? Describe.
g. Any sounds made by the UAS?
h. Total number of UAS seen?
    i. If more than one UAS, did they fly in formation (synchronized) or appear scattered/random/uncoordinated?

3. Gather Drone Operator Information

a. Did you see the person flying the drone? If so, provide a description of the person.
b. Did the operator have a vehicle? If so, provide description of the vehicle and license plate.

4. Additional Details

a. Were you able to take photos or videos of your observations which you can provide?
b. Have you reported this information to any other law enforcement agency?
    i. When (date/time) and how did you report the information (i.e., call or e-mail)?
    ii. What phone number or e-mail address did you use when making the report (i.e., complainant's phone number/e-mail in case different from what was provided already)?
    iii. What's the name of the law enforcement agency?
    iv. Do you have a police report number or any kind of reference number?

Appendix E: FBI Field Office Contact Sheet

- **Alabama**

Birmingham Field Office

1000 18th Street North
Birmingham, AL 35203-1000

Phone: (205) 326-6166

Mobile Field Office

200 N. Royal Street
Mobile, AL 36602-3998

Phone: (251) 438-3674

USPS Only:
P. O. Box 2128
Mobile, AL 36652-2128

- **Alaska**

Anchorage Field Office

101 East 6th Avenue
Anchorage, AK 99501-2523

Phone: (907) 276-4441

- **Arizona**

Phoenix Field Office

21711 North 7th Street
Phoenix, AZ 85024-5118

Phone: (623) 466-1999

- **Arkansas**

Little Rock Field Office

24 Shackleford W. Blvd
Little Rock AR 72211-3755

Phone: (501) 221-9100

- **California**

Los Angeles Field Office

11000 Wilshire Blvd., Suite 1700, FOB
Los Angeles, CA 90024-3601

Phone: (310) 477-6565

Sacramento Field Office

2001 Freedom Way
Roseville, CA 95678

Phone: (916) 746-7000

San Diego Field Office

10385 Vista Sorrento Parkway
San Diego, CA 92121

Phone: (858) 320-1800

San Francisco Field Office

450 Golden Gate Avenue, 13th Floor
San Francisco, CA 94102-9523

Phone: (415) 553-7400

USPS Only:
P. O. Box 36015
San Francisco, CA 94102

- **Colorado**

Denver Field Office

8000 East 36th Avenue
Denver, CO 80238-2831

Phone: (303) 629-7171

- **Connecticut**

New Haven Field Office

600 State Street
New Haven, CT 06511-6505

Phone: (203) 777-6311

- **District of Columbia**

Washington Field Office

USPS and FedEx Only:
601 4th Street NW
Washington, D.C. 20535-0002

Phone: (202) 278-2000

All Other Commercial Shipments:
FBI - Washington Field Office
2400 Schuster Drive
Cheverly, MD 20781-1121

- **Florida**

Jacksonville Field Office

6061 Gate Parkway
Jacksonville, FL 32256-7287

Phone: (904) 248-7000

Miami Field Office

2030 S.W. 145th Avenue
Miramar, FL 33027-6150

Phone: (754) 703-2000

Tampa Field Office

5525 West Gray Street
Tampa, FL 33609-1007

Phone: (813) 253-1000

- **Georgia**

Atlanta Field Office

2635 Century Parkway NE, Suite 400
Atlanta, GA 30345-3128

USPS Only:
P. O. Box 98128
Atlanta, GA 30359-1828

Phone: (404) 679-9000

- **Hawaii**

  Honolulu Field Office

  91-1300 Enterprise Avenue
  Kapolei, HI 96707

  Phone: (808) 566-4300

- **Illinois**

  Chicago Field Office

  2111 W. Roosevelt Road
  Chicago, IL 60608-1128

  Phone: (312) 421-6700

  Springfield Field Office

  900 E. Linton Avenue
  Springfield, IL 62703-5920

  Phone: (217) 522-9675

- **Indiana**

  Indianapolis Field Office

  8825 Nelson B. Klein Parkway
  Indianapolis, IN 46250-3512

  Phone: (317) 595-4000

- **Kentucky**

  Louisville Field Office

  12401 Sycamore Station Place
  Louisville, KY 40299-6198

  Phone: (502) 263-6000

- **Louisiana**

  New Orleans Field Office

  2901 Leon C. Simon Blvd.
  New Orleans, LA 70126-1061

  Phone: (504) 816-3000

- **Maryland**

  Baltimore Field Office

  2600 Lord Baltimore Drive
  Baltimore, MD 21244-2754

  Phone: (410) 265-8080

- **Massachusetts**

  Boston Field Office

  201 Maple Street
  Chelsea, MA 02150

  Main: (857) 386-2000

- **Michigan**

  Detroit Field Office

  477 Michigan Avenue
  26th Floor, P. V. McNamara FOB
  Detroit, MI 48226-2598

  Phone: (313) 965-2323

- **Minnesota**

  Minneapolis Field Office

  1501 Freeway Blvd.
  Brooklyn Center, MN 55430-1705

  Phone: (763) 569-8000

- **Mississippi**

  Jackson Field Office

  1220 Echelon Parkway
  Jackson, MS 39213-8219

  Phone: (601) 948-5000

- **Missouri**

  Kansas City Field Office

  11180 NW Prairie View Road
  Kansas City, Missouri 64153

  Phone: (816) 512-8200

  St. Louis Field Office

  2222 Market Street
  St. Louis, MO 63103-2516

  Phone: (314) 231-4324

- **Nebraska**

  Omaha Field Office

  4411 South 121st Court
  Omaha, NE 68137-2112

  Phone: (402) 493-8688

- **Nevada**

  Las Vegas Field Office

  John Lawrence Bailey Memorial Bldg.
  1787 West Lake Mead Blvd.
  Las Vegas, NV 89106-2135

  Phone: (702) 385-1281

- **New Jersey**

  Newark Field Office

  Barry Lee Bush Memorial Bldg.
  Claremont Tower
  11 Centre Place
  Newark, NJ 07102-4533

  Phone: (973) 792-3000

  USPS Only:
  P. O. Box 1158
  Newark, NJ 07101-1158

- **New Mexico**

  Albuquerque Field Office

  4200 Luecking Park Avenue NE
  Albuquerque, NM 87107-4743

  Phone: (505) 889-1300

- **New York**

Albany Field Office

200 McCarty Avenue
Albany, NY 12209-2095

Phone: (518) 465-7551

Buffalo Field Office

One FBI Plaza
Buffalo, NY 14202-2698

Phone: (716) 856-7800

New York City Field Office

26 Federal Plaza, 23rd Floor
New York, NY 10278-0004

Phone: (212) 384-1000

- **North Carolina**

Charlotte Field Office

7915 Microsoft Way
Charlotte, NC 28273-8200

Phone: (704) 672-6100

- **Ohio**

Cincinnati Field Office

2012 Ronald Reagan Drive
Cincinnati, OH 45236-2373

Phone: (513) 421-4310

Cleveland Field Office

1501 Lakeside Avenue
Cleveland, OH 44114-1138

Phone: (216) 522-1400

- **Oklahoma**

Oklahoma City Field Office

3301 W. Memorial Road
Oklahoma City, OK 73134-0902

Phone: (405) 290-7770

USPS Only:
P. O. Box 568801
Oklahoma City, OK 73156-8801

- **Oregon**

Portland Field Office

9109 NE Cascades Parkway
Portland, OR 97220-6813

Phone: (503) 224-4181

- **Pennsylvania**

Philadelphia Field Office

Pittsburgh Field Office

William J. Green Jr. FOB
600 Arch Street, 8th Floor
Philadelphia, PA 19106-1675

Phone: (215) 418-4000

3311 E. Carson Street
Pittsburgh, PA 15203-2148

Phone: (412) 432-4000

- **Puerto Rico**

San Juan Field Office

Federal Bureau of Investigation
140 Carlos Chardon Avenue
Hato Rey, PR 00918

Phone: (787) 754-6000

USPS Only:
P. O. Box 366269
San Juan, PR 00936-6269

- **South Carolina**

Columbia Field Office

151 Westpark Blvd.
Columbia, SC 29210-3857

Phone: (803) 551-4200

- **Tennessee**

Nashville Field Office

2868 Elm Hill Pike
Nashville, TN 37214

Phone: (615)-232-7500

- **Texas**

Dallas Field Office

J. Gordon Shanklin Bldg.
One Justice Way
Dallas, TX 75220-5220

Phone: (972) 559-5000

Houston Field Office

El Paso Field Office

660 South Mesa Hills Drive
Suite 3000
El Paso, TX 79912-5533

Phone: (915) 832-5000

USPS Only:
P. O. Box 926277
Houston, TX 77072-6277

San Antonio Field Office

5740 University Heights
San Antonio, TX 78249-1835

Phone: (210) 225-6741

1 Justice Park Drive
Houston, TX 77092-1908

Phone: (713) 693-5000

- **Utah**

Salt Lake Field Office

5425 W. Amelia Earhart Drive
Salt Lake City, UT 84116-3713

Phone: (801) 579-1400

USPS Only:
P. O. Box 3235
Salt Lake City, UT 84110-3235

- **Virginia**

Norfolk Field Office

509 Resource Row
Chesapeake, VA 23320

Phone: (757) 455-0100

Richmond Field Office

1970 E. Parham Road
Richmond, VA 23228-2206

Phone: (804) 261-1044

- **WASHINGTON**

Seattle Field Office

1110 Third Avenue
Seattle, WA 98101-2904

Phone: (206) 622-0460

- **Wisconsin**

Milwaukee Field Office

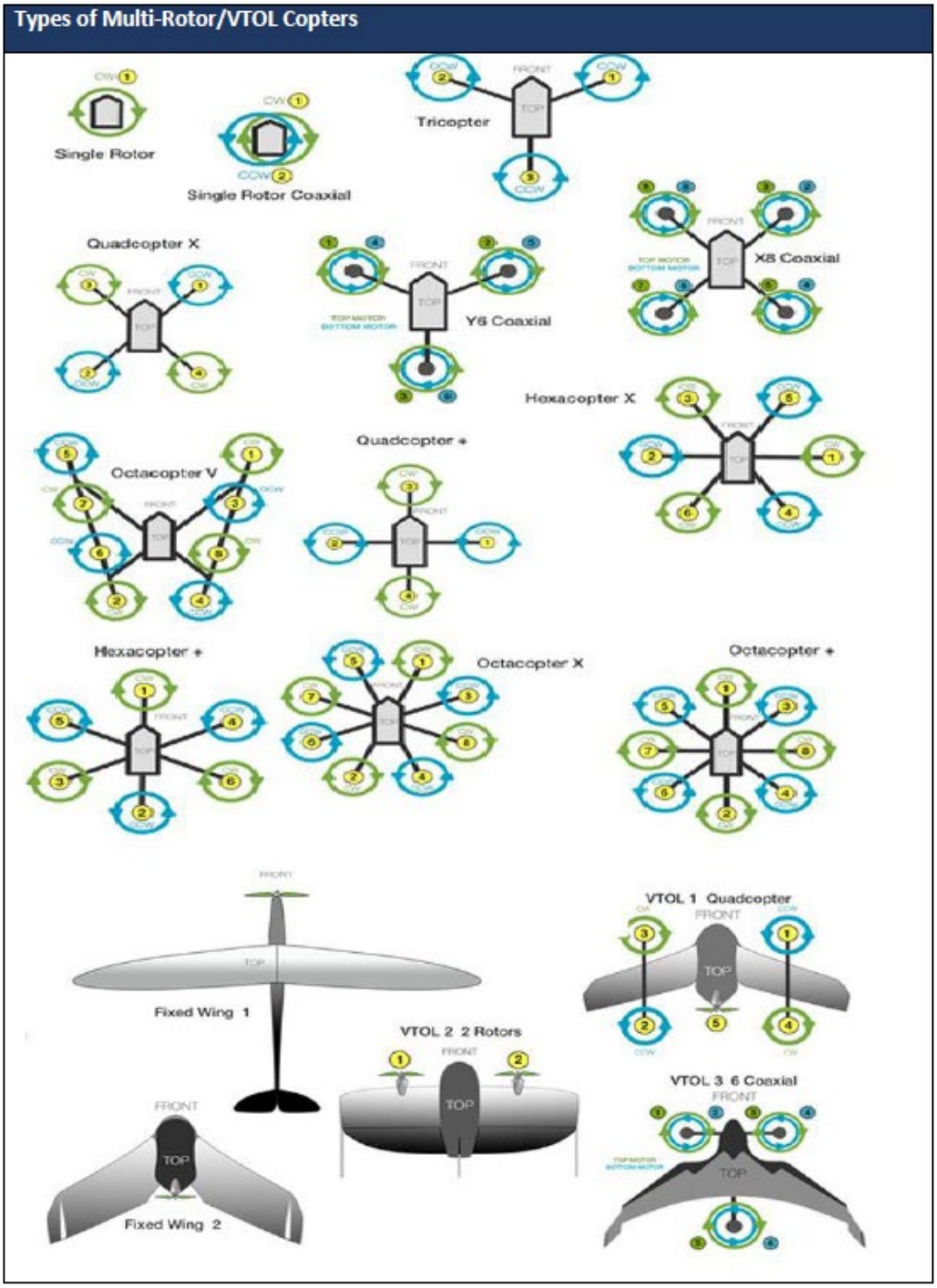
3600 S. Lake Drive
St. Francis, WI. 53235-3716

Phone: (414) 276-4684

Appendix F: Types of UAS/Drones

Drone Type	Pros	Cons	Typical Uses
Multi-Rotor 	• Accessibility. • Ease of use. • VTOL and hover flight. • Good camera control. • Can operate in a confined area.	• Short flight times. • Small payload capacity.	Aerial photography and video aerial inspection
Fixed-Wing 	• Long endurance. • Large area coverage. • Fast flight speed.	• Launch and recovery can require a lot of space. • No VTOL/hover. • Non-autonomous are harder to fly, more training needed. • Expensive.	Delivery, aerial mapping, and pipeline and power line inspection
Single-Rotor 	• VTOL and hover flight. • Long endurance (with gas power). • Heavier payload capability.	• More dangerous. • Harder to fly, more training needed. • Expensive.	Aerial LIDAR laser scanning
Fixed-Wing Hybrid 	• VTOL and long-endurance flight.	• Not perfect at either hovering or forward flight. • Still in development.	Delivery
Elios 	• Collision tolerant. • Designed for indoor/confined space operation. • Dust and splash resistant.	• Expensive.	Accessing the inaccessible, and indoor/confined space inspection

Appendix F: Types of UAS/Drones Cont.



Appendix G: FBI Technical Exploitation Unit (TExU) UAS Evidence Collection and Handling Slick Sheet (Printable Copy Available on SharePoint)

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE

Unmanned Aerial System (UAS) Evidence Collection and Handling

PURPOSE: To provide recommendations regarding the collection and handling of unmanned aerial system evidence.

Technical Exploitation Unit (TExU)

Email: TEDAC_TEXU@fbi.gov
Unet Sharepoint: https://dojfbi.sharepoint.us/teams/007436

(U) Safety:
When approaching a downed or crashed UAS, keep safety procedures in mind as the device could present a hazardous situation. UASs may carry dangerous materials as payloads, including deadly narcotics or explosives.

(U//LES) Render Safe Considerations:
If the UAS appears to have been modified, have a payload other than a camera/sensor, or other circumstances exist which warrant further evaluation of the UAS, then:
- Secure a perimeter around the UAS
- Contact the local bomb squad or FBI SABT, as required

(U) Collection:
Wear gloves and masks!
- Avoid excessive contact with areas prone to have latent prints and/or DNA
- Consider trace evidence (hairs or fibers) when tape or Velcro tabs are present

Why? Biometric evidence may be critical in identifying the owner/operator of the UAS. Gloves and masks help to prevent contaminating the evidence.

Areas for Biometrics
Propellers
Battery
Power button
Drop mechanism
Tape / Velcro

(U) Items for collection:
- Unmanned System device – often capable of storing media and flight data on internal memory components
- Device controller – may contain media files, flight data, and user information
- Mobile devices associated with controllers – cell phones and tablets
- External Media – micro-SD cards

(U) Evidence Handling:
- Ensure the device is powered **OFF** as soon as safe to do so
- Remove device power source – disconnect or remove battery
- Do not attempt to power on

Why? Data can be destroyed or altered. UAS devices transmit signals to controllers and satellites, which can overwrite stored flight data and/or capture images.

(U) Evidence Packaging:
Package UAS(s) for transportation in an appropriately sized, clean, and sturdy box or container that prevents excessive movement.

Package UAS batteries as hazardous material and ship via certified hazmat shippers. Devices involved in a crash or detonation may pose a fire hazard.

(U) Technical Exploitation:
The FBI's Technical Exploitation Unit (TExU) employs non-destructive methods to extract data from UAS platforms in a forensically sound manner. The techniques produce results beyond the capabilities of current commercially available tools. Contact TExU for assistance on investigations requiring UAS exploitation.

Potential Data Recovery
Images (saved / deleted)
Videos
Device Information
- Bluetooth Addresses
- MAC Addresses
- Model/Serial Numbers
- Firmware Version

Flight Data
- GPS Coordinates
- Deleted Flight Data
- Home Points
- Log Files
- Network Information
- Battery Information

User Information
- Email address
- Registered account

System Logs

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE

Appendix H: UAS Resources

Law Enforcement:

- Law Enforcement Enterprise Portal (LEEP), Justice Connect/COI/sUAS Outreach Toolbox
- FBI CIRG C-UAS Team:
- eGuardian (Suspicious Activity Reporting)

FAA:

- FAA LEAP
- FAA Public Safety & LE Toolkit
- FAA Drone Zone
- Policy Document Library: faa.gov/uas/resources/policy_library

FAA Approved Open-Source Apps

General Use Phone Applications

Restricted Air Space Phone Applications

Appendix I: Summary of Code of Federal Regulations: Part 107—Small Unmanned Aircraft Systems

Certificated Remote Pilots including Commercial Operators	The Operations Over People rule became effective on April 21, 2021. Drone pilots operating under Part 107 may fly at night, over people and moving vehicles without a waiver as long as they meet the requirements defined in the rule. Airspace authorizations are still required for night operations in controlled airspace under 400 feet. If you have a small drone that is less than 55 pounds, you can fly for work or business by following the Part 107 guidelines. To fly under Part 107 rules, there are 3 main steps. Step 1: Learn the Rules Make sure you understand what is and is not allowed under Part 107 rules. • 14 CFR Part 107 Small Unmanned Aircraft Systems If you are not sure if Part 107 rules work for you and your intended operation check our user identification tool. Some operations will require a waiver. Here are the regulations specified in §107.205 that are subject to waiver: • Operation from a moving vehicle or aircraft - §107.25 • Operation at Night - §107.29(a)(2) and (b) • Visual line of sight aircraft operation - §107.31 • Visual observer - §107.33 • Operation of multiple small unmanned aircraft systems - §107.35 • Yielding the right of way - §107.37(a) • Operation over human beings - §107.39 • Operation in certain airspace - §107.41 • Operating limitations for small unmanned aircraft - §107.51 • Operations Over Moving Vehicles - §107.145 Learn more about Part 107 Waivers. Drone operators should avoid flying near airports because it is difficult for manned aircraft to see and avoid a drone while flying. Remember that drone operators must avoid manned

	aircraft and are responsible for any safety hazard their drone creates in an airport environment. Step 2: Become an FAA-Certified Drone Pilot by Passing the Unmanned Aircraft General - Small (UAG) Knowledge Test To be eligible to get your Remote Pilot Certificate, you must be: • At least 16 years old • Able to read, write, speak, and understand English • Be in a physical and mental condition to safely fly a UAS Study for the Knowledge Test • Review Knowledge Test Suggested Study Materials provided by the FAA. Obtain an FAA Tracking Number (FTN) • Create an Integrated Airman Certification and Rating Application (IACRA) profile prior to registering for the knowledge test. **Schedule an Appointment** • Take the Unmanned Aircraft General - Small (UAG) Knowledge Test at an FAA-approved Knowledge Testing Center. **Complete FAA Form 8710-13** • Once you've passed your test, for a remote pilot certificate (FAA Airman Certificate and/or Rating Application) login the FAA Integrated Airman Certificate and/or Rating Application system (IACRA)* to complete FAA form 8710-13. • Review the full process to get your Remote Pilot Certificate. Step 3: Register your Drone with the FAA Registration costs $5 and is valid for 3 years. You'll need a credit or debit card and the make and model of your drone handy in order to register. Learn more about registering your drone. • Create an account and register your drone at FAADroneZone. Select "Fly sUAS under Part 107." • Once you've registered, mark your drone (PDF) with your registration number in case it gets lost or stolen. • Beginning September 16, 2023, if your drone requires an FAA registration number it will also be required to

	broadcast Remote ID information (unless flown within a FRIA). For more information on drone registration, visit How to Register Your Drone. **Visiting from another country? Using a foreign-registered drone?** Be sure to check out our page: International UAS Operators in the United States Learn more about Registration and Marking Requirements for Small Unmanned Aircraft, 14 CFR part 48. Remember • Always fly your drone safely and within FAA guidelines and regulations. • It is up to you as a drone pilot to know the rules of the sky, and where it is and is not safe to fly. Aren't sure if Part 107 is right for you and your operation? Contact us for more information.
CODE OF FEDERAL REGULATIONS: PART 107—SMALL UNMANNED AIRCRAFT SYSTEMS **Authority:49 U.S.C. 106(f), 40101 note, 40103(b), 44701(a)(5), 46105(c), 46110, 44807.** **Source:Docket FAA-2015-0150, Amdt. 107-1, 81 FR 42209, June 28, 2016, unless otherwise noted.**	**§ 107.1 Applicability.** (a) Except as provided in paragraph (b) of this section, this part applies to the registration, airman certification, and operation of civil small unmanned aircraft systems within the United States. This part also applies to the eligibility of civil small unmanned aircraft systems to operate over human beings in the United States. (b) This part does not apply to the following: (1) Air carrier operations; (2) Any aircraft subject to the provisions of 49 U.S.C. 44809; (3) Any operation that the holder of an exemption under section 333 of Public Law 112-95 or 49 U.S.C. 44807 elects to conduct pursuant to the exemption, unless otherwise specified in the exemption; or (4) Any operation that a person elects to conduct under part 91 of this chapter with a small unmanned aircraft system that has been issued an airworthiness certificate. [Amdt. 107-8, 86 FR 4381, Jan. 15, 2021]
Operational Limitations	**§ 107.19 Remote pilot in command.** (a) A remote pilot in command must be designated before or during the flight of the small unmanned aircraft.

	(b) The remote pilot in command is directly responsible for and is the final authority as to the operation of the small unmanned aircraft system. (c) The remote pilot in command must ensure that the small unmanned aircraft will pose no undue hazard to other people, other aircraft, or other property in the event of a loss of control of the small unmanned aircraft for any reason. (d) The remote pilot in command must ensure that the small UAS operation complies with all applicable regulations of this chapter. (e) The remote pilot in command must have the ability to direct the small unmanned aircraft to ensure compliance with the applicable provisions of this chapter. [Docket FAA-2015-0150, Amdt. 107-1, 81 FR 42209, June 28, 2016, as amended by Amdt. 107-8, 86 FR 4382, Jan. 15, 2021] **§ 107.21 In-flight emergency.** (a) In an in-flight emergency requiring immediate action, the remote pilot in command may deviate from any rule of this part to the extent necessary to meet that emergency. (b) Each remote pilot in command who deviates from a rule under paragraph (a) of this section must, upon request of the Administrator, send a written report of that deviation to the Administrator. **§ 107.23 Hazardous operation.** No person may: (a) Operate a small unmanned aircraft system in a careless or reckless manner so as to endanger the life or property of another; or (b) Allow an object to be dropped from a small unmanned aircraft in a manner that creates an undue hazard to persons or property. **§ 107.25 Operation from a moving vehicle or aircraft.** No person may operate a small unmanned aircraft system— (a) From a moving aircraft; or (b) From a moving land or water-borne vehicle unless the small unmanned aircraft is flown over a sparsely populated area and is not transporting another person's property for compensation or hire. **§ 107.31 Visual line of sight aircraft operation.**

	(a) With vision that is unaided by any device other than corrective lenses, the remote pilot in command, the visual observer (if one is used), and the person manipulating the flight control of the small unmanned aircraft system must be able to see the unmanned aircraft throughout the entire flight in order to: (1) Know the unmanned aircraft's location; (2) Determine the unmanned aircraft's attitude, altitude, and direction of flight; (3) Observe the airspace for other air traffic or hazards; and (4) Determine that the unmanned aircraft does not endanger the life or property of another. (b) Throughout the entire flight of the small unmanned aircraft, the ability described in paragraph (a) of this section must be exercised by either: (1) The remote pilot in command and the person manipulating the flight controls of the small unmanned aircraft system; or (2) A visual observer. **§ 107.33 Visual observer.** If a visual observer is used during the aircraft operation, all of the following requirements must be met: (a) The remote pilot in command, the person manipulating the flight controls of the small unmanned aircraft system, and the visual observer must maintain effective communication with each other at all times. (b) The remote pilot in command must ensure that the visual observer is able to see the unmanned aircraft in the manner specified in § 107.31. (c) The remote pilot in command, the person manipulating the flight controls of the small unmanned aircraft system, and the visual observer must coordinate to do the following: (1) Scan the airspace where the small unmanned aircraft is operating for any potential collision hazard; and (2) Maintain awareness of the position of the small unmanned aircraft through direct visual observation. **§ 107.35 Operation of multiple small unmanned aircraft.** A person may not manipulate flight controls or act as a remote pilot in command or visual observer in the operation of more than one unmanned aircraft at the same time.

	[Amdt. 107-8, 86 FR 4382, Jan. 15, 2021] **§ 107.41 Operation in certain airspace.** No person may operate a small unmanned aircraft in Class B, Class C, or Class D airspace or within the lateral boundaries of the surface area of Class E airspace designated for an airport unless that person has prior authorization from Air Traffic Control (ATC). **§ 107.43 Operation in the vicinity of airports.** No person may operate a small unmanned aircraft in a manner that interferes with operations and traffic patterns at any airport, heliport, or seaplane base. **§ 107.45 Operation in prohibited or restricted areas.** No person may operate a small unmanned aircraft in prohibited or restricted areas unless that person has permission from the using or controlling agency, as appropriate. **§ 107.51 Operating limitations for small unmanned aircraft.** A remote pilot in command and the person manipulating the flight controls of the small unmanned aircraft system must comply with all of the following operating limitations when operating a small unmanned aircraft system: (a) The groundspeed of the small unmanned aircraft may not exceed 87 knots (100 miles per hour). (b) The altitude of the small unmanned aircraft cannot be higher than 400 feet above ground level, unless the small unmanned aircraft: (1) Is flown within a 400-foot radius of a structure; and (2) Does not fly higher than 400 feet above the structure's immediate uppermost limit. (c) The minimum flight visibility, as observed from the location of the control station must be no less than 3 statute miles. For purposes of this section, flight visibility means the average slant distance from the control station at which prominent unlighted objects may be seen and identified by day and prominent lighted objects may be seen and identified by night. (d) The minimum distance of the small unmanned aircraft from clouds must be no less than: (1) 500 feet below the cloud; and (2) 2,000 feet horizontally from the cloud.

Pilot Eligibility and Remote Pilot Certification	**§ 107.61 Eligibility.** Subject to the provisions of §§ 107.57 and 107.59, in order to be eligible for a remote pilot certificate with a small UAS rating under this subpart, a person must: (a) Be at least 16 years of age; (b) Be able to read, speak, write, and understand the English language. If the applicant is unable to meet one of these requirements due to medical reasons, the FAA may place such operating limitations on that applicant's certificate as are necessary for the safe operation of the small unmanned aircraft; (c) Not know or have reason to know that he or she has a physical or mental condition that would interfere with the safe operation of a small unmanned aircraft system; and (d) Demonstrate aeronautical knowledge by satisfying one of the following conditions, in a manner acceptable to the Administrator: (1) Pass an initial aeronautical knowledge test covering the areas of knowledge specified in § 107.73; or (2) If a person holds a pilot certificate (other than a student pilot certificate) issued under part 61 of this chapter and meets the flight review requirements specified in § 61.56, complete training covering the areas of knowledge specified in § 107.74. [Docket FAA-2015-0150, Amdt. 107-1, 81 FR 42209, June 28, 2016, as amended by Amdt. 107-8, 86 FR 4382, Jan. 15, 2021] **§ 107.63 Issuance of a remote pilot certificate with a small UAS rating.** An applicant for a remote pilot certificate with a small UAS rating under this subpart must make the application in a form and manner acceptable to the Administrator. (a) The application must include either: (1) Evidence showing that the applicant passed an initial aeronautical knowledge test. If applying using a paper application, this evidence must be an airman knowledge test report showing passage of the knowledge test; or (2) If a person holds a pilot certificate (other than a student pilot certificate) issued under part 61 of this chapter and meets the flight review requirements specified in § 61.56, a certificate of completion of an initial training course under this part that covers the areas of knowledge specified in § 107.74.

	(b) If the application is being made pursuant to paragraph (a)(2) of this section: (1) The application must be submitted to the responsible Flight Standards office, a designated pilot examiner, an airman certification representative for a pilot school, a certificated flight instructor, or other person authorized by the Administrator; (2) The person accepting the application submission must verify the identity of the applicant in a manner acceptable to the Administrator; and (3) The person making the application must, by logbook endorsement or other manner acceptable to the Administrator, show the applicant meets the flight review requirements specified in § 61.56 of this chapter. [Docket FAA-2015-0150, Amdt. 107-1, 81 FR 42209, June 28, 2016, as amended by Docket FAA-2018-0119, Amdt. 107-2, 83 FR 9172, Mar. 5, 2018; Amdt. 107-8, 86 FR 4382, Jan. 15, 2021]] **§ 107.64 Temporary certificate.** (a) A temporary remote pilot certificate with a small UAS rating is issued for up to 120 calendar days, at which time a permanent certificate will be issued to a person whom the Administrator finds qualified under this part. (b) A temporary remote pilot certificate with a small UAS rating expires: (1) On the expiration date shown on the certificate; (2) Upon receipt of the permanent certificate; or (3) Upon receipt of a notice that the certificate sought is denied or revoked.

Appendix J: Examples of Certificates/Licenses

Remote Pilot Certificate Sample

Law enforcement and public safety officials may ask pilots operating under Part 107 (typically aircraft weighing under 55 lbs) for their FAA Remote Pilot Certificate.

The Recreational UAS Safety Test (TRUST) Completion Certificate Sample

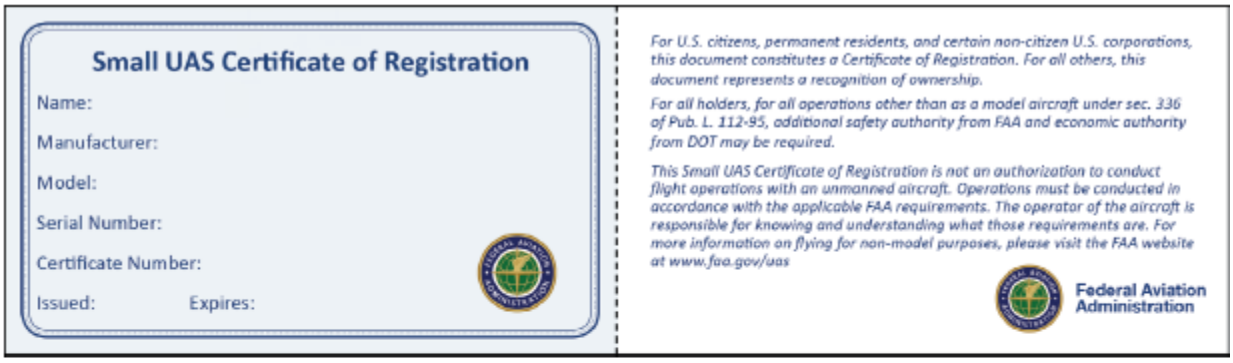
Law enforcement and public safety officials may ask pilots operating under the recreational exception in 49 U.S.C. 44809 for a copy of their TRUST completion certificate.

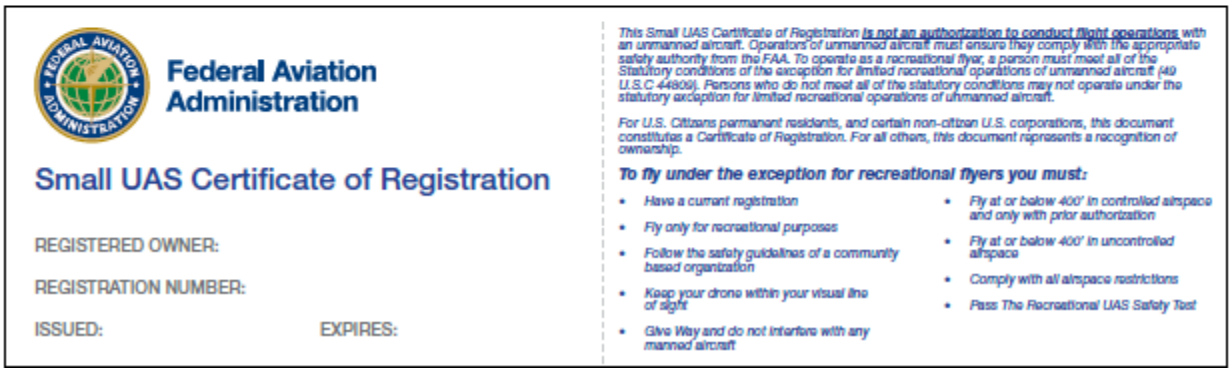
Registration Samples

Law enforcement officials may ask drone operators for the drone's registration documentation. Failure to provide the document for inspection is unlawful. Generally, FAA registration numbers

Appendix J: Examples of Certificates/Licenses Cont.

for drones start with “FA” and have eight additional numbers such as FA12345678. An aircraft over 55 lbs may have a number that starts with the letter “N.”



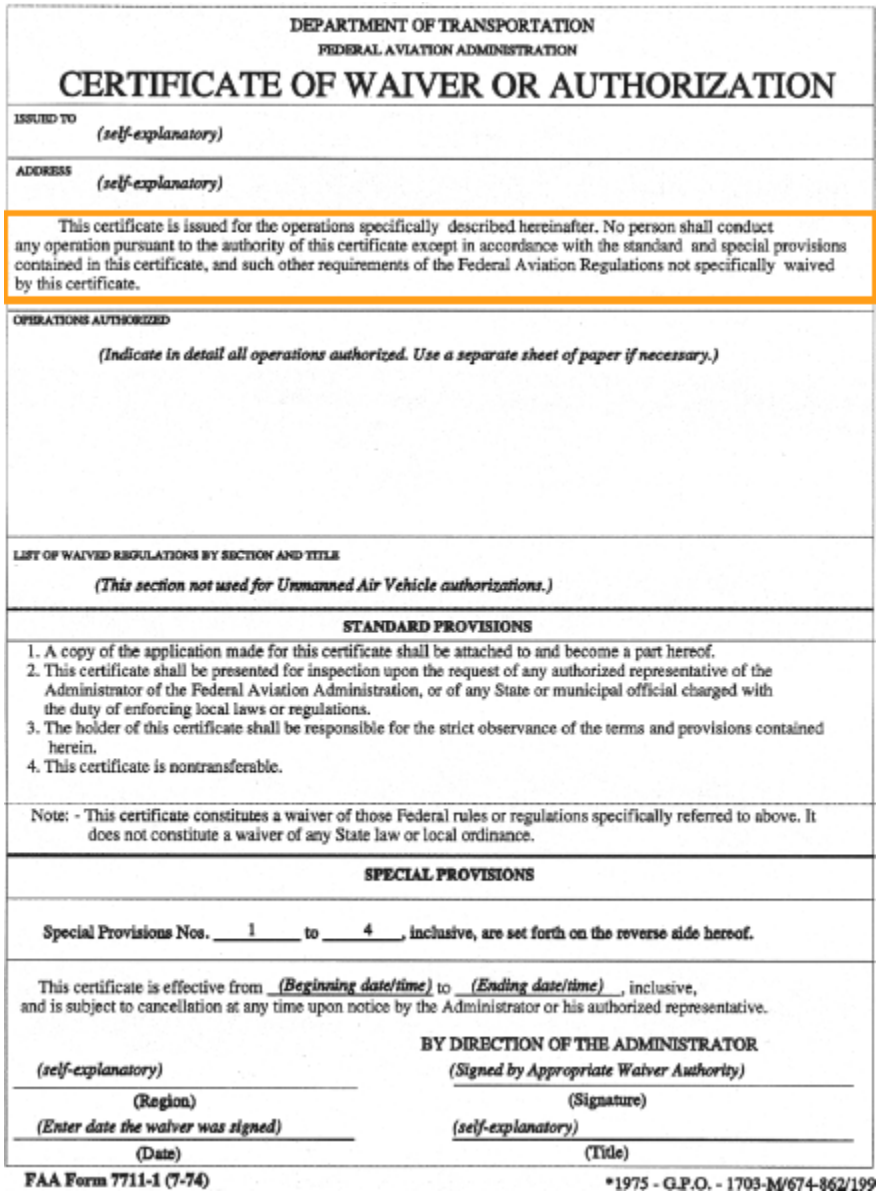


Certification of Waiver/Authorization (COA)

An authorization issued by the Air Traffic Organization to a public operator for a specific activity and specific date ranges. Upon submission, the FAA conducts a comprehensive operational and technical review. If necessary, provisions or limitations may be imposed as part of the approval to ensure the UAS can operate safely with other airspace.

Law enforcement may ask to see a UAS operator’s FAA approved Certificate of Waiver or Authorization (COA).

Appendix J: Examples of Certificates/Licenses Cont.



DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION

CERTIFICATE OF WAIVER OR AUTHORIZATION

ISSUED TO *(self-explanatory)*

ADDRESS *(self-explanatory)*

This certificate is issued for the operations specifically described hereinafter. No person shall conduct any operation pursuant to the authority of this certificate except in accordance with the standard and special provisions contained in this certificate, and such other requirements of the Federal Aviation Regulations not specifically waived by this certificate.

OPERATIONS AUTHORIZED

(Indicate in detail all operations authorized. Use a separate sheet of paper if necessary.)

LIST OF WAIVED REGULATIONS BY SECTION AND TITLE

(This section not used for Unmanned Air Vehicle authorizations.)

STANDARD PROVISIONS

1. A copy of the application made for this certificate shall be attached to and become a part hereof.
2. This certificate shall be presented for inspection upon the request of any authorized representative of the Administrator of the Federal Aviation Administration, or of any State or municipal official charged with the duty of enforcing local laws or regulations.
3. The holder of this certificate shall be responsible for the strict observance of the terms and provisions contained herein.
4. This certificate is nontransferable.

Note: - This certificate constitutes a waiver of those Federal rules or regulations specifically referred to above. It does not constitute a waiver of any State law or local ordinance.

SPECIAL PROVISIONS

Special Provisions Nos. 1 to 4, inclusive, are set forth on the reverse side hereof.

This certificate is effective from *(Beginning date/time)* to *(Ending date/time)*, inclusive, and is subject to cancellation at any time upon notice by the Administrator or his authorized representative.

BY DIRECTION OF THE ADMINISTRATOR

(self-explanatory)	*(Signed by Appropriate Waiver Authority)*
(Region)	(Signature)
(Enter date the waiver was signed)	*(self-explanatory)*
(Date)	(Title)

FAA Form 7711-1 (7-74) *1975 - G.P.O. - 1703-M/674-862/199

LAANC Authorization

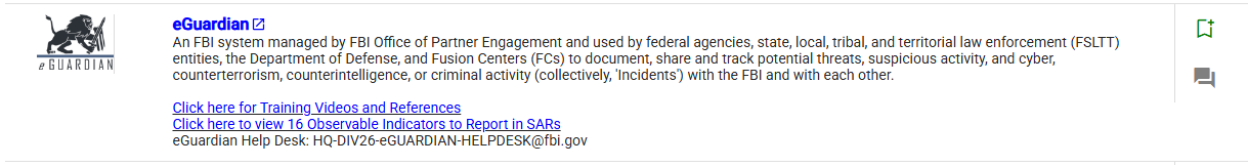
Law enforcement may ask to see a UAS operator's FAA approved authorization through the Low Altitude Authorization and Notification Capability (LAANC).

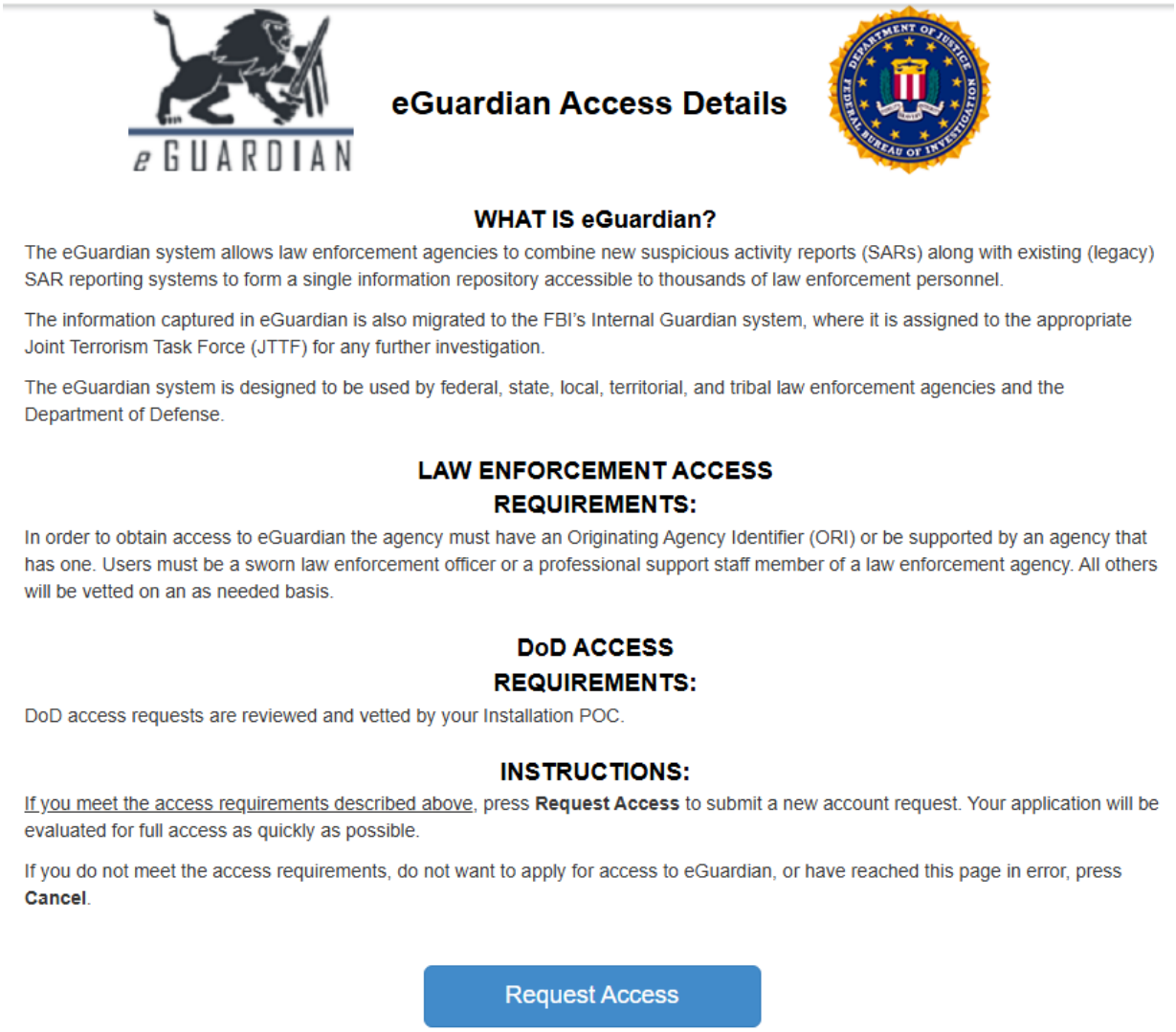
Appendix J: Examples of Certificates/Licenses Cont.

LAANC Authorization Details

APYMOKZ6RCJ0 / SFO, 5/7/2024 7:00 am PDT - 5//7/2024 8:00 PDT, Max Alt 150 ft: In accordance with Title 14 CFR Part 107.41, your operation is authorized within the designated airspace and time frame constraints. Altitude limits are absolute values above ground level which shall not be added to the height of any structures. This Authorization is subject to cancellation at any time upon notice by the FAA Administrator of his/her authorized representative. This Authorization does not constitute a waiver of any State law or local ordinance. _____ is the person designated as responsible for the overall safety of UAS operations under this Authorization. During UAS operations for on-site communication/recall, _____ shall be continuously available for direct contact at **802-123-4567** by Air Traffic. Remote pilots are responsible to check the airspace they are operating in and comply with all restrictions that may be present in accordance with 14 CFR 107.45 and 107.49 (a)(2), such as restricted and Prohibited Airspace, Temporary Flight Restrictions, etc. Remote pilots are also responsible for complying with the operating requirements in 14 CFR 107.29(a) when operating at night. Operations are not authorized in Class E airspace when there is a weather ceiling less than 1,000 feet AGL. If the UAS loses communications or loses its GPS signal, it must return to a predetermined location within the operating area and land. The remote pilot in command must abort the flight in the event of unpredicted obstacles or emergencies. This certificate shall be presented for inspection upon the request of any authorized representative of the Federal Aviation Administration, or of any State or municipal official charged with the duty of enforcing local laws or regulations.

Appendix K: eGuardian





eGuardian

An FBI system managed by FBI Office of Partner Engagement and used by FSLTT law enforcement entities, the DoD, and Fusion Centers (FCs) to document, share and track potential

Appendix K: eGuardian Cont.

threats, suspicious activity, and cyber, counterterrorism, counterintelligence, or criminal activity (collectively, 'Incidents') with the FBI and with each other.

Click here for Training Videos and References
Click here to view 16 Observable Indicators to Report in SARs
eGuardian Help Desk: HQ-DIV26-eGUARDIAN-HELPDESK@fbi.gov

Appendix L: Reporting Alternatives

Contact Us

- Report threats, incidents, or suspicious activity at the Submit a Tip webpage.
- Private Sector Businesses can direct any requests and questions to the private sector coordinator at your local field office.

Field Office Connectivity

The relationships between the FBI field offices and the DSAC member companies are at the core of the DSAC program. Each DSAC member representative is connected with the local FBI office through the FBI's Private Sector Coordinator (PSC) who directly supports the field office leadership.

The PSC focuses on partnering with private industry to understand their risks and needs relative to the FBI's emerging mission priorities. The PSC coordinates meetings between DSAC members and local FBI entities, shares tailored threat-related products and information, and facilitates information exchanges among government and DSAC member companies. The PSC may also facilitate meetings and conferences for local DSAC members and arrange for their attendance at events hosted by FBI Headquarters.

The FBI field offices and PSCs work closely with the Office of Private Sector and DSAC Program Office to identify strategic engagement opportunities for DSAC members, keeping them informed of emerging threats, best practices, and other matters of interest. The PSC serves as a "one-stop shop" for companies. In today's threat environment, a company may be targeted by any number of different types of threats carried out by a variety of threat actors. Whether a company is the victim of a fraud scheme, a computer intrusion, an insider threat, or any other

Appendix L: Reporting Alternatives Cont.

type of malicious activity, a company can contact the PSC who will connect them with the substantive FBI squad responsible for investigating that activity.

Connect with a local field office

DSAC is a strategic partnership that enhances timely communication and effective exchange of security and intelligence information between the federal government and the private sector. DSAC currently includes over 600 member companies, representing almost every critical sector. **DSAC Website** | **Fact Sheet**

InfraGard

InfraGard is a partnership between the FBI and members of the private sector. The InfraGard program provides a vehicle for seamless public-private collaboration with government that expedites the timely exchange of information and promotes mutual learning opportunities relevant to the protection of critical infrastructure. InfraGard has 77 chapters with tens of thousands of members, each dedicated to contributing industry-specific insight and advancing national security. **InfraGard Website** | **Fact Sheet** | **Brochure** | **Video**

Glossary

Glossary: Terms and Acronyms

ALV	Autonomous Land Vehicle
AR	Augmented Reality
BLOS	Beyond Line of Sight
C2	Command and Control
CBRNE	Chemical Biological Radiological Nuclear Explosives
CCD	Camouflage Concealment Deception
CIRG	Critical Incident Response Group
COTS	Commercial Off-the-Shelf
C-UAV (C-UAS)	Counter Unmanned Aircraft Vehicle (System)
FLIR	Forward Looking Infrared Radar
GPS	Global Positioning System
HME	Homemade Explosives
HMI	Human Machine Interface
LiDAR	Light Detection and Ranging
NCITF	National Counterintelligence Task Force
NJTTF	National Joint Terrorism Task Force
RADAR	Radio Detection and Ranging
RPF	Remotely Piloted Vehicle
sUAS	Small Unmanned Aircraft System
UAS	Unmanned Aircraft System(s)
UGS	Unmanned Ground System(s)
UGV	Unmanned Ground Vehicle
UMS	Unmanned Maritime System(s)
USV	Unmanned Surface Vehicle/Vessel
UUV	Unmanned Underwater Vehicle/Vessel
UxS	Unmanned System(s)
VLOS	Visual Line of Sight
VR	Virtual Reality
WMD	Weapons of Mass Destruction
UAV	Unmanned Aerial Vehicle
UAM	Urban Air Mobility
AI	Artificial Intelligence
ML	Machine Learning
sUUV	Small Unmanned Underwater Vehicle/Vessel
NOTAM	Notice to Airmen
SSI	Special Security Instruction
SGI	Special Governmental Interest