American Fuel & Petrochemical Manufacturers
afpm.org

White Paper
2023

AFPM

2023 Uncrewed Aircraft Systems (UAS) Tool Kit

Prepared by
Hogan Lovells US LLP

Table of Contents

I. Introduction

Uncrewed Aircraft Systems (UAS), or so-called "drones," have gained popularity across industries for their efficiency and safety benefits in performing tasks ranging from infrastructure inspection and precision agriculture to real estate marketing and filmmaking. The benefits of UAS operations for refineries, petrochemical manufacturers, and their customers are great. Among other activities, UAS can be used to inspect and monitor equipment and facilities, or to access and evaluate emergency situations from different perspectives. By utilizing UAS, the need for human personnel to directly undertake such potentially hazardous activities is greatly reduced, if not eliminated. While the industry has much to gain from using UAS, there is also reason for concern. The use of UAS by unauthorized operators or for unauthorized operations presents critical safety, privacy, and security risks for the refinery and petchem communities.

This 2023 edition of the AFPM UAS Tool Kit is designed to provide refiners and petrochemical manufacturers an updated understanding of the existing UAS legal framework, including the Federal Aviation Administration's (FAA) Part 107 Small UAS Rule and the waiver process for authorizing more advanced operations than broadly permitted under the rule, as well as the framework for operating larger drones weighing 55 pounds or more. It also outlines the risks to the industry as a result of the increasingly prevalent use of this technology, particularly by rogue operators, and describes what protections are available (or may soon be available) including FAA enforcement, common law torts, and certain UAS-specific state laws. As part of this 2023 AFPM UAS Tool Kit, we have included hyperlinks to current FAA guidance material (as of January 2023).[1]

This 2023 AFPM UAS Tool Kit provides a general overview of a complex and evolving topic. For legal advice on particular issues, the authors of this report are available to answer any questions that individual companies may have.

Lisa Ellman
Partner, Washington, D.C.
T +1.202.637.6934
lisa.ellman@hoganlovells.com

Patrick Rizzi
Counsel, Washington, D.C
T +1.202.637.5659
patrick.rizzi@hoganlovells.com

Matt Clark
Senior Associate, Washington, D.C.
T +1.202.637.5430
matt.clark@hoganlovells.com

[1] For a library of guidance documents, see https://www.faa.gov/uas/resources/policy_library.

II. UAS Legal Framework

The use of UAS for hobbyist or recreational purposes has been part of American tradition, and broadly authorized in the United States, for decades. Over the last several years, as UAS and information technology have improved at a rapid pace, UAS have become cheaper, smaller, more mobile, and increasingly able to capture data from the air safely and efficiently. With these technological advances, the commercial marketplace, including the oil and gas industry, has embraced the use of this technology.

However, UAS technology has moved much more quickly than U.S. policymaking. This Section of the AFPM UAS Tool Kit provides an overview of the current UAS legal framework for hobbyist, public, and commercial use of drones in the United States in order to guide industry activity and provide a roadmap for the future. This Section also provides a brief overview of the airworthiness process and the differing regulatory requirements applicable to the operation of larger uncrewed aircraft (UA) weighing 55 pounds or more.

A. Hobbyist Use

The operation of small UAS (sUAS) weighing less than 55 pounds for purely recreational or hobbyist use may be exempt from the regulatory requirements applicable to commercial (civil) sUAS operations if the operation complies with certain statutory requirements.[2]

For the refinery and petchem industries, it is important to recognize that a flight only qualifies as an authorized hobbyist flight if it is flown *strictly for hobby or recreational use*. This means that an employee hobbyist may not fly a model aircraft to benefit the company (even if he or she also flies for fun) and still fall under the hobbyist umbrella. A hobbyist who flies a UAS for the benefit of the company, even if the individual is not paid to do so, is engaging in commercial activity, which is regulated by the FAA, as is flying for both recreational and commercial purposes in one single flight. Doing so without complying with the applicable regulations and authorizations raises legal and regulatory liability issues for both the individual employee and the company for which he/she is flying.

B. Public Use

Public use of UAS is relevant to AFPM members for at least two reasons. First, private companies often seek to collaborate with public entities, such as public universities, in order to fly in partnership under a public Certificate of Waiver or Authorization (COA). By way of background, federal, state, and local agencies may operate UAS under a more flexible regulatory framework if the operation qualifies as a public aircraft operation. A public operation involves a "public aircraft" UAS (meaning that it is publicly owned or operated on behalf of a public agency or government), carrying out a "governmental

[2] Under 49 U.S. Code § 44809 (*Exception for limited recreational operations of unmanned aircraft*), the following requirements apply to the operation: (1) the flight must be for strictly recreational purposes, (2) the sUAS must be operated in accordance with or within the programming of a community-based organization's set of safety guidelines that are developed in coordination with the FAA; (3) the sUA must be flown within visual line of sight of pilot or co-located visual observer; (4) the sUA must not interfere with, and must give way to, crewed aircraft; (5) the operator must obtain FAA authorization to fly in controlled airspace; (6) the sUA must fly below 400 feet AGL in uncontrolled Class G airspace; (7) the pilot must have passed an FAA aeronautical knowledge and safety test; and (8) the sUAS must be registered with the FAA.

function”[3] under the authority of a public COA issued to the government entity. FAA oversight of public aircraft operations is more limited and public aircraft do not need to comply with the same regulatory requirements applicable to commercial UAS operations.

In recent years, the FAA has taken a more conservative view on the ability of private companies to partner with public entities to operate UAS as public aircraft. For example, the FAA has limited the ability of industry to partner with UAS Test Sites and public universities to do flight testing and other R&D operations as public aircraft operations. This change in the FAA’s view may impact the ability of AFPM members to collaborate with public entities or other governmental partners. Notably, the FAA is expected to issue waiver approvals to test sites under a different framework (Section 44803 of the FAA Reauthorization Act of 2018) that may enable collaboration between test sites and industry outside of the PAO context.

Second, refineries and petrochemical manufacturers should be aware that local, state, and federal agencies, including those related to environmental and regulatory enforcement, may themselves be operating UAS as public aircraft. Companies may therefore be on the receiving end of UAS surveillance from the government.

C. Commercial / Civil Use

Any UAS operations that do not meet the requirements for hobbyist or public use are treated as civil or commercial UAS operations. As discussed in Section III below, the FAA imposes additional certification and operating restrictions on commercial UAS operations, as compared to hobbyist and public use operations.

III. FAA Small UAS Rule (Part 107) Overview

Since 2016 commercial sUAS operations must comply with the FAA’s Small UAS Rule, which is codified in various parts of the Federal Aviation Regulations (FARs) but referred to collectively as “Part 107.”

Part 107 contains several key operating restrictions, some of which are quite strict. Below we provide a summary of the key Part 107 requirements that refineries and petrochemical manufacturers should be aware of.

A. UAS Registration and Remote Identification

All sUAS operated commercially that weigh more than 250 grams must be registered with the FAA. Soon, beginning September 16, 2023, UAS operators will

[3] The term “governmental function” means an activity undertaken by a government, such as national defense, intelligence missions, firefighting, search and rescue, law enforcement (including transport of prisoners, detainees, and illegal aliens), aeronautical research, or biological or geological resource management. 49 U.S.C. § 40125(a)(2).

also need to comply with the FAA's new Remote Identification (Remote ID) Rule.[4] UAS will be required to broadcast certain identification information regarding the UA, its location and the location of the operator.

1. UAS Registration

Below is a summary of the key registration requirements for commercial UAS operators.

- UAS can be registered electronically using the FAA DroneZone Portal.
- Commercial operators are required to register each individual UAS and pay a $5 registration fee for each application. Registration lasts 3 years, and there is a $5 renewal fee for each renewal. These fees are the same as those currently required under the paper-based registration system.

- Commercial operators are required to provide UAS-specific information in addition to basic contact information. The owner will receive a Certificate of Aircraft Registration with a registration number for each individual UAS registered. As part of the Remote ID Rule finalized in early 2021, the FAA added a requirement for a serial number as part of the registration process.
- Prior to operation, UA must be marked on its exterior with its registration number.
- While there is a U.S. citizenship requirement for registration, as is the case for crewed aircraft, UAS owned by non-U.S. citizen corporations qualify for registration so long as the corporation is organized and doing business under the laws of the U.S. or a U.S. State, and the UAS is "based and primarily used in" the U.S. The FAA has strict guidelines for meeting the "based and primarily used in" test.
- If the UAS is destroyed, sold, lost, or transferred, the UAS registration should be cancelled using the FAA's DroneZone portal.

2. UAS Remote Identification

Certain aspects of the FAA's UAS Remote Identification Rule (14 CFR Part 89) recently went into effect. Once fully implemented, the Rule will require most UA operating in U.S. airspace to broadcast remote ID. Remote ID will provide information about UA in flight, such as the identity, location, and altitude of the UA and its control station or take-off location. Authorized individuals from public safety organizations may request the identity of the UA's owner from the FAA.

The Remote ID Rule imposes separate requirements on UAS operators and UAS manufacturers. The requirements applicable to UAS manufacturers went into effect on September 16, 2022. Unless an exception applies, all new UAS designed and produced for operation in the U.S. must be equipped with remote ID equipment. There are additional requirements associated with remote ID modules that allow previously manufactured UA to be retrofitted to broadcast remote ID information.

[4] Remote ID requirements are set forth in Part 89 of the FARs. Under the RID Rule, nearly all UAS manufactured for operation in the U.S. must be equipped with remote ID technology capable of broadcasting certain UAS identify information. The Remote ID regulatory requirements applicable to operators go into effect on September 16, 2023.

Operator requirements under the Remote ID Rule go into effect on September 16, 2023. Once the operator requirements go into effect, nearly all UA operated in the U.S. will be required to broadcast UA remote ID information.

AFPM members procuring new UAS should ensure that the UAS is equipped with required remote ID broadcast equipment.

B. Remote Pilot Certification Requirements

Part 107 contemplates three potential types of personnel, or flight crewmembers, involved in UAS operations: a remote pilot-in-command (remote PIC), a person manipulating the flight controls (if different than the PIC), and a visual observer (VO). All UAS flights must have a designated remote PIC. The remote PIC is responsible for a number of aspects of the UAS flight and operation. VOs and the person manipulating the controls of the UAS (if not the remote PIC), are not required to possess a pilot certificate of any kind.

In order to be eligible for a Remote Pilot Certificate, applicants must be at least 16 years old, be able to read, speak, write, and understand the English language, and be in a physical and mental condition that would not interfere with the safe operation of a UAS. Applicants with no prior crewed aircraft pilot's certificate must take an initial aeronautical knowledge exam (multiple-choice questions) designed for UAS operations. This test must be taken at one of the more than 800 FAA-approved testing centers, and the applicant's identity will be verified at that time. Upon receiving a passing score, the applicant will apply for the certificate online using the FAA's electronic FAA Integrated Airmen Certificate and/or Rating Application (IACRA) system.[5] After the application is submitted, the Transportation Security Administration (TSA) conducts a background security screening on the applicant. The FAA anticipates that the TSA vetting will be completed within 10 days, although there could be delays depending on the number of applicants at the time the pilot-applicant's application is made. Once TSA approval has been received, the FAA will issue a temporary Remote Pilot Certificate that is valid for 120 days. This will allow sufficient time for processing the official certificate. The certificate does not expire; however, the certificate holder must pass a recurrent aeronautical knowledge test every 24 months to remain active.

Licensed crewed aircraft pilots (other than student pilots) who are current with respect to their flight review requirements have the option of either taking the initial knowledge test or taking an online training program. If taking the knowledge test, the pilot follows the same steps as outlined above, but

[5] Additional details on the application process are available at: https://www.faa.gov/uas/commercial_operators/become_a_drone_pilot.

the 10-day TSA waiting period will not apply since the individual has already been vetted by TSA. If choosing to take only the training, the pilot must submit the application for a Remote Pilot Certificate to one of several individuals authorized by the FAA. The point of this requirement is to confirm the individual's identity and to verify that the applicant meets the relevant flight review requirements. As is the case with individuals with no previous crewed aircraft pilot's license, there is a recurrent training requirement every 24 months for the Remote Pilot Certificate to remain valid for these manned aircraft pilots.

C. General Operating Requirements Under Part 107

While Part 107 broadly authorizes low-risk commercial sUAS operations in the United States, the rule contains several key operating restrictions to maintain the safety of the NAS. Key operational restrictions in Part 107 include the following:

- UA must weigh less than 55 lbs. (25 kg) including payload.
- Visual line of sight (sometimes abbreviated "VLOS") operations only. The UA must remain within VLOS of the remote PIC and visual observer (if one is used) (VO). At all times, the UA must remain close enough to the remote PIC for the remote PIC to be capable of seeing the UA with vision unaided by any device other than corrective lenses.
- VOs may be used, but they are not required. The remote PIC may choose to use a VO to supplement situational awareness and VLOS. Although the remote PIC and person manipulating the controls (if different from the remote PIC) must maintain the capability to see the UA , using one or more VOs allows the remote PIC and person manipulating the controls to conduct other mission-critical duties (such as checking display monitors) while still ensuring situational awareness of the UA.
- No person may act as the remote PIC, a person manipulating the controls, or a VO for more than one UA operation at one time.
- UA may operate at night when the UA is equipped with lighted anti-collision lighting visible for at least 3 statute miles.
- Must yield right-of-way to other aircraft, crewed or uncrewed.
- First-person view (FPV) camera cannot satisfy "see-and-avoid" requirement but can be used as long as requirement is satisfied in other ways.
- Small UA may not operate over any persons not directly involved in the operation (i.e., other than the UAS flight crew and direct participants, described below).
- No operations from a moving aircraft.
- No operations from a moving land or water-borne vehicle, except when flown over a sparsely populated area and not carrying another person's property for compensation or hire.
- Maximum airspeed of 100 mph (87 knots).
- Maximum altitude of 400 feet above ground level unless flown within a 400-foot radius of a structure and no higher than 400 feet above the structure's immediate uppermost limit.
- Minimum weather visibility of 3 statute miles from control station.

- No operations are allowed in Class A (18,000 feet and above) airspace.
- Operations in Class B, C, D, and E airspaces are allowed with the required Air Traffic Control (ATC) permission. ATC permission comes in the form of an airspace authorization. Requests for airspace authorizations can be submitted using the Low Altitude Authorization and Notification Capability (LAANC) system.
- Operations in Class G airspace are allowed without ATC permission.
- No careless or reckless operations.

IV. Part 107 Waivers

To provide flexibility and help accommodate new and innovative UAS technology, Part 107 contains a waiver process for authorizing expanded operations beyond the scope of what is currently permitted under the rule. Below we provide a summary of the waiver process and identify specific waivers that AFPM members may want to apply for.

Waivable sections of Part 107 include:

- Operation from a moving vehicle or aircraft (§ 107.25)
- Anti-collision lighting requirement for operation at night (§ 107.29)
- Visual line of sight aircraft operation (§ 107.31)
- Visual observer (§ 107.33)
- Operation of multiple sUAS (§ 107.35)
- Yielding the right of way (§ 107.37(a))
- Operation over people (§ 107.39)
- Operation in certain airspace (§ 107.41)
- Operating limitations for sUA (§ 107.51)
- Operations over moving vehicles (§ 107.145)

To be eligible for a waiver, applicants must be able to demonstrate to the FAA that the proposed operation can be conducted safely (§ 107.200). The FAA evaluates waiver applications on a case-by-case basis. Factors considered by the FAA include the nature of the proposed operation, the unique environment in which the operation will take place, and proposed safety mitigations. Each waiver contains conditions and limitations that need to be complied with (referred to as “common”, “special”, “technical” and “environmental” conditions).

Waiver applications can be submitted electronically using the FAA DroneZone portal. The FAA’s instructions for filing a waiver application are available here. The waiver application form itself only requires applicants to submit basic information about the proposed operations (type of waiver requested, applicant contact information, etc.). After completing the waiver form, applicants have the option of attaching PDF files to the waiver application. If the PDF files are too large or numerous to attach to the waiver application filing in DroneZone, additional supporting documentation can be

emailed to the FAA at the following address: 9-afs-800-part107Waivers@faa.gov. When emailing the FAA, be sure to reference the application reference number assigned to the filing on DroneZone.

The FAA's Waiver Safety Guideline Questions (WSEG Questions) describe information needed to make a successful safety case for granting a waiver. There are certain general questions that apply universally to all waiver types, including basic operational details, UAS details, and pilot/personnel details. The general WSEG Questions are available here. There are also more specific WSEG Questions that vary based on the type of waiver being requested which are available here. The level of detail and the additional supporting documents that will be necessary for adequately responding to the FAA's WSEG Questions will vary depending on the complexity of the proposed operation. In other words, the riskier or more complex the proposed operation, the more substantial your responses and safety case will need to be in order for the FAA to grant the waiver.

After submitting the waiver application, additional documents and information supporting the safety case for granting a waiver can be submitted to the FAA via email at: 9-afs-800-part107Waivers@faa.gov. On all documents submitted to the FAA as part of your waiver application (whether as a PDF attachment to the form, or in a subsequent email to FAA), it is important to always include "Proprietary and Confidential" markings (or something similar) on every page of a document that you consider to be proprietary or otherwise commercially sensitive in nature. This will help protect the documents from being made public in response to a Freedom of Information Act (FOIA) request filed with the FAA.

Depending on individual facility needs and characteristics, AFPM members may want to consider applying for waivers from the following provisions of Part 107.

A. Operation Over People and Moving Vehicles (§§ 107.39 and 107.145)

The original Part 107 Rule prohibited sUA flights over unsheltered individuals and moving ground vehicles not directly participating in a UAS operation unless a waiver from the FAA was received by the operator. Direct participants in the operation include the pilot, visual observer and any other individuals necessary for the safety of the UAS operation. In December 2020, the FAA issued a Final Rule on "Operations of Small Unmanned Aircraft Systems Over People" (OOP Rule), which allows sUA to operate over people without the need to obtain a waiver from the FAA under certain conditions.

Notwithstanding the new OOP Rule, operators still have the option of seeking a waiver from § 107.39 if they are unable to comply with the OOP Rule. The most likely reason for why compliance with the OOP Rule would not be feasible is that the sUA is simply too heavy to comply with the Rule's conservative impact energy thresholds.

While there is still the option to apply for a § 107.39 waiver, as of January 2023, the FAA has only issued sixteen (16) such waivers since issuance of the OOP Rule in December 2020. The FAA has a clear preference that operators utilize the new OOP Rule rather than pursue a waiver from the prohibition on flights over people.

The recent § 107.39 waivers that have been issued generally fall into one of two categories: (1) operations involving sUAS that are currently going through the FAA type certification process; and (2) operations in a controlled-access environment where nonparticipating individuals have been have undergone a safety briefing related to the UAS operations. This second category may be relevant to AFPM members seeking to conduct sUAS operations over a controlled-access industrial site where it may be necessary for a sUA to briefly transient over employees that are not directly participating in the UAS operation, but whom have undergone a safety briefing. These waivers typically require the UA to be equipped with a parachute system that has been tested to an ASTM standard. For example, the FAA has approved § 107.39 waivers involving various UAS when equipped with ASTM F3322-18 compliant parachute systems.

The safety case to substantiate a § 107.145 waiver for operations over moving vehicles is largely identical to that of an operations over people waiver. Additional guidance from the FAA for pursuing a §§ 107.39 and/or 107.145 waiver is available here. To the extent you have an existing safety management system (SMS) for site operations, consider whether there are opportunities to incorporate UAS operations into your existing SMS procedures. While UAS operators are not required to have an SMS, the FAA strongly supports the adoption of voluntary SMS programs. Incorporating your UAS operations into an existing company SMS program may help support a safety case for issuance of various Part 107 waivers, including waivers to operate over people and moving vehicles.

B. Visual Line of Sight Aircraft Operation (§ 107.31)

As previously noted, Part 107 requires the remote PIC and the person manipulating the controls of the UAS (if different from the remote PIC) to be able to see the UA at all times during the flight with unaided vision (except glasses or contact lenses).[6] While companies may voluntarily choose to use a VO to assist the remote PIC in maintaining situational awareness, it is important to note that Part 107 still requires that the remote PIC and the person manipulating the controls always be capable of exercising visual line of sight (VLOS) with the sUA.

The benefit to using a VO is that it relieves the remote PIC from the obligation of always exercising VLOS, freeing-up the remote PIC to conduct other mission-critical duties (such as checking displays). It does not, however, relieve the remote PIC from the requirement that he/she always be located in a position that would permit him/her to see the sUA. In practice, depending on the size of the sUA and other conditions affecting visibility, the VLOS requirement effectively limits the area of sUAS operation to within a mile or so of the remote PIC. This limitation on the geographic scope of operation can make it difficult or impractical to conduct a variety of sUAS operations, including, for example, aerial inspections of large facilities or other linear assets like pipelines where the sUA would typically need to operate at greater distances from the remote PIC. In these scenarios, a waiver permitting sUAS operations beyond VLOS (sometimes abbreviated “BVLOS”) would make these activities much easier by expanding the

[6] Vision aids, such as binoculars, may be used only momentarily to enhance situational awareness.

geographic scope of sUAS operations. A key issue in all BVLOS waiver applications will be demonstrating to the FAA how the remote PIC will see and avoid / detect and avoid all other aircraft and ground-based obstacles, as well as avoid flying over people when the sUA is operated BVLOS of the remote PIC.

To date, the majority of BVLOS waivers issued by the FAA have generally fallen into one of two categories: (1) those requiring the use of one or more VOs to monitor the airspace around the sUA for other aircraft[7]; and (2) "true" BVLOS waivers that rely upon detect and avoid (DAA) technologies capable of detecting non-cooperative aircraft[8], such as ground-based radar, cameras or acoustic sensors. A hot topic of discussion within the FAA as of January 2023 relates to the issue of infrastructure masking (sometimes referred to as shielding) as a mitigation to support BVLOS operations. Infrastructure masking essentially refers to a UA operating in close proximity to infrastructure (likely 50 feet, although it could vary in different scenarios) in airspace where it would not be possible for a crewed aircraft to operate. In January 2023, the FAA issued a handful of BVLOS waivers that rely upon infrastructure masking as a DAA mitigation. The specific details vary, but the masking BVLOS waivers typically impose a maximum operating altitude of 50 feet AGL **or** a maximum altitude of an object or obstacle when the sUA is operated within a 200 foot radius of the object or obstacle **and** below 400 feet AGL. Some of the waivers have also imposed a requirement that the sUA cannot exceed a distance of 1,000 feet horizontally from the remote PIC and that the remote PIC be located onsite at the sUA launch and recovery area.[9]

The FAA's recent approval of BVLOS waivers that rely upon infrastructure masking as a DAA mitigation (e.g., no VOs or DAA technology) may provide an excellent opportunity for AFPM members to pursue waivers for conducting low-altitude BVLOS sUAS infrastructure inspections that rely on infrastructure masking as a DAA mitigation.

C. Operating Limitations for Small Unmanned Aircraft (§ 107.51)

Under Part 107, the operating limitations for sUAS include limitations on speed, altitude, flight visibility, and cloud clearance. For refiners and petrochemical manufacturers operating sUAS, the operating limitations relating to flight visibility and cloud clearance minimums are more relevant than the speed and altitude limitations. The minimum flight visibility under Part 107 is 3 statute miles from the location of the sUAS ground control station, and the minimum distance of the sUA from the clouds must be no less than 500 feet vertically and 2,000 feet horizontally. In order to receive a waiver from these operating limitations, an applicant needs to provide a method by which: (1) the VLOS requirement in § 107.31 will be satisfied; (2) the sUA will avoid non-participating aircraft; and (3) the conspicuity of the sUA can be increased to allow it to be seen at a distance of at least 3 statute miles.

[7] Sometimes referred to as "extended visual line of sight operations" or EVLOS.

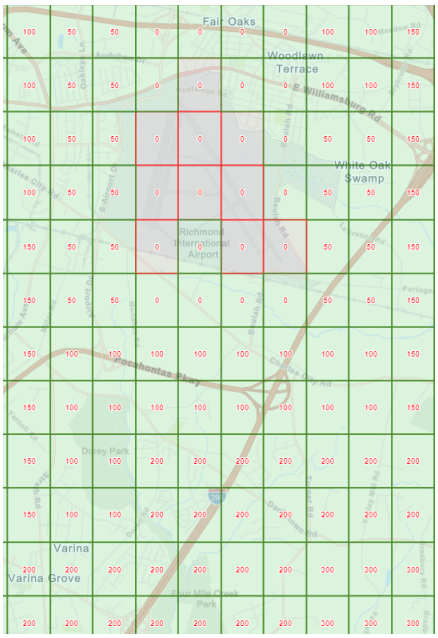
[8] Non-cooperative aircraft means aircraft *not* equipped with ADS-B out that is used to broadcast the location of the aircraft.

[9] *See e.g.*, Waiver No. 107W-2022-01836.

V. Airspace Access

Part 107 authorizes sUAS to be operated in Class G airspace without prior approval from ATC. Small UAS may be operated in Class B, C, D airspace or within the lateral boundaries of the surface area of Class E airspace designated for an airport with prior approval from ATC. ATC approval can be obtained by submitting an application through either the Low Altitude Authorization or Notification Capability a/k/a "LAANC", or if needed, through the FAA's DroneZone Portal.

A. LAANC Airspace Authorization



LAANC is not available everywhere, but in the locations where it is available, using LAANC will be the fastest way to obtain an airspace authorization needed to fly in controlled airspace.

LAANC is a collaboration between the FAA and private industry partners to automate the application and approval process for airspace authorizations. Prior to LAANC, UAS operators needing airspace authorizations would need to submit a request via the FAA DroneZone, which could take weeks or months to process. LAANC automates the airspace authorization process and allows operators to obtain near real-time approvals for certain operations occurring in controlled airspace. As of January 2023, a list of FAA-approved LAANC UAS Service Suppliers is available here: Airbus, Airspacelink, Aloft, AutoPylot, Avision, eTT Aviation, UASidekick, and Wing.

The FAA publishes UAS Facility Maps that depict maximum altitudes using a grid format around airports where airspace authorizations may be issued without any additional safety analysis. Altitudes range from 0-400 feet above ground level (AGL). If an operator seeks authority to fly below a designated grid altitude on the UAS Facility Maps, an airspace authorization may be issued in near real-time. If an operator seeks to fly higher than the altitudes designated on the UAS Facility Maps, the FAA may need to coordinate with the local air traffic control (ATC) facility prior to issuance of an airspace authorization, a process which can take several days.

B. Expedited Approvals for Emergency UAS Operations

In some cases, public (governmental) and civil (commercial) UAS operators who need to fly emergency response missions, which provide crucial benefits to the public good and address exigent circumstances, may be able to use the FAA's Special Governmental Interest (SGI) process (formerly called "Emergency COAs") to obtain Part 107 waivers and authorizations on an expedited basis. There are likely many scenarios where refineries and petrochemical manufacturers could qualify for expedited approvals through the SGI process. Response missions that may qualify for expedited approvals through the FAA's SGI process include, among other things, activities relating to utility and other critical infrastructure restoration, and incident awareness and analysis. For example, a refinery or petrochemical manufacturer may be able to qualify for expedited approvals through the SGI process to use UAS for

infrastructure inspection and damage assessment following a natural disaster event, or to conduct accident incident response flights.

To submit a request through the FAA's SGI process, this Emergency Operation Request Form should be filled out and emailed to the FAA's System Operations Support Center (SOSC) at 9-ator-hq-sosc@faa.gov. For assistance in this process, the FAA's SOSC can be contacted at (202) 267-8276. Additional guidance regarding the SGI application process is available in FAA Order JO 7200.23C, *Processing of Unmanned Aircraft System Requests*.

VI. Recent Rule Changes

A. UAS Remote Identification

As discussed above, certain aspects of the FAA's UAS Remote Identification Rule recently went into effect. Once fully implemented (in fall 2023), the Rule will require most UA operating in U.S. airspace to broadcast remote ID.

B. Operations of Small Unmanned Aircraft Systems Over People

The original Part 107 Rule prohibited sUA flights over unsheltered individuals and moving ground vehicles not directly particpating in UAS operation unless a waiver from the FAA was received by the operator. In December 2020, the FAA issued a Final Rule on "Operations of Small Unmanned Aircraft Systems Over People" (OOP Rule)[10], which allows sUA to operate over people without the need to obtain a waiver from the FAA under certain conditions.

To date, the OOP Rule has failed in its goal of establishing a process for enabling more routine operations over people. As on January 2023, only a single sUA model has been approved for operations over people under the OOP Rule – the AgEagle (senseFly) eBee X series.

Under FAR § 107.39, a small UA cannot operate over a human being unless:

i. That human being is directly participating in the operation of the small UA;

ii. (b) That human being is located under a covered structure or inside a stationary vehicle that can provide reasonable protection from a falling small UA; or

iii. (c) The operation meets the requirements of at least one of the four operational categories specified in subpart D of Part 107 (described below).

The four operational categories for operations over people have different requirements based on risk levels.[11] Category 2 and Category 3 sUA must meet certain injury severity limits. The method that an applicant uses to show its sUA meets the applicable requirements is referred to as a means of compliance (MOC), which must be accepted by the FAA. After an applicant determines that its sUA

[10] 86 Fed. Reg. 4314 (Jan. 15, 2021) (effective April 21, 2021).

[11] For purposes of this section, the terms "person" or "people" refers to unsheltered individuals who are not directly participating in the UAS operation.

meets an FAA-accepted MOC, the applicant makes a filing with the FAA declaring that the sUA complies with the FAA-accepted MOC (referred to as a Declaration of Compliance or DOC).[12] Below are the general requirements for each sUA Category. For AFPM members, Category 3 will likely be the most relevant given its focus on enabling operations over people located restricted-access sites, such as employees on a gated facility.

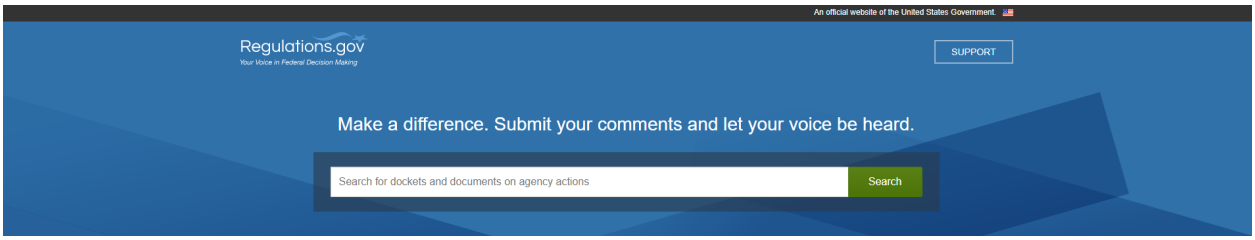
- Category 1: sUA weighing 0.55 pounds or less (including all attachments) which have no exposed rotating parts that would lacerate human skin on impact with a human being. Category 1 sUA may be operated in sustained flight over open-air assemblies (i.e., hovering over a crowd of people). No MOC or DOC is required.

- Category 2: sUA must: (1) not cause injury to a person "equivalent or greater than the severity of injury caused by a transfer of 11 foot-pounds of kinetic energy upon impact from a rigid object"; (2) not contain exposed rotating parts that could lacerate human skin upon impact; and (3) be free from safety defects. The sUA must be tested to an FAA-accepted MOC and a DOC must be filed with the FAA. Category 2 sUA may operate in sustained flight over people (i.e., hover), as well as operate over open air assemblies of people (i.e., crowds of people).

- Category 3: The design requirements are the same as Category 2 sUA except that the severity of injury threshold is 25 foot-pounds of kinetic energy transfer. The sUA must be tested using an FAA-accepted MOC, and a DOC must be filed with FAA. Category 3 sUA may not operate over crowds of people. For operations occurring on a restricted-access site, sustained flight over people is authorized. For operations occurring outside of a restricted-access site environment, sUA flights over people must be transient only (i.e., no sustained flight).

- Category 4: Applies to sUA that have been issued an airworthiness certificate by the FAA. The sUA must be operated in accordance with its FAA-approved Flight Manual. Additional maintenance and inspection requirements apply. No MOC or DOC is required. As of January 2023, no sUA have been approved for Category 4 operations over people.

VII. Operating Large UAS: The 44807 Exemption Process



The Part 107 regulatory framework does not apply to the operation of UA weighing 55 pounds or more. To the extent that AFPM members seek to operate larger UAS, the general operating rules in Part 91 of the FARs will likely apply. Part 91 applies to all civil aircraft operated in the U.S. and the rules were originally drafted with crewed aircraft in mind. For this reason, there are several regulatory requirements in Part 91 that UAS, due to their design and manner in which they are operated, are unable to comply with the regulatory requirements. The most common example is relief from the

[12] Declarations of Compliance are filed electronically with the FAA here.

requirement in Part 91 that all aircraft have an airworthiness certificate. As of January 2023, the only UAS that has been type certified by the FAA and eligible for an airworthiness certificate is Matternet's M2 UAS.

Under 49 U.S.C. § 44807 and its existing rulemaking authority, the FAA has the ability to issue UAS operators exemptions from various sections of the FARs that they are unable to comply with or in situations where compliance would be impractical and overly burdensome. This is essentially the regulatory framework used to enable commercial UAS operations before Part 107 was issued. Prior to Part 107, operators needed to obtain relief from various FARs using the "Section 333" exemption process. After Part 107 was issued, Section 333 exemptions were no longer needed to operate small UAS, however, for the most part, exemptions are still necessary to operate larger UA weighing 55 pounds or more.

Section 333 was subsequently replaced by 49 U.S.C. § 44807, but the overall process essentially remains the same. A company seeking to operate a large UAS must file a petition for exemption with the FAA that: (1) identifies the specific FARs it needs an exemption from; (2) explains how the operator will ensure an equivalent level of safety if the exemption is granted; and (3) an explanation of why granting the exemption would be in the public interest.

The procedural requirements for filing a petition for exemption with the FAA are located in Part 11 of the FARs. The timeframe for issuance of a § 44807 exemption may vary from a few months to a year or more depending on how novel the relief sought is and whether there is past precedent for the relief sought (i.e., has the FAA previously issued an exemption to another entity to operate the same UAS for a similar purpose).

VIII. UAS Type Certification

Type certification involves extensive testing and review of an aircraft's design. Over the past several years, a handful of UAS manufacturers have worked closely with the FAA in an effort to type certify their UA with the FAA. Type certification of UA has proved challenging for industry and FAA alike given the lack of defined standards for certifying unique and novel design features of UAS compared to traditional crewed aircraft.

As noted above, as of January 2023, the only UAS that has been type certified by the FAA and eligible for an airworthiness certificate is Matternet's M2 UAS. We hope to see more UA type certificates issued in 2023, including for UA intended to operate in critical infrastructure environments. If and when ongoing efforts to type certify additional UA are successful, market availability of type certified UA may pave the way for broader and more scalable UAS operations and could potentially eliminate the need for operators to obtain § 44807 exemptions in some scenarios depending on the planned operations and UA equipage.

IX. FAA UAS BEYOND Program (previously the Integration Pilot Program)

In 2017, the White House announced the "Unmanned Aircraft Systems Integration Pilot Program" (IPP), which directed the DOT Secretary to launch an initiative to safely test and validate expanded UAS operations, such as flights at night, over people and BVLOS of the pilot in partnership with state and local governments in select jurisdictions. The IPP concluded on October 25, 2020, as mandated by statute.

The IPP was superseded by the FAA BEYOND Program, which began in October 2020 immediately following the conclusion of the IPP. BEYOND continued partnerships with eight of the original IPP participants.

UAS BEYOND provides an opportunity for state, local, and tribal governments to partner with private sector entities, such as UAS operators or manufacturers, to accelerate safe UAS integration. The FAA is tackling challenges still facing UAS integration including:

i. BVLOS operations that are repeatable, scalable, and economically viable with specific emphasis on infrastructure inspection, public operations, and small package delivery;

ii. Leveraging industry operations to better analyze and quantify the societal and economic benefits of UAS; and

iii. Focusing on community engagement efforts to collect, analyze, and address community concerns.

The list of BEYOND Lead participants include the Choctaw Nation of Oklahoma; Virginia Tech Center for Innovative Technology; Kansas Transportation Department; Memphis-Shelby County Airport Authority of Tennessee; North Carolina Transportation Department; North Dakota Transportation Department; the City of Reno, Nevada; and the University of Alaska-Fairbanks.

X. Restricted Flight Areas

The FARs generally do not require UAS operators to obtain consent before flying over private property, and there are no explicit protections for property owners against UAS overflight. Thus, while the benefits of UAS use to AFPM members are great, there is also the concern that unlicensed individuals will fly UAS over their facilities without permission and/or in violation of federal, state, or local laws (so-called "rogue" UAS or drones). For example, UAS could be used for surveillance or photography of facilities, personnel, or sensitive areas within facilities, which have been identified as critical

infrastructure by the U.S. government. Environmental groups could use drones to support citizen suits, or rely on the same information captured by a hobbyist's drone. A UAS could be armed with explosives and flown into a refinery. Less threatening but nevertheless very concerning, a hobbyist could accidentally crash his or her UAS into a refinery or petchem facility.

A. FAA Flight Restrictions

In the example of a UAS being used for environmental surveillance, the relevant threshold question from an FAA enforcement perspective would be whether the environmental group is categorized as a hobbyist or non-hobbyist operator. An environmental group operating its drone to further a lawsuit would likely be considered a non-recreational flight under the FAA's current understanding, as the flight is not solely for "hobby or recreational purposes." Assuming it is a small UAS, the flight would need to comply with Part 107, and the individual operating the sUAS on behalf of the environmental group would be required to have a Remote Pilot Certificate with a small UAS rating issued by the FAA.

However, legal questions remain as to whether that same environmental group could use a hobbyist drone operator's video images against a refinery in court. In the news media context, the FAA has indicated that it may be acceptable for newsgatherers to use hobbyist-captured drone images for commercial purposes, so long as the model aircraft operator's original intention in flying the aircraft was actually recreational.[13] As one could imagine, the difficulty with this standard is that it may be difficult to prove what the operator's initial intent was for conducting the flight. Under an FAA policy addressing aviation-related videos or other electronic media on the internet, the FAA noted: (1) FAA inspectors "have no authority to direct or suggest that electronic media posted on the Internet must be removed"; and (2) "electronic media posted on a video Web site does not automatically constitute a commercial operation or commercial purpose, or other non-hobby or non-recreational use."[14]

The FAA maintains a variety of security-driven airspace restrictions around the country to help protect sensitive locations, events, and activities through Temporary Flight Restrictions (TFRs), prohibited areas, and other mechanisms such as the Washington, DC, Flight Restricted Zone (DC FRZ). UAS operations, including hobbyist flights, are generally prohibited within these defined volumes of airspace. Under FAA rules, refineries along with a number of other sensitive facilities are covered by Notice to Air Missions Advisory 4/0811 (NOTAM 4/0811). NOTAM 4/0811 does not prohibit flight over the sensitive facility, but prohibits "loitering" over sensitive facilities:

[14] FAA Notice N 8900.292 (effective April 8, 2015).

FDC 4/0811 SPECIAL NOTICE

THIS IS A RESTATEMENT OF A PREVIOUSLY ISSUED ADVISORY NOTICE.

IN THE INTEREST OF NATIONAL SECURITY AND TO THE EXTENT PRACTICABLE, PILOTS ARE STRONGLY ADVISED TO AVOID THE AIRSPACE ABOVE, OR IN PROXIMITY TO SUCH SITES AS POWER PLANTS (NUCLEAR, HYDRO-ELECTRIC, OR COAL), DAMS, REFINERIES, INDUSTRIAL COMPLEXES, MILITARY FACILITIES AND OTHER SIMILAR FACILITIES. PILOTS SHOULD NOT CIRCLE AS TO LOITER IN THE VICINITY OVER THESE TYPES OF FACILITIES.

WIE UNTIL UFN

This NOTAM applies to all aircraft and pilots, including UAS; however, it is only advisory in nature and not mandatory. Part 107 prohibits a small UAS from "operating in prohibited or restricted areas unless that person has permission from the using or controlling agency, as appropriate." It is important to note that prohibited or restricted areas are designated by the FAA under 14 CFR Part 73. In other words, it does not encompass areas deemed restricted or prohibited by private entities, unless that area is also designated as such by the FAA under Part 73.

B. Private Entity Restrictions on UAS and Other Protections

In addition to governmental restrictions, some private entities have worked with the FAA to establish flight restrictions over certain lands, usually based on security concerns. Airspace over Disney theme parks, for example, is restricted from the surface to 3,000 feet.[15] This restriction applies to UAS as well as to manned aircraft. More recently, private entities, like ski resorts, have enacted policies restricting UAS without involving the FAA. However, such policies, particularly as they pertain to UAS launched or operated from outside resort boundaries, raise unresolved legal issues over whether a private entity has any right or authority to limit the use of low-altitude airspace over its land, or whether such actions are strictly under the purview of FAA. Some companies advertise they provide the ability for companies to detect, track, and identify low-altitude, small UAS. However, as discussed below, there may be legal questions around the use of drone security technology, particularly with regard to mitigation techniques.

XI. Enforcement Against Rogue Drones

The FAA has several civil enforcement tools to assert its authority over "rogue drones" flown by commercial and hobbyist operators alike. The FAA may elect to take no action, pursue an administrative action, or pursue a legal enforcement action. Administrative action may take the form of a warning notice or letter of correction. A warning notice is similar to a traffic warning in that the FAA retains a record of the event, but declines to pursue further punitive action. A letter of correction outlines required action for the recipient, which if complied with,

[15] FAA, NOTAM FDC 4/3634, Temporary Flight Restrictions for Special Security Reasons: Disney World Theme Park, Orlando, Florida; Federal Aviation Administration, NOTAM FDC 4/2625, Temporary Flight Restrictions for Special Security Reasons: Disneyland Theme Park, Anaheim, California Near Seal Beach VORTAC (SLI).

results in no further action by the FAA. Failure to comply with a letter of correction would elevate the incident to a legal enforcement action. Legal enforcement actions can include either certificate action or civil penalties. In the case of certificated pilots, the FAA may take action against that airmen's certificate, including suspension or revocation. If a company holds additional FAA authorizations in the form of a Part 107 Waiver or Section 44807 Exemption, the FAA could revoke those authorizations. Alternatively, the FAA may elect to pursue legal enforcement action by levying a civil penalty or fine.

The FAA is authorized to issue civil penalties for certain violations of the FARs pursuant to 49 U.S.C. § 46301. Civil penalties issued against commercial and hobbyist UAS operators vary widely and have ranged from $400 to $200,000. The FAA determines the amount of the civil penalty using, in significant part, a Sanction Guidance Table, which provides ranges for civil penalties based upon the type and size of the business, the type and severity of alleged violation, and the number of alleged violations. For most UAS violations, the per-violation penalty ranges are outlined in FAA Order 2150.3C and summarized in the table below. There are additional sanction ranges not listed below for small business violations under § 46301(a)(1), but not § 46301(a)(5)(A), for UAS interfering with wildfire suppression, emergency response or law enforcement under 49 U.S.C. § 46320, and for operation of a UAS equipped with a dangerous weapon. In the absence of aggravating or mitigating circumstances, the FAA typically recommends a sanction at the middle of the sanction range.

	Large Business Concern	Small Business Concern[16]
Maximum	$28,500-$37,377	$8,000-$14,950
High	$20,500-$28,500	$5,500-$10,000
Moderate	$9,500-$20,500	$2,500-$7,500
Minimum	$3,000-$9,500	$1,000-$4,500

It is important to note that sanctions are applied to each individual violation, and a separate violation occurs for each day the violation continues. In addition, the FAA recently issued its 2023 civil penalty adjustments, whereby the new maximum for large business concerns has increased from $37,377 to $40,272 and the maximum small business concern penalty above has increased from $14,950 to $16,108.[17] As illustrated by the FAA's record setting proposed civil penalty of $1.9 million dollars against Chicago-based UAS operator SkyPan International, a single activity could violate more than one regulation, and if the action is continuous and ongoing, each action is a new violation that will continue to compound the civil penalty amount. In October 2015, the FAA alleged that SkyPan International conducted 65 unauthorized flights in controlled airspace over Chicago and New York City. As a small business concern, the maximum amount for any individual infraction would be $11,000. However, since each of the 65 unauthorized flights violated more than one regulation (operating in a reckless manner,

[16] Section 503 of Vision 100 — Century of Aviation Reauthorization Act sets different limits on the civil penalties the FAA may seek for violations by small business concerns, as opposed to violations by other entities. Vision 100 CARA gives the term "small business concern" the same meaning as in the Small Business Act (15 U.S.C. § 632). Section 632 defines small business concern as an enterprise "which is independently owned and operated and which is not dominant in its field of operation."

[17] *See,* Revisions to Civil Penalty Amounts, 88 Fed. Reg. 1114, 1115 (January 6, 2023).

failure to display an airworthiness certificate/registration, failing to have proper equipment/clearance for Class B airspace), the FAA alleged 389 individual violations. In January 2017, SkyPan reached a settlement agreement with FAA, agreeing to pay a $200,000 civil penalty. The company also agreed to pay an additional $150,000 if it violates Federal Aviation Regulations in the next year, and $150,000 more if it fails to comply with the terms of the settlement agreement.

Beyond imposing civil penalties, the FAA has indicated that some federal criminal statutes may be implicated by some UAS operations, but most violations of the FAA's regulations would be dealt with by administrative enforcement actions.

Despite its authority to act against unauthorized and unsafe UAS operations, carrying out enforcement actions has proved challenging for the FAA. This may be partly due to difficulty in identifying possible violators. Moreover, with the competing demands on the FAA's limited resources, the FAA is not able to monitor every UAS operation, particularly unauthorized ones, by itself.

As discussed above, to help combat threats posed by rogue drones, in January 2021 the FAA finalized a remote identification rule that requires nearly all drones to broadcast a publicly viewable "digital license plate" that includes identifying information about the drone, its location, and the location of the operator. This rule goes into effect for operators in September 2023 and will assist in identifying rogue drones and their operators. To fill the enforcement gap, the FAA has stated it considers state and local law enforcement agencies best positioned to detect and immediately investigate rogue UAS or UAS operations. To that end, the FAA has issued a guidance document, "Law Enforcement Guidance for Suspected Unauthorized UAS Operations" ("LEA Guidance"), so that state and local officials are educated about what to do in case of a rogue (or allegedly rogue) UAS flight.

Congress has also taken notice of the threats posed by rogue drones. The FAA Reauthorization Act of 2018 created new enforcement tools to bring criminal penalties against rogue UAS operators. Section 381 of the 2018 Act makes it a criminal offense under Title 18 of the U.S. Code to knowingly and intentionally direct or otherwise cause such UAS to enter or operate within or above a restricted building or grounds. Section 382 and 384 of the 2018 Act also make it a criminal offense to interfere with wildfire suppression efforts and to knowingly interfere with certain aircraft operations or to operate in a runway exclusion zone at an airport.

A. Defending Against Rogue Drones: Countermeasures

So what should a company do if there is evidence that an unauthorized UA has, is, or will be flying over facility property? As a threshold matter, and despite what many may have heard or read about the so-called Kentucky "Drone Slayer," it is never appropriate to try and shoot down or capture a rogue UA, even if it is operating over one's facility/property without permission. Since both commercial and hobbyist UAS are considered aircraft, it would technically be a felony act to try and destroy or capture a UA in flight.[18]

In recent years, growing security and privacy concerns over rogue drones have prompted the development of a variety of counter-UAS systems designed to detect, identify, and track rogue drones. Many of these systems also provide the ability to mitigate the threat, by interfering with, hacking, capturing, or destroying rogue drones. Before deploying UAS countermeasures, it is important for facility owners and operators to understand the legal and regulatory risks around their use. Depending on the type of counter-UAS technology deployed, different federal, state, and local laws may apply.

In August 2020, the FAA, Department of Justice (DOJ), Federal Communications Commission (FCC), and Department of Homeland Security (DHS) issued a joint "Advisory on the Application of Federal Laws to the Acquisition and Use of Technology to Detect and Mitigate UAS", which provides an overview of the statutory and regulatory requirements applicable to the use of various types of UAS detection and mitigation technologies.

As a general rule, companies may typically detect, identify, and track rogue drones under the law. For example, one may legally use specialized radar and video technology to identify UA that may be invisible to traditional radar, including small plastic drones. The technology deployed in this scenario is passive in nature and does not actually interfere with the UA or its wireless communication links. Thus, unlike counter-UAS measures that involve destroying or disrupting a UA's control links or navigation technology, there are few, if any, restrictions on the use of technology used to identify and track rogue drones. Mitigation methods may run afoul of the law, however. Broadly speaking, counter-UAS mitigation methods generally fall into one of three categories:

[18] *See, e.g.*, 18 U.S.C. § 32 - Destruction of aircraft or aircraft facilities.

1. Targeting the operator and neutralizing the operator's ability to operate the drone;
2. Targeting the drone and destroying it; or
3. Targeting the drone's command and control links or its navigation technology and flying it away, or otherwise preventing it from operating in particular areas.

In the first scenario, a combination of visual spotting and electronic listening devices can be used to locate the operator, who can then be approached and compelled to land the UA. The FAA and Department of Homeland Security are experimenting with this technology, which tries to monitor UAS radio signal activity around sensitive areas and pinpoints an operator's likely location. In most scenarios, this technology is legal to deploy because it is generally passive in nature and does not physically interfere with the flight of the rogue drone or violate Federal Communication Commission (FCC) regulations against jamming or interfering with wireless communications.

In the second scenario, the rogue drone itself is targeted. The most common example of this is use of a projectile, such as a firearm, beanbag gun, or water cannon, to knock the rogue drone out of the sky. In almost all instances, these forms of counter-UAS measures will run afoul of federal laws. For purposes of federal law, UAS are considered "aircraft." Under 18 U.S.C § 32 – Destruction of aircraft or aircraft facilities – destroying or disabling an aircraft is a federal crime punishable by up to a 20-year prison sentence. Shooting down a rogue drone may also give rise to criminal liability under state laws. Most states have laws that criminalize the intentional destruction of property. For example, in Virginia, intentionally damaging property is a Class 1 misdemeanor or a Class 6 felony depending on the value of the property.[19] There could also be criminal liability under local ordinances criminalizing vandalism, destruction of property, reckless endangerment, or, depending on the location, discharging of a firearm. Moreover, in some states, the owner of a damaged or destroyed UA could potentially have a cause of action for personal property damage. There is also the risk of potential civil liability for personal injury or property damage in the event that someone is injured or property is damaged on account of the counter-UAS activity.

Rather than using methods that physically interfere with the rogue drone, some companies are marketing counter-UAS services or equipment that are designed to target the wireless control links or navigation technology of a UA. This technology generally works by either: (1) creating a virtual "geo-fence" that prevents the UA from flying into certain airspace; or (2) providing a means for a third party to take over control of the UA and fly it to a specific location. The main obstacle to deploying this technology is that federal law makes it illegal to interfere with wireless communications. Most counter-UAS technology that involves the use of a radio transmitting device to interfere with the UAS's wireless communications (otherwise known as "jamming") would be illegal under federal law, and could give rise to civil and criminal liability. For example, using a device to interfere with a UAS's radio communications,

[19] VA. Code Annot. Sec. 18.2-137(A); 18.2-1347(B).

GPS link, Wi-Fi, or Bluetooth connection would be illegal.[20] The FCC defines a "jammer" as a radio frequency transmitter that is "designed to block, jam, or otherwise interfere with authorized radio communications," by "emitting radio frequency waves that prevent the targeted device from establishing or maintaining a connection." The FCC considers any effort to market, sell, or use a transmitter designed to block, jam, or interfere with any wireless communications, including the unlicensed Wi-Fi frequency bands, to be a violation of the Communications Act of 1934.[21] To the extent a person interdicts and or "takes over" a rogue drone on its property, it may also constitute a violation of the Federal Wiretap Act, which generally prohibits "intentionally intercept[ing], endeavor[ing] to intercept, or procur[ing] any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication."[22]

Due to potential national security concerns posed by rogue drones, Congress authorized the Department of Defense (DoD) and the Department of Energy (DOE) to use counter-UAS equipment to protect certain facilities and assets in the United States in the National Defense Authorization Act for Fiscal Year 2017 (P.L. 114-328). DoD's authority was further clarified in the National Defense Authorization Act for Fiscal Year 2018 (P.L. 115-91). In the FAA Reauthorization Act of 2018, Congress approved similar authorities for the Department of Homeland Security (DHS) and Department of Justice (DOJ). Section 1602 of the 2018 Act authorizes DOJ and DHS to mitigate (i.e., take down) UAS that pose a "credible threat" to a "covered facility or asset." Covered facilities and assets include certain federal facilities, mass gatherings, and other assets typically protected by various national security agencies. The authority granted in Section 1602 of the 2018 Act does not extend to state and local law enforcement or private entities.

With the growth in the drone market, federal policymakers recognize there is a need to further develop counter-UAS technology policy and law, and they are working to do so now. For example, the 2018 Act directs the FAA to charter an Aviation Rulemaking Committee (ARC) around counter-drone technology. We expect FAA to launch this ARC in 2023. It will be important for the AFPM community to be engaged in the policymaking around these issues.

In the meantime, for now, rather than deploying counter-UAS measures that interfere with or target the rogue drone or its communication/navigation system, facility management should instead legally gather as much data and information as possible that would facilitate a law enforcement or FAA investigation. Arguably, someone flying directly over people and/or sensitive facilities such as an oil refinery without the owner's/operator's knowledge or consent may be operating in a hazardous or reckless fashion, which is illegal regardless of whether the UAS operator is a commercial operator or hobbyist. Additionally, as discussed in Section XII below, several states have passed legislation that make it a criminal offense to operate UAS over certain critical infrastructure facilities. Accordingly, if there is

[20] 47 C.F.R. § 2.803 (2008).

[21] 47 U.S.C. §§ 301, 302a (b), 333.

[22] 18 U.S.C. § 2511(1)(a).

evidence that a rogue drone will fly over your property, or is currently flying there, the first step should be to contact local law enforcement and advise them of the rogue drone.

B. Building a Case Against a Rogue UAS Operator

While federal, state, and local governments have clear authority to enforce the law against rogue UAS operators that fly recklessly or in violation of state law property or privacy rights, in practice regulators and law enforcement agencies have difficulty identifying possible violators. Most of the time, an operator flying illegally will not reveal himself or herself. It is therefore very important to be thorough in gathering evidence in order to build a case against a rogue UAS operator.

While the LEA Guidance referenced above is principally aimed at law enforcement officials investigating suspected illegal UAS flights, the guidance also provides helpful tips for facility owners/operators about how to document suspected rogue UAS flight activity during and after the flight occurrence. Immediately upon noticing a suspected rogue UAS flight, facility owners/operators should legally gather as much data and information as possible that would facilitate a law enforcement investigation, FAA investigation, or potential civil action against the operator. For example, helpful information for enforcement purposes would include:

- Descriptive information about the UA, including whether it is a rotorcraft or fixed wing;
- Registration number or markings (if any);
- Time/date of the flight;
- Duration of flight over facility or property;
- Approximate altitude; and
- Any visible payload.

The next step is to gather as much information as possible relating to each of these points, and to work with local law enforcement to report the issue to the FAA. In particular, the following steps should be taken:

1. **Witness Identification and Interviews**. Identify potential witnesses and conduct initial interviews, documenting what each witness observed while the event is still fresh in their minds. Depending on the circumstances, it may also be a good idea to ask witnesses to provide written statements documenting their observations.
2. **Identification of Operators and the UAS**. As noted above, it is often difficult to identify the UAS operator. In a future civil action against a rogue operator, facility owners/operators will bear the burden of proof for showing who was actually operating the UAS. Similarly, in any legal enforcement action against the rogue operator, the burden will be on the FAA. If possible, you should try to photograph or videotape the operator, the UA itself, and any observable registration and/or serial numbers on the UA. You should try to record the license plate number of associated motor vehicles if any are spotted.

3. **Viewing and Recording the Location of the Event**. Pictures taken in close proximity to the event are often helpful in describing light and weather conditions, any damage or injuries, and the number and density of people on the surface, particularly in populated areas. During any witness interviews, use of fixed landmarks that may be depicted on maps, diagrams, or photographs help immeasurably in fixing the position of the aircraft. Such landmarks also should be used to describe lateral distances and altitude above the ground, structures, or people (e.g., below the third floor of Building X).
4. **Identifying Sensitive Locations, Events, or Activities**. The FAA maintains a variety of security-driven airspace restrictions around the country to help protect sensitive locations, events, and activities through Temporary Flight Restrictions (TFRs), Prohibited Areas, and other mechanisms. UAS operations, including model aircraft hobbyist flights, are generally prohibited within these defined areas of airspace. Commercial UAS operations are prohibited in controlled airspace (anything other than Class G) without air traffic control ("ATC") airspace authorization. Hobbyist flights are generally prohibited within 5 miles of an airport/ heliport absent airport/ATC notification. You should become familiar with airspace restrictions over and around the location of your facility.
5. **FAA Notification**. Immediately report suspected rogue UAS flights to one of the FAA Regional Operation Centers (ROC) located around the country. This will allow the FAA to initiate an investigation into the flight activity. FAA ROC contact information is below:

FAA Regional Operations Centers

Location Where Accident Occurred:	**Telephone**
DC, DE, MD, NJ, NY, PA, WV, and VA	404.305.5150
AL, CT, FL, GA, KY, MA, ME, MS, NC, NH, PR, RI, SC, TN, VI, and VT	404.305.5156
AK, AS, AZ, CA, CO, GU, HI, ID MP, MT, NV, OR, UT, WA, and WY	425.227.1999
AR, IA, IL, IN, KS, LA, MI, MN, MO, ND, NE, NM, OH, OK, SD, TX, and WI	817.222.5006

C. Potential Legal Actions at the Federal Level

Depending on how a UAS is being operated, UAS flying over critical infrastructure facilities, such as refineries and petrochemical sites, may be violating a number of Federal or state laws. It will be important for owners/operators of critical infrastructure facilities to understand these laws so that you know when it is appropriate to initiate contact with local law enforcement and how to best advise them once on the scene.

For purposes of federal law, UAS are considered "aircraft" and are regulated as such. The FARs are located in Title 14 of the Code of Federal Regulations (14 CFR). FAR § 91.13 prohibits careless or reckless aircraft operations and is one the most commonly cited regulations in FAA enforcement actions. It states, in part:

§ 91.13 Careless or reckless operation.

i. Aircraft operations for the purpose of air navigation. No person may operate an aircraft in a careless or reckless manner so as to endanger the life or property of another.

Section 91.13 is a catch-all regulation that commonly serves as the basis for FAA enforcement actions brought against careless or reckless UAS or crewed aircraft operators. Arguably, someone flying directly over or close to company employees, vehicles, facilities, and/or structures, without the company's knowledge or consent, may be operating in a hazardous or reckless fashion, which is illegal regardless of whether the UAS is being operated for commercial or hobbyist/recreational purposes. The same thing could be true for UAS that are operated near or over sensitive facilities and infrastructure. If company personnel observe a UAS flying near or over company property in a manner that could potentially be hazardous to its employees or any company facility, building or infrastructure (whether because of proximity or some other reason), local law enforcement and the applicable FAA Regional Operations Center (see chart above) should be contacted immediately and advised of the unsafe flight operation.

In addition, company personnel interacting with local law enforcement should familiarize themselves with any airspace restrictions surrounding their facilities that would make a UAS flight illegal. These restrictions could provide a basis for law enforcement or FAA enforcement action against the operator of the UAS.

D. Potential Legal Actions at the State and Local Level

In addition to FAA enforcement against unauthorized UAS operations, individual states offer varying levels of protection against misuse of UAS in the form of UAS-specific privacy laws, platform-neutral laws, and common law tort. As a general matter, the FAA's safety authority preempts any state or local government regulation of aircraft operations.[23] However, state and local governments do retain certain authority to limit the aeronautical activities of their own departments and institutions.[24] Over the past few years, state and local governments have enacted UAS rules that test the boundaries of this authority.[25]

There are several potential state law causes of action against an individual or entity operating UAS over or near critical infrastructure facilities without permission from the facility owner/operator. Over the past few years, many states, including Arkansas, Florida, Idaho, Indiana, Louisiana, North Carolina, Oregon, Tennessee, Texas, and Wisconsin, have enacted privacy laws that impact commercial and private use of UAS. Several cities and towns have done the same, and most states and cities are considering legislation or ordinances that would restrict UAS flights. State and local UAS-related laws are

[23] Federal Aviation Administration, Fact Sheet – State and Local Regulation of UAS (December 17, 2015) *available at*: https://www.dot.nv.gov/Home/ShowDocument?id=6834.

[24] *Id.*

[25] For instance, the City of Newton, Massachusetts passed an ordinance that banned UA flights below 400 feet and over private and public property without the landowner's permission, and also required local registration of drones. Newton resident and drone enthusiast Michael Singer sued, arguing that the federal government has exclusive jurisdiction over the national airspace and, as a result, municipal attempts to regulate drones were prohibited. In *Singer v. Newton Singer v. Newton, D. Mass., No. CV 17-10071-WGY (Sept. 21, 2017),* the U.S. District Court agreed with Singer, finding that Newton's ordinance "thwarts" Congress's objective to integrate drones into the national airspace, and that the ordinance was therefore preempted by federal legislation directing the FAA to incorporate drones into the national airspace.

continuously changing, and some laws restricting UAS use have been struck down in State and Federal courts on federal preemption and First Amendment constitutional grounds.

The laws that have been passed take many different forms. For example, Idaho's law specifically prohibits UAS from photographing or recording an individual for purposes of publicly disseminating the information without the individual's written consent. Other laws prohibit the use of UAS to record or survey private property. Louisiana's UAS law, for instance, prohibits the use of UAS to conduct surveillance of certain manufacturing facilities. Importantly, most of these state laws have an exception to the general prohibitions on image capture with a person's or property owner's consent.

Additionally, some states have privacy laws that do not explicitly mention UAS but may be broad enough to cover UAS activities. California law, for instance, prohibits the capture of images taken in an offensive manner of an individual engaging in a personal or familial activity.[26] Also, most states have general consumer protection laws that prohibit "unfair" or "deceptive" acts or practices,[27] the enforcement of which theoretically could include UAS activities that violate a person's privacy expectations. Companies also could pursue a misappropriation of trade secrets claim.

Also, as discussed above, facility owners/operators should work with law enforcement as appropriate to help prosecute rogue UAS flights over or near its properties.

XII. State Laws Protecting Critical Infrastructure Facilities

In general, state specific UAS laws are enforced by state law enforcement or regulatory agencies. AFPM members may wish to work with the state government on these matters by providing video of the flight, information about the operator (or the operator's employer), and other evidence documenting details of the flight, as previously discussed in Section XI(B).

In addition to state laws protecting against UAS misuse and privacy protections generally, some states have laws that make it a criminal offense to operate UAS over certain critical infrastructure facilities. Ten states currently have laws that specifically restrict drone access near critical infrastructure facilities. While barring UAS operation around certain facilities, these statutes often provide exemptions – usually for law enforcement agencies, owners and operators of facilities, and those with the written consent of owners and operators. In some cases, UAS are restricted from going within a certain distance of a facility's perimeter. In Tennessee, for instance, UAS are prohibited from going within 250 feet of a protected facility's external perimeter, regardless of the height. Other states – like Oklahoma and Oregon – have made it illegal to operate a UAS above critical facilities at a height of less than 400 feet above the ground. This creates a column of restricted airspace above facilities that ends 400 feet above

[26] Cal. Civ. Code § 1708.8; California Assembly Bill 2306, (2014), *available at* http://www.leginfo.ca.gov/pub/13-14/bill/asm/ab_2301-2350/ab_2306_bill_20140904_enrolled.html (A person is liable for constructive invasion of privacy when the person "attempts to capture, in a manner that is offensive to a reasonable person, any type of visual image, sound recording, or other physical impression of the plaintiff engaging in a personal or familial activity under circumstances in which the plaintiff had a reasonable expectation of privacy, through the use of any device, regardless of whether there is a physical trespass, if this image, sound recording, or other physical impression could not have been achieved without a trespass unless the device was used.").

[27] Justin J. Hakala, Follow-On State Actions Based on the FTC's Enforcement of Section 5 at 9-11 (2008), *available at* https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID1283261_code791336.pdf?abstractid=1283261&mirid=1&type=2

the ground. However, given that FAA rules generally prohibit UAS operation above 400 feet, the combination creates a de facto no-fly zone over these facilities.

The classification of critical infrastructure varies by state, but generally includes facilities such as petroleum refineries, chemical manufacturing facilities, pipelines, wastewater treatment facilities, power generating stations, electric utilities, chemical or rubber manufacturing facilities, and other similar facilities. Oklahoma and Oregon have some of the broadest – most inclusive – definitions. Their statutes outline more than a dozen types of infrastructure and facilities, including various types of refineries and power plants; certain components of electric grid; chemical manufacturing plants; many aspects of the natural gas processing and distribution system; and various components of oil and chemical pipelines. Other states have defined critical infrastructure more narrowly.

Tennessee, for instance, defines critical infrastructure as one of the following five types of facilities: electric power plants, petroleum refineries, manufacturing facilities that use combustible chemicals, facilities that manufacture chemicals or rubber, and petroleum or chemical storage facilities.

Below is a summary of various UAS-specific state laws that restrict and/or criminalize UAS misuse over critical infrastructure facilities. The statutory text of relevant state UAS laws is located in the Appendix of this Tool Kit.

> **Cautionary Note**: This list is constantly evolving and changing as states and localities consider and pass legislation. It is also important to note that state and local UAS laws are often subject to court challenges, some of which have been successful. For example, in March of 2022, several Texas state laws criminalizing unauthorized UAS flights over critical infrastructure were all struck down as unconstitutional by U.S District Court for the Western District of Texas.[28]

A. Alabama

Alabama codified a law that increases protections for critical infrastructure and enhances penalties for damaging critical infrastructure. For the purposes of this law, critical infrastructure does not explicitly mention petroleum, however, the list of facilities is not exclusive and does mention pipelines and refineries. The offense of unauthorized entry may be a Class A misdemeanor or rise to a Class C felony.

B. Arkansas

Arkansas codified the offense of "unlawful use of UAS," which is committed when anyone knowingly uses a UAS to "conduct surveillance of, gather evidence or collect information about, or photographically or electronically record critical infrastructure without the prior written consent of the owner..." For the purpose of this law, critical infrastructure includes an electrical power generation or

[28] *National Press Photographers Association, et al. v. Steven McGraw, et al.*

delivery system, a petroleum refinery, a chemical or rubber manufacturing facility, or a petroleum or chemical storage facility. The offense is a class B misdemeanor.

C. Delaware

In Delaware, there is a state that makes it a criminal offense to operate a UAS over a critical infrastructure facility without written permission from the property owner/occupier. The statute's definition of "critical infrastructure" includes petroleum refineries, petroleum storage facilities, chemical storage facilities, chemical manufacturing facilities, fuel storage facilities, electric substations, power plants, electric generation facilities, military facilities, commercial port and harbor facilities, rail yard facilities, drinking water treatment or storage facilities, correctional facilities, government buildings, and public safety buildings or facilities.

D. Florida

In June 2017, Florida passed legislation that makes it a criminal offense to operate a drone over, to come into contact with, or to otherwise interfere with or cause a disturbance at a critical infrastructure facility. The statute's definition of "critical infrastructure facility" is fairly broad and includes, among other things, electrical power generation and transmission facilities, chemical or rubber manufacturing or storage facilities, natural/ compressed gas compressor stations and storage facilities, natural/compressed gas pipelines, liquid natural gas or propane gas terminals or storage facilities with a capacity of 4,000 gallons or more, and any portion of aboveground oil or gas pipelines. The crime is punishable by imprisonment for up to 60 days for a first offense and up to 1 year for a second offense.

E. Louisiana

Louisiana has enacted criminal statutes aimed at unauthorized drone operations, including unauthorized flights occurring over critical infrastructure. Unauthorized drone flights may provide a basis for a state criminal enforcement action against the operator. Depending on the specific nature of the violation, the operator could be subject to a fine of up to $5,000 and/or up to one year in prison.

F. Nevada

Under Nevada law, anyone who operates a UAS within a horizontal distance of 500 feet or a vertical distance of 250 feet from a "critical facility" without the written consent of the owner of the critical facility is guilty of a misdemeanor. The law's definition of a "critical facility" includes petroleum refineries and petroleum or chemical production facilities, among others.

G. Oklahoma

Oklahoma recently passed a law making it a criminal offense to: (1) operate a UAS over a critical infrastructure facility at an altitude below 400 feet above ground level; (2) allow a UAS to make contact with a critical infrastructure facility, including any person or object on the premises of or within the facility; or (3) allow a UAS to come within a distance of a critical infrastructure facility that is close enough to interfere with the operations of or cause a disturbance to the facility. The Oklahoma statute's definition of a "critical infrastructure facility" includes, among others, petroleum refineries and chemical manufacturing facilities.

H. Oregon

In 2016, Oregon passed a law making it a class A violation to operate UAS over critical infrastructure. Critical infrastructure is defined to include petroleum and alumina refineries; electrical power facilities; and chemical, polymer, and rubber manufacturing facilities, among others. Oregon also has a statute providing a private cause of action by property owners against the operator of a UAS in circumstances where the property owner has previously warned the operator not to fly over the property.

I. Tennessee

In 2016, Tennessee passed a law making it a criminal offense to operate a UAS within 250 feet of a critical infrastructure facility for the purpose of conducting surveillance or gathering information about the facility without the owner or business operator's written consent:

J. Potential Legal Actions at the State and Local Level

In addition to statutory restrictions, there are common law privacy rules that may protect against certain misuse of UAS. For instance, a person is subject to liability for the tort of intrusion upon seclusion, if the person "intentionally intrudes...upon the solitude or seclusion of another or his private affairs or concerns...if the intrusion would be highly offensive to a reasonable person."[29] In the context of UAS, an individual could claim that aerial images of his or her property captured private details and intruded on his or her seclusion. However, the requirement that the intrusion be "highly offensive to a reasonable person" can be a difficult standard to meet, and courts have rejected the claim that simply looking at another's property is sufficiently invasive of privacy to meet the standard.[30]

Below is a brief summary of some of the relevant common law rules that may protect against certain misuse of UAS:

- Trespass: A number of states have enacted laws that prohibit the use of drones over private property without the consent of the owner. In some cases, the property owner may have a private cause of action to sue the UAS operator for trespass, and, in other cases, the state might prosecute the operator for use of a UAS in contravention of state law. Under the Restatement of Torts, flights constitute a trespass if (a) the aircraft enters the immediate reaches of the airspace next to the land, and (b) it interferes substantially with the other's use and enjoyment of the land.
- Nuisance: Relatedly, a property owner may be able to invoke nuisance doctrine to prohibit unwanted UAS. A nuisance is "an activity which arises from unreasonable, unwarranted or unlawful use by a person of his own property, working obstruction or injury to the right of another, or to the public, and producing such material annoyance, inconvenience and discomfort that law will presume resulting damage." Theoretically, a plaintiff could argue that the use of UAS interferes with his or her normal occupancy of the land by creating noise or flying low enough to create a safety or privacy risk. Depending upon the size of a UAS, consistent use of it over one's own property could make enough noise to disturb neighboring property owners in the quiet enjoyment of their own property, possibly resulting in a potential lawsuit for nuisance. Similarly, a powerful UAS could kick up enough

[29] RESTATEMENT (SECOND) OF TORTS § 652B.

[30] *See*, *e.g., GTE Mobilnet of S. Texas Ltd. P'ship v. Pascouet*, 61 S.W.3d 599, 618 (Tex.App. 2001) (finding that "the mere fact that maintenance workers...look[ed] over into the adjoining yard is legally insufficient evidence of highly offensive conduct.").

dust and dirt, and blow it over to a neighbor's property. If this occurs regularly, it may potentially interfere with the neighbor's use of his or her property to the point where the neighbor sues to stop the intrusion.

- Privacy: Some states have passed laws or may soon do so that prohibit photography or recording of an individual in circumstances where an individual has a reasonable expectation of privacy (for example, inside a home). A UAS operator that invades that privacy and publishes the result may be subject to a lawsuit for the invasion under state law.
- Stalking and Harassment: Traditional crimes such as stalking, harassment, voyeurism, and wiretapping may all be committed through the operation of a UAS.
- Reckless Endangerment: Some states may have the crime of reckless endangerment, which could be applied to the operation of a UAS under certain circumstances. Under a reckless endangerment scenario, the UAS operator could be charged if he or she operates the UAS in such a manner so as to put him/her or third parties at risk of injury, or has actually caused injury to third parties.

K. Limitations on State and Local Regulations of UAS

In discussing state laws protecting privacy and restricting UAS use, it is important to understand the overall scope of permissible UAS regulation at the state and local level. As previously noted, the FAA's safety authority preempts any state or local government regulation of aircraft operations. In response to a flurry of local and state UAS policy proposals, the FAA clarified in a Fact Sheet on State and Local Regulation of UAS published in December 2015 that the FAA maintains regulatory authority over matters pertaining to aviation safety. More recently, in response to a proposal from the National Conference of Commissioners for Uniform State Laws (NCCUSL) to establish a uniform drone tort law that would create a strict liability per se aerial trespass claim for drones operated below 200 feet above ground level or any structure on the land, the FAA published a Press Release Statement on Federal vs. Local Drone Authority in July 2018 which reaffirmed the FAA's exclusive authority to regulate aviation safety, the efficiency of the navigable airspace, and air traffic control, among other things, and clarified that cities and municipalities are not permitted to have their own rules or regulations governing the operation of aircraft.

This preemption debate has broad implications for what states and localities are trying to do. Across the country, states and cities are attempting to impose their own registration and operational requirements for UAS – but these may in fact be preempted. For example, the FAA declared that federal registration is the exclusive means for registering UAS for purposes of operating an aircraft in navigable airspace. Therefore, no state or local government may impose additional registration requirements on UAS operating in navigable airspace without first obtaining FAA approval. The federal district court case, *Singer v. Newton*, held that although the federal government did not have exclusive regulatory authority over UAS, it struck down certain provisions of the city's ordinance because those provisions conflicted with federal law. Such provisions included registration requirements, ban on flights over city or school property without permission, line of sight requirements, and others. In addition, state lawmakers seeking to mandate equipment or training for UAS, such as geo-fencing, would find such state laws to be preempted.

However, in 2020, Virginia enacted legislation that allows localities to regulate takeoff and landing of UAS on property that is owned by the locality.[31] Notwithstanding the general prohibition that a political subdivision cannot regulate the use of privately-owned UAS, the law carves out an exception for take-off or landing of UAS by a commercial operator acting in compliance with FAA regulations, or deemed reasonable or necessary for emergency or maintenance support functions – which includes maintenance and protection of private critical infrastructure. In addition, a federal district court in Texas denied a plaintiff's claim of preemption for a "No-Fly Provision" intended to protect certain structures including sports venues, critical infrastructure, and correction or detention facilities.[32]

However, the FAA has also stated that laws traditionally related to state and local police power – including land use, zoning, privacy, trespass, and law enforcement operations – generally are not subject to federal preemption. Therefore, the FAA acknowledged that it is within local and state government purview to require their police to obtain a warrant prior to using a UAS for surveillance, or specify that UAS may not be used for voyeurism.

Looking ahead to the FAA reauthorization in 2023, preemption is still a critical topic for Congress. In a Senate Commerce Committee hearing, senators were particularly interested in the scope of federal preemption and the potential risk for the delay of UAS integration. The prior 2018 FAA reauthorization bill also contained strong federal preemption language for state and local laws relating to the design, manufacture, testing, licensing, registration, certification, operation, or maintenance of a UAS, including airspace, altitude, flight paths, equipment or technology requirements, purpose of operations, and pilot, operator, and observer qualifications, training, and certification. In addition, it stated that laws (including common law causes of action) relating to nuisance, voyeurism, harassment, reckless endangerment, wrongful death, personal injury, property damage, or other illegal acts arising from the use of UAS would not be preempted if they are not specifically related to the use of a UAS.

XIII. Drone Management Measures

Drones are a dynamic risk and may be a threat vector. Not only are drones easy to access, they provide a wide range of mobility and surveillance capability to their users. As the prevalence of drone use grows, so does the corresponding airspace security risk to Critical Infrastructure sites. With that, there is both knowledge to learn and steps companies can take now to reduce the threat and risks associated with drones.

A. DHS Guidance

DHS has provided a general overview of what measures you can take to secure your facilities. Reference: Department of Homeland Security – UAS and Critical Infrastructure – Understanding the Risk.

These measures are:

1. Research and implement legally approved counter-UAS technology

[31] See Code of Virginia § 15.2-926.3.

[32] *Nat'l Press Photographers Ass'n v. McCraw*, 504 F. Supp. 3d 568 (W.D. Tex. 2020). We also note a recent state court case in Michigan which involved state preemption of local ordinances. *See generally Michigan Coal. of Drone Operators, Inc. v. Ottawa Cnty.*, 2022 WL 17073493 (Mich. Ct. App. Nov. 17, 2022).

2. Know the air domain around the facility and who has the authority to take action to enhance security
3. Contact the FAA to consider UAS restrictions in close proximity to fixed site facilities.
4. Update Emergency/Incident Action Plans to include UAS Security and response strategies
5. Build Federal, State, and local partnerships for adoption of best practices and information sharing.
6. Train your employees that if they see something say something.
7. Report Potential UAS threats to your local law enforcement agency.

These measures are helpful guidelines for companies to create effective protocols. We will go further in-depth into specific prudent steps that facilities can take now to better secure their facilities.

B. Training Personnel

Site Security Personnel will be the first responders to drone intrusion events. Regardless of what future technology is employed to prevent drones from flying in your airspace, Security Personnel must be ready to make a judgment call. Because of that, we recommend that personnel in charge of any response be trained in the following competencies to be able to respond and escalate action effectively:

1. **Legal Context of Operations**
   a. Federal
   b. State
   c. Municipal

2. **UAS/UAV lexicon of terms regarding**
   a. Platforms
   b. Behavior
   c. Payloads

3. **Know and Understand tools available**
   a. Facility Maps and Pattern of Life Analysis
   b. How to communicate a common operating picture to relevant stakeholders
   c. How to assess behavior and respond with appropriate escalation

Like all training programs, you must periodically reassess effectiveness. Below is a simple self-assessment to re-assess your site's level of preparedness.

Action: Facility Security Manager Self-Assessment

1. **Protocol**
   a. Does my security team (personnel/contractors) have an established protocol to deal with Unauthorized Drone flights?
   b. Is my protocol easily understandable such that the observer/reporter can easily identify and communicate intrusions and know the proper action to take based on a set escalation procedure?
   c. Do my security personnel know the rules of engagement given all levels of law?
   d. Have our security staff conducted drills and rehearsals to respond to these events?

2. **Escalation Procedures**
    a. Does my team have escalation procedures to notify decision makers at my facility?
    b. Does my team have an established process to know when and how to notify law enforcement?
    c. Does my team know we have a process in place to inform non-decision-making stakeholders at the corporate level who need to be apprised of this event?
    d. Do I have a notification tree for this specific type of event and branch events?

3. **External Organization Contact and Coordination**
    a. Have we rehearsed a response plan with local law enforcement?
    b. Does my team know who to contact at the DHS?

C. Developing Site Situational Awareness through Pattern of Life Analysis

Conduct a pattern of life analysis around your facility and build your response program around it. Before building your UAS Mitigation Process, it is important to develop a threat profile of your facility for this specific threat vector. You can do so by knowing two categories of information regarding your facility: the criticality (from a risk standpoint) of your assets, as well as local terrain. In terms of specific steps, you can do the following to evaluate risk.

1. **Develop your Area of Operations**
    a. Know your facility boundaries as well as the air domain authorities around your area
    b. Knowing Key Assets – EPA and DHS regulations require Petrochemical facilities to report data which can help evaluate the level of risk associated with each asset at your facility:
        i. Risk Management Plan Rule – Worst-Case Scenario Modeling.
        ii. The EHS staff are required by law to model the effects that released quantities of material at your facility may have. Work with your Air Permitting staff to know your worst-case scenario models to help you assess which assets to protect.
        iii. Chemical Facility Anti-Terrorism Standards Reporting – Your facility is required by law to report any and all Chemicals of Interest above threshold quantities.
        iv. Leverage both of these data sources to help establish a criticality score for assets with these chemicals. By doing so, you can also use this information to guide and prioritize future investments of technology based on the criticality of each asset.

2. **Develop Areas of Interest around your facility**
    a. It is important to develop a risk profile of your facility. You can do this by developing an understanding of your local area. For example, Petrochemical facilities located next to recreational facilities would likely experience risk-based intrusions from human factors such as someone accidently flying their drone into your facility. Each facility has a different relative risk profile. It is important to conduct an analysis to help develop effective mitigation procedures as well as to keep security personnel at your facility aware of relative risk to better allow them to escalate action as needed. Information sources that can assist with this:
    b. Local Law Enforcement Crime data and trends
    c. DHS local threat data
    d. Map and geospatial data – Drone flight times will help define the area of interest.

Prior to establishing effective protocol, it is important to be aware of internal assets and your surroundings. By better establishing these two items, you will be equipped with the information needed to build localized and effective mitigation procedures for drone intrusion.

At the end of taking these actions to understand your surroundings, you will have a security plan which identifies critical assets, as well as identified areas of interest around your facility which could be used as launch sites for drone intrusions. This will help facility staff to better anticipate drone intrusions, respond more quickly and effectively, and increase the chance of catching or stopping future perpetrators.

D. Update Integrated Contingency/Security Plans

Title 6 CFR 27 – CHEMICAL FACILITY ANTI-TERRORISM STANDARDS (CFATS) established the requirement for facilities to conduct Security Vulnerability Assessments. As UAS were not as prevalent when the rule was enacted, they did not account for the potential threat. Because of this, a gap exists between the Security Plan and the new UAS threat. Facilities must reassess security plans to account for it. We recommend that each facility reassess their plans by conducting an audit of existing vulnerability assessments given the new threat vector. Once the audit is complete, companies can use this data as a basis for addressing security gaps.

Action: Reassess Security Plans with Drones in Mind:

1. Audit
2. Reassess
3. Rebuild
4. Repeat as needed

Resources:

Chemical Facility Anti-Terrorism Standards

Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries

E. Implementing Detection Hardware

Barring no procedure at all, your facility may operate on a Be on the Lookout Out (BOLO) basis when it comes to drone detection. While this is an important first step, it is important to note that these measures may not adequately provide 360°, 24/7 situational awareness required to mitigate drone risk. A way to solve this lack of persistent coverage is to implement drone detection systems.

As mentioned earlier in previous sections, drone detection devices track the flight patterns of drones. These systems can provide stakeholders with a picture of just how many drones are operating within their airspace. The steps to properly install are as follows:

1. **Cover Key Assets**
   a. Detection devices should be centrally located near critical assets, installed properly, and have proper power supply to prevent disruption.

2. **Use Data**
   a. As with all security plans, your initial plan may change upon gathering additional data through detection and further developing a risk profile. Use collected data properly to

anticipate potential threats based on areas of interest and pattern of life analysis and plan mitigation procedures accordingly.

b. Use data gathered from detection to inform all stakeholders involved. This data will help to further understanding of this threat, and help government agencies to develop policy further.

3. Routine Reporting

a. Establish reporting reviews of gathered data in order to develop mitigation procedures further, identify any threats currently existing, or stop any identified rogue drones in your airspace.

F. Data Sharing

Through the processes outlined above, facilities will generate key data points which they can use to continually secure their facilities. As these threats become more sophisticated and as regulations change, this data will be critical to developing the scope of local security plans. Other ways to leverage data are as follows:

1. Building a Legal Case

a. Flight data will be needed to describe behavior of flight and help establish pilot intent. This will assist facilities in the event of prosecuting rogue pilots during intrusion events.

2. Assisting Law Enforcement

a. By sharing data with Local Law enforcement and DHS, these law enforcement agencies will be better able to address the threats in the future and help coordinate government action needed to better combat or prevent future threats.

3. Petitions

FESSA 2209 is currently in rulemaking. What has not yet been established is whether private entities will have the authority to restrict local airspace. However, by collecting airspace drone utilization data, companies will be able to clearly depict the threat profile to regulatory agencies and advocate for change.

G. Funding

One barrier to implementing detection systems is achieving the company buy-in to make a financial investment. One funding mechanism used by Critical Infrastructure owners to defray the cost is the Port Security Grant Program by the Federal Emergency Management Agency (FEMA).

According to FEMA,

> *"The Port Security Grant Program (PSGP) plays an important role in the implementation of the National Preparedness System by supporting the building, sustainment and delivery of core capabilities essential to achieving the National Preparedness Goal of a secure and resilient nation."*

The purpose of the program is to directly support maritime infrastructure security programs and activities. Details on the Port Security grant can be found in the following link:

https://www.fema.gov/print/pdf/node/635840

XIV. Recent Congressional and Executive Activity

A. Preventing Emerging Threats Act

To assist the DOJ and DHS in combating UAS threats, Congress passed the Preventing Emerging Threats Act of 2018 (codified at 6 U.S.C. § 124n). The Act authorizes the DOJ and DHS to "take actions" to "mitigate a credible threat that an unmanned aircraft poses to the security of a covered facility or asset", notwithstanding Title 18 and Title 49 provisions that may otherwise criminalize the activity. Mitigation can include physically disabling a UAS, taking it over, intercepting its communications, or seizing the UAS itself.

"Covered facility or asset" refers to operations near the U.S. Coast Guard and U.S. Customs and Border Protection; DOJ operations; Federal Bureau of Prisons; National Special Security Events; federal law enforcement investigations; and other mass gatherings.

The Act does *not* extend counter-UAS (C-UAS) authority to state and local law enforcement or national critical infrastructure entities and DOJ and DHS may not delegate authority to any other entities. The Act was originally scheduled to sunset in October of 2022; however, Congress passed a clean one-year extension of the Act.

B. Peters Legislation: Safeguarding the Homeland from the Threats Posed by UAS

In July 2022, the Safeguarding the Homeland from the Threats Posed by UAS bill was introduced by Senate Homeland Security and Governmental Affairs Committee Chairman (HSGAC) Gary Peters (D-MI). The legislation would authorize state, local, territorial and Tribal (SLTT) law enforcement and critical infrastructure owners and operators to deploy UAS detection technology and authorize DHS and DOJ to use existing authorities to protect critical infrastructure. The legislation would also create a five-year Pilot Program through which, in coordination with the DHS/DOJ/FAA, SLTT law enforcement agencies could detect, monitor, and mitigate credible threats that UAS pose to domestic facilities or assets that are identified as high-risk.

The Senate HSGAC marked up a substitute amendment in August 2022, reporting the bill favorably to the full Senate. The bill did not pass in 2022, as various committees in the House of Representatives had concerns primarily related to privacy and civil liberties. This issue will be an important one during the FAA Reauthorization Act process in 2023.

C. White House Counter-Drone National Action Plan

In April 2022, the Biden Administration released its Domestic Counter-Unmanned Aircraft Systems National Action Plan (NAP), which calls for expanding where C-UAS technology can be deployed to protect against nefarious UAS activity, who is authorized to take action, and how it can be accomplished lawfully.

The Plan seeks to close critical gaps in existing law and policy that currently impede government and law enforcement use of C-UAS technology, including:

- Creation of a federally approved list of U.S. government authorized detection equipment to help guide UAS detection system purchases;
- Development of new oversight and authorization mechanisms to help critical infrastructure owners and operators purchase counter-UAS equipment for authorized federal entities or SLTT law enforcement agencies;
- Creation of a new National Counter-UAS Training Center;
- Expansion of the Preventing Emerging Threats Act;
- Enact a comprehensive criminal statute that clearly defines legal and illegal use of C-UAS technology, closes loopholes in existing Federal law, and establishes adequate penalties to deter the most serious UAS-related crimes.

D. FESSA Section 2209 Update

In July 2016, Congress passed and the President signed into law the FAA Extension, Safety, and Security Act of 2016 (FESSA). Section 2209 of FESSA directs the Secretary of Transportation to establish a process to allow critical infrastructure owners and operators to petition the FAA to prohibit or restrict the operation of an unmanned aircraft in close proximity to a fixed site facility. Appropriate applicants include operators and proprietors of critical infrastructure, such as energy production, transmission, and distribution facilities and equipment, oil refineries and chemical facilities, amusement parks, and other locations that warrant such restrictions.

One implemented, this provision may prove valuable to AFPM members seeking to ensure that rogue UAS are not flying above or near their facilities. Unfortunately, implementation of Section 2209 has been continually delayed. As of January 2023, the expected implementation date has been pushed to February 2024.

In the near term, as mandated in the 2018 Reauthorization, the FAA is expected to charter an Aviation Rulemaking Committee (ARC) around counter-drone technology in 2023, with a focus on airport safety and security. It will be important for the AFPM community to be engaged in the policymaking around these issues.

XV. *APPENDIX A*: State UAS Laws Protecting Critical Infrastructure

Alabama

AL Code § 13A-7-4.3 (2021)

(a) For the purposes of this section, the following words have the following meanings:
(1) CRITICAL INFRASTRUCTURE. The term includes, but is not limited to, a chemical manufacturing facility, a pipeline, a refinery, an electrical power generating facility and the area surrounding the facility, an electrical transmission tower and substation and distribution substation, an electric utility control center, communication equipment, a switching station, a water intake structure and water treatment facility, a natural gas transmission compressor station, a liquefied natural gas (LNG) terminal and storage facility, a natural gas and hydrocarbon storage or production facility, mining operations, beneficiation infrastructure and 8 mining infrastructure, and a transportation facility, such as a port, airport, railroad operating facility, or trucking terminal.

(4) UNMANNED AIRCRAFT SYSTEM. A powered, aerial vehicle that does not carry a human operator, uses aerodynamic forces to provide vehicle lift, may fly autonomously through an onboard computer or be piloted remotely, and may be expendable or recoverable. The term does not include a satellite orbiting the Earth or a spacecraft beyond Earth's atmosphere and may not be construed to implicate the provider of a telecommunications link between an owner or operator of an unmanned aircraft system and the unmanned aircraft system.

(b) A person commits the crime of unauthorized entry of a critical infrastructure if the person does any of 6 the following:

(1) Intentionally enters without authority into any structure or onto any premises belonging to another that constitutes in whole or in part a critical infrastructure that is completely enclosed by any type of physical barrier or clearly marked with a sign or signs that are posted in a conspicuous manner and indicate that unauthorized entry is forbidden.

(2) Uses or attempts to use a fraudulent document for identification for the purpose of entering a critical infrastructure.

(3) Remains upon or on the premises of a critical infrastructure after having been forbidden to do so, either orally or in writing, by any owner, lessee, or custodian of the property or by any other authorized person.

(4) Intentionally enters into a restricted area of a critical infrastructure which is marked as a restricted or limited access area that is completely enclosed by any type of physical barrier when the person is not authorized to enter the restricted or limited access area.

(c) A person who commits the crime of unauthorized 2 entry of a critical infrastructure is guilty of a Class A misdemeanor.

(d) If, during the commission of the crime of unauthorized entry of a critical infrastructure, the person injures, removes, destroys, or breaks critical infrastructure property, or otherwise

interrupts or interferes with the operations of a critical infrastructure asset, the person is guilty of a Class C felony.

(e) A person who commits the crime of unauthorized entry of a critical infrastructure while possessing or operating an unmanned aircraft system with an attached weapon, firearm, explosive, destructive device, or ammunition is guilty of a Class C felony.

Arkansas

AR Code § 5-60-103 (2015)

(a) As used in this section:
- (1) "Critical infrastructure" means:
- (A) An electrical power generation or delivery system;
- (B) A petroleum refinery;
- (C) A chemical or rubber manufacturing facility; or
- (D) A petroleum or chemical storage facility; and

(b) A person commits the offense of unlawful use of an unmanned aircraft system if he or she knowingly uses an unmanned aircraft system to conduct surveillance of, gather evidence or collect information about, or photographically or electronically record critical infrastructure without the prior written consent of the owner of the critical infrastructure.

(d) Unlawful use of unmanned aircraft system is:
- (1) A Class B misdemeanor; or
- (2) A Class A misdemeanor for a second or subsequent offense.

Arizona

AZ Rev. State § 13-3729. Unlawful operation of model or unmanned aircraft; state preemption; classification; definitions

A. It is unlawful for a person to operate a model aircraft or a civil unmanned aircraft if the operation:
- 1. Is prohibited by a federal law or regulation that governs aeronautics, including federal aviation administration regulations.
- 2. Interferes with a law enforcement, firefighter or emergency services operation.

B. It is unlawful for a person to operate or use an unmanned aircraft or unmanned aircraft system to intentionally photograph or loiter over or near a critical facility in the furtherance of any criminal offense.
- 3. "Critical facility" means any of the following:
  - (a) A petroleum or alumina refinery.
  - (b) A petroleum, chemical or rubber production, transportation, storage or processing facility.
  - (c) A chemical manufacturing facility.

Delaware

11 DE Code § 1334 (2017). Unlawful use of an unmanned aircraft system; unclassified misdemeanor; class B misdemeanor; class A misdemeanor.

(a) *Definitions.* — The following terms shall have the following meanings as used in this section.

(1) "Critical infrastructure" means petroleum refineries, petroleum storage facilities, chemical storage facilities, chemical manufacturing facilities, fuel storage facilities, electric substations, power plants, electric generation facilities, military facilities, commercial port and harbor facilities, rail yard facilities, drinking water treatment or storage facilities, correctional facilities, government buildings, and public safety buildings or facilities.

(2) "First responder" means federal, state, and local law-enforcement officers, fire, and emergency medical services personnel, hazardous materials response team members, 9-1-1 dispatchers, or any individual who is responsible for the protection and preservation of life and is directed to respond to an incident that could result in death or serious injury.

(3) "Unmanned aircraft system" means a powered, aerial vehicle that:

a. Does not carry a human operator;

b. Uses aerodynamic forces to provide vehicle lift;

c. Can fly autonomously or be piloted remotely; and

d. Can be expendable or recoverable.

(b) *Prohibited acts.* — Except as provided in this section, no person shall knowingly operate, direct, or program an unmanned aircraft system to fly:

(1) Over any sporting event, concert, automobile race, festival, or other event at which more than 1500 people are in attendance; or

(2) Over any critical infrastructure; or

(3) Over any incident where first responders are actively engaged in response or air, water, vehicular, ground or specialized transport.

(c) *Exemptions.* — The prohibitions set forth in subsection (b) of this section shall not apply to:

(1) An unmanned aircraft system used for law-enforcement purposes; or

(2) An unmanned aircraft system flying over property where written permission has been granted by the property owner or occupier; or

(3) An unmanned aircraft system operated by an institution of higher education for educational purposes in compliance with Federal Aviation Administration regulations; or

(4) An unmanned aircraft system that is being used for a commercial or other purpose if the operator is authorized by the Federal Aviation Administration.

(d) *Penalties.* — Unlawful use of an unmanned aircraft system is an unclassified misdemeanor for a first offense and a class B misdemeanor for a second or subsequent offense, except that in any case where physical injury to a person or damage to property occurs as a result of a violation of this section unlawful use of an unmanned aircraft system is a class A misdemeanor.

(e) *Preemption.* — Only the State may enact a law or take any other action to prohibit, restrict, or regulate the testing or operation of an unmanned aircraft systems in the State. This section preempts the authority of a county or municipality to prohibit, restrict, or regulate the testing or operating of unmanned aircraft systems and supersedes any existing law or ordinance of a county or municipality that prohibits, restricts, or regulates the testing or operating of unmanned aircraft systems.

Florida

330.41 Unmanned Aircraft Systems Act.

(a) "Critical infrastructure facility" means any of the following, if completely enclosed by a fence or other physical barrier that is obviously designed to exclude intruders, or if clearly marked with a sign or signs which indicate that entry is forbidden and which are posted on the property in a manner reasonably likely to come to the attention of intruders:

1. An electrical power generation or transmission facility, substation, switching station, or electrical control center.t
2. A chemical or rubber manufacturing or storage facility.
3. A natural gas or compressed gas compressor station, storage facility, or natural gas or compressed gas pipeline.
4. A liquid natural gas or propane gas terminal or storage facility with a capacity of 4,000 gallons or more.
5. Any portion of an aboveground oil or gas pipeline.

(4) Protection Of Critical Infrastructure Facilities.

(a) A person may not knowingly or willfully:

1. Operate a drone over a critical infrastructure facility;
2. Allow a drone to make contact with a critical infrastructure facility, including any person or object on the premises of or within the facility; or
3. Allow a drone to come within a distance of a critical infrastructure facility that is close enough to interfere with the operations of or cause a disturbance to the facility.

(b) A person who violates paragraph (a) commits a misdemeanor of the second degree, punishable as provided in s. 775.082 or s. 775.083. A person who commits a second or subsequent violation commits a misdemeanor of the first degree, punishable as provided in s. 775.082 or s.775.083.

(c) This subsection does not apply to actions identified in paragraph (a) which are committed by:

1. A federal, state, or other governmental entity, or a person under contract or otherwise acting under the direction of a federal, state, or other governmental entity.
2. A law enforcement agency that is in compliance with s. 934.50, or a person under contract with or otherwise acting under the direction of such law enforcement agency.
3. An owner, operator, or occupant of the critical infrastructure facility, or a person who has prior written consent of such owner, operator, or occupant.

(d) Subparagraph (a)1. does not apply to a drone operating in transit for commercial purposes in compliance with Federal Aviation Administration regulations, authorizations, or exemptions.

Louisiana

Louisiana Revised Statutes § 14:63. Criminal trespass

A. No person shall enter any structure, watercraft, or movable owned by another without express, legal, or implied authorization.

B. (1) No person shall enter upon immovable property owned by another without express, legal, or implied authorization.

(2) For purposes of this Subsection, the phrase "enter upon immovable property" as used in this Subsection, in addition to its common meaning, signification, and connotation, shall include the operation of an unmanned aircraft system as defined by R.S. 14:337 in the air space over immovable property owned by another with the intent to conduct surveillance of the property or of any individual lawfully on the property.

(3) The provisions of Paragraph (1) of this Subsection shall not apply to any person operating an unmanned aircraft system in compliance with federal law or Federal Aviation Administration regulations or authorization.

C. (1) No person shall remain in or upon property, movable or immovable, owned by another without express, legal, or implied authorization.

(2) For purposes of this Subsection, the phrase "remain in or upon property" as used in this Subsection, in addition to its common meaning, signification, and connotation, shall include the operation of an unmanned aircraft system as defined by R.S. 14:337 in the air space over immovable property owned by another with the intent to conduct surveillance of the property or of any individual lawfully on the property.

. . .

Louisiana Revised Statutes §337. Unlawful use of an unmanned aircraft system

A. Unlawful use of an unmanned aircraft system is either of the following:

(1) The intentional use of an unmanned aircraft system to conduct surveillance of, gather evidence or collect information about, or photographically or electronically record a targeted facility without the prior written consent of the owner of the targeted facility.

. . .

B. As used in this Section, the following definitions shall apply:

. . .

(3) "Targeted facility" means the following systems:

(a) Petroleum and alumina refineries.

(b) Chemical and rubber manufacturing facilities.

. . .

(e) Critical *infrastructure as defined by R.S. 14:61(B).*[33]

Nevada

NRS 493.109. Unmanned aerial vehicles: Operation near critical facility or within 5 miles of airport prohibited; exceptions; penalty.

1. A person shall not operate an unmanned aerial vehicle within:

(a) A horizontal distance of 500 feet or a vertical distance of 250 feet from a critical facility without the written consent of the owner of the critical facility.

(b) Except as otherwise provided in subsection 2, 5 miles of an airport.

2. A person may operate an unmanned aerial vehicle within 5 miles of an airport only if the person obtains the consent of the airport authority or the operator of the airport, or if the person has otherwise obtained a waiver, exemption or other authorization for such operation pursuant to any rule or regulation of the Federal Aviation Administration. A person who is authorized to operate an unmanned aerial vehicle within 5 miles of an airport pursuant to this subsection shall, at all times during such operation, maintain on his or her person documentation of any waiver, exemption, authorization or consent permitting such operation.

3. A person who violates this section is guilty of a misdemeanor.

4. As used in this section, "airport" means any area of land or water owned, operated or maintained by or on behalf of a city, county, town, municipal corporation or airport authority that is designed and set aside for the landing and taking off of aircraft and that is utilized in the interest of the public for such purposes.

Oklahoma

3 OK Stat § 3-322 (2021). Critical infrastructure facility – Unmanned aircraft prohibited.

A. As used in this section:
1. "Critical infrastructure facility" means:

[33] "Critical infrastructure" is defined by Nev. R.S. 14:61(B) as, "any and all structures, equipment, or other immovable or movable property located within or upon chemical manufacturing facilities, refineries, electrical power generating facilities, electrical transmission substations and distribution substations, water intake structures and water treatment facilities, natural gas transmission compressor stations, liquified natural gas (LNG) terminals and storage facilities, natural gas and hydrocarbon storage facilities, transportation facilities, such as ports, railroad switching yards, pipelines, and trucking terminals, or any site where the construction or improvement of any facility or structure referenced in this Section is occurring."

a. one of the following, if completely enclosed by a fence or other physical barrier that is obviously designed to exclude intruders, or if clearly marked with a sign or signs that are posted on the property, are reasonably likely to come to the attention of intruders, and indicate that entry is forbidden or flight of unmanned aircraft without site authorization is forbidden:
(1) a petroleum or alumina refinery,
(2) an electrical power generating facility, substation, switching station or electrical control center,
(3) a chemical, polymer or rubber manufacturing facility,
(4) a water intake structure, water treatment facility, wastewater treatment plant or pump station,
(5) a natural gas compressor station,
(6) a liquid natural gas terminal or storage facility,
(7) a telecommunications central switching office,
(8) wireless telecommunications infrastructure, including cell towers,
(9) a port, railroad switching yard, trucking terminal or other freight transportation facility,
(10) a gas processing plant, including a plant used in the processing, treatment or fractionation of natural gas or natural gas liquids,
(11) a transmission facility used by a federally licensed radio or television station,
(12) a steelmaking facility that uses an electric arc furnace to make steel,
(13) a facility identified and regulated by the United States Department of Homeland Security Chemical Facility Anti-Terrorism Standards (CFATS) program,
(14) a dam that is regulated by the state or federal government, or
(15) a natural gas distribution utility facility, including, but not limited to, pipeline interconnections, a city gate or town border station, metering station, aboveground piping, a regulator station and a natural gas storage facility, or
b. any aboveground portion of an oil, gas, hazardous liquid or chemical pipeline that is enclosed by a fence or other physical barrier that is obviously designed to exclude intruders;
2. "Dam" means any barrier, including any appurtenant structures, that is constructed for the purpose of permanently or temporarily impounding water; and
3. "Unmanned aircraft" means an aircraft without occupants that is flown by a pilot via a ground control system or autonomously through use of an onboard computer and other additional equipment necessary to operate the aircraft and includes unmanned aircraft commonly called drones.
B. Except as provided in subsection C of this section, a person shall not intentionally or knowingly:
1. Operate an unmanned aircraft over a critical infrastructure facility if the unmanned aircraft is less than four hundred (400) feet above ground level;
2. Allow an unmanned aircraft to make contact with a critical infrastructure facility, including any person or object on the premises of or within the facility; or
3. Allow an unmanned aircraft to come within a distance of a critical infrastructure facility that is close enough to interfere with the operations of or cause a disturbance to the facility.
C. This section shall not apply to conduct committed by:
1. The federal government, the state or a political subdivision of the state;
2. A person under contract with or otherwise acting under the direction or on behalf of the federal government, the state or a political subdivision of the state;

3. A law enforcement agency;
4. A person under contract with or otherwise acting under the direction or on behalf of a law enforcement agency;
5. An owner or operator of the critical infrastructure facility;
6. A person under contract with or otherwise acting under the direction or on behalf of an owner or operator of the critical infrastructure facility;
7. A person who has the prior written consent of the owner or operator of the critical infrastructure facility;
8. The owner or occupant of the property on which the critical infrastructure facility is located or a person who has the prior written consent of the owner or occupant of that property; or
9. An operator of an unmanned aircraft that is being used for a commercial purpose, if the operator is authorized by the Federal Aviation Administration to conduct operations over that airspace.
D. Any person in violation of this section may be civilly liable for damages to the critical infrastructure facility to include, but not be limited to, damage to property, the environment or human health.

Oregon

ORS 837.372. Operation over critical infrastructure facility

(1) As used in this section, "critical infrastructure facility" means any of the following facilities, if completely enclosed by a fence or other physical barrier that is obviously designed to exclude intruders, or if marked with a sign conspicuously posted on the property that indicates that entry is forbidden:

(a) A petroleum or alumina refinery;

(b) An electrical power generating facility, substation, switching station or electrical control center;

(c) A chemical, polymer or rubber manufacturing facility;

(d) A water intake structure, water treatment facility, wastewater treatment plant or pump station;

(e) A natural gas compressor station;

(f) A liquid natural gas terminal or storage facility;

(g) A telecommunications central switching office;

(h) A port, railroad switching yard, trucking terminal or other freight transportation facility;

(i) A gas processing plant, including a plant used in the processing, treatment or fractionation of natural gas;

(j) A transmission facility used by a federally licensed radio or television station;

(k) A steelmaking facility that uses an electric arc furnace to make steel;

(L) A dam that is classified as a high hazard by the Water Resources Department;

(m) Any portion of an aboveground oil, gas or chemical pipeline that is enclosed by a fence or other physical barrier that is obviously designed to exclude intruders; or

(n) A correctional facility or law enforcement facility.

(2) Except as provided in subsection (3) of this section, a person commits a Class A violation if the person intentionally or knowingly:

(a) Operates an unmanned aircraft system over a critical infrastructure facility at an altitude not higher than 400 feet above ground level; or

(b) Allows an unmanned aircraft system to make contact with a critical infrastructure facility, including any person or object on the premises of or within the facility.

(3) This section does not apply to:

(a) The federal government.

(b) A public body.

(c) A law enforcement agency.

(d) A person under contract with or otherwise acting under the direction or on behalf of the federal government, a public body or a law enforcement agency.

(e) An owner or operator of the critical infrastructure facility.

(f) A person who has the prior written consent of the owner or operator of the critical infrastructure facility.

(g) The owner or occupant of the property on which the critical infrastructure facility is located.

(h) A person who has the prior written consent of the owner or occupant of the property on which the critical infrastructure facility is located.

(i) A person operating an unmanned aircraft system for commercial purposes in compliance with authorization granted by the Federal Aviation Administration.

ORS 837.380. Action by owner of real property

(1)Except as provided in subsections (2) and (3) of this section, a person who owns or lawfully occupies real property in this state may bring an action against any person or public body that operates an unmanned aircraft system that is flown over the property if:

(a)The operator of the unmanned aircraft system has flown the unmanned aircraft system over the property on at least one previous occasion; and

(b)The person notified the owner or operator of the unmanned aircraft system that the person did not want the unmanned aircraft system flown over the property.

(2)A person may not bring an action under this section if:

(a)The unmanned aircraft system is lawfully in the flight path for landing at an airport, airfield or runway; and

(b)The unmanned aircraft system is in the process of taking off or landing.

(3)A person may not bring an action under this section if the unmanned aircraft system is operated for commercial purposes in compliance with authorization granted by the Federal Aviation Administration. This subsection does not preclude a person from bringing another civil action, including but not limited to an action for invasion of privacy or an action for invasion of personal privacy under ORS 30.831 (Action for invasion of personal privacy).

(4)A prevailing plaintiff may recover treble damages for any injury to the person or the property by reason of a trespass by an unmanned aircraft system as described in this section, and may be awarded injunctive relief in the action.

(5)A prevailing plaintiff may recover attorney fees under ORS 20.080 (Attorney fees for certain small tort claims) if the amount pleaded in an action under this section is $10,000 or less.

(6)The Attorney General, on behalf of the State of Oregon, may bring an action or claim for relief alleging nuisance or trespass arising from the operation of an unmanned aircraft system in the airspace over this state. A court shall award reasonable attorney fees to the Attorney General if the Attorney General prevails in an action under this section.

Tennessee

TN Code § 39-13-903 (2015)

(a) Subject to the exceptions set forth in § 39-13-902(a), a person commits an offense if the person:

(6) (A) Without the owner or business operator's written consent, knowingly uses an unmanned aircraft within two hundred and fifty feet (250) of the perimeter of any critical infrastructure facility for the purpose of conducting surveillance of, gathering evidence or collecting information about, or photographically or electronically recording critical infrastructure data.

(B) As used in this subdivision, "critical infrastructure facility" means:

(i) An electrical power generation system;

(ii) A petroleum refinery;

(iii) A manufacturing facility that utilizes any combustible chemicals either in storage or in the process of manufacturing;

(iv) A chemical or rubber manufacturing facility; or

(v) A petroleum or chemical storage facility.

AFPM
American
Fuel & Petrochemical
Manufacturers

1800 M Street, NW
Suite 900 North
Washington, DC
20036

202.457.0480
afpm.org