AFPM

American
Fuel & Petrochemical
Manufacturers

Unmanned Aircraft Systems (UAS) Tool Kit

PREPARED BY
HOGAN LOVELLS US LLP and 4C FOR
THE AMERICAN FUEL & PETROCHEMICAL MANUFACTURERS

AFPM
American
Fuel & Petrochemical
Manufacturers

TABLE OF CONTENTS

AFPM
American
Fuel & Petrochemical
Manufacturers

I. INTRODUCTION

Unmanned Aircraft Systems (UAS), or so-called "drones," are gaining 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.[1] The potential 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 to the refinery and petrochemical communities.

This AFPM UAS Tool Kit is designed to provide refiners and petrochemical manufacturers an understanding of the existing UAS legal framework, including the Federal Aviation Administration's (FAA) new Part 107 Small UAS Rule and the waiver process under the rule for authorizing more advanced operations beyond the scope of what is permitted under the rule. It also outlines the risks to the industry as a result of the increasingly prevalent use of this technology by hobbyists, public entities, news organizations, and commercial industry, 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 AFPM UAS Tool Kit, we have assembled a portfolio of key UAS reference documents from a range of sources that contain valuable information and guidance material for commercial UAS operators. A hyperlinked index of this guidance material is attached as *Appendix A*.

This 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, members of the Hogan Lovells Global UAS team, are available to answer any questions that individual companies may have. Operational or site-specific questions can be addressed to 4C.

[1] A UAS consists of an unmanned aircraft, an aircraft control station, and command and control links.

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@hognalovells.com

Uzkar Ibrahim
Email: uzi@4cmarketplace.com
Mobile: 304-532-5284

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.

A. Hobbyist Use

The Small UAS Rule (14 Code of Federal Regulations Part 107; hereinafter "Part 107"), which will be discussed in detail below, does not apply to operations of small UAS carried out strictly for hobby or recreational purposes. And until the FAA Reauthorization Act of 2018 ("2018 Act") was signed into law, hobbyist use of drones was broadly authorized in the United States without regulation. However, in light of recent high-profile drone security incursions and incidents, Congress repealed Section 336, the hobbyist legislative carve-out, in the 2018 Act. Under the 2018 Act, all UAS operators will have to pass a basic aeronautical safety test. In addition, Congress granted FAA explicit authority to require remote identification for all, including hobbyists; and to regulate all UAS, including model aircraft, as safety and security require.

The FAA is currently reviewing the 2018 Act and will soon take steps to implement the new law. In the meantime, the rules around hobbyist flight remain unchanged. Model aircraft are generally permitted to be flown less than 400 feet above ground level[2] if the model aircraft weigh less than 55 pounds,[3] is flown within visual line of sight, and is operated in accordance with a community-based set of guidelines in a manner that does not interfere with, and gives way to, manned aircraft.[4] Model aircraft operators do not have complete flexibility, however; they must provide advance notice to air traffic control and airport operators in order to fly within five miles of an airport, and the FAA has the ability to enforce the law against hobbyists who fly their model aircraft in a way that recklessly endangers the public.[5]

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. Doing so without complying with the applicable regulations and authorizations raises legal liability issues for both the individual employee and the company for which he/she is flying.[6]

B. Public Use

Federal, state, and local agencies may also operate UAS in the United States with authorization from the FAA. 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 function"[7] under the authority of a public Certificate of Waiver or Authorization (COA) issued to the government entity.

Public use of UAS is relevant to AFPM members for at least two reasons. First, private companies often collaborate with public entities, such as public universities, in order to fly in partnership under a public COA. Refineries and petrochemical manufacturers interested in UAS may consider partnering with a public university for this purpose. Second, refineries and

---

2 Advisory Circular 91-57A, Model Aircraft Operating Standards (September 2, 2015).

3 Unless otherwise properly certified. *See* FAA Reauthorization Act of 2012, Section 336 (Special Rule for Model Aircraft).

4 FAA Reauthorization Act of 2012, Section 336.

5 *See e.g.*, http://www.ntsb.gov/legal/alj/OnODocuments/Aviation/5730.pdf, Docket No. CP-217 (N.T.S.B. Nov. 17, 2014).

6 For additional guidance on the distinction between hobbyist and commercial use, see Interpretation of the Special Rule for Model Aircraft Notice of Interpretation and Request for Comment, 79 Fed. Reg. 36172 (June 25, 2014; Docket FAA-2014-0396).

7 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).

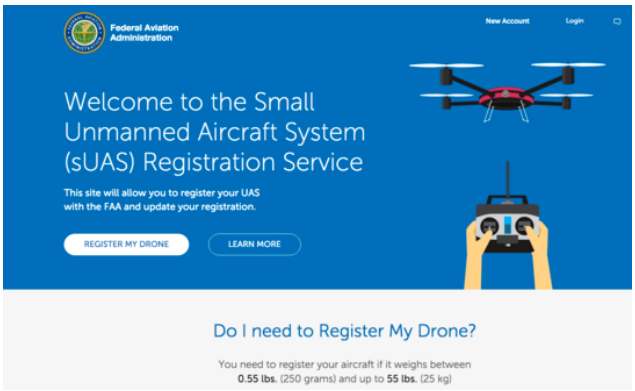
petrochemical manufacturers should be aware that local, state, and federal agencies, including those related to environmental and regulatory enforcement, may themselves be operating UAS under this provision. Companies may therefore be on the receiving end of UAS surveillance from the government.

In addition to operating UAS under a public COA, governmental entities can also voluntarily choose to operate as a civil (commercial) aircraft under the regulatory framework of Part 107.

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.[8] 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. UAS REGISTRATION AND MARKING REQUIREMENTS



Over the past several years there has been a surge in news events involving careless operators misusing drones, including crashes at stadium sporting events and hundreds of incidents involving close encounters between UAS and manned aircraft. In response to these news reports, and in an effort to educate new airspace users on the safe operation of UAS in the National Airspace System (NAS), in December 2015 the FAA published an Interim Final Rule that mandated the registration of small UAS with the FAA, including those used for recreational or hobby use. In May 2017, the U.S. Court of Appeals for the District of Columbia Circuit issued an opinion in Taylor v. Huerta striking down the FAA's registration rule as applied to model aircraft owners. In response to this decision, Congress passed–and President Donald Trump signed–Section 1092(d) of the National Defense Authorization Act for Fiscal Year 2018 (NDAA 2018), which included a legislative fix to allow the FAA to require registration/marking of model aircraft. While commercial operators were already required to register UAS, hobbyist operators were historically exempt from registration requirements.

While the registration rule upset the hobbyist community, the commercial UAS community was generally pleased with the

[8] This means that a non-governmental organiza sampling would be treated the same as a commercial us

development. The rule, which applies to all UAS weighing more than 250 grams (0.55 pounds) and less than 55 pounds, created an alternative web-based UAS registration system (called the "DroneZone") designed to be simpler and more streamlined than the FAA's existing (archaic) paper-based aircraft registration system that commercial operators were required to use.

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

- 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.

- Although each UAS must be assigned a unique registration number, commercial operators will be given a single online profile that allows them to manage the registration application process for each UAS.

- Prior to operation, unmanned aircraft must be marked with its registration number. The UAS can be marked using a permanent marker, label, or engraving, as long as the number remains affixed to the unmanned aircraft during routine handling and all operating conditions and is readily accessible and legible upon close visual inspection. The registration number may also be enclosed in a compartment that is readily accessible, such as a battery compartment.

- While there is a U.S. citizenship requirement for registration, as is the case for manned 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 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.

- There is no requirement to re-register UAS that have already been registered under the existing system. Operators may continue using the existing registration system or, alternatively, switch over to the new registration system when the registration is renewed.

- If the UAS is destroyed, sold, lost, or transferred, the UAS registration should be cancelled using the FAA's DroneZone portal.

IV. FAA SMALL UAS RULE (PART 107)

In 2012, Congress passed the FAA Modernization and Reform Act (FMRA) of 2012. FMRA Section 333 directed the Secretary of Transportation to determine whether UAS operations posing the least amount of public risk and no threat to national security could safely be operated in the NAS

and, if so, to establish requirements for the safe operation of these systems in the NAS. On February 23, 2015, as part of its ongoing efforts to integrate UAS operations in the NAS and in accordance with FMRA Section 333, the FAA issued a Notice of Proposed Rulemaking (NPRM) proposing to amend its regulations to adopt specific rules for the operation of UAS in the NAS. The FAA received over 4,600 public comments on the proposed rule before the comment period closed on April 24, 2015. AFPM submitted comments to the FAA on behalf of its membership, urging the FAA to move expeditiously to finalize the proposed UAS regulations and suggesting several revisions to the proposed rule. AFPM's comment requested enhanced protections for critical infrastructure from unauthorized UAS overflights and enhanced flexibility for the FAA to provide relief from certain operational restrictions.

After considering comments submitted in response to the NPRM, the FAA released its highly anticipated and long-awaited Small UAS Rule on June 21, 2016. The rule was implemented on August 29, 2016. The new rule represents a significant milestone for the commercial UAS industry, and will benefit a wide range of commercial industries, including refineries and petrochemical manufacturers. Prior to the new rule, businesses seeking to operate UAS needed to apply for and receive a "Section 333 Exemption" from the FAA, which was often a time-consuming and expensive process.

The final rule is codified in various parts of the Federal Aviation Regulations (FARs), but is referred to collectively as "Part 107," which is the new part of the FARs specifically reserved for commercial small UAS activities. Part 107 provides clarity and a streamlined operational pathway for operators seeking to use UAS commercially.

Part 107 contains several key operating restrictions, some of which are quite strict. Notably, as discussed in more detail below, Part 107 does contain a waiver process that will allow for more advanced small UAS operations beyond the scope of Part 107 in circumstances where it can be done safely. This AFPM UAS Tool Kit provides a summary of the new rule and identifies the key requirements and restrictions that refineries and petrochemical manufacturers should be aware of when operating small UAS. The Tool Kit also describes the Part 107 waiver process and discusses key issues AFPM members should consider when pursuing FAA waivers.

A. Part 107 Pilot Certification Requirements

Prior to the enactment of Part 107, businesses seeking to operate UAS needed to apply for and receive a "Section 333 Exemption" from the FAA. One of the most burdensome requirements for operations conducted under the "Section 333" framework was the requirement that the operator of the UAS hold a manned aircraft pilot's license. Part 107 eliminates the manned aircraft pilot's license requirement and instead

requires operators to obtain a Remote Pilot Certificate with a small UAS rating.

Unlike the requirements for obtaining manned aircraft pilot certificates, the FAA does not require actual flight training, practical examinations, or separate medical certification to receive a remote pilot certificate.

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, and a visual observer (Observer). 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. However, the remote PIC does not have to be the person manipulating the flight controls (although often he or she will be) and can instead supervise that individual. Observers 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 manned 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 700 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 here.[9] 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 manned 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 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 manned 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.

[9] Additional details on the application process are available at:
https://www.faa.gov/uas/getting_started/fly_for_work_business/becoming_a_pilot/

B. General Operating Requirements Under Part 107

While Part 107 broadly authorizes low-risk commercial small UAS operations in the United States, the rule contains several key operating restrictions to maintain the safety of the NAS and ensure that small UAS do not pose a threat to national security. Key operational restrictions in Part 107 include the following:

- Unmanned aircraft must weigh less than 55 lbs. (25 kg) including payload.
- Visual line of sight (sometimes abbreviated "VLOS") operations only. The unmanned aircraft must remain within VLOS of the remote pilot-in-command (PIC) and visual observer (if one is used). At all times, the unmanned aircraft must remain close enough to the remote PIC for the remote PIC to be capable of seeing the aircraft with vision unaided by any device other than corrective lenses.
- Observers may be used, but they are not required. The remote PIC may choose to use a Visual Observer (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 unmanned aircraft, 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 unmanned aircraft.
- No person may act as the remote PIC, a person manipulating the controls, or an Observer for more than one unmanned aircraft operation at one time.
- Daylight-only operations (official sunrise to official sunset, local time). Twilight operations are approved when the small UAS is equipped with lighted anti-collision lights.
- Must yield right-of-way to other aircraft, manned or unmanned.
- 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 unmanned aircraft 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 FAA's online portal here.
- Operations in Class G airspace are allowed without ATC permission.
- No careless or reckless operations.

C. UAS Requirements

Part 107 does not establish any design standards for UAS, and an FAA airworthiness certification is not required. However, remote PICs must maintain the UAS in a condition for safe operation and, prior to each flight, must verify that it is actually in a condition for safe operation. Upon request from the FAA, remote PICs are required to make the UAS available for testing or inspection, as well as any associated documents and records (for example, maintenance logs and manufacturer manuals). While not required by Part 107, whenever possible, the operator should maintain and inspect the UAS and its components in accordance with the manufacturer's instructions.

D. Effect of Part 107 on Section 333 Exemptions

Now that Part 107 is in effect, many companies that have a "Section 333" Exemption are wondering how Part 107 impacts their exemptions. Part 107 allows UAS operators who have received and are currently operating under approved Section 333 Exemptions to conduct operations under their Section 333 Exemptions or under Part 107, whichever provides the broadest regulatory permission. For example, operators with a current Section 333 Exemption allowing nighttime operations can continue to conduct nighttime operations under their Section 333 Exemption until the exemption expires, avoiding the immediate need to obtain a waiver for such operations under Part 107 but subject to the conditions and limitations set forth in the Section 333 Exemption. Prior to expiration, applicants can seek renewal, at which time the FAA will evaluate the operations covered by the Exemption. If the operations fall within the scope of Part 107 and may be eligible for a waiver, the FAA will likely find no need to renew the Section 333 Exemption. Instead, the FAA would require the operator to seek a waiver under Part 107. In the vast majority of cases, Part 107 is more lenient and provides more operational flexibility than Section 333 Exemptions. For this reason, there would be little, if any, incentive for refiners and petrochemical manufacturers to continue operating UAS under a Section 333 Exemption.

While most commercial UAS operations relevant to refineries and petrochemical manufacturers can occur under Part 107, including waivers issued under Part 107, operations involving UAS that weight 55 pounds or more fall outside of the scope of Part 107 and require either a Special Airworthiness Certificate or, historically, an Exemption. Prior to passage of the 2018 Act, UAS operations outside the scope of Part 107 typically required an Exemption issued under Section

333 of FMRA. This process will be different now because Section 347 of the 2018 Act repealed Section 333 of FMRA and replaced it with a new process that allows the FAA to permit UAS to operate under a "special authority," including beyond visual line of sight, over populated areas and at night. As part of this new permitting process, the FAA will use a "risk-based approach" that considers "which types of unmanned aircraft systems, if any, as a result of their size, weight, speed, operational capability, proximity to airports and populated areas, operation over people, and operation within or beyond the visual line of sight, or operation during the day or night, do not create a hazard to users of the national airspace system or the public…" The new permitting process established under Section 347 of the 2018 Act expires on September 30, 2023.

V. PART 107 WAIVERS & AUTHORIZATIONS

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. Waivable sections of Part 107 include:

- Operation from a moving vehicle or aircraft (§ 107.25)
- Daylight operation (§ 107.29)
- Visual line of sight aircraft operation (§ 107.31)
- Visual observer (§ 107.33)
- Operation of multiple small unmanned aircraft systems (§ 107.35)
- Yielding the right of way (§ 107.37(a))
- Operation over people (§ 107.39)
- Operation in certain airspace (§ 107.41)
- Operating limitations for small unmanned aircraft (§ 107.51)

To be eligible for a waiver, applicants must be able to demonstrate to the FAA that the proposed operation can be conducted safely. 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. Similar to Exemptions granted under the "Section 333" framework, each waiver contains conditions and limitations that need to be complied with (called "common provisions" and "special provisions").

As of September 10, 2018, the FAA has granted 2,037 waivers, the vast majority of which are waivers to permit UAS operations at night (1,867 waivers).[10] The remaining waivers granted thus far include:

- 106 airspace waivers
- 37 waivers authorizing a single remote pilot to operate multiple UAS simultaneously
- 22 waivers authorizing limited beyond visual line of sight operations (BVLOS)
- 28 waiver from visibility and cloud minimum operating limitations

[10] Some companies have been granted waivers from multiple sections of Part 107.

- 13 waivers relating to visual observer requirements
- 13 waivers authorizing flights over people
- 4 waivers authorizing UAS operations from a moving vehicle (non-sparsely populated area)

Waiver applications can be submitted electronically using the FAA DroneZone portal here. 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 up to 5 PDF files to the waiver application.

The FAA's Waiver Safety Guideline Questions (previously referred to as "performance-based standards") describe information needed to make a successful safety case for granting a waiver. There are certain questions that apply universally to all waiver types, including basic operational details, UAS details, and pilot/personnel details. There are also more specific questions that vary based on the type of waiver being requested. The level of detail and the additional supporting documents that will be necessary for adequately responding to the FAA's Waiver Safety Guideline Questions will vary depending on the complexity of the proposed operation. In other words, the riskier 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 form, applicants receive an automated email confirmation with an assigned waiver tracking number. 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 trademark, 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.

A. Relevant Waivers for Refiners and Petrochemical Manufacturers

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

i. Daylight operation (§ 107.29)

As previously noted, Part 107 only authorizes UAS operations during daylight and civil twilight hours (30 minutes before official sunrise and 30 minutes after sunset). A waiver waiving the Daylight operation requirement in § 107.29 would allow UAS operations to be conducted at night. This is currently the most popular waiver being applied for and the safety case mitigations have become fairly standardized. Generally speaking,

the FAA has found the following safety mitigations to be sufficient for granting a waiver authorizing night operations:

- Mandatory use of one or more Observers;
- The remote PIC and Observer must be trained to recognize and overcome visual illusions caused by darkness, and understand physiological conditions which may degrade night vision;
- Sufficient illumination to allow both the remote PIC and Observer to identify people or obstacles on the ground, or conduct a daytime site assessment prior to conducting operations to identify hazards; and
- The unmanned aircraft must be equipped with lighted anti-collision lighting visible from a distance of no less than 3 statute miles.

ii. Operation over people (§ 107.39)

Part 107 authorizes UAS operations directly over people "directly participating" in the UAS operation or other individuals who are located under a protective structure or stationary vehicle. As long as it is safe to do so and does not create a hazard, the UAS can be operated near, but not directly over, other people who are not directly participating in the UAS operation. The group of people "directly participating" in the operation does not include individuals participating in a broader endeavor, such as on-site company employees, even if they consent to the overflight. "Directly participating" only refers to specific personnel that the remote pilot has deemed to be involved with the flight operation, including the person manipulating the controls of the UAS (if different from the remote PIC) and the Observer. Direct participants also include any person who is necessary for the safety of the UAS flight operation. This could include, for example, security personnel tasked with ensuring that the area of operation below where the UAS is operating remains free from people or other potential hazards. Depending on a plant's layout and other characteristics, it may be difficult or impractical to control the flow of company employees or other people on the ground. For these plants, the prohibition of flights over people, including brief moments of overflight, could make it difficult or impossible to conduct on-site UAS operations. In these types of scenarios, a waiver authorizing operations over nonparticipating plant employees would provide more UAS operational flexibility.

iii. 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 unmanned aircraft at all times during the flight with unaided vision (except glasses or contact lenses).[11] While companies may voluntarily choose to use an Observer 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). The benefit to using an Observer 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 unmanned aircraft. In practice, depending on the size of the unmanned aircraft and other conditions affecting visibility, the VLOS requirement effectively limits the area of UAS 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 UAS operations, including, for example, aerial inspections of large facilities or other linear assets like pipelines where the unmanned aircraft would typically need to operate at greater distances from the remote PIC. In these scenarios, a waiver permitting UAS operations beyond VLOS (sometimes abbreviated "BVLOS") would make these activities much easier by expanding the geographic scope of UAS 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 unmanned aircraft is operated BVLOS of the remote PIC.

iv. Operating limitations for small unmanned aircraft (§ 107.51)

Under Part 107, the operating limitations for UAS include limitations on speed, altitude, flight visibility, and cloud clearance. For refiners and petrochemical manufacturers operating UAS, the operating limitations relating to flight visibility and cloud clearance minimums are likely more relevant than the speed and altitude limitations. The minimum flight visibility under Part 107 is 3 statute miles from the location of the UAS ground control station, and the minimum distance of the unmanned aircraft 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 unmanned aircraft will avoid non-participating aircraft; and (3) conspicuity of the unmanned aircraft can be increased to allow it to be seen at a distance of at least 3 statute miles.

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

B. Part 107 Airspace Authorizations

Part 107 authorizes UAS to be operated in Class G airspace without prior approval from ATC. UAS may be operated in Class B, C, D, and E airspace with prior approval from ATC. ATC approval can be obtained by submitting an application through either the Low Altitude Authorization or Notification Capability "LAANC", or through the FAA's DroneZone Portal.

i. LAANC Airspace Authorizations

Airspace authorization applications submitted through the FAA DroneZone Portal are subject to long waiting periods; it can take the FAA several months to issue an authorization. To address these challenges, the FAA is collaborating with private industry to facilitate the sharing of airspace data in an effort to streamline the airspace authorization process. The FAA's National Beta test of LAANC commenced in April 2018 and will last throughout 2018. The Beta seeks to test the capability nationwide; the results will inform future expansions of the capability. LAANC deployed in waves regionally and is now active at nearly 300 air traffic facilities covering approximately 500 airports.

Under the FAA's "UAS Data Exchange" umbrella, the agency will support multiple partnerships, the first of which is the Low Altitude Authorization and Notification Capability or "LAANC." LAANC is an industry-developed application with the goal of providing UAS operators near real-time processing of airspace notifications and automatic approval of requests that are below approved altitudes in controlled airspace. As of October 2018, there are currently fourteen approved LAANC UAS Service Suppliers: Aeronyde, Airbus, AirMap, AiRXOS, Altitude Angel, Converge, DJI, Harris Corporation, Kittyhawk, Project Wing, Skyward, Thales Group, UASidekick, and Unifly. The FAA is expected to approve additional LAANC UAS Service Suppliers in 2019.

Airspace data is provided through the UAS facility maps created by ATC facilities which show the maximum altitude around airports where the FAA may authorize operations without further coordination with the individual ATC facility. Altitudes range from 0-400 feet above ground level (AGL).

ii. DroneZone Airspace Authorizations

Airspace authorization requests to operate at altitudes above the limits designated on the UAS facility map will require further coordination between FAA and the individual ATC facility and these applications must therefore be submitted using the FAA's DroneZone Portal. Additionally, at least initially, LAANC cannot be used to obtain an airspace authorization that is combined with a Part 107 operational waiver. For example, if a company holds a waiver from § 107.29 to authorize UAS operations a night, and the company wants to fly an unmanned aircraft at night in controlled airspace, an airspace authorization would need to be obtaining using the FAA's DroneZone Portal—not LAANC. For areas where LAANC is not yet active, airspace authorization requests will need to be submitted using the FAA DroneZone Portal.

iii. 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.[12]

VI. UPCOMING FAA REGULATORY ACTIONS

The commercial drone industry anxiously awaits broad "expanded operations," particularly for flights BVLOS, over people, and more. In the 2018 Act, Congress expressed its sense that FAA ought to prioritize broad authorization of these expanded operations. Previously, the federal government had stated that the FAA needs the authority to regulate hobbyist drones, including "remote ID for all," before expanded operations are approved. Now that the FAA has that authority, the roadblocks are gone, and the FAA is seeking to move these actions forward.

Right now, there are two regulatory actions under formal review: an NPRM on operations over people, and an Advance Notice of Proposed Rulemaking (ANPRM) on drone security. We expect to see these regulatory actions imminently. A Remote ID rule is expected in early 2019, and a rule authorizing BVLOS flights is longer term.

---

12 Additional details regarding the SGI process are located in Chapter 7 of FAA Order JO 7200.23A.

A. Operations Over People / Micro-UAS Update

On February 23, 2016, the FAA announced the creation of a new aviation rulemaking (ARC) committee to study and recommend rules for authorizing some UAS to fly over people. The ARC was composed of various industry stakeholders, including UAS manufacturers, operators, academics, and trade organizations. On April 1, 2016, the ARC Recommendations Final Report was published. The recommendations made by the ARC, and the rules ultimately adopted by the FAA for operating UAS over people, will significantly affect not only how UAS are manufactured, but could broaden the scope of permissible UAS operations for many commercial industries, including operations for refineries and petrochemical manufacturers.

The ARC report presented the FAA with four categories of UAS operations based on the level of risk. Below is a summary of the four categories:

Category 1: Includes small UAS weighing 250g (0.55 lbs.) or less. The ARC determined that the level of risk of injury posed by this category of UAS is so low that no performance standards and no operational restrictions beyond those imposed by the proposed Part 107 are necessary.

Category 2: Under Category 2, a small UAS weighing more than 250g may operate over people if it meets certain certification and operational requirements. It would require the manufacturer of the small UAS to provide an operating manual to the operator, which would need to include operator requirements for flights over people. There is a requirement to maintain minimum set-off distances of 20 feet above people's heads, or 10 feet laterally away from people, and the UAS may not operate so close to people as to create an undue hazard.

Category 3: Category 3 operations present a higher level of risk than Category 2 operations. As such, operations are prohibited over crowds or dense concentrations of people. Limited operations over people are permitted if the operation is conducted over a closed-site or restricted-access area, or if the flight is limited to brief overflight of people incidental to the operation.

Category 4: Category 4 operations are those that present the same level of risk as Category 3, but that involve sustained flight over crowds and/or dense gatherings of persons. Category 4 operations require the operator to have a risk mitigation plan specific to the operation, similar to what helicopter operators have to submit to the FAA for operations over congested areas.

It is important to note that the ARC report contains only *recommendations*. The FAA still must review the recommendations and issue a proposed rule for operating UAS over people. The FAA initially planned to publish the Operations of Small Unmanned Aircraft Over People Notice of Proposed Rulemaking (NPRM) in December 2016, however this action stalled over security concerns raised during the federal interagency review process. In May 2018, the FAA sent the Operations of Small Unmanned Aircraft Over People back to the White House (specifically, the

Office of Information and Regulatory Affairs (OIRA) at the Office of Management and Budget (OMB)) for interagency review. The proposed rule would establish performance-based standards and means-of-compliance for allowing small UAS operations over people. The FAA is expected to publish the Operations of Small Unmanned Aircraft Over People NPRM sometime in the coming months or early 2019. After the NPRM is published, the proposed rule will go through the notice and public comment process. Given that the ability to fly over people, including facility employees not directly involved with operating the UAS, will make it easier to conduct critical infrastructure inspections, it will be important for the AFPM community to be engaged in the policymaking around this issue.

B. Safe and Secure Operations of Small Unmanned Aircraft Systems

The FAA's ANPRM for the Safe and Secure Operations of Small Unmanned Aircraft Systems was also sent to OIRA for review in May 2018. The ANPRM would seek public comments on UAS-security related issues to address safety and security concerns from the homeland security, federal law enforcement, and national defense communities. Specifically, public comment will be solicited on several operational limitations, airspace restrictions, hardware requirements, and associated remote identification or tracking technologies for UAS. This ANPRM would follow the recent release of the UAS Identification and Tracking ARC report, which includes recommendations on issues related to identifying and tracking drones in flight. The ANPRM is expected to be released soon.

VII. FAA UAS INTEGRATION PILOT PROGRAM

On October 25, 2017, the White House announced the "Unmanned Aircraft Systems Integration Pilot Program," directing 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. This pilot program was codified by Congress in the 2018 Act.

The UAS Integration Pilot Program 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 Program is expected to provide immediate opportunities for new and expanded commercial UAS operations, foster a meaningful dialogue on the balance between local and national interests related to UAS integration, and provide actionable information to the DOT on expanded and universal integration of UAS into the NAS. The three primary objectives of the Pilot Program are to:

i. Test and evaluate various models of State, local, and tribal government involvement in the development and enforcement of Federal regulations for UAS operations;
ii. Encourage UAS owners and operators to develop and safely test new and innovative UAS concepts of operations; and

iii. Inform the development of future Federal guidelines and regulatory decisions on UAS operations nationwide.

The first round of entities selected to participate include the Choctaw Nation of Oklahoma; the City of San Diego; Virginia Tech Center for Innovative Technology; Kansas Transportation Department; Lee County Mosquito Control District of Fort Myers, Florida; 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.

The FAA may consider new applicants for the Pilot Program on a rolling-basis up to one year before the Program is scheduled to terminate in October 2020.

VIII. RESTRICTED FLIGHT AREAS

While the potential 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, similar to what happened when a hobbyist crashed his UAS onto the White House lawn in October 2015 or, more recently, the Seattle Space Needle.

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."[13] The flight would need to comply with Part 107 and the individual operating the UAS 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.[14] 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. In a recent Notice of national policy about aviation-related videos or other electronic media on the internet, the

---

13 *See* https://www.faa.gov/uas/media/model_aircraft_spec_rule.pdf

14 *See* https://www.faa.gov/about/office_org/headquarters_offices/agc/practice_areas/regulations/interpretations/data/interps/2014/williams-afs-80%20-%20(2014)%20legal%20interpretation.pdf

FAA noted: (1) FAA inspectors "have no authority to direct or suggest that electronic media posted on the Internet must be removed"; and (2) "[e]lectronic 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."[15]

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 Model Aircraft 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 Airmen Advisory 4/0811 (NOTAM 4/0811). NOTAM 4/0811 does not prohibit flight over the sensitive facility, but says instead: "Pilots are strongly advised to avoid the airspace above, or in proximity to such sites as...refineries, industrial complexes...and other similar facilities……Pilots should not circle as to loiter in the vicinity over these types of facilities."[16] The advisory applies to all aircraft and pilots, including UAS.

As a general matter, the FAA's safety authority preempts any state or local government regulation of aircraft operations.[17] However, state and local governments do retain certain authority to limit the aeronautical activities of their own departments and institutions.[18] Over the past few years, state and local governments have enacted UAS rules that test the boundaries of this authority. For instance, the City of Newton, Massachusetts passed an ordinance that banned unmanned aircraft 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*[19], the Massachusetts 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 Federal Aviation Administration to incorporate drones into the national airspace.

---

15 FAA Notice N 8900.292 (effective April 8, 2015).

16 Federal Aviation Administration, FDC Special Notice, Notice to Airmen Advisory 4/0811 ("Power Plant NOTAM. Nuclear, hydro-electric or coal power plants, dams, refineries, industrial complexes, military facilities and other similar facilities are covered by NOTAM 4/0811...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.")

17 Federal Aviation Administration, Fact Sheet – State and Local Regulation of UAS (December 17, 2015) *available at*: https://www.faa.gov/uas/resources/uas_regulations_policy/media/uas_fact_sheet_final.pdf

18 *Id.*

19 *Singer v. Newton*, D. Mass., No. CV 17-10071-WGY (Sept. 21, 2017).

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.[20] 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 are legal issues with mitigation techniques.

IX. 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, 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 (which applies only to FAA-certificated individuals) 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 333 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 Federal Aviation Regulations 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 dollars. The FAA determines the amount of the civil penalty using 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. In the absence of aggravating or mitigating circumstances, the FAA typically recommends a sanction at the middle of the sanction range.

[20] 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).

	Large Business Concern	Small Business Concern[21]
Maximum	$18,750-$25,000	$8,250-$11,000
Moderate	$10,000-$18,749	$4,400-$8,249
Minimum	$2,000-$9,999	$1,100-$4,399

It is important to note that sanctions are applied to each individual violation. 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, 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 that 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 and model aircraft 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. 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 rogue (or allegedly rogue) UAS flight.

Congress has also taken notice of the threats posed by rogue drones. On July 14, 2016, Congress promulgated the FAA Extension, Safety, and Security Act of 2016. Section 2205 of the

[21] 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.

Act amended the United States Code to add 49 U.S.C. § 46320 - Interference with wildfire suppression, law enforcement, or emergency response effort by operation of unmanned aircraft. The statute authorizes the FAA to impose a civil penalty of not more than $20,000 against an individual who operates a UAS and in so doing knowingly or recklessly interferes with a wildfire suppression, law enforcement, or emergency response effort. Similarly, the 2018 Act also includes 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 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 unmanned aircraft 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 unmanned aircraft, 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 an unmanned aircraft in flight.[22]

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.

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

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 unmanned aircraft 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 unmanned aircraft or its wireless communication links. Thus, unlike counter-UAS measures that involve destroying or disrupting an unmanned aircraft'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:

1) Targeting the operator and neutralizing 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 unmanned aircraft. The FAA and Department of Homeland Security are experimenting with this approach in the form of CACI International Inc.'s SkyTracker 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.[23] 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 unmanned aircraft 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 an unmanned aircraft. This technology generally works by either: (1) creating a virtual "geo-fence" that prevents the unmanned aircraft from flying into certain airspace; or (2) providing a means for a third party to take over control of the unmanned aircraft and

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

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, GPS link, Wi-Fi, or Bluetooth connection would be illegal.[24] 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.[25] 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."[26]

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). Congress just 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 around counter-drone technology, 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.

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 VIII(E) below, several states have passed legislation that make it a criminal offense to operate UAS over certain critical infrastructure facilities.

---

24 47 C.F.R. § 2.803 (2008).

25 47 U.S.C. §§ 301, 302a (b), 333.

26 18 U.S.C. § 2511(1)(a).

Accordingly, if there is 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 unmanned aircraft, 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. If possible, you should try to photograph the operator, the unmanned aircraft itself, and any observable registration and/or serial numbers on the aircraft. 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 Federal Aviation Regulations are located in Title 14 of the Code of Federal Regulations (14 CFR). Title 14 CFR § 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.

> (a) 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 manned 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.

i. Part 107 and Prohibited or Restricted Areas

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. In response to comments made to the proposed small UAS rule, the FAA stated the following in its analysis of Part 107:

> Restricted airspace is designated when the FAA determines it is necessary to confine or segregate activities hazardous to nonparticipating aircraft. The FAA does not create special use airspace applicable to only one particular airframe or aircraft type. The public's right of free transit through the airspace includes the users of unmanned aircraft. Accordingly, the FAA declines commenters' suggestions to create UAS-specific restricted airspace around certain facilities.[27]

In response to commenters' concerns that Part 107 did not go far enough in protecting overflights of sensitive buildings and infrastructure, the FAA emphasized that FDC NOTAM 4/0811 advises pilots to avoid airspace over sensitive facilities:

> …[T]he FAA acknowledges commenters' concerns. In response to these concerns, the FAA emphasizes FDC NOTAM 4/0811, which states that "…to the extent practicable, pilots are strongly advised to avoid the airspace above, or in proximity to such sites as power plants

[27] 81 FR 42147 (June 28, 2016).

> (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." This NOTAM applies with equal force to pilots of manned and unmanned aircraft…. [T]he FAA notes that FDC NOTAM 4/0811 is advisory and thus, does not constitute a regulatory prohibition.[28]

Thus, an operator may not hover over critical infrastructure facilities, but there is no blanket rule against flying over such facilities. Moreover, NOTAMs are advisory only, and violation of a NOTAM is not itself an enforceable offense.

Finally, Part 107 does not require operators to obtain consent before flying over private property. Thus, while Part 107 includes several operational requirements that would make it difficult in practice to legally operate over third party property without permission from the owner/controller, and which could provide a basis for an FAA enforcement action if not met, such as the restriction on flights over people and prohibition on careless or reckless operations, it does not provide explicit protections for property owners against UAS overflight.

D. Potential Legal Actions at the State and Local Level

In addition to FAA enforcement, 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. 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 flight.

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.[29] Also, most

---

28 *Id.*

29 Cal. Civ. Code § 1708.8; California Assembly Bill 2306, (2014), *available at* http://leginfo.ca.gov/pub/13-14/bill/asm/ab_2301-2350/ab_2306_bill_20140930_chaptered.pdf. (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

states have general consumer protection laws that prohibit "unfair" or "deceptive" acts or practices,[30] 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.

At a high level, refiners and petrochemical manufacturers should consider bringing a private cause of action against a UAS operator in situations where a rogue UAS is flown:

1) At a relatively low altitude over the property and in a way that interferes with the use of the property;

2) Over or near a property and causes a noise or other disturbance;

3) Over or near a property and captures images of company trade secrets; or

4) Over or near property in a way that intrudes upon a person's private affairs and that intrusion is highly offensive to a reasonable person (such as peering through a bathroom window).

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.

E. 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 VII(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 facility's external perimeter, regardless of the height. Other states—like Oklahoma, Oregon, and Texas—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 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.

---

physical trespass, if this image, sound recording, or other physical impression could not have been achieved without a trespass unless the device was used.").

[30] Justin J. Hakala, Follow-On State Actions Based on the FTC's Enforcement of Section 5 at 9-11 (2008), *available at* http://www.ftc.gov/sites/default/files/documents/public_comments/section-5-workshop-537633-00002/537633-00002.pdf.

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, Oregon, and Texas 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. Note that this list is constantly evolving and changing as states consider and pass legislation.

i. 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 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.

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.

ii. Arizona

Arizona made it a class 1 misdemeanor to operate a UAS in violation of a federal law or regulation or to interfere with a law enforcement, firefighter or emergency services operation using UAS. It also made using a UAS to intentionally photograph or loiter over or near a critical facility in furtherance of a criminal offense a class 6 felony. Critical facility is defined to include petroleum production facilities, chemical manufacturing facilities, energy control centers, any railroad infrastructure or facility, courthouses and military installations, among others. The law also clarifies that the definition of aircraft includes UAS for the purpose of the offense of careless or reckless aircraft operation.

> 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.
> . . .

iii. Delaware

In Delaware, 11 DE Code § 1334 (2017) makes it a criminal offense to operate a UAS over a critical infrastructure facility without written permission from the property owner/occupier. The Bill'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.

iv. 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 board 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.

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.
2. A chemical or rubber manufacturing or storage facility.
. . .
4. A natural gas or compressed gas compressor station, storage facility, or natural gas or compressed gas pipeline.
5. A liquid natural gas or propane gas terminal or storage facility with a capacity of 4,000 gallons or more.
6. 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.

v. Louisiana

Louisiana created the crime of unlawful use of a UAS, defined as the intentional use of a UAS to conduct surveillance of a targeted facility without the owner's prior written consent. Targeted

facilities include petroleum and other refineries, chemical and rubber manufacturing facilities, and nuclear power electric generation facilities. The crime is punishable by a fine of up to $500 and imprisonment for six months. A second offense can be punished by a fine of up to $1,000 and one year imprisonment.

> LA Rev Stat § 14:337 Unlawful use of an unmanned aircraft system
>
> A. Unlawful use of an unmanned aircraft system is 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.
> . . .

vi. 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 guilt of a misdemeanor. The law's definition of a "critical facility" includes petroleum refineries and petroleum or chemical production facilities, among others. Nev. Rev. Statute 493.109

vii. 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. See Oklahoma House Bill 2599 - Unmanned aircraft; prohibiting operation of an unmanned aircraft over a critical infrastructure facility; effective date. The Oklahoma statute's definition of a "critical infrastructure facility" includes, among others, petroleum refineries and chemical manufacturing facilities.

viii. 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. OR Rev. Stat. § 837.380 (2015)

ix. 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:

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.

x. Texas

Texas has particularly strong state laws in terms of pursuing civil and/or criminal penalties against rogue UAS flights. Texas state law also provides a private cause of action. Depending on the exact nature of the flight and the intent of the individual operating the UAS, the following sections of the Texas Government Code (Tex. Gov't Code Ann.) could provide a basis for pursuing an action against a UAS operator flying near or over your facility's property:

§ 423.003. OFFENSE: ILLEGAL USE OF UNMANNED AIRCRAFT TO CAPTURE IMAGE.

(a) A person commits an offense if the person uses an unmanned aircraft to capture an image of an individual or privately-owned real property in this state with the intent to conduct surveillance on the individual or property captured in the image.
(b) An offense under this section is a Class C misdemeanor.
(c) It is a defense to prosecution under this section that the person destroyed the image:
(1) as soon as the person had knowledge that the image was captured in violation of this section; and
(2) without disclosing, displaying, or distributing the image to a third party.
. . .

§ 423.004. OFFENSE: POSSESSION, DISCLOSURE, DISPLAY, DISTRIBUTION, OR USE OF IMAGE.

(a) A person commits an offense if the person:

(1) captures an image in violation of Section 423.003; and
(2) possesses, discloses, displays, distributes, or otherwise uses that image.
(b) An offense under this section for the possession of an image is a Class C misdemeanor. An offense under this section for the disclosure, display, distribution, or other use of an image is a Class B misdemeanor.
(c) Each image a person possesses, discloses, displays, distributes, or otherwise uses in violation of this section is a separate offense.
. . .

Sec. 423.0045. OFFENSE: OPERATION OF UNMANNED AIRCRAFT OVER CRITICAL INFRASTRUCTURE FACILITY.

(a) In this section:
(1) "Critical infrastructure facility" means:
(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:
(i) a petroleum or alumina refinery;
(ii) an electrical power generating facility, substation, switching station, or electrical control center;
(iii) a chemical, polymer, or rubber manufacturing facility;
(iv) a water intake structure, water treatment facility, wastewater treatment plant, or pump station;
(v) a natural gas compressor station;
(vi) a liquid natural gas terminal or storage facility;
(vii) a telecommunications central switching office;
(viii) a port, railroad switching yard, trucking terminal, or other freight transportation facility;
(ix) a gas processing plant, including a plant used in the processing, treatment, or fractionation of natural gas;
(x) a transmission facility used by a federally licensed radio or television station;
(xi) a steelmaking facility that uses an electric arc furnace to make steel; or
(xii) a dam that is classified as a high hazard by the Texas Commission on Environmental Quality; or
(B) 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.
…
(b) A person commits an offense if the person intentionally or knowingly:
(1) operates an unmanned aircraft over a critical infrastructure facility and the unmanned aircraft is not higher than 400 feet above ground level;
(2) allows 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) allows 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.
…
(d) An offense under this section is a Class B misdemeanor, except that the offense is a Class A misdemeanor if the actor has previously been convicted under this section.

§ 423.006. CIVIL ACTION.

(a) An owner or tenant of privately-owned real property located in this state may bring against a person who, in violation of Section 423.003, captured an image of the property or the owner or tenant while on the property an action to:
(1) enjoin a violation or imminent violation of Section 423.003 or 423.004;
(2) recover a civil penalty of:
(A) $5,000 for all images captured in a single episode in violation of Section 423.003; or
(B) $10,000 for disclosure, display, distribution, or other use of any images captured in a single episode in violation of Section 423.004; or
(3) recover actual damages if the person who captured the image in violation of Section 423.003 discloses, displays, or distributes the image with malice.
. . .
(d) In addition to any civil penalties authorized under this section, the court shall award court costs and reasonable attorney's fees to the prevailing party.
. . .

F. State Common Law Actions Against Rogue UAS Operators

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."[31] 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.[32]

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.

---

31 RESTATEMENT (SECOND) OF TORTS § 652B.

32 *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.").

- **Nuisance**: Relatedly, a property owner can 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 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 by UAS. 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.

G. Federal Preemption of State and Local UAS Laws

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 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. State lawmakers seeking to mandate equipment or training for UAS, such as geo-fencing, would likely find such state laws to be preempted.

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.

The Senate version of the proposed FAA reauthorization bill also contains 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. Consistent with powers historically granted to state and local governments, the Senate's proposed FAA reauthorization bill states 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.

X. DRONE MANAGEMENT MEASURES

Introduction:
As the current regulation stands, these drones are virtually untraceable on a national scale but have the capability to provide private owners with commercial grade imagery and uncontrolled site access. Due to this dynamic, a major influx of commercial grade drones is occurring within the U.S. airspace, and with it, corresponding airspace security risks to industrial sites. Drones enable a delivery platform for a multitude of different payloads. Many industrial sites with critical assets may want to now consider managing and mitigating this business and public relations risk by implementing the basic security measures outlined below.

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

Measures to be taken to address Unmanned Aircraft System Related Security Challenges:

1. Research and implement legally approved counter-UAS technology
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 adaption 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 general guidelines provide great 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.

Pattern of Life Analysis

Conduct a pattern of life analysis around your facility and build your response program around it. Before building your UAV Mitigation it's important to develop a threat profile of your facility given 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 – Two sources of information that your company produces for EPA and DHS requirements can help you evaluate which assets are key to protect 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. Leverage this data as well as modelling data to help establish a criticality score for assets with these chemicals.
2. Develop Areas of Interest around your facility
    a. Developing Areas of Interest and understanding how they can affect you. Vulnerability to drone penetration of facilities can vary by location. It's important to develop a risk profile of your facility. You can do this by developing an understanding of your local area. For example, an area next to recreational facilities may lend towards risk-based events as human factors cause a drone to fly near your facility versus an area near a military facility or airport with restricted air space. Large parking lots for apartment buildings may be an opportunity for risk reduction measures. Each facility has a different relative risk profile. It's importance 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's 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 action, you should have a security plan which identifies critical assets, overlaid with detection coverage, as well as identified areas of interest around your facility which could be used as launch vectors for drones. This will help facility staff to better anticipate drone intrusions, respond quicker and more effectively, and increase the chance of catching or stopping future perpetrators.

Update Integrated Contingency/Security Plans

When 6 CFR 27 - CHEMICAL FACILITY ANTI-TERRORISM STANDARDS (CFATS)* was enacted in 2007 and established the need for facilities to conduct Security Vulnerability Assessments, they did not account for the type of threat posed by the UAV platform. As stated in earlier sections, given recent improvements to battery life and software on UAV platforms, the need to reassess exists. 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, use this SVA data as a basis for addressing security gaps in current security and response plans. These steps are summarized in the following:

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

Training Personnel

Site Security Personnel are at the frontline of responding to any drone intrusion events. We believe that regardless of what future technology is employed, Security Personnel will always be in charge of responding and deciding what to do. Because of that, they must at minimum be trained in the following to allow them to respond effectively and escalate response as needed:

1. Current Legal Context of Operations
    a. Federal
    b. State
    c. Municipal
2. UAS/UAV lexicon of terms regarding
    a. Platforms
    b. Behavior
    c. Commonly communicated terms to Subject Matter Experts
3. Know and Understand tools available
    a. How to use Terrain 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

These are the minimum standards to which your security personnel must be trained in order to respond effectively to drone intrusion events. Like all training programs, you must periodically

reassess effectiveness. We provide the following questions as a simple self-assessment to test your own level of preparedness.

1. Protocol
    a. Do my security personnel/contractors have an established protocol to deal with these types of situations?
    b. Are my protocol easily understandable such that the frontline person identifying and communicating intrusion know proper actions to take based on a decision matrix and 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? When was the last time these rehearsals were completed? Have any personnel changed since then and is retraining needed?
2. Escalation Procedures
    a. Does my team know escalation procedures to notify relevant decision makers at my facility?
    b. Do I have an established process with notifying law enforcement and when and how to do that?
    c. Do they know who to contact or have the completed the reporting needed for 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. Law Enforcement Contacts
    a. Have we rehearsed a response plan with local law enforcement?
    b. Does my team know who to contact at the DHS?
    c.

Implementing Detection Hardware

Most company incident plans include provisions whereas security personnel operate on a Be on the Lookout Out (BOLO) basis when it comes to drones. While this is an important first step, it's important to note that these measures may not adequately provide 360-degree, 24/7 situational awareness required to actively mitigate this threat. Facilities may consider the use of Drone Detection devices in order to properly maintain situational awareness around their facilities.
As mentioned earlier in previous sections, drone detection devices track the flight patterns of drones and overall can provide stakeholders with a clear picture of just how many drones are operating legally and illegally within their airspace. The steps to properly install are as follows:

1. Cover Key Assets
    a. Location of detection devices to the maximum extent possible cover the critical assets based on Risk Management Plans of your facility. Detection devices should be centrally located near these assets, installed properly, and have proper power supply to prevent disruption of security
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 this data properly to anticipate potential threats based on areas of interest and pattern of life analysis and plan mitigation procedures accordingly.

   b. Use data to inform all stakeholders involved to influence further understanding of this threat, and provide, where possible, data to Department of Homeland Security personnel to help 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.

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. Build your 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. Assist 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 as needed to better combat or prevent threats.
3. Petitions
   a. As stated in a previous section, FESSA 2209 is currently in rulemaking. What has not yet been established is whether private entities will have the authority to restrict local airspace.

There are additional references that can be leveraged to help establish a baseline. One of those is the FAA's drone registration list in your facility's vicinity.

XI. RECENT CONGRESSIONAL ACTIVITY

A. FAA Extension, Safety, and Security Act of 2016

In July 2016, Congress passed and the President signed into law the FAA Extension, Safety, and Security Act of 2016 (FESSA). FESSA included provisions that impact the ability of a critical infrastructure owner to protect, inspect, and maintain that infrastructure using UAS.

Specifically, FESSA requires the expedited development of procedures for processing, on an emergency basis, exemptions, certificates of authorization or waivers for the use of UAS by civil or public operators in response to a catastrophe, disaster, or other emergency to facilitate emergency response operations, such as firefighting, search and rescue, and utility and infrastructure restoration efforts.

In addition, Section 2209 of FESSA directs the Secretary of Transportation to establish a process to allow critical infrastructure owners and operators to petition the FAA Administrator 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. In making such determinations, the FAA Administrator is to consider aviation safety, protection of persons and property on the ground, national security, and homeland security issues. This provision may prove valuable to AFPM members seeking to ensure that rogue UAS are not flying above or near their facilities. The Department of Transportation and the FAA are still in the process of establishing the Section 2209 application for designation process, which is expected to be completed in the next year or two.

Finally, and while certain aspects of this may be redundant given Part 107, FESSA provides for expanded operations, including beyond the visual line of sight during both day and at night, when such operations are associated with certain critical infrastructure. For purposes of this section, critical infrastructure includes, among others, pipelines and oil or gas production, refining, or processing facilities. It eases some of the regulatory challenges for natural gas and oil pipelines, as well as other critical infrastructure owners and operators, and it authorizes critical infrastructure operators to use UAS to conduct any activity already permissible with manned aircraft. This provision was originally introduced by Senator Jim Inhofe (R-Okla.) as a standalone bill titled, UAVs for Energy Infrastructure Act (S.2684). The language of section 2210 is as follows:

SEC. 2210. OPERATIONS ASSOCIATED WITH CRITICAL INFRASTRUCTURE.

(a) In General.--Any application process established under section 333 of the FAA Modernization and Reform Act of 2012 (49 U.S.C. 40101 note) shall allow for a person to apply to the Administrator of the Federal Aviation Administration to operate an unmanned aircraft system, for purposes of conducting an activity described in subsection (b)--

(1) beyond the visual line of sight of the individual operating the unmanned aircraft system; and

(2) during the day or at night.

(b) Activities Described. --The activities described in this subsection are—

(1) activities for which manned aircraft may be used to comply with Federal, State, or local laws, including--

(A) activities to ensure compliance with Federal or State regulatory, permit, or other requirements, including to conduct surveys associated with applications for permits for new pipeline or pipeline systems construction or maintenance or rehabilitation of existing pipelines or pipeline systems; and

(B) activities relating to ensuring compliance with—

(i) parts 192 and 195 of title 49, Code of Federal Regulations; and

(ii) the requirements of any Federal, State, or local governmental or regulatory body, or industry best practice, pertaining to the construction, ownership, operation, maintenance, repair, or replacement of covered facilities;

(2) activities to inspect, repair, construct, maintain, or protect covered facilities, including for the purpose of responding to a pipeline, pipeline system, or electric energy infrastructure incident; and

(3) activities in response to or in preparation for a natural disaster, manmade disaster, severe weather event, or other incident beyond the control of the applicant that may cause material damage to a covered facility.

(c) Definitions. --In this section, the following definitions apply:

(1) Covered facility. --The term ``covered facility'' means—

(A) a pipeline or pipeline system;

(B) an electric energy generation, transmission, or distribution facility (including a renewable electric energy facility);

(C) an oil or gas production, refining, or processing facility; or

(D) any other critical infrastructure facility.

(2) Critical infrastructure. --The term ``critical infrastructure'' has the meaning given that term in section 2339D of title 18, United States Code.

(d) Deadlines. —

(1) Certification to congress.--Not later than 90 days after the date of enactment of this Act, the Administrator shall submit to the appropriate committees of Congress a certification that a process has been established to facilitate applications for unmanned aircraft systems operations described in this section.

(2) Failure to meet certification deadline.--If the Administrator cannot provide a certification under paragraph (1), the Administrator, not later than 180 days after the deadline specified in paragraph (1), shall update the process under section 333 of the FAA Modernization and Reform Act of 2012 (49 U.S.C. 40101 note) to facilitate applications for unmanned aircraft systems operations described in this section.

(e) Exemptions.--In addition to the operations described in this section, the Administrator may authorize, exempt, or otherwise allow other unmanned aircraft systems operations under section 333 of the FAA Modernization and Reform Act of 2012 (49 U.S.C. 40101 note) that are conducted beyond the visual line of sight of the individual operating the unmanned aircraft system or during the day or at night.

B. FAA Reauthorization Act of 2018

Since October 1, 2017, FAA has operated under two short-term extensions of FAA's legislative authority: the Disaster Tax Relief and Airport and Airway Extension Act of 2017[33], extended FAA's funding and authorities through March 31, 2018; and the Consolidated Appropriations Act, 2018[34], further extended FAA's funding and authority through September 30, 2018.

On October 5, 2018, the President signed into law the FAA Reauthorization Act of 2018, which renews funding for another five years. The Act includes significant provisions that enhance the necessary safety and security framework for proper NAS integration—thereby promoting innovation and providing the path forward for commercial drone technology to take off in the United

33 H.R.3823 (P.L. 115-63).

34 H.R. 1625 (P.L. 115-141).

States. From improving the Part 107 waiver process, to promoting Unmanned Aircraft Traffic Management efforts, to expressing the sense of Congress that integrating UAS into the NAS is top priority, the Act expresses clearly the federal government's strong desire to enable expanded commercial drone operations (including flights over people, beyond visual line of sight, and at night) in an expeditious way. And with a framework now in place to enhance drone security, the federal government has the green light to pave the way for broad commercial drone operations.

A list of UAS-related provisions in the 2018 Act is attached as ***Appendix B***.

XII. FEDERAL GOVERNMENT AND UAS PRIVACY

On a federal government level, the FAA regulates the safety and operations of the National Airspace – but it generally does not regulate privacy. To fill this gap, the White House requested the National Telecommunications and Information Administration (NTIA) at the Department of Commerce to convene stakeholders to draft a set of voluntary best practices for UAS operators to follow when privacy concerns may be implicated. In May 2016, stakeholders agreed on a set of best practices, which include a recommendation that UAS operators make a reasonable effort to minimize UAS operations over or within private property without the consent of the property owner. However, the best practices provide an exception for flying over private property without consent when the UAS operator has the "appropriate legal authority" to do so. Given the arguments surrounding what "appropriate legal authority" could entail, and the fact that the best practices are voluntary guidelines, we do not expect the industry best practices document to be a significant deterrent to unauthorized operations over critical infrastructure facilities. However, the best practices can be pointed to in court or otherwise in the course of a dispute as setting a consensus baseline, in terms of privacy, for not operating over or within private property without consent.

Notwithstanding NTIA's efforts, Congress recently instructed the Comptroller General to conduct its own review of privacy issues and concerns associated with UAS use. Congress also made explicit the authority of the Federal Trade Commission (FTC) to enforce violations of the privacy policies of commercial users and expressed the sense of Congress that commercial operators ought to have a privacy policy that is publicly available. Finally, Congress required the FAA to make certain authorizations and details about civil operations available to the public where appropriate.

AFPM
American
Fuel & Petrochemical
Manufacturers

Appendix A: FAA UAS Guidance Material Index

1. Airman Knowledge Testing Center List
2. Advisory Circular (AC) 21-12C – *Application for U.S. Airworthiness Certificate*
3. AC 91-57A – *Model Aircraft Operating Standards*
4. Advisory Circular (AC)107-2 - *Small UAS*
5. FAA Extension, Safety, and Security Act of 2016
6. FAA Fact Sheet on State and Local Regulation of UAS
7. FAA Fact Sheet on UAS (June 2016)
8. FAA Interim Operational Approval Guidance 08-01, *UAS Operations in the National Airspace System* (NAS) (March 13, 2008)
9. FAA Law Enforcement Guidance for Suspected Unauthorized UAS Operations
10. FAA Memorandum Re Educational Use of UAS
11. FAA Letter to COA Holders Regarding UAS Registration
12. FAA Order 2150.3C – FAA Compliance and Enforcement Program
13. FAA Order 8900.1 – UAS Surveillance/Compliance and Enforcement
14. FAA Order JO 7200.23A – Unmanned Aircraft Systems
15. FAA Office of Chief Counsel Legal Interpretation Regarding Media Use of UAS
16. FAA Pilot Handbook, Chapter 15 – *Airspace*
17. FAA Reauthorization Act of 2018
18. FAA UAS Facility Map for LAANC
19. FAA UAS Registration FAQ
20. Database of FAA Waivers Granted
21. Part 107 (full version)
22. Sporting Events Special Security NOTAM

23. Notice JO 7210.891 – *Unmanned Aircraft Operations in the NAS*

24. NAMIC - State Laws Addressing Use Cases Presented in UAS

25. NTIA Voluntary Best Practices for UAS Privacy, Transparency, and Accountability

26. Remote Pilot Exam Sample Questions

27. Remote Pilot Knowledge Test Guide

28. Remote Pilot Small UAS Airman Certification Standards

29. Summary of Small UAS Rule (Part 107)

30. Waiver and Airspace Authorization Application Instructions

31. Waiver Safety Explanation Guidelines for Part 107 Waiver Applications

32. UAS Remote ID ARC Report

AFPM
American
Fuel & Petrochemical
Manufacturers

Appendix B

SUMMARY OF UAS SECTIONS IN THE 2018 FAA REAUTHORIZATION BILL

SEC. 341. DEFINITIONS. This section defines UAS-related terms in the Act.

SEC. 342. UPDATE OF FAA COMPREHENSIVE PLAN. –This section requires the FAA to update the comprehensive plan required by the FAA Modernization and Reform Act of 2012 (FMRA) within 270 days to address certain matters including unmanned aircraft system traffic management.

SEC. 343. UNMANNED AIRCRAFT TEST RANGES. – This section requires the FAA to carry out certain activities and programs in support of the six test ranges established by FMRA.

SEC. 344. SMALL UNMANNED AIRCRAFT IN THE ARCTIC. – This section codifies a provision enacted in section of 331 the FAA Modernization and Reform Act of 2012 governing UAS operations in the Arctic.

SEC. 345. SMALL UNMANNED AIRCRAFT SAFETY STANDARDS. – Directs FAA to establish risk-based consensus safety standards relating to the design, production and modification of sUAS. In order to sell most small UAS in the U.S. market, manufacturers would be required to certify to the FAA that the sUAS conforms to the consensus safety standards.

SEC. 346. PUBLIC UNMANNED AIRCRAFT SYSTEMS. - Codifies Section 334 of the FMRA, which directs the DOT Secretary to help facilitate operations of UAS by government entities. Includes a provision that requires FAA to issue guidance regarding how tethered public UAS that are operated below 150' AGL, and within Class G airspace, or below altitudes designated on the FAA UAS Facility Map can operate without a COA, waiver or other FAA approval.

SEC. 347. SPECIAL AUTHORITY FOR CERTAIN UNMANNED AIRCRAFT SYSTEMS. – This section creates an independent basis for the FAA to authorize unmanned aircraft operations including those that are beyond the visual line of sight and over people based on the unmanned aircraft's safety and operational characteristics. This section also allows the agency to determine whether an airworthiness certificate is required for the proposed operation.

SEC. 348. CARRIAGE OF PROPERTY BY SMALL UNMANNED AIRCRAFT SYSTEMS FOR COMPENSATION OR HIRE. - Within one year of enactment, the FAA Administrator must update existing regulations to authorize sUAS carriage of property for compensation or hire (small UAS package delivery) in the U.S.

SEC. 349. EXCEPTION FOR LIMITED RECREATIONAL OPERATIONS OF UNMANNED AIRCRAFT. – Repeals the Special Rule for Model Aircraft in FRMA Section 336, directs FAA to develop an aeronautical knowledge and safety test for model aircraft operators, and authorizes FAA to impose regulations (including remote ID) on all UAS as necessary.

SEC. 350. USE OF UNMANNED AIRCRAFT SYSTEMS AT INSTITUTIONS OF HIGHER EDUCATION. – This section permits certain unmanned aircraft operations in the course of

educational and research activities at universities to operate under the legal framework for recreational aircraft.

SEC. 351. UNMANNED AIRCRAFT SYSTEMS INTEGRATION PILOT PROGRAM. – Codifies the UAS Integration Pilot Program created by DOT.

SEC. 352. PART 107 TRANSPARENCY AND TECHNOLOGY IMPROVEMENTS. – Within 30 days after enactment of the Act, FAA must publish on the FAA website a representative sample of the safety justifications offered by applicants for sUAS waivers and airspace authorizations; Within 90 days the Administrator must revise the online waiver process to provide real time confirmation that an application has been received by FAA and to provide the applicant with a status of the application (Note: the FAA has already done this with the DroneZone portal).

SEC. 353. EMERGENCY EXEMPTION PROCESS. – This section contains a sense of Congress regarding the beneficial uses of unmanned aircraft in disaster recovery and related uses. This section also requires the FAA to update guidance and develop best practices for law enforcement and other governmental operators of unmanned aircraft.

SEC. 354. TREATMENT OF UNMANNED AIRCRAFT OPERATING UNDERGROUND. – Clarifies that sUAS operating underground for mining purposes shall not be subject to regulation or enforcement by the FAA.

SEC. 355. PUBLIC UAS OPERATIONS BY TRIBAL GOVERNMENTS. – Amends the definition of "public aircraft" in 49 USC § 40102(a)(41) to include an unmanned aircraft that is owned and operated by, or exclusively leased for at least 90 continuous days by an Indian tribal government.

SEC. 356. AUTHORIZATION OF APPROPRIATIONS FOR KNOW BEFORE YOU FLY CAMPAIGN. – Provides $1M in funding each FY through 2023 for the Know Before You Fly educational campaign.

SEC. 357. UNMANNED AIRCRAFT SYSTEMS PRIVACY POLICY. – Clarifies that it is the policy of the United States that the operation of UAS be carried out in a manner that respect and protect privacy consistent with federal, state and local law.

SEC. 358. UAS PRIVACY REVIEW. – Directs the Comptroller General of U.S., in consideration of relevant efforts led by NTIA, to conduct a review of the privacy issues and concerns associated with the operation of UAS.

SEC. 359. STUDY ON FIRE DEPARTMENT AND EMERGENCY SERVICE AGENCY USE OF UNMANNED AIRCRAFT SYSTEMS. – Directs FAA to study UAS use by fire departments and emergency services agencies.

SEC. 360. STUDY ON FINANCING OF UNMANNED AIRCRAFT SERVICES. - Directs the Comptroller General of U.S. to study appropriate fee mechanisms to recover the cost of providing regulation and oversight of UAS and the provision of air navigation services to UAS.

SEC. 361. REPORT ON UAS AND CHEMICAL AERIAL APPLICATION. – Requires FAA to submit a report to Congress within 1 year evaluating which safety requirements under 14 CFR Part 137 should apply to UAS engaged in aerial spraying of chemicals for agricultural purposes.

SEC. 362. SENSE OF CONGRESS REGARDING UNMANNED AIRCRAFT SAFETY. – This section expresses the concern of Congress about the safety risks caused by unauthorized operation of UAS in proximity to airports and the safety risks of potential collisions between UAS and manned aircraft. Further, this section states Congress' sense that the FAA should take measures to reduce such risks through enforcement actions and educational initiatives.

SEC. 363. PROHIBITION REGARDING WEAPONS. – Establishes a $25k civil penalty for a person who operates a UAS equipped with a dangerous weapon unless authorized by the FAA.

SEC. 364. U.S. COUNTER-UAS SYSTEM REVIEW OF INTERAGENCY COORDINATION PROCESSES. – Requires the FAA to review interagency coordination processes and standards for federal use of counter-UAS systems. Requires the FAA to report to certain congressional committees within 180 days of enactment on various matters related to counter-UAS use by federal agencies.

SEC. 365. COOPERATION RELATED TO CERTAIN COUNTER-UAS TECHNOLOGY. - Requires the DOT Secretary to consult with the Secretary of Defense on matters related to the deployment of counter-UAS in the NAS by drawing upon the expertise and experience of the Department of Defense.

SEC. 366. STRATEGY FOR RESPONDING TO PUBLIC SAFETY THREATS AND ENFORCEMENT UTILITY OF UNMANNED AIRCRAFT SYSTEMS. – Requires the FAA to develop a strategy for providing state and local governments and law enforcement with guidance relating to responding to UAS public safety threats and guidance for taking advantage of opportunities to use UAS to enhance the effectiveness of local law enforcement agencies and first responders.

SEC. 367. INCORPORATION OF FAA OCCUPATIONS RELATING TO UNMANNED AIRCRAFT INTO VETERANS EMPLOYMENT PROGRAMS OF THE ADMINISTRATION. – Requires FAA to consult with the Secretary of Veterans Affairs, the Secretary of Defense, and the Secretary of Labor to determine whether FAA occupations relating to UAS can be incorporated into the Veterans' Employment Program of the Administration.

SEC. 368. PUBLIC UAS ACCESS TO SPECIAL USE AIRSPACE. – Directs the DOT Secretary to issue guidance for the expedited and timely access to special use airspace for public UAS in order to assist Federal, State, local, or tribal law enforcement organizations in conducting law enforcement, emergency response, or for other activities.

SEC. 369. APPLICATIONS FOR DESIGNATION. – Amends Section 2209 of the FAA Extension, Safety, and Security Act of 2016 (FESSA) to add "railroad facilities" to the definition of a "fixed site facility" that is eligible for designation.

SEC. 370. SENSE OF CONGRESS ON ADDITIONAL RULEMAKING AUTHORITY. – Emphasizes that integrating UAS into the NAS, including BVLOS operations, nighttime operations and operations over people should remain a top priority for the FAA.

SEC. 371. ASSESSMENT OF AIRCRAFT REGISTRATION FOR SMALL UNMANNED AIRCRAFT. – Requires the DOT Secretary to enter into an agreement with the National Academy of Public Administration, to estimate and assess compliance with and the effectiveness of the registration of sUAS by the FAA pursuant to the interim final rule on registration and marking requirements for sUAS.

SEC. 372. ENFORCEMENT. – Directs the FAA to establish a program to utilize remote detection or identification technologies for safety oversight, including enforcement actions against non-compliant UAS operators.

SEC. 373. FEDERAL AND LOCAL AUTHORITIES. – Directs the Comptroller General to conduct a study on the relative roles of the Federal Government, State, local and Tribal governments in the regulation and oversight of low-altitude operations of UAS and to submit a report to Congress with findings.

SEC. 374. SPECTRUM. - This section requires the FAA, National Telecommunications and Information Administration, and the Federal Communications Commission (FCC) to submit to Congress a report on whether UAS operations should be permitted to operate on spectrum designated for aviation use. This section requires the report to include recommendations of other spectrum frequencies (such as LTE) that may be appropriate for operating UAS.

SEC. 375. FEDERAL TRADE COMMISSION AUTHORITY. – This section makes explicit the authority of the Federal Trade Commission (FTC) to enforce violations of the privacy policies of commercial users.

SEC. 376. PLAN FOR FULL OPERATIONAL CAPABILITY OF UNMANNED AIRCRAFT SYSTEMS TRAFFIC MANAGEMENT. – In connection with the UTM pilot program established in FESSA, directs FAA to coordinate with NASA and industry stakeholders to develop a plan for the implementation of UTM services that expand operational capability, including BVLOS operations.

SEC. 377. EARLY IMPLEMENTATION OF CERTAIN UTM SERVICES. – Within 120 days of enactment of the Act, the FAA must, upon request of a UTM service provider, determine if certain UTM services may operate safely in the NAS before completion of the implementation plan required by section 376.

SEC. 378. SENSE OF CONGRESS. - Expresses Sense of Congress that commercial UAS operators, except those operated for purposes protected by the First Amendment, should have a written privacy policy that is publicly available.

SEC. 379. COMMERCIAL AND GOVERNMENTAL OPERATORS. – Requires the FAA to make available in a single location any COA issued to a governmental entity, a spreadsheet with UAS registration data, a summary of descriptions and general purposes of public UAS operations,

summary descriptions of common civil UA operations, the expiration dates of authorizations, and details regarding the use of facial recognition software.

SEC. 380 TRANSITION LANGUAGE. This section ensures that certain orders, determinations, rules and other actions with legal effect based on authority in certain provisions of the FAA Modernization and Reform Act of 2012 continue to have legal effect after their repeal or recodification.

SEC. 381. UNMANNED AIRCRAFT SYSTEMS IN RESTRICTED BUILDINGS OR GROUNDS. – Makes it a criminal offense under Title 18 to knowingly and willfully operate a UAS with the intent to knowingly and willfully direct or otherwise cause such UAS to enter or operate within or above a restricted building or grounds.

SEC. 382. PROHIBITION. – Makes it a criminal offense under Title 18 to operate a UAS in a manner that interferes with wildfire suppression efforts.

SEC. 383. AIRPORT SAFETY AND AIRSPACE HAZARD MITIGATION AND ENFORCEMENT. – Directs the FAA to work with DOD and DHS and other relevant Federal agencies to help ensure counter-UAS systems to detect and mitigate hostile UAS do not adversely impact airport operations or the NAS; Requires FAA to develop a plan and charter an ARC for the certification, permitting, and authorizing deployment of technology for detection and mitigation of UAS. The plan shall not delegate any authority granted to the FAA to other Federal, State, local, territorial, or tribal agencies, or an airport sponsor.

SEC. 384. UNSAFE OPERATION OF UNMANNED AIRCRAFT. - Makes it a criminal offense under Title 18 to operate a UAS and knowingly interfere with certain aircraft operations or to operate in a runway exclusion zone at an airport.

SEC. 542. PROHIBITED AIRSPACE ASSESSMENT. – Within a year, requires DOT to conduct an assessment on security of prohibited airspace.

SEC. 631. COMMUNITY AND TECHNICAL COLLEGE CENTERS OF EXCELLENCE IN SMALL UNMANNED AIRCRAFT SYSTEM TECHNOLOGY TRAINING. – Requires the DOT Secretary, in consultation with the Secretary of Education and the Secretary of Labor, to establish a process for designating a consortia of public, 2-year institutions of higher education as Community and Technical College Centers of Excellence in sUAS Technology Training.

SEC. 632. COLLEGIATE TRAINING INITIATIVE PROGRAM FOR UNMANNED AIRCRAFT SYSTEMS. – Requires the FAA to establish a collegiate training initiative program relating to UAS by making new agreements or continuing existing agreements with institutions of higher education under which the institutions prepare students for careers involving UAS.

SEC. 721. UNMANNED AIRCRAFT SYSTEMS RESEARCH AND DEVELOPMENT ROADMAP. – Requires DOT to submit a UAS roadmap to Congress on an annual basis.

SEC. 1602. PROTECTION OF CERTAIN FACILITIES AND ASSETS FROM UNMANNED AIRCRAFT. – Authorizes DOJ and DHS to mitigate UAS that pose a safety or security threat to a "covered facility or asset."

SEC. 1603. PROTECTING AGAINST UNMANNED AIRCRAFT. – Authorizes the U.S. Coast Guard to conduct missions related to the security of facilities and assets assessed to be a high-risk and a potential target for unlawful UAS activity.