

UNMANNED AIRCRAFT SYSTEMS INDUSTRY AND REGULATORY UPDATE

Despite the unprecedented challenges facing the energy industry, heightened by the global COVID-19 pandemic, Unmanned Aircraft Systems (UAS) experienced healthy industry growth in 2019 and 2020. In its annual <u>2019</u>

Aerospace Forecast, the Federal Aviation Administration (FAA) reported a 6.4 percent growth rate for commercial and recreational UAS in the U.S. in 2019. Market reports focused on the global UAS market size forecast, a steady annual growth rate of 5.4 percent in the years 2020 through 2025, with the market size projected to grow from \$4.4 Billion in 2019 to \$5.4 Billion by 2025. Of particular note is that the UAS energy industry market is particularly well poised for growth, with an annual growth rate of 25.53 percent forecasted between 2018 and 2025.



UAS are now considered essential tools by energy industry professionals. They are relied on for conducting complex inspection and monitoring of difficult to access infrastructure and locations. UAS are routinely deployed to conduct monitoring, inspection and maintenance of well sites, pipelines, refineries and other oil and gas infrastructure, and are used for a myriad other uses, including the monitoring and tracking of ocean-going ships, inspection of offshore platforms and refineries, inspection and monitoring of power lines, wind turbines and solar panels and field installations. While traditional oil and gas companies have been leveraging UAS technology for nearly a decade, some of the highest growth projections are expected to occur in the renewable energy space (particularly among high power producing nations in Asia-Pacific). However, this industry sector growth is somewhat curtailed by regulatory limitations and the other UAS market challenges outlined below.

FAA Regulatory Activities

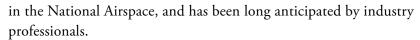
The FAA has reported a slowing trend in recreational UAS, but reports that "[t]he commercial UAS sector is dynamic and appears to be at an inflexion point, demonstrating powerful stages of growth." The reason for such robust growth is an increase in regulatory certainty that Part 107 brings to commercial UAS operations, the ability to obtain waivers for certain UAS operations, and new proposed rulemaking activities by the FAA (such as rules concerning the operation of small UAS over people, nighttime operations and remote identification). The continued engagement by the FAA in issuing waivers, using such waivers to evaluate specific types of UAS operations, and then relying on lessons from the field to continue

rulemaking activities all bodes well for sustainable industry growth over the next several years. In fact, the FAA has been successful in promoting its own online platform – the <u>FAA Drone Zone</u>, as well as other commercial platforms that serve as a one-stop-shop for UAS operational information. These platforms and services reflect the FAA's commitment to ensuring safety and transparency in the information shared with its community and the public.

Several key trends dominated 2019 and 2020, reflecting a positive shift towards expansion of safe commercial small UAS operations.

Remote ID

In December 2019, the FAA announced a Notice of Proposed Rulemaking (NPRM) for Remote Identification (Remote ID) to be mandatory for all UAS over .55 lbs. operating in the National Airspace. Remote ID, or the ability to identify a UAS while in flight, is a critical step in the FAA working to establish unmanned traffic management system





The NPRM "establishes design and production requirements for two categories of remote identification: standard remote identification UAS and limited remote identification UAS. Standard remote identification UAS would be required to broadcast identification and location information directly from the unmanned aircraft and simultaneously transmit that same information to a Remote ID USS through an

internet connection. Limited remote identification UAS would be required to transmit information through the internet only, with no broadcast requirements; however, the unmanned aircraft would be designed to operate no more than 400 feet from the control station."

Under the proposed rules, the following data would be collected and publicly shared via Remote ID, which has drawn some criticism and concern about privacy rights:

- The identity of the UAS consisting of one of the following:
 - the drone's serial number;
 - a session ID (a randomly-generated alphanumeric code);
- The control station's latitude and longitude;
- The control station's barometric pressure altitude;



- A time mark;
- The emergency status of the UAS, which could include lost-link or downed aircraft;
- The unmanned aircraft's latitude and longitude; and
- The unmanned aircraft's barometric pressure altitude.

In May 2020, the FAA announced eight technology partners to help develop the Remote ID framework including Airbus, AirMap, Amazon, Intel, One Sky, Skyward, T-Mobile, and Wing.

LAANC

Throughout 2019, the FAA significantly expanded the <u>Low Altitude Authorization</u> and <u>Capability</u> system (LAANC) that automates the application and approval process for drone operators to obtain airspace authorizations and significantly expedites the authorization process. By year end, LAANC was available for UAS operations near all U.S. airports, and the FAA has reported a near tripling in LAANC authorization requests.

Part 135 and Cargo Delivery

2019 saw an increase in activity related to cargo delivery. Notably, in October 2019, <u>UPS Flight Forward received the first full Part 135 Standard certification</u> from the FAA to be a UAS commercial airline and deliver cargo to consumers. The COVID-19 pandemic in 2020 has only highlighted the need, demand, interest (and concern by some) in accelerating UAS cargo delivery in the United States.



Restrictions on UAS Operations

Throughout 2019, the FAA, in collaboration with the Department of Defense and other state and federal agencies, expanded restrictions on UAS operations near sensitive areas such as prisons, DOD-defined national security sensitive areas, naval vessels offshore, etc.

Changes to FAA Airman Certificate

In January 2020, the FAA required that all applicants for an FAA airman certificate (including certified UAS remote pilots) get an FAA Tracking Number by creating an Integrated Airman Certification and Rating Application profile prior to registering for a knowledge test.

Industry Challenges

Despite the optimistic market projections, the UAS industry is not without challenges. Some of these challenges include uncertainty relating to regulations, changes in technology (particularly battery limitations, and limitations on the processing of raw data), a slow-moving waiver and rulemaking process under Part 107, remaining regulatory restrictions on UAS operations (such as Beyond Visual Line of Sight operations and full autonomy) which are seen as crippling, and concerns about rogue drone operations, as well as threats to cybersecurity and privacy rights.

Chinese-Made UAS Concerns

In October of 2019, the U.S. Department of the Interior, as part of its drone program review, issued an <u>order</u> to ground all Chinese-made drones or drones that include Chinese-made parts. This came as a particular blow to Chinese UAS manufacturer and market leader DJI, especially in the wake of its effort to build a "government edition" UAS in the U.S. This move builds on the U.S. government's growing concerns about the possibility of espionage and theft of classified and confidential information, unauthorized surveillance, as well as the deployment of potentially unsafe and easily hackable systems.

Shortly before the Department of the Interior order, the American Security Drone Act of 2019 was unanimously passed by the Senate Homeland Security and Governmental Affairs Committee (and currently awaits Senate vote and approval). The American Security Drone Act includes a ban on (i) Chinese drones for local, state, and federal agencies, and (ii) Chinese drone components.



Privacy and Cybersecurity Concerns

2019 and 2020 saw a significant increase in activity related to UAS and privacy and data security concerns. Examples include:

- In April 2020, the Inspector General for the Department of Transportation issued a <u>report</u> finding that the FAA does not adequately protect the personally identifiable information that it collects and stores through its systems.
- In 2019, the American Law Institute's Fourth Restatement of Property drafters created a
 trespass action called "Trespass by Overflight" addressing concerns of landowners about
 UAS flyovers over their property.
- In 2019, The Uniform Law Commission (ULC) drafted a <u>Uniform Tort Law Related</u> to <u>Drones Act</u>, which is a proposed law that considers whether a UAS is operated "in



the airspace over the land possessor's real property and causes substantial interference with the use and enjoyment of the property." Significant public reaction led the ULC to suspend activities on the proposed law.

In February 2020, the ABA adopted Resolution 111, calling for federal, state, local, territorial, and tribal governments to protect real property interests "with respect to any statute, ordinance, regulation, administrative rule, order, or guidance pertaining to the development and usage of unmanned aircraft systems over private property."

In the absence of specific federal binding laws on these issues, we are left with the National Telecommunications and Information Administration best practices issued in 2016, which outline recommendations for notice of UAS operations, consent for UAS overflights, and other privacy and cybersecurity measures.

Voluntary Best Practices for UAS Privacy, Transparency, and Accountability

Consensus, Stakeholder-Drafted Best Practices Created in the NTIA-Convened Multistakeholder Process

May 18, 2016