Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

Updated September 3, 2020

Protecting Against Rogue Drones

Rules for Unmanned Aircraft

As of September 2020, the Federal Aviation Administration (FAA) had registered about 1.7 million unmanned aircraft systems (UAS), often referred to as drones. More than 70% are operated by recreational users. FAA estimates that by 2024, about 2.3 million UAS, including 1.5 million recreational drones and model aircraft and about 800,000 commercial UAS, will be registered to fly in U.S. airspace. As the UAS market expands, there may be an increasing risk that rogue drones that either fail to obey safety rules or are operated for nefarious purposes could threaten manned aircraft operations, airports, critical infrastructure facilities, and high-profile events. These concerns have prompted Congress to examine options for detecting and interdicting drones.

The FAA Modernization and Reform Act of 2012 (P.L. 112-95) mandated that FAA develop a plan to integrate UAS into the national airspace and promulgate regulations allowing certain commercial drone operations. In 2016, FAA issued regulations (14 C.F.R. Part 107) allowing routine operations of commercial UAS weighing less than 55 pounds so long as they are conducted during daylight hours, in good visibility, and at low altitude, provided the drones remain within the operator's visual line of sight and away from airports and manned aircraft. FAA may grant waivers to these restrictions on a case-by-case basis.

UAS flown strictly for noncommercial purposes, including recreational drones and radio-controlled model aircraft that can sometimes be much larger than the 55-pound limit for commercial UAS, were exempted from these rules and, instead, operate under safety guidelines set by recreational user groups. Like commercial operators, recreational users must register with FAA and may do so through an online registration system. The FAA Reauthorization Act of 2018 (P.L. 115-254) imposed additional requirements for hobbyists, limiting recreational drone flights to altitudes below 400 feet and mandating testing to assess operators' knowledge of airspace and safety regulations. FAA is in the process of implementing these testing requirements.

Potential Threats from UAS

These requirements that recreational drones remain at low altitudes and that operators learn safety rules were imposed following close calls and collisions with manned aircraft. Between 2016 and 2019, airline pilots reported, on average, more than 100 drone sightings per month to FAA, and social media have transmitted photos and videos taken by drones in close proximity to airports and passenger airliners. In September 2017, a hobby drone launched from a park in Brooklyn, New York, was intentionally flown beyond its operator's line of sight and collided with a U.S. Army Black Hawk helicopter patrolling a temporary no-fly zone around New York City. The helicopter landed safely, but the incident damaged the main rotor assembly, where fragments of the drone were found. The following month, a drone struck a chartered turboprop near Quebec City, Canada. That aircraft also was damaged but managed to land safely. According to National Transportation Safety Board data, there have been three confirmed collisions between drones and manned aircraft in the United States so far, and a similar number of manned aircraft have been damaged from incidents that plausibly involved UAS. FAA-sponsored research has found that collisions with drones weighing eight pounds or less can cause more structural damage than collisions with birds of similar weight. Experts fear that a collision between a small drone and a manned aircraft, or a drone being ingested into a jet engine, could be catastrophic.

Airport officials have treated drone threats with considerable caution. In December 2018, hundreds of flights at London's Gatwick airport were canceled over a three-day period after multiple drone sightings near the runway. Three weeks later, London's Heathrow airport was also briefly shut down due to a drone sighting, as was Newark-Liberty Airport in New Jersey in January 2019.

In addition to careless and reckless drone operations, homeland security and law enforcement agencies have uncovered incidents involving drones transporting illegal drugs across U.S. borders, dropping contraband into prison yards, and conducting industrial espionage. The Federal Bureau of Investigation (FBI) has warned of an escalating threat that terrorists and criminal organizations might launch domestic drone attacks on critical infrastructure facilities, landmarks, and high-profile mass gatherings, citing the use of reconnaissance and weaponized drones by insurgents in Afghanistan, Iraq, and Syria. In 2011, the FBI thwarted a terrorist plot to attack the Pentagon and the U.S. Capitol with explosives-laden model aircraft.

Controlling the Threat

FAA has encouraged UAS manufacturers to incorporate technology that could reduce the risk of rogue operations, such as built-in "geofencing" capabilities that prevent the drone from entering airspace that is off-limits to UAS. These systems, however, may not have current information, as they usually require the operator to keep airspace data up to date. FAA has also developed the Low Altitude Authorization and Notification Capability (LAANC) system to disseminate information regarding low-altitude controlled airspace in the vicinity of airports and to grant airspace access to certain commercial UAS operations on a case-by-case basis. In the future, FAA envisions that these resources will be integrated with "Remote Identification" capabilities to monitor compliance.

Remote Identification

The FAA Extension, Safety, and Security Act of 2016 (P.L. 114-190) required FAA to develop standards for the remote

identification of UAS and to coordinate with the National Aeronautics and Space Administration to develop technologies for managing UAS traffic. P.L. 115-254 authorized FAA to require remote identification for all drones, including recreational drones. FAA recently published a proposed rule that would require all UAS to transmit location and identification information. This requirement could necessitate extensive retrofitting or replacement of existing drones. Educating operators about compliance and enforcing remote identification requirements on older UAS could pose significant challenges to effective implementation.

Detection and Interdiction Technologies

Given the potential threat posed by rogue drones, there is considerable interest in deploying counter-UAS systems that can detect and interdict unauthorized unmanned aircraft. Commercial airports have a particular interest in drone detection technologies because they have a regulatory responsibility to inform airlines about airfield conditions that may adversely affect the safety of flight operations.

U.S. airports and state and local law enforcement agencies that protect them do not have specific legal authority to deploy counter-UAS technologies. FAA has warned that these technologies pose potential risks to manned aircraft and to surveillance, navigation, and communications signals used by air traffic control. Moreover, a multiagency legal advisory published in August 2020 cautioned nonfederal public and private entities that UAS detection technologies could run afoul of a wide gamut of federal statutes and regulations pertaining to privacy and the use of radiofrequency spectrum, while systems designed to interdict drones could violate federal laws and regulations regarding aviation safety and security and prohibitions against jamming or interfering with radio communications or impeding navigation through the airspace.

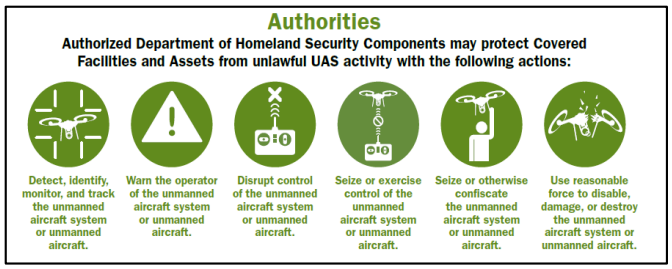
While interdicting drones near airports is particularly difficult because of potential safety implications, protecting other facilities and high-profile events may depend on effective interdiction capabilities to neutralize drone threats. Available interdiction systems rely primarily on jamming devices that disrupt flight control signals between the drone and the controller, but these may not be able to stop fully autonomous drones and may interfere with air navigation signals and other radio transmissions. Other techniques involve systems that transmit signals to spoof drone guidance systems or take over control of the drone, capture drones in nets, or disable or destroy drones with lasers. These technologies are nascent, and may not be as effective as some manufacturers and advocates may assert. The absence of standards raises questions about performance and safety of interdiction technologies, especially near airports where radiofrequency jamming could impact flight operations, and mass gatherings where interdiction could pose a hazard to people on the ground.

Legal Restrictions and Authorities

Certain civil and criminal penalties have been enacted to punish violations involving UAS, and, in some instances, unlawful drone flights have been prosecuted. FAA relies extensively on assistance from federal, state, and local public safety and law enforcement agencies to investigate drone-related incidents. P.L. 114-190 directed FAA to establish procedures for imposing unmanned aircraft restrictions around critical infrastructure and other sensitive "fixed site" facilities, including amusement parks, and to set up a pilot program to detect unmanned aircraft near airports. P.L. 115-254 expanded the list of eligible fixed-site facility types and also included language explicitly prohibiting operators from affixing dangerous weapons to unmanned aircraft.

P.L. 115-254 established criminal penalties for operators of drones that interfere with firefighting, law enforcement, or other emergency response to wildfires. It directed the Department of Transportation to work with the Department of Defense to streamline the deployment of counter-UAS technologies and required FAA to establish a pilot program to assess the use of remote detection and identification technologies to conduct safety oversight and carry out enforcement actions against drone operators. P.L. 115-254 also authorized the Department of Justice and the Department of Homeland Security, including the Coast Guard, to interdict hostile or unauthorized drones in certain instances to protect critical infrastructure and designated high-profile events and mass gatherings (see **Figure 1**). The language parallels authorities granted to the Department of Defense and the Department of Energy in the National Defense Authorization Act for Fiscal Year 2017 (P.L. 114-328) to protect certain military and nuclear facilities in the United States from drones.

Figure 1. Department of Homeland Security Counter-UAS Authorities



Source: Department of Homeland Security.

While these federal agencies have been granted limited authority to deploy counter-UAS systems, FAA has issued stern warnings to event organizers and local authorities that have deployed such systems of their own accord to protect high-profile events. Unauthorized use of counter-drone technologies is potentially in violation of both FAA and Federal Communications Commission regulations, as well as federal aviation laws. The National Football League, which has teamed with FAA to educate fans about drone restrictions, has urged Congress to extend counter-UAS authorities to state and local law enforcement in order to enforce temporary flight restrictions around large sporting events. In considering such requests, Congress faces complex trade-offs in weighing the inherent risks of expanding counter-UAS authorities against the level of threat posed by rogue drones.

Bart Elias, Specialist in Aviation Policy

IF11550

Disclaimer