New Drone Regulations Will Require Cellular IoT Connectivity and GPS

FEBRUARY 14, 2020 / WRITTEN BY DERRICK WOLBERT

New drone regulations are coming.

As drone traffic increases exponentially and commercial drone fleets seek permission to take to the air, the Federal Aviation Administration (FAA) wants to use remote ID technology to track drones as they fly, as it does airplanes and helicopters. To that end, it proposes a new rule that will require most drones in U.S. airspace to carry technology that allows them to be tracked at all times.

It's part of a larger effort, as the FAA and the Unmanned Aircraft Systems (UAS) industry move toward creating an Unmanned Aircraft System Traffic Management that is separate from but complementary to the FAA's air traffic management system.

Currently, there are 1.5 million drones registered in the United States. With companies such as Amazon, Uber, UPS, and Google parent company Alphabet all preparing and testing drone delivery systems, those numbers are increasing fast.

And yet as drone traffic increases, laws and regulations have been slow to follow. Reports of near midair collisions, especially in major metropolitan areas, have become frequent. For more than a year, there was nearly one a day reported in the greater New York City area. A Cessna aircraft in San Diego once returned to the airport with quadcopter parts sticking out of its wing.

The proposed drone regulation, which has been in the works for several years, is the next in a series of steps taken by the FAA and the UAS industry to safely integrate the vast and growing number of drones into the nation's airspace.

Since 2015, anyone operating a drone weighing more than half a pound has been required to submit their name, email address, and home address to the FAA. But that does not allow airports or other officials to identify a drone's owner quickly and on-the-spot.

"Remote ID technologies will enhance safety and security by allowing the FAA, law enforcement, and federal security agencies to identify drones flying in their jurisdiction," said U.S. Transportation Secretary Elaine L. Chao.

Drone regulation in plain English

What will the new drone regulations mean, exactly? They say that almost every drone in flight, with very few exceptions, will have to emit a signal that indicates both where it is located, derived from a position source such as GPS, and its operator's identity. This remote ID technology will allow the FAA and public safety officials to identify them and track their location at all times.

The rule would apply to all drones required to register with the FAA, meaning those that weigh more than .55 pounds. It also applies to anyone who operates a foreign civil drone within the U.S. The proposed rule states that the FAA expects drones to have such remote ID within three years.

ID and tracking requirements do not apply to Tier 0 drones, which are those operating within visual line of sight and not designed to be able to fly beyond 400 feet of a remote pilot.

The new drone regulation calls for two different types of Remote ID depending on the drone – direct broadcast and network publishing.

METHOD 1: DIRECT BROADCAST AND HOW IT WORKS

Direct broadcast is a type of local broadcast where identifying data is transmitted by the drone in one direction only. There is no specific recipient or destination—anyone within the broadcast range can receive the data. No special network is necessary, and any public safety officials with an appropriate receiver can attain information transmitted from a drone by direct broadcast.

WHAT TYPES OF DRONES WILL REQUIRE DIRECT BROADCAST?

Direct broadcast regulations pertain to drones that are within what the FAA calls Tier 1. Those are drones that fly beyond 400 feet of their remote pilot, beyond visual line of sight, and which do not qualify as Tier 0 or Tier 2 or 3 (see below). Most drones described in Part 107 are Tier 1.

Tier 1 UAS must either broadcast their ID and tracking information locally, or, if a network is available, publishing to an FAA-approved internet-based database (as described in Method 2) also fulfills the requirement.

PROS AND CONS

Because there is no need for "repeater" infrastructure, this is a dependable technology. It is especially useful around sensitive areas such as airports,

defense installations, critical infrastructure, and remote locations where there is no network coverage.

Not all public safety officials, though, have receivers equipped to pick up all possible direct broadcast technologies. Therefore, the Aviation Rulemaking Committee (ARC) recommends the FAA adopt an industry standard for such data transmission, so transmittal equipment and safety receivers are compatible.

METHOD 2: NETWORK PUBLISHING AND HOW IT WORKS

The FAA's Method 2 requires that ID and tracking data be transmitted via networked cellular, such as LTE, satellite, or software-based flight notification with telemetry. It can also broadcast to a networked ground station. Whatever the technology, data transmits to an FAA-approved internet-based database where Air Traffic Control and public safety officers can access it as needed to obtain identification and tracking information for a specific UAS.

WHAT TYPES OF DRONES FALL UNDER NETWORK PUBLISHING?

Network publishing applies to Tier 2 drones, which generally means drones that are operating beyond their pilots' visual line of sight, above Part 107 maximum altitudes, or flying over unprotected persons.

WHO CAN ACCESS THE DATA

The FAA, law enforcement, and other public safety officials will be able to access direct broadcast data.

"As a pilot, my eye is always on safety first," said FAA Administrator Steve

Dickson in a statement. "Safety is a joint responsibility between government, pilots, the drone community, the general public, and many others who make our nation so creative and innovative."

Law enforcement having better access to data from UAS that could post a security threat means that corporations working on adding unmanned aircraft to their delivery fleets, such as Amazon, Alphabet, and others, will be a step closer to their goals.

The UPS subsidiary Flight Forward, for example, recently received federal approval to operate a fleet of drones and plans to start by delivering packages to hospital campuses. It's a milestone approval, the first time the FAA has given such broad permission for a company to operate a UAS fleet as an airline. The drones will be allowed to fly at night, out of the operator's sight, and carry cargo weighing more than 55 pounds.

PROS AND CONS

With network publishing, there is no need for compatible technologies between the sender and receiver. It's only necessary that the UAS's transmitting hardware can send data to the internet-based service and that the client can connect to that service as well.

This method could deploy fairly quickly by taking advantage of existing technologies, can help companies increase and improve their fleet operations, and will help public safety officials conduct drone investigations. It means the FAA can monitor flying drones for air traffic safety and potential terrorism threats.

There are, though, also privacy considerations. Tracking information would need to be protected and the use and dissemination of that data governed by restrictive use conditions.

Some are concerned about the cost of this technology for drone pilots and operators. Others note that the requirements are not practical for drones that operate where there is no cellular or other way of connecting to the internet.

Keep a Look Out (and Up) for Final Rules

The FAA will develop its final rule on these drone regulations after hearing public comments on its Notice of Proposed Rulemaking for Remote Identification (Remote ID) of UAS.

Explore Hologram Inflight

Learn More

Contact Sales

GET CONNECTED

Cellular Data

Dashboard

IoT SIM Card

Hologram Nova

See Supported Hardware

RESOURCES