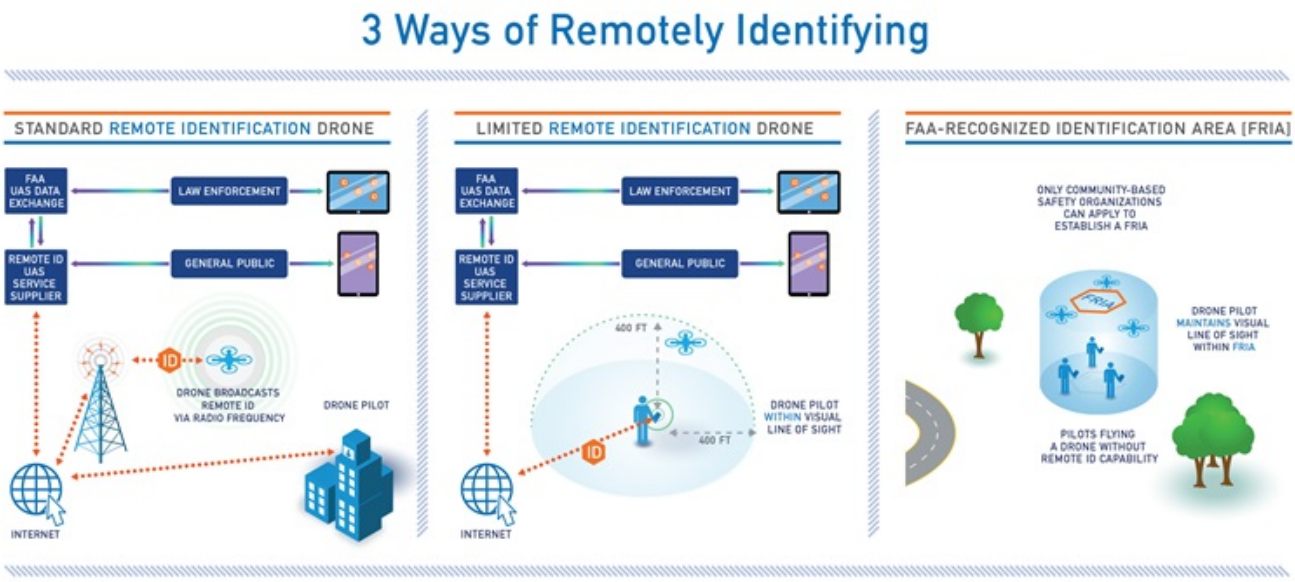
FAA gets early earful on drone ID

FAA GETS EARLY EARFUL ON DRONE ID

CONCERNS ABOUT PRIVACY, COST

January 9, 2020 By Jim Moore

The FAA published on December 31 a detailed and long-awaited proposal to create a system to track and manage every flight by millions of drones, and many stakeholders responded swiftly: The online document logged more than 100,000 views and 1,000 comments within three days of its publication.



The FAA has proposed three ways to fly a drone once remote identification begins. The rulemaking proposal is subject to coments for 60 days, and further changes are possible before a final rule is published. Graphic courtesy of the FAA.

Initial feedback on the drone identification and tracking **notice of proposed rulemaking** was decidedly negative. Many if not most of the first 1,000 comments voiced concern about remote pilot privacy, new limitations on where and how drones can be flown, and financial costs both known and unknown. The FAA set a March 2 deadline for public comment.

AOPA Director of Regulatory Affairs Christopher Cooper said the association's analysis of this notice of proposed rulemaking is ongoing, and the association will weigh in on specifics once the details of what the FAA has put forward are fully understood. Cooper said feedback from members will also inform the association's positions, and more time may be needed to allow all stakeholders to fully digest and understand FAR Part 89, the new regulation the FAA seeks to create while amending others. (AOPA invites those who submit comments to copy the association **via this email address** when submitting.)

"We plan to carefully review this very important proposed rule to determine all of the potential impacts to both our manned and unmanned members," Cooper said. "Meanwhile, at first glance, this proposed rule is a step in the right direction toward further integrating UAS safely into the National Airspace System, while also providing tools to protect the public from nefarious and reckless operators. However, you can expect we will have much more to say in the weeks ahead on how the FAA can improve this proposed rule."

The short version

- The FAA seeks to require all drones larger than 0.55 pounds (250 grams) to be individually registered and to broadcast identifying information in order to fly in most locations;
- The FAA has made clear that Remote Identification (RID) is a prerequisite for a long list of advanced operations being allowed without waivers, including routine drone flights at night, over people, and beyond the remote pilot's line of sight;
- A system to track and remotely identify drones is the key to creating a new unmanned aircraft traffic management (UTM) system, and the details of exactly how this new system is implemented remain to be decided. The FAA is leaving much of this to private industry, creating performance standards without dictating how they are achieved;
- Nothing is going to change soon: The proposed rulemaking calls for various requirements to be phased in over three years, and the details, including that timing, can still be changed prior to publishing of the final rule;
- With very few exceptions, the FAA proposes that virtually every unmanned aircraft in the airspace (at any altitude) must be quickly identifiable by other users, and law enforcement, which will have access to the pilot's location information as well as the aircraft's location. Those unable or unwilling to participate, no matter what credentials the operator may hold, will be relegated to flying only in federally approved, designated areas called FAA-recognized identification areas (FRIA). (The FAA expects existing locations designated for flying traditional radio-controlled model aircraft will be among the first FRIAs approved.)

Bad actors drove the rule

The FAA **announced** that RID was coming in March 2017, and assembled a committee of stakeholders (including AOPA) to provide recommendations on how best to minimize the downsides of drones and maximize the opportunities—delivery of food and medicine, infrastructure inspection at a fraction of the cost of other

methods, disaster response, and scores of others. The aviation rulemaking committee **report** was published in December 2017, though some of the 74 members submitted dissenting views on some key points.

A DJI Phantom 4 Pro Obsidian Edition is flown at night (with LED strobe lights attached to enhance visibility as required by FAA waiver). Photo by Jim Moore.

Meanwhile, drones grew in number and in capability, and the dark side of the technology captured the attention of law enforcement and the public, in the form of smuggling and other criminal activity. A growing body of evidence shows that the technology is equally adept at fulfilling nefarious intentions as it is at achieving humanitarian good and economic efficiency.

For all the demonstrable good that drones have done, bad actors have been intent on ruining it for everybody: Among the examples referenced by the FAA in the proposal published December 31, a drone **dropped Nazi propaganda** leaflets outside a concert in California in May (the drone was flown illegally over people).

Arguably worse than that, drone sightings have prompted flight cancellations and shut down entire airports, including **Heathrow Airport in London** at the height of the holiday travel season. The FAA noted similar disruptions at airports across the United States in recent years.

Some hazards created by bad behavior remain unseen, and unknown until wreckage or documentation emerges. Examples of this include an intentional close encounter between a small drone and a passenger jet **approaching Las Vegas** in 2018 that prompted the FAA to investigate after a video was published online.

More often, drones transit restricted airspace without leaving an identifiable trace. Small unmanned aircraft have buzzed Major League Baseball and National Football League games several times (that are known). While those flights proved largely benign, notwithstanding a crash or two in a stadium or arena that put spectators at risk of injury, the FAA **noted in the remote identification rulemaking proposal** that terrorists have been practicing overseas:

> **"Recent reports in the news including the Islamic State of Iraq and Ash-Sham's modifications of commercial UAS, the assassination attempt of Nicolás Maduro in Venezuela, a foiled plot in the United Kingdom to fly an unmanned aircraft into an airliner, and a bomb-laden unmanned aircraft flown by Huthi forces and detonated over a military parade in Yemen illustrate the ways in which UAS may be used to threaten life, critical infrastructure, and national security. Remote identification of UAS would enable national security agencies and law enforcement to quickly identify potential threats and act to prevent such incidents."**

Drones have also put the safety of firefighters and law enforcement flying manned aircraft at risk. They have disrupted rescue missions and shut down aerial operations at major wildfires. The FAA noted that the cost of

enforcing the rules nationwide is prohibitive, and one of the key functions of remote identification is to reduce the agency's workload while **increasing compliance**:

> **"Although Federal, State, and local law enforcement agencies are responsible for the investigation and prosecution of illegal activities, the FAA retains the regulatory and civil enforcement authority and oversight over aviation activities that create hazards and pose threats to the safety of flight in air commerce. Both safety and security enforcement are extremely difficult absent a remote identification requirement that enables the prompt and accurate identification of UAS and operators."**

Days before the long-awaited rulemaking proposal was published, citizens and law enforcement began reporting mysterious drone sightings in Colorado and Nebraska. Drones have been reported hovering over houses, or flying in formation with other drones, and the ongoing mystery over who is behind these flights has caused consternation as the motives and intent of the operators remain unknown. One Colorado newspaper **has reported** that the drones might be flying on a secret U.S. Air Force mission to test the security of nuclear missile installations, though the FAA has said the reason for the reported flights remains unknown, and the agency is investigating.

FAA officials have told the media that the onset of this particular mystery days before the remote identification plan was spelled out is a coincidence.

The FAA has made no secret of the fact that the agency will not abide careless, reckless, or illegal behavior by drone pilots, and without the ability to remotely track and identify drones and their operators in real time, there is zero chance the agency will supply the big carrot: a more **permissive approach** to unmanned aircraft that allows package delivery and other use cases that are practical only when the drone is flown beyond line of sight.

Costs and limitations

Unmanned aircraft that are able to broadcast remote identification information via radio frequency *and* connect via the internet (when internet service is available) to a UAS Service Supplier (USS), a private party approved by the FAA, will be able to fly under "standard remote identification" rules. The FAA believes, based on information provided by manufacturers, that most drones already meet both of the requirements (internet connection capability and radio frequency broadcast capability) for standard remote identification, or can be enabled to meet the requirements with a software update.

The FAA **estimated that 93 percent** of the drones currently registered under Part 107 already comply with the standard remote identification requirements, or can be retrofitted to do so with a software update. The percentage of drones flown strictly for recreation that already meet the requirements or can do so with a software update was more difficult to calculate, since a single recreational pilot can register any number of aircraft under a single number. That is going to change under the proposed changes to drone registration rules, with every drone required to register individually (the current fee is $5 per aircraft).

Unmanned aircraft that are unable to broadcast identification information may still be flown outside of an FAA designated area (FRIA), but these "limited remote identification" UAS must be able to connect to the internet, must be connected to a USS during flight, and must be programmed to remain within 400 feet of the ground control station at all times.

AOPA file photo.

Unlike standard remote identification-capable drones, those flown under the **limited remote identification provisions** would not have the option of flying in areas where there is no available internet connection.

The benefits of flying beyond visual line of sight (BVLOS) without a waiver, and other advanced operations the FAA expects to streamline once remote identification is in place, will be reserved for standard remote identification drones.

While the FAA made no attempt to forecast what USS services required for remote identification compliance will cost consumers, the agency did do some math on the gas money required for recreational pilots to travel from their home to the nearest FRIA, where unmanned aircraft can fly within defined boundaries free of RID requirements. The agency compared hobbyist registrations to locations of current Academy of Model Aeronautics flying fields, by zip code:

"The **zip code analysis** indicates a person operating UAS that are not standard remote identification UAS would be required to travel an average of 16 miles one-way to the nearest FAA-recognized identification area," the proposed rule states. Based on assumptions including 52 visits to that "identification area" each year, and the number of non-RID drones currently operated by hobbyists, the FAA estimated that this group will spend $2.28 billion on gas in the first decade of remote identification, starting in the fourth year once all requirements are in effect.

There will be other costs for those who wish to fly where they choose. In addition to requiring registration of all drones flown outside of a FRIA, a new marketplace will be created for USS, and it's not clear what those services will cost.

The FAA did not make the law enforcement community entirely happy by allowing three years for the RID rules to take full effect, and presented that as a concession to owners of unmanned aircraft that cannot meet the identification requirements without hardware changes:

> **The FAA analyzed the costs of allowing up to three years for owners/operators to be in compliance and found this alternative minimizes costs to owners/operators since on average the affected existing fleet of UAS could be replaced at the end of useful life (three years). In addition, this alternative is more likely to reduce uncertainty of adverse impacts to producers with inventories of UAS produced before the compliance date that would likely not meet the remote**

> identification provisions of this proposal. Given the average three-year UAS lifespan, the three-year operational compliance period would likely assist producers in depleting existing non-compliant inventories with reduced impact compared to the proposed one-year compliance period.

Counter-drone counter arguments

Some of the early objections appear to be based on misunderstanding of the actual requirements. To dispense with one of these: UAS operating "standard" remote identification (the drone broadcasts the RID information electronically, from the aircraft, and/or via internet connection to an FAA-designated UAS service provider) will, in fact, be able to operate legally in areas without internet service.

As the **FAA puts it**:

> A standard remote identification UAS would be required to broadcast and transmit the remote identification message elements from takeoff to landing. If the internet is available at takeoff, the standard remote identification UAS would have to connect to the internet and transmit the message elements through that internet connection to a Remote ID USS and would also be required to broadcast the message elements directly from the unmanned aircraft. If the internet is unavailable at takeoff, the standard remote identification UAS would only be required to broadcast the message elements directly from the unmanned aircraft.

The proposed requirements will not effectively ground drones outside of cellular coverage areas, as some have suggested. The directive to "land as soon as practicable" applies only to the in-flight loss of **both** the unmanned aircraft system's internet connection **and** a loss of RID broadcast capability by the unmanned aircraft. The FAA will require drone manufacturers to enable the remote pilot to monitor both internet connectivity and RID broadcast functionality (if applicable, in the case of standard RID) throughout the flight.

Remote pilot privacy is another area of concern raised by many commenters. With every drone subject to Part 89 (the proposed new RID regulation) required to transmit a unique identification number, GPS location, barometric altitudes of both drone and pilot (standard category only), and an emergency code if a malfunction ensues when flying anywhere outside of a FRIA, many remote pilots voiced apprehension (even outrage) that their location will become public knowledge.

That may or may not be the case, depending on how remote identification is implemented. DJI, the manufacturer of nearly 80 percent of drones flown under Part 107 and a significant portion of the recreation-only fleet as well, **announced in November** that it was developing a mobile application that will allow anyone with a mobile device to collect the remote identification data being broadcast by DJI drones (a feature that remote pilots can currently disable).

The FAA proposes that private industry will ultimately decide how the data is handled, and while law enforcement will have access to all of the available information, individual USS will serve as conduits for distributing customer information at the network level, and "the FAA anticipates that there will be some Remote ID USS available to the general public and that others will be private."

Users may have to pay more for that privacy, as the FAA noted:

> For example, if Company ABC sets up a private Remote ID USS to provide remote identification services exclusively to its fleet of UAS, then the private Remote ID USS would only be available to the UAS operators of Company ABC. In comparison, if Company XYZ sets up a Remote ID USS that can be accessed by the general public for remote identification services, then Company XYZ's Remote ID USS would be considered available to all operators of UAS flying in the airspace of the United States, irrespective of whether that access requires a monetary cost. The FAA is not proposing to establish specific requirements regarding Remote ID USS business models, (e.g., charging fees, requiring user agreements, and requiring information from Remote ID USS users). The FAA believes that operators will choose a Remote ID USS that best meets their operational needs.

It remains to be seen what USS will cost for individual users, public or private. The FAA expects many of the current providers of Low Altitude Authorization and Notification Capability, which allows Part 107-compliant flights in certain controlled airspace, will seek USS designation, though there are likely to be others.

AOPA continues to evaluate the FAA cost estimates and technical details of the notice of proposed rulemaking. Given its scope and significant impacts on all airspace users, AOPA may ask the FAA to extend the comment period beyond the current March 2 deadline, Cooper said.

Many hobbyists, including traditional radio control model aircraft enthusiasts, were among the first to decry the FAA approach to RID, arguing that the rules should not be applied to aircraft flown without automated stabilization and first-person view. Others seek a carve-out for racing drones and other FPV models, and worry that RID will devastate hobby flying.

Photo by Bob Knill.

Jim Moore

Editor-Web

Editor-Web Jim Moore joined AOPA in 2011 and is an instrument-rated private pilot, as well as a certificated remote pilot, who enjoys competition aerobatics and flying drones.

GO TO JIM MOORE'S PROFILE >

Topics: Advocacy, Unmanned Aircraft