Alliance for Drone Innovation

ADI's Remote ID NPRM Guide: Submitting Comments on the FAA's Proposal

The mission of the Alliance for Drone Innovation (ADI) is to support the amazing drone innovation that is here today, generated by those who design, build, and use drones in their personal and professional lives. Our members include first responders, drone racing leagues, model aircraft manufacturers, commercial drone service providers, and software developers — all who have active and growing businesses today that will be impacted by the Federal Aviation Administration's recent Notice of Proposed Rulemaking (NPRM) for Remote Identification (Remote ID).

The Alliance for Drone Innovation supports the FAA's initiative to implement Remote ID for drones, but is concerned about the redundant, overly strict, and costly approach the FAA proposed in the NPRM. As ADI prepares formal comments to submit to the FAA by its March 2, 2020 deadline, we wanted to highlight some of our top concerns, which anyone who is interested in drone innovation may also wish to consider as they prepare their own comments.

Comments should be submitted at the official Regulations.gov website prior to the March 2 deadline: https://www.regulations.gov/comment?D=FAA-2019-1100-0001

ADI encourages everyone in the drone community to take this limited but crucial opportunity to comment thoughtfully on the FAA proposal, focusing on the aspects that impact you specifically. If you share our concerns, use them in your own comments, but we suggest taking the time to draft your own perspective, explaining the proposal's impact on you in your own words.

Requiring Broadcast and Network Methods is Too Burdensome

Rationale — The main method FAA proposes for remote ID requires every drone both to broadcast its ID with a radio signal and send it through an internet-based service. There are only a few very limited exceptions to this (such as if the internet is *always* unavailable for the life of the drone in all locations in which it is ever going to be used, which is not likely). So practically speaking, the FAA proposal requires every drone innovator to use and pay for a remote ID service, as well as use a radio broadcast transmitter. This approach is unreasonably burdensome and costly to drone innovators, for several main reasons:

1. Many drones in use today, including but not limited to more traditional model airplanes and helicopters, and brief-flying racing drones, do not have a way to connect to the internet. The FAA seems to underestimate the broad range of UAS technologies in use today.

2. The network service is anticipated to involve paying monthly fees to a private service company. We believe there is no way to know what the subscription fee costs will be. FAA estimates $2.50 per month, but that is based on LAANC, which is a much simpler system that is still in its "startup" period with many companies

offering the service for free, or below their own costs, in the hopes of establishing themselves. We are concerned that true long-term costs, after the initial startup period, will be higher, and that maintaining accounts, passwords and payment information will add extra steps that discourage compliance.

Rationale — If the FAA mandates a more complex or costly way to achieve the same goal in some locations, it should explain and justify that decision, which it has not done. FAA has also not adequately explained why drones need to comply with Remote ID two different ways, imposing two sets of costs.

- **Recommended Solution —** To keep costs low, and thereby enhance the rate of compliance across the broadest set of innovators, the Broadcast method of Remote ID should be allowed as a way to comply with Remote ID, all on its own. This avoids monthly subscription service costs, will be easier for many people to use, and works everywhere regardless of internet connectivity. Network remote ID has its own potential benefits, including additional ways to anonymize flights, links to additional services, and a pathway to advanced operations in years to come. So, drone operators should have a choice between doing either Network Remote ID or Broadcast Remote ID. They should not have to do both.

The Exceptions Are Too Limited

Rationale — The proposal to only allow Community Based Organizations (CBOs) to propose FAA Recognized Identification Areas (FRIAs) is too limiting. There is also no explanation of the FAA's criteria or process for designating a CBO. The only CBO the FAA seems to refer to, the Academy of Model Aeronautics (AMA), consists of an affiliated group of private club sites that have their own annual membership fees, capacity constraints, and policies that may not welcome all types of technologies.

Rationale — It is not appropriate for the FAA to constrain the use of technology to locations that are controlled by a closed private membership organization. Because of the broad range of UAS that already exist, and that will continue to be developed, places to fly non-compliant equipment will remain essential to the cause of drone innovation.

- **Recommended Solution —** The FAA should allow schools, teachers/professors, universities, cities, states, trade associations, and other types of organizations, individuals, and groups, to apply for a FRIA as well. The FAA should also allow applications for temporary FRIAs, since they might be useful for events and competitions, and they should be more easily granted than permanent locations.

Rationale — There should not be a 12-month cut-off deadline for applications for FRIAs. This is too limiting and precludes the identification of other locations where Remote ID requirements are not needed, or locations proposed by new CBOs that are formed in the future. It is not plausible that the need for such locations will be substantially diminished in the near future, if ever.

- **Recommended Solution —** FAA should allow any non-compliant aircraft to fly in a FRIA, rather than limiting those locations to "amateur built" UAS. The definition of "amateur built" is ambiguous and too restrictive, contemplating only that people who "fabricate" most of their UAS will qualify. Many products on the market are sold as kits, or are customized by drone innovators, but these would seem not to be covered. Because a FRIA substitutes for the identification of any UAS operated there, it should not matter what type of UAS is being flown there.

The Limited Category Should Be Reformed

Rationale — The 2017 Aviation Rulemaking Committee (ARC) working group report recommended that drones that can only fly less than 400 feet from the operator should not require Remote ID at all. The NPRM requires such drones (which are placed in the "Limited" category) must identify, but may only use Network Remote ID, which is costly and will entirely preclude their use in rural areas. This does not make sense, in light of the lower risks and concerns with these low-performing drones.

- **Recommended Solution —** The FAA should either exempt such low-capability drones from the Remote ID requirements entirely, or create far easier means of compliance that do not require equipage on board the aircraft or ground control station. The FAA should also find a way to exempt drones that can fly only for a short time, which ensures they are flown close to their pilots, such as racing drones which the ARC report recommended be exempt.

Product Certification Approach, Placing Regulatory Responsibility Almost Entirely on the Technology, Is Too Burdensome

Rationale — Most FAA regulations require that pilots adhere to them, rather than be enforced through technological means. By creating an effective sales ban on drones that do not comply with Remote ID, as well as a flight-restriction function when Remote ID does not perform as expected, FAA is shifting the responsibility of compliance from pilots to manufacturers, and treating innovative products (with an impeccable safety record) as inherently dangerous, while also treating pilots as assumedly irresponsible.

Rationale — One substantial problem with this approach is that it regulates all drones, including those flown only indoors, such as in a warehouse, mine, school gym, or home. It also grounds drones owned by Americans who take them from the U.S. to overseas where there are no (or differing) Remote ID requirements. For example, while drone racing is an international sport, the FAA's proposal would require American competitors to have a separate drone to use outside the U.S. Because locations abroad would not have a Remote ID UAS Service Supplier (USS), a drone being flown outside the U.S. would be required by the FAA to prevent its own takeoff even though the flight is outside of FAA jurisdiction.

Rationale — The proposed product certification and auditing requirements are a serious burden on small and new producers. They also effectively preclude someone from using an add-on Remote ID module, building a customized kit, or retrofitting an older drone, because the resulting flight-ready UAS would have to be tested, certified, audited, and its assembler's

certificate accepted by the FAA. That is too large a burden on individual builders, and small companies. These requirements will also delay the release of products into the market as developers await the backlog at FAA, would create serious barriers to market entry, and would penalize small start-up companies during a period in which the U.S. government otherwise is trying to encourage the domestic development and production of drone technologies.

- **Recommended Solution —** To address both the dilemma of indoor and international operations, and the burden of compliance, the FAA should: (1) require *drone pilots* to ensure compliance with Remote ID at the time of operation; and (2) require manufacturers to *label* their products as being capable of complying (or not). Because it is easy for anyone to check a product's compliance during use simply by checking that it appears on a receiving device or service, the FAA should randomly test products on the market for compliance. There is no need for costly and disruptive audits or FAA facility visits. This recommended approach also preserves flexibility in emergency operations where the FAA's proposed self-disabling function risks impeding life-saving operations. The costs, burdens, and challenges of the FAA's product "ban" and certification approach outweigh the marginal benefits of heightened anticipated compliance.

Privacy and Due Process Require Additional Protection

Rationale — Privacy and fair enforcement are important to drone innovators. The FAA does not fully address privacy issues because of the mandate to establish a Remote ID USS service account, which allows providers to tie six months of operations to your identity. Any USS providing this service should be prevented from selling or using Remote ID data for other commercial purposes without the pilot's express consent.

Rationale — These no-use restrictions should be contained in the FAA's regulations, not just in future operating agreements, so that violations of those restrictions have real enforcement mechanisms. This is especially important given the FAA's observation that some LAANC providers are offering "free" service, suggesting that their customers' operational data is what they may hope to monetize somehow.

- **Recommended Solution —** The "session ID" alternative to using a drone serial number is a good way to help protect identity with respect to the public observation of remote ID information, but does not address the privacy issues associated with services providers who can aggregate their data and who will be in possession of identifying information (because a service account is needed for each user). It is not clear from the proposal what consequences would be imposed on a Remote ID supplier who shares private information or who has a data breach. It is not clear how law enforcement officials will access historic flight data and whether constitutional due process protections will be respected, requiring probable cause prior to accessing activity records. These issues need to be made clear before the proposal is finalized, so that drone innovators can comment on them.

Alliance for
Drone Innovation

Recreational Registration Should Remain $5 per person

Rationale — Charging more money contradicts the FAA's 2015 Registration Task Force recommendations, and is likely to lead to lower compliance, as well as a sense that the burden of complying is disproportionate to the benefit. Registration is the first step to compliance, and should be kept as inexpensive as possible.

- **Recommended Solution —** FAA should not charge $5 per aircraft for recreational UAS registration. Instead, to meet the FAA's goal of individually identifying all aircraft, people should be able to enter all their UAS serial numbers in their registration account, but without paying extra fees for each one.

The Implementation Timeline is Reasonable

Rationale — The FAA contemplates a three-year phased approach to implementation. Drone innovators need that time to understand the final requirements, implement performance-based standards, and design and produce their products by the time Remote ID is mandatory. It is likely, however, that an "either/or" approach to the network/broadcast methodology will facilitate early and rapid compliance sooner than a "both of the above" approach, because developers will be able to focus their resources and time on the single path to compliance that is most practical for their products and markets.

- **Recommended Solution —** Given the vast array of UAS technologies on the market and in development — as well as the uncertainty of what the Remote ID requirements will be once the FAA finalizes this proposal — the three-year phased implementation is reasonable and appropriate.

Drone Pilots Need Protection Against Harm

Rationale —There is substantial concern that providing control station location information will cause drone pilots to be targeted by people who are fearful of drones, leading to unpleasant and potentially dangerous encounters. On the other hand, this information, provided live, is very useful at facilitating law enforcement response and cooperative mitigation, as well as friendly conversations with the responsible pilot.

- **Recommended Solution —** The FAA should evaluate whether control station location is necessary to disclose to the public. Notably, creating systems that limit access to that information to specified authorities creates a far more complex and costly account management and credentialing challenge among remote ID service suppliers as well as broadcast solutions.

  At a minimum, the FAA should confirm, reinforce and publicize that interfering with the pilot of an aircraft is a crime, by expressly creating a UAS-specific provision in the federal regulations similar to existing provisions that prohibit interference with aircraft crewmembers. The FAA should penalize, and encourage the Department of Justice to prosecute, anyone who assaults a UAS pilot during any

stage of the flight operation. This policy should be as widely socialized as other drone safety and security messages published on FAA's media channels.

Additionally, the differing levels of concern about this issue — which will depend on the operational environment and other factors — further bolster the need for the Remote ID rule to allow *either* broadcast or network as a means of compliance. Having a variety of available compliance methods will result in a greater number of potential solutions to address this concern, allowing pilots to opt in to solutions that address what they care about most.

###