DJI's Recommendation for Remote-ID
Simpler, Easier and Much Less Costly

DJI wants governments to require Remote ID for drones, but the FAA has proposed a complex, expensive, and intrusive system that would make it harder to use drones in America, and that jeopardizes the success of the Remote ID initiative. Instead, we support a simpler, easier, and free version of Remote ID that doesn't need a cellular connection or a service subscription. Read on to discover why the future of drone innovation in America is at risk – and how you can make your voice heard between now and the FAA's March 2 deadline for submitting comments on the official government website.

Unfortunately, the FAA's vision of Remote ID released late last month is deeply flawed. The "Notice of Proposed Rulemaking" proposal would hurt people who have safely and successfully used drones across the country for years. It would hamper the adoption of a technology that is bringing enormous value to America, as well as create costs and complications that far outweigh the benefits.

The FAA's proposed rule is the most momentous step in American drone policy in years. Thousands of people are expected to file comments on the proposal by the March 2 deadline, because they know how much is at stake. The FAA's response will set the curve for how many new drone jobs and businesses will be created in America, how well companies can transform their operations to be safer and easier with drones, how many students become drone filmmakers or entrepreneurs, and how many American lives will be saved in emergencies.

The FAA's Proposal

The FAA's proposal requires virtually all drones to be networked to a "remote ID service" managed by private supplier companies anticipated to charge mandatory subscription fees. These companies would store the drones' flight records for at least six months. This proposed requirement creates undue financial and compliance burdens and would impede America's existing drone industry.

Thousands of drones and radio-controlled aircraft currently on the market have no means for internet connection and would be grounded. Many manufacturers would face increased equipment costs on new products. Drone "kits" that are used to develop technical skills or allow for customization by the assembly of separate components would essentially be outlawed. Drone operators with limited cellphone service coverage may need to sign up for more expensive data plans. Service fees estimated by the FAA to cost upwards of $5 per month alone would add an approximate 20% extra cost, per year, for the average drone user – even though the benefits of Remote ID are all for police and other authorities, not for drone users. (Actual fees would surely be much higher because that FAA estimate is based on an existing drone service called LAANC, which is far simpler.)

High as they are, those fees might not cover the cost of companies creating the infrastructure that would provide the required low latency and high security. Casual drone

users would have to establish, maintain, and renew subscriptions just to fly occasionally in their backyards. School programs that use drones may decide the costs are just too high to continue. A gift of a drone on Christmas would saddle your recipient with endless monthly fees. And connecting all drones to the internet would create new cybersecurity vulnerabilities.

Compare this with the FAA's new mandate for equipment to prevent airborne collisions between passenger planes. That technology, known as automatic dependent surveillance-broadcast (ADS-B), is required only in controlled airspace, a limited fraction of the country, and needs just a one-time installation of equipment – for which the FAA offered pilots a rebate. But for small modern drones, which are responsible for zero reported fatal accidents worldwide, the FAA proposes the most burdensome solution conceivable.

Worse yet, the FAA's proposal creates unacceptable points of failure. If the Remote ID service providers have technical difficulties, a substantial portion of the civilian drone fleet could be unintentionally grounded without warning. This stark reliance on unproven systems could shut down expensive Hollywood productions, complex industrial operations, and even lifesaving rescue missions. Drones rescue people from peril about once a week in America, and that statistic is increasing, but the FAA proposal could stop that progress in its tracks.

The FAA Inexplicably Declined to Adopt Good Advice

DJI may have been the first to deploy Remote ID, but it wasn't our idea, and neither is the recommended way to implement it. In 2016, Congress instructed the FAA to convene industry stakeholders to determine how to accomplish Remote ID based on "consensus standards." The FAA convened 74 people to serve as stakeholder representatives on the agency's Remote ID Aviation Rulemaking Committee (ARC). 75% of those ARC members represented law enforcement, telecom providers, airports, security technology vendors, and others who stood to gain from Remote ID, while fewer than 7% of the members would primarily face burdens.

Despite this skewed membership composition, the ARC produced a final report that did not recommend mandatory internet-based services. Rather, the consensus recommendation was for drones flying under existing FAA rules to perform Remote ID via a radio broadcast, with network solutions an optional alternative. The ARC's many months of work demonstrated how broadcast technologies scored best for inexpensive retrofit, ease of compliance, and performance. Network-based solutions involved the highest costs, burdens, and privacy intrusions.

Aviation officials in Europe, who also weigh the aviation safety and terrorism risks of drones, agree with that assessment. There, after much debate and thorough evaluation, the Remote ID regulation taking effect this summer requires a direct radio broadcast, not a network-based solution. We know this issue is challenging, and it is not an easy task to balance all the interests involved in protecting innovation while addressing security and safety concerns. Fortunately, the FAA received thoughtful, collaborative advice on how to

do it, which we are disappointed to see has been disregarded without sufficient explanation.

Broadcast Remote ID Is Proven Technology

Remote ID doesn't have to be costly or complex. For the past two years, DJI has demonstrated a Remote ID method that, as predicted by the ARC, is effective, free, automatic, and requires no service-provider middlemen: broadcast technologies.

Our first version of this, called AeroScope, has helped airports, security officials, law enforcement, and infrastructure owners identify drones flying nearby, locate their pilots, and resolve threats and regulatory violations. If you have one of our drones but didn't notice this feature – because it didn't cost you any money or impose any hassle – well, that's the point. Our latest version, demonstrated last year in Montreal, uses an open drone-to-phone standard developed with officials from the FAA and our industry colleagues. The existing Wi-Fi and Bluetooth antennas installed in most drones become Remote ID transmitters once modified by a software update. Those signals are received by an app for off-the-shelf smartphones, making Remote ID effectively free for the authorities who need it. It works.

Unlike proponents of network-based solutions that don't exist outside of pilot programs and controlled demonstrations, we have evidence that broadcast solutions work in the real world: the FAA itself (among others) has already used DJI's broadcast Remote ID to solve problems and pursue investigations. In its proposal, the FAA cites unauthorized drone flights at sporting events, prisons, and at a hot-air balloon festival. DJI's broadcast solution allowed authorities to resolve several of these documented incidents and obtain information for subsequent investigations. The FAA even cited DJI's initiative on broadcast Remote ID at the balloon festival, and we know that our solution was used in the subsequent enforcement investigations because the FAA asked for our help.

The FAA Provides No Credible Explanation

The FAA's only explanation for designing a burdensome "kitchen sink" proposal is that requiring networked drones is "more complete." Network-based tracking of cars would be "more complete" than license plates too, but it would be so burdensome that drivers wouldn't accept it, even if it would serve important accountability functions such as solving the estimated 700,000 hit-and-run crashes in the United States each year. As the FAA's own committee emphasized, "[B]road compliance is critically important for an ID and tracking solution to have value" – and the likelihood that people will comply depends on factors that include "the relative ease of complying [and] the perceived costs of complying." Creating a solution that involves low costs and burdens, and that fosters hassle-free willing compliance, is actually the best way to make it "more complete."

Already, the FAA proposal has prompted an intensely negative response from the drone community, including serious commercial operators who otherwise support the need for Remote ID. That does not bode well for compliance rates. Rather than fostering a culture of compliance, this proposal risks creating a culture of circumvention that could doom the entire Remote ID endeavor.

It remains a mystery why the FAA has diverged so far from the advice it received from 74 stakeholders who devoted their summer to the cause. It may be that security agencies influential on this topic insisted on a panopticon of total awareness, without recognizing that the high costs it imposes may actually thwart the comprehensive solution they need. It may also be that influential companies with visions of future complex drone operations, or new captured sources of recurring revenue, urged expensive forms of control for all other drone operators, even if they unfairly constrain the applications that are already saving lives and improving jobs today. Whatever the reasons behind the startling departure from a reasonable Remote ID rule, the FAA should be transparent with the public about them, so the thousands of people who will submit official comments can be truly informed.

The Future of Drone Innovation Needs You

DJI supports Remote ID but is advocating against the FAA's Remote ID proposal to save drone innovators needless expense and hassle, and because we believe a less complex and costly Remote ID approach will do a better job of fulfilling the safety and security needs the FAA has articulated. We all want safe and secure skies. But few people who understand drone technology will support this proposal, except those who stand to profit from it.

We hope the FAA reconsiders its proposal and enables cost-free and easy-to-use broadcast Remote ID to be a sufficient means of compliance, with network solutions available as an alternative for those who might prefer it. The only way for the FAA to reconsider is for them to hear from you, the drone innovators who will be most directly impacted by this proposal. That is the purpose of the current public comment period.

Between now and March 2, 2020, please take the time to read the FAA's proposal and submit comments at this link. DJI is preparing tips and suggestions for what to include in your comment, but we already see drone operators of every kind sharing ideas among themselves, so be sure to consult your favorite social media sites, user forums, and community groups as well.

The FAA proposal is a watershed moment for the future adoption of drones in America, and the FAA needs to hear from everyone who could be harmed by its insistence on a complex, expensive, intrusive, and over-engineered Remote ID solution. Together, we can ensure that drone innovation is protected and that the safety and security of the skies are assured.