



February 6, 2020

**Submitted electronically via regulations.gov**

Kittyhawk's Comments Regarding the NPRM for Remote Identification of Small Unmanned Aircraft Systems (Docket Number: FAA-2019-1100 / RIN: 2120-AL31)

**About Kittyhawk:**

Kittyhawk sells software solutions for large enterprise and government aviation programs, as well as provides airspace awareness products like the FAA's B4UFLY app. Dynamic Airspace is our data integration engine that turns manual workflows, data entry and phone calls into seamless user experiences that make flying safer and smarter for all types of unmanned operations. Enterprise drone programs - from law enforcement and first responders to large corporate operations with hundreds of licensed drone operators - use the Kittyhawk platform every day to accomplish their goals, inspect assets and save lives when used by emergency responders. Nearly 100,000 people use Kittyhawk every month.

Kittyhawk is an FAA-approved UAS Service Supplier (USS) for the LAANC program, which enables on-demand airspace authorizations in controlled airspace. Our free, publicly available applications for LAANC are used every day for commercial and recreational airspace authorizations. Based on publicly available data, we estimate that Kittyhawk performs 40% of recreational and 25% of commercial LAANC authorizations. In addition, we power the FAA's official mobile application for nationwide drone airspace awareness, B4UFLY. Since Kittyhawk relaunched the application in August 2019, B4UFLY app store reviews have improved 3X and users have made 2.2 million airspace safety checks.

For the last two years, Kittyhawk has been a thought leader and built technology in support of Remote ID. Kittyhawk is a member of the FAA's Unmanned Aircraft Safety Team, the ASTM F38 committee on Remote ID, and a participant in the open source InterUSS Remote ID initiative. In March 2019, Kittyhawk released a white paper titled "Remote ID - Enabling Transparency and Identification in the National Airspace System" to better explain the concept of Remote ID and what methods were available to achieve the goals of Remote ID. The paper has been downloaded more than 3,000 times. For more information and to download our white paper, please visit [www.kittyhawk.io/remote-id](http://www.kittyhawk.io/remote-id).

Remote ID is already enabled in the Kittyhawk platform including our new enterprise platform Air Control. Mission control centers have long been using Kittyhawk's live telemetry, streaming, and identity solutions to run their operations and manage emergency response situations. Along with our recent Remote ID survey results and direct interactions across our user base, our comments on the NPRM are based on our experience of having already brought Remote ID solutions to market and our direct experience of powering safe and compliant flight across commercial, recreational, and law enforcement user bases.



## **Kittyhawk Comments:**

Kittyhawk joins many stakeholders in the drone industry who welcome the release of this NPRM for Remote ID. Kittyhawk has been a longtime supporter of Remote ID and we look forward to the next phase of drone industry growth that will be made possible with timely and widespread adoption of Remote ID. The current situation, in which the industry is held back by the lack of Remote ID, is not sustainable.

We appreciate that the NPRM represents the views of many industry stakeholders, particularly public safety and law enforcement organizations, who need to ensure that they can quickly identify nearly any drone they encounter, and enterprise drone programs who want to use Remote ID so that they can perform advanced operations. Yet, the scope, complexity, and associated timeline of the NPRM makes achieving these goals unlikely in our estimation. In fact, the current NPRM framework sets the safe integration of drones into our national airspace on a course for confusion, frustration and most importantly, extremely low compliance. 3.8 million square miles of 0-400 foot airspace in the United States are uncontrolled. At that scale and with no decrease in the popularity of drones in sight, we need a new approach in strategy that thinks in tiers and volumes and less about command and compel. More math and fewer steps.

Whereas many of the proposed rules in the NPRM would require a series of needle threading in decision-making and execution to promote fair, interoperable, and effective solutions, our comments approach Remote ID from a different angle of attack. We see ways to leverage existing technology and existing USS infrastructure to enable fast, effective, and zero cost options to get to a material baseline of Remote ID in 2020.

## **Kittyhawk Supports A Tiered Approach to Remote ID**

Kittyhawk supports an approach to Remote ID that is closely calibrated to an operation's actual risk. Lower risk operations, such as those within visual line of sight and at lower altitudes, should have less onerous data sharing requirements. Higher-risk operations, such as those advanced operations beyond visual line of sight, should be required to share a significant amount of information with the FAA, USS, and first responders. Thus, a tiered approach to Remote ID where we prioritize zero cost solutions is the best way forward.


Instead of the proposed Standard, Limited, and FRIA options as outlined in the NPRM, we propose a method that all types of operations and all types of aircraft -- from quadcopters to models -- can adopt today. This starts with volume-based Remote ID as outlined in the ASTM standard that can immediately and effectively solve for identification without retrofitting hardware or requiring aircraft to be equipped with real-time broadcast or network capabilities.

We recommend a three tiered approach to Remote ID compliance based on the complexity of the operation. These three tiers correspond to the most common types of envisioned operations. Tier 1 would be operations occurring at low altitudes and within the visual line of sight of the operator that would accommodate the vast majority of model, recreational, and commercial unmanned flights. Tier 2 would unlock higher altitudes by introducing real-time requirements along with volumes. Tier 3 would provide for BVLOS operations with the highest communication and data requirements.

Together these tiers provide a path for immediate compliance while also fulfilling the promise of Remote ID.

**Table 1**

## Zero Cost Tiered System for Remote ID of Drones



	TIER 1	TIER 2	TIER 3
<b>Ceiling (Uncontrolled Airspace)</b>	Up to 200ft	Up to 400ft	Up to 400ft
<b>Ceiling (Controlled Airspace)</b>	Up to 100ft*	Up to 400ft*	Up to 400ft*
<b>Range</b>	VLOS	VLOS	BVLOS
<b>Remote ID Requirements</b>	<p>Volume-based reservation of a time/place.</p> <p>Can be done remotely, up to 90 days in advance.</p>	<p>Volume-based reservation of a time/place.</p> <p>Plus live sharing of telemetry via broadcast or network.</p>	<p>Volume-based reservation of a time/place.</p> <p>Plus live sharing of telemetry via broadcast or network.</p> <p>Plus network connection for aircraft or control stations to send and receive real-time messages.</p>
<b>Process</b>	Submitted and processed like LAANC to a USS.	<p>Submitted and processed like LAANC to a USS.</p> <p>Broadcast or network to meet data requirements.</p>	<p>Submitted and processed like LAANC to a USS.</p> <p>Broadcast or network to meet data requirements.</p>

\*Or lower if flying in controlled airspace and LAANC ceiling is lower than the corresponding tier.

In the successful LAANC program, together government and industry have illustrated that operators will comply if given clear, effective, and zero cost options. These tiers could be implemented and adopted in short order, and Tier 1 specifically could be implemented literally overnight and give operators a reason to start using Remote ID in a pre-rule, early adoption period.

### **Kittyhawk Supports A Tiered Approach to Remote ID Data**


Just as the airspace should open up depending on the richness and timeliness of the Remote ID data, data requirements should vary at the different tiers. Remote ID data can provide identity for both aircraft deconfliction and law enforcement use cases without sacrificing operator privacy.

Real-time operator location data should not be available to the general public as proposed in the NPRM. The general public should be able to see a UAV's real-time location/volume and its Session ID or UAS registration number for law enforcement use cases, but not the operator's location. We recommend that the operator location only be shared during Tier 3 operations for BVLOS, and even then the exact location should be obfuscated to the general public (with only the exact location shared with regulators, USS, and law enforcement).

The knowledge of the UAS operator's location by the general public is a significant privacy issue without any additional benefit for public safety. There is a real risk that misinformed members of the general public could be irritated by a compliant UAS operation and attempt to take enforcement into their own hands and harass or even assault UAS operators while the UAV is in the air. In our NPRM survey of over 100 respondents, only 12% of respondents said they would be comfortable sharing the latitude and longitude of the operator with the general public.

The best way forward is to treat UAVs in the air the same as how we treat cars on the road. The general public should be able to receive real-time information on the UAV's location and its Session ID or UAS serial number, just like the general public can see where a car on the road is located in real-time and its license plate number. If someone sees a UAV that they believe is violating some law, they can report the serial number or session ID and where they saw the UAV to their local law enforcement or the FAA, and either organization can take appropriate action.

Table 2

Tier-Based Remote ID Data


	TIER 1	TIER 2	TIER 3
<b>Aircraft Identity</b>	Serial Number or Anonymous Session ID**	Serial Number or Anonymous Session ID**	Serial Number or Anonymous Session ID**
<b>Aircraft Location</b>	N/A	Real-time LAT/LONG	Real-time LAT/LONG
<b>Operator Identity</b>	Optional	FAA Registration Number or Anonymous Operator ID**	FAA Registration Number or Anonymous Operator ID**
<b>Operator Location</b>	N/A	N/A	Real-time LAT/LONG***
<b>Operator Contact Information</b>	Optional	Optional	Required
<b>Flight Plan</b>	Optional	Optional	Submitted with takeoff, landing, route, and emergency landing points.  Updated in real-time.
	<small>**Generated and stored by a USS. ***Obfuscated to general area for public view, with precise coordinates available to regulators and law enforcement.</small>		

## **Remote ID Should Unlock Routine Advanced Operations**

Kittyhawk has been a consistent supporter of Remote ID because we understand the value that routine advanced operations will have for growing the drone industry. All Part 107 waivers except for a 107.29 waiver to allow Night Operations are prohibitively expensive and/or time-consuming, making them out of reach for all but the most advanced and well-funded organizations. Even then, there are often significant operational limitations for those who are operating with a waiver.

Allowing these advanced operations to happen more often and with fewer limitations is very important to the growth of the commercial side of the drone industry, and the FAA has been clear that a final rule for these operations is contingent on first finalizing requirements for Remote ID. Therefore, we recommend that the FAA allow advanced operations without a waiver as soon as possible. Opting in and using Remote ID in advance of a final rule should also allow routine advanced operations to occur without a waiver.

Lowering the burden on those wanting to perform routine advanced operations should be a priority because it will lower the cost for anyone to perform these operations. For large enterprises, this could mean a big increase in efficiency and confidence in performing their operations, and for smaller companies, this could mean they are able to offer more and higher-value services.

In Table 1 above, our recommendation for Tier 3 flight compliance should enable BVLOS operations.

## **Kittyhawk Advocates for Timely & Zero Cost Solutions**

One of the most affected groups from the NPRM would be recreational operators, and specifically the modeler communities. These groups in particular are the grassroots and future of the aviation industry, are key stakeholders in the success of mass compliance with Remote ID, and should be encouraged to continue to participate in their hobby. Tier 1 as described above presents an opportunity for recreational and model flights to flourish as their aircraft would not be relegated to the trash heap and their flights would not be relegated to FRIA zones.

Kittyhawk is uniquely positioned in the center of the UAS community. In addition to our enterprise customers, we handle a critical mass of airspace authorizations and airspace safety searches across the country. Between powering B4UFLY, the FAA's official mobile app for the recreational community, and being the largest provider of recreational LAANC, Kittyhawk understands how the recreational community operates and we have insight into how to best serve these operators. Providing options that require no new hardware or connectivity is a must for the recreational and model communities.

This is why we recommend the FAA keep open more airspace for the hobbyist community than the FRIAs proposed in the NPRM, and determine additional methods for easy, zero cost compliance with Remote ID. For example, model aircraft operators are not well accounted for in the NPRM, and we have heard very real concerns about how model aircraft operators will be able to continue their hobby. Model aircraft are exactly the type of UAS operator who would be best served by a volume-based approach to Remote ID that does not require additional hardware. This type of volume-based approach would make it possible for modelers to fly compliantly without OEM and real-time Remote ID requirements.

If an increase in cost of Remote ID compliance is going to lower the compliance rate significantly, then Remote ID is not as valuable and the FAA needs to evaluate options that can be achieved at zero cost and zero friction to the operator and thus provide a robust compliance rate for the entire spectrum of unmanned operations.

### **Manufacturers - Too Much Cost, Too Much Control & Too Much Risk**

Kittyhawk recommends that the FAA empower UAS operators with tools that allow them to be responsible, compliant operators as soon as possible. This means that the FAA should be seeking zero cost, software-based solutions that can be implemented in 2020, not 2024.

The proposed rules force manufacturers to bear too much responsibility of Remote ID while also giving them too much control over UAS operations. There is no precedent for OEMs to have that much responsibility and that much control over functionality. The inclusion of OEM requirements and manufacturers having a central role in access to the airspace presents not only complexity in execution, but also and more importantly national security risks.

**Costs:** The NPRM proposes a system that will impose additional costs on operators, and we disagree with this approach. Costs that a manufacturer must bear are costs likely to be passed on to end-users. This could be in the form of additional hardware to be included on new models which would increase the costs of purchasing UAS, or it could be in the form of expensive retrofits to make sure that aircraft that are compliant today continue to be compliant. Even the largest OEMs will have trouble retrofitting or redesigning dozens of different makes and models, and smaller hardware manufacturers may encounter even more challenges, especially for model aircraft and American-based startup manufacturers.

**Control:** A top-down “No Compliance No Takeoff” framework is not in the best interests of end users of UAS technology or national security, and we disagree with this approach. Instead of making the (largely foreign) OEM manufacturers the gatekeeper of the National Airspace System, we can reduce the cost to the operator and the speed and rate of adoption by moving the role of compliance to the Remote Pilot In Command (RPIC). OEM control of aircraft performance and airspace access via Remote ID greatly expands the target landscape for hackers and data breaches.

**Complexity & Security:** Arguably the biggest problem with having OEMs control Remote ID is the complexity and detail that must be considered before requirements are given to manufacturers to implement. The nature of hardware is slow with long cycles for iteration. Getting any element wrong in how OEMs allow access to the air can have years of impact in slowing down implementation or worse breaking something already implemented. Too many security concerns and user cost and control are sacrificed by giving OEMs this unprecedented power.

For example, the language in the NPRM suggests that the FAA is open to allowing UAS to be manufactured to only be compatible with certain USS and anticipates that some companies may be both a UAS manufacturer and a USS. This means that many UAS could be manufactured to only work with one specific USS, and that specific USS could be the manufacturer itself. This removes the fundamental choice of how a RPIC can comply with Remote ID.

The NPRM points out that such a policy has precedent in the recent past, when mobile phone networks sold hardware that would only work on its own network. However, this analogy has a fatal

flaw – allowing certain mobile devices to only be compatible with one network lasted only a few years before the marketplace realized that the model did not serve end users or the market very well or get innovative new hardware in the hands of more people. This also ignores the key element of Remote ID to be interoperable.

For example, when the first iPhone was released in 2007, it was only compatible with one of the four major cellular networks. If you wanted to utilize the hardware you purchased on any other network, you were out of luck. Now imagine if Apple operated a cellular network and only built the iPhone to be compatible with its own network. What's more, imagine Apple not allowing you to use your phone because it can't connect to Apple's network – even when other networks are available. If Apple decided that it wanted to triple the price of using its network, the end user would have two choices: they could pay the extra cost or turn their iPhone into an expensive paperweight. Allowing such a model would discourage the goals of innovation and getting more-capable hardware into the hands of more people. The FAA should be supporting the idea of mass compatibility, not vertical integration which could limit end user choice.

The best recommendation for this issue is to allow a company to be both a UAS manufacturer and a USS, but that manufacturers must make their UAS compatible with and able to be used on the platform of any FAA-approved USS. (i.e. manufacturers must produce UAS and related software that are at least capable of being used on any USS platform that uses official FAA protocols).

A better approach, which is already the standard in aviation, would be to make the RPIC the one responsible for compliance. Give UAS operators a variety of means and methods to comply with Remote ID. As detailed in Table 1 above, our recommendation would be to utilize the existing USS network to enable operators to file volume-based flight plans to create an effective base layer of Remote ID. If time and security are of the essence, then hardware should have no place in the NPRM. Too much is sacrificed and nothing is gained by putting OEMs and manufacturers as the gatekeepers to fly in American airspace.

### **Registration of All Aircraft**

Kittyhawk supports the increased registration requirements for recreational operators, including requiring a registration for each recreational UAV and requiring the operator's phone number upon registration. These are rules that the Part 107 community have been operating under for years, and part of the personal responsibility of operating a UAS should be that you are able to be contacted by the authorities if necessary.

### **Indoor Operations Need a Path Forward**

Kittyhawk seeks clarity on operating Remote ID-enabled UAS indoors, and this is another example of complexity that we can avoid in the first place by removing OEM requirements at the outset.

The NPRM as written does not seem to allow indoor operations by either standard or limited Remote ID-enabled UAS because of the real-time network and GPS requirements. GPS would be limited or unavailable in many indoor environments, so a Remote ID-enabled UAS would not be able to take off indoors. There is no reason to make Remote ID-enabled UAS unlikely to be able to operate in many indoor environments. Even if we decide that indoor flights have a role in the NAS, then a UAS operator should be able to utilize a volume-based reservation of time and place to fulfill Remote ID



requirements. This is another example of how operators could use network-based solutions to reserve and announce their operation in order to fulfill Remote ID requirements, and by doing so, avoid seeing their UAS restricted due to lack of GPS or network signal, and all at zero cost.

### **Broadcast & Network Both Play Key Roles in Remote ID**

LAANC is a network solution that has been an unambiguous success for the FAA, so we know network solutions will work well and scale well. However, we acknowledge the fact that to achieve maximum compliance, we need to give operators the option to achieve Remote ID compliance in a variety of methods, beginning with network-based Remote ID volumes that can be utilized by all operators and all existing aircraft today.

Kittyhawk recommends that some operations, particularly advanced operations such as those described in Tier 2 or 3 in Table 1, provide for the option of choosing network and/or broadcast Remote ID to comply with real-time telemetry requirements. We understand that broadcast and network methods of Remote ID are critical components of achieving maximum Remote ID compliance, but we also understand that different technologies will be best suited for certain situations. Kittyhawk believes strongly that network based solutions are the most agile, scalable, and information-rich solutions that allow for bidirectional communications.

### **NPRM Survey Results**

As part of Kittyhawk's goal of providing informed comments to this NPRM, we asked our user community to take a survey to gauge attitudes towards the NPRM and ways in which drone operators anticipate complying and sharing information. We have received over 100 responses from a mix of large scale enterprise drone apps to individual 107 and 44809 pilots and the results were as follows:

1. Limited Remote ID as described in the NPRM will be very limited, and unlikely to be adopted in large numbers.

52% of respondents anticipate needing to utilize standard Remote ID UAS to comply with Remote ID. This is because 75% of respondents said that they perform at least half of their operations beyond 400 feet of the operator but within visual line of sight.

2. Session ID as described in the NPRM will be utilized in large numbers because people are concerned with privacy.

In our survey, 92% of respondents showed discomfort with the general public knowing the registration number of their UAS. Of that 92% who showed concern, 46% of respondents said they would always use a Session ID whenever possible, 26% said that if the public could see the UAS registration number, they would use Session ID whenever possible, but that they were OK with law enforcement having their registration number, while the remaining 19% said that even a Session ID was insufficient to protect privacy.

3. Drone operators don't want to use Remote ID enabled UAS before the mandatory adoption date if the current proposed requirements are left in place.

64% of respondents said that they don't plan to use Remote ID until required by the FAA for continued operation. We believe that part of the reason this number is so high is that drone operators are very concerned that the Remote ID requirements are overly onerous and therefore will delay complying until they must. The OEM component is also a large factor as to why many respondents have minimal inclination for early adoption given the uncertainty around costs and feasibility of retrofits of millions of existing aircraft and models.

In our discourse with customers and users across the Kittyhawk platform, we gained a clear insight as to how respondents' attitudes would change if Remote ID compliance required no new hardware and zero cost compliance via the internet. We're confident that a significant number of those reluctant respondents would change their mind. Removing OEM involvement in compliance achieves greater operational security and does so at no additional cost to replace relegated hardware.

### **The Compliance Period Is Too Long**

The compliance deadline for universal compliance with Remote ID regulations is too far into the future and proposes few intermediate steps on the way to universal compliance. This approach is overly complicated and restrictive, and leaves too many complex questions unanswered. These proposed rules are much too focused on the giant leap to achieving a Remote ID system 4-5 years from now when instead the primary focus should be on the iterative steps needed to make UAS operations in the NAS safer and more efficient for all stakeholders in the coming months than they are today.

The major provisions of the NPRM take effect 2 and 3 years after the effective date of the Final Rule, with another year at least to complete the rulemaking. This makes it likely that full Remote ID implementation and compliance shouldn't be expected until 2024 or 2025. Waiting 4-5 years for full implementation risks undermining the security argument for Remote ID and a potentially confusing and overly conservative operational environment if people are operating under different rules for a period of time.

One reason why the implementation period needs to be made shorter is that the FAA has made it clear that routine (i.e. waiverless) advanced operations like those beyond visual line of sight, operations over people, or operations at night, require Remote ID. Not allowing these operations to occur for another 5 years is an eternity in a growing industry. As discussed above, these higher-ROI advanced operations are needed to grow the industry. Further, in a confusing period of technology and hardware adoption, many UAS operators, from Fortune 100 companies to small businesses to modelers, will be faced with uncertainty about the future of their existing fleets, and may make fewer buying decisions in the coming years.

If Remote ID is so important to implement for security reasons, and the status quo is so unsustainable, how is it that we can wait 5 years for the rules proposed to actually be effective and enforced? This is precisely why we recommend the Tiered approach as described herein as it results in immediate implementation and supports the security concerns that we and many of our customers share. Further, the NPRM asked about early adoption ideas, and our Tier 1 Remote ID solution is something that regulators and USSs could implement in very short order and provide an option for Remote ID that the majority of recreational and commercial operations could utilize without any additional hardware or related costs. We can do this in 2020.