ORAL ARGUMENT SCHEDULED FOR DECEMBER 15, 2021

No. 21-1087

IN THE UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

TYLER BRENNAN AND RACEDAYQUADS LLC,
Petitioners

v.

STEPHEN DICKSON, ADMINISTRATOR, AND FEDERAL AVIATION ADMINISTRATION,
Respondents

On Petition for Review of a Final Rule of the Federal Aviation Administration

---

BRIEF OF THE ASSOCIATION FOR UNMANNED VEHICLE SYSTEMS INTERNATIONAL AS *AMICUS CURIAE* IN SUPPORT OF RESPONDENTS

Joshua S. Turner
Sara M. Baxenberg
WILEY REIN LLP
1776 K Street NW
Washington, DC 20554
(202) 719-7000
jturner@wiley.law
Counsel for the Association for Unmanned Vehicle Systems International

October 12, 2021

CORPORATE DISCLOSURE STATEMENT

Pursuant to D.C. Circuit Rules 29(b) and 26.1, the Association for Unmanned Vehicle Systems International states as follows:

The Association for Unmanned Vehicle Systems International ("AUVSI") is a not-for-profit trade association representing companies and professionals involved in autonomous and remote systems and robotics, including drones. AUVSI advocates for the commercial, professional, and other common interests of its members. The association does not have any parent companies, and no publicly-held companies have a 10% or greater ownership interest in it.

Respectfully Submitted,

/s/ Joshua S. Turner

Joshua S. Turner
Sara M. Baxenberg
WILEY REIN LLP
1776 K Street NW
Washington, DC 20006
(202) 719-7000
jturner@wiley.law
Counsel for the Association for Unmanned Vehicle Systems International

October 12, 2021

CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES

Pursuant to D.C. Circuit Rule 28(a)(1), the Association of Unmanned Vehicle Systems International certifies as follows:

Parties and Amici:

As of the date of this filing, the Association for Unmanned Vehicle Systems International is the only *amicus curiae*. Petitioners in this case are Tyler Brennan and RaceDayQuads LLC. Respondents are Stephen Dickson, Administrator, and the Federal Aviation Administration.

Ruling Under Review:

The final rule of the Federal Aviation Administration under review is captioned *Remote Identification of Unmanned Aircraft*, FAA Docket No. 2019-1100, Final Rule (Jan. 15, 2021). It was published in the Federal Register on January 15, 2021 *See* 86 Fed. Reg. 4390 (JA1). Corrections made to the final rule were published in the Federal Register on March 10, 2021. *See* 86 Fed. Reg. 13,629.

Related Cases:

This case was not previously before this Court or any other court. Counsel is not aware of any other related cases.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases **Page(s)**

U.S. Constitution

Statutes

Regulations

Other Authorities

GLOSSARY

APA	Administrative Procedure Act
AUVSI	Association for Unmanned Vehicle Systems International
FAA	Federal Aviation Administration
JA	Joint Appendix
NPRM	Notice of Proposed Rulemaking
Remote ID	Remote identification

STATUTES AND REGULATIONS

Pertinent statutes and regulations not included in the addenda submitted by Petitioners and Respondents are provided in *amicus curiae*'s Addendum.

RULE 29 STATEMENT OF IDENTITY, INTEREST, AUTHORITY, AUTHORSHIP, AND FINANCIAL CONTRIBUTION

Pursuant to Federal Rule of Appellate Procedure 29, subsections (a)(4)(D) and (a)(4)(E), AUVSI states as follows:

AUVSI is the world's largest autonomous and remote systems trade association. Its members include systems manufacturers, professional societies, charitable organizations, academic institutions, students, and government agencies involved in autonomous and remote systems and robotics.

AUVSI is committed to advancing widespread deployment of autonomous and remotely operated systems, including drones, and to promoting regulatory structures that will facilitate expanded operations of such technology. Accordingly, AUVSI and its members have a strong interest in the disposition of this case, in which Petitioners challenge a rule of the Federal Aviation Administration imposing requirements related to the remote identification of drone systems during flight. As the Federal Aviation Administration has repeatedly recognized, remote identification is a necessary step towards enabling expanded operations of such systems such as operations over people and beyond visual line of sight. *See, e.g., Remote Identification of Unmanned Aircraft*, Final Rule, 86 Fed. Reg. 4390, 4391

(JA2) (Jan. 15, 2021). Vacating or remanding the remote identification rule would set the development of rules governing remote and autonomous systems back months, if not years.

AUVSI moved the Court for leave to file this *amicus* brief in support of Respondents on October 5, 2021. Although Respondents consented to AUVSI's participation, Petitioners indicated they would consent only if AUVSI agreed to limitations on the scope of its briefing beyond those provided for in this Court's rules governing *amicus* participation. AUVSI's motion was granted on October 7.

No counsel for a party authored AUVSI's brief in whole or in part; no party or party's counsel contributed money to fund preparing or submitting the brief; and no person other than the *amicus curiae*, its members, or its counsel contributed money to fund preparing or submitting the brief.

Respectfully Submitted,

Joshua S. Turner
Sara M. Baxenberg
WILEY REIN LLP
1776 K Street NW
Washington, DC 20006
(202) 719-7000
jturner@wiley.law
Counsel for the Association for Unmanned Vehicle Systems International

INTRODUCTION AND SUMMARY

This case concerns an effort by the Federal Aviation Administration ("FAA") to continue implementing a Congressional directive to integrate remotely piloted aircraft into the national airspace. Here, the FAA adopted regulations, critical to that integration, enabling the electronic identification and location of remotely piloted aircraft and their operators during flight, similar to the flight information provided by traditional manned aircraft. *Remote Identification of Unmanned Aircraft*, 86 Fed. Reg. 4390 (JA1) (Jan. 15, 2021) ("Final Rule"). The remote identification ("remote ID") rulemaking is one piece of an ongoing, incremental process by the FAA to enable remotely piloted aircraft (referred to herein as "drones," "drone systems" or "unmanned aircraft systems," as appropriate) to operate at scale in the complex, highly regulated U.S. airspace. The FAA has been engaged in this process pursuant to multiple, iterative legislative mandates issued over the past ten years.

Once fully implemented, the Final Rule will have a tremendous positive impact on the drone industry and its ability to bring this transformative aviation technology to the American people. The Final Rule's adoption already has allowed the FAA to expand its existing regulations to allow flights over crowds of people using aircraft that are equipped with remote ID and meet other safety criteria. Because drones are more agile, less expensive, and safer to deploy than traditional aircraft, the availability of routine drone flights will allow for a significant number

of innovative and beneficial applications. As drone integration continues, capabilities such as remote delivery of lifesaving medicine, faster and better disaster response, unparalleled access to news, delivery, and, eventually, pilotless air taxis, can all become a reality.

Petitioners ask this Court to vacate the Final Rule, claiming that it is arbitrary and capricious in violation of the Administrative Procedure Act ("APA"), 5 U.S.C. § 551 *et. seq.*, and inconsistent with the Fourth Amendment, U.S. Const. amend. IV. At the crux of the Petitioners' brief are Petitioners' concerns about the Final Rule's impact on drone hobbyists and Petitioners' claim that those hobbyists should be entitled to operate their aircraft without having to electronically signal their location. However, Congress has made clear time and again that the airspace is a unique national resource, and that the responsibility for ensuring the safety and security of that resource is vested with the FAA. Congress further has repeatedly expressed the importance of integrating drones into that airspace to unlock this important technology for the American people, including through the adoption of remote ID requirements applicable to *all* drones operating in U.S. airspace.

This rulemaking was a cut-and-dry fulfillment of congressional directives. The FAA's process comported with the APA and relevant statutes, and the result is supported by the significant public record developed in the proceeding. Moreover, contrary to Petitioners' claims, the Final Rule raises no Fourth Amendment issues—

claims about how the government may theoretically use data are not ripe for adjudication, and the arguments raised by Petitioners rest on a fundamental misunderstanding of airspace rights. The rule should be affirmed.

ARGUMENT

I. THE FAA'S REMOTE ID RULE IS AN ESSENTIAL STEP FORWARD FOR THE SAFE INTEGRATION OF DRONES INTO THE NATIONAL AIRSPACE.

Petitioners decry the FAA's remote ID proceeding as a "sham," and claim that it produced an arbitrary rule that defies the will of Congress and fails to advance aviation safety. Pet. Br. 14. In reality, this proceeding was an essential, and expected, component of a broader effort to integrate drones into the airspace pursuant to multiple Congressional mandates. The rules that the FAA adopted were properly teed up in the agency's Notice of Proposed Rulemaking ("NPRM"), 84 Fed Reg. 72,438 (Dec. 31, 2019) (JA125), were well-supported by the voluminous record amassed in the proceeding, and serve as an essential step to enable the kind of expanded drone operations that will garner significant public benefit. In fact, the rules ultimately adopted by the FAA were more modest in scope than those that had been proposed in the NPRM.

The advent of commercial drones promises transformative benefits for nearly every aspect of modern society. The popular term "drone" encompasses many types of aircraft, spanning a wide range of sizes, designs, and use cases, but they share a

critical characteristic: the ability to be piloted remotely (and, in some cases, autonomously). Because of this feature, drones can provide access to, and vantage points of, locations that are too dangerous, difficult, or expensive to reach on foot or using larger manned aircraft. Without the need for a pilot on board, drones can accommodate a range of capabilities into an extremely compact airframe, and thus can be manufactured at a price point that offers commercial enterprises and members of the public unprecedented access to aviation.

This technology thus has fostered numerous uses across myriad industries. For instance, railroads, cellular carriers, electric utilities, and others are using drones to inspect their facilities, ensuring the ongoing operation of important national infrastructure while limiting the need for treacherous in-person inspection. Others have taken this a step further, using drones to enhance that infrastructure. For instance, AT&T uses its "Flying COWs" – drones equipped with radio antennas – to provide additional cellular coverage and capacity. *See* Comments of AT&T Services, FAA-2019-1100-50630, at 5 (Mar. 2, 2020) (Amicus Addendum ("Add.")[1]

[1] In this brief, AUVSI cites to several public comments submitted in response to the NPRM that do not appear in the parties' Joint Appendix. Because the parties have already submitted the completed appendix to the Court, and because Circuit Rule 30(e) permits only parties to move to supplement the Appendix, for ease of the Court's review of these materials AUVSI has included them in an addendum to this brief. Each of the materials included in this addendum was incorporated in Respondents' Certified Index to the Record, which refers to the publicly available rulemaking docket at https://www.regulations.gov/document/FAA-2019-1100-0001/comment?sortBy=postedDate.

Add.3) ("AT&T Comments"). It has deployed Flying COWs in the aftermath of natural disasters including hurricanes in Puerto Rico, North Carolina, and Florida—providing critical connectivity during utility outages and periods of high usage. *Id*.

Drones have a valuable role to play in other emergency situations, including search and rescue, monitoring conditions such as wildfires, and newsgathering. Because they can carry physical payloads in addition to cameras and sensors, drones are also opening the door to new opportunities in the delivery of goods, ranging from mobile defibrillators, to the provision of medicine in remote areas, to everyday package delivery that enhances convenience and minimizes road congestion. These solutions are not hypothetical; they are already being deployed in the United States in limited circumstances with special approvals from the FAA. For instance, UPS's Flight Forward pilot program delivers medical products between hospitals at multiple locations in the United States. Comments of UPS Flight Forward & United Parcel Serv. Co., FAA-2019-1100-36514, at 2 (Mar. 2, 2020) (Add.5) ("UPS Comments"). Wing Aviation provides commercial delivery services in Christiansburg, Virginia, and globally has logged more than 80,000 flights. Comments of Wing Aviation LLC, FAA-2019-1100-51456, at 3 (Mar. 2020) (Add.10) ("Wing Aviation Comments").

These are just a handful of applications that drones are poised to provide at scale, which collectively will create hundreds of thousands of jobs and generate

billions of dollars in revenue. *See, e.g.,* AUVSI, The Economic Impact of Unmanned Aircraft Systems Integration in the United States, at 3 (2013), https://higherlogicdownload.s3.amazonaws.com/AUVSI/958c920a-7f9b-4ad2-9807-f9a4e95d1ef1/UploadedImages/New_Economic%20Report%202013%20Full.pdf. And these benefits will only increase as drone manufacturers embrace additional innovation, such as Skydio's platform that leverages next-generation artificial intelligence to enable autonomous flights. Comments of Skydio, FAA-2019-1100-51388, at 2 (Mar. 2, 2020) (Add.16) ("Skydio Comments").

To unlock the potential of this transformative aviation technology, the FAA, at the direction of multiple acts of Congress, has been engaged over the past decade in an incremental regulatory effort to integrate drones into the national airspace. Because the United States boasts the safest, most complex airspace in the world, the integration of remotely piloted aircraft is no easy task. In 2011, when the concept of widespread recreational and commercially operated drones began to gain traction among policymakers, the airspace already was subject to pervasive FAA regulation governing categories of airspace, flight routes, aircraft design and registration, and pilot training, among other areas. These comprehensive regulations presented challenges for emerging drone technologies. For instance, regulations adopted with an aircraft cabin and an on-board crew in mind were difficult or impossible to apply. The small size of many drone models meant that registration numbers displayed on

the side of the aircraft would be unreadable during flight. The pilot being located apart from the aircraft, and the need to rely on cameras and sensors for remote navigation, raised novel operational questions, such as how to ensure that drones could "see and avoid" other air traffic.

In order to address these challenges, Congress has enacted a series of laws to ensure that the FAA has the requisite authority and direction to safely enable drone operations in U.S. airspace. Its efforts began with legislation in 2011 directing the FAA to establish drone test sites. National Defense Authorization Act for Fiscal Year 2012, Pub. L. No. 112-81, § 1097, 125 Stat. 1298, 1608-09. This was followed closely by the 2012 FAA Modernization and Reform Act ("FAA Modernization Act"), which required the Secretary of Transportation to "develop a comprehensive plan to safely accelerate the integration of civil [drones] into the national airspace system," establish rules for the operation of small drones, and provide regulatory exemptions to enable drones to operate in the airspace on a case-by-case basis. Pub. L. No. 112-95, §§ 332, 333, 126 Stat. 11, 73-76.

In 2016, after issuing a series of regulatory exemptions to specific drone operators, the FAA adopted its Part 107 regulations. 14 C.F.R. pt. 107. Part 107 broadly enabled routine commercial small drone operations without prior FAA authorization subject to a number of operating limitations, including that the aircraft remain within visual line of sight of the operator, weigh less than 55 pounds, be

operated only during daytime, and not operate over people, among others. *See generally id*. These limitations were part of the FAA's incremental approach to integrating drones into the airspace, enabling the agency to "move to quickly issue a final rule" on "small [drone] operations posing the least amount of risk," while it continued working on more complex use cases "pos[ing] additional safety issues that require more time to resolve." *Operation and Certification of Small Unmanned Aircraft Systems*, Final Rule, 81 Fed. Reg. 42,064, 42,071 (June 28, 2016).

As the FAA considered how to safely expand drone operations, it became clear that providing situational awareness of the airspace would be a key piece of the puzzle. While traditional manned aircraft have long been required to provide their location via radiofrequency transmission and submit to aircraft coordination and deconfliction through air traffic control—and are large enough to display registration numbers readable from the ground—no similar regimes were in place for drones. *See Statement of Policy for Authorizations to Operators of Aircraft That are Not Equipped With Automatic Dependent Surveillance-Broadcast (ADS–B) Out Equipment*, 84 Fed. Reg. 12,062, at 12,062 (Apr. 1, 2019) (describing the history of surveillance requirements for manned aircraft, which transitioned from radar-based technology to Automatic Dependent Surveillance – Broadcast in early 2020).

Two concepts emerged that would help to solve these problems: remote ID and unmanned aircraft system traffic management. Remote ID describes the

technical capability to remotely identify drones and drone pilots during flight through electronic means, and unmanned aircraft system traffic management refers to an air traffic control system for drone systems. Congress addressed both in the 2016 FAA Extension, Safety, and Security Act ("Extension Act"), directing the FAA to convene stakeholders to develop remote ID standards and adopt regulations or guidance on remote ID, and to continue its ongoing research with NASA on developing a traffic management system. Pub. L. No. 114-190, §§ 2202, 2208, 130 Stat. 615, 629, 633-34.

The FAA determined that it could not take steps to expand Part 107, including enabling operations over people and at night, until it finalized a rule or policy concerning remote ID. *See Operation of Small Unmanned Aircraft Systems Over People*, Notice of Proposed Rulemaking, 84 Fed. Reg. 3856, 3861 (Feb. 13, 2019). However, the agency faced a legal obstacle: the Modernization Act had divested the FAA of authority over certain hobbyist drones—in other words, drones flown recreationally, called "model aircraft." *See* FAA Modernization Act § 336, 126 Stat. at 77-78. A functional remote identification system, and an eventual drone traffic management system, depends on the participation of *all* aircraft in the national airspace, not just those serving commercial purposes. Thus, while the FAA convened stakeholders on remote ID by chartering an Aviation Rulemaking Committee, and while that Committee provided a report and recommendations to

the FAA in 2017, *see* UAS Identification and Tracking (UAS ID) Aviation Rulemaking Committee: ARC Recommendations, Final Report (Sept. 30, 2017) (JA561), the agency remained powerless to impose comprehensive remote ID rules covering all airspace users absent further legislation.

Again, Congress took action to ensure the FAA had the requisite authority and direction to continue with drone integration: the 2018 FAA Reauthorization Act ("Reauthorization Act") amended the carveout for model aircraft to expressly enable the FAA to "promulgat[e] rules generally applicable to [drones] … relating to … the registration and marking of [drones]; … the standards for remotely identifying owners and operators of [drone] systems and associated [] aircraft; and … other standards consistent with maintaining the safety and security of the national airspace system." Pub. L. No. 115-254, § 349(f), 132 Stat. 3186, 3299.

Armed with this authority, in 2019 the FAA moved forward with establishing remote ID requirements, adopting an NPRM seeking comment on a remote ID regulatory regime for drones. The NPRM was comprehensive, inviting input on a detailed framework that included criteria for the remote ID message elements, message transmission standards, performance requirements and operational constraints, manufacturers' declarations of compliance, labeling obligations, retrofitting for existing drones, and the creation of "FAA-recognized identification areas" that would be exempt from remote ID obligations, among other proposals.

See generally NPRM (JA125-211). As Petitioners explain, in the NPRM the FAA sought comment on establishing a two-tiered scheme for remote ID: "standard" remote ID, which would both broadcast message elements using unlicensed spectrum and transmit those elements over the internet, and "limited" remote ID, which would use only internet-based transmission and would require that the operator of a limited remote ID system remain within 400 feet of the aircraft. Pet. Br. 5-6.

In the Final Rule, the FAA adopted a significant number of its initial proposals, while revising other proposed requirements in light of more than 53,000 public comments filed in the docket. *See generally* Final Rule (JA1-124). Those revisions included a policy decision by the FAA to adopt a more limited approach to remote ID, which foregoes imposing network remote ID obligations for the time being and instead requires only broadcast remote ID, pending further evaluation of the operational and implementation complexities of an internet-based remote ID system. *Id*. at 4408-4409 (JA21-22).

The adoption of the remote ID rules has already allowed the FAA to issue rule changes expanding Part 107. Simultaneously with the Final Rule, the FAA released another final rule revising Part 107 to permit commercial drone operations over people and at night subject to various conditions and restrictions. *Operation of Small Unmanned Aircraft Systems Over People*, Final Rule, 86 Fed. Reg. 4314 (Jan. 15,

2021). Under those rules, drones can conduct sustained flights over open-air assemblies of people only if the aircraft is equipped with remote ID in accordance with the Final Rule challenged here. 14 C.F.R. §§ 107.110(c), 107.115(b). Thus, the Final Rule is already serving as a building block for expanded drone operations.

The Final Rule that Petitioners ask this Court to vacate is a critical step in a lengthy process at the FAA that has hewn closely to multiple Congressional mandates contained in several legislative acts. This proceeding was not, as Petitioners imply, a frolic and a detour by the FAA to invade personal privacy and impose unnecessary requirements. Instead, it was an effort to carry out a Congressional directive to adapt existing aviation paradigms to new users of the airspace through a careful rulemaking process. The Final Rule is necessary for the continued expansion of drone operations and the fulfillment of Congress's vision of an integrated airspace that brings significant benefits to the American people.

II. INDUSTRY PARTICIPATION IN THE FAA PROCEEDING WAS ROBUST AND ESTABLISHED THE NEED FOR BROADCAST REMOTE ID AND OTHER ASPECTS OF THE FAA'S RULE.

Given the critical importance of remote ID to widespread and expanded drone deployment, a large number of stakeholders in the drone industry—including AUVSI and many of its members—were active participants in the FAA's proceeding. These commenters included companies, associations, and research institutions that have significant experience with building, deploying, and operating

drones, and their comments provided thorough and nuanced analysis about the need for remote ID and the best way to implement it. The expansive record they helped to create demonstrated the importance of remote ID to the future of the drone industry and provided support for particular policy choices that the FAA made in the Final Rule, including the adoption of a single-tier broadcast remote ID framework and the use of geometric altitude, among others.

Numerous drone industry participants discussed the foundational importance of implementing remote ID to ensure safe and secure drone operations, and the need for the FAA to take action in the proceeding below. *See, e.g.*, Comments of AUVSI, FAA-2019-1100-43205, at 1 (Mar. 1, 2020) (Add.18) ("AUVSI Comments"); AT&T Comments at 2 (Add.2); Comments of Lockheed Martin Corp., FAA-2019-1100-49902, at 1 (Mar. 2, 2020) (Add.19) ("Lockheed Martin Comments"); Comments of Virginia Polytechnic Institute and State University's Mid-Atlantic Aviation P'ship, FAA-2019-1100-51738, at 1-2 (Mar. 3, 2020) (Add.22-23) ("MAAP Comments"); Wing Aviation Comments at 4 (Add.11).

Drone industry participants emphasized that the crucial safety and security benefits provided by remote ID would facilitate widespread drone operations, including beyond visual line of sight, flights over people, and flights at night. *See, e.g.*, Comments of Aerospace Indus. Assoc., FAA-2019-1100-50889, at 2 (Mar. 2, 2020) (Add.30) ("AIA Comments"); Comments of AiRXOS, Inc., FAA-2019-1100-

50167, at 1 (Mar. 2, 2020) (Add.31) ("AiRXOS Comments"); Comments of Amazon Prime Air, FAA-2019-1100-36349, at 1 (Mar. 2, 2020) (Add.35) ("Amazon Comments"); AT&T Comments at 2 (Add.2); UPS Comments at 3 (Add.6); Comments of Verizon & Skyward, FAA-2019-1100-50346, at 1 (Mar. 2, 2020) (Add.40); Wing Aviation Comments at 4 (Add.11).

Commenters also emphasized the extent to which remote ID will drive public acceptance of widespread drone operations, which is a critical aspect of drone integration that must accompany sound regulatory policy. *See, e.g.*, AUVSI Comments at 1 (Add.18); MAAP Comments at 1 (Add.22); UPS Comments at 3 (Add.6). The record further showed that remote ID will set the stage for a future drone traffic management system that will fully integrate drones into the national airspace. *See, e.g.*, Wing Aviation Comments at 4 (Add.11); Lockheed Martin Comments at 2 (Add.20); *see* NPRM, 84 Fed. Reg. at 72,439 (JA126).

While there was disagreement about whether broadcast or network-based remote ID provided the best path forward, a number of industry comments addressed the significant complexities—concerning both operations and implementation—of networked remote ID, *i.e.*, remote ID that required the operator to maintain an internet connection to transmit information about the aircraft and its operator to a central service provider. One of these complexities, according to industry commenters, is that internet access is often unreliable in remote locations, after

natural disasters, and on federal government test range sites. *See, e.g.,* Amazon Comments at 2-3 (Add.36-37); Lockheed Martin Comments at 3 (Add.21); MAAP Comments at 3-4 (Add.24-25); UPS Comments at 5 (Add.8). Industry also pointed out a host of other difficulties associated with a networked solution, such as the need to be within range of network access points, having to troubleshoot connectivity issues, cybersecurity vulnerabilities, and an inability to retrofit existing products. *See, e.g.*, Comments of DJI Technology Inc., FAA-2019-1100-51823 (Mar. 2, 2020) (Add.41) ("DJI Comments"); Lockheed Martin Comments at 3 (Add.21). Industry comments also highlighted a number of benefits offered by a broadcast solution—including a simplified infrastructure, a lack of dependencies on various external steps and services, and tamper resistance—making clear that such a solution could be a sensible policy choice for remote ID implementation. *See, e.g.,* DJI Comments at 21, 23 (Add.42-43); Lockheed Martin Comments at 3 (Add.21).

In addition to offering support for a broadcast remote ID solution, industry comments helped persuade the FAA to revisit several other aspects of the proposed rule. For example, several industry commenters voiced opposition to the FAA proposal to require barometric pressure altitude measurements for the aircraft and control station because barometric sensors are highly susceptible to error and most aircraft and control stations are not currently equipped to measure barometric pressure altitude. *See, e.g.*, MAAP Comments at 10-12 (Add.26-28); Wing Aviation

Comments at 18, 20 (Add.12-13). In the Final Rule, the FAA abandoned barometric pressure altitude requirements in favor of geometric altitude and explicitly referred to its review of the public comments opposing barometric pressure altitude as a reason for the change. Final Rule at 4420, 4422 (JA33, 35). Additionally, industry commenters were successful in urging the FAA to expand eligibility for remote-ID-exempt FAA-recognized identification areas to include educational institutions, *see, e.g.*, AiRXOS Comments at 6 (Add.33); Wing Aviation Comments at 20-21 (Add.13-14); Final Rule at 4437 (JA50), and to remove the 12-month limitation on applications to establish such identification areas, *see, e.g.*, AiRXOS Comments at 6 (Add.33); Wing Aviation Comments at 20 (Add.13); DJI Comments at 76 (Add.56); Final Rule at 4438 (JA51).

The drone industry also voiced its support for other provisions that the FAA adopted in the Final Rule, including allowing retrofitting of remote ID capability, setting the size threshold for the remote ID requirement at 0.55 pounds, and allowing the use of a session identification number as a unique identifier during flight, in order to further enhance operator privacy and security. *See, e.g.*, AIA Comments at 11 (Add.30) (supporting the option to retrofit); Skydio Comments at 17 (Add.17) (same); Final Rule at 4431 (JA44) (permitting an operator to retrofit drones with a remote ID broadcast module); AiRXOS Comments at 4 (Add.32) (supporting size threshold of 0.55 pounds); UPS Comments at 4 (Add.32) (same); Final Rule at 4403

(JA44) (setting size threshold at 0.55 pounds); AiRXOS Comments at 13 (Add.34) (supporting the use of a session identification number); DJI Comments at 85 (Add.52) (same); Final Rule at 4417 (JA30) (permitting the use of a session identification number to satisfy the unique identifier requirement).

The FAA's Final Rule was thus the culmination of rulemaking efforts that began when the FAA chartered the aviation rulemaking committee pursuant to the Extension Act, and was supported by a robust record before the agency.

III. RESPONDENTS ARE CORRECT THAT PETITIONERS' APA AND PROCEDURAL CLAIMS LACK MERIT.

Petitioners claim that the FAA violated the APA by producing a Final Rule that was not the "logical outgrowth" of the NPRM, failing to adequately respond to comments in the record, and either improperly relying on ex parte contacts or failing to collect public comment on significant information relevant to the rulemaking. Pet. Br. 30-59. Petitioners further assert that the FAA failed to consult the Radio Technical Commission for Aeronautics and the National Institute of Standards and Technology in convening stakeholders for the aviation rulemaking committee, thereby violating the Extension Act. *Id*. 45.

Respondents are correct that "[a]ll of these challenges lack merit," Resp. Br. 37, and Respondents' analysis – coupled with the lengthy and comprehensive record, detailed above – demonstrates both that the Final Rule complies with the APA and that the FAA properly consulted with the relevant entities. AUVSI elaborates on

two aspects of the Government's response to Petitioners' APA claims: the FAA's consideration of comments in the record, and its establishment of a cohort on remote ID technical implementation.

A. The FAA's Consideration of Comments in the Record Satisfies the APA.

As Respondents explain, "[t]he APA required the FAA to 'respond to major substantive comments' in the course of the rulemaking . . . but the FAA was not required to 'discuss every item or fact or opinion included in [those] comments.'" Resp. Br. 55 (citing *Sierra Club v. EPA*, 863 F.3d 834, 838 (D.C. Cir. 2017) and *Environmental Def. Fund v. EPA*, 922 F.3d 446, 458 (D.C. Cir. 2019)). Consistent with this precedent, "comments which themselves are purely speculative and do not disclose the factual or policy basis on which they rest require no response." *Home Box Office, Inc. v. FCC*, 567 F.2d 9, 35 n. 58 (D.C. Cir. 1977).

Thus, with respect to the constitutional claims Petitioners assert required a response from the FAA, Respondents are correct that there was no APA violation, not only because "[t]he rule's notice laid of FAA's legal position," thus obviating the need for further FAA response that "'would mainly restate what had already been set forth in [its] published notice,'" Resp. Br. 61 (quoting *Texas Mun. Power Agency v. EPA* 89 F.3d 858, 870 (D.C. Cir. 1996) (additional quotation marks omitted)), but also because the claims at issue were entirely speculative. Indeed, Petitioners appear to concede that many of the so-called Constitutional claims raised by commenters

were frivolous, and do not even attempt to raise the various Commerce Clause, First Amendment, and Fifth Amendment arguments made in the proceeding below on the merits here. Petitioners do bring Fourth Amendment challenges to the Final Rule, but as Respondents explain and as AUVSI addresses below in Section IV.A., *infra*, the Final Rule itself does not implicate the Fourth Amendment because it does not constitute a government search. Because Petitioners' Fourth Amendment claims rest entirely on conduct that government entities could potentially undertake in the future using remote ID information, they too were speculative and merited no response.

Petitioners' claim that the Final Rule is arbitrary because the FAA failed to address arguments about the FAA's statutory authority similarly should be rejected. Respondents are correct that the NPRM "laid out FAA's legal position … and articulated the statutory authority for this rulemaking," thus eliminating any obligation to repeat the same basis of authority in the Final Rule. Resp. Br. 61. Respondents are likewise correct that the Petitioners here have stopped short of "challeng[ing] the rule as exceeding the FAA's statutory authority[,] … instead argu[ing] that the agency failed to address comments raising these legal concerns." *Id*. at 61. However, in making this argument, Petitioners inaccurately characterize the Final Rule as regulating drones operating in "non-navigable" airspace, "including down to non-navigable airspace in a private backyard." Pet. Br. 15, 50-52.

In fact, the airspace in which drones operate, and in which the Final Rule's remote ID obligations apply, is "navigable airspace" within the jurisdiction of the FAA. The FAA has directed that small drones are generally confined to airspace below 400 feet, and has declined to set a minimum altitude for these aircraft. *See* 14 C.F.R. § 107.51(b)(2). Petitioners are correct that the U.S. Code defines navigable airspace as "'airspace above the minimum altitudes of flight prescribed by [FAA] regulations.'" Pet. Br. at 51 (quoting 49 U.S.C. § 40102(a)(32)). However, the FAA's decision not to impose a minimum altitude for drones—which would be unnecessary in this context because of the ability of drones to safely operate both close to the ground and in the proximity of structures in a way manned aircraft cannot—does not mean that drones are operating in "non-navigable airspace." It means that the minimum altitude for drones, and thus the navigable airspace for drones, begins at the ground.

Petitioners' contrary characterization of the "navigable airspace" offers a dangerous vision of the skies, in which the FAA somehow lacks jurisdiction over the very low-altitude airspace in which it has directed that drones operate—decisions that have been repeatedly ratified by Congress. This strained interpretation would call into question the FAA's status as the agency charged with ensuring safe flight in the United States airspace, and potentially leave room for control of that low-altitude airspace by a range of others, including private property owners, other

federal agencies, or state and local governments. Such a result would be completely at odds with how control over airspace must be allocated to ensure a safe, navigable airspace system.

As Respondents correctly explain, in the context of aviation, it is well settled that "'Federal control is intensive and exclusive. Planes … move only by federal permission, subject to federal inspection.'" Resp. Br. 24 (quoting *Northwest Airlines v. Minnesota*, 322 U.S. 292, 303 (1944) (Jackson, J., concurring)). Congress has made the FAA the central authority for providing that oversight, "direct[ing] the FAA to 'promote safe flight of civil aircraft in air commerce,'" "vesting the FAA with broad authority to issue 'regulations and minimum standards … necessary for safety in air commerce and national security,'" and "direct[ing] the FAA to 'prescribe air traffic regulations of the flight of aircraft … for navigating, protecting and identifying aircraft.'" Resp. Br. 2, 24 (quoting 49 U.S.C. §§ 44701, 40103(b)(2)(A)). Likewise, as discussed above, Congress has provided the FAA with the sole authority to integrate drones, specifically, into the airspace, including express authority to adopt rules for remote ID and a mandate to develop remote ID standards. *See* Sec. I., *supra* (discussing the Modernization Act, Extension Act, and Reauthorization Act).

Petitioners' claims addressing—and implicitly attacking—the FAA's authority therefore should be rejected, both because the FAA appropriately

addressed its authority in the course of the rulemaking, and because as a matter of law the FAA plainly had authority to promulgate the Final Rule as it applies to all drone flights in the United States.

B. The Court Should Reject Petitioners' Claims Regarding the FAA's Interaction with the Service Suppliers Cohort.

Respondents also are correct that the FAA did not consider any improper *ex parte* communications in issuing the Final Rule. As Respondents explained, the cohort of potential remote ID service suppliers was convened as one of "several 'interdependent parts that are being developed concurrently'" to implement remote ID. Resp. Br. 39 (quoting NPRM, 84 Fed. Reg. at 72,439) (JA126). In convening the cohort, "[t]he FAA repeatedly noted that the Remote ID rules would not be discussed during cohort meetings, and that if cohort members wished to comment on the rule, they had to submit comments on the public rulemaking docket," as many cohort members, including AUVSI members, did. *Id*. at 40-41. Accordingly, Respondents accurately explain that the FAA did not consider feedback from the cohort in the Remote ID rulemaking, and the "FAA's passing reference to the cohort in the final rule" is of no moment given the "FAA's reliance on thousands of comments opposing the proposed Remote ID network requirement." *Id*. 43, *see also* Sec. II., *supra* (discussing the feedback of several commenters identifying operational and implementation challenges with network remote ID).

It is also true that "[e]ven assuming that the FAA considered materials from the cohort in abandoning the rule's internet-transmission requirement … given that petitioner Brennan advocated that the FAA abandon the … requirement … petitioners cannot demonstrate that they were prejudiced by the FAA's purported consideration of any cohort-related materials[.]" Resp. Br. 45. Accordingly, Petitioners lack standing to challenge the FAA's alleged consideration of cohort information, and any such consideration was harmless error. *Id.*; *see also Air Transport Ass'n of America v. CAB*, 732 F.2d 219, 224 n. 11 (D.C. Cir. 1984) (explaining that an agency's consideration of evidence received during ex parte communications "generally would be found harmless" when the petitioner does not claim that the evidence is erroneous and "does not explain what it would have said had it been given earlier access to" the evidence).

In addition, any such error is harmless not only because of the lack of prejudice to Petitioners, who support the FAA's policy decision to not adopt networked remote ID, but because there remains the opportunity for public comment on the complexities of internet-based remote ID, as the FAA has not yet imposed that requirement. Indeed, the effect of the FAA's decision on networked remote ID was to *remove* a requirement proposed in the NPRM, and take it up at a later time in a "future regulatory action[]." Final Rule, 86 Fed. Reg. at 4406 (JA19). To the extent the FAA eventually seeks to impose requirements for networked remote ID,

it may be appropriate to incorporate and seek public comment on information learned from the cohort, at which point the public will have full opportunity to comment. But at this time, such action would be premature.

In fact, the posture of the rulemaking supports the conclusion that even if the FAA relied on information learned from the cohort in finalizing the remote ID rule (which it did not), the FAA was not required to "reopen the comment period" as Petitioners assert. Pet. Br. 32 (quoting 49 C.F.R. § 5.5(a)(5)); *id*. at 37. The relevant regulation provides that the FAA should collect further public comment "if [the Department of Transportation] learns of significant new information, such as new studies or data, after the close of the comment period that the [FAA] wishes to rely upon in finalizing the rule." 49 C.F.R. § 5.5(a)(5). But once the FAA rescinded the network-based remote ID proposal in the Final Rule, the provisions of the rule that remained—broadcast remote ID and requirements related thereto—could not possibly have been based on information learned from the cohort, which was formed solely to develop implementation of a networked solution. *Id*. The cohort information was therefore irrelevant to the rule that the FAA ultimately adopted.

IV. RESPONDENTS ARE CORRECT THAT THE COURT SHOULD REJECT PETITIONERS' FOURTH AMENDMENT CLAIMS.

A. Petitioners' Claims Are Unripe.

Petitioners advance a number of claims based on the expectation of privacy under the Fourth Amendment. Pet. Br. 20-30. Respondents' brief explains why the

Final Rule does not infringe on a reasonable expectation of privacy and does not otherwise violate the Fourth Amendment. Resp. Br. 21-37. In so doing, Respondents correctly explain that "[t]he rule merely requires that [drones] broadcast certain information[.] … The rule does not address how various government agencies may subsequently use that information," and thus in and of itself does not constitute a search. *Id*. at 26.

Because the Final Rule does not constitute a search, Petitioners' Fourth Amendment claims are not only meritless, they are nonjusticiable because they are not ripe. *See, e.g., United Transp. Union v. Foster*, 205 F.3d 851, 858 (5th Cir. 2000) (pre-enforcement challenge to a statute authorizing post-collision toxicological testing of railroad crews involved in railroad crossing collisions was not ripe for judicial review because an uncertain chain of events, including law enforcement ordering testing without probable cause, would have to occur); *Ass'n of Am. Physicians & Surgeons, Inc. v. U.S. Dep't Of Health & Hum. Servs.*, 224 F. Supp. 2d 1115, 1123 (S.D. Tex. 2002), *aff'd*, 67 F. App'x 253 (5th Cir. 2003) (finding Plaintiff's claim that certain medical privacy regulations gave the government "virtually unrestricted access" to medical records in violation of the Fourth Amendment was not ripe for judicial review because "Plaintiffs have not alleged that the government has accessed their medical records pursuant to the" challenged regulations) (internal quotations omitted).

B. Petitioners' Suggestion That Low-Altitude Airspace Is Part of a Person's Property Is Wrong As a Matter of Law.

Finally, in advancing its Fourth Amendment claims, Petitioners assert that the remote ID rule constitutes a "warrantless search of curtilage." Pet. Br. at 22-23. It is not clear whether the Petitioners are referring here to the location of the drone itself in the airspace over property, or merely to the location of the drone operator on land that the operator may own. But Petitioners suggest that the location of the drone in flight is relevant to this claim, arguing that "FAA is requiring drone users flying drones below the tree line in their backyards to broadcast their location while doing so," thereby "demanding access into the very curtilage of private property." *Id*. To the extent that Petitioners are arguing that airspace adjacent to private property is part of that property, this contention rests on a fundamental misunderstanding about the nature of airspace that has dangerous implications for the continued function of the FAA and aviation safety.

In *U.S. v. Causby*, 328 U.S. 256 (1946), the Supreme Court confirmed that real property owners do not have a property right in the adjacent airspace that would allow them to exclude aircraft from flying over that property. Evaluating a takings claim based on frequent, low overflights of large military aircraft using a nearby airfield, the Court explained that compensation is due only when aircraft overflights are "so low and so frequent as to be a direct and immediate interference with the enjoyment and use of the land," thereby constituting a taking. *Id*. at 266. Thus, the

military aircraft operations at issue in *Causby* were an unconstitutional taking because of their effect on the Causbys' chicken farm, not simply because the planes entered the airspace at a low altitude. *See also* Pet. Br. 51-52 (citing *Causby* for the proposition that "the air is a public highway," 328 U.S. at 261). Under the doctrine of aerial trespass, which is based on *Causby* and its progeny, an aircraft must both "enter into the immediate reaches of the air space next to the land" *and* "interfere[] substantially with the [owner's] use of enjoyment of his land" to perpetrate a trespass. Restatement (Second) of Torts § 159(2) (1965) (emphasis added).

This must be so; otherwise, property owners would be able to dictate terms to, or otherwise interfere with, aircraft operating in the national airspace pursuant to FAA regulations and airspace management systems such as air traffic control. Just as low-altitude airspace regulated by the FAA must be considered "navigable airspace," *see* Section III.C., *supra*, that airspace cannot be subject to the ownership or control of millions of private property owners across the country. Such a notion puts the very concept of the national airspace, and a central coordinating and safety authority for that airspace, at risk. It is both inconsistent with precedent and entirely at odds with the exclusive federal control over the airspace of the United States, which is necessary for both aviation safety and air commerce.

Although Petitioners' claims here are grounded in Fourth Amendment jurisprudence and not takings or property-based torts, their arguments about

curtilage have potentially significant implications for legal questions about ownership of the airspace. This Court should reject Petitioners' Fourth Amendment claims for the reasons Respondents provide and because they are unripe, but in any event the Court should avoid endorsing Petitioners' suggestion that property owners possess a right to airspace, or wading into a complex area of property law not squarely raised by this case.

CONCLUSION

AUVSI urges the Court to reject the Petition and uphold the FAA's remote ID rule.

Respectfully Submitted,

/s/ Joshua S. Turner

Joshua S. Turner
Sara M. Baxenberg
WILEY REIN LLP
1776 K Street NW
Washington, DC 20006
(202) 719-7000
jturner@wiley.law
Counsel for the Association for Unmanned Vehicle Systems International

October 12, 2021

RULE 32 CERTIFICATE OF COMPLIANCE

Pursuant to Federal Rules of Appellate Procedure 29(a)(4)(G) and 32(g)(1), I hereby certify that the foregoing brief complies with the type-volume limitation of Rule 32(a)(7)(B). The brief contains 6,486 words, excluding the items excluded from length pursuant to Rule 32(f). The brief also complies with the typeface requirements of Rule 32(a)(5).

Respectfully Submitted,

/s/ Joshua S. Turner

Joshua S. Turner
WILEY REIN LLP
1776 K Street NW
Washington, DC 20006
(202) 719-7000
jturner@wiley.law
Counsel for the Association for Unmanned Vehicle Systems International

October 12, 2021

CERTIFICATE OF SERVICE

I hereby certify that on October 12, 2021, I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the District of Columbia Circuit by using the Court's CM/ECF system, which will serve the filing on all participants in the case who are registered CM/ECF users.

Date: October 12, 2021

Respectfully Submitted,

/s/ Joshua S. Turner

Joshua S. Turner
WILEY REIN LLP
1776 K Street NW
Washington, DC 20006
(202) 719-7000
jturner@wiley.law

ADDENDUM OF PERTINENT STATUTES AND REGULATIONS

ADDENDUM TABLE OF CONTENTS

14 C.F.R. § 107.110

To conduct Category 1 operations -

(a) A remote pilot in command must use a small unmanned aircraft that -

(1) Weighs 0.55 pounds or less on takeoff and throughout the duration of each operation under Category 1, including everything that is on board or otherwise attached to the aircraft; and

(b) Does not contain any exposed rotating parts that would lacerate human skin upon impact with a human being.

(c) No remote pilot in command may operate a small unmanned aircraft in sustained flight over open-air assemblies of human beings unless the operation meets the requirements of either § 89.110 or § 89.115(a) of this chapter.

***

14 C.F.R § 107.115

To conduct Category 2 operations -

(a) A remote pilot in command must use a small unmanned aircraft that -

(1) Is eligible for Category 2 operations pursuant to § 107.120(a);

(2) Is listed on an FAA-accepted declaration of compliance as eligible for Category 2 operations in accordance with § 107.160; and

(3) Is labeled as eligible to conduct Category 2 operations in accordance with § 107.120(b)(1).

(b) No remote pilot in command may operate a small unmanned aircraft in sustained flight over open-air assemblies of human beings unless the operation meets the requirements of either § 89.110 or § 89.115(a) of this chapter.

***

FAA Extension, Safety, and Security Act of 2016, Pub. L. No. 114-190, § 2208, 130 Stat. 633

§ 2208. Unmanned Aircraft Systems Traffic Management.

(a) RESEARCH PLAN FOR UTM DEVELOPMENT AND DEPLOYMENT.—

(1) IN GENERAL.—The Administrator of the Federal Aviation Administration (in this section referred to as the ''Administrator''), in coordination with the Administrator of the National Aeronautics and Space Administration, shall continue development of a research plan for unmanned aircraft systems traffic management (in this section referred to as ''UTM'') development and deployment.

(2) REQUIREMENTS.—In developing the research plan, the Administrator shall—

(A) identify research outcomes sought; and

(B) ensure the plan is consistent with existing regulatory and operational frameworks, and considers potential future regulatory and operational frameworks, for unmanned aircraft systems in the national airspace system.

(3) ASSESSMENT.—The research plan shall include an assessment of the interoperability of a UTM system with existing and potential future air traffic management systems and processes.

(4) DEADLINES.—The Administrator shall—

(A) initiate development of the research plan not later than 60 days after the date of enactment of this Act; and

(B) not later than 180 days after the date of enactment of this Act—

(i) complete the research plan;

(ii) submit the research plan to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science, Space, and Technology and the Committee on Transportation and Infrastructure of the House of Representatives; and

(iii) publish the research plan on the Internet Web site of the Federal Aviation Administration.

(b) PILOT PROGRAM.—

(1) IN GENERAL.—Not later than 90 days after the date of submission of the research plan under subsection (a)(4)(B), the Administrator, in coordination with the Administrator of the National Aeronautics and Space Administration, the Drone Advisory Committee, the research advisory committee established by section 44508(a) of title 49, United States Code, and representatives of the unmanned aircraft industry, shall establish a UTM system pilot program.

(2) SUNSET.—Not later than 2 years after the date of establishment of the pilot program, the Administrator shall conclude the pilot program.

(c) UPDATES.—Not later than 180 days after the date of establishment of the pilot program, and every 180 days thereafter until the date of conclusion of the pilot program, the Administrator shall submit to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science, Space, and Technology and the Committee on Transportation and Infrastructure of the House of Representatives an update on the status and progress of the pilot program.

***

FAA Modernization and Reform Act of 2012, Pub. L. No. 112-95, 126 Stat. 11

§ 332. Integration of Civil Unmanned Aircraft Systems Into National Airspace System.

(a) REQUIRED PLANNING FOR INTEGRATION.—

(1) COMPREHENSIVE PLAN.—Not later than 270 days after the date of enactment of this Act, the Secretary of Transportation, in consultation with representatives of the aviation industry, Federal agencies that employ unmanned aircraft systems technology in the national airspace system, and the unmanned aircraft systems industry, shall develop a comprehensive plan to safely accelerate the integration of civil unmanned aircraft systems into the national airspace system.

(2) CONTENTS OF PLAN.—The plan required under paragraph (1) shall contain, at a minimum, recommendations or projections on—

(A) the rulemaking to be conducted under subsection (b), with specific recommendations on how the rulemaking will—

(i) define the acceptable standards for operation and certification of civil unmanned aircraft systems;

(ii) ensure that any civil unmanned aircraft system includes a sense and avoid capability; and

(iii) establish standards and requirements for the operator and pilot of a civil unmanned aircraft system, including standards and requirements for registration and licensing;

(B) the best methods to enhance the technologies and subsystems necessary to achieve the safe and routine operation of civil unmanned aircraft systems in the national airspace system;

(C) a phased-in approach to the integration of civil unmanned aircraft systems into the national airspace system;

(D) a timeline for the phased-in approach described under subparagraph (C);

(E) creation of a safe

(F) airspace designation for cooperative manned and unmanned flight operations in the national airspace system;

(G) establishment of a process to develop certification, flight standards, and air traffic requirements for civil unmanned aircraft systems at test ranges where such systems are subject to testing;

(H) the best methods to ensure the safe operation of civil unmanned aircraft systems and public unmanned aircraft systems simultaneously in the national airspace system; and

(I) incorporation of the plan into the annual NextGen Implementation Plan document (or any successor document) of the Federal Aviation Administration.

(3) DEADLINE.—The plan required under paragraph (1) shall provide for the safe integration of civil unmanned aircraft systems into the national airspace system as soon as practicable, but not later than September 30, 2015.

(4) REPORT TO CONGRESS.—Not later than 1 year after the date of enactment of this Act, the Secretary shall submit to Congress a copy of the plan required under paragraph (1).

(5) ROADMAP.—Not later than 1 year after the date of enactment of this Act, the Secretary shall approve and make available in print and on the Administration's Internet Web site a 5-year roadmap for the introduction of civil unmanned aircraft systems into the national airspace system, as coordinated by the Unmanned Aircraft Program Office of the Administration. The Secretary shall update the roadmap annually.

(b) RULEMAKING.—Not later than 18 months after the date on which the plan required under subsection (a)(1) is submitted to Congress under subsection (a)(4), the Secretary shall publish in the Federal Register—

(1) a final rule on small unmanned aircraft systems that will allow for civil operation of such systems in the national airspace system, to the extent the systems do not meet the requirements for expedited operational authorization under section 333 of this Act;

(2) a notice of proposed rulemaking to implement the recommendations of the plan required under subsection (a)(1), with the final rule to be published not later than 16 months after the date of publication of the notice; and

(3) an update to the Administration's most recent policy statement on unmanned aircraft systems, contained in Docket No. FAA–2006–25714.

(c) PILOT PROJECTS.—

(1) ESTABLISHMENT.—Not later than 180 days after the date of enactment of this Act, the Administrator shall establish a program to integrate unmanned aircraft systems into the national airspace system at 6 test ranges. The program shall terminate 5 years after the date of enactment of this Act.

(2) PROGRAM REQUIREMENTS.—In establishing the program under paragraph (1), the Administrator shall—

(A) safely designate airspace for integrated manned and unmanned flight operations in the national airspace system;

(B) develop certification standards and air traffic requirements for unmanned flight operations at test ranges;

(C) coordinate with and leverage the resources of the National Aeronautics and Space Administration and the Department of Defense;

(D) address both civil and public unmanned aircraft systems;

(E) ensure that the program is coordinated with the Next Generation Air Transportation System; and

(F) provide for verification of the safety of unmanned aircraft systems and related navigation procedures before integration into the national airspace system.

(3) TEST RANGE LOCATIONS.—In determining the location of the 6 test ranges of the program under paragraph (1), the Administrator shall—

(A) take into consideration geographic and climatic diversity;

(B) take into consideration the location of ground infrastructure and research needs; and

(C) consult with the National Aeronautics and Space Administration and the Department of Defense.

(4) TEST RANGE OPERATION.—A project at a test range shall be operational not later than 180 days after the date on which the project is established.

(5) REPORT TO CONGRESS.—

(A) IN GENERAL.—Not later than 90 days after the date of the termination of the program under paragraph (1), the Administrator shall submit to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Transportation and Infrastructure and the Committee on Science, Space, and Technology of the House of Representatives a report setting forth the Administrator's findings and conclusions concerning the projects.

(B) ADDITIONAL CONTENTS.—The report under subparagraph (A) shall include a description and assessment of the progress being made in establishing special use airspace to fill the immediate need of the Department of Defense—

(i) to develop detection techniques for small unmanned aircraft systems; and

(ii) to validate the sense and avoid capability and operation of unmanned aircraft systems.

(d) EXPANDING USE OF UNMANNED AIRCRAFT SYSTEMS IN ARCTIC.—

(1) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Secretary shall develop a plan and initiate a process to work with relevant Federal agencies and national and international communities to designate permanent areas in the Arctic where small unmanned aircraft may operate 24 hours per day for research and commercial purposes. The plan for operations in these permanent areas shall include the development of processes to facilitate the safe operation of unmanned aircraft beyond line of sight. Such areas shall enable over-water flights from the surface to at least 2,000 feet in altitude, with ingress and egress routes from selected coastal launch sites.

(2) AGREEMENTS.—To implement the plan under paragraph (1), the Secretary may enter into an agreement with relevant national and international communities.

(3) AIRCRAFT APPROVAL.—Not later than 1 year after the entry into force of an agreement necessary to effectuate the purposes of this subsection, the Secretary shall work with relevant national and international communities to establish and implement a process, or may apply an applicable process already established, for approving the use of unmanned aircraft in the designated permanent areas in the Arctic without regard to whether an unmanned aircraft is used as a public aircraft, a civil aircraft, or a model aircraft.

§ 333. Special Rules for Certain Unmanned Aircraft Systems.

(a) IN GENERAL.—Notwithstanding any other requirement of this subtitle, and not later than 180 days after the date of enactment of this Act, the Secretary of Transportation shall determine if certain unmanned aircraft systems may operate safely in the national airspace system before completion of the plan and rulemaking required by section 332 of this Act or the guidance required by section 334 of this Act.

(b) ASSESSMENT OF UNMANNED AIRCRAFT SYSTEMS.—In making the determination under subsection (a), the Secretary shall determine, at a minimum—

(1) which types of unmanned aircraft systems, if any, as a result of their size, weight, speed, operational capability, proximity to airports and populated areas, and operation within visual line of sight do not create a hazard to users of the national airspace system or the public or pose a threat to national security; and

(2) whether a certificate of waiver, certificate of authorization, or airworthiness certification under section 44704 of title 49, United States Code, is required for the operation of unmanned aircraft systems identified under paragraph (1).

(c) REQUIREMENTS FOR SAFE OPERATION.—If the Secretary determines under this section that certain unmanned aircraft systems may operate safely in the national airspace system, the Secretary shall establish requirements for the safe operation of such aircraft systems in the national airspace system.

§336. Special Rule for Model Aircraft.

(a) IN GENERAL.—Notwithstanding any other provision of law relating to the incorporation of unmanned aircraft systems into Federal Aviation Administration plans and policies, including this subtitle, the Administrator of the Federal Aviation Administration may not promulgate any rule or regulation regarding a model aircraft, or an aircraft being developed as a model aircraft, if—

(1) the aircraft is flown strictly for hobby or recreational use;

(2) the aircraft is operated in accordance with a community-based set of safety guidelines and within the programming of a nationwide community-based organization;

(3) the aircraft is limited to not more than 55 pounds unless otherwise certified through a design, construction, inspection, flight test, and operational safety program administered by a community-based organization;

(4) the aircraft is operated in a manner that does not interfere with and gives way to any manned aircraft; and

(5) when flown within 5 miles of an airport, the operator of the aircraft provides the airport operator and the airport air traffic control tower (when an air traffic facility is located at the airport) with prior notice of the operation (model aircraft operators flying from a permanent location within 5 miles of an airport should establish a mutually-agreed upon operating procedure with the airport operator and the airport air traffic control tower (when an air traffic facility is located at the airport)).

(b) STATUTORY CONSTRUCTION.—Nothing in this section shall be construed to limit the authority of the Administrator to pursue enforcement action against persons operating model aircraft who endanger the safety of the national airspace system.

(c) MODEL AIRCRAFT DEFINED.—In this section, the term ‘‘model aircraft’’ means an unmanned aircraft that is—

(1) capable of sustained flight in the atmosphere;

(2) flown within visual line of sight of the person operating the aircraft; and

(3) flown for hobby or recreational purposes.

***

FAA Reauthorization Act of 2018, Pub. L. No. 115-254, § 349(f), 132 Stat. 3186, 3299

§ 349. Exception for Limited Recreational Operations of Unmanned Aircraft.

(a) IN GENERAL.—Chapter 448 of title 49, United States Code, as added by this Act, is further amended by adding at the end the following:

‘‘§ 44809. Exception for limited recreational operations of unmanned aircraft
‘‘(a) IN GENERAL.—Except as provided in subsection (e), and notwithstanding chapter 447 of title 49, United States Code, a person may operate a small unmanned aircraft without specific certification or operating authority from the Federal Aviation Administration if the operation adheres to all of the following limitations:

‘‘(1) The aircraft is flown strictly for recreational purposes.

‘‘(2) The aircraft is operated in accordance with or within the programming of a community-based organization’s set of safety guidelines that are developed in coordination with the Federal Aviation Administration.

‘‘(3) The aircraft is flown within the visual line of sight of the person operating the aircraft or a visual observer colocated and in direct communication with the operator.

‘‘(4) The aircraft is operated in a manner that does not interfere with and gives way to any manned aircraft.

‘‘(5) In Class B, Class C, or Class D airspace or within the lateral boundaries of the surface area of Class E airspace designated for an airport, the operator obtains prior authorization from the Administrator or designee before operating and complies with all airspace restrictions and prohibitions.

‘‘(6) In Class G airspace, the aircraft is flown from the surface to not more than 400 feet above ground level and complies with all airspace restrictions and prohibitions.

‘‘(7) The operator has passed an aeronautical knowledge and safety test described in subsection (g) and maintains proof of test passage to be made available to the Administrator or law enforcement upon request.

‘‘(8) The aircraft is registered and marked in accordance with chapter 441 of this title and proof of registration is made available to the Administrator or a designee of the Administrator or law enforcement upon request.

‘‘(b) OTHER OPERATIONS.—Unmanned aircraft operations that do not conform to the limitations in subsection (a) must comply with all statutes and regulations generally applicable to unmanned aircraft and unmanned aircraft systems.

‘‘(c) OPERATIONS AT FIXED SITES.—

‘‘(1) OPERATING PROCEDURE REQUIRED.—Persons operating unmanned aircraft under subsection (a) from a fixed site within Class B, Class C, or Class D airspace or within the lateral boundaries of the surface area of Class E airspace designated for an airport, or a community-based organization conducting a sanctioned event within such airspace, shall make the location of the fixed site known to the Administrator and shall establish a mutually agreed upon operating procedure with the air traffic control facility.

‘‘(2) UNMANNED AIRCRAFT WEIGHING MORE THAN 55 POUNDS.—A person may operate an unmanned aircraft weighing more than 55 pounds, including the weight of anything attached to or carried by the aircraft, under subsection (a) if—

‘‘(A) the unmanned aircraft complies with standards and limitations developed by a community-based organization and approved by the Administrator; and

‘‘(B) the aircraft is operated from a fixed site as described in paragraph (1).

‘‘(d) UPDATES.—

‘‘(1) IN GENERAL.—The Administrator, in consultation with government, stakeholders, and community-based organizations, shall initiate a process to periodically update the operational parameters under subsection (a), as appropriate.

‘‘(2) CONSIDERATIONS.—In updating an operational parameter under paragraph (1), the Administrator shall consider—

‘‘(A) appropriate operational limitations to mitigate risks to aviation safety and national security, including risk to the uninvolved public and critical infrastructure;

‘‘(B) operations outside the membership, guidelines, and programming of a community-based organization;

‘‘(C) physical characteristics, technical standards, and classes of aircraft operating under this section;

‘‘(D) trends in use, enforcement, or incidents involving unmanned aircraft systems;

‘‘(E) ensuring, to the greatest extent practicable, that updates to the operational parameters correspond to, and leverage, advances in technology; and

‘‘(F) equipage requirements that facilitate safe, efficient, and secure operations and further integrate all unmanned aircraft into the national airspace system.

‘‘(3) SAVINGS CLAUSE.—Nothing in this subsection shall be construed as expanding the authority of the Administrator to require a person operating an unmanned aircraft under this section to seek permissive authority of the Administrator, beyond that required in subsection (a) of this section, prior to operation in the national airspace system.

‘‘(e) STATUTORY CONSTRUCTION.—Nothing in this section shall be construed to limit the authority of the Administrator to pursue an enforcement action against a person operating any unmanned aircraft who endangers the safety of the national airspace system.

‘‘(f) EXCEPTIONS.—Nothing in this section prohibits the Administrator from promulgating rules generally applicable to unmanned aircraft, including those unmanned aircraft eligible for the exception set forth in this section, relating to—

‘‘(1) updates to the operational parameters for unmanned aircraft in subsection (a);

‘‘(2) the registration and marking of unmanned aircraft;

‘‘(3) the standards for remotely identifying owners and operators of unmanned aircraft systems and associated unmanned aircraft; and

‘‘(4) other standards consistent with maintaining the safety and security of the national airspace system.

‘‘(g) AERONAUTICAL KNOWLEDGE AND SAFETY TEST.—

‘‘(1) IN GENERAL.—Not later than 180 days after the date of enactment of this section, the Administrator, in consultation with manufacturers of unmanned aircraft systems, other industry stakeholders, and community-based organizations, shall develop an aeronautical knowledge and safety test, which can then be administered electronically by the Administrator, a community-based organization, or a person designated by the Administrator.

‘‘(2) REQUIREMENTS.—The Administrator shall ensure the aeronautical knowledge and safety test is designed to adequately demonstrate an operator’s—

‘‘(A) understanding of aeronautical safety knowledge; and

‘‘(B) knowledge of Federal Aviation Administration regulations and requirements pertaining to the operation of an unmanned aircraft system in the national airspace system.

‘‘(h) COMMUNITY-BASED ORGANIZATION DEFINED.—In this section, the term ‘community-based organization’ means a membership-based association entity that—

‘‘(1) is described in section 501(c)(3) of the Internal Revenue Code of 1986;

‘‘(2) is exempt from tax under section 501(a) of the Internal Revenue Code of 1986;

‘‘(3) the mission of which is demonstrably the furtherance of model aviation;

‘‘(4) provides a comprehensive set of safety guidelines for all aspects of model aviation addressing the assembly and operation of model aircraft and that emphasize safe aeromodelling operations within the national airspace system and the protection and safety of individuals and property on the ground, and may provide a comprehensive set of safety rules and programming for the operation of unmanned aircraft that have the advanced flight capabilities enabling active, sustained, and controlled navigation of the aircraft beyond visual line of sight of the operator;

‘‘(5) provides programming and support for any local charter organizations, affiliates, or clubs; and

‘‘(6) provides assistance and support in the development and operation of locally designated model aircraft flying sites.

‘‘(i) RECOGNITION OF COMMUNITY-BASED ORGANIZATIONS.—In collaboration with aeromodelling stakeholders, the Administrator shall publish an advisory circular within 180 days of the date of enactment of this section that identifies the criteria and process required for recognition of community-based organizations.’’.

(b) TECHNICAL AND CONFORMING AMENDMENTS.—

(1) TABLE OF CONTENTS.—The table of contents for chapter 448 of title 49, United States Code, as added by this Act, is further amended by adding at the end the following:

‘‘44809. Exception for limited recreational operations of unmanned aircraft.’’.

(2) REPEAL.—Section 336 of the FAA Modernization and Reform Act of 2012 (49 U.S.C. 40101 note) and the item relating to that section in the table of contents under section 1(b) of that Act are repealed.

***

National Defense Authorization Act for Fiscal Year 2012, Pub. L. No. 112-81, § 1097, 125 Stat. 1298, 1608-09f

§ 1097. Unmanned Aerial Systems and National Airspace.

(a) ESTABLISHMENT.—Not later than 180 days after the date of the enactment of this Act, the Administrator of the Federal Aviation Administration shall establish a program to integrate unmanned aircraft systems into the national airspace system at six test ranges.

(b) PROGRAM REQUIREMENTS.—In establishing the program under subsection (a), the Administrator shall—

(1) safely designate nonexclusionary airspace for integrated manned and unmanned flight operations in the national airspace system;

(2) develop certification standards and air traffic requirements for unmanned flight operations at test ranges;

(3) coordinate with and leverage the resources of the Department of Defense and the National Aeronautics and Space Administration;

(4) address both civil and public unmanned aircraft systems;

(5) ensure that the program is coordinated with the Next Generation Air Transportation System; and

(6) provide for verification of the safety of unmanned aircraft systems and related navigation procedures before integration into the national airspace system.

(c) LOCATIONS.—In determining the location of a test range for the program under subsection (a), the Administrator shall—

(1) take into consideration geographic and climatic diversity;

(2) take into consideration the location of ground infrastructure and research needs; and

(3) consult with the Department of Defense and the National Aeronautics and Space Administration.

(d) TEST RANGE OPERATION.—A project at a test range shall be operational not later than 180 days after the date on which the project is established.

(e) REPORT.—Not later than 90 days after the date of completing each of the pilot projects, the Administrator shall submit to the appropriate congressional committees a report setting forth the Administrator's findings and conclusions concerning the projects that includes a description and assessment of the progress being made in establishing special use airspace to fill the immediate need of the Department of Defense to develop detection techniques for small unmanned aircraft systems and to validate sensor integration and operation of unmanned aircraft systems.

(f) DURATION.—The program under subsection (a) shall terminate on the date that is five years after the date of the enactment of this Act.

(g) DEFINITION.—In this section:

(1) The term ''appropriate congressional committees'' means—

(A) the Committee on Armed Services, the Committee on Transportation and Infrastructure, and the Committee on Science, Space, and Technology of the House of Representatives; and

(B) the Committee on Armed Services and the Committee on Commerce, Science, and Transportation of the Senate.

(2) The term ''test range'' means a defined geographic area where research and development are conducted.

***

ORAL ARGUMENT SCHEDULED FOR DECEMBER 15, 2021

No. 21-1087

IN THE UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

TYLER BRENNAN AND RACEDAYQUADS LLC,
Petitioners

v.

STEPHEN DICKSON, ADMINISTRATOR, AND FEDERAL AVIATION ADMINISTRATION,
Respondents

On Petition for Review of a Final Rule of the Federal Aviation Administration

---

ADDENDUM OF ADMINISTRATIVE RECORD MATERIALS CITED BY *AMICUS CURIAE* ASSOCIATION FOR UNMANNED VEHICLE SYSTEMS INTERNATIONAL

Joshua S. Turner
Sara M. Baxenberg
WILEY REIN LLP
1776 K Street NW
Washington, DC 20554 (202)
719-7000
jturner@wiley.law
Counsel for the Association for Unmanned Vehicle Systems International

October 12, 2021

Table of Contents

DEPARTMENT OF TRANSPORTATION
Federal Aviation Administration

Remote Identification of Unmanned Aircraft Systems

14 CFR Parts 1, 47, 48, 89, 91 and 107

Notice of Proposed Rulemaking

Docket No. FAA-2019-1100; Notice 20-01

RIN 2120-AL31

COMMENTS OF AT&T SERVICES, INC.

AT&T Services, Inc., on behalf of itself and its affiliates (together, "AT&T"), respectfully submits these comments in response to the *Notice of Proposed Rulemaking ("NPRM")* in the above-referenced proceeding. In that *NPRM,* the Federal Aviation Administration seeks comment on proposed rules that would require the remote identification of unmanned aircraft systems ("UAS") to "address safety, national, security and law enforcement concerns regarding the further integration of these aircraft into the airspace of the United States while also enabling greater operational capabilities" of the UAS themselves.[1]

AT&T is a global leader in telecommunications, media, entertainment and technology. The company offers one of the most advanced and powerful global backbone networks, provides wireless service to millions of customers with voice coverage and data roaming in hundreds of countries, is one of the largest providers of IP-based communications services for businesses, and is a global leader in delivering a full portfolio of end-to-end reliable and highly secure network, voice, data and IP solutions to its customers. AT&T also is at the cutting edge of

[1] *Remote Identification of Unmanned Aircraft Systems*, Notice of Proposed Rulemaking, 84 Fed. Reg. 72438 (Dec. 31, 2019).

innovation in bringing the Internet of Things to the nation's consumers and businesses. And through Warner Media, we deliver popular content to global audiences from a diverse array of talented storytellers and journalists.

In all of those undertakings UAS represent a key component of AT&T's current operations and of its vision for the future. AT&T thus has a significant interest in the FAA's efforts to further integrate UAS into the national airspace through this rulemaking. Indeed, AT&T affiliate CNN, which has been a trailblazer in the use of UAS in its newsgathering operations, has been a vocal proponent of the need for appropriate remote ID requirements.

The *NPRM* properly focuses on the vital importance of remote ID regulations in contributing to safety and security and how the rules will consequently facilitate that integration. These regulations, if promptly and properly implemented, should allow for increasingly complex UAS operations, including operation beyond visual line of sight ("BVLOS") and flight over people. Robust and well-structured remote ID rules will also allow the FAA and other law enforcement agencies to differentiate between cooperative and non-cooperative UAS and, where authorized, allow authorities to implement appropriate UAS counter-measures.

Given the importance of safety and security to ongoing UAS airspace integration, the *NPRM* has properly opted for network remote ID solutions that can be satisfied using secure cellular technologies, which have the added virtue of being widely deployed at scale across the United States. Commercial wireless networks are enabled through secure and reliable licensed spectrum that a wide variety of users, including law enforcement, already trust to authenticate users and devices through International Mobile Equipment Identity ("IMEI") technology. Network operators employ a variety of measures at the network, device, and applications layers

recover AT&T voice and data service network elements and restore communications to an area affected by disaster. The NDR team has a fleet that includes hundreds of technology recovery and support trailers that can be deployed quickly to support customers and first responders by restoring communications when infrastructure has been damaged. AT&T's Flying COW™ (Cell on Wings) is now a standard part of AT&T's NDR fleet. The Flying COW™ functions as an LTE cell site on a drone and can provide wireless connectivity to consumers and first responders on the ground. AT&T has deployed its Flying COWs™ in response to hurricanes in Puerto Rico, North Carolina, and Florida. Most recently, AT&T's Flying COWs™ stood ready to deploy in the aftermath of Hurricane Dorian.[4]

The final rules adopted in this proceeding should provide special consideration for these and other disaster recovery and public safety operations. For example, AT&T deploys its Flying COW™ when internet is not available for the purpose of providing connectivity to consumers and first responders. If the internet is not available at takeoff and the operator can no longer broadcast the remote ID message elements, the proposed rules would require AT&T to land its Flying COW™ "as soon as practicable." However, if a Flying COW™ is providing connectivity for first responders, whether it be firefighters responding to a structure fire or wildfire, or police responding to an active shooter or to a bomb detonation, and it is required to land, the first responders would lose connectivity, which could jeopardize the mission and place public safety at risk.

The *NPRM* would also prohibit the use of ADS-B Out equipment unless the operation is conducted under a flight plan and the operator maintains two-way communication with Air

[4]https://www.faa.gov/news/updates/?newsId=89185&omniRss=news_updatesAoc&cid=101_N_U

1400 N. Hurstbourne Parkway
Louisville, KY 40223
502.329.3000 Tel

March 2, 2020

Docket Operations, M–30
U.S. Department of Transportation (DOT)
1200 New Jersey Avenue SE
Room W12–140, West Building Ground Floor
Washington, DC 20590–0001

Re: Comments of UPS Flight Forward and United Parcel Service Co. to FAA Notice of Proposed Rulemaking for Remote Identification of Unmanned Aircraft Systems FAA Docket No.: FAA-2019-1100

UPS Flight Forward ("UPSFF") and United Parcel Service Co. ("UPS Airlines"), by and through counsel, present their comments on the FAA Notice of Proposed Rulemaking for Remote Identification of Unmanned Aircraft Systems – FAA Docket No.: FAA-2019-1100 ("NPRM").

For your convenience, these comments are organized as follows:

I. INTRODUCTION

UPSFF is on the cutting edge of UAS operations in the United States, and is the nation's first recipient of a 14 C.F.R. Part 135 standard certificate to operate UAS-based delivery services. Flight Forward currently operates a nascent delivery service supporting hospital campuses in the United States. Flight Forward's pilot programs deliver medical products between locations on a hospital campus using Matternet UAS operating at low altitudes. UPSFF is actively working with FAA to expand its operations and in the future, will offer time-critical delivery of medical and other supplies in locations across the United States. UPSFF understands the complex hurdles confronting the FAA and law enforcement as UAS are fully integrated into the National Airspace System (NAS). Among the most critical of these is the ability to remotely identify unmanned aircraft.

UPS Airlines is a Part 121 certificated airline and serves more destinations than any air carrier in the world. UPS Airlines' aircraft fly over 2,300 flight segments every day. UPS Airlines' rapid, efficient, and reliable air cargo and express service is a critical element of the national and international infrastructure for commerce, and the nation's economic strength. UPS Airlines' extensive air operations give it a unique perspective on the needs of air commerce, use of the nation's airspace and flight safety.

Based on these unique perspectives, UPSFF and UPS Airlines offer their comments to the FAA's Notice of Proposed Rulemaking for Remote Identification of Unmanned Aircraft.

II. SUMMARY

UPSFF and UPS Airlines support the goals of the NPRM. The comprehensive approach proposed to remote identification will provide a solid cornerstone on which the other elements of complex UAS operations will be built. The NPRM will support the development of the unmanned traffic system required for BVLOS operation and provide the security necessary to enforce the rules for flight over people. UPSFF and UPS Airlines agree that the FAA must utilize a technology based solution to this problem that includes the imposition of design requirements and a comprehensive system of oversight of design and production of unmanned aircraft.

Finally, it is clear that the public will not accept widespread use of UAS without some method of remotely identifying aircraft. If illegal and unsafe operators cannot be identified and stopped, confidence in the system will be eroded and voluntary compliance will be undermined. The NPRM is tailored to meet these goals, and will lead to broader acceptance of UAS services by the public.

III. STANDARD REMOTE ID OPERATIONS

UPSFF and UPS Airlines support the adoption of a performance based approach to remote identification. UAS technology is still progressing at a rapid pace, and the adoption of a rigid standard or methodology for remote identification runs the risk of foreclosing work on promising new approaches to the problems. Also, a performance-based approach leaves the industry free to seek cost-effective design solutions that can leverage emerging technologies without having to rely on additional rulemakings to accommodate their adoption.

UPSFF and UPS Airlines support the FAA's decision to apply the Remote ID standard to all unmanned aircraft weighing in excess of .55 pounds, and not providing any regulatory carve-out for hobby aircraft. The safety and security concerns that surround unmanned aircraft operations are not dependent on whether the aircraft is operated for recreation or for a commercial purpose. The risk comes from the physical characteristics of the aircraft and the manner in which it is flown. Creating an arbitrary distinction between hobby and commercial aircraft would only serve to undermine the public's trust in the efficacy of the remote ID system and would provide potential loopholes for individuals to exploit.

While there will be an additional cost associated with requiring legacy UAS to comply with the requirements of the remote ID system, the benefits of a fully compliant air fleet outweigh these additional costs.

UPSFF and UPS Airlines agree that the radio transmission requirement utilizing an FCC Part 15 device capable of broadcasting at maximum range is a suitable initial solution for this problem. However, the FAA should, in coordination with the FCC, determine if additional spectrum for higher power broadcast can be made available. The limited range of Part 15 devices, accompanied with the potential issues of interference between similarly situated operators, potentially makes this a sub optimal solution. UPSFF and UPS Airlines do not believe, however, that there would be any justification for delaying the current rulemaking to pursue an additional solution. Rather, the current rulemaking should proceed as expeditiously as possible while other alternatives continue to be explored.

IV. STANDARD REMOTE ID OPERATIONS - INTERNET CONNECTIVITY

While UPSFF and UPS Airlines agree that operation of the Remote ID system on both broadcast signals and the internet provides a robust framework for operations and future growth, the FAA should keep a flexible approach to the internet component under certain circumstances.

UAS have proven that they can offer extremely valuable, even lifesaving, services in remote locations and during recovery from a natural disaster. In the aftermath of an earthquake or hurricane, extended power failures and physical damage will affect cellular communications, making an internet connection difficult or impossible. Under such circumstances, the flights will often occur in an internet-deprived area. In addition, under such circumstances, even if a connection can be established, the lack of system capacity and increased demand on the operating parts of the system will make communications unreliable or increase latency beyond the point at which internet transmitted remote ID data is reliable.

The FAA should, therefore, ensure that the requirement for internet connectivity does not become a bottleneck that hampers the ability to use UAS under such exigent circumstances.

V. REGISTRATION REQUIREMENTS

UPSFF and UPS Airlines support the proposed changes to the UAS registration requirements. The safety and reliability of UAS operations in the NAS require that each aircraft be reliably identified and matched to its operator. While the current system for hobby registration is adequate for operation in a system where UAS are strictly

Wing

Comments of Wing Aviation LLC on the Notice of Proposed Rulemaking for Remote Identification of Unmanned Aircraft Systems (FAA-2019-1100)

March 2020

c. The rule should permit operators to shield their control station position from public observers when transmitting via Remote ID USS. This message element would be available to the FAA.

d. The rule should outline a legal process governing access to retained data if that data is directly or indirectly identifiable. Access should be limited to certain purposes related to compliance, accident investigation, and security. The use of aggregated data should be subject to strict de-identification protocols.

3. **The rule should support all airspace users.** Hobbyists should be able to share the skies. Standard and Limited categories should be distinguished based on relevant risk factors. Design and production requirements should apply only to highly automated UAS that are produced for sale to third parties or commercial use. Limited UAS should mean UAS not subject to these requirements. Limited UAS operators should be permitted to declare their flight intent via a Remote ID USS, similar to declarations for access to controlled airspace under the FAA's Low Altitude Authorization and Notification Capability (LAANC).

4. **The rule should adopt consensus standards for message elements.** Message elements should be aligned to the ASTM International 'Standard for Remote ID and Tracking' (ASTM standard) to reflect established industry consensus about the feasibility and effectiveness of particular message elements, such as barometric altitude and emergency status.

5. **The rule should expand and clarify exceptions.** Community based organizations should be permitted to apply for and renew FAA-recognized identification areas beyond 12 months. Further, the final rule should outline factors that weigh in favor of an authorized exception for aeronautical research.

Background

Wing is an Alphabet company that enables delivery by UAS. Wing has developed a lightweight, electric, and highly automated aircraft to deliver small goods to customers, and a set of UTM capabilities to help operators share the airspace. Wing began in 2012 within X, formerly Google X, and became an independent Alphabet company in 2018.

Today, Wing provides commercial delivery services in the United States (Christiansburg, VA), Australia (Mitchell, ACT and Logan, QLD), and Finland (Helsinki). Globally, Wing has undertaken over 80,000 flights, including commercial deliveries. Wing holds relevant approvals in each jurisdiction, including the first FAA air carrier certificate under Part 135 for commercial UAS delivery operations beyond visual line of sight (BVLOS).

In addition, Wing is a participant in the FAA UAS Integration Pilot Program (IPP); the FAA UTM Pilot Program (UPP); National Aeronautics and Space Administration (NASA) Technology Capability Level (TCL) demonstrations for UTM; LAANC; and the FAA Drone Advisory Committee.

Comments

Wing agrees that remote ID will help to lay the foundation for advanced UTM capabilities. A scalable approach to UTM is necessary to support the expected volume and diversity of UAS. Like the FAA, Wing anticipates a network of interoperable USS that communicate digitally for a range of purposes, including remote ID and strategic deconfliction. Remote ID will be the first implementation of real time information sharing via this network, and will help to establish an ecosystem that supports additional UAS services.

Further, Wing agrees that safety and security are paramount. Remote ID is an important capability that will help the FAA and law enforcement to identify and respond to potential threats. It will improve accountability, promote compliant UAS operations, and encourage public acceptance of UAS technology.

However, the draft rule poses a number of challenges. In particular, the NPRM claims that remote ID will enable other capabilities, such as detect-and-avoid (DAA). Wing believes that DAA will depend on a range of different technologies in different environments, and it should be the subject of an independent rulemaking process. The expectation that remote ID will enable DAA gives rise to unnecessary or unduly onerous requirements. As drafted, the rule will impose prescriptive and duplicative obligations on UAS operators (see *I. The rule should identify required performance*); compromise privacy (see *II. The rule should mitigate risks to privacy*); and make compliance difficult or impossible for hobbyists (see *III. The rule should support all airspace users*) with negligible benefits for effective remote ID.

Wing believes that remote ID should serve three specific and clearly-defined functions. It can support regulatory compliance and enforcement; facilitate the investigation of accidents and serious incidents; and help law enforcement to detect and respond to security threats. Wing is confident that modest amendments will achieve these objectives in a way that supports diverse UAS, protects privacy, and offers viable pathways to compliance for all airspace users (see *Annex B: Detailed recommendations).*

I. The rule should identify required performance

The airspace supports a diverse range of UAS operations with different aircraft characteristics, different privacy considerations, and different operating environments. Different remote ID systems may be more appropriate for different operations. To that end, the rule should permit operators to choose between network or broadcast remote ID, subject to meeting the required performance for message content, frequency, latency, and accuracy in their specific operating environment.

IV. The rule should adopt consensus standards for message elements

Barometric altitude of aircraft

Wing recommends amending the requirement for Standard UAS to share barometric altitude referenced to standard sea level. First, Wing recommends that the rule should adopt WGS 84 as the altitude reference system for determining the UAS altitude. That approach is consistent with the ASTM standard and all NASA TCL, FAA UPP, and FAA IPP activities to date. WGS 84 provides a method to determine altitude that, with appropriate sensors, is independent of time- and location-specific atmospheric conditions. With a terrain and building structures database, WGS 84 supports translation to Above Ground Level, which is the reference system used to specify altitude limits in Part 107 (specifically §107.51(b)).

Second, Wing recommends that the rule should adopt a performance-based approach to sensor requirements. The rule should permit UAS operators to use any sensor or suite of sensors to measure altitude against the WGS 84 reference system, subject to meeting performance requirements for accuracy. Operators may use GPS, barometric sensors, vision-based sensors, or any other combination of sensors to improve the altitude estimate. Manufacturers would be required to demonstrate that the sensor or sensors deliver the required accuracy performance across the intended operating range.

Wing recommends against barometric sensors. Wing has surveyed a number of barometric sensors in the course of research and development. At this scale, barometric sensors are highly vulnerable to error (beyond the manufacturer's declared accuracy) depending on orientation, exposure to light, or plumbing within the aircraft. The infrastructure required to ensure a stable and accurate reading may be heavier, more complex, and more costly than the sensor itself. In the absence of a regular, standardized, and costly calibration process, undetected errors may develop. These characteristics make barometric sensors unsuitable for many UAS operations.

Affordable barometric sensors cannot deliver the required accuracy						
Manufacturer	**Model**	**Cost**	**Actual accuracy (total error band)**	**Error in Pa +/-**	**Error in ft +/-**	**Rated temperature**
Bosch	BME680	$12.80	0.05%	60	20	Rated to 0°C only
ST Micro	LPS22HB	$2.92	0.08%	100	33	
ST Micro	LPS25HB	$4.05	0.08%	100	33	
ST Micro	LPS33HW	$6.28	0.08%	100	33	
Infineon	DPS310	$2.89	0.08%	100	33	
TDK/InvenSense	ICP-10101	$4.30	0.09%	100	33	
Bosch	BMP280	$3.48	0.09%	100	33	Rated to

- It can be difficult to measure air pressure in a UA since the rotors could be quite close to the pressure sensors and cause constant changes in pressure. In a normal aircraft the sensors are far away from the propellers.

Other height measurement sensors, eg. sound, light, radio or a geodetic approach, could be more accurate than a barometric one.

Barometric altitude of control station

Many control stations are not equipped to measure barometric altitude, and Wing contends that this information is either unnecessary or does not correspond to actual position. In general, the latitude and longitude will enable law enforcement to easily identify the control station. For control stations located in structures above ground level, barometric altitude will fluctuate significantly based on ventilation, climate control, and local airflow. Barometric sensors are not capable of a stable and accurate measurement in these conditions. Even if they were capable, the proposed accuracy of 20ft per means that the reported control station position could be multiple storeys above or below the actual position. If required, operators should be permitted to use any sensor or suite of sensors to measure the altitude, including GPS, subject to reasonable performance requirements for accuracy.

Emergency status

In addition, "emergency status" is an ambiguous message element. A UAS should not be required to transmit non-critical, off-nominal conditions that do not affect compliance or security. For example, a highly automated UAS may be highly tolerant of interruptions in the communication link, and should not be required to treat these conditions as an "emergency". The message element should be clarified to mean critical emergencies that affect compliance and security without including non-critical conditions.

V. The rule should expand and clarify exceptions

Community based organizations (CBOs) should be permitted to apply for an FAA-recognized identification area beyond 12 months, subject to meeting the eligibility requirements in § 89.205 and § 89.215. The area should be renewable following the expiration period. For CBO-affiliated members, FAA-recognized identification areas will be the only way to continue to fly if they cannot comply with other remote ID requirements. Subject to maintaining appropriate procedures and mitigations, there is no compelling reason to refuse applications for new, temporary, or renewed FAA-recognized identification areas following commencement of the rule.

Wing also encourages the FAA to consider extending the eligibility criteria for FAA-recognized identification areas. The FAA should permit a range of organizations to make an application, such as schools. The definition of a CBO (a "membership-based association entity… the mission of which is demonstrably the furtherance of model aviation") may be highly restrictive, and may

exclude a range of other community-oriented entities or educational institutions from establishing FAA-recognized identification areas, even if they can demonstrate comparable procedures and mitigations as a CBO.

In addition, the rule should outline the factors that weigh in favor of an authorized exemption for "aeronautical research". It is essential that commercial designers and manufacturers can test aircraft in a controlled environment without carrying ancillary equipage. Relevant factors include research and development operations (whether commercial, government, or not-for-profit) that are conducted on access-controlled property known to the FAA, with effective mitigations in place to ensure containment of the operation.

Conclusion

Remote ID is an essential capability that will help to support compliance, accident investigation, and security. Wing is confident that remote ID can be implemented in a way that meets these objectives while supporting diverse UAS, protecting legitimate privacy interests, and enabling hobbyists to continue sharing the skies. Together, the proposed changes will help to maximize opportunities for compliance, improving safety and security outcomes for all airspace users.

March 2, 2020

Submitted Electronically

The Honorable Elaine L. Chao
Secretary, U.S. Department of Transportation
1200 New Jersey Avenue, SE
Washington, D.C. 20590

The Honorable Stephen Dickson
Administrator, Federal Aviation Administration
800 Independence Avenue, SW
Washington, D.C. 20591

SUBJECT: **Comments of Skydio, Inc. on the NPRM regarding Remote Identification of Unmanned Aircraft Systems in Docket No. FAA-2019-1100**

Skydio, Inc. ("Skydio") welcomes the opportunity to comment on the Notice of Proposed Rulemaking (NPRM) on the remote identification of unmanned aircraft systems (UAS) in the United States. Skydio supports the development of a regulatory system designed to enable expanded drone operations—for both recreational and commercial operators—within a framework that promotes safety, provides accountability and protects privacy. Remote identification plays an important role in achieving that objective. Although Skydio supports the need to establish a system of remote identification, we believe that system should maximize the

flexibility of operators to fly for business or for fun. The rule should also account for advanced technology capable of making unmanned flight safer than ever before—especially the ability to see and avoid obstacles in the environment. Based on this unique perspective and experience designing, building and flying UAS, Skydio submits the following comments to Docket No. FAA-2019-1100.

I. BACKGROUND ON SKYDIO

Based in Redwood City, California, Skydio is the leading and largest U.S. drone manufacturer. Skydio is dedicated to making drones more useful than ever by making them smarter than ever. Co-founded by former MIT classmates and the first engineers on Google X's Project Wing, Skydio builds drones from the ground up for autonomy, leveraging advances in artificial intelligence and computer vision technology.

Released in 2018, Skydio's first product, the R1, was widely regarded as a breakthrough in autonomous drones for consumers and as a platform for commercial development. Building on that foundation, Skydio released its second product, the Skydio 2, in October 2019. Skydio 2 packs next-generation artificial intelligence into a small, affordable and powerful UAS. Utilizing 45 megapixels of visual sensing from six 200-degree color cameras, Skydio 2 sees its surroundings in every direction with unprecedented resolution and clarity. Fueled by an onboard supercomputer, Skydio 2's autonomy engine uses that imagery to make intelligent decisions about its location, nearby objects and terrain, and flight path.

Skydio 2 has attracted incredible interest across the consumer and commercial markets. Since October, we have manufactured and delivered thousands of units in the United States and select countries overseas. Although we have scaled our production processes, we continue to face unprecedented demand. The level of demand is easy to understand. The last decade of drone development has been defined by manually flown drones that depend on pilots to see and avoid obstacles. Consumer and commercial operators have long dreamed of a drone smart enough to sense and avoid obstacles and navigate complex environments without direct control inputs from a human pilot. Skydio 2 delivers on that dream.

should permit operators to comply with the remote ID standard based on the type of operation. That would allow OEMs to produce drones for the widest possible market, providing the best opportunity to compete domestically and overseas.

Harmonizing the remote ID rule across borders would alleviate burdens on manufacturers and operators alike. As a manufacturer of UAS used in the U.S. and abroad, Skydio urges the FAA to harmonize the Final Rule on remote ID, as appropriate, with rules and standards promulgated by other countries. If countries adopt separate or conflicting design/production/ performance rules and standards for remote ID, manufacturers will find it difficult to service the global marketplace. High compliance costs will have the most significant impact on smaller companies, potentially limiting the global competitiveness of many American manufacturers.

Skydio welcomes FAA's expression of intent "to rely increasingly on consensus standards as FAA-accepted means of compliance for UAS performance-based regulations for remote identification, consistent with FAA precedent for general aviation aircraft and other initiatives taken with respect to UAS."[31] Consistent with AUVSI's comments on this rulemaking, harmonized regulations will allow manufacturers and operators to build to a single set of standards globally and will encourage consistency and compliance. For this reason, performance requirements and message elements should generally be aligned with the ASTM standard, consistent with industry consensus. As discussed above, in the event FAA does seek full alignment with the ASTM standard, Skydio asks only that the FAA acknowledge and permit operations that leverage advanced awareness technology like computer vision to operate in areas without reliable GPS connectivity.

D. Allowing Retrofit Solutions

Finally, in the spirit of enabling flexibility for operators and lowering the costs of compliance, the FAA should allow retrofit solutions. In the Preamble, the FAA predicts that most UAS would be able to meet the Final Rule's requirements by retrofits involving software and related updates. The ability for operators to retrofit UAS would increase efficiencies, enable the continued use of older UAS, and ensure greater compliance with the Final Rule.

[31] *Id.* at 72472.

Before the
FEDERAL AVIATION ADMINISTRATION
Washington, DC 20590

In the matter of Remote Identification of Unmanned Aircraft Systems	Docket No. FAA-2019-1100

COMMENTS OF THE ASSOCIATION FOR UNMANNED VEHICLE SYSTEMS INTERNATIONAL

The Association for Unmanned Vehicle Systems International ("AUVSI")[1] applauds the Federal Aviation Administration ("FAA") for promulgating this Notice of Proposed Rulemaking on Remote Identification of Unmanned Aircraft Systems ("NPRM").[2] The FAA and other stakeholders have long viewed the remote identification ("remote ID") of unmanned aircraft systems ("UAS") as a prerequisite to the broader deployment and expanded operations of UAS, and AUVSI has strongly and consistently supported its expedient implementation. AUVSI agrees that rapid adoption of remote ID is critical to help drive public acceptance of UAS, answer legitimate security concerns raised by law enforcement and security agencies, and help pave the way for expanded and more complex operations. AUVSI also concurs with the FAA's assessment that remote ID lays the groundwork for a future UAS Traffic Management ("UTM") system, which

[1] AUVSI is the world's largest nonprofit organization dedicated to the advancement of unmanned systems and robotics and represents corporations and professionals from more than 60 countries involved in industry, government, and academia. AUVSI members work in the defense, civil, and commercial markets.
[2] *See* Remote Identification of Unmanned Aircraft Systems, 84 Fed. Reg. 72438 (Dec. 31, 2019) (to be codified at 14 C.F.R. pts. 1, 47, 48, 89, 91, and 107) ("*NPRM*").

BEFORE THE
DEPARTMENT OF TRANSPORTATION
WASHINGTON, D.C. 20590

In the Matter of	)	
	)	
Remote Identification of Unmanned Aircraft Systems	)	Docket No. FAA-2019-1100
	)	

To: Federal Aviation Administration

COMMENTS OF LOCKHEED MARTIN CORPORATION

Lockheed Martin Corporation ("Lockheed Martin") hereby responds to the Department of Transportation/Federal Aviation Administration ("FAA") notice seeking comment on proposed rules that would require the remote identification of unmanned aircraft systems ("UAS") operating in United States airspace.[1]

Lockheed Martin is an industry leader in the design and development of unmanned aircraft and the systems architecture to support UAS operations. Lockheed Martin's unmanned products reflect a wide variety of unmanned aircraft size and capabilities that are designed to operate across all classes of airspace in the United States, with different performance and operational characteristics. We recognize that a crucial commonality of these operations is the need for consistent and ubiquitous vehicle identification to support safe and reliable operations. To this end, Lockheed Martin sees the work of formalizing an operational framework for remote vehicle identification as a critical step in fulfilling the industry objective of harmonized unmanned aircraft operations throughout the national airspace.

[1] *In the Matter of Remote Identification of Unmanned Aircraft Systems*, Docket No. FAA-2019-1100, Notice No. 20-01, 84 Fed. Reg. 250 (rel. Dec. 31, 2019).

Lockheed Martin has been an active contributor to the multiple stakeholder discussions, both domestically and internationally, that have focused in recent years on the desired deployment of services in support of unmanned aircraft missions. Lockheed Martin appreciates that the unmanned aircraft that it develops and manufactures, as well as the operational missions critical to its customers, will rely upon both terrestrial and satellite-based networks for communicating a variety of aircraft functions in addition to payloads. These requirements inform Lockheed Martin's efforts to support the development of enabling regulatory frameworks in support of widespread operations.

Lockheed Martin contributes to the FAA Drone Advisory Committee and has participated on several FAA Advisory Rulemaking Committees. Lockheed Martin supports the work of the ICAO Unmanned Aircraft Systems Advisory Group, Remotely Piloted Aircraft Systems Panel, and Frequency Spectrum Management Panel. Furthermore, Lockheed Martin has been engaged in the work of the International Telecommunication Union on spectrum regulatory matters for UAS. Accordingly, Lockheed Martin is well-suited to comment on the questions raised by the FAA's NPRM and welcomes the opportunity to contribute further to the development of a robust regulatory framework in support of routine UAS operations.

I. ANY REMOTE IDENTIFICATION CAPABILITY NEEDS TO FIT INTO THE EXISTING OPERATIONAL ENVIRONMENT AND BE BOTH SCALABLE AND FLEXIBLE.

Lockheed Martin supports the ambitious goal of the FAA's NPRM and agrees that an interconnected remote identification capability is fundamental not only for safe operations and ensuring public safety, but also as an essential element of any widespread deployment of UAS Unmanned Traffic Management ("UTM") schemes. Given the variety of objectives and potential ancillary benefits to be achieved by the FAA's proposed rules, Lockheed Martin thus encourages the FAA to ensure that its final rules be sufficiently scalable and flexible both as to

leverage existing technical capabilities on aircraft and to identify a variety of approved, certifiable methods for feeding essential information into a comprehensive remote identification system.

As a starting point, while Lockheed Martin agrees with the FAA's presumption that most unmanned aircraft should have broadcast capability to transmit the essential element related to their location and trajectory (with appropriate accommodation for sensitive missions for which such information would be broadcast to only a limited set of suitable, approved recipients), Lockheed Martin questions the FAA's recommendation that the appropriate mechanism is for unmanned aircraft to be equipped with internet connectivity – in effect, making internet connections, with a presumed emphasis on cellular architectures, the default means of satisfying an aircraft's remote identification requirements regardless of existing broadcast equipage already onboard, the geography or location of the mission, or the availability of internet access at the location of flight initiation.

This proposal strikes us as far too prescriptive. It renders the entire remote identification framework overly dependent upon the availability of internet networks, which networks have limited availability in more remote areas of the United States and on United States government test ranges where Lockheed Martin conducts a significant portion of its unmanned aircraft flight testing. Several important questions must also be addressed related to potential vulnerability of some datalinks depending on the communications protocol that might be employed.

Furthermore, the FAA's proposal discounts already available and installed broadcast equipage. Notable is the strict prohibition on ADS-B equipage to satisfy the remote identification requirements – even as many unmanned aircraft, including some classes of aircraft that Lockheed Martin manufactures, are necessarily equipped with ADS-B in order to

MID-ATLANTIC AVIATION PARTNERSHIP
VIRGINIA TECH

Before the
FEDERAL AVIATION ADMINISTRATION
Washington, DC 20005

In the matter of Remote Identification of Unmanned Aircraft Systems	Docket No. FAA-2019-1100

COMMENTS OF THE VIRGINIA TECH MID-ATLANTIC AVIATION PARTNERSHIP

Virginia Polytechnic Institute and State University's (Virginia Tech) Mid-Atlantic Aviation Partnership (MAAP) is pleased to submit comments on the Federal Aviation Administration's (FAA) Notice of Proposed Rulemaking (NPRM) for Remote Identification (remote ID) of Unmanned Aircraft Systems[1]. MAAP is one of seven FAA-designated Unmanned Aircraft Systems (UAS) Test Sites and leads the operations of Virginia's Integration Pilot Program (IPP). MAAP applauds the release of this NPRM to address multiple critical barriers to the integration of UAS into the national airspace system.

MAAP's work through the IPP and other engagements with local communities has demonstrated the tremendous value of educating the public and members of public safety organizations regarding drone operations. When concerns are expressed by community members during our outreach events, they are often tied to concerns about who is operating the drones around their neighborhoods and places of work. Lack of information appears to be at the root of many individuals' concerns, which remote ID directly addresses. Furthermore, remote ID provides

[1] Remote Identification of Unmanned Aircraft Systems, 84 Fed. Reg. 72438 (Dec. 31, 2019) to be codified at 14 CFR Pts. 1, 47, 48, 89, 91, and 107) ("*NPRM*")

law enforcement and public safety officials information needed to ensure the security and safety of the public. For these reasons, MAAP is excited to see progress on the implementation of a remote ID rule that will unlock many future applications of UAS technology while promoting positive interactions with our communities.

MAAP agrees with both the need for this proposed rule and the large majority of the requirements contained therein. However, there are several aspects of the proposed rule that pose significant risk of incurring damage to both the commercial UAS and model aircraft industries ranging from mild to devastating. MAAP submits these comments recommending a number of revisions to the proposed rule that will address many of the negative effects of the current proposed language while preserving the primary capabilities and intent of the rule. These include performance-based requirements for implementation of remote ID rather than the current prescribed approach, a more functional and useful structure for the limited remote ID category, significant modifications to the FAA-Recognized Identification Areas (FRIAs) requirements to prevent the stifling of a thriving and beneficial recreational drone community, and a number of additional recommendations to promote compliance and effectiveness of the rule.

I. PERFORMANCE REQUIREMENTS VERSUS PRESCRIPTIVE SOLUTIONS

The FAA often professes the positive benefits of performance-based rulemaking versus prescriptive mandates that stifle innovation and limit the flexibility of the evolving aviation industry. However, the proposed rule, while ostensibly performance-based, includes prescriptive technology requirements in the form of a mandate for both broadcast and internet transmission ("network") remote ID technologies. Mandating specific solutions for remote ID, rather than identifying the performance requirements which could be met through a variety of means, runs counter to the FAA's stated intention to "evolve in our rulemaking by transitioning from

prescriptive to performance-based rules."[2] It is also contrary to the recommendations of the remote ID and tracking Aviation Rulemaking Committee (ARC)[3] and the specifications in ASTM's F3411-19 Standard Specification for Remote ID and Tracking[4] which was developed through broad and extensive industry collaboration.

The FAA should set the minimum performance requirements for remote ID—for example how often a message must be transmitted, minimum receivable distance for the message, compatibility with existing and future receivers—and then allow the industry to develop solutions that meet the FAA's requirements. As long as these requirements are met, the specific method should not matter—and will be invisible to the end user, who will likely be accessing this information through a mobile app or web interface that can receive source-agnostic inputs. Notably, the ASTM Remote ID standard is a significant step towards an industry-developed solution that can meet a regulator's performance requirement. By contrast, the currently proposed prescriptive solution limits flexibility and, in fact, encourages non-compliance by imposing a heavy burden on the existing commercial and recreational UAS fleet. This is detailed in the following sections.

A. Different operations work well with different types of remote ID technology

Some UAS operations, such as package delivery, are conducted primarily in developed areas where ready availability of wireless network access means that those applications can maintain a continuous connection to a network remote ID service. On the other hand, for operations in rural

[2] Elwell, Daniel K. "Uber Elevate Urban Air Mobility Summit 2019", Ronald Reagan Building, Washington DC, June 11, 2019. https://www.faa.gov/news/speeches/news_story.cfm?newsId=23794

[3] ARC Recommendations Final Report, UAS Identification and Tracking (UAS ID) Aviation Rulemaking Committee (ARC) (Sept. 30, 2017), https://www.faa.gov/regulations_policies/rulemaking/committees/documents/media/UAS%20ID%20ARC%20Final%20Report%20with%20Appendices.pdf ("*ARC Recommendations*").

[4] ASTM International, ASTM F3411-19, *Standard Specification for Remote ID and Tracking* (2020) ("*ASTM Remote ID Standard*").

areas with inconsistent wireless access, broadcast technology makes sense as a preferred solution. Network and broadcast solutions each have advantages and disadvantages. However, the FAA's approach to bridging gaps in each technology by requiring both disregards the significant burden of equipage—a burden that is wholly unnecessary for the many applications for which one solution is vastly better suited and will gain no value from having both.

For example, a package delivery operation occurring in a suburban area with strong network coverage will have access to remote ID USS services throughout the operation. Equipping with broadcast remote ID technology will likely not benefit this type of operation: the rapid cruise speeds often desirable for delivery mean that a delivery aircraft may enter and depart the field of view of a remote ID end user before the broadcast signal can be received, processed, and displayed. Additionally, the network-based remote ID solution offers the privacy of a "session ID"[5] and allows protective measures to be put in place to prevent bulk aggregation of remote ID data—a particular concern for delivery of packages to personal residences.

Of course, the primary challenge of network remote ID is that network access is not available everywhere. In these areas, an alternative method of compliance is necessary, and broadcast remote ID technology is one potential solution. However, broadcast remote ID technologies present two major problems: 1) privacy to the UAS operator and customer, as referenced briefly above, and 2) a massive retrofit burden on the existing fleet of unmanned aircraft. There is no way to prevent the collection of bulk data on the routes of UAS equipped with broadcast remote ID systems through a network of receiving nodes across regions of interest. This is common practice for existing flight tracking companies that collect ADS-B signals from overflying aircraft, which often provide receivers free of charge to parties interested in tracking flight data. However, the

[5] *See NPRM* at 72519.

outreach, and student interest in model aircraft are building momentum towards a new local group of modelers. If this group were to formalize too late, then they would miss the window of opportunity to establish a FRIA in the local community. The FAA should allow applications for FRIAs to be submitted indefinitely because non-equipped model aircraft are not likely to disappear and to accommodate the dynamic and thriving model aircraft community.

B. Revisions to FAA-recognized identification areas should be accepted in a manner to facilitate long-term continuation of the approved locations

The FAA proposes to place strong limitations or prohibitions on the modification, renewal, deactivation/activation, and transfer of FRIAs,[14] presumably due to the aforementioned position that non-equipped UAS will dwindle rapidly. All of these restrictions appear to be designed to ensure a rapidly decreasing number of FRIAs over time, however they are based on the same faulty understanding of the model aircraft community as previously described. The FAA should develop reasonable methods to accommodate changes and transfers of FRIAs indefinitely, because they will fill a vital need long term. Moreover, FRIAs pose little security risk if the approval process factors in proximity to areas of particular security concern. MAAP strongly contends that the proposed rule, without modification, would have a devastating impact on the model aircraft community and must be modified to ensure the sustainment and growth of this critical workforce pipeline and enriching recreational pastime.

IV. BAROMETRIC PRESSURE ALTITUDE REPORTING REQUIREMENT

The FAA proposes to require reporting of both the unmanned aircraft and control station barometric pressure altitude for standard remote ID or control station barometric pressure altitude only for limited remote ID.[15] Barometric pressure altitude was chosen over geometric position

[14] *See id.* at 72487.
[15] *See id.* at 72473.

altitude because "barometric pressure altitude is a more precise measurement than geometric altitude and is the standard altitude reference for aviation."[16] MAAP agrees that reporting the position of the aircraft and control station, to include altitude, is an important component of an effective remote ID solution, albeit with potential privacy concerns not addressed here. However, the requirement for barometric pressure altitude reporting should be replaced with geometric altitude reporting for the following reasons: 1) static pressure measuring systems are highly susceptible to error; 2) complexity of adding static pressure measuring systems to unmanned aircraft and controls stations; and 3) there is not a critical need to utilize a standard aviation altitude reference for remote ID systems that are not intended for navigation or deconfliction.

A. Static pressure measuring systems are inherently prone to error

Barometric pressure altitude must be measured onboard the aircraft by a static pressure system that can measure the free-stream ambient pressure. The movement of the aircraft through the air generates numerous pressure differentials around the airframe that may be either above or below the free-stream ambient pressure. Additionally, static system leaks can cause errors due to pressure differences between the static port location and the location of the leak. For this reason, manned aircraft static systems are regularly tested in order to ensure continued accuracy, but only after the location of the static port has been carefully determined to be the closest representation of free-stream ambient pressure during the aircraft development phase. UAS face a unique challenge from manned aircraft in that their configurations are diverse and differ dramatically across the spectrum of unmanned aircraft. Locating a static pressure measurement system on a UA would be uniquely challenging and likely prone to additional sources of error from various propulsion and airframe configurations that induce unusual airflows. Verifying the initial

[16] *Ibid.*

installation and then ensuring continued system accuracy places a much greater burden on the manufacturer and operator of the UAS than using a geometric altitude source such as GPS.

B. Static pressure systems add significant complexity to unmanned aircraft systems

Almost all current UA do not incorporate static pressure systems to measure barometric pressure altitude, instead they typically rely on geometric altitude from a GPS system that is also utilized for directional navigation. Adding a static pressure system to all UA, especially small UA, would significantly increase complexity of the aircraft systems and may also negatively impact the payload capacity of the aircraft. This is an even larger issue for control stations. MAAP is not aware of any control station currently on the market that measures barometric pressure altitude. Many modern UAS utilize simple interfaces through smartphones and basic laptops to control the aircraft. Requiring these control stations to measure the ambient static pressure would necessitate additional equipment that could dramatically increase the complexity, and potentially decrease the reliability, of the control station. However, geometric altitude of the control station could be accomplished with relative ease, as long as reasonable accuracy requirements were placed on the systems.

C. Standard aviation altitude is not necessary for remote identification of UAS

As discussed previously, remote ID is not a flight safety critical technology. Since remote ID is not performing a vital navigation or air traffic separation role, there is not a specific need for reporting altitude in a standard aviation format. The purpose of remote ID is to provide users on the ground with information about unmanned aircraft in nearby airspace and the location of the control station. Users on the ground are far more likely to reference geometric altitudes than barometric pressure altitudes when trying to understand the location of the control station or the aircraft above them. Providing the aircraft and control station locations in barometric pressure

Docket Operations, M-30
Department of Transportation
Room W12-140, West Building Ground Floor
1200 New Jersey Avenue SE
Washington, DC 20590-0001

Re: Docket No.: FAA-2019-1100; Notice No. 20-01; Remote Identification of Unmanned Aircraft Systems

The Aerospace Industries Association (AIA) is pleased to respond to the Department of Transportation's (DOT) request for comments on the Notice of Proposed Rulemaking (NPRM) for Remote Identification of Unmanned Aircraft Systems (UAS).[1] DOT's request comes as the Federal Aviation Administration (FAA) proposes to amend its rules to require the remote identification of unmanned aircraft systems (Remote ID) operating in the National Airspace System.[2]

INTRODUCTION

AIA is the voice of the American aerospace and defense industry, representing nearly 340 leading aerospace and defense manufacturers and suppliers, supporting over 2.5 million jobs and over $151 billion in annual exports. Our members are on the cutting edge of innovation and are leading the industry on developing emerging technologies such as UAS that will revolutionize the way in which goods are moved, services are performed and people connect.

[1] See Remote Identification of Unmanned Aircraft Systems, 84 Fed. Reg. 72438 (Dec. 31, 2019) (to be codified at 14 C.F.R. pts. 1, 47, 48, 89, 91, and 107) ("NPRM").
[2] iBid.

AIA and its members applaud the Federal Aviation Administration's intent with Remote ID and believe that this rule is critical to the future of the UAS industry. Remote ID will be the key enabler for both safe integration of UAS into the NAS, as well as unlocking the true potential of the UAS industry. Once implemented truly non-segregated aircraft operations such as package delivery, beyond visual line of sight operations and more will be possible due to the ability to understand in real time where UAS are and who is operating said UAS.

AIA anticipates that our member companies will provide comments to the DOT that are more technical in nature and therefore will focus our comments on high level issues that we feel are critical to the entirety of the aviation industry.

INDUSTRY CAN PROACTIVELY WORK TODAY TO EQUIP FOR THE FUTURE

The work towards equipping for this future can begin now. As stated in the NPRM, "Requirements that prohibit operation of UAS without remote identification would begin 36 months after the effective date of the rule."[3] This 36 month phase-in period is important so that operators and manufacturers have time to comply with the final rule, however AIA and its members believe that much of this new rule can be implemented in advance of the 36 month phase-in period and possibly even today.

The FAA's Drone Advisory Committee (DAC) is a Federal Advisory Committee, made up of leaders from across the drone industry, recently formed a task group to look at ways industry can voluntarily equip in advance of the rule implementation period.[4] The task group, composed of DAC members as well as other subject matter experts used the 90-day period to define a set of recommendations for the drone industry to prepare for and equip prior to the full

[3] iBID
[4] See FAA, Drone Advisory Committee eBook (Oct. 17, 2019), https://www.faa.gov/uas/programs_partnerships/drone_advisory_committee/media/eBook_10- 17-2019_DAC_Meeting.pdf.

AiRXOS
Part of GE Aviation

March 2, 2020

Submitted Electronically

U.S. Department of Transportation
Docket Operations
West Building Ground Floor, Room W12-140
1200 New Jersey Avenue, SE
Washington, DC 20590

Subject: Comments of AiRXOS Inc. to the Notice of Proposed Rulemaking on Remote Identification of Unmanned Aircraft Systems Docket No. FAA-2019-1100

AiRXOS, Inc. ("AiRXOS") submits the following comments in response to the Federal Aviation Administration's Notice of Proposed Rulemaking on Remote Identification of Unmanned Aircraft Systems ("NPRM").[1]

I. Introduction

AiRXOS is a wholly owned subsidiary of GE Aviation, the world's largest aircraft engine manufacturer. GE Aviation has worked with the Federal Aviation Administration ("FAA") for decades to improve aviation safety. AiRXOS appreciates the FAA's ongoing efforts to move the drone industry forward while ensuring the continued safe and secure integration of Unmanned Aircraft Systems ("UAS") into the National Airspace System ("NAS"). AiRXOS also recognizes the common interest that the government, industry, commercial enterprise, and the general public share in: (1) establishing reasonable limitations to protect public safety and national security so that UAS operations may become more ubiquitous in the United States; and (2) providing the broad societal benefits of UAS operations, such as reduced emissions, better to healthcare, and reduced human risk, among others. This NPRM on Remote Identification ("Remote ID" or "RID") is a critical step in that evolution, particularly because the FAA has made clear that proposed regulations for expanded UAS operations, such as small UAS operations over people and at night, will not become effective unless comprehensive Remote ID requirements are in place.[2]

1 84 Fed. Reg. 72438 (December 31, 2019) ("the NPRM").
2 84 Fed. Reg. 3856, 3865 (February 13, 2019) ("As a result, the FAA plans to finalize its policy concerning remote identification of small UAS—by way of rulemaking, standards development, or other activities that other Federal agencies may propose—prior to finalizing the proposed changes in this rule that would permit operations of small UAS over people and operations at night.")

- Retrofits
  - The FAA should allow retrofit solutions and should specifically codify tamper-resistant and cybersecurity requirements.
- Operations Under Waiver and Early Compliance
  - The FAA should accelerate the adoption of Remote ID through use in advanced operational approvals.

III. Detailed Comments

AiRXOS submits the following additional detailed comments on key items in the proposed rule:

1. Applicability

AiRXOS concurs with the FAA's proposed requirement that all UAS registered under FAA regulations have and support Remote ID, unless operating at a FAA Recognized Identification Area (FRIA). AiRXOS actively participated in the 2017 RID Aviation Rulemaking Committee ("ARC") and dissented from the ARC Report with respect to the applicability of Remote ID requirements. AiRXOS advocated for a simple, adaptable, enforceable, comprehensive, and future-proofed general rule that any UAS or model aircraft weighing 250 grams or more must comply with the RID regulations. AiRXOS is therefore supportive of proposed Part 89's applicability threshold for Remote ID.

AiRXOS does not agree that the DOD or other agencies should be exempt from the Final Rule when conducting operations within the NAS. Such an exemption could confuse law enforcement or counter-UAS systems to incorrectly perceive a legitimate DOD UAS as a "rogue" operation and would undermine the whole construct of a comprehensive Remote ID system. Additionally, allowing Remote ID-exempt operations within the NAS would increase the risk of collision with a commercial or recreational UAS operator.

Because of the legitimate security concern about DOD or other agencies participating in the Remote ID ecosystem, the FAA should establish a "Trusted Remote ID USS" category capable of authenticating users and protecting distribution of sensitive user information. A "Trusted Remote ID USS" would also be capable of integrating UAS tactical requirements of DOD and other agencies into the broader strategic needs for secure, safe, and efficient UAS operations within the NAS. Network-based Remote ID supports such a concept by allowing for secure sharing of sensitive information with authenticated users on a need-to-know basis.

B. FAA-Recognized Identification Areas

AiRXOS has several concerns with the proposed restrictions related to applications for a FRIA designation as outlined in § 89.21. First, there is no justification or explanation in the NPRM for establishing the overly restrictive 12-month period in which applications for FRIA designations may be submitted. The 12-month limitation has the appearance of being an arbitrary and unnecessary restriction. FRIA-designation applications should be accepted by the FAA for consideration at any time, and included in the regular FAA chart update cycle.

Second, there is no compelling rationale for limiting FRIA applications and designations to community-based organizations ("CBO"), as suggested in the proposed rule. Companies and educational institutions should be allowed to apply and be eligible for FRIA designations. Making such organizations eligible to apply for FRIA designations will advance innovation in the United States and promote workforce development in this industry, while also maintaining the safety and security of the NAS. Accordingly, AiRXOS supports the establishment of a risk-based process for approving a FRIA and applying that standard whenever a CBO, commercial or educational entity seeks a FRIA-designation to support non-Remote ID operations.

The NPRM also provides no reasonable explanation for preventing applicants from applying to reestablish a previously approved FRIA. This limitation does not appear to be risk-based and has the appearance of being an arbitrary restriction. AiRXOS therefore urges that this prohibition be eliminated from the Final Rule.

The FAA states that draft Advisory Circular 91-57C, which is not yet published, will provide definitions and a process for establishing a CBO. To make any comment related to the definition and establishment of a "CBO," AiRXOS would need to understand the criteria the Administrator will use to make his or her determination.

The FAA also proposes in § 89.120 that, in addition to VLOS operations at a FRIA, FAA-authorized UAS operations for aeronautical research could be performed without Remote ID when authorized by the FAA Administrator. AiRXOS disagrees with this approach, and instead supports the FAA expanding the limitations in § 89.205 to allow commercial entities involved in research, development, and testing to have the ability to request and be issued a FRIA to support technical innovations and advancements. This minimizes the requirement in the NPRM for the FAA to approve prototype UAS operations in accordance with § 89.120 and ensures the geographical area details are made available to relevant stakeholders through FRIA publication.

3. Internet Availability

The FAA is soliciting comments on whether there are ways to address the unlikely event that all Remote ID USS become unavailable at the same time within the framework of the rule as

requests that the Final Rule provide more information defining routine maintenance and UAS repair requirements in order to meet the approved DoC- and MoC- approved standards.

Finally, as previously noted, the UAS MoC/DoC approvals must be independent of the Remote ID USS so that UAS operators can switch Remote ID USS without invalidating their MoC/DoC.

14. Operator Privacy

The proposed Remote ID rule is designed to establish authentication and security requirements necessary to support law enforcement and security concerns while respecting and protecting personal identification information ("PII") of the UAS operator.

AiRXOS fully supports the option of an operator using a session ID, as proposed in the draft rule. AiRXOS also supports the establishment of different tiers of Remote ID USS capabilities that meet advanced security, authentication, privacy, and operational requirements, including "Trusted Remote ID USS" for law enforcement users that have access to sensitive security and privacy information not otherwise available to the public. Trusted Remote ID USS and network-based Remote ID will enable law enforcement to operate sensitive missions without disclosing their position to the public.

15. Remote ID USS Requirements

AiRXOS supports a Remote ID USS on-boarding process that ensures information collected by the Remote ID USS is used to support the safe and secure operations of UAS within the NAS but not used for illicit or commercial purposes that violate an operator's privacy. AiRXOS recommends that such Remote ID USS onboarding requirements be made clear in documents that are publicly available and reviewable, such as an Advisory Circular, instead of specifying them through the opaque MOU process used with LAANC. As AiRXOS has experienced with the LAANC program, the FAA's traditional contracting vehicles and authorities are not an effective or publicly transparent way to specify technical requirements for UTM services. A more transparent and collaborative process for approving remoted ID USS' based on compliance with defined requirements may be more appropriate for a service that does not involve financial compensation from the FAA.

16. Definitions

Several key terms and performance requirements need clarification and/or definition to facilitate compliance with the Final Rule. Examples include "tamper-resistance" (§89.310.(e)), "cybersecurity protections" (§89.310.(k)), and "internet is available" (§89.310(f)).

March 2, 2020

Docket Operations, M-30
U.S. Department of Transportation
1200 New Jersey Avenue SE, Room W12-140
West Building, Ground Floor
Washington, DC, 20590

Re: Docket FAA-2019-1100, Comments on Notice of Proposed Rulemaking for Remote Identification of Unmanned Aircraft Systems

Amazon Prime Air appreciates the opportunity to comment on the FAA's Notice of Proposed Rulemaking for Remote Identification of Unmanned Aircraft Systems (NPRM). We strongly support implementing remote identification (RID) of unmanned aircraft systems (UAS) to protect the interests of all airspace users; the public; and the FAA, law enforcement, and security agencies charged with protecting lives and property. RID is critical to ensuring safe, secure, and transparent UAS operations, and only a comprehensive solution—requiring both broadcast and network for standard RID UAS, as defined in the NPRM—will guarantee those benefits. We applaud the FAA's effort to create a rule that facilitates UAS integration and innovation and builds the infrastructure necessary for expanded UAS operations, and we respectfully submit these comments to strengthen certain areas of the NPRM. We urge the FAA to (1) retain the requirement that standard RID UAS must both broadcast RID message elements directly from the unmanned aircraft (UA) and transmit them via network, (2) adopt RID requirements that promote international standardization, (3) accept ASTM's RID standard as an acceptable means of compliance, (4) allow RID message elements to include either barometric pressure altitude or geometric altitude, (5) expedite implementation, and (6) take appropriate steps to ensure security of flight data.

I. Amazon Prime Air

Amazon Prime Air designs, manufactures, and operates UAS that will safely deliver packages weighing up to five pounds to Amazon customers in 30 minutes or less. Amazon Prime Air is driven by innovation, yet inspired by aviation tradition, and we will always prioritize safety, security, and transparency. This is essential to retaining the public trust and is the foundational element for UAS growth and innovation.

Amazon Prime Air is fully committed to safety and promoting innovation and growth in the UAS sector. As part of Amazon's broader activities in advancing the UAS industry,[1] we are a member of the FAA RID Aviation Rulemaking Committee, a member of the FAA's initial RID UAS Service Suppliers (USS) cohort, and a member of the ASTM RID standard working group.

II. Amazon Strongly Supports the NPRM's Proposed Requirement that Standard RID UAS Must Broadcast and Transmit via a Network

UAS traffic management (UTM) is key to safely integrating UAS into the National Airspace System and to enabling a myriad of current and emerging UAS use cases, including precision agriculture, search and rescue, infrastructure inspection, package delivery, and other UAS support services.[2] Safety and security are top priorities within the UTM architecture: the system must know who is flying what UA, where they are flying or intend to fly, and whether they are conforming to mandatory operating requirements. To enable this, a set of fundamental components (of which RID is one) are combined to support the necessary capabilities required to securely and safely manage UAS operations. These components form the core of an authentication-, authorization-, and auditing-based (AAA) architecture.

In this AAA architecture, the NPRM addresses the authentication role because it requires RID to be integrated within each UAS that meets the needs of industry, law enforcement, and public services users.[3] A successful UTM architecture depends on a RID system that includes (1) a distributed database, accessible by approved authorities, that contains a unique identifier for all registered UAS; (2) the capability to leverage the transmission of this unique identifier from registered UAs and/or associated ground control stations through both direct broadcast and network mechanisms; and (3) public and private application programming interfaces for accessing the system.

Only a comprehensive RID solution that requires standard RID UAS to both broadcast RID message elements directly from the UA and transmit them via a network can fully meet public and private safety concerns and support UTM because requiring both provides the necessary coverage and redundancy.[4] It may be difficult to receive broadcast RID messages from UAS flying low to the ground or around obstacles, and a network solution may not be reliable in an

[1] Amazon is a founding member of the senior advisory body of the FAA's Drone Advisory Committee (DAC), a member of the Nevada UAS Test Site team selected to participate in 2019 UTM Pilot Program, one of the lead elements in European U-space 2019 demonstrator events, and long-time participant in the NASA Technical Capabilities Level (TCL) project. Amazon directly contributes to seven different UAS-specific ASTM standards committees, previously chaired the ASTM UTM working group, and currently contributes extensively to the ASTM F38 standards groups. Finally, Amazon co-chairs FAA's UAS Safety Team (UAST), sharing this duty with the Executive Director of the FAA UAS Integration Office, and together assists UAST with national UAS safety initiatives and industry recommendations.

[2] Remote Identification of Unmanned Aircraft Systems, 84 Fed. Reg. 72,438, 72,454 (Dec. 31, 2019).

[3] As the NPRM contemplates, the authorization and auditing requirements of the UTM solution are fulfilled by FAA-certified service suppliers, which could be industry, governmental authorities, or a combination of the two.

[4] *See, e.g.*, 84 Fed. Reg. 72,438, 72,465.

area with limited cellular coverage. A redundant system that provides the ability to verify that UAS operations have been appropriately authorized will build trust, aid law enforcement, and help ensure regulatory compliance.

Additionally, this combined RID broadcast and network RID information architecture allows broad availability to multiple relevant parties, and flexibility to authorize additional information with credentials for security and safety authorities. Moreover, the standard "beacon" from such hardware can convey to any nearby smartphone a digitally-signed, and therefore, secure, identification. UTM system operators (operating as USS Remote ID Network providers) and partners can develop applications to use this information for specific requirements.

III. The FAA Should Adopt RID Requirements that Promote International Standardization

The FAA should take steps to standardize RID message elements because there would be significant benefit to UAS operators in having UAS that could accomplish RID in a similar fashion regardless of the country in which they are operating. As the RID ARC report noted, several countries are considering approaches to RID and tracking,[5] and the European Union Aviation Safety Agency (EASA) has promulgated RID requirements.[6] For example, EASA requires RID messages to include UA route course and ground speed.[7] Requiring these message elements would promote international standardization and further support the implementation of UTM and U-space.

IV. The FAA Should Accept ASTM's RID Standard as a Means of Compliance

ASTM is a leading standards development body, and FAA has an "extensive history"[8] of working with ASTM and has accepted ASTM standards in the past as a means of compliance for other safety-critical FAA requirements.[9] As with its other standards, ASTM's RID standard was

[5] *See* UAS Identification and Tracking (UAS ID) Aviation Rulemaking Committee (ARC), ARC Recommendations Final Report at 49 (Sept. 30, 2017) ("In addition, a number of countries around the world are considering approaches to ID and tracking."). Some of these countries include the United Kingdom, *see* House of Commons Science and Technology Committee, *Commercial and Recreational Drone Use in the UK, Twenty-Second Report of Session 2017-19*, Publications Parliament (Oct. 11, 2019), available at https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/2021/2021.pdf; France, *see U-space Together: Fast-tracking Drone Integration in a Safe Sky,* DSNA (Mar. 2019), available at https://www.ecologique-solidaire.gouv.fr/sites/default/files/2019_WAC19_USPACE_BAT.pdf; and Singapore, *see CASS to Implement Mandatory Unmanned Aircraft Registration*, CAAS (Nov. 4, 2019) available at https://www.caas.gov.sg/about-caas/newsroom/Detail/caas-to-implement-mandatory-unmanned-aircraft-registration.

[6] *See* Commission Delegated Regulation (EU) 2019/945, On Unmanned Aircraft Systems and on Third-Country Operators of Unmanned Aircraft Systems, O.J. (L 152) 31.

[7] Id.

[8] 84 Fed. Reg. 72,438, 72,472.

[9] *See, e.g.*, Notice of Availability, 70 Fed. Reg. 43,505 (July 27, 2005) (adopting standards developed by ASTM International Committee F37 for certification of light sport aircraft); Notice of Availability, 72 Fed. Reg. 178 (Jan. 3, 2007) (accepting two new ASTM standards developed with FAA for certification of light sport aircraft); Notice of Availability, 83 Fed. Reg. 21,850 (May 11, 2018) (accepting 63 Means

Before the
FEDERAL AVIATION ADMINISTRATION
Washington, DC 20591

In the Matter of	)	
	)	
Remote Identification of Unmanned Aircraft Systems	)	Docket No. FAA-2019-1100
	)	Notice No. 20-01
	)	RIN 2120–AL31
	)	

COMMENTS OF VERIZON

William H. Johnson
Of Counsel

Melissa Glidden Tye
VERIZON
1300 I Street, NW
Suite 500 East
Washington, DC 20005
(202) 515-2400

Matt Fanelli
Skyward, A Verizon Company
1300 I Street, NW
Suite 500 East
Washington, DC 20005
(202) 515-2400

March 2, 2020

TABLE OF CONTENTS

Before the
FEDERAL AVIATION ADMINISTRATION
Washington, DC 20591

In the Matter of	)	
	)	
Remote Identification of Unmanned Aircraft Systems	)	Docket No. FAA-2019-1100
	)	Notice No. 20-01
	)	RIN 2120–AL31
	)	

COMMENTS OF VERIZON

Unmanned aerial systems ("UAS" or "drones") present huge opportunities for innovation, consumer welfare, and commercial success. Remote identification rules are the next step toward fully integrating UAS into the national airspace, and the choices made for these rules will determine how quickly the industry can realize its full potential. By adopting rules to establish the fundamental building blocks of the larger traffic management system necessary to integrate UAS into the national airspace, the FAA has the opportunity to move industry on a path toward the widespread deployment of drones in a future-proof manner.

As explained in detail below, the FAA should adopt a Remote ID rule that requires virtually all UAS, with a few specific exceptions, to transmit Remote ID information to a UAS Service Supplier ("USS") in real time, regardless of the distance between the drone and the operator. Where connectivity to a USS is unavailable, such as in remote or rural areas, a broadcast transmission available only to local receivers would be allowed.

A USS Remote ID solution is clearly superior to broadcast Remote ID for many reasons, including its essentiality as a building block for Universal Traffic Management ("UTM"); its authentication, flight planning, and deconfliction advantages; the protection it offers against cybersecurity threats; and the ease with which operators can simply upgrade existing software already installed on the drones to access new and custom solutions. And USS Remote ID will

Before the Federal Aviation Administration

In the Matter of Remote Identification of Unmanned Aircraft Systems	)))	Docket No. FAA-2019-1100 (RIN 2120–AL31)

Comments of DJI Technology, Inc.

March 2, 2020

Contents

connections and interfaces (such as a screen or SIM card) needed to connect to an internet-based service.

We believe it is obvious that a broadcast remote ID solution is far less complex and costly than a network solution, simply by virtue of its simplicity. A single component on the UAS is all that is needed to take an average type of UAS used today, already moderately capable of remote-control navigation and GPS positioning, and have it perform remote ID. In contrast, a network solution requires hardware on board the UAS, accessible infrastructure to reach the internet, a service provider dedicated to Remote ID, another service provider to share in that information and send it to the interested observer over the network. It requires access controls and data storage capabilities, as well as a robust level of security because of the aggregation of data in one location.

One way to understand the stark contrast in costs between network and broadcast methods is to visualize the cost centers of each. In the following figures, we illustrate the number and type of cost centers for each solution:

[NEXT PAGE]

Tamper Resistance

A broadcast remote ID function is implemented by the manufacturer and has no dependencies on other steps or services. When the UAS is turned on, the ID broadcast functions. Because for many UAS the function will be incorporated into the C2 radio equipment, tampering or disabling the feature will be challenging for most pilots/operators without disabling the control function of the UAS.

Ease of Compliance

As the 2017 ARC report noted, "[t]o be effective, any regulation associated with UAS ID and tracking will need a high degree of UAS owner/operator compliance.. broad compliance is critically important for an ID and tracking solution to have value." 2017 ARC Report § 5.1.2.1. Otherwise, with a substantial percentage of UAS not participating in Remote ID, discrimination between "friend" and "foe" will be impossible for security officials. Whether people willingly comply is a function of how easy it is to do so.

Broadcast solutions are "easy" because there are no steps that are additional to the operation of the UAS. Turn it on, and the ID broadcast functions. Doing Remote ID becomes unnoticeable and routine, like having a license plate affixed to a car and never worrying about it again. In contrast, a network approach requires various demands of time, effort and trouble on a recurring basis:

- Researching and selecting a service provider (among a choice of the anticipated nine providers FAA envisions to provide service under varying service models).
- Paying monthly bills from the service supplier, including updating any new payment information or change of address.
- Determining and ensuring that the UAS is within range of cellular or other network access points, and logging into them in some cases.
- Troubleshooting or moving locations when the network connectivity isn't reliable or performing at the required level.

- When the function fails, taking time to figure out whether the failure is with the UAS hardware, the network connectivity, or the USS service, as compared with broadcast which is always supported by the manufacturer.

- Logging into a remote ID service with an ID and password.

- Assigning each UAS in a fleet to a USS account, which could prove problematic for companies and organizations who share UAS among varying end-users, which would require repeated log-in and log-out steps for each user, and perhaps each mission.

Over the course of time, this method may also involve changing providers as they shift their pricing or service models, or if they go out of business. The recurring and persistent hassles of dealing with third-party service providers just to provide others with identity information represents a poor ease of compliance that, by virtue of its design, can never really improve.

Although these factors (and others, described elsewhere in our comment) compel a conclusion that Broadcast solutions are best for most operations today, DJI supports UAS pilots/operators having a choice of Remote ID method, based on industry consensus standards. We understand that, notwithstanding our analysis, there are operators and pilot who will prefer network Remote ID. The best approach would be for FAA to allow a choice of either broadcast or network remote ID, and to evaluate how costs and other factors play out in the coming years.

B. DJI AeroScope Has Proven the Concept of Broadcast Remote ID, in the Real World

DJI launched its AeroScope remote identification feature in October 2017.[24] Implementation involves broadcasting a packet of ID information in the radio downlink from the UA, something we accomplished by modifying the software on existing UAS products. That software makes use of a proprietary variant of Wi-Fi technology to broadcast remote ID information. This was the broadcast

[24] See DJI Unveils Technology To Identify And Track Airborne Drones, DJI Newsroom, available at https://www.dji.com/newsroom/news/dji-unveils-technology-to-identify-and-track-airborne-drones .

D. The FAA Proposal Needlessly Creates Cybersecurity Vulnerabilities Across the Entire UAS Industry

In recent months, the issue of cybersecurity of small UAS has come to the fore, with agencies such as DHS issuing recommendations about mitigating potential risks. DJI has both anticipated and responded to such needs by collaborating with our customers on solutions, including with the U.S. Department of the Interior. One of our simplest cybersecurity risk mitigation features is called Local Data Mode, and it was introduced in 2017. Local Data Mode turns off connectivity and data transfer between the drone's software and the internet. This feature, which can be validated by any user simply by monitoring network traffic between the ground control station and the internet, provides assurance that no UAS-related data is being sent to unauthorized parties, and no unauthorized parties are able to hack into the UAS from the internet.

Indeed, guidance issued by the US Department of Homeland security recommends that UAS operators "[u]se standalone UAS-associated mobile devices with no external connections, or disable all connections between the Internet and the UAS and UAS-associated mobile devices during operations."[40]

The FAA proposal precludes this cybersecurity solution, depriving DJI and other manufacturers of a simple and effective way to provide data assurance to its customers. Without any cybersecurity assessment or economic impact analysis concerning existing product features, the FAA proposes to prohibit such a feature. There is no option for complying with Remote ID requirements other than to connect the UAS to the internet whenever the internet can be reached. This will require DJI and other manufacturers to remove the Local Data Mode feature from its products, and for users to avoid

[40] Cybersecurity Best Practices For Operating Commercial Unmanned Aircraft Systems, US Department of Homeland Security, *available at* https://www.waterisac.org/system/files/articles/Cybersecurity%20Best%20Practices%20for%20Operating%20Commercial%20Unmanned%20Aircraft%20Systems%20Fact%20Sheet.pdf

disabling internet connection features on their own. This requirement introduces pathways for cyber-vulnerabilities that do not exist today, and costs that are not accounted for by the FAA.

Broadcast Remote ID solutions would avoid creating this vulnerability, and allow manufacturers to implement their own Local Data Mode (and comparable features), because the Broadcast method is a one-way radio signal out from the drone that verifiably contains only the information required by the FAA's Remote ID rule, and does not expose other UAS data to exfiltration or hacking via the internet. Because it does not require a connection to any internet service, Broadcast Remote ID does not create a new cyberattack pathway for hackers between the internet and drone.

To be clear, DJI expects to be able to meet or exceed the cybersecurity needs of its customers. We have already done so, at considerable expense, and with an emphasis on our products that are designed for enterprise or government use. But by requiring all drones to connect to the internet, even those operating safely at very low altitudes in remote locations away from airports or other secure facilities, the FAA creates a dramatic burden of entry for U.S. manufacturers, by requiring all devices to potentially meet unknown cybersecurity requirements that would otherwise be completely unnecessary for those manufacturers.

E. The FAA Proposal Appears to Create Unnecessary Obstacles to the Foreign Commerce of the United States

As the FAA notes, "The Trade Agreements Act of 1979 (Pub. L. 96–39), as amended by the Uruguay Round Agreements Act (Pub. L. 103–465), prohibits Federal agencies from establishing standards or engaging in related activities that create unnecessary obstacles to the foreign commerce of the United States." NPRM at 72508.

Most small UAS products are, like consumer electronics, manufactured overseas and imported into the United States. As pointed out by industry leader Precision Hawk, access to affordable, capable

imports that otherwise meet the FAA's safety objectives. By making the operation of UAS hardware, which is legal for import, dependent on the functioning of an online service, and then prohibiting non-U.S.-based entities from offering that service, the NPRM appears to violate the Trade Agreements Act of 1979 by creating unnecessary obstacles to foreign commerce.

VI. Issues Created for Manufacturers and Technology Producers

A. The FAA Is Incorrect About Retrofit Rates, Which DJI Estimates at Zero Percent

The FAA's NPRM asserts that "The FAA reviewed UAS registered to part 107 operators and found 93% of the existing part 107 UAS fleet may have technical capabilities to be retrofit based on information received by industry (i.e., could support software updates through internet)." NPRM at 72489. The FAA then concludes that "at least 93% of the current part 107 fleet and at least 20% of the current recreational fleet would be eligible for retrofits." NPRM at 72496. This estimate seems to be largely premised on information provided by DJI during discussions and meetings, prior to the publication of the NPRM, and the large fraction of the Part 107 fleet that consists of DJI products. ("The FAA received information from industry on the potential to retrofit during Executive Order 12866 meetings from September through December, 2019." NPRM Footnote 81; and "[small UAS] manufactured by one producer (DJI) … provided information to the FAA suggesting they could retrofit." NPRM at 72490.)

Although DJI has been optimistic about the potential for cost-free retrofit via software updates, having now examined the NPRM we believe the true retrofit rate is zero percent, for the following reasons.

First, the NPRM requires the *producer* of the UAS product to test and certify that Remote ID is functioning properly, and to implement auditing functions. DJI does not believe this is possible for units

that have already been sold and delivered prior to the effective date of the Remote ID rule. DJI cannot control (let alone test and audit) whether its customers have modified, upgraded, or tampered with the UAS after its sale. Only at the time of sale does DJI have control of the product sufficient to represent to a national aviation authority that that product properly performs a function required by law. Requiring customers to return the unit to DJI for the retrofit would be prohibitively expensive and is not included in the FAA's economic analysis, which presumes retrofit to be free. It would not be appropriate to impose responsibility and certification liability upon DJI for products already in the market, but that is what the NPRM will do.

Second, the Proposal requires producers to provide a list of serial numbers to the FAA corresponding to which aircraft are certified to be compliant with the Remote ID regulations and standards. This raises a few problems. Our units on the market do not necessarily conform to the ASTM/ANSI standard for serial numbers required by the FAA in the regulation. Indeed, no producer seems to be using this standard at the present time, and all manufacturers may wait until the Remote ID Rule is finalized before switching their numbering systems, especially given that the European Union's approach to Remote ID appears to be five years ahead of the United States, and may compel taking a different approach. Second, we do not have a function that tracks whether our users have updated all of the necessary software according to the aircraft serial number. While updates are available to be "pushed" to our users over the internet, these software updates, including aircraft firmware, end up on the user's mobile device. Only the user can confirm that the updates required between the mobile device and the other UAS components (the aircraft, batteries and remote controller) were actually successfully installed across the aircraft, the ground control app, and the remote control devices. We do not track which aircraft users connect to their mobile device at any given time. Even if we implemented such functions, the NPRM would require us to individually track and report these numbers to the FAA on a real time basis, increasing administrative costs that are not accounted for by the FAA.

Third, as noted elsewhere, with limited exceptions, DJI does not sell the smart-device[43] that is attached by the pilot to the DJI radio controller to serve as the display interface of the ground station. Given the wide variety of brands and models of smart devices, and varying operating system versions, DJI cannot know whether a retrofit was successfully achieved. Adding software routines to provide this type of information to DJI would be invasive to our users' data privacy and we would not voluntarily choose to do it, nor should the FAA force us to. Moreover, upon installing a software update, the user could always switch to another smart device whose older app software lacks the Remote ID function, thereby rendering the UAS non-compliant, and DJI's "certification" false.

Fourth, all of our discussions with FAA (and OIRA) providing informal estimates of retrofit were premised on the 2017 ARC recommendation, the nascent ASTM International standard (which has recently been published), as well as the advice provided by the Drone Advisory Committee to the FAA, that Remote ID could be achieved by *either* a network *or* a broadcast method. DJI has some products on the market whose best (or only) retrofit path is a software update to the Wi-Fi radio system, achieving broadcast ID, and other products on the market that might be best (or only) updated by modifying software to perform network remote ID. Indeed, DJI has at least five ground station apps (DJI GO, DJI GO4, DJI Pilot, DJI Flight Hub, DJI Terra) and seven active hardware product lines (Phantom, Inspire, Spark, Wind, Agras, Matrice, Mavic), each of which has multiple aircraft models, and we may not choose to update all of these, depending on equipment configurations, resource constraints, and product lifecycle timing. In discussions with FAA, we had relied upon being able to evaluate upgrade paths under an "either/or" approach. The NPRM's proposal to require *both* network and broadcast Remote ID in the Standard category (in which our products clearly belong) means that our retrofit estimate is substantially lower, as some products will not *be able* to achieve both methods. And, some products

[43] A smart phone or a computing tablet.

will not be *economically feasible* for us to upgrade across all model and ground station app configurations, especially if we must perform the retrofit by two different methods.

Our communications on this retrofit issue have been clear. On October 1, 2019, an FAA official inquired by email about whether DJI could meet the network and broadcast portions of the ASTM standard. In our reply that day, we indicated that "we believe *a substantial portion* of our products will be able to conform with the ASTM *broadcast* standard by the time the requirements exist" but also made clear that "we remain concerned about the cost and complexity of [network] solutions and *do not have a company position on its implementation at this time*, because a substantial number of questions about the network access controls, subscription costs, equipage, privacy, and other costs, remain unknown, as well as the scope of when network solutions might be required." (Emphasis added.) We also indicated that, as to the broadcast method, "[w]e believe it is indeed a software upgrade for *many but not all* current models." (Emphasis added.) In light of these communications, we cannot account for why the NPRM incorrectly presumes that 100% of DJI models can and will be retrofit to perform *both* broadcast and network Remote ID. Our reply in October also assumed a user-compliance approach to the requirement, not an approach requiring DJI to certify the performance of each UAS by serial number, auditing and testing, as well as implementation of an interlock function that is dependent on the performance of a USS.

In light of the actual NPRM's requirements, DJI now estimates its ability (and those of other OEMs) to retrofit products sold prior to the effective date of the Remote ID rule at a rate of zero percent if the Remote ID rule were to be finalized as currently written in the NPRM. Importantly, a Remote ID requirement that imposes compliance responsibility upon the pilot/operator, rather than upon the OEM, would solve some of these challenges and improve the "retrofit" rate, as would a Remote ID rule that permits the use of *either* network or broadcast solutions.

providing flexibility in the choice of Remote ID solution, and permitting add-on modules and declared-intent mechanisms in place of integrated features that can only be accomplished by sophisticated manufacturers.

Second, the scope and process of the FAA-Recognized Identification Areas is far too narrow. The FAA has arbitrarily limited the application window for such locations to 12 months, seemingly in an effort to artificially constrain the number and longevity of these sites. But considering how challenging it will be for amateurs, students, and hobbyists to comply with the Remote ID provisions in the proposal, it is clear that a broader set of locations will be required to accommodate the many types of UAS that will be unable to comply with the rule's requirements. If the FRIA concept is kept in the final rule, the process should not have a sunset.

Third, the FRIA process raises legal questions. The FAA proposes that recognized Community Based Organizations will be the only ones who can apply for an FRIA, but the FAA has not stood up the criteria or process for CBO recognition, making it impossible for the public to comment on this aspect of the proposal. This creates, as a regulatory requirement limiting operations in the national airspace system, something that is the subject of unknown future FAA internal policy. This strikes us as a legal defect in this aspect of the NPRM. Moreover, the Community Based Organizations, and their affiliated clubs and sites, are private, member organizations, which allows them to discriminate based on any number of criteria, from technology to religion to race and gender. It is not appropriate, and potentially illegal, for the authority of Americans to legally operate an aircraft to be governed by the unchecked whims of a private club or association.[50] The FRIA process must be open to other individuals and organizations, including but not limited to schools, trade associations, local government agencies, tribal

[50] Even if legal remedies are available, we cannot imagine anyone wants to sue a model aircraft club over a membership discrimination claim. It should be addressed by proper policy.

comments on our Remote ID communications, and that Dr. Dippon noticed as well, in his survey analysis. As the 2017 ARC wrote:

> [H]istorical tracking information for UAS, although not necessarily falling within certain definitions of PII, raises serious pilot privacy concerns that must also be addressed through various legal, technical and procedural protections. Owners and operators have legitimate reasons to keep the locations, dates, and times of their UAS flights private even if that data is not directly associated with PII in the same database. Tracking information for UAS indicates very precisely the location of a specific person or company operating the UAS for a specific personal or business purpose. Aggregate historical tracking information can reveal patterns that compromise business confidentiality or personal privacy. It could indicate that a certain farmer's field is of particular economic interest, for example. Many people use small UAS for personal and private purposes, such as family photography. Because UAS ID and tracking will be a regulatory mandate, rather than a consumer option, and because the ARC has recommended a threshold that captures a broad range of UAS aircraft and operations, this privacy concern is heightened compared to location-enabled technologies in the marketplace that are used voluntarily.
>
> These concerns require the FAA, in consultation with privacy experts and other agencies, to consider whether and how historical tracking information is recorded or maintained in a regional or central database and whether any non-governmental third party should generate, maintain, or have access to any repository of UAS historical tracking information, as well as any safeguards that might be put into place to mitigate these privacy concerns.

2017 ARC Report Sec. 7.1.5.

> Owner/operators may view negatively the loss of control of information associated with their flight operations. Even without disclosure of PII, the widespread availability of operational sensitive information (e.g., time, location, duration, flight frequency) could have an impact on an owner/operator's perceived privacy and/or commercial interests. The holding of such information by a third party may be concerning to some UAS owner/operators, whereas some may prefer it. If broad operational data is available, it may be archived and mined for information which could be perceived as detrimental to the owner/operator. Even if access to such information is limited to public safety officials or through use agreements, the perception may be detrimental to the willingness to comply.

2017 ARC Report Sec. 5.1.2.1

The "Session ID" concept is a good way of obscuring some types of operations from aggregate data collection by observers, and this contributes to good privacy outcomes. However, this does not fully address DJI's or the 2017 ARC's privacy concerns because each USS will have and store the Session ID that corresponds to their own customer's identity, which they will obtain during the account sign-up