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.

As advanced as it is, Skydio 2 represents only the beginning of a new era of unmanned flight enabled by onboard intelligence. FAA rulemaking should be designed with that future in mind: one in which drones are smarter, safer, more intuitive, and more useful than ever before.

II. PROVIDING PATHWAYS TO PERMIT TRUSTWORTHY AUTONOMY

The Executive branch and Congress have consistently and appropriately stressed the importance of ensuring America's continued global leadership in emerging technologies, including UAS and automated vehicles. As proclaimed in the White House Presidential Memorandum establishing the UAS Integration Pilot Program, "To promote continued technological innovation and to ensure the global leadership of the United States in this emerging industry, the regulatory framework for UAS operations must be sufficiently flexible to keep pace with the advancement of UAS technology."[1] In the related context of automated vehicles (AVs), the Administration concluded, in a report released in January 2020, that, "with the development of AVs, America has the potential to once again transform the future of transportation, while also increasing economic growth and overall productivity. AVs—if developed properly—also have the potential to make our roadways safer by reducing crashes caused by human error, including crashes involving impaired or distracted drivers."[2] Trustworthy autonomy will define the future of transportation on the ground and in the air. In the context of unmanned aircraft, FAA rulemaking must be designed to capture the benefits of this new and promising technology.

That premise applies with special force to the FAA's proposed rule on remote identification of UAS, which will shape our skies for years to come. In particular, the Final Rule must permit operations in GPS-degraded or GPS-denied environments enabled by advanced capabilities, such as proven computer-vision technology. Enabling operations with advanced autonomy technology will have no adverse impact on safety and security in the airspace, and will greatly enhance safety for people who would no longer need to perform critical infrastructure and other important inspections themselves. Failing to permit intelligent operations in general,

---

[1] *Presidential Memorandum for the Secretary of Transportation on Unmanned Aircraft Systems Pilot Program*, October 2017, page 1, https://www.transportation.gov/briefing-room/presidential-memorandum-secretary-transportation.

[2] *Ensuring American Leadership in Automated Vehicle Technologies: Automated Vehicles 4.0*, January 2020, page 2, https://www.transportation.gov/sites/dot.gov/files/2020-02/EnsuringAmericanLeadershipAVTech4.pdf.

and especially in areas where GPS-reliant drones are incapable of operating, will unnecessarily restrict beneficial UAS operations in the United States, remove incentives for companies to innovate in this area, and jeopardize the ability of the United States to maintain its leading role in UAS development and operations.

This is an issue of significant, real-world importance. Enabled by advanced computer vision technology, Skydio 2 is not reliant on GPS connectivity to initiate or continue flight. It is capable of taking off and operating using computer vision to understand its location and the world around it. Skydio 2's vision system also enables it to estimate its position in the surrounding environment even after losing GPS connectivity. That technology enables Skydio 2 to operate in areas inaccessible to the vast majority of drones, which (1) rely on GPS connectivity to determine their location and (2) are highly vulnerable to electromagnetic interference (a common phenomenon near cell-phone towers and transmission lines), which often degrades or denies GPS connection.[3]

New technology offers new utility and use cases. Today, numerous companies in the United States and abroad use the Skydio 2 to conduct close-in inspections of critical infrastructure in areas where GPS signals are severely degraded or denied, including in the vicinity of cell-phone towers, transmission lines, large structures, inside buildings,[4] beneath bridges and inside bridge trusses. These use cases provide incredible value to our customers. To understand that value, it is useful to see it firsthand. To that end, we have prepared a short video demonstrating real-world operations made possible by Skydio 2: https://tinyurl.com/Skydio2-UseCases-RemoteID.[5] We urge the FAA to review the video, which shows Skydio 2 navigating a range of environments likely to lack reliable GPS connectivity. In

[3] *See* S. Storm van Leeuwen, *Electromagnetic Interference on Low Cost GPS Receivers*, National Aerospace Laboratory, October 2008, https://pdfs.semanticscholar.org/4bce/5176ff91452ff551be6c4805403e274312d5.pdf ("GPS receivers are vulnerable to unintentional radiation from nearby radio transmitters, and to intentional radiation such as jamming, meaconing and spoofing."). In addition to its resistance from GPS interference, Skydio 2's ability to rely solely on computer vision safeguard it from the impact of GPS jamming and spoofing, which may cause other drones to believe they are located far from their actual location.

[4] *See* discussion below in Section V on indoor operations.

[5] In the event the abbreviated link is not functioning, please use the following link: https://www.youtube.com/watch?v=U1YmtOM4RzE&feature=youtu.be. We incorporate the video in our comments by reference.

the past, many of these operations would have been performed by a human under dangerous and difficult conditions.

Unfortunately, the FAA's proposed rule may inadvertently prohibit these safe and beneficial operations. To grasp why the rule may prevent this important, emerging technology, we begin by examining the required message elements. The message elements for limited remote identification UAS include the latitude and longitude of the control station. The message elements for standard remote identification UAS include the latitude and longitude of the control station and the UAS. "The reported position of the unmanned aircraft and the control station must be accurate to within 100 feet of the true position, with 95 percent probability,"[6] and transmitted once a second.[7]

UAS typically rely on GPS receivers to determine their latitude and longitude. Without a solid and reliable GPS connection, a UAS may be unable to transmit latitude and longitude information every second. If the GPS signal were degraded, a UAS may be able to comply with the requirement to transmit latitude and longitude information every second, but fall short of meeting the required accuracy threshold. The proposed rule appears to prohibit operations in those scenarios. Among other potential reasons, operators may only operate UAS "if the [UAS] sends the remote identification message elements . . . from takeoff to landing."[8] If a UAS could not obtain sufficiently accurate latitude and longitude information, it either could not take off or would need to land "as soon as practicable."[9]

Those constraints are unjustified based on the known deficiencies of GPS technology and the safety and efficiency advantages associated with computer vision-enabled UAS. According to the official U.S. government website on GPS technology, "GPS satellites broadcast their signals in space with a certain accuracy," but the information received "depends on additional factors, including satellite geometry, signal blockage, atmospheric conditions, and receiver design features/quality."[10] The limitations associated with GPS accuracy are well documented.[11]

---

[6] *NPRM*, § 89.310(j)(2).
[7] *Id.* § 89.310(j)(5).
[8] *Id.* § 89.110(a).
[9] *Id.* § 89.110(b).
[10] GPS.gov, www.gps.gov.
[11] *See, e.g.,* Olcay Yiğita, Havva Esra Bilişikb, Eren Demirc, Radosveta Sokullud, Korkut Yeğine, *GPS Signal Channel Modeling and Verification*, International Workshop on IOT, M2M and Healthcare (IHM 2017), Procedia

Indeed, anyone who has used a smartphone has almost certainly experienced these phenomena in play. Try to use a ride-sharing service in a dense urban environment, and you are likely to see firsthand the shortcomings of GPS. As discussed by Google, one of the world's largest providers of location information, "[i]n dense urban environments like New York or San Francisco, it can be incredibly hard to pinpoint a geographic location due to low visibility to the sky and signals reflecting off of buildings. This can result in highly inaccurate placements on the map, meaning that your location could appear on the wrong side of the street, o*r even a few blocks away*."[12]

According to the U.S. government, GPS signal is often degraded or denied in three primary scenarios: (1) "Satellite signal blockage due to buildings, bridges, trees, etc."; (2) "[i]ndoor or underground use [of a GPS receiver]"; and (3) "[s]ignals reflected off buildings or walls."[13] **Those scenarios are exactly where UAS with advanced awareness and avoidance features like Skydio provide the most value**. As discussed above, GPS connectivity is notoriously limited in areas that benefit from close-proximity drone inspection operations, such as bridges, cell-phone and radio towers, transmission lines, piers, near structures and inside buildings. Operations in these settings provide tremendous value, often enabling companies to spare humans from conducting delicate and dangerous tasks, such as climbing towers or using bucket-trucks to inspect the underside of bridges (the latter of which also requires shutting down traffic, impacting the travel of individuals and goods along the roadway).

It is imperative that the proposed rule on remote identification recognize and permit safe UAS operations in these settings. Computer vision and other forms of intelligent sensors allow UAS to perform these operations with a high level of safety and accuracy, even when access to GPS is intermittent or nonexistent. The Final Rule must account for, and indeed embrace, the new levels of safety made possible by intelligent situational awareness features. To that end, Skydio respectfully requests that the FAA take the following actions:

Computer Science 113 (2017), p. 621-22, https://tinyurl.com/GPSprocedia ("GPS is not suitable to be used indoors due to signal lost within contact of building walls…. GPS behaves brilliant [sic] in the open outdoor area, but as a result of the low satellite signal power, the signal attenuation phenomenon becomes very serious in the dense urban environment or under the bad weather condition.").

[12] Tilman Reinhardt, *Using Global Localization to Improve Navigation*, Google AI Blog, February 11, 2019, https://ai.googleblog.com/2019/02/using-global-localization-to-improve.html (emphasis added).

[13] GPS.gov, www.gps.gov.

First, the Final Rule should permit UAS operators to declare their intent to operate in a given area using a network Unmanned Aircraft System Service Supplier (USS), and to conduct operations in that area even if they do not have at the beginning of the flight, or they lose during the flight, connectivity to GPS. Skydio suggests permitting a limited mechanism for operators to declare intent regardless of the operating environment, but, at a minimum, it must be permitted in GPS-denied or GPS-degraded areas. Skydio notes that the ASTM standard would permit certain operators to declare their intent to operate in a given area using a network USS.[14] Specifically, the ASTM standard would allow operators of non-equipped UAS to "submit[] an operation plan which identifies the location and schedule for the operation, and the ID of the aircraft."[15] Operators of equipped UAS should be able to comply with remote ID by using the same method, at least in geographical areas with degraded or denied GPS connectivity. This proposed change would not adversely affect the safety or security of the airspace, but would enhance safety by enabling UAS to perform beneficial tasks that would otherwise be done by individuals in environments that can be dangerous. If the FAA is willing only to permit declared-intent operations in the context of GPS-denied or GPS-degraded operations, the FAA could implement that approach by clarifying in the Final Rule that, in the event a UAS is unable to obtain latitude/longitude information because GPS connectivity is degraded or unavailable, operators may continue the operation, provided:

- The UAS continues to transmit the other required message elements (altitude, etc); and
- The operator declares an intention to operate in a given area through a network remote ID USS.

The FAA would also need to clarify that, in the above scenario, a UAS that lacked latitude and longitude information would still be "functional" as that term is used in the rule.

Second, the 100-foot tolerances for the accuracy of location information specified the message elements performance requirements should be increased, at least in areas subject to degraded or denied GPS connectivity. Based on our unique experience designing and building drones capable of compensating for the shortcomings of GPS, Skydio believes that 500 feet

[14] *See* ASTM FY311-19, § 5.5.3.1.
[15] *See id.*

would be a more reasonable standard. As reviewed above, GPS is notoriously unreliable in areas uniquely suited for the use of UAS with computer vision technology. Let us assume, for instance, that the reported GPS position during a particular operation in a dense urban environment is 60 feet or more from the true position of the UAS. If the UAS had even a minimal drift rate of 1%, it could exceed the proposed 100-foot tolerance limit for GPS during the course of a short, one-mile operation (60 feet from the incorrect GPS location, and 53 feet from the drift rate). And this example is optimistic. In dense urban settings, the reported GPS location could easily exceed the 100-foot tolerance by itself.

By increasing the range of permissible location tolerance, the FAA would permit UAS operations in areas that suffer from GPS degradation, and enable UAS operators to conduct their missions in those areas with the corresponding significant benefits in safety and efficiency, e.g., eliminating the need for individuals to climb on, over, or under critical infrastructure. In this regard, the FAA may wish to provide guidance on how the requisite level of locational accuracy will be established. The proposed rule requires location data "to be accurate to within 100 feet of the *true* position."[16] But a variety of factors can cause GPS to report an incorrect position that may be off by a significant margin.

Third, if—despite the justifications outlined above—the FAA is unwilling to relax location tolerances in GPS-degraded or GPS-denied environments generally, the Final Rule should at the very least increase the tolerances to 500 feet for operations very close to structures (which may be subject to degraded or denied GPS connectivity). Specifically, for operations conducted within 20 meters (or 65 feet) of a structure under inspection by a remote pilot operating under 14 CFR Part 107 or a public safety operator flying under 14 CFR Part 91, the GPS tolerances should be increased to 500 feet. Operations conducted within 20 meters of a structure do not present any risk to air traffic because manned aircraft generally could not operate in that area. Skydio believes this recommendation is critically important and would welcome the opportunity to discuss it further with the FAA.

[16] *NPRM*, § 89.310(j)(2).

III. SUPPORTING PUBLIC SAFETY UAS OPERATORS[17]

Public safety agencies across the country employ UAS everyday to protect first responders and members of the public. It is critically important to craft the Final Rule in a manner that minimizes compliance burdens on resource-limited public safety agencies using UAS to perform life-saving work. Skydio has a unique perspective on this issue. The Skydio 2 has been widely adopted by public safety agencies. As a company, we are committed to meeting the needs of public safety stakeholders, who rely on Skydio's autonomy engine to allow first responders to focus on the mission, while the drone focuses on the flying.

Our personnel reflect the priority of this mission. Skydio's Head of Public Safety UAS Integration, Fritz Reber, formerly served as a Captain in the Chula Vista Police Department. In that role, he founded CVPD's path-breaking Drone as a First Responder program, which has conducted 1,702 missions and supported almost 250 arrests. Our Head of Regulatory and Policy Affairs, Brendan Groves, formerly served as Associate Deputy Attorney General at the U.S. Department of Justice, where he oversaw DOJ's drone program across its components. Brendan also served on the 2017 Aviation Rulemaking Committee on Remote ID, co-chairing the Law Enforcement and Security Working Group.

Drawing on that experience, we submit the following recommendations.

A. The Case for Reasonable Limitations on Sharing the Location of Public Safety UAS Operators

To understand this issue, we begin by reviewing relevant text in the proposed rule. Initially, the NPRM makes clear that "the FAA is not proposing for the identity of the owner of the UAS to be included in the message elements, because the message elements would generally be available to the public. The message elements that the FAA is proposing are the minimum necessary to achieve the FAA's safety and security goals while avoiding potential privacy concerns."[18] In addition, "the FAA anticipates that the message elements related to any standard

[17] This section corresponds with and supports many of the important comments submitted by DRONERESPONDERS, a national organization committed to representing the interests of public safety agencies that use UAS in support of their missions.

[18] *NPRM* at 72460.

remote identification UAS or limited remote identification UAS are publicly available information and may be accessed by any person able to receive a broadcast or who has access to a Remote ID USS."[19]

Furthermore, the NPRM states that "the remote identification message elements transmitted by a standard remote identification UAS or limited remote identification UAS to a Remote ID USS may be available to the general public."[20] Specifically, 14 CFR § 89.305(b) and (c)[21] and §89.315(b) and (c)[22] detail the message for standard and limited remote ID. In both cases, the latitude/longitude and altitude of the control station must be included in the message elements. This means that the location of the control station will be available to the public.

Skydio understands that DRONERESPONDERS, a national organization representing the interests of public safety organizations using UAS, will raise concerns that, in certain cases, making the operator's control station location available to the public may place public safety officers at risk. We urge the FAA to address that issue.

B. Accommodating Trusted Operators

Skydio also understands that DRONERESPONDERS will recommend that FAA create limited exceptions to its proposed Remote ID categories, including by allowing additional flexibility for "trusted users," particularly public safety agencies and potentially members of the critical infrastructure industries, whose missions often provide inherent public safety benefits. A "Trusted Users" exception would ensure that responsible and sophisticated entities are able to continue their critical work, while preserving the safe operational environment created by the proposed remote ID rule.

Skydio supports that suggestion, which resembles separate recommendations (including from the Commercial Drone Alliance) to include a Known Operator System ("KOS") category in the Final Rule for remote ID. This category would enhance the effectiveness of any comprehensive remote ID rule beyond a minimum threshold for compliance and would incentivize authorized public safety, law enforcement or commercial operators to proactively gain the trust of government officials and the general public. Ultimately, such a tier would allow

[19] *Id.* at 72471.
[20] *Id.* at 72485.
[21] *Id.* at 72519.
[22] *Id.* at 72520.

the domestic UAS market to realize its enormous potential, to the benefit of the American public and economy.

Skydio supports the KOS concept as a general matter. Establishment of such a framework would benefit public safety agencies, law enforcement, the public, and the commercial UAS industry.

IV. PROTECTING THE PRIVACY OF UAS OPERATORS

Skydio strongly supports measures designed to protect the privacy of commercial, public safety, and recreational UAS operators. In Skydio's view, the proposed rule raises privacy issues that should be addressed in the Final Rule.

As an initial matter, the FAA should clarify what message elements would be publicly available in the network context and what privacy protections would apply to restrict the use of such information. The Preamble indicates that the remote ID message elements transmitted to a Remote ID USS "would be considered publicly accessible information," that they "may be available to the general public," and that Remote ID USS would be "required to provide to the public, for no cost, the UAS Identification message element, either the UAS serial number or session ID."[23] The Final Rule should provide clear, appropriate restrictions on the use of these message elements.

UAS position data can reveal sensitive information about UAS operators and third parties. Uncontrolled access to this information can compromise privacy and commercial sensitivity. FAA should therefore consider including in the Final Rule restrictions on the use of message elements. In the context of network remote ID, the FAA should consider requiring certain technical mitigations for networks, such as the corresponding ASTM Standard F3411, to provide appropriate protections for the transmitted message elements and data. Additionally, the Final Rule should outline performance-based restrictions on data sharing and data disposal between Remote ID USS to prevent the illegitimate use of network data.

Along those lines, Skydio believes that, consistent with the underlying purposes of the proposed rule, the message elements should be available only for legitimate safety, security,

[23] *Id*. at 72485.

compliance, and accident/incident investigation purposes. In addition, there should be a public-facing application for network that enables law enforcement and members of the public to identify a particular UA at the time of flight, but the public should not have access to historical information because, *as to the public*, that information does not fulfill the remote ID rule's objectives. Indeed, if the general public had full visibility and access to the historical data, it could be used for purposes other than those addressed by the rule, including, for example, to track where drone delivery flights begin and end over a period of time. Anonymizing the data, through the use of a session ID or otherwise, does not resolve the issue because the historical data would still reveal information from which identities could be recognized (e.g., the control station's fixed address, repeated flights from a particular warehouse or to a particular destination).[24]

The NPRM proposes requiring Remote ID USS to retain any remote ID message elements for six months.[25] That proposal should similarly be revised to limit the use of any such data. The Preamble indicates that six months was appropriate for FAA enforcement purposes and to balance the interests of security and law enforcement, on the one hand, and privacy interests, on the other hand.[26] The FAA should consider limiting who may use the data held for six months by the Remote ID USS and for what purposes. Access to that data should probably be limited to (i) the FAA, NTSB, law enforcement, or other security agencies solely for legitimate safety, security, compliance, and accident/incident investigation purposes; and (ii) FAA-approved, independent third-party entities, such as academic institutions or FFRDCs, solely for the purpose of supporting safety risk assessments on an aggregated, de-identified basis.

[24] Skydio understands that other parties intend to recommend that the Final Rule should limit the aggregation of historical remote ID data, other than by FAA-approved, independent third-party entities, such as academic institutions or FFRDCs, solely for the purpose of supporting safety risk assessments. We believe the FAA should address this issue in the Final Rule.
[25] *NPRM*, § 89.135.
[26] *Id.* at 72484.

V. ENABLING EQUIPPED UAS TO OPERATE INDOORS

Skydio is concerned that certain parts of the proposed rule may effectively prevent indoor flights of UAS, even though indoor space is not part of the National Airspace System. That would exceed the FAA's jurisdiction and seriously curtail the utility of UAS.

The NPRM proposes to prescribe design and production requirements for UAS. A person would be prohibited from producing a UAS for operation in the United States under Section 89.510, unless the UAS is "designed and produced to meet the minimum performance requirements" for standard or limited remote ID UAS and "in accordance with an FAA-accepted means of compliance." Under the minimum performance requirements for standard and limited remote ID UAS, the UAS would need to be designed and produced to automatically test remote ID functionality when the UAS is powered on, and prohibit the UA from taking off if remote ID equipment is not functional.[27]

As discussed above, most UAS use GPS to determine the position of the unmanned aircraft (UA), and GPS is often unavailable when a UA is operated indoors. In circumstances where GPS is unavailable and where the UA relies on GPS functionality to determine its latitude/longitude coordinates, the UAS would not be capable of transmitting the UA's or control station's location (or, in the case of limited remote ID UAS, only the control station's location), and therefore remote ID would not be "functional." Consequently, under the proposed rule, it may be a violation to fly a standard or limited remote ID UAS indoors. Moreover, the interplay of the proposed regulations might mean that there are no (or very few) commercially available UA that would be capable of flying in an indoor or other GPS-denied environment.

The Final Rule should be modified so that it does not, directly or indirectly, prevent indoor operations of UAS. This issue is important to Skydio. Some of our customers use the Skydio 2's autonomy engine to navigate and map indoor spaces—and even to conduct sophisticated inventory control operations. Indeed, on the day that comments for this rulemaking were due, Ware announced "the first warehouse inventory automation system built on Skydio 2, the world's smartest drone."[28] We urge the FAA to resolve this issue and permit these new, safe,

---

[27] *NPRM*, §§ 89.310 and 89.320.

[28] *Ware launches drone-based inventory automation for $1.9 trillion warehousing industry*, https://ajot.com/news/ware-launches-drone-based-inventory-automation-for-1.9-trillion-warehousing-industry (March 2, 2020).

and incredibly useful operations.

VI. MAXIMIZING FLEXIBILITY FOR OPERATORS AND ENSURING U.S. COMPETITIVENESS IN THE INDUSTRY

The Executive branch and Congress have repeatedly stressed the importance to our economic and national security of maintaining a domestic manufacturing base capable of producing market-leading small UAS.[29] Unfortunately, the FAA's remote ID proposal places the full burden of compliance on manufacturers like Skydio. This top-down, command-and-control approach contravenes longstanding aviation norms and principles of good governance, makes UAS less useful, and inadvertently harms the ability of smaller companies to compete with larger companies better able to bear what could be dramatic compliance costs. It also risks thwarting the government's objective of restoring the domestic production capability for small UAS.

A. Burden Shifting and the Role of Remote Pilots in Command

The NPRM appears to shift responsibility to operate in a safe manner to original equipment manufacturers (OEMs), rather than the pilot in command. For instance, in the case of limited remote ID UAS, the proposed rule directs OEMs to produce UAS incapable of flying more than 400 feet away from the operator. We discuss the flaws with that approach in subsection (B) below. The proposed rule also requires OEMs to ensure UAS cannot take off if remote ID equipment is not functional, instead of simply requiring the system to issue a warning to the remote pilot in command. On that topic, we agree with AUVSI that equipping the system to "lock" the UA if its remote ID is malfunctioning, either upon takeoff or in flight, would be technologically challenging, would raise costs to consumers and operators, and would be fundamentally inconsistent with the idea that the pilot in command must remain in command and bear responsibility for safe operation of the aircraft.

In general, the rule contains a variety of prescriptive requirements that fly in the face of aviation norms, which hold pilots responsible for the safe operation of their aircraft. UAS operations are no different. Under 14 C.F.R. § 91.3(a), the "pilot in command of an aircraft is

[29] Memorandum on Presidential Determination Pursuant to Section 303 of the Defense Production Act of 1950, as amended, June 10, 2019, https://www.whitehouse.gov/presidential-actions/memorandum-presidential-determination-pursuant-section-303-defense-production-act-1950-amended/.

directly responsible for, and is the final authority as to, the operation of that aircraft." OEMs should have the flexibility to manufacture UAS capable of performing multiple missions by different types of operators. It is the responsibility of UAS operators to use the aircraft in a manner compliant with FAA regulations.

During a trip to Davos earlier this year, Transportation Secretary Chao appeared to endorse that approach. During an interview, Secretary Chao characterized the U.S. approach to regulating transportation (including flight) in the following terms: "We are not into industrial policy in this country. We're not into command and control and we're not top-down . . . . We want the consumer . . . to decide how best they want to use these new technologies."[30]

We support Secretary Chao's approach. To achieve that objective, the remote ID rule should empower operators to select the method of remote ID—network, broadcast, or both—that suits the operation they plan to conduct. OEMs like Skydio will manufacture UAS capable of performing the full range of remote ID options. We have a strong incentive to do so, even in the absence of any performance and design requirements. OEMs survive only to the extent that they meet the needs of their customers, and our customers would be required to use reasonable methods of remote identification.

A simple way to implement this streamlined approach would be to replace the standard and limited remote ID UAS categories with a requirement to comply with the ASTM standard on remote ID. The product of a two-year-long, consensus-based industry process, the ASTM standard establishes performance-based requirements for both network and broadcast remote identification, but does not require operators to pick one standard or the other (or employ both). The ASTM standard also enables recreational operators to comply with remote ID without any equipage requirements, keeping our skies open to experienced modelers and beginning pilots exploring the wonder of flight. In the event the FAA decides to require compliance with the ASTM standard and disregards the proposed categories of standard and limited, it is imperative that the Final Rule and the ASTM standard accommodate the proposal on trustworthy autonomy outlined above (in particular, the need to permit safe, autonomy-enabled operations in areas without reliable GPS connectivity).

[30] Secretary Elaine Chao, Interview with Yahoo Finance, January 24, 2020, https://www.youtube.com/watch?v=HeOoAAiLUXI&feature=youtu.be (beginning at 10:00 minutes).

B. The Limited Utility of Limited Remote ID UAS

The NPRM's overly prescriptive approach restricts the utility of UAS without appropriate justification and risks harming manufacturers. In the case of limited remote ID UAS, the rule's 400-foot operational limitation makes little sense. Almost every drone on the market is capable of flying beyond 400 feet from the operator—including many so-called "toy" drones. Forcing drones to remain within 400 feet by design—even when they can safely operate farther away and *fully within visual line of sight*—will make drones less useful, tying the hands of public safety operators, content creators, and Part 107 pilots flying for business.

The limitations associated with the category of limited remote ID carry clear commercial consequences. Drones with limited utility will have a limited market—and, hence, a limited and costly production. Because the same drone cannot satisfy both the limited and remote ID categories in the proposed rule, OEMs may need to produce limited remote ID UAS as a separate product line, even if almost all of the underlying technology is the same. It is difficult to estimate the potential market for a product with such limited range and utility. History has shown that drones are general utility tools; those capable of meeting a range of needs tend to be the most successful and useful. Platforms designed for consumers often work equally well in commercial settings. Drones designed to fill niche interests are less likely to scale. In this rule, the FAA substitutes its own judgment for the wisdom of the marketplace, forcing manufacturers to create separate product lines for the same drone, aside from the way in which it communicates the remote ID elements. Revising the rule to permit operators to choose would offer clear benefits. Among other things, OEMs could pass on the savings from lower compliance costs to their customers in the form of a lower price, which would benefit an industry still in its early stages.

C. Ensuring the Competitiveness of the Industry and the Importance of Regulatory Harmonization

As a result of the restrictive nature of, and the undefined market for, FAA's proposed categories of remote ID UAS, the rule may inadvertently benefit large companies with diverse product lines at the expense of smaller U.S. companies, which may find it challenging to build multiple product lines with unknown commercial viability. To remedy that concern, the FAA

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.

At bottom, to enhance the competitiveness of U.S. UAS manufacturers, streamline the remote ID implementation process, and reduce compliance costs associated with the rule, the FAA should consider placing the primary burden on operators, rather than manufacturers, and harmonizing the U.S. approach to remote ID with other countries. That approach would enhance the competitiveness of U.S. manufacturers like Skydio, in line with the Administration's policy, and bring more choice to the marketplace, ultimately benefiting both consumers and commercial operators.

VII. FACILITATING MANUFACTURER COMPLIANCE

Skydio submits several recommendations designed to ensure rapid and effective compliance with the rule by manufacturers.

A. Means and Declarations of Compliance

To begin, Skydio offers three comments on the proposed rule's notion of means of compliance (MoC) and declarations of compliance (DoC). The proposed rule would require manufacturers to submit a DoC that lists, among other things, the UAS make, model, and serial number or range of serial numbers.[32] It is unclear precisely how manufacturers producing UAS at scale would comply with this requirement. First, Skydio recommends that the FAA allow manufacturers to file DoCs that cover multiple models for which the manufacturer is declaring compliance, simplifying the process without sacrificing any of the substance.[33]

Second, the NPRM does not specify a timeline by which the FAA will review proposed MoCs and DoCs. We recommend that the NPRM commit the agency to review applications and render a decision within 90 days, unless a delay is necessary under the circumstances. The agency should notify applicants of the reason for any delay in writing.

Third, the proposed rule enables the FAA to deny MoC and DoC applications, but does not require the FAA to inform the applicant of the reasons for the rejection.[34] We believe the Final Rule should require the FAA to explain the grounds on which it rejected an application.

---

[32] *Id.* at 72522.

[33] We understand that AUVSI intends to submit the same comment, which illustrates the need for greater clarity on this issue.

[34] *NPRM*, § 89.525(b).

That approach accords with basic due process and administrative procedure. It also benefits the FAA by enabling applicants to understand and remedy any defects in their initial submission.

B. Refining Barometric Pressure Altitude Measurements

The proposed rule requires that barometric pressure altitude measurements be accurate to within 20 feet for altitudes between 0 and 10,000 feet.[35] We agree with AUVSI that this requirement may be somewhat unrealistic, given the size of error known for typical altitude measuring technologies. Instead, the FAA should use a more realistic performance standard, such as that utilized by Transport Canada, which provides for a margin of error in altitude of plus or minus 52 feet.[36] The FAA should not mandate a specific technology to meet this standard.

C. Clarifying the Aeronautical Research Exemption

Under the proposed rule (89.120), FAA-authorized operations for aeronautical research or to demonstrate compliance with regulations may be conducted without remote ID. The NPRM's Preamble provides a general description of "aeronautical research" and notes that "this provision does not extend to any other type of research using a UAS." The proposed rule, however, does not expressly define "aeronautical research" or what it means to be demonstrating compliance with regulations.

Skydio designs, manufactures, and sells advanced UAS. As part of those efforts, it conducts a significant amount of research, testing, and compliance demonstrations before offering a UAS in the marketplace. Commercial research and compliance demonstrations, which as Skydio and other UAS manufacturers and operators conduct as a matter of course, should be expressly listed as part of what the FAA considers to be "aeronautical research" or compliance demonstrations for purposes of the remote ID rule.

In addition, since such UAS operations without remote ID would still require FAA authorization, the Final Rule should provide detailed guidance about how companies would seek such FAA authorization, by what standards the FAA would review such applications, and the timeline envisioned by the FAA for handling such applications.

---

[35] *Id.* at 72477.

[36] *See* Canadian Aviation Regulations, SOR/96-433, Standard 922.02 (Can.).

VIII. REMOTE ID USS SECURITY

Skydio endorses the proposed rule's establishment and use of Remote ID UAS Service Suppliers ("USS") to provide certain important services as part of the remote ID system. Skydio also strongly supports the FAA's proposal in the Preamble to review prospective Remote ID USS for consistency with national security and cybersecurity requirements and export administration regulations.[37] The proposed rule does not categorically preclude foreign companies (or non-U.S. citizens) from serving as a Remote ID USS. Instead, it adopts a thoughtful, risk-based approach. The Final Rule should incorporate this review process into the text of the rule. It should also address the factors relevant to the analysis. Skydio suggests that those factors consider, among other things, whether a prospective Remote ID USS is domiciled in a covered foreign country, as that term is defined in Section 848 of the Fiscal Year 2020 National Defense Authorization Act.

The risks associated with foreign companies serving as a Remote ID USS take two forms. The first risk involves privacy and data protection. Remote ID USS will acquire significant amounts of sensitive information on those who use their services, including personally identifiable information about the operator and a record of the flights (which must be retained for at least six months). The second risk involves the protection of critical infrastructure. As a general rule, the United States, like other nations, seeks to ensure that critical infrastructure assets are not subject to the control of, or influence from, foreign powers. Few assets are more critical than the air traffic control and awareness system. For that reason, it is difficult to imagine that the United States would allow foreign companies, especially those associated with adversarial states, to control or operate the Air Traffic Control (ATC) systems for manned aircraft. In the United States, the number of UAS registered with the FAA greatly exceeds the number of manned aircraft. Skydio welcomes the FAA's proposal to permit private companies to play an important role in the development of a first-of-a-kind UTM system, which this NPRM will facilitate. As this new system will soon be responsible for millions of UAS flights in the low-altitude airspace above American businesses and homes, the FAA and other U.S. government agencies should exercise the same degree of prudence and caution as they would with respect to the manned ATC system and any other critical infrastructure asset.

[37] *NRPM* at 72485.

IX. FAA-RECOGNIZED IDENTIFICATION AREAS

Skydio supports the establishment of FAA-recognized identification areas (FRIAs) as described in the NPRM, § 89.120. However, the proposed requirement that applications for designation as a FRIA be submitted within one year of the Final Rule's effective date is overly restrictive and lacks proper justification. Land use changes over time, as does the need for different types of operations, and the need or desire for a FRIA designation may therefore evolve over time. The Final Rule should take a longer-term approach and recognize that the need for FRIAs may change over the years. The Final Rule should not contain a time limit on when FRIA-designation applications may be filed with the FAA.

In addition, Skydio believes that entities other than community-based organizations (CBO's) should be eligible to apply for FRIA designations.[38] Skydio agrees that FAA-recognized CBOs should be eligible to apply for such designations, but urges the FAA to also allow other entities to apply for such designations. For example, companies or educational institutions that manufacture, operate, test or otherwise use UAS (like Skydio) should be able to apply for designation of a FRIA where they can use UAS without remote ID but within VLOS. Skydio does not believe that there is any, much less a compelling, justification for limiting the pool of FRIA-designation applicants to just CBOs.

[38] Proposed §§ 89.205, 89.210(a).

X. CONCLUSION

Skydio appreciates the opportunity to comment on this important proposal. A system of remote identification that incorporates the above considerations will make UAS operations safer and more efficient, enabling UAS to achieve their full potential to benefit our economy and way of life. Thank you for considering our comments.

Respectfully submitted,

/s/ Adam Bry
Adam Bry
Co-Founder and Chief Executive Officer
Skydio, Inc.
114 Hazel Ave.
Redwood City, CA 94061

/s/ Brendan Groves
Brendan Groves
Head of Regulatory and Policy Affairs
Skydio, Inc.
114 Hazel Ave.
Redwood City, CA 94061