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 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*").

is necessary for full integration of UAS into the national airspace system ("NAS").

While AUVSI fully supports rapid adoption of clear and achievable remote ID standards, it also acknowledges that the goals in promulgating remote ID regulations can best be achieved when compliance is facilitated, technical standards are consistent and performance-oriented, and all stakeholders have a clear understanding of the requirements and benefits of the regulatory regime. As a result, AUVSI submits these comments recommending a number of revisions to the approach offered in the NPRM. Those include recommending a less prescriptive approach when it comes to broadcast versus network compliance; the FAA should promulgate performance-based regulations for the required message elements and UAS service suppliers ("USS") and allow industry to fulfill those requirements. AUVSI also proposes revisions to Ground Control Station ("GCS") requirements, harmonization with international standards, and clarification regarding certain technical proposals, along with other suggestions designed to increase compliance and ensure that UAS operators can pilot safely and efficiently within the new standard.

I. IMPLEMENTATION OF REMOTE ID SHOULD MOVE FORWARD AS QUICKLY AS POSSIBLE.

Remote ID has the potential to allow the development and execution of more complex UAS operations, and therefore to create significant value for the industry and the broader economy. Given the potential benefits of a robust remote ID system, implementation and voluntary compliance should move forward as quickly as possible. The FAA can best facilitate this next step with related proceedings, allowing early compliance, and taking further steps to incentivize remote ID adoption.

A. Three Years Is a Reasonable Time for Mandatory Implementation, But Waiting for Widespread Adoption of Remote ID Should Not Further Delay Proceedings for Authorizing Expanded Operations.

The NPRM provides for an implementation timeline of 36 months—to provide UAS

operators time to acquire hardware, subscribe to a USS, and undertake other transitional steps.[3] This is a generous amount of time to allow the industry to adopt new standards and require compliance across the UAS ecosystem, but there should be incentives for transition, and this implementation timeline should not delay the FAA's other proceedings for integration of UAS into the NAS. Specifically, the NPRM itself references the need for eventual development of a UTM system and "a means to conduct routine BVLOS [beyond visual line of sight] operations."[4] These proceedings, in addition to regulations allowing for nighttime and other complex operations, are necessary for the expansion of UAS innovation and their integration into the NAS.

As a result, the FAA should not wait until the expiration of the remote ID implementation period before moving forward in authorizing expanded operations. Once the FAA adopts a remote ID framework, there is no reason for any further delay in drafting and implementing additional regulatory requirements for expanded operations. The regulatory lead times for adopting new rules allowing expanded operations are such that unless the FAA begins work on these rules immediately following the adoption of the remote ID regulations, there will be further extensive and unnecessary delays in achieving full integration.

B. The FAA Should Allow Compliant Operations Before Full System-Wide Compliance Is Achieved.

The FAA should not only move forward rapidly with rulemakings on expanded operations, it should prioritize permitting expanded operations for operators that are in compliacne with the final remote ID rule, rather than waiting until the compliance timeline expires. Not only would this incentivize rapid implementation among operators, but it would allow the public to reap the benefits of UAS operations sooner rather than later. On the other hand, not allowing compliant

[3] *See NPRM* at 72497.
[4] *See id.* at 72454.

operators to engage in expanded operations within the three-year implementation period would unnecessarily slow the process of airspace integration. As a result, the FAA should allow early voluntary compliance while allowing the full three years for operators who need it.

The FAA can do two things to achieve this goal. *First*, it can immediately begin taking remote ID rule and ASTM Standard Specification for Remote ID and Tracking[5] ("ASTM") compliance into account in 14 C.F.R. § 107.200 and § 107.205 waiver decisions and 14 C.F.R. Part 135 exemption decisions. Operators who voluntarily comply with the FAA's regulations before they are required to do so by law, as well as those who comply with international standards through ASTM compliance, should have such efforts recognized in actions the FAA takes with respect to their flight operations. This was one of the key recommendations of the Drone Advisory Committee ("DAC") in late 2019, when it considered ways in which the FAA could encourage rapid, voluntary compliance with the remote ID regime.[6] As the DAC noted, using remote ID compliance as a means of satisfying waiver or exemption criteria affords a positive, clear benefit for equipping aircraft with remote ID, and offers direct incentives to operators and manufacturers to move forward before the final implementation date.[7]

Second, the FAA can draft regulations allowing expanded operations over people or BVLOS for operations with a remote ID compliant aircraft, even in advance of full, system-wide remote ID compliance. An operator who can certify compliance with remote ID rules should be able to begin operating under any expanded operations regulation on day one, even if full

---

[5] *See* ASTM International, ASTM F3411-19, *Standard Specification for Remote ID and Tracking* (2020) ("*ASTM Remote ID Standard*").
[6] *See* FAA, Drone Advisory Committee eBook 69 (Oct. 17, 2019), https://www.faa.gov/uas/programs_partnerships/drone_advisory_committee/media/eBook_10-17-2019_DAC_Meeting.pdf.
[7] *Id.*

systemwide compliance remains months or years in the future. The FAA's draft remote ID rules properly recognize the importance of moving to full system-wide compliance, but the safety and security goals served by the remote ID rules can be met in individual cases as long as each particular aircraft engaged in expanded operations is remote ID compliant. So long as the operators are compliant, federal, state, local, and tribal law enforcement or security personnel would be able to utilize remote ID tools to determine the identity of individual aircraft engaged in these operations, and take the relevant actions necessary if these operations pose a risk or concern.

C. Consistent with the DAC's Recommendations, the FAA Should Take Further Steps to Incentivize Remote ID Adoption.

The DAC identified three steps that the FAA can take in order to further encourage the rapid adoption of remote ID, even before the regulatory mandate takes final effect.[8] Given the critical importance of remote ID, the FAA should adopt each of these measures as quickly as practicable.

First, the FAA should give preferential treatment to remote ID compliant aircraft in its regulatory processes. The DAC suggested allowing remote ID to be a factor in waiver or exemption decisions.[9] As discussed above, the FAA should implement this recommendation and make compliance with remote ID part of its exemption and waiver decision making process, including the preferential and expedited processing of compliant applications.[10] The DAC also proposed that federal agencies give preference to operators that are remote ID compliant in other processes, as well. The DAC recommended that government agencies procuring a contract for UAS services give preferential treatment to potential contractors who have remote ID.[11] The DAC

[8] *Id.* at 12–13.
[9] *Id.* at 12.
[10] *Id.*
[11] *Id.*

also recommended that the FAA allow voluntarily compliant operators increased airspace access, including in "the outer ring (between the 10 and 30 NM ring) of a 14 CFR 91.141 VIP Temporary Flight Restriction (TFR)" and other restricted areas.[12] It additionally suggested future action to increase airspace access for voluntarily compliant operators, both in future rulemakings, such as those implementing Section 2209 of the 2016 FAA Extension, Safety, and Security Act of 2016, and in investigating raising the allowable altitude for automatic LAANC approvals from zero feet to 100 feet.[13] Each of these recommendations are reasonable, low-cost, high-reward ways for the FAA to incentivize aircraft manufacturers and operators to build and operate remote ID compliant aircraft before the implementation deadline occurs.

Second, the DAC recommended several ways for the FAA to introduce financial incentives for voluntary compliance. The FAA could partner with manufacturers and software suppliers to offer a rebate, like the rebate that was offered for ADS-B implementation.[14] Other financial incentives could include reimbursement of the cost of the Part 107 knowledge exam, if a recognized practical course of training is undertaken with a compliant UAS, discounts on drone-related FAA events for compliant operators, and waivers on future registration fees or renewal for compliant systems.[15] These, too, are reasonable, low-cost ways for the FAA to reach its goal of full remote ID compliance as early as possible.

Third, the DAC recommended that the FAA make the remote ID compliance process transparent, and promote it by publishing both a database of manufacturers that build compliant unmanned aircraft ("UA"), and also a database of qualified USS providers, as well as by

[12] *Id.* at 13.
[13] *Id.*
[14] *Id.*
[15] *Id.*

advertising these and other incentives on the FAA website and apps.[16] Adopting these recommendations would make it easier for operators to identify remote ID compliant equipment, which will help both ensure that new operators purchase compliant drones, and that existing operators are able to find new equipment and software patches to either replace non-compliant legacy UA or retrofit them as quickly as possible.

II. THE FAA SHOULD SET PERFORMANCE REQUIREMENTS, RATHER THAN SPECIFYING PARTICULAR SOLUTIONS FOR REMOTE ID COMPLIANCE.

As emphasized above, remote ID will be most successful when it is most widely adopted. To that end, the FAA can create lower compliance burdens by allowing flexibility in the technological approaches taken by UAS operators. The FAA should thus recognize the contribution of the UAS Identification and Tracking Aviation Rulemaking Committee ("ARC") regarding flexibility; adopt real, performance-based rules that comply with international standards, and do not include prescriptive technology requirements; recognize a need for flexibility where different use cases warrant different approaches; and focus the current rulemaking on the needs of remote ID.

A. The Aviation Rulemaking Committee Recognized the Importance of Flexibility and Noted That Different Technologies May Be Appropriate in Different Contexts.

The ARC identified two viable pathways for unmanned aircraft to remotely identify: broadcast or network remote ID solutions.[17] The ARC analyzed eight different types of technical solutions, some of which were broadcast-based and some of which were network-based. As a

[16] *Id.* at 12–13. This should include the FAA's B4UFLY app, which shows recreational UA users where they may and may not fly, as well as any apps the FAA develops in the future.

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

result, the ARC noted that "[t]hroughout the[ir] discussions . . . members acknowledged a need for tiered, context-appropriate solutions."[18] The ARC thus resisted adopting a top-down, one-size-fits-all technology recommendation.

Subsequently, standards-making bodies like ASTM F38[19] have worked to develop standards that define the parameters of remote ID independent of technology choice; the standards are designed to be agnostic, and manufacturers and operators can comply using either broadcast or network solutions. By the same token, there may be circumstances or applications that require both solutions in order to meet performance requirements.

On the other hand, if the FAA disregards the ARC recommendations, it could have significant negative consequences going forward. The ARC recommendations are the result of hundreds of hours of work by industry and other stakeholders, and thus offer a reasonable, data-driven compromise proposal for remote ID implementation. ARCs are valuable to the FAA's rulemaking processes, as they bring together significant expertise across the industry and save the FAA resources in developing policy that depends on such expertise. Casting these recommendations aside not only will result in worse public policy outcomes, it will also raise significant doubt about the value of ARC participation, potentially disincentivizing future collaboration efforts and jeopardizing a critical FAA resource.

The FAA should support the good faith efforts of the ARC and industry standards-making bodies and implement in its final remote ID rules the recommendations of industry consensus solutions and advice from its advisory committees. By following these recommendations, the FAA can respect security needs, while facilitating high compliance rates with minimal cost and

[18] *See id.*, at 35.
[19] *See Committee F38 on Unmanned Aircraft Systems*, ASTM International, https://www.astm.org/COMMITTEE/F38.htm (last visited Feb. 28, 2020).

low burden to drone owners and operators.

B. The FAA Should Adopt Real Performance-Based Rules in Compliance with International Standards and Avoid Technology Mandates.

The policy undergirding remote ID—and the benefits that will follow—aims to achieve certain outcomes and should thus be agnostic to the technologies used to achieve those outcomes. Yet while the FAA's proposal is ostensibly performance-based, in reality it is based on prescriptive technology mandates: a directive that standard remote ID employ both broadcast and network technologies, and that limited remote ID use only network technology. These directives are inconsistent with the FAA's overall goal of promoting the use of any technology that can meet the agency's performance goals for accurate identification. Therefore, the FAA should adopt a remote ID rule that focuses on performance requirements for reliability and security that are consistent with the ASTM F38 remote ID standard,[20] without requiring the use of particular methodologies to achieve those goals. This approach will enable the most rapid adoption with the highest rates of compliance. These standards indicate the industry's consensus about what is feasible based on existing technology, for drones ranging from complex commercial systems to high-end recreational drones and self-built model aircraft.

C. Different Use Cases Warrant Different Approaches.

Consistent with the foregoing, the FAA should provide additional flexibility and choice for operators and should not require using both network and broadcast remote ID simultaneously in all circumstances. For example, the FAA need not require both solutions for straightforward VLOS operations under existing 14 C.F.R. § 107.31 and more complex operations that are subject to a waiver under 14 C.F.R. § 107.205.

Both the network solution and the broadcast solution have unique benefits and meet

[20] *See ASTM Remote ID Standard*.

common accuracy performance requirements. As the ARC recognized, the network solution boasts a highly effective pre-existing infrastructure run by regulated entities,[21] which can allow for identification at greater range and can provide authentication of user identity. On the other hand, the broadcast solution operates independent of any preexisting network coverage and thus ensures high dependability.[22] Operators may also be concerned about the ability to protect personally identifiable information ("PII") implicated in the required message elements, and should be able to choose a compliance solution that best protects that sensitive information. Indeed, some operators may wish to use both network and broadcast remote ID, as the NPRM proposes. However, doing so should be an option that can be employed where appropriate or needed to meet performance requirements—not a mandate.

To the extent that the FAA has specific objectives in mind, it should set these objectives out, rather than dictating technology. For example, if the FAA believes that it is important to allow a user to be authenticated in particular circumstances, it should lay out those circumstances and allow operators and manufacturers to determine how to meet those goals. Similarly, if the agency wants to ensure that federal, state, local, or tribal law enforcement or security personnel can identify aircraft from BVLOS (for example, from a command center), it should set that requirement out and give parties the ability to work to meet it. It may well be that for particular requirements there is a limited means of complying, and that certain requirements will have the practical effect of dictating current technology choices. However, that type of true performance-based requirement is far different from simply imposing a regulatory mandate that operators employ a particular type of technology, because it allows technology to morph and grow, making

[21] *See ARC Recommendations*, at 34.
[22] *Id.* at 33.

the overall regulatory objective clear and ascertainable.

D. The FAA Should Keep the Focus of the Remote ID Rules on Remote ID.

Although the FAA rightfully acknowledges that remote ID is a necessary building block for UTM and other new UAS technologies, applications, and capabilities,[23] the FAA should not let concerns about how these systems and technologies will work dictate the shape of the remote ID rules. Developments on these issues are ongoing, and international standards bodies are hard at work creating comprehensive solutions.[24] Technology is changing quickly, and the full scope of how UTM may be implemented is not yet known. Therefore, the FAA should be cautious in setting the scope of this rulemaking and prioritize what is directly needed for rapid implementation of remote identification.

III. THE FAA SHOULD EMPHASIZE THE IMPORTANCE OF OPERATOR SECURITY.

A. AUVSI Broadly Supports Making Operator Location Publicly Accessible, but the FAA Should Protect Confidential Information.

Encouraging integration of UAS and adoption of new technologies requires that the public accept and support those technologies. Additionally, law enforcement and first responders need access to data in the event of an emergency. As a result, AUVSI understands the need for public availability of operator location. However, there are also serious privacy concerns involved in the accessibility of locational data. For example, complex operations may have a "headquartered" fixed control station, and thus knowledge of this location could enable the public to determine the operator, even if the operator is using a session ID. Such a compromised situation would be

[23] *See, e.g.*, *NPRM*, at 72454 (UTM), 72476 (detect-and-avoid).

[24] *See, e.g.*, International Civil Aviation Organization, Unmanned Aircraft Systems Traffic Management System (UTM) – A Common Framework with Core Principles for Global Harmonization, Ed. 2, International Civil Aviation Organization, https://www.icao.int/safety/UA/Documents/UTM-Framework%20Edition%202.pdf (last visited Feb. 28, 2020).

contrary to the FAA-intended degree of anonymity.[25]

Because of this complication, the FAA should consider ways to protect confidential information from being inferred in contravention of the principles underpinning the use of a session ID. For example, there may be categories of operator or operation that could, by default, seek to have the ground control station location made available only to law enforcement or security partners, rather than to the public at large. Some possibilities include a "trusted" operator category or a "newsgatherer" certification that would be subject to additional verification, so that the public could trust that the operator was legitimate, while allowing the operator to choose to keep control station location data private.

B. The FAA Should Also Emphasize that Interfering with UAS Operators Is Dangerous and Unlawful.

In addition to confidentiality issues, public knowledge of operator locations can potentially create safety concerns. Although AUVSI acknowledges the importance of public acceptance of UAS, ensuring operator safety in the face of these risks is paramount. Transmitting operator location could lead to productive, positive conversations between people who have concerns about UAS operations and the aircraft's operator(s). However, it also has the potential for confrontation, due to ignorance and frustration with a legitimate UAS operation. In particular, transmitting operator location could lead onlookers to try and engage in self-help in order to curtail UAS operations.[26] This could jeopardize the safety not only of the UA operator and pilot in command

[25] *See NPRM*, at 72473 ("[Using a session ID] would provide a layer of operational privacy. The association between a given session ID and the unmanned aircraft serial number would not be available to the public through the broadcast message.").
[26] *See, e.g.*, *Police: Hammond duo assaulted drone operator*, NNY360 (Apr. 23, 2018), https://www.nny360.com/news/police-hammond-duo-assaulted-drone-operator/article_4a029b14-55d3-52eb-9d47-6316fae89efd.html.

("PIC"), but also the public, should there be a loss of UA control.

Because of these concerns, AUVSI urges the FAA to make clear that interfering with a UAS operator is a federal offense that will be penalized. Under federal law, it is a felony—punishable by up to 20 years in prison—to interfere with an aircraft pilot.[27] The FAA should emphasize that UAS operators fall within the scope of this statute, and that consistent with that rule, the agency will assist federal, state, local, and tribal law enforcement agencies in protecting drone pilots. It should also clearly indicate that protecting UAS pilots will protect the public at large, which is put at risk when individuals interfere with pilots.

IV. THE FAA SHOULD BE MINDFUL OF INTERNATIONAL HARMONIZATION.

International harmonization will facilitate smooth integration of the airspace, as has been the case in manned flight. The FAA is appropriately considering this principle by taking ASTM standards into account in developing Part 89, acknowledging that "consensus standards are one way, but not the sole means, to show compliance with the performance requirements of the proposed [P]art 89," and stating that the agency "intends 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."[28] AUVSI supports these efforts and emphasizes that adopting rules that comply with ASTM standards is important. Harmonization will allow manufacturers and operators to build to a single set of standards globally and will encourage

[27] *See* 18 U.S.C. § 32(a)(5) ("Whoever willfully . . . interferes with or disables, with intent to endanger the safety of any person or with a reckless disregard for the safety of human life, anyone engaged in the authorized operation of such aircraft or any air navigation facility aiding in the navigation of any such aircraft . . . shall be fined under this title or imprisoned not more than twenty years or both.").

[28] *NPRM*, at 72472.

consistency and compliance. For this reason, performance requirements—as discussed *supra*—and message elements should be aligned with the ASTM standard, consistent with industry consensus.

While harmonization is important, the FAA should not pursue this policy to the extent it will result in any delay to finalizing the remote ID rules. Despite the advantages of setting uniform standards, it is likely that different regulatory bodies will make use of the standards in different ways. The benefits of using these industry consensus standards do not require full harmonization with other regulatory bodies, so long as they leverage the ASTM standard. As a result, while the FAA should continue to consider and use ASTM standards in its rulemaking, it should not delay implementation of remote ID in order to achieve full harmonization.

V. AUVSI URGES THE FAA TO MAKE SEVERAL TECHNICAL ADJUSTMENTS TO BETTER EFFECTUATE ITS IMPORTANT POLICY OBJECTIVES.

A. The FAA Should Adopt "UA" as an Abbreviation for the Term "Unmanned Aircraft."

In this rulemaking, the FAA has the opportunity to standardize the language used in remote ID and the UAS industry more generally. In the NPRM, "[t]he FAA is proposing to define a number of new terms to facilitate the implementation of remote identification of UAS."[29] Current FAA regulations define "unmanned aircraft" as "an aircraft operated without the possibility of direct human intervention from within or on the aircraft."[30] However, that definition—unlike other defined terms—does not include an abbreviation,[31] and thus creates ambiguity.

AUVSI urges the FAA to adopt "UA" as an abbreviation for "unmanned aircraft" as part of its new definitions and abbreviations for § 1.1. Adopting "UA" as an abbreviation would further

[29] *NPRM*, at 72461.
[30] 14 C.F.R. § 1.1.
[31] *See id.*

efficiency and harmonization with other stakeholders who use the abbreviation, including the ARC;[32] ASTM standards;[33] the European Aviation Safety Agency ("EASA");[34] and the International Civil Aviation Organization ("ICAO").[35] As with the use of international and industry consensus standards, standardizing this language will allow more efficient coordination of integration efforts.

B. The FAA Should Not Adopt the ARC's Tiered Approach to Remote ID and Tracking Requirements.

The FAA notes that the ARC recommended a complex three-tiered approach to remote ID implementation.[36] The NPRM correctly rejects this three-tiered approach, which layers on complexity that would make navigating the airspace overly cumbersome for operators. Although, as noted above, it is important to take the work of the ARC into consideration, the agency is correct in concluding that the three-tiered structure is unnecessarily complicated and would further slow compliance efforts. AUVSI thus supports a simpler structure with regard to classifying UAS for the purposes of remote ID.

C. The FAA Should Exempt from Remote ID Requirements those UAS that are Required to Use Automatic Dependent Surveillance-Broadcast Out or Air Traffic Control Transponder and Altitude Reporting Equipment.

The FAA is proposing to amend its rules to generally prohibit Automatic Dependent

---

[32] *See ARC Recommendations*, at 9.
[33] *See ASTM Remote ID Standard.*
[34] *See* EASA, Acceptable Means of Compliance (AMC) and Guidance Material (GM) to Commission Implementing Regulation (EU) 2019/947 (Oct. 9, 2019), https://www.easa.europa.eu/sites/default/files/dfu/AMC%20%26%20GM%20to%20Commission%20Implementing%20Regulation%20%28EU%29%202019-947%20%E2%80%94%20Issue%201.pdf.
[35] *See* ICAO, Remotely Piloted Aircraft System (RPAS) Concept of Operations For International IFR Operations, at 1 (Mar. 2017), https://www.icao.int/safety/UA/Documents/ICAO%20RPAS%20Concept%20of%20Operations.pdf ("Unmanned aircraft (UA) include a broad spectrum from meteorological balloons that fly freely to highly complex aircraft piloted from remote locations by licensed aviation professionals.") .
[36] *See NPRM*, at 72458.

Surveillance-Broadcast ("ADS-B") Out and Air Traffic Control ("ATC") transponder use for UAS.[37] An exception to this prohibition would allow the use of ADS-B Out and ATC transponders for UAS where "[1] the operation is conducted under a flight plan and [2] the person operating the unmanned aircraft system maintains two-way radio communication with air traffic control."[38] But under the NPRM, such aircraft would also have to comply with the remote ID rule, which layers a redundant and complex set of technical obligations onto aircraft that are already fully cooperative with existing air traffic control. AUVSI believes that this may be an unintended side-effect of the agency's efforts to ensure that the remote ID rule applies broadly.

In any event, it makes little sense to impose remote ID rules on aircraft that are already subject to ATC, and AUVSI thus encourages the FAA to exempt UAS operating pursuant to this exception from the remote ID requirements. ADS-B Out and ATC transponders broadcast UAS' identity, position, and velocity,[39] thus allowing air traffic controllers to "identify aircraft under radar surveillance," obtain "the location of the aircraft," and "correlate the target to a flight plan."[40] These capabilities are sufficient to meet the FAA's twin goals of safety and security in adopting these remote ID rules.[41] Indeed, by virtue of being in contact with ATC, these UAS are already fully integrated into the NAS, and need not also have remote ID (any more than manned aircraft do). While the FAA emphasizes the need for universal compliance with Part 89 in order to lay the building blocks for UTM, exempting these aircraft will not have a practical impact on UTM,

[37] *See id.* at 72487–88.
[38] *Id.* at 72487.
[39] 14 C.F.R. § 91.227(a) (emphasis added) ("*ADS-B Out* is a function of an aircraft's onboard avionics that periodically broadcasts the aircraft's state vector (3-dimensional position and 3-dimensional velocity) and other required information as described in this section.").
[40] *NPRM*, at 72452.
[41] *Id.* at 72460 ("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.").

because these aircraft are few in number and are much more similar to manned aircraft in terms of integration than they are to smaller UAS.

AUVSI thus suggests the following change to the FAA's proposed 14 C.F.R. § 89.120:

> § 89.120 Unmanned aircraft systems without remote identification. A person may operate an unmanned aircraft system that does not meet the requirements for a standard remote identification unmanned aircraft system under § 89.110 or a limited remote identification unmanned aircraft system under § 89.115 only if the requirements of (a), (b), or (c) are met.
>
> (a) Operations at FAA-recognized identification areas. Unless otherwise authorized by the administrator: (1) The unmanned aircraft system is operated within visual line of sight. (2) The unmanned aircraft system is operated within an FAA-recognized identification area.
>
> (b) Operations for aeronautical research. The person is authorized by the administrator to operate the unmanned aircraft system without remote identification for the purpose of aeronautical research or to show compliance with regulations.
>
> (c) The operation is conducted under a flight plan and the following conditions are met: (1) The UAS meets the requirements stated in 14 C.F.R. § 91.225 or § 91.215. (2) The person operating the UA maintains two-way radio communication with ATC.

D. AUVSI Urges the FAA to Avoid Becoming Entangled in Issues of Spectrum Management.

In the NPRM, the FAA correctly notes the complexity involved in spectrum management issues. For example, the NPRM explains that "the FAA would consider proposed methods for dealing with interference considerations and would verify that they are appropriate for the types of equipment and operations applicable to those means of compliance and do not run counter to any applicable regulations, including [Federal Communications Commission ('FCC')] regulations."[42] It also "envisions that remote identification broadcast equipment would broadcast using spectrum similar to that used by Wi-Fi and Bluetooth devices," but declines to identify a

[42] *Id.* at 72476.

"specific frequency band."[43]

While the FAA is correct to recognize that remote ID implicates important spectrum questions, the FAA need not and should not make granular decisions regarding the allocation and use of spectrum, including (for example) setting RF interference requirements. Rather, such decisions are fully within the purview of the FCC and the National Telecommunications and Information Administration ("NTIA").[44]

To the extent the FAA offers any guidance on spectrum issues, that guidance should be performance-based, and should recognize that different environments pose different spectrum challenges. The FAA should leave it to manufacturers and operators to develop standards to mitigate the difficulties of operating in complex spectral environments.

E. The FAA Should Recognize Clear Encryption and Tamper Resistance Standards as a Baseline for Compliance.

As indicated in the complex considerations of safety, transparency, and compliance involved in a remote ID rulemaking, the security of the message involved in remote ID is paramount to the system's success. As such, the NPRM provides that "[t]he Remote ID USS and UAS producers would be responsible for ensuring that UAS remote identification data and connections would be protected against cyber-attacks."[45] Additionally, the text for proposed regulation 14 C.F.R. § 89.310(k) states, "[t]he unmanned aircraft system must incorporate cybersecurity protections for the transmission and broadcast of the message elements[.]"[46]

In order to best facilitate compliance with this requirement and security of the data involved, however, the FAA should provide the industry with guidance on this point. Specifically,

---

[43] *Id.*
[44] *See, e.g.*, 47 U.S.C. §§ 303, 305; 47 C.F.R. § 2.105.
[45] *NPRM*, at 72485.
[46] *Id.* at 72520.

the FAA should recognize one or more performance-based industry standards for encryption that are sufficient to satisfy this requirement. AUVSI does not advocate for prescriptive technological requirements, but providing a specific standard that is sufficient to satisfy this requirement would have positive outcomes for both the FAA and UAS operators: the FAA would incentivize compliance with a standard of which it approves, and operators would have at least one clear path to compliance.[47]

Relatedly, the NPRM requires UAS producers to "design[] and produce[] [UAS with remote identification] in a way that reduces the ability of a person to tamper with the remote identification functionality."[48] The NPRM and the proposed regulations do not specify what kind of tamper resistance features would be compliant with this requirement. For example, physical tamper resistance could range from screws that use non-standard bits to glued-down circuit boards to more robust, military-grade tamper resistance features. Software tamper resistance has a similar range in terms of complexity, cost, and degree of resistance. Accordingly, AUVSI requests that the FAA clarify a mode of compliance, or set a performance standard that more clearly defines what level of resistance is expected.

F. The FAA Should Protect Operator Data.

The NPRM's final rule on data retention should include limitations on the type of public entities that can access historical data stored by a remote ID USS—directly or indirectly—and that

---

[47] *Cf.* U.S. Chamber, Institute for Legal Reform, Mapping a Privacy Path: Liability and Enforcement Recommendations for States, at 11 (Dec. 2019), https://www.instituteforlegalreform.com/uploads/sites/1/Privacy_Policymaking_Report_Liability_and_Enforcement_Recommendations_for_States.pdf ("[S]afe harbors give businesses certainty that the processes they are putting in place—which often require significant organizational resources—will actually meet or exceed the requirements of the law and protect them from liability. This type of assurance goes a long way in incentivizing desired behaviors. In its absence—and in light of the complex and ever-developing state of privacy and security law—businesses lack certainty that their compliance efforts will protect them from liability.").

[48] *NPRM*, at 72475.

can correlate public information (session ID) with non-public information (*e.g.*, registration and contact details). The NPRM requires remote ID USS providers to store remote ID message elements for six months after transmission.[49] As discussed above, these message elements contain sensitive information about operators and their flight operations, and while retention of such information may be necessary for law enforcement and other public safety considerations, such data should also be protected from misuse. To implement these protections, the rule should outline both performance-based restrictions on data sharing between USS providers and a legal process for access and correlation of that data, consistent with community expectations of due process. These restrictions should prevent illegitimate use of operator data. Additionally, having such a process clarified before the rule's implementation will ensure that those who need access to such data will have a clear path to access it, and that any disputes over such access issues have an appropriate resolution mechanism. This process should appropriately balance transparency and law enforcement with operator privacy and security, and should limit access to that which is required for compliance auditing, incident investigation, and security. Finally, the rule should clarify who is required to retain USS data and for how long and ensure robust protection of such data. While the rule requires protections against cyberattacks, the rule should also give more guidance about how USS providers need to protect sensitive data.

G. The FAA Should Allow Community-Based Organizations to Apply for, and Renew, FAA-Recognized Identification Areas Beyond 12 Months.

Among exceptions to the remote ID requirement, the NPRM "proposes in § 89.205 to only allow a [community-based organization ("CBO")] recognized by the Administrator to apply for the establishment of an FAA-recognized identification area ["FRIA"]. . . . Under the proposed § 89.210, a request to establish an FAA-recognized identification area would have to be submitted

[49] *Id.* at 72518.

within 12 calendar months from the effective date of a final rule."[50] The FAA reasons that such a timeline is logical because "the FAA also expects that as compliance with remote identification requirements becomes cheaper and easier, the need to operate only at FAA-recognized identification areas would likely decrease."[51] AUVSI supports the existence of a mechanism for CBOs to establish such areas; however, such a limited timeline for the applications of such areas would significantly limit their effectiveness. Recreational users—like those who would likely utilize FRIAs—are a source not only of public interest in UAS, but of individuals who may eventually make up the labor force of the UAS industry. The establishment of FRIAs accomplishes the goal of the rule, as "the FAA-recognized identification area itself becomes the form of identification."[52] Additionally, as the FAA acknowledges, "[s]hould the FAA not allow [FRIAs] . . . for the operation of UAS without remote identification, it is estimated that as many as 400,000 UAS that are used for recreational flying would be grounded at the end of year 3."[53] The limitation of the application window to only twelve months will similarly result in the loss of use of UAS in areas in which new CBOs could otherwise have formed after the twelve-month mark, or in which existing CBOs could have discovered a need for an addition FRIA after the time to apply expired. The FAA acknowledges that FRIAs comply with the goal of the remote ID rule and prevent the loss in value of legacy UAS; therefore, the FAA should allow CBOs to establish FRIAs more than one year following the effective date of the final rule.

H. Manufacturer Compliance Should Be Streamlined.

The FAA proposes to require manufacturers to submit a declaration of compliance ("DoC") that lists, among other things, the UAS make, model, and serial number or range of serial

[50] *NPRM*, at 72486.
[51] *Id.* at 72500.
[52] *Id.* at 72504.
[53] *Id.*

numbers.[54] There is limited information in the NPRM regarding how large UA manufacturers can achieve a DoC for batch production of a particular model; this could be undertaken via a Part 107 waiver, a Part 135 exemption, or a Part 21 Durability and Reliability ("D&R") process. This could also be achieved under the Modernization of Special Airworthiness Certificates ("MOSAIC") process.[55] AUVSI urges the FAA to allow manufacturers to file DoCs that cover multiple models for which the manufacturer is declaring compliance, so as to simplify the process for manufacturers without losing any of the substance. Additionally, the process for accepting a DoC should be on as short of a timeline as possible to facilitate rapid compliance.

I. The Responsibility for the Preparation and Execution of a UA Flight Should Remain with the Pilot in Command, and not a Take-Off Lock.

The current proposal requires, under proposed 14 C.F.R. § 89.320(d)(2), that a UA be unable to take off if its Remote ID equipment is not functioning.[56] However, under 14 C.F.R. § 91.3(a), the "pilot in command of an aircraft is directly responsible for, and is the final authority as to, the operation of that aircraft."[57] This should continue to be the case for UA pilots: while the UAS should provide an indication of malfunction to the pilot in command ("PIC"), it must be the responsibility of the PIC to determine the appropriate action to take. Requiring 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 PIC must remain in command and bear

[54] *Id.* at 72522.
[55] *See Pushing GA Forward with MOSAIC*, EAA (Jan. 3, 2019), https://www.eaa.org/en/eaa/news-and-publications/eaa-news-and-aviation-news/news/2019-01-03-Pushing-GA-Forward-With-MOSAIC?mkt_tok=eyJpIjoiWkdSaE5XTXpNalEwTkRjdyIsInQiOiJ2ODlMcWpIQmx2VXFVbDVNNUJLaGlKNGZqSEZvYkRLZDU4OUtEenBsWVViVGhZYWIxSkFjcllYXC9VeEtPK2tTQzZRS3dXRzFIT3JmQytoOFNBeURVc1E9PSJ9&fbclid=IwAR3vi5MmNSDNBRngWhTAzJJ2B9FdMgBPa3P47yIvlb-prs5Mt1GrTeGt7MA.
[56] *NPRM*, at 72520.
[57] 14 C.F.R. § 91.3(a).

responsibility for safe operation of the aircraft. Moreover, take-off locks would have the effect of impermissibly extending the FAA's regulations into areas where UAS have the legal right to fly and that the FAA cannot legally regulate, such as indoor environments.

J. The Accuracy Requirements for Positioning Are Unrealistic and Should Be More Lenient.

The proposed rule requires that barometric pressure altitude measurements be accurate to within 20 feet for altitudes between 0 and 10,000 feet.[58] However, this is 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; this standard provides for a margin of error in altitude of plus or minus 52 feet, and plus or minus 33 feet in lateral positioning.[59] The FAA should not mandate a specific technology to meet this accuracy standard.

VI. THE FAA SHOULD ISSUE FURTHER CLARIFICATION ON SEVERAL OF ITS POLICY CHOICES.

A. The FAA Should Provide More Information Regarding Its Rationale for Mandating the Provision of a Control Station's Barometric Pressure Altitude.

The FAA is currently looking to require "an indication of the control station's barometric pressure altitude, referenced to standard sea level pressure of 29.92 inches of mercury or 1013.2 hectopascals," for both standard and limited remote ID.[60] AUVSI asks the Commission to provide further information on this policy choice, by answering four key questions.

First, AUVSI requests clarification as to how the FAA will contend with the fact that many ground control stations will not have the capability to record barometric altitude.

Second, AUVSI asks the FAA what performance-based goal it seeks to achieve by

[58] *NPRM*, at 72477.
[59] *See* Canadian Aviation Regulations, SOR/96-433, Standard 922.02 (Can.).
[60] *NPRM*, at 72473.

mandating ground control station height location information. If the FAA intends to use this data to allow emergency personnel to determine which floor of a particular building an operator is standing on, compliance with that standard may not be technically feasible. Ground control station altitude information is not easily ascertainable to the required level of accuracy and certainty with existing technology. For example, the FCC currently has before it a similar issue in its proceeding on location accuracy in wireless 9-1-1 calls.[61] In that proceeding, it noted that GPS and cell-network based error thresholds have ranged from 1.8 meters to 4.8 meters for commercial mobile radio services (including cell phones).[62] While the FCC is proposing new rules that will tighten accuracy standards in order to allow first responders to find and identify particular floors, these standards will not take effect for several years—in the interim, few, if any, wireless devices will provide position data accurate enough to be useful for this purpose. It is not clear that any UAS control stations would be able to achieve better accuracy in the near term. Similarly, under the FAA's regulations for manned aircraft, the expected error threshold for barometric altitude under 1000 feet is plus or minus 20 feet,[63] an error threshold that will likely not allow the FAA to accomplish its goals with this section of the regulation.

Third, given that many operators will likely be operating UAS from a laptop or a cell phone, AUVSI requests clarification on how the FAA would confirm that an operator was using compliant technology, *e.g.*, the correct cell phone, and whether such technology is widely available for cell phones and laptops. Using third-party, operator-supplied equipment to provide any of the information or technical capability necessary to meet the remote ID standard would present an

[61] *See Wireless E911 Location Accuracy Requirements*, Fifth Report and Order and Fifth Further Notice of Proposed Rulemaking, FCC PS Docket No. 07–114 (Nov. 25, 2019), amended by Erratum (Jan. 15, 2020).
[62] *Id.* ¶ 5.
[63] *See* 14 C.F.R. § 43 Appendix E.

enormous challenge for UAS manufacturers. Even if particular devices could be certified as compliant, the product cycle for consumer devices would soon render any list of compliant devices obsolete—and, indeed, software changes made by third-party manufacturers could impact the compliance of even a device that had been tested and found to work.

B. The FAA Should Provide More Information on Its Plans for UAS Type Certification in Light of the Fast-Approaching End to the UAS Integration Pilot Program.

Currently, the FAA, through its UAS Integration Pilot Program ("IPP"), allows operators to receive either Part 107 waivers or Part 135 air carrier certification exemptions for UAS.[64] However, the IPP is slated to end in October 2020, and the exemptions that the FAA has granted to existing operators terminate at certain dates, necessitating renewal of those so authorized. This introduces uncertainty both for operators who currently operate pursuant to the IPP and for operators who hope to receive such certifications in the future.

AUVSI understands that the FAA plans to implement an interim solution: the D&R Means of Compliance initiative, via issuance of a type certificate for special classes of aircraft that are novel and/or unusual in design, under 14 CFR Part 21.17(b) Amdt 21-60. In order to resolve some of the uncertainty around the sunset of the IPP, as well as the availability and requirements of this new initiative, the FAA should provide further details about this program and the future of UAS type certifications. This ought to include comment on the MOSAIC initiative, and whether existing Part 107 waivers and Part 135 exemptions will be extended for compliance purposes until September 2023 as a result.[65] If the FAA does not do so in this proceeding, then it should address such questions in a future rulemaking.

C. The FAA Should Provide More Information Regarding the Exception for

[64] *See Package Delivery by Drone (Part 135)*, FAA (Oct. 1, 2019), https://www.faa.gov/uas/advanced_operations/package_delivery_drone/.
[65] *See* 49 U.S.C. § 44807(d).

"Aeronautical Research."

Among its exceptions to remote ID compliance, the FAA includes "UAS designed or produced exclusively for the purpose of aeronautical research."[66] Specifically, the proposed draft of 14 C.F.R. § 89.120(b) allows a person to operate a UAS that is not remote ID-compliant if he or she is authorized by the administrator to operate it "for the purpose of aeronautical research or to show compliance with regulations."[67] Proposed 14 C.F.R. § 89.501, which governs the scope of design and production of UAS, excepts "[u]nmanned aircraft systems designed or produced exclusively for the purpose of aeronautical research or to show compliance with regulations" in Section 89.501(c)(4).[68] The NPRM notes that "the FAA would consider aeronautical research to be limited to the research and testing of the unmanned aircraft, the control systems, equipment that is part of the unmanned aircraft (such as sensors), and flight profiles, or development of specific functions and capabilities for the UAS."[69] However, "aeronautical research" is not defined with the proposed rule text itself nor in the FAA's existing rules,[70] and this explanation remains ambiguous. In order to limit uncertainty in the design and testing process and to promote compliance, the FAA should clarify exactly what kinds of operations would qualify under the "aeronautical research" exception and clarify that it includes commercial research and development activities, subject to approval.

VII. CONCLUSION

Remote ID is a vital step toward the complete integration of UAS and the ability to harness the promise of future UAS technology. AUVSI appreciates the opportunity to participate in this

---

[66] *NPRM*, at 72480.
[67] *Id.* at 72518.
[68] *Id.* at 72522.
[69] *Id.* at 72467.
[70] 14 C.F.R. § 1.1 mentions "aeronautical research" in the definition of "public aircraft," but does not define it.

rulemaking proceeding and looks forward to collaborating with the FAA in the future as the Administration continues to promote UAS innovation.

Respectfully submitted,

THE ASSOCATION FOR UNMANNED VEHICLE SYSTEMS INTERNATIONAL

/s/ Joshua S. Turner

Brian Wynne
President and CEO
AUVSI
2700 S. Quincy St., Ste 400
Arlington, VA 22206

March 1, 2020

Joshua S. Turner
Sara M. Baxenberg
Boyd Garriott
WILEY REIN LLP
1776 K Street, N.W.
Washington, D.C. 20006

Counsel to AUVSI