BEFORE THE
DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION
WASHINGTON, D.C.

REMOTE IDENTIFICATION OF UNMANNED AIRCRAFT SYSTEMS – NOTICE OF PROPOSED RULEMAKING

Docket No. FAA-2019-1100

COMMENTS OF THE SMALL UAV COALITION

Gregory S. Walden
McGuireWoods Consulting, LLC
2001 K Street NW, 4th floor
Washington, DC 20006
Counsel to the Small UAV Coalition

March 2, 2020

Filed with www.regulations.gov

BEFORE THE
DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION
WASHINGTON, D.C.

REMOTE IDENTIFICATION OF UNMANNED AIRCRAFT SYSTEMS – NOTICE OF PROPOSED RULEMAKING

Docket No. FAA-2019-1100

COMMENTS OF THE SMALL UAV COALITION

The Small UAV Coalition[1] (Coalition) provides its comments in response to the FAA's Notice of Proposed Rulemaking (NPRM) for Remote Identification of Unmanned Aircraft Systems, 84 Fed. Reg. 72438 (Dec. 31, 2019).

General Comments

The Coalition supports the proposed rule, with important revisions

The Small UAV Coalition applauds the FAA for moving the remote identification (remote ID) rulemaking forward and commends the FAA, which faced complex considerations when developing this proposal, for its continued engagement with industry to further development of this and future regulations. The Coalition has consistently called for a remote ID rule as the next critical step in enabling ubiquitous unmanned aircraft systems (UAS) operations for a myriad of use cases and unlocking further regulatory measures to authorize advanced, more complex operations, at scale. An Unmanned Traffic Management (UTM) system, the ultimate architecture

[1] Members of the Small UAV Coalition are listed at www.smallauvcoalition.org.

for the entire UAS ecosystem, must consist of UAS operators with remote ID technology. Once the rule is in place, public authorities will be able to identify operators who are compliant and address those who are noncompliant. Therefore, the Coalition generally supports the FAA's NPRM.

In several significant respects, however, the Coalition believes certain elements of the proposed rule warrant revisions to maximize the final rule's effectiveness. Most notably, the Coalition believes that UAS operators should be permitted to use network or broadcast remote ID, subject to meeting performance requirements, as set forth in the ASTM standard and reflected in the proposed rule, in their specific operating environment.

Detailed section-by-section comments are provided below.

The Coalition supports measures to promote compliance and early equipage

In the preamble to the proposed rule, the FAA seeks comments on whether waivers for operations over people (OOP), at night, or for other purposes, should be conditional on remote ID equipage that is in compliance with the proposed requirements. The Coalition supports FAA's proposal to provide incentives to early adopters of remote identification. The FAA should incentivize operators to promptly implement remote ID to enhance safety and security and lay the foundation for more in-demand complex operations in the sector's fastest-growing segment.

The Coalition supports allowing certain waivers to be augmented with remote ID equipage, but believes that incentives should also be employed, such as fast tracking waivers for night operations

and operations over people (in compliance with the operational limitations in the FAA's NPRM). For example, UAS with remote ID that are compliant with message element and other performance requirements in this proposed rule could be given special permission to operate in national parks, certain controlled airspace, and near military bases.

One of the first taskings of the Drone Advisory Committee (DAC) was to explore options to encourage voluntary early remote ID equipage. The Coalition provided several ideas to the DAC and the DAC provided a series of recommendations to the FAA last year. The Coalition endorsed the DAC's recommendations and urged the FAA to act on these recommendations during the pendency of this rulemaking. The Coalition is pleased that at the February 27 DAC meeting, the FAA committed to a number of the DAC's recommendations, including:

- Using remote ID equipage as risk mitigation in Part 107 waivers;
- Creating FAA online databases of FAA-accepted manufacturer declarations of compliance and remote ID service suppliers (Remote ID USS);
- The FAA's commitment to work with interagency security partners to use remote ID equipage as a positive consideration in authorizing access to airspace to which security instructions have been applied, including Temporary Flight Restrictions; and
- Encouraging State and local governments to proactively consider the benefits of remote ID equipped aircraft.

Compliance dates should be shortened

As explained more fully in the following detailed comments, the Coalition believes 36 months is too long a period to allow the industry to come into compliance, as well as too long a period for

recreational operators to register each unmanned aircraft they own. The FAA can and should shorten the compliance deadline in proposed 89.105 for manufacturers and operators in recognition that the ASTM remote identification standard is available for FAA's review and acceptance well before the final rule becomes effective, thereby eliminating the one-year period the FAA has allotted for the development of a FAA-accepted means of compliance. The FAA can also accelerate the registration deadline in proposed section 48.5, especially if it provides an incentive to registration as the Coalition recommends below.

Privacy interests of UAS owners and operators should be protected

The Coalition supports the FAA's recognition of the privacy interests held by UAS operators. While the Coalition expects that the accountability that comes with the remote ID rule will deter irresponsible operations, including invasions of privacy by UAS, the privacy interests of both UAS end-users and operators are also deserving of protection. As discussed more fully in the detailed comments on section 89.135, the FAA should limit the (1) type of entities that can access historical data stored by a Remote ID USS, (2) the purpose for accessing the data within a 30-day period and (3) the correlation of public information (e.g., session ID) with non-public information (e.g., registration and contact details). Consistent with the FAA's explanation in the preamble to the proposed rule, the final rule should include clear requirements and processes to access and correlate registration data, and limit such access to law enforcement and national security entities upon an adequate factual and legal predicate, such as probable cause. The Coalition also supports the FAA's intention to require a Remote ID USS to agree to privacy protections in the Memorandum of Agreement. The Coalition also recommends that FAA revise its proposed requirement that a Remote ID USS retain data for six months to 30 days and to limit its own

retention of this data to the same period of time the FAA adopts for Remote ID USSs in the final rule.

The Coalition supports international harmonization of remote ID rules and standards

The Coalition generally supports international harmonization of UAS rules and standards to the maximum practical extent. With respect to remote ID, the Coalition urges the FAA to continue to engage with the European Commission in an effort to adopt similar remote ID regulatory frameworks, including message elements and performance requirements. As explained in its detailed comments, the Coalition recommends changes to the set of message elements to match those adopted by the Commission.

The Coalition supports the role of Remote ID UAS Service Suppliers

The Coalition supports the use of private sector (and government) Remote ID USS to receive the transmission of the required message elements from network remote ID UAS. The Coalition recognizes that the FAA has not proposed any requirements in the NPRM (other than data retention in proposed section 89.135), and that the FAA intends to handle the Remote ID USS process through contractual Memoranda of Agreement. The Coalition agrees with the FAA that the Low Altitude Authorization and Notification Capability (LAANC) process may serve as a model for the Remote ID process. The Coalition notes further that the FAA is not proposing to set requirements for remote ID USS business models with respect to fees, user agreements, and other matters.

Detailed Comments

Part 48 – Registration and Marking Requirements for Small Unmanned Aircraft

48.5 Compliance dates

The proposed rule would require previously registered UAS, including aircraft registered exclusively as model aircraft, to come into compliance 36 months from the effective date of the final rule, or when renewal is required, whichever is sooner. The Coalition believes that one year is enough time for an owner of multiple UAS to come into compliance with the new requirement. As stated below, the Coalition believes that compliance could be accelerated by offering a discounted registration fee.

48.15 Requirement to register

The Coalition supports the proposal to continue to exempt from the registration requirement unmanned aircraft that weigh 0.55 pounds or less on takeoff, including payload. The proposed rule, following section 349 of the FAA Reauthorization Act of 2018, 49 U.S.C. 44809, would change the label from "model aircraft" to "limited recreational aircraft." The Coalition supports this provision, which requires registration of drones weighing 0.55 pounds or less that are used for commercial services or that will operate beyond the visual line of sight of the remote pilot.

48.30 Fees

In proposing to require a $5 fee for each drone registered, the Coalition believes that the fee requirement may be more than nominal for individual owners of multiple drones. Thus, the Coalition supports the FAA's statement in the preamble that it "would explore ways to minimize the registration fee when multiple aircraft are registered at the same time." 84 Fed. Reg. at 72463.

In particular, the Coalition urges the FAA to offer a single $5 fee to an owner of multiple aircraft who registers all aircraft at the same time *and* within a certain period, such as 30 or 60 days. That option would also encourage prompt compliance with the registration requirement.

48.100 Application

The proposed rule would require the same information to be submitted in a registration application for both a standard and limited remote ID UAS. The Coalition supports this proposal, as well as the proposal to add an owner's telephone number as required information, provided that such information is not subject to public disclosure.

Part 89 – Remote Identification of Unmanned Aircraft Systems

Subpart B – Operating requirements

89.101 Applicability

The Coalition supports the requirement that all drones weighing 0.55 pounds or more, as well as drones used for commercial purposes or that will be operated beyond visual line of sight (BVLOS), be subject to remote ID requirements, as further modified by the Coalition's recommendations below.

89.105 Remote identification requirements

The Coalition supports setting a compliance date after which no UAS may be operated unless it complies with the standard or limited remote ID requirements, as applicable, or is exempt from remote ID requirements as set forth in proposed section 89.120. However, the Coalition believes the 36-month compliance date is too long. The Coalition recognizes that remote ID standards, an

FAA-accepted means of compliance, and an FAA-accepted declaration of compliance are prerequisites for compliance with the proposed remote ID requirements, and that these steps will take time. However, the ASTM F38 New Specification for UAS Remote ID and Tracking has been published, and thus believes the compliance date should be shortened to the 18 to 24 month range.

89.110 Standard remote identification unmanned aircraft systems

The Coalition shares the FAA's goals of ensuring that the remote ID rule is capable of promoting safety, security, and privacy of UAS operations without imposing an unreasonable economic burden on any segment of the UAS community. Further, the Coalition, consistent with past comments, supports the FAA's reliance on performance-based requirements and industry standards. The Coalition agrees network and broadcast remote ID both offer opportunities to fulfill these shared goals, and that the FAA's proposal to require both network and broadcast remote ID would enhance safety and security through redundancy. *However, the Coalition recommends a performance-based approach to remote ID that permits UAS operators a choice between network or broadcast when the network is available.*

The fundamental requirement for remote ID, regardless of technology, is to meet the minimum performance-based requirements included in the proposed rule, based on ASTM's performance-based standard. In that regard, there are significant benefits from network remote ID, including: readily available and tested solutions (as demonstrated in the LAANC program) and near ubiquitous availability. Beyond the scope of this proceeding, longer term benefits of network remote ID include connectivity with USS networks and the ability to assist in the safety and efficiency of a UTM system.

Allowing a UAS operator to choose either broadcast or network remote ID transmission in line with required performance standards in the specific operating environment will increase compliance. Further, meeting these requirements will satisfy the accountability objectives of the law enforcement and national security communities.

The choice to transmit using either network or broadcast remote ID does not preclude a UAS from being capable of using both technologies. In fact, a number of operators will utilize both technologies.

Accordingly, the Coalition recommends the FAA allow either network or broadcast remote ID technology for standard remote ID UAS. Recognizing that network remote ID will be needed to enable advanced operations, different remote ID systems are appropriate for different aircraft and operations. The rule should permit standard remote ID UAS operators to select the most appropriate technology for their operations provided the UAS complies with required performance standards in the specific operating environment.

89.115 Limited remote identification unmanned aircraft systems

As explained above, standard remote ID operations should be those in which key message elements are shared in real-time via integrated broadcast equipment or the USS network. Limited remote ID should be permitted to declare flight intent via a Remote ID USS, consistent with the process for LAANC declarations. Declaration of flight intent for limited remote ID should be subject to clear performance requirements, but would not require a persistent connection to the USS network. The

distinction between standard and limited remote ID UAS operations should be based on the risk and capabilities of different UAS, and the extent of integration that can be achieved between the remote ID system and the aircraft system. The limited category would mean include amateur-built and non-automated UAS. These limited UAS would not be permitted to engage in complex operations (e.g., BVLOS). However, these UAS would be permitted to operate in public and private areas beyond FAA-recognized (non-) identification areas, subject to compliance with applicable regulations.

Industry has recently demonstrated declaration via the USS network in the US and overseas using non-equipped hobbyist aircraft flying in controlled and uncontrolled airspace, consistent with the ASTM remote ID standard, the same approach taken to airspace authorization requests under LAANC.

Based on recent proofs of concept, the Coalition believes the FAA should revise the proposed performance requirement in section 89.320 (l) that a limited remote ID UAS must be *designed* to operate no more than 400 feet from a control station. The design limit in the proposal suggests that it would not allow a geo-fencing add-on after manufacture. The Coalition recommends that the FAA permit after-manufacture geo-fencing technology to achieve the 400 feet limit, consistent with the FAA's explanation in the preamble that this requirement may be met through a range of solutions, including geo-fencing.

The FAA seeks comment on whether there are ways to address the "extremely unlikely situation" in which all remote ID USS are unavailable at the same time, but the internet remains available.

In this situation, the proposed rule would prohibit a standard or limited remote ID UAS from taking off. The Coalition recommends the FAA develop reliability standards for Remote ID USS to minimize the risk of this situation occurring.

89.120 Unmanned aircraft systems without remote identification

(a) FAA-recognized identification area.

The Coalition recommends the FAA change the name to more accurately describe these areas. One alternative is to label them "FAA-recognized non-identification areas." Another alternative is to label them "FAA-recognized non-Remote ID areas." The current label suggest that drones operating in such areas are identified, when in fact they are not.

The Coalition supports mandating that any drone without remote ID may operate only within the visual line of sight of the remote pilot, and only within the confines of a designated non-remote ID zone, unless used for aeronautical research, as discussed below with reference to proposed subsection (b).

The Coalition also supports allowing UAS with both standard and limited remote ID to transit through and within a FAA-recognized non-remote ID area. The FAA seeks comment on its proposal to require a UAS without remote ID that receives a software update to make it a standard or limited remote ID UAS to thereafter comply with standard or limited remote ID requirements, even when operating in such FAA-recognized areas. The Coalition supports this proposal. It would add a logistical burden on UAS operators, as well as the USS, to require or allow operators to turn off remote ID in these FAA-recognized areas.

(b) Aeronautical research or to show compliance with regulations

The FAA proposes to exempt UAS operated for the purpose of aeronautical research from complying with, or showing compliance with, remote ID regulations. The Coalition supports allowing UAS operations for the purposes of research and development, such as operating prototypes, as well operations to demonstrate regulatory compliance, to operate without remote ID as long as the FAA imposes appropriate conditions and limitations to protect other airspace users and the public. The Coalition recommends that the exemption should be clarified to include both commercial and academic research and development activities. The Coalition believes the "authorized by the Administrator" proviso will ensure that such operations do not increase the risk to other operators or persons on the ground.

89.125 Automated Dependent Surveillance-Broadcast (ADS-B) Out prohibition

The Coalition supports the proposal to prohibit the use of ADS-B Out to comply with remote ID requirements. The Coalition notes its support for the statement in the preamble, 84 Fed. Reg. 72487, that ADS-B In technology will be permitted for standard and limited remote ID UAS.

89.130 Confirmation of Identification

The Coalition supports the proposed requirement that operators of foreign-registered civil UAS must submit a notice of identification and obtain a Confirmation of Identification before operating in the United States. The Coalition notes that such foreign-registered civil aircraft must comply with the applicable operational requirements in the proposed rule, whether for standard or limited remote ID aircraft or aircraft without remote ID. Thus, this would avoid any question of whether

remote ID technology installed on a foreign-registered drone might be incompatible with the remote ID data provided to a Remote ID USS.

89.135 Record retention

The Coalition believes that a Remote ID USS should retain all remote identification message elements for only 30 days after receipt of the data, consistent with the LAAANC program, and not the six months suggested in the NPRM. The FAA should impose the same time limit on its own retention of message element data. The Coalition is also concerned that Federal departments and agencies, as well as State and local governments, may establish databases to collect real time message element data. The Coalition believes that all government databases should be subject to the same time limit on retaining data.

Following the public's real time access to message element data via broadcast reception or access to a Remote ID USS, the Coalition recommends that this information be subject to sufficient privacy protections against dissemination to any third party, whether a government or private entity, as well as protections against public disclosure. Further, the final rule should require a Remote ID USS to promptly delete such data within a reasonable period after expiration of the 30 days, unless a duly authorized request has been made to preserve such data before that expiration.

In particular, the Coalition strongly recommends the proposed rule be revised to prohibit any Remote ID USS from sharing historical message element data with a Federal department or agency, State, or local government for any purpose other than law enforcement or national security, or upon consent of the UAS operator. The Coalition is concerned that there will otherwise be an

incentive for State and local governments to access remote ID messages to facilitate efforts to impose restrictions on otherwise lawful UAS operations. Such use would dissuade people from buying and operating UAS and would economically disadvantage businesses.

Within the 30 days a Remote ID USS may retain message element data, the rule should also include limitations on (1) the type of entities that can access historical message element data stored by a Remote ID USS (directly or indirectly), (2) the purposes for accessing this data, and (3) the correlation of public information (e.g., session ID) with non-public information (e.g., registration and contact details), as well as correlation of message element data with registration data. The rule should outline the requirements and processes for accessing historical data, and the limitations on access in respect to privacy interests of the UAS end-users, operators, and other persons.

In the preamble to the proposed rule, the FAA explains it may pair certain registration data with real-time access to the remote ID message elements, "when necessary," for "accredited and verified law enforcement and Federal security partners." 84 Fed. Reg. at 72470. Consistent with this "when necessary" limitation, the final rule should include a process to request access from a Remote ID USS or FAA to correlated message element and registration (including Session ID) data, and limit such access to law enforcement and national security purposes agencies, and only upon an adequate factual and legal predicate, such as probable cause.

Subpart C – FAA-Recognized Identification Areas

As stated above, the Coalition recommends the FAA change the name to more accurately describe these areas. One alternative is to label them "FAA-recognized non-identification areas." Another

alternative is to label them "FAA-recognized non-Remote ID areas." The current label suggest that drones operating in such areas are identified when in fact they are not.

89.205 Eligibility

The FAA proposes to allow only FAA-recognized community based organizations (CBOs) to apply to establish a FAA-recognized (non-)identification area. While CBO is defined in 49 U.S.C. 44809, the FAA explains in the preamble that a FAA-recognized (non-) identification area is "different" than the fixed site concept in that statutory provision. The Coalition believes that other fixed sites should be given due consideration to be recognized also as non-remote ID areas, but that in any event, the FAA must clearly establish the contours of each area it designates, with respect to longitude, latitude, altitude, and references to the corresponding surface locations.

89.210 Request for establishment of an FAA-recognized identification area

Proposed subsection (a) requires applications to be submitted within 12 months of effective date of final rule. The FAA seeks comment on whether the 12-month deadline should be extended. The Coalition does not support any deadline to establish an area in which remote ID technology is not required. While the Coalition supports widespread, if not universal, remote ID equipage, and supports incentives to increase remote ID equipage among operators using drones without remote ID, the 12-month deadline unduly and unnecessarily limits the availability of low-level airspace to recreational and model aircraft operators. Under proposed section 89.230, the FAA retains the authority to terminate an area's designation for safety or security reasons. This provides adequate protection for the airspace users that are remote ID-equipped.

Accordingly, the Coalition recommends deleting the text "within 12 calendar months from [EFFECTIVE DATE OF FINAL RULE]."

Proposed subsection (b) provides the required information. The Coalition recommends that maximum altitude be included in paragraph (5) of subsection (b), to read:

> (5) The latitude and longitude coordinates delineating the geographic boundaries and the maximum altitude above ground level of the proposed FAA-recognized identification area.

89.215 Approval of FAA-recognized identification areas

This proposed section contains factors the FAA considers in whether to approve or deny applications. The Coalition does not believe the FAA should be limited to a binary choice to approve or deny the application. The FAA should be allowed to approve the application in part, for instance by revising the proposed geographical boundaries of the area. In fact, proposed section 89.220 contemplates a CBO request to amend the FAA-recognized area by changing the geographic boundaries.

89.225 Duration of FAA-recognized identification area

The FAA proposes that recognition of a (non-)identification area will expire 48 months from the date the FAA approves the request for establishing an FAA-recognized (non-)identification area, subject to renewal, upon a request that must be submitted no later than 120 days before the expiration date. The Coalition does not object to an expiration period, provided there is an avenue

to renew the designation. The Coalition suggests an alternate approach in which an impending expiration date is extended pending the FAA's review of a renewal request, provided the request is submitted before the expiration date.

The Coalition does not support any artificial deadline by which the FAA might seek to limit the availability of these non-remote ID compliant areas.

Subpart D – Requirements for Unmanned Aircraft Systems with Remote Identification

As a general comment, the Coalition believes the requirements in Subpart D should align closely with the performance requirements and message elements in the published ASTM standard, as this standard reflects industry consensus.

89.305 Minimum message elements broadcast and transmitted by standard remote identification unmanned aircraft systems

The Coalition supports the proposal in subsection (a), paragraph (2), to allow a UAS operator to seek a Session ID from a Remote ID USS to protect the operator's privacy from the general public.

The Coalition does not support requiring barometric pressure altitude for either the control station (subsection (c)) or the unmanned aircraft (subsection (e)). This message element was not included as a compulsory part of the ASTM standard. Moreover, barometric pressure altitude of the control station may be difficult to ascertain and would be of limited utility since the control station will in the vast majority of cases be 0 feet Above Ground Level (AGL). The AGL altitude could be calculated from known map data, latitude/longitude of aircraft, and aircraft altitude. The Coalition

believes the small UAS industry is using GPS (WGS84) almost exclusively, requiring barometric pressure altitude for either the control station or the unmanned aircraft is unnecessary.

With respect to safety, remote ID is not being used to ensure aircraft separation; rather it is intended to allow the public, FAA, and law enforcement to authenticate a UAS operation, locate the ground control station if needed, and provide basic situational awareness to other aircraft operators. 84 Fed. Reg. 72,473-74. The accuracy of geometric altitude derived from GPS (or a combination of other Global Navigation Satellite Systems) is sufficient for those purposes, and FAA in a number of exemptions has consistently allowed UAS operators to use geometric altitude as a substitute for, or supplement to, barometric pressure to determine an unmanned aircraft's altitude.[2]

With respect to the Universal Time (UTC) mark of a position source output, subsection (f), the Coalition agrees with the assumption that a means of compliance that specifies a GPS position source would also specify a GPS time mark.

The Coalition does not support the proposed requirement for emergency status indication, subsection (g), which is not part of the ASTM standard. The FAA contemplates that this message

[2] *See, e.g.*, Exemption No. 11138, Docket FAA-2014-0481 (Jan. 5, 2017) at 19 ("the petitioner has a barometric altimeter and GPS derived altitude capabilities . . . . The petitioner may choose to set the altimeter to zero feet AGL rather than local barometric pressure of field altitude before flight."); Exemption No. 12783, Docket FAA-2015-1586 (Sept. 8, 2015) at 13 (noting that because "the UAS may not have a barometric altimeter, but instead a GPS altitude read out," an exemption from 14 CFR 91.121 may be needed); Exemption No. 12199, Docket FAA-2015-1752 (July 28, 2015) (approving an exemption from 14 CFR 91.121 for unmanned aircraft that would set the altimeter to zero feet AGL in lieu of using local barometric pressure or field altitude); Exemption No. 18163, Docket FAA-2018-0835 (Apr. 2, 2019) at 22 ("The Hummingbird v2 7000 series small UA uses GPS and pressure sensors to select and maintain its height above the ground."); Exemption No. 18339, Docket FAA-2019-0628 (Sept. 23, 2019) at 13 ("The Matternet M2 sUA altimetry augmenting instrumentation and software includes GPS sensors and a barometric pressure altimeter.").

element would specify emergency status code, which could involve "lost-link, downed aircraft, or other abnormal status of the aircraft." 84 Fed. Reg. at 72474. The Coalition requests further clarification of the types of emergencies the FAA hopes to capture with the emergency status message element. For example, not all UAS will respond to a lost link in the same way. Some will hover and land if the link is not reestablished, while others may continue to a set waypoint or fly home, all while attempting to regain link. It is not clear how the FAA envisions making this information useful beyond simply identifying remote ID-compliant UAS that are inadvertently flying in controlled or restricted airspace due to an emergency. The Coalition also requests clarity on how the FAA plans to ensure uniformity in the characterization of emergency status given the availability of several remote ID technologies.

In the preamble, the FAA seeks comments on other message elements it considered, but rejected (additional contact information for UAS operator or control station; velocity; direction; route; and altitude above ground level). The Coalition supports adding velocity, direction, and route to the required set of message elements. This would be consistent with the European Union Aviation Safety Agency (EASA) remote identification framework and would support international harmonization and further the groundwork required for complex operations.

89.310 Minimum performance requirements for standard remote identification unmanned aircraft systems

Proposed subsection (b) requires the UAS to maintain connection to the internet and transmit message elements to remote ID USS when internet is available, from takeoff to landing. The FAA

seeks comment on whether the connection should instead be required from start up to shut down. The Coalition believes that remote identification should be required only from takeoff to landing.

Proposed subsection (d) pertains to self-testing and monitoring. When powered on, a UAS must automatically test functionality of remote identification and notify the remote pilot of the test result. The drone must not be able to takeoff if remote ID equipment is not functional. The Coalition seeks clarification on how this requirement may be structured in a way that does not add another potential failure condition that could lead to loss of control during flight.

The Coalition also is concerned with the proposal to prohibit standard remote ID aircraft from operating in FAA-recognized (non-)identification areas if equipped with inoperable remote ID equipment. The proposed rule requires remote ID equipment to be functional for any operation, even if that operation would occur within a non-remote ID area.

Proposed subsection (e) requires tamper resistance of the UAS, restated as reducing or hindering the ability of a person to tamper with remote ID's functionality. The Coalition requests clarification as to what "tamper resistant" means for the UAS. Conflating the UAS with remote ID functionality means that any design of remote ID architecture can be determined to not be "tamper resistant" without any real consideration of how the tamper resistance requirement could reasonably be met. The Coalition requests the FAA provide a list of approved maintenance procedures and methods of interaction with the remote ID that would not be considered tampering, but would allow for maintenance and repair by the operator.

With regard to connectivity, proposed subsection (f) provides that if the internet is available at takeoff, the UAS must not be able to takeoff unless it is connected to internet and transmitting the message elements through that connection to a Remote ID USS. If the connection is later lost, or if the UAS is no longer transmitting the message elements to a Remote ID USS, the UAS must notify the remote pilot. In the event of an abnormal condition, such as loss of internet connectivity, there may be an extra safety risk introduced by the multi-layer approach to prevent flights from launching. The proposal does not clarify how these systems will be implemented. Direct auto pilot integration or software code, a mechanical lockout, or other features all have their own safety concerns and potential malfunctions in the event of an abnormal or emergency condition. The Coalition requests clarification in the rule text or in the preamble to the final rule.

Proposed subsection (g), error correction, states that the UAS must incorporate error corrections in transmission *or* broadcast. The preamble, at 84 Fed. Reg. 72475, refers to this requirement as transmission *and* broadcast, "as appropriate." The Coalition seeks clarification that the error correction will be incorporated in any technology that is required to be used to comply with applicable remote ID requirements.

Proposed subsection (i) requires, for broadcast message transmission, that the UAS must be capable of broadcasting message elements using non-proprietary broadcast specification and radio frequency spectrum in accordance with 47 CFR Part 15 where operations may occur without FAA license that is compatible wireless devices. Any broadcasting device must be integrated into a UAS without modification to its authorized radio frequency parameters and designed to maximize the

range at which the broadcast can be received, while complying with Part 15 and any other laws in effect on the date the declaration of compliance is submitted.

As an initial matter, we suggest the FAA makes clear that message encryption is permitted. The Coalition also recommends removing the requirement that the "broadcasting device be designed to maximize the range at which the broadcast can be received." The inclusion of the word "maximize" could be understood as a requirement that is in excess of what is needed to ensure the broadcast transmission is received. For example, Federal Communications Commission (FCC) rules uniquely allow power levels up to four Watts (cf. Europe's 100mW) on ISM bands. Such power levels are well beyond what is necessary for UAS remote ID and may result in the inclusion of components such as oversized amplifiers and heat sinks that are designed to meet this regulatory obligation, but are excessive for the operation of the UAS. The Coalition recommends this requirement be removed, or alternatively that it be replaced with a performance-based requirement for minimum range for the intended operation (e.g., reception available in the line of sight areas for visual line of sight operations).

The FAA seeks comments on how connecting to the internet directly from a UAS (as opposed to from a ground station) might impact networks using radio frequency spectrum and users or license holders of either licensed or unlicensed spectrum. The FAA also seeks comments on whether any existing UAS is capable of connecting to the internet from the aircraft, and if so, what methods are used for those connections.

The Coalition notes that remote ID over cellular networks would not overwhelm those networks. The amount of data that a remote ID transmission will require is extremely small (comparable to SMS messaging) and therefore, cellular networks can easily support even a very large number of remote ID messages. Moreover, cellular networks, which are continually evolving to increase reliability and efficiency, can use techniques, such as densification (adding additional cell sites to increase capacity) to alleviate congestion on their networks. Additionally, as more spectrum becomes available for licensed and unlicensed use, the opportunities to meet the needs for UAS can be addressed. As noted in the Coalition's comments to the FCC's Public Notice on spectrum use for UAS, wireless carriers are well incentivized to ensure not only compliance with FCC rules, but also to ensure that network connectivity is not degraded for any customer on their respective networks.

UAS operating on spectrum bands designated for unlicensed use are not protected from interference from other users and must, in fact, accept such interference. While these bands present a viable opportunity, the FAA should consider this limitation as it establishes operational rules, including the viability of the broadcast system overall.

With respect to message elements performance requirements, proposed subsection (j), the Coalition as a threshold matter urges the FAA to remove barometric pressure altitude as a required message element and replace it with a performance-based standard of maximum allowed deviation. The Coalition has several concerns about the performance requirement that the reported barometric pressure altitude of the control station and unmanned aircraft must be "accurate to within 20 feet for pressure altitudes ranging from 0 to 10,000 feet."

The proposed barometer measurements lack the precision necessary to be applied to drones given existing technological capabilities. The Coalition recommends, in the event the barometric altimeter reporting requirement is retained, that pressure altitude of the control station and the UAS should not be held to a more stringent altitude reporting standard than the requirement for manned aviation (see 14 CFR 91.215(b)). 14 CFR Part 43 App. E, Table 1 defines the tolerances required of manned systems to accurately report altitude. The proposed accuracy of +-20 feet proposed for all small UAS operations, regardless of altitude, is the same as required for manned operations below 1,000 feet Mean Sea Level (MSL). For operations in an area with a surface elevation of 4,800 feet MSL, the required +-20 feet of accuracy for small UAS is more stringent than the manned requirement of +-35 feet. To match the requirements for barometric altimeter accuracy of aircraft that range from 0.55 lbs. to 55 lbs. to those that weigh in excess of 1,000 lbs. ignores the size, weight, and power (SWaP) limitations that are an inherent component of small UAS design and operation.

For comparison, the 5506 Series Servoed Encoding Altimeter by United Instruments Inc. has a declared accuracy of +-35 feet throughout the calibrated range and weighs approximately 3.5 lbs. This would not meet the requirements in the proposed rule, and would consist of anywhere from 1/8 to ¼ of the total weight of the typical UAS in use today. Thus, this proposed requirement is unreasonable, nearly impossible to demonstrate compliance with, and adds no safety gain that justifies its inclusion in the proposed rule.

The Coalition notes that geometric (GPS-based) altitude is more than sufficient for reporting altitude. Geometric altitudes are typically +- 30 feet from true altitude. There is no justifiable safety gain from the proposed +-20 feet requirement over the currently attainable +- 30 feet accuracy.

With respect to the proposed latency requirement, the FAA proposes to require the transmission and broadcast rate of at least one message per second on the grounds that this requirement is achievable by currently available equipment. The Coalition seeks confirmation that the operator must report the drone and operator location data via transmit or broadcast at least once per second.

The Coalition is concerned about the proposed cybersecurity performance requirements, subsection (k), because a simple requirement to "incorporate cybersecurity protections" for transmission and broadcast is inadequate. The Coalition appreciates that the FAA is not proposing any specific protection methods, but requests clarification as to what protections will be deemed sufficient. The Coalition supports strong end-to-end cybersecurity protections and encryption, but believes the FAA should identify standards (e.g., the cybersecurity standards of the National Institute of Standards and Technology (NIST)) it believes are acceptable or processes by which standards will be identified. It may be best to determine this requirement during the means of compliance process. The Coalition also seeks clarification as to whether anti-spoofing technology will be required. The network should be encrypted so anti-spoofing cybersecurity would not be necessary. As for broadcast, it is not intended to be private, but it also less susceptible to hacking as it is a one-way ad hoc transmission. Something must be in place to minimize the risk of hacking or nefarious manipulation of the signal. Encryption technology could provide protection for broadcast messages.

89.315 Minimum message elements transmitted by limited remote identification unmanned aircraft systems

For the Coalition's comments on the proposed requirements, please refer to the comments on these same message elements in proposed section 89.305.

89.320 Minimum performance requirements for limited remote identification unmanned aircraft systems

For the proposed performance requirements in this section that are the same as the proposed requirements in proposed section 89.310, please refer to the comments in that section.

Proposed subsection (l) requires the UAS to be *designed* to operate no more than 400 feet from a control station. The Coalition understands 400 feet was determined by the FAA UAS Identification and Tracking Aviation Rulemaking Committee (the ARC) as the maximum distance for law enforcement to locate and identify an unmanned aircraft. The FAA explains in the preamble that this requirement may be met through a range of solutions, including geo-fencing. As explained above, the Coalition recommends the FAA revise its proposal to clarify that the design requirement can be met by geo-fencing installed after design and production of the UAS.

With respect to proposed subsection (m), broadcast limitation, the Coalition refers to its comments on the proposed requirements for limited remote ID. Assuming the FAA retains the proposed requirement for network transmission only, the Coalition asks whether the requirement that the

UAS "cannot" broadcast remote message elements can be achieved after design and production, through a disabling of any broadcast technology.

Subpart E—Means of Compliance

As a general matter, it appears this subpart does not cover an add-on device (or puck), like a supplemental type certificate capability. The Coalition believes the FAA should consider an add-on device as a means of compliance if it goes through the same inspection process for transmission by network or broadcast (depending on capability).

Subpart F—Design and Production of Unmanned Aircraft Systems with Remote Identification

89.501 Applicability

The Coalition asks the FAA to clarify that UAS intended to be operated exclusively indoors are not subject to the design and production requirement in this subpart. The FAA does not have authority over aircraft operated inside a closed building as that space is not airspace. The Coalition requests that subsections (a) and (b), which cover design and production of UAS "operated in the United States" be revised to be limited to the "airspace of the United States." At a minimum, the FAA should clarify the inapplicability of the remote ID to UAS intended to be operated exclusively indoors.

The FAA proposes in subsection (c) that this subpart does not apply to UAS designed or produced exclusively for aeronautical research or to show compliance with regulations, or to UAS weighing less than 0.55 pounds, unless the UAS is designed to be a UAS with standard or limited remote

ID. By way of clarification, the Coalition recommends that UAS intended to be operated BVLOS, regardless of weight, or operated outside of the FAA-recognized (non-)identification areas, must have either standard or limited remote ID.

The FAA seeks comments on whether a person should be allowed to produce kits for sale that contain 100% of the parts and instructions for assembly necessary to build a fully functioning UAS without remote ID. Once built, the UAS must weigh under 0.55 lbs. or operate only within FAA-recognized (non-)identification areas. The Coalition believes the model aircraft community should be allowed to build remote controlled UAS, but if a kit-built UAS is to be operated in areas other than the FAA-recognized (non-)identification area, it should be permitted to declare flight intent via the USS network – like LAANC – as a limited remote ID UAS.

The Coalition also believes that manufacturer performance requirements should apply only to "highly automated" aircraft that are intended either for commercial use or sale to third parties, which must operate as a "standard" UAS with integrated broadcast remote ID or real-time network remote ID. "Highly automated" may refer to a combination of geo-awareness, self-flying, and self-navigation capabilities. Manufacturer performance requirements should not apply to recreational aircraft built for personal use. UAS kits, amateur-built UAS, and UAS assembled completely from pre-fabricated parts should not be defined based on arbitrary percentage thresholds or ambiguous "fabrication" assessments.

This proposed section exempts amateur-built aircraft. Many self-built aircraft are professionally built and operated, especially advanced aircraft for use cases such as cinematography, industrial

inspections, and other commercial use cases. Such pro-built systems are often acquired as partial systems that are completed by the operator/builder. This proposed rule would upset this market that supplies such integrators.

The Coalition also notes that by focusing on remote ID design and production by the UAS manufacturer, this subpart does not address add-ons. Existing UAS manufactured prior to this rule will require a compliant plug-and-play solution to continue flying in the same manner as they have been operated to date. Excluding this method of remote ID integration effectively bans the use of all small UAS in the NAS manufactured before the effective date of the final rule. Such a ban would have a significantly larger financial and operational impact than is estimated in the NRPM.

89.505 Serial numbers

The FAA proposes to incorporate by reference ANSI/CTA-2063-A, *Small Unmanned Aerial Systems Serial Numbers* (September 2019) into this regulation and require UAS with standard or limited remote ID to have a serial number in compliance with that standard. The FAA explains that there is consideration to update this standard from 15 to 18 characters, so the Coalition recommends that this section be revised to require compliance with the ANSI serial number standard in effect at the time of manufacture.

89.510 Production requirements

Under proposed subsection (a), no person may produce a UAS unless it is designed and produced to meet minimum performance requirements for standard or limited remote ID in accordance with

FAA-accepted means of compliance, the UAS meets the design and production requirements in this subpart F, and the FAA has accepted the declaration of compliance for the UAS.

The Coalition recommends this subsection be limited to standard and limited remote ID UAS. The preceding section, proposed section 89.505, starts with more appropriate text: "No person may produce a standard remote identification unmanned aircraft system or a limited remote identification unmanned aircraft system . . . ." That subsection implies that one is producing a "remote identification" aircraft and therefore claiming compliance. That qualifier is more fitting.

The Coalition does not support moving airspace requirements from the remote pilot to the manufacturer. In general, a FAA regulatory event occurs when an operation begins, rather than when something is created. One can build an aircraft in one's garage without a regulatory event taking place. Once a person commences to operate the aircraft, the Federal Aviation Regulations apply and no person may operate a civil aircraft unless it is in airworthy condition (14 CFR 91.7).

The proposed subsection, by stating that "no person may produce an unmanned aircraft system", creates a regulatory event at time of production. The Coalition recognizes that the FAA regulates aircraft type and production certification. However, the chain of responsibility starts with the pilot in command to confirm the aircraft is airworthy; it is not up to the manufacturing ecosystem to ensure pilots are flying a certified aircraft.

The Coalition believes the FAA intends to ensure remote ID compliance through acceptance of a means of compliance and a declaration of compliance. This rule should reflect that intention and

properly enforce “truth in labeling” for declarations of compliance. The ARC, which represented many diverse stakeholders including police and national security personnel, ultimately found that it should be up to the pilot in command to ensure the aircraft has a valid compliance label.

With respect to proposed subsection (b), inspection, audit, and notification, the Coalition recommends the FAA consider the model the FAA has proposed for the LAANC program.

89.520 Submission of a declaration of compliance for FAA acceptance

The Coalition is concerned that, as drafted, this section would be almost entirely unmanageable for the incorporation of a plug-and-play remote ID solution which will be necessary for retrofitting UAS already in service. The Coalition proposes a revision to make allowances for compliant use of retrofitting remote ID onto UAS manufactured prior to the effective date of the final rule.

89.535 Record retention

The FAA proposes to require supporting information to be retained for as long as the UAS listed on a declaration of compliance are produced, plus 24 calendar months. The Coalition is concerned that the proposed requirement to retain “all test results” is vague and potentially overbroad. The Coalition requests clarification of what tests are included.

Part 107 – Small Unmanned Aircraft Systems

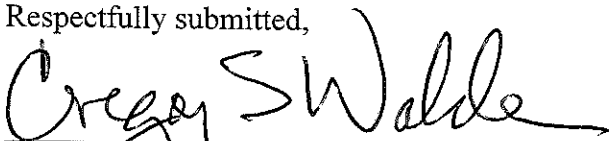
107.52 ATC transponder equipment prohibition

The Coalition supports the prohibition on operating a small UAS with a transponder on, unless authorized by the Administrator.

107.53 ADS-B Out Prohibition

The Coalition supports the prohibition on operating a small UAS with ADS-B Out equipment in transmit mode under Part 107 unless authorized by Administrator.

Respectfully submitted,



Gregory S. Walden
McGuireWoods Consulting, LLC
2001 K Street NW, 4th floor
Washington, DC 20006
202-857-2928
gwalden@mwcllc.com
Counsel to the Small UAV Coalition

March 2, 2020