March 2, 2020

Submitted Electronically via regulations.gov

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

The Honorable Steve Dickson
Administrator, Federal Aviation

800 Independence Avenue, SW
Washington, D.C. 20591

Re: Comments of the Commercial Drone Alliance on the Notice of Proposed Rulemaking regarding Remote Identification of Unmanned Aircraft Systems (**Docket No. FAA-2019-1100**)

Dear Secretary Chao and Administrator Dickson:

The Commercial Drone Alliance ("CDA") appreciates the opportunity to provide comments on the Federal Aviation Administration's ("FAA") Notice of Proposed Rulemaking ("NPRM") regarding Remote Identification of Unmanned Aircraft Systems ("UAS").[1]

The CDA is an independent non-profit organization led by key members of the commercial drone industry.[2] The CDA works with policymakers at all levels of government to promote policies for industry growth and seeks to educate the public on the safe and responsible use of commercial drones to achieve economic benefits and humanitarian gains.

[1] 84 Fed. Reg. 72438 (December 31, 2019).

[2] The CDA brings together commercial drone end-users, manufacturers, service providers, and vertical markets including oil and gas, precision agriculture, construction, security, communications technology, infrastructure, newsgathering, filmmaking and more. For more information on the Commercial Drone Alliance, please see www.commercialdronealliance.org.

Commercial UAS can provide extensive benefits to American citizens, consumers, and businesses:

- delivering supplies, products, life-saving medical equipment, and medicines;
- assisting with law enforcement, fire, accident, and natural disaster responses, crop assessments, search and rescue missions, and newsgathering;
- inspecting and monitoring industrial equipment, wind turbines, communications towers, parked aircraft, energy facilities, railroad tracks, bridges, power lines, pipelines, and other critical infrastructure; and
- countless other beneficial use cases.

However, the federal government has made clear that remote identification ("remote ID" or "RID") must be implemented if broad expanded UAS operations, such as operations over people or beyond visual line of sight, are to become a reality and these substantial benefits are to be realized.[3] Moreover, remote ID will play a key role in ongoing and future UAS Traffic Management ("UTM") efforts.

This rulemaking is therefore vitally important to our members as expanded and scalable UAS operations are key to unlocking the enormous potential of commercial UAS operations here in the United States. For its part, the CDA has long been committed to working with the federal government to integrate drones safely and securely into our National Airspace System ("NAS") and has supported the federal government's desire to establish a remote ID framework as part of that effort.

The NPRM necessarily has implications for a wide variety of stakeholders with firmly held, and sometimes conflicting, views – from national security agencies, to law enforcement, to commercial UAS operators, to UAS manufacturers, to UTM providers, to recreational operators, and others. The CDA nonetheless strongly supports the spirit of the FAA's Remote Identification

[3] 84 Fed. Reg. 3856, 3865 (February 13, 2019) ("As a result, the FAA plans to finalize its policy concerning remote identification of small UAS—by way of rulemaking, standards development, or other activities that other Federal agencies may propose—prior to finalizing the proposed changes in this rule that would permit operations of small UAS over people and operations at night.")

proposal as a crucial step towards expanded drone operations. The CDA believes that the FAA's proposed remote ID rule is a good start for addressing the applicability, safety, security, and technological requirements for remote ID to support the future development, expanded operations, and commercialization of UAS operations in the United States.

The CDA does have concerns about various details of the proposal, but remains optimistic that the major issues can be easily remedied. As explained below, the CDA believes that (i) certain parts of the proposed rule need modification, supplementation, and/or clarification, and (ii) other aspects of the proposed rule are unnecessarily complicated and overly restrictive for some operations including certain recreational or hobbyist operations.

I. THRESHOLD APPLICABILITY AND CARVE-OUTS FOR REMOTE ID

RID Threshold Applicability. The CDA actively participated in the 2017 RID Aviation Rulemaking Committee ("ARC") and led a dissent from the ARC Report with respect to the applicability of remote ID requirements. Essentially, the CDA's dissent advocated for a simple, adaptable, enforceable, comprehensive, and future-proofed general rule that any UAS or model aircraft weighing 250 grams or more must comply with the RID regulations.[4] The CDA recognized that any such regulations must encompass all but the smallest and most unsophisticated UAS in order to be effective, with the possibility for certain limited geographic carve-outs, such as UAS operating at registered AMA fields.

The proposed rule even goes farther than the CDA (joined by many other stakeholders) had advocated. Under the operating requirements of the proposed rule, remote ID would apply to (i) persons operating unmanned aircraft ("UA") registered or required to be registered under 14 C.F.R. Parts 47 or 48 and (ii) persons operating foreign civil UA in the United States.[5] The Preamble explains that this broader applicability is necessary because a UAS "may be used in a wide variety of types of operations that may present a range of safety and security risks" and that tying the remote ID requirement to registration is warranted because "the FAA, national security

[4] 84 Fed. Reg. at 72458.

[5] Proposed § 89.101.

agencies, and law enforcement agencies have a need to correlate [RID] and registration data."[6] The CDA concurs with the applicability threshold for remote ID set forth in Proposed Part 89.

RID Carve-Outs. The CDA has long endorsed the general idea of a geographic carve-out from remote ID. Under Proposed § 89.120, a UAS that does not meet the remote ID standards may still be operated if (i) it is flown within visual line of sight ("VLOS") and within an FAA-recognized identification area ("FRIA"), or (ii) the operator is authorized by the FAA to operate without RID for "the purpose of aeronautical research or to show compliance with regulations." The CDA in principle supports these limited carve-outs from the remote ID requirements, but urges the FAA to modify and/or clarify this Section as follows.

First, the proposed requirement that applications for designation as a FRIA be submitted within one year of the Final Rule's effective date is overly restrictive.[7] It would compel a race to the FAA to seek such a designation and would preclude applications from those who may not want or need a FRIA designation until well after the first year. Land use changes over time, as does the need for different types of operations, and the need or desire for a FRIA designation may therefore evolve over time. The Final Rule should take a longer-term approach and recognize that the need for FRIAs may change over the years. The purported justification for this limited application window (i.e., that "most UAS without [remote ID] will reach the end of their useful lives or be phased out"[8] over time) is not supported by the record of the NPRM. To be locked into those limited FRIAs for which applications were filed within the first 12 months and approved is not in the public interest. The Final Rule should not put any time limit on when FRIA-designation applications may be filed with the FAA.

Second, the proposed restriction that only FAA-recognized community-based organizations ("CBO") are eligible to apply for a FRIA designation is overly restrictive.[9] The CDA agrees that FAA-recognized CBOs should be eligible to apply for such designations, but so

6 84 Fed. Reg. at 72459-460.
7 Proposed § 89.210.
8 84 Fed. Reg. at 72486.
9 Proposed §§ 89.205, 89.210(a).

too should other entities. For example, companies or educational institutions that manufacture, operate, test or otherwise use UAS should be able to apply for designation of a FRIA where they can use UAS without remote ID but within VLOS. There is simply no reasonable justification for limiting the pool of FRIA-designation applicants to just CBOs. Accordingly, Proposed § 89.205 should not be part of the Final Rule (or should be revised to include a broader group of eligible FRIA-designation applicants), and corresponding changes should be made through the remainder of Proposed Subpart C to make clear that other entities are eligible to apply for FRIA designations.

Third, the CDA supports the spirit of the language in Proposed § 89.215 which asks the FAA to consider factors like critical infrastructure and use of airspace when reviewing a request for establishment of a FRIA. But, we believe that this Section should be strengthened from "may" to "must." Given existing TFRs and other limitations, the FAA should be required to consider factors like location and proximity of critical infrastructure, major sports stadiums, and airports in its designation of FRIAs.

Fourth, in the Preamble to the Final Rule or the Final Rule itself, the FAA should clarify that the term "aeronautical research" encompasses commercial research. The NPRM's Preamble currently provides: "In this context, 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. Under this provision, producers and other persons authorized by the Administrator would have the ability to operate UAS prototypes without remote identification exclusively for researching and testing the UAS design, equipment, or capabilities. This provision does not extend to any other type of research using a UAS."[10] Commercial research should be expressly listed as part of what the FAA considers to be "aeronautical research" for purposes of the remote ID rule, including Proposed § 89.120(b) and Proposed § 89.501(c)(4). For maximum clarity, the Final Rule should also state that aeronautical research may be conducted in FRIAs without the burden of requesting a waiver from the FAA.

[10] 84 Fed. Reg. at 72467.

II. STANDARD REMOTE ID

The CDA does not take a position on whether remote ID information can be both broadcast and, if the internet is available, transmitted over a network for Standard Remote ID.[11] However, the CDA strongly believes that operators should be permitted to use network only when internet is available, subject to meeting the performance requirements of Proposed Subpart D in their specific operating environment. The CDA also urges the FAA to clarify certain aspects of the proposed Standard Remote ID regulation, as explained below.

"As Soon As Practicable". As proposed, if a Standard Remote ID UAS can no longer broadcast or transmit the requisite message elements, the operator/pilot must land the UA "as soon as practicable" unless otherwise authorized by the FAA.[12] Although this does not constitute an "immediate landing" requirement, absent modification, the "as soon as practicable" standard would not be in the public interest. The Preamble explains:

> "The FAA does not define the phrase ''land as soon as practicable'' and expects that the person manipulating the flight controls of the UAS will take steps to land in a safe manner. For instance, if the aircraft is still within visual line of sight, the safest option may be to keep the aircraft within sight to avoid other aircraft and return to the departure point. For a standard remote identification UAS operating BVLOS, the safest way to land may be to continue to the intended destination."[13]

That explanatory language, however, does not adequately address the issue.

For situations where such a landing requirement would be implicated, the CDA urges the FAA to clarify the standard to expressly incorporate the concepts of "reasonableness" and "safety" (e.g., as soon as reasonably practicable and can be done safely). In addition, compelling an operator to land as soon as practicable when there is a transient loss of network connectivity is simply unnecessary. Accordingly, the CDA recommends that this provision be revised to make

---

11 Proposed § 89.110(a).
12 Proposed § 89.110(b).
13 84 Fed. Reg. at 72468.

clear that operators who experience a transient loss of network connectivity can continue to fly (and thus need not land as soon as practicable).

Finally, the FAA should also consider an exception for critically important, time-sensitive, public safety missions performed by public safety officials or commercial personnel in emergency or similar situations (e.g., inspecting a nuclear reactor following an incident, a bridge after an earthquake, an ongoing wildfire or an ongoing crime scene). In this regard, the Final Rule could specify that, in the event that the UA loses its ability to provide the required remote ID message elements during a critically important, time-sensitive, public safety mission, the remote pilot in command could continue to conduct operations within VLOS upon: (1) determining that continued operation does not present undue risk to persons or property on the ground, notwithstanding the loss of remote ID services; (2) determining that other UAS or manned aircraft in the area could be safely detected and avoided; and (3) notifying local law enforcement.

Internet Availability. The proposed requirements for Standard Remote ID depend on whether the internet is "available" or "unavailable".[14] The FAA should provide additional clarity on what is meant by these terms in this context.

"Takeoff to Landing". The CDA supports the requirement that a person may operate a Standard Remote ID UAS if it sends the required message elements "from takeoff to landing."[15] There will be occasions when a UAS may have power for purposes of maintenance or other non-flying activities, and it would be of little, if any, benefit for the UAS to send the message elements in those cases when there will be no flying. Accordingly, the "from takeoff to landing" requirement is more appropriate than, for example, from power-on to power-off.

"*Unless Otherwise Authorized By The Administrator*". The proposed standard remote ID regulation involves certain requirements "unless otherwise authorized by the

[14] Proposed §§ 89.110(a)(1),(2) and 89.310(b),(f).
[15] Proposed § 89.110(a).

Administrator."[16] The same or similar language is also used elsewhere in the proposed rule.[17] The Final Rule or its Preamble should provide detailed guidance about the process or processes by which one could seek the requisite authorization from the Administrator in each particular case.

III. LIMITED REMOTE ID

The CDA does not take a position on the category of Limited Remote ID UAS, though some of our members expressed skepticism about the category's utility. One area of agreement is that, to the extent that this category remains in the Final Rule, it should be a performance-based standard. The proposed rule requires Limited Remote ID UAS to be designed and produced such that they are not capable of operating more than 400 feet from the control station.[18] This proposal is arbitrary in that it fails to acknowledge that VLOS may exceed beyond 400 feet, and it does not contemplate that certain operations will involve vertical flight above infrastructure. Rather than imposing such a design restriction, assuming the category remains in the Final Rule, it should just require operators to fly within VLOS instead of within 400 feet of the control station. Such an approach would still ensure safe operations, without unduly burdening the marketplace. If VLOS becomes the standard, then the Final Rule should also require that the geographic area of the flight (or the UA's location) is also part of the message elements (and not just the location of the control station as the current draft rule proposes[19]).

IV. PRIVACY

In the CDA's view, the proposed rule raises substantial privacy issues that should be addressed in the Final Rule.

---

[16] Proposed § 89.110(a),(b),(c).

[17] See, e.g., Proposed §§ 89.115(a),(b),(c) (limited remote ID), 89.120(a),(b) (no remote ID), 89.105 (remote ID requirements), 107.53 (ADS-B Out prohibition).

[18] Proposed § 89.320(l).

[19] Proposed § 89.315(a).

As an initial matter, the FAA should clarify what message elements would be publicly available in the network context and what privacy protections would apply to restrict the use of such information. The Preamble indicates that the remote ID message elements transmitted to a Remote ID USS "would be considered publicly accessible information", that they "may be available to the general public," and that Remote ID USS would be "required to provide to the public, for no cost, the UAS Identification message element, either the UAS serial number or session ID."[20] The proposed rule should provide clear, appropriate restrictions on the use of these message elements.

UAS position data can reveal sensitive information about UAS operators and third parties. Uncontrolled access to this information can compromise privacy and commercial sensitivity. The Final Rule should therefore codify specific restrictions on the use of message elements, and although network remote ID will inherently provide greater privacy protection, the Final Rule should require certain technical mitigations for networks, such as the corresponding ASTM Standard F3411, to provide appropriate protections for the transmitted message elements and data. Additionally, the Final Rule should outline performance-based restrictions on data sharing and data disposal between Remote ID USS to prevent illegitimate use of network data.

To that point, the CDA strongly believes that, consistent with the underlying purposes of the proposed rule, the message elements should be available only for legitimate safety, security, compliance, and accident/incident investigation purposes. The Final Rule should outline a legal process restricting government access to retained data for such limited purposes. In addition, there should be a public-facing application for network so that law enforcement and members of the public can identify a particular UA at the time of flight, but the public should not have access to historical information because, *as to the public*, that information does not fulfill the remote ID rule's objectives. Indeed, if the general public had full visibility and access to the historical data, it could be used for purposes other than those addressed by the rule, including, for example, to track for commercial purposes where drone delivery flights begin and end over a period of time. Anonymizing the data, through the use of a session ID or otherwise, does not resolve the issue

[20] 84 Fed. Reg. at 72485.

because the historical data would still reveal information from which identities could be recognized (e.g., the control station's fixed address, repeated flights from a particular warehouse or to a particular destination). In addition, the Final Rule should limit the aggregation of historical remote ID data, other than by FAA-approved, independent third-party entities, such as academic institutions or FFRDCs, solely for the purpose of supporting safety risk assessments.

Proposed § 89.135 requiring Remote ID USS to retain any remote ID message elements for six months should similarly be revised to limit the use of any such data. The Preamble indicates that six months was appropriate for FAA enforcement purposes and to balance the interests of security and law enforcement, on the one hand, and privacy interests, on the other hand.[21] The final version of this Section should be revised to expressly limit who may use the data held for six months by the Remote ID USS and for what purposes. Access to that data should be limited to (i) the FAA, NTSB, law enforcement, or other security agencies solely for legitimate safety, security, compliance, and accident/incident investigation purposes; and (ii) FAA-approved, independent third-party entities, such as academic institutions or FFRDCs, solely for the purpose of supporting safety risk assessments on an aggregated, de-identified basis.

In sum, the Final Rule should codify (i) specific restrictions on the availability and use of the message elements and historical data and (ii) technical mitigations for networks, as described above.

V. KNOWN OPERATOR SYSTEM

The CDA urges the FAA to include a Known Operator System ("KOS") category in the Final Rule for remote ID. This category would enhance the effectiveness of any comprehensive remote ID rule beyond a minimum threshold for compliance and would incentivize authorized commercial operators (or public safety operators) to proactively gain the trust of public officials and the general public. Ultimately, such a tier would allow the commercial UAS market to realize its enormous potential, to the benefit of the American public and economy.

[21] 84 Fed. Reg. at 72484.

The KOS envisioned by the CDA would be similar in concept to the TSA Pre✓ system and the TSA Known Shipper Program. Under the KOS, safe and responsible operators would pay a reasonable fee to voluntarily provide additional details about their organization and UAS operations to TSA, FAA or other appropriate federal agency for vetting and evaluation. Upon successful completion of the vetting and evaluation process, the operator-applicant would be granted "Known Operator" status.

Under the KOS, Known Operators would have the option of voluntarily making additional information available to both public safety officials and members of the public. Information made available to public safety officials could include company information, FAA authorizations and approvals held, mission type, pre-planned navigation data, operating status of the UAS (including the mode in which the UA is currently operating), and track record of the company's UAS operational history. Members of the public would then receive a signal that the company is a "Known Operator". As incentive to undergo the extra vetting and evaluation process, those who achieve "Known Operator" status could be permitted to operate closer to critical infrastructure or in geographic areas where other UAS operators would not be able to operate, or could be relieved of providing certain message element information.

Establishment of this KOS would benefit public safety agencies, law enforcement, the public, and the commercial UAS industry, effectively making it a win-win for each of these stakeholder groups.

Benefits to Public Safety Agencies and Law Enforcement: With remote ID for UAS, public safety agencies will be able to enhance their incident investigation and active monitoring of heightened awareness areas. The KOS will help on both counts. First, with regard to incident investigation, when an individual inquires about the identity and purpose of a sighted UA, additional information provided by the Known Operator may reduce confusion for public safety agencies and law enforcement, and enhance the safety and security of the National Airspace System. "Known Operator" status will allow these agencies and law enforcement to save

precious time and resources when investigating potential UAS threats. Second, with regard to active monitoring of heightened awareness areas, where a UAS could potentially pose an imminent threat to public safety and security, the additional information provided by the Known Operator would assist officials to focus resources for the purposes of threat discrimination and emergency response. For example, in many such situations, UAS may be flown in support of critical infrastructure facility inspection in an authorized way. As a Known Operator, public safety agencies and law enforcement would be able to avoid utilizing unnecessary mitigation techniques on such operations. Finally, Known Operator status could assist public safety agencies and law enforcement in emergency situations where access may still be granted to specific UA operations, such as media or disaster response.

Benefits to the General Public: Establishment of a KOS would also provide a means to inform members of the public that a particular UAS is being flown by a known safe operator that has undergone vetting and evaluation, and that the UAS should not be a cause for alarm or concern. While the remote ID regime proposed in the NPRM would make certain message elements publicly accessible information, the KOS could choose to allow the general public access to additional information, such as the name of the operating entity and the fact that it is an approved KOS. This enhanced transparency would help inform the public that an otherwise worrisome sighting of unknown UA is actually an authorized commercial (or public) operation by a known entity that is part of the KOS, thereby helping to assuage any concerns the public might have with such an operation and avoiding unnecessary emergency calls to public safety agencies and law enforcement about such UAS operations. The KOS would also help the growth of public trust in UAS use as the public learns about the many beneficial uses for UAS in their communities.

Benefits to Commercial Industry / Public Safety Operators: Establishment of a KOS would enhance the commercial and public safety UAS industry's ability to operate UAS safely, securely, and responsibly. As described above, the system would reduce the likelihood that public safety and law enforcement officials would expend resources or otherwise take unnecessary drastic measures against possible or perceived threats which are, in fact, authorized

UAS operations. In case of a flagged potential incident, the additional information provided under the KOS would lead to the presumption that the UAS being flown is, in fact, being flown legally. And, as noted above, the general public would be less likely to report a UAS flight to the authorities if they understand that there has been a vetting process and the operator is a responsible Known Operator. The KOS would also assist authorized commercial operators in gaining the trust of the general public and government officials (and eventually, therefore, avoiding being disabled or otherwise mitigated unnecessarily by counter-UAS technology).

VI. INDOOR OPERATIONS

The Preamble to the NPRM begins: "This proposed rule would establish requirements for the remote identification of unmanned aircraft systems (UAS) operated in the airspace of the United States."[22] However, certain aspects of the production and design requirements of the proposed rule may effectively prevent indoor flights of UAS without remote ID, even though such indoor space is not part of the National Airspace System. The FAA does not have jurisdiction over indoor space, which we urge the FAA to clarify in the Final Rule.

Proposed Subpart F of the NPRM prescribes design and production requirements for UAS with remote ID. Under Proposed § 89.510(a)(1), two years after the effective date of the Final Rule, a person would be prohibited from producing a UAS for operation in the United States unless the UAS is "designed and produced to meet the minimum performance requirements" for Standard or Limited Remote ID UAS and "in accordance with an FAA-accepted means of compliance." Under the minimum performance requirements for both Standard and Limited Remote ID UAS, the UAS would need to be designed and produced to:

(1) automatically test remote ID functionality when the UAS is powered on; and
(2) prohibit the UA from taking off if remote ID equipment is not functional.[23]

In the context of Standard Remote ID UAS, for remote ID equipment to be deemed "functional", it must be capable of transmitting the latitude and longitude of the UA and control station.[24] For

[22] 84 Fed. Reg. at 72439.
[23] Proposed § 89.310(d) (Standard Remote ID) and Proposed § 89.320(d) (Limited Remote ID).
[24] Proposed § 89.305(b),(d).

Limited Remote ID UAS, the latitude and longitude of the control station must be transmitted to a Remote ID USS.[25] As the Preamble explains: "Under this proposed rule, all UAS with remote identification would be designed and produced such that the remote identification functionality is always enabled and cannot be disabled except as otherwise authorized by the Administrator."[26]

Given these requirements, under the FAA's proposal, it may not be possible to fly a Standard or Limited Remote ID UAS indoors as a practical matter. Moreover, the interplay of the proposed regulations might mean that there are no (or very few) commercially available UA even capable of flying in an indoor or other GPS-denied environment. The FAA should not indirectly regulate operations, like indoor operations, that it does not regulate directly. The Final Rule should be modified to make clear that nothing in the rule is meant to prevent indoor operations of UAS.

VII. REMOTE ID UAS SERVICE SUPPLIER

The CDA supports the use of Remote ID UAS Service Suppliers ("USS") as a critical part of the remote ID system. The CDA also endorses the FAA's decision to refrain from mandating a specific business model for Remote ID USS, choosing instead to permit flexibility (e.g., whether to provide such services for free or to require a subscription, payment, or personal information to access; whether to provide a suite of different services or just one service).[27]

As explained in the NPRM's Preamble, a Remote ID USS would perform four principal functions: (1) collecting and storing the remote ID message elements; (2) providing ID services on behalf of the UAS operator and acting as the UAS operator's access point to ID services; (3) providing the FAA access to the remote ID information collected and stored upon request through a data connection that may be on-demand or a continuous connection depending on safety and security needs; and (4) informing the FAA when its services are active and inactive.[28] These activities are vitally important to the success and effectiveness of the comprehensive

[25] Proposed § 89.315(b).
[26] 84 Fed. Reg. at 72465.
[27] 84 Fed. Reg. at 72484.
[28] 84 Fed. Reg. at 72484.

remote ID regime, and FAA-qualified Remote ID USS are an appropriate mechanism to handle them.

The FAA intends to provide oversight of the Remote ID USS through contractual agreements and is therefore not proposing specific rules related to how the Remote ID USS offer services. Instead of handling the oversight and "rules" solely through the contractual agreements, the FAA should – at a minimum – publish an Advisory Circular or similar guidance about what those parameters would be. If the MOU negotiation process is informative, it takes a significant amount of time and resources to reach such agreement. That challenge could be reduced if the Remote ID USS are provided with detailed guidance at the outset.

The FAA should use the successfully implemented LAANC on-boarding process as the framework for Remote ID USS. Like the on-boarding process for the FAA to approve a USS LAANC provider, an approved Remote ID USS would need to meet rigorous security, authentication, and PII requirements. The FAA clarifies in the Preamble that prospective Remote ID USS would be reviewed for consistency with national security and cybersecurity requirements and export administration regulations, and the CDA supports this approach.[29] The CDA recommends that the FAA engage industry subject matter experts to publish guidance that sets out the on-boarding requirements for Remote ID USS.

It is also critically important that all systems be interoperable to avoid Remote ID USS not being able to communicate or law enforcement having to try multiple apps to receive data. The ASTM Remote ID standard establishes a means for any approved and participating Remote ID USS to be fully interoperable with the broader Remote ID USS ecosystem. The CDA encourages the FAA to adopt this principle in the final remote ID rulemaking.

[29] 84 Fed. Reg. at 72485.

VIII. RETROFIT

The FAA should allow retrofit solutions. In the Preamble, the FAA predicts that most UAS would be able to meet the Final Rule's requirements by retrofits involving software and related updates.[30] This would enable faster and, in many cases, less expensive means of complying with the remote ID rules and obviate the need for operators to buy new Standard or Limited Remote ID UAS. The ability to retrofit UAS will thus also ensure greater compliance with the Final Rule. However, it is important that retrofits meet all of the remote ID standards in the Final Rule applicable to UAS generally, including being tamper-resistant and labelling. And, in that regard, the tamper-resistant and cybersecurity requirements in the proposed rule are very general and high-level. The FAA should specifically codify those requirements and standards in the Final Rule.

IX. IMPLEMENTATION PERIOD

We recognize and applaud recent agency action in publishing the proposed rule, but we note the proposal's three-year implementation period and (assuming the changes we describe in this document are made) emphasize the need for more immediate implementation. The three-year implementation period in the rule is too long. As long as implementation of remote ID is delayed, broad expanded UAS operations and the enormous potential of commercial UAS operations are on hold. We implore the FAA to make prompt implementation and deployment of the remote ID system a priority.

X. CONCLUSION

The CDA appreciates the opportunity to provide its comments on the NPRM, including the concerns described above:

- The 12-month application period for FRIAs is overly restrictive.
- Companies or educational institutions that manufacture, operate, test or otherwise use UAS should be able to apply for a FRIA designation.

[30] 84 Fed. Reg. at 72489-490.

- Operators should be permitted to use network only when internet is available, subject to meeting performance requirements in their specific operating environment.
- The NPRM should define certain Standard Remote ID UAS components with sufficient clarity, such as land "as soon as practicable" and internet availability.
- The NPRM should resolve significant privacy concerns by codifying specific restrictions on the availability and use of message elements; setting technical mitigations for networks to address privacy concerns; and limiting access to, and use of, retained data.
- The FAA should include a Known Operator System ("KOS") category in the Final Rule.
- The Final Rule should clarify that it does not regulate indoor operations.
- The FAA should publish guidance for how Remote ID USS oversight will be handled and how Remote ID USS can offer services.
- The FAA should allow retrofit solutions and should specifically codify tamper-resistant and cybersecurity requirements.
- If the changes described above are made, the FAA should prioritize prompt implementation and deployment of the remote ID system.

The CDA urges the FAA to address these concerns in any Final Rule. We thank you for your consideration of the CDA's comments, and we look forward to continuing our collaboration with the federal government, industry stakeholders, and others to safely integrate UAS into the NAS.