

Tim Day
Senior Vice President
U.S. Chamber of Commerce

1615 H Street, NW
Washington, DC 20062

March 2, 2020

VIA ELECTRONIC FILING

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

Re: Remote Identification of Unmanned Aircraft Systems (Docket No.: FAA-2019-1100)

To Whom It May Concern:

The U.S. Chamber of Commerce’s Technology Engagement Center (“C_TEC”)¹ appreciates the opportunity to provide comments to the Federal Aviation Administration (“FAA”) in response to the above-referenced proceeding.² Safely integrating unmanned aircraft systems (“UAS”) into the National Airspace System (“NAS”) will bring significant economic benefits for consumers as well as safety benefits for the public so it is essential that UAS integration is conducted in a secure and safe manner so these benefits can be fully realized.

C_TEC applauds the FAA’s publication of this notice of proposed rulemaking (“NPRM”) and encourages the FAA to continue moving at an expeditious pace on this NPRM and on other regulatory actions to facilitate UAS innovation. Remote identification (“Remote ID”) lays the foundation for safe integration through providing greater transparency to the NAS for manned and unmanned users as well as for stakeholders on the ground. Also, remote identification will

¹ The U.S. Chamber of Commerce is the world’s largest business federation representing the interests of more than three million businesses of all sizes, sectors, and regions. C_TEC was launched to advance technology’s role in strengthening business by leveraging tech innovations that drive economic growth in the United States. C_TEC promotes policies that foster innovation and creativity and sponsors research to inform policymakers and the public.

² Remote Identification of Unmanned Aircraft Systems, 84 Fed. Reg. 72438 (Dec. 31, 2019) (“NPRM”).

enable advanced operations including detect and avoid, operations over people, and beyond visual line of sight operations, which are essential to enable the full economic and societal potential of UAS. Finally, C_TEC believes that remote identification should serve as a basis for the future development of a UAS Traffic Management (“UTM”) system.

In general, C_TEC supports the approach taken by the NPRM, in particular the focus on network-based remote identification, but believes that several improvements can be included in a final rule to advance innovation and ensure sufficient compliance.

Standard Remote Identification

C_TEC generally supports the approach taken in this NPRM on standard remote identification and its emphasis on a network-based solution, which promotes both safety and security as well as is key for providing the basis for the future development of UTM. However, C_TEC cautions against requiring an unmanned aircraft using both network and broadcast remote identification simultaneously when operating in the NAS considering the substantial privacy and confidentiality concerns presented by a broadcast requirement. Instead, an unmanned aircraft using standard remote identification should only be required to broadcast if the unmanned aircraft loses connectivity to a Remote ID UAS service supplier (“Remote ID USS”). This balanced approach would still allow a UAS complying with standard remote identification to operate in areas with limited or no internet connectivity while ensuring the protection of the privacy and the confidentiality of other operations where a network-based option is more feasible.

Additionally, a preference for network-based remote identification will increase the availability of historical information about particular UAS operations to law enforcement authorities to facilitate more effective compliance and enforcement. As the NPRM envisions, remote identification information will be available on an historical basis only if the information passes over a network and is processed by a Remote ID USS. The NPRM does not seem to consider a mechanism by which broadcast remote identification information could be transmitted to a USS for archiving historical information. Consequently, utilizing network-based remote identification when available will avoid the historical blind spots that could accompany the use of broadcast-only remote identification solutions.

A final rule should also address several other important matters relating to standard remote identification. First, as noted above, there will be circumstances where an internet connection may not always be available, a problem particularly acute in rural or remote areas of the United States. When developing the final rule and during implementation, it is essential that the FAA consider the implications of remote identification requirements on rural or remote areas and consider methods to ensure that the benefits of greater UAS integration are not limited to only certain parts of the United States.

Some commentators have expressed concern that a network-based requirement would impose unnecessary costs to UAS operators that will ultimately hinder compliance. C_TEC disagrees with that assessment. A network-based solution would allow for competition between different Remote ID USSs, which will reduce prices and provide better and innovative services

for both commercial and recreational UAS operators. As the FAA notes in the NPRM, subscription costs for the Low Altitude Authorization Notification Capability (“LAANC”), which the Remote ID USS is modeled off of, range from \$0.00 to \$5.00 per month indicating minimal compliance costs.³ Finally, and as detailed later in these comments, the FAA, the private sector, and other stakeholders have a wide range of tools available to facilitate compliance with remote identification requirements.

Limited Remote Identification

The NPRM also establishes limited remote identification as an additional means to comply with remote identification, through requiring an internet transmission through a Remote ID USS while prohibiting broadcast remote identification entirely. C_TEC believes that as drafted, limited remote identification seems excessively restrictive and should be significantly revised in the final rule. C_TEC proposes an alternative approach that would ensure greater compliance with remote identification while protecting the safety and security of the NAS.

The present restrictions placed on UAS operations with limited remote identification, including operation within visual line of sight and within 400 feet of the control station, should be maintained. However, while limited remote identification would continue to use a network-based solution, the connection to a Remote ID USS would not need to be persistent, enabling continued operation of a UAS even if there is a loss in connectivity. Instead, a UAS operator using limited remote identification would declare their identifier and flight intent via a Remote ID USS to provide situational awareness for other airspace users. This approach is similar to LAANC, which was endorsed as an effective model in the NPRM for the Remote ID USSs.⁴

In addition, the NPRM’s present prohibition on broadcast for limited remote identification should be lifted and would instead be optional for UAS operators utilizing limited remote identification. Accordingly, the message elements transmitted by an unmanned aircraft broadcasting under limited remote identification would be required to be consistent with any standards established for broadcasting under standard remote identification to prevent inconsistencies in broadcasted message elements.

Finally, it is important that the types of operations currently envisioned under limited remote identification should not get expanded beyond the current limitations to ensure that complex and advanced UAS operations utilize a more robust compliance method for remote identification.

Exemptions to Remote Identification

The underlying purpose of a remote identification requirement is to identify all UAS operations in the NAS to provide sufficient situational awareness for unmanned and manned airspace users as well as for stakeholders on the ground. However, the NPRM correctly recognizes that there may be some situations where exemptions to remote identification are warranted.

³ See NPRM at 72492.

⁴ See *id.* at 72508.

Specifically, C_TEC supports exemptions for aeronautical research and operations in FAA-recognized identification zones (“FRIA”), but recommends several improvements. First, the definition of aeronautical research should be clarified in the final rule to ensure that private sector stakeholders conducting research and testing do not inadvertently fail to comply with remote identification requirements. Second, community-based organizations should be allowed to apply for a FRIA beyond the twelve month period delineated in the NPRM. While the FAA notes that non-remote identification compliant UAS are likely to be phased out over time, it is important that recreational users are granted some additional flexibility to operate without remote identification in the short-term. In considering new applications for a FRIA, the FAA should also be mindful of approving a FRIA by any adjacent critical infrastructure or other sensitive sites to ensure the safety and security of those sites.

C_TEC supports requiring all government UAS operations, federal, state, and local, to comply with the NPRM’s remote identification requirements to further promote the safety of the NAS. The final rule should continue ensure that federal, state, and local government users are covered under remote identification to provide additional transparency in their operations and strengthen situational awareness for all airspace users. However, C_TEC recognizes that there will be varying degrees of transparency that can be provided in government operations, and a final rule should consider additional levels of protection for security-related or other sensitive operations.

Finally, the NPRM grants the FAA Administrator the authority to grant requests allowing for the disabling of a remote identification capability. A potential issue could arise where the FAA receives a voluminous number of requests to disable remote identification which would both shift resources from other key FAA functions and potentially lead to reduced overall compliance. C_TEC recommends that the FAA either eliminate this authority or provide additional guidance and restrictions to prevent abuse of this authority.

Secure Remote Identification

There is a substantial concern among some stakeholders that the present structure for remote identification is insufficiently secure and presents privacy risks for UAS operators. To address these concerns, and provide an additional path for compliance, C_TEC proposes that the final rule establish secure remote identification, an approach consistent with the tiered remote identification framework presently contained in the NPRM.

Secure remote identification will provide additional layers of security and privacy protections for certain types of UAS operations including sensitive and security-related operations for law enforcement as well as certain categories of commercial operations such as those pertaining to critical infrastructure. However, recreational, commercial, and government operators would be eligible for to opt-in to secure remote identification. Also, it is critical that secure remote identification can support the future development of a comprehensive UTM system. C_TEC encourages the FAA to collaborate with industry and non-industry stakeholders to further develop the parameters for secure remote identification.

Compliance and Timeline

Full implementation of remote identification will enable operations beyond the restrictions contained in Part 107 including operations over people and beyond visual line of sight operations. Many innovative companies already have the capability and interest to engage in these types of operations, but are limited by a lack of a regulatory framework. The NPRM requires compliance with remote identification 36 months after the effective date of the final rule. C_TEC believes that this the deadline for compliance is too lengthy and instead supports an 18 month compliance deadline to facilitate the faster implementation of remote identification.

To support an expedited implementation period, C_TEC advocates for several actions that the FAA and industry should take. First, the FAA should adopt and implement the FAA's Drone Advisory Committee's ("DAC") recommendations on remote identification voluntary compliance.⁵ Last year, the DAC established a tasking group to develop a consensus list of options to further voluntary remote identification compliance. Some of these options include prioritization for Part 107 waiver applications, airspace access to otherwise restricted areas, and active public promotion by the FAA. These activities can be conducted in conjunction with non-FAA efforts including insurance incentives and industry education. The FAA should assess and prioritize the options recommended by the DAC before the final rule is published so they can be implemented immediately when the final rule is published.

Second, the FAA should encourage the retrofitting of existing unmanned aircraft to comply with remote identification. In the NPRM, the FAA estimates that 93% of the Part 107 fleet and 20% of the recreational fleet would be eligible for retrofits and that these retrofits could be conducted with minimal cost and before the compliance deadline.⁶ The NPRM considers that an owner or operator attaching a retrofit module to an unmanned aircraft may be deemed to be a UAS manufacturer under the rule. This has the unintended effect of discouraging retrofitting and would thus make it more challenging for retrofitting to be an effective tool to facilitate compliance. C_TEC recommends that the FAA collaborate with industry stakeholders to establish a specific Retrofit Module Manufacturer category with a respective Means of Compliance to address this concern.

Third, the FAA should consider the impact of remote identification on indoor UAS operations. UAS can be operated indoors for a wide variety of reasons including filmmaking and sports entertainment, and it is important that those use cases are able to continue after the publication of this final rule. Unfortunately, the remote identification requirements would effectively prohibit indoor operations even though there is a minimal security risk deriving from those operations. This unintended consequence could effectively prohibit those types of use cases and also exceeds the FAA's existing legal authority by regulating indoor UAS operations.

Finally, the final rule should more explicitly specify that during the implementation period, non-compliant unmanned aircraft can operate in the NAS without additional restrictions.

⁵ 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.

⁶See NPRM at 72489

This will ensure that ongoing operations using unmanned aircraft can continue without presenting confusion for UAS operators.

Registration Reforms

C_TEC strongly supports applying the existing registration requirements to all unmanned aircraft, including recreational unmanned aircraft. Registration will help to ensure compliance and transparency of users of the NAS. The NPRM proposes several changes to the registration requirements to ensure that all registered unmanned aircraft are individually registered and include unique serial numbers for each aircraft. These reforms will strengthen the existing regulations on registration and should be included in a final rule. Also, to ensure standardization of serial numbers, the FAA should issue ANSI/CTA-2063-A compliant serial numbers for unmanned aircraft registration. Finally, the FAA should clarify what information is required from operators if there are multiple users of a particular unmanned aircraft. At times, operators of unmanned aircraft may have multiple individuals able to safely operate an unmanned aircraft and operators would want to ensure they remain compliant with FAA registration requirements.

Confidential and Sensitive Operations

Some unmanned aircraft may be used for sensitive operations including for enforcement, critical infrastructure protection, filmmaking, newsgathering and other operations that require a degree of confidentiality. Specifically, C_TEC has a concern regarding providing information on the location of the control station too widely and to individuals outside of law enforcement who could interfere with legitimate UAS operations. C_TEC believes that these types of operations must be balanced with the purpose of remote identification, which is to ensure the identification of unmanned aircraft in the NAS to enhance safety and security. A final rule should take into account confidential and sensitive operations in order to preserve the integrity of those operations while balancing the needs of law enforcement and aviation safety.

The FAA should consider several approaches to mitigate these concerns. One approach would be to limit the remote identification message elements that can be shared outside of the Remote ID USS. Specifically, the final rule should limit the dissemination of historical data outside of the Remote ID USS as well as limit information that can correlate public information (such as a session ID), control station location, and non-public information. However, there may be circumstances where law enforcement requires data from a Remote ID USS to carry out legitimate law enforcement activities. Consequently, the FAA should establish a process for law enforcement to access the aforementioned types of data while protecting the confidentiality and due process of the operator. Both law enforcement and industry stakeholders should be involved in developing this process to ensure that it strikes the appropriate balance.

Remote Identification Message Elements

The NPRM delineates a list of remote identification message elements that will assist in the remote identification of unmanned aircraft. C_TEC appreciates that the NPRM notes that these message elements would also support a future UTM system. It is important the FAA

consider any relevant industry-based consensus standards in the final rule or in any future regulatory actions to promote an innovative environment for UAS operations.

While the message elements will provide important safety and security benefits to UAS operations, C_TEC does not support the inclusion of barometric pressure readings as a message element. While measuring the altitude is important, not all unmanned aircraft can present barometric pressure data, and the FAA should consider other performance-based methods of measuring the altitude of an unmanned aircraft.

Remote Identification USSs

As noted in C_TEC's comments to the Safe and Secure Operations ANPRM last April, C_TEC endorses a public-private partnership approach to facilitate UAS integration considering the existing air traffic management system cannot effectively support the forecasted expansion in UAS traffic. C_TEC is pleased to see that the FAA continued this public-private partnership approach through establishing a system of Remote ID USSs. Remote ID USSs will effectively leverage the resources and expertise of the private sector to facilitate UAS integration. The implementation of LAANC demonstrated that this concept is workable and can effectively serve the requirements of all UAS operators.

There are several important benefits of a Remote ID USS. First, a Remote ID USS will facilitate competition between different service providers and business models ensuring consumer choice and incentivize service providers to continually innovate. Second, a Remote ID USS will retain sufficient flexibility to serve as a basis for the eventual implementation of UTM and will not be bound by unnecessary prescriptive requirements.

Finally, a key component of a Remote ID USS system will be establishing a cooperative data exchange mechanism that will allow for information sharing between different Remote ID USSs. C_TEC is encouraged by the FAA's efforts to obtain information from prospective service providers through recent requests for information, and recommends that the FAA continue its collaboration with the private sector to support Remote ID USSs.

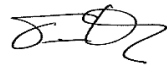
Cybersecurity

In our interconnected world, cybersecurity is of increasing importance, and UAS are no exception. C_TEC supports the FAA's recognition that cybersecurity protections are important, in particular the NPRM's adoption of the National Institute of Standards and Technology's ("NIST") standards on cybersecurity for Remote ID USSs. However, some additional clarification is welcome as to how the FAA-accepted means of compliance would contemplate cybersecurity. The NPRM currently requires that a means of compliance would include cybersecurity protection methods, but a lack of definition exists as to what factors the FAA would take into account when reviewing and evaluating the means of compliance. Some factors that the FAA could consider include confidentiality, integrity and authenticity, authorization and access control, and validation. Finally, the FAA should consider adopting the ASTM standard on remote identification security to facilitate this objective.

Conclusion

C_TEC applauds and thanks the FAA for its leadership in issuing a NPRM on remote identification. The robust adoption of remote identification will strengthen the safety and security of the NAS and unlock the ability for innovators to engage in advanced UAS operations. Moving forward, it is critical the FAA continue to engage with stakeholders to expeditiously resolve various concerns in order to advance other critical UAS regulatory actions. C_TEC stands ready to collaborate with the FAA and any other relevant federal entities on this issue and others.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'T. Day', with a stylized flourish at the end.

Tim Day
Senior Vice President
Chamber Technology Engagement Center
U.S. Chamber of Commerce