October 14, 2020

**VIA ELECTRONIC FILING**

The Honorable Steve Dickson
Administrator
Federal Aviation Administration
U.S. Department of Transportation
800 Independence Avenue, SW
Washington, DC 20591

**Re:** **Ex *Parte* Letter**, Remote Identification of Unmanned Aircraft Systems; Docket No. FAA-2019-1100

Dear Administrator Dickson:

CTIA respectfully submits this letter to supplement the record in response to the Federal Aviation Administration's ("FAA") Notice of Proposed Rulemaking proposing to establish rules for remote identification ("Remote ID") of unmanned aircraft systems ("UAS").[1] CTIA applauds the FAA for engaging in this proceeding to help facilitate safe and secure UAS operations and for proposing an approach that relies on a sensible and workable framework for Remote ID that relies principally on established and secure technologies.

As the FAA and law enforcement know, today's wireless networks are enabled through secure and reliable licensed spectrum that a wide variety of users, including law enforcement, already trust to authenticate users and provide device security via IMSI

[1] *Remote Identification of Unmanned Aircraft Systems*, Notice of Proposed Rulemaking, 84 Fed. Reg. 72438 (Dec. 31, 2019), https://www.govinfo.gov/content/pkg/FR-2019-12-31/pdf/2019-28100.pdf ("FAA Remote ID NPRM" or "NPRM") (to be codified at 14 C.F.R. parts 1, 47, 48, 89, 91, and 107).

and IMEI technology.[2] Today's 4G wireless networks offer the most advanced security features to date, and CTIA members are proud that security features in 3GPP networks improve with each release. We continue to believe that networked cellular can and should be relied upon to securely convey Remote ID information to the internet.

A number of stakeholders have raised concerns about the proposed requirement for a broadcast function, whether such a function is necessary, and the security concerns it would present. There is no question that requiring secure connections to the internet over networked cellular or other secured spectrum resources will offer a superior solution for Remote ID of UAS, and will solve the essential security issues that are at the heart of Remote ID regulations.[3] CTIA applauds the FAA for recognizing this. CTIA also supports the FAA incorporating flexibility in the Remote ID framework to ensure its long-term functioning for the UAS industry. Therefore, if the FAA decides to adopt a requirement for a secondary broadcast function for UAS in the final rules, CTIA recommends that the FAA include strong cybersecurity requirements for the broadcast Remote ID mode. CTIA requests that the FAA require that UAS information transmitted by broadcast be authenticable and integrity protected whether or not network communications are available.

The FAA should define performance-based broadcast Remote ID rules that mandate the UAS locally broadcast an identity or authorization-type that enables Remote ID receivers to verify and authenticate the UAS ID and tracking information when backhaul communications are absent or degraded. In addition, the FAA's cybersecurity requirements should ensure there is interoperability so that device receivers can properly interpret and authenticate the transmitted Remote ID even when offline. Without an interoperability requirement, law enforcement entities and other officials will not be able to trust the integrity or source of the broadcasted information.

---

[2] Comments of CTIA, FAA Remote ID NPRM, Docket No. FAA-2019-1100 (filed Mar. 2, 2020), at 7.

[3] CTIA Comments at 10.

This goal may be accomplished by use of the IEEE 1609.2 standard, which is a mature standard that a number of countries have adopted to address authentication, encryption, and message consistency/relevance checks. This standard incorporates strong cryptography, has a reduced spectrum impact due to its small certificate size, and is low cost due to its wide scale adoption. In the United States, the Department of Transportation has sponsored this standard for securing vehicular broadcasts in V2X (vehicle-to-everything) technology.

Secure transmission of Remote ID information will be critical to reliable, trustworthy UAS operations. While licensed wireless connections can and should be used to support this effort, CTIA further urges the FAA to ensure that any rules requiring broadcast Remote ID incorporate considerations to enable secure, interoperable operations using performance-based standards. CTIA appreciates the thoughtful approach taken by the FAA in proposing rules for Remote ID and believes that with the appropriate considerations the FAA's Remote ID regulations will establish a foundation of secure and safe UAS use.

Please do not hesitate to contact the undersigned with any questions.

Sincerely,

Avonne Bell

Avonne Bell
Director, Connected Life