CTIA Meeting with
Office of Information & Regulatory Affairs
FAA Remote ID Rule

November 2, 2020 at 1:30pm
Call-in: (202) 757-6419; Conference ID: 2559694

CTIA Members and Staff:

Avonne Bell, CTIA
Pascale Dumit, T-Mobile
Jeffrey Dygert, AT&T
Stefano Faccin, Qualcomm
John Kuzin, Qualcomm
Jennifer Richter, Akin Gump
Raj Sengupta, CTIA
Melissa Tye, Verizon
Steve Willingham, T-Mobile
Chris Wieczorek, T-Mobile
Amanda Armistead, Amazon

Discussion

Introduction.

- CTIA represents the U.S. wireless communications industry and companies throughout the mobile ecosystem that enable Americans to lead a 21st century connected life.
- In the UAS space, CTIA brings together wireless network providers, device manufacturers, drone operators, and other relevant stakeholders to address UAS communications functions that can be supported by commercial wireless solutions ("networked cellular").
- CTIA and its members have participated with the FAA on remote ID efforts since the beginning, from the ARC where CTIA played an important role, through the FAA Rulemaking, and continuing with the 3GPP standards development for Remote ID functionality on the cellular networks.
- CTIA was and is supportive of the FAA's approach to Remote ID as detailed in the NPRM, with certain improvements noted in our comments. We hope the Final Rule bears a strong resemblance to the content of the NPRM.

Readily Available Networks and Technologies.

- The FAA rightly suggested bringing together three widely-used technologies to support Remote ID:
    - (1) the Internet;
    - (2) cellular connections to the Internet; and
    - (3) common end user devices such as consumer cellular phones, tablets, and other wireless devices that can readily receive Remote ID message elements.
- Choosing readily available networks, technologies, and devices that can connect to the cloud, and easily share Remote ID information and situational awareness, will enable seamless integration with UTM and will support easy access to Remote ID information by law enforcement.

- The NPRM correctly advances the use of existing cellular connections to the internet to enable Remote ID. Networked cellular can and should be relied upon to convey securely Remote ID information to the internet.
- Mobile wireless networks are already built and ready for use. These networks cover over 99% of Americans. CTIA and its members have the most at stake in the use of cellular for UAS operations.
- There is strong incentive on the part of wireless providers to not only continue to expand and upgrade their coverage but ensure successful coexistence of UAS transmissions with terrestrial service, remove potential for harmful interference, and manage network security.

Security.

- As we have discussed in past meetings with OIRA, and emphasized throughout the ARC and in our comments, the safety and security of Remote ID solutions are critical.
- As the FAA has acknowledged a number of times, licensed wireless connections can and should be relied upon to securely convey Remote ID information to the Internet and share encrypted information with law enforcement.
- Network operators employ a variety of measures at the network, device, and application layers to maximize network security and efficiency, allowing its networks to be reliably used by a variety of users
- CTIA agrees with the proposed application of NIST cybersecurity standards to Remote ID UAS Service Suppliers ("USS") and UAS producers.
    - CTIA urges requiring observance of NIST standards for all components of the Remote ID system, including the transmission/ broadcast layer.

Broadcast Function.

- 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.
- CTIA agrees with concerns raised by other stakeholders such as federal safety organizations about the technical capabilities and security of using Bluetooth and Wi-Fi for the "broadcast" function.
- Broadcast Remote ID can be accomplished by any spectrum band that can support the two essential broadcast features set forth by the FAA (i.e., a non-proprietary broadcast specification; and delivery of Remote ID message elements to personal off-the-shelf wireless devices). These two features can be satisfied by either licensed or unlicensed spectrum bands, and the final rule for Remote ID should not be prescriptive about which one is used.
    - The references in the proposed rule to the use of "Part 15" spectrum for the broadcast function are too limiting, and should be deleted.
    - If the Part 15 references are not deleted, then if the FAA desires at some point to clear a DME channel to provide spectrum for a nationwide broadcast Remote ID solution, it will not be able to implement this solution without first changing the rule that requires use of "Part 15" spectrum.

- In a recent *ex parte* filing from CTIA, dated October 14, 2020 and attached, CTIA made the point that the FAA should define performance-based broadcast Remote ID rules that mandate verification and authentication requirements for any local broadcasts of Remote ID.
- The FAA's cybersecurity requirements should ensure there is interoperability so that device receivers can properly interpret and authenticate 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.
    - 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.

Restricting Availability of Message Elements.

- CTIA hopes the final rule for Remote ID is discriminating about the availability of Remote ID message elements. CTIA does not believe that "any message element that is broadcast" should be publicly available, particularly transmission of UAS serial numbers and controller location information.
    - Instead, the final rule should provide a framework that makes all Remote ID message elements available to government authorities, but minimal Remote ID message elements to the general public.

Conclusion/Wrap Up.

- We appreciate your time and would be happy to answer any questions you have, or provide any additional information that would be helpful.