Before the
FEDERAL AVIATION ADMINISTRATION
Washington, D.C. 20590

In the Matter of )
) FAA Docket No. FAA-2019-1100
Remote Identification of Unmanned Aircraft Systems )

COMMENTS OF CTIA

Thomas C. Power
Senior Vice President and General Counsel

Scott K. Bergmann
Senior Vice President, Regulatory Affairs

Kara Graves
Assistant Vice President, Regulatory Affairs

Jennifer L. Oberhausen
Director, Regulatory Affairs

Raj Sengupta
Director, Wireless Technology

CTIA
1400 16th Street, NW, Suite 600
Washington, D.C. 20036
(202) 736-3200

March 2, 2020
TABLE OF CONTENTS

I. INTRODUCTION .................................................................................................................. 1

II. CTIA APPLAUDS THE FAA ON ITS PRACTICAL APPROACH TO REMOTE ID, WHICH RELIES ON ESTABLISHED AND SECURE TECHNOLOGIES THAT, IN COMBINATION, CAN SUPPORT THE UAS INDUSTRY ......................................................... 3
   A. Reliance On Cellular Connections to the Internet and Common End User Devices is the Right Solution for UAS Remote ID. ....................................................................... 4
   B. CTIA and Its Members are Working to Ensure Successful Coexistence of UAS Transmissions Over Wireless Spectrum with Terrestrial Services .............................. 5

III. THE FAA IS RIGHT TO PROMOTE SAFE AND SECURE TECHNOLOGIES TO ACCOMPLISH REMOTE ID, INCLUDING THROUGH APPLICATION OF NIST CYBERSECURITY STANDARDS ................................................................................................. 6
   A. CTIA Agrees that Licensed Wireless Connections Can and Should Be Rely Upon to Securely Convey Remote ID Information to the Internet ......................................... 7
   B. CTIA Supports Leveraging the NIST Cybersecurity Standards for Remote ID ...... 8
   C. The FAA Should Not Impose Its Own Internal Security Standards on Third-Party USS ...................................................................................................................... 9

IV. TO THE EXTENT THE FINAL REMOTE ID RULE INCLUDES THE SECONDARY BROADCAST FUNCTION, THE FAA SHOULD REFINE THE REQUIREMENTS TO INCLUDE ANY SPECTRUM BAND THAT CAN SATISFY THE TWO ESSENTIAL “BROADCAST” FEATURES ................................................................. 9
   A. A Part 15 Limitation Contradicts Other Parts of the NPRM and Will Unnecessarily Restrict the Usefulness of the Broadcast Function ............................................... 10
   B. Commercial Wireless Networks Incorporate Licensed and Unlicensed Bands and Can Satisfy The Two Essential Requirements of the Broadcast Capability ........... 11
   C. The FAA Desires Maximum Range for the Broadcast Function, But Part 15 Spectrum Has Limited Range ....................................................................................... 12
   D. Relying on Broadcasts Over Part 15 Spectrum and Using Bluetooth and Wi-Fi Technologies Will Result in the Remote ID Capability Not Functioning in Many Scenarios, Contrary to the FAA’s Intent ................................................................. 13
   E. The FAA Should Refine the Requirements for Any Broadcast Function Adopted to Include Specification of Any Spectrum Band ..................................................... 15

V. THE FAA SHOULD RECONSIDER THE REQUIREMENT TO MAKE ALL REMOTE ID MESSAGE ELEMENTS AVAILABLE TO THE GENERAL PUBLIC ... 16

VI. CONCLUSION ...................................................................................................................... 18
In the Matter of
Remote Identification of Unmanned Aircraft Systems

FAA Docket No. FAA-2019-1100

COMMENTS OF CTIA

CTIA\(^1\) respectfully submits these comments in response to the Notice of Proposed Rulemaking (“NPRM”) issued by the Federal Aviation Administration (“FAA”) proposing to establish rules for remote identification (“Remote ID”) of unmanned aircraft systems (“UAS”).\(^2\)

I. INTRODUCTION.

CTIA commends the FAA on the approach it takes in the NPRM. CTIA has spent many productive months working with the FAA and UAS stakeholders on Remote ID issues, and was pleased to volunteer in 2017 as an active and voting member on the FAA’s Aviation Rulemaking Committee (“ARC”) for Remote ID. In the NPRM, the FAA proposes a sensible and workable framework for Remote ID that relies principally on established and secure technologies such as networked cellular and that will support continued growth for the UAS industry, enabling easy integration of Remote ID messaging with critical UAS traffic management (“UTM”).

\(^1\) CTIA – The Wireless Association® (“CTIA”) (www.ctia.org) represents the U.S. wireless communications industry and the companies throughout the mobile ecosystem that enable Americans to lead a 21st century connected life. The association’s members include wireless carriers, device manufacturers, suppliers as well as apps and content companies. CTIA vigorously advocates at all levels of government for policies that foster continued wireless innovation and investment. The association also coordinates the industry’s voluntary best practices, hosts educational events that promote the wireless industry and co-produces the industry’s leading wireless tradeshow. CTIA was founded in 1984 and is based in Washington, D.C.

The NPRM repeatedly suggests bringing together three widely-used technologies to support Remote ID for all UAS: (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. The importance of leveraging these existing technologies cannot be overestimated, as it will hasten advanced operations for the UAS industry. These three technologies, in combination, will provide a powerful foundation for the Remote ID system. Moreover, choosing readily available networks, technologies, and devices that can connect to the cloud, and easily share Remote ID information and situational awareness about UAS, will enable seamless integration with UTM and will support easily getting critical Remote ID information to “law enforcement and other officials charged with ensuring public safety.”

While CTIA generally supports the FAA’s approach, CTIA encourages the FAA to consider several modifications to the proposed Remote ID rules in order to better promote the goal of this proceeding to “ensure public safety and the safety and efficiency of the airspace of the United States.” Specifically, CTIA recommends that the FAA:

- **Rely on the National Institute of Standards and Technology ("NIST") cybersecurity standards for all components of the Remote ID ecosystem.** Since the purpose of the Remote ID regulations is to address safety and security concerns associated with use of UAS, the FAA is right in the NPRM to reference the use of safe and secure technologies to accomplish it, including cellular connections to the internet. CTIA agrees with the proposed application of NIST cybersecurity standards to Remote ID UAS Service Suppliers (“USS”) and UAS producers and urges the

---

3 *Id.* at 72439.

4 *Id.*

5 The National Institute of Standards and Technology is housed in the United States Department of Commerce. Its mission is to promote innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. NIST has developed a Cybersecurity Framework.
FAA to go further by supporting use of the NIST standards for all components of the Remote ID system, including the transmission/broadcast layer.

- **Expand the spectrum options for the “broadcast” function and not limit broadcasts to Part 15 spectrum.** To the extent the final Remote ID rule continues to require the secondary broadcast function for standard UAS, which some commenters view as redundant, unnecessary, and technologically sub-optimal, the FAA should recognize that the broadcast function 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 off-the-shelf wireless devices). These two features can be satisfied by either licensed or unlicensed spectrum bands. The references in the proposed rule to satisfy the broadcast function with “Part 15” spectrum are too limiting, will erect barriers and limitations to sharing Remote ID information, and should be deleted.

- **Restrict availability of “all” Remote ID message elements to law enforcement.** CTIA urges the FAA to reconsider its proposal that “any message element that is broadcast would be publicly available,” particularly transmission of UAS serial numbers and controller location information. Instead, the FAA should provide a framework for network service authorization and user profile management such that all Remote ID message elements are available to government authorities, but minimal Remote ID message elements are broadcast to the general public.

By adopting the proposals in the NPRM, modified as discussed herein, the FAA will provide the UAS industry with a solid foundation for future growth and expanded UAS operations.

II. **CTIA APPLAUDS THE FAA ON ITS PRACTICAL APPROACH TO REMOTE ID, WHICH RELIES ON ESTABLISHED AND SECURE TECHNOLOGIES THAT, IN COMBINATION, CAN SUPPORT THE UAS INDUSTRY.**

CTIA members—who own, build, and operate today’s cellular networks—are proud that their networks can play an essential role in supporting important UAS communications functions, including Remote ID, which are critical for UAS safety and security. CTIA applauds the FAA for recognizing this approach, and its members are working to ensure successful coexistence of UAS transmissions with terrestrial wireless services.

---

6 FAA Remote ID NPRM at 72485.

A. Reliance on Cellular Connections to the Internet and Common End User Devices is the Right Solution for UAS Remote ID.

CTIA agrees with the FAA that reliance on the internet to disseminate Remote ID information to law enforcement, USSs, and UTM is key. This approach was implicit in the work of the ARC and will ensure the availability of Remote ID messaging to the greatest number of stakeholders. As the FAA notes:

[A]n internet-based solution is appropriate [for Remote ID], when the internet is available, because the internet is the largest, most multifaceted, and prevalent platform for data transmission. Under the proposed rule, the internet would be considered available if cellular or other forms of wireless internet connectivity such as Wi-Fi are available in an operational area with sufficient signal strength to maintain a connection between the UAS and the internet. UAS with remote identification would automatically connect to the internet when it is available, similar to how wireless devices, such as smart phones, connect automatically to the internet when there is sufficient signal strength and coverage.  

Choosing readily available networks, technologies, and devices that can connect to UAS, the internet, and the cloud will enable sharing of Remote ID information and UAS situational awareness with all stakeholders that have a need to know, including “law enforcement and other officials charged with ensuring public safety.” It is not lost on the FAA that leveraging existing cellular systems, technologies, and devices for Remote ID is important for law enforcement, a constituency that needs a ready-built ecosystem for Remote ID in order to address safety and security concerns raised by UAS operations. During Remote ID ARC deliberations, for example, representatives of public safety raised the importance of receiving Remote ID messages

---

8 FAA Remote ID NPRM at 72467. As the NPRM notes, operators of UAS typically already “own a smartphone or other electronic device which is capable of transmitting the location of the control station to the internet.” Id. at 72499, n.159.

9 Id. at 72439.
over existing cellular devices—tools public safety already uses every day and relies upon. The FAA approach to Remote ID ensures this result and notes that the “FAA anticipates that in the future, third parties may develop mobile phone applications [for Remote ID] for law enforcement use.”

B. CTIA and Its Members are Working to Ensure Successful Coexistence of UAS Transmissions Over Wireless Spectrum with Terrestrial Services.

Although the NPRM strongly—and correctly—advances the use of existing cellular connections to the internet to enable Remote ID, it also raises questions regarding the impact of UAS connecting directly to the internet from the air. As the FAA knows, CTIA members, who provide valuable wireless services to more than 99 percent of the U.S. population and nearly 422 million devices nationwide, have the most at stake to protect their networks from interference. CTIA members are working on coexistence issues through independent testing, the FAA’s Integration Pilot Program, industry standards-setting bodies such as 3GPP, and with the Federal Communications Commission (“FCC”) and FAA directly to address any concerns related to UAS transmissions. For example, as Verizon noted recently to the FCC, degrading service to its wireless customers would almost certainly “expose Verizon to tremendous

---

10 Id. at 72471, n.66.


12 The 3rd Generation Partnership Project is a global standards organization that develops protocols for mobile telephony.

13 In view of the FCC’s spectrum management role, which is different from the FAA’s safety mandate, it is essential that the FAA and FCC continue their ongoing dialogue about spectrum solutions for UAS and collaborate with industry and standards-setting bodies on any open questions. See, e.g., CTIA Reply Comments, FCC GN Docket No. 19-356, at 14 (filed Jan. 27, 2020).
economic downside.”14 Likewise, causing interference to other carriers’ networks would only undermine the industry’s collective interest in promoting the use of cellular networks for UAS. To that end, CTIA members have investigated and are continuing to examine the degree to which drone deployments impact both their own networks and the networks of neighboring licensees in adjacent bands or geographies. Verizon, for instance, reports that its results have been “encouraging,” and it intends to share its ongoing progress and findings with the FCC and FAA in the near future.15 In short, the wireless industry is intensely competitive, and carriers will work to ensure that spectrum consumption by UAS does not create harmful interference to core terrestrial wireless services, including services in adjacent markets and bands.

III. THE FAA IS RIGHT TO PROMOTE SAFE AND SECURE TECHNOLOGIES TO ACCOMPLISH REMOTE ID, INCLUDING THROUGH APPLICATION OF NIST CYBERSECURITY STANDARDS.

The purpose of the Remote ID regulations for UAS is clear—to ensure safe and secure use of UAS. Security agencies and the FAA have been concerned for years about the inherent anonymity of UAS and the absence of a workable system for remotely identifying UAS, which is essential to executing counter UAS measures. The FAA is thus correct to develop rules that achieve this goal. Indeed, adopting such rules will allow the FAA to move on to promulgating more progressive and permissive UAS regulations that will allow for increasingly complex UAS operations such as flight beyond visual light of sight and flight over people. The FAA should thus rely on NIST standards to ensure compliance with the agency’s requirements and guidelines where appropriate.16 To further enhance the safety and security objectives, the FAA should

15 Id. at 7-8.
16 FAA Remote ID NPRM at 72485.
leverage the NIST standards for all components of the Remote ID system, including the transmission/broadcast layer.

A. CTIA Agrees that Licensed Wireless Connections Can and Should Be Relyed Upon to Securely Convey Remote ID Information to the Internet.

In view of the mandate to provide a Remote ID solution that will alleviate safety and security concerns, the NPRM takes the right approach to embrace use of secure technologies. In particular, the FAA correctly rejects the use of unencrypted, unlicensed broadcasts to convey Remote ID information for all UAS. The FAA also correctly rejects use of unencrypted ADS-B technology. Instead, the FAA emphasizes a number of times that it is licensed wireless connections that can be relied upon to securely convey Remote ID information to the internet and share that encrypted information with law enforcement. 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 and IMEI technology.17 Network operators employ a variety of measures at the network, device, and application layers to maximize network security and efficiency, allowing for reliable transmission of Remote ID messages. Moreover, the wireless industry has a long history of protecting consumers, networks, and technology from cyber threats. Networked cellular is equipped with a variety of security approaches, including authentication technologies that validate and authorize users. Today’s 4G wireless networks

---

17 IMSI stands for “International Mobile Subscriber Identity,” a unique number, usually 15 digits, associated with GSM and Universal Mobile Telecommunications System (“UMTS”) network mobile phone users. The IMSI is a unique number identifying a GSM subscriber and is stored in the Subscriber Identification Module (“SIM”) inside the phone. IMEI is short for “International Mobile Equipment Identity,” a unique number, typically 15 or 17 digits, stored on the backside of a device’s battery. The IMEI is used for identification by GSM, Wideband Code Division Multiple Access (“WCDMA”), and some satellite devices. Unlike the IMSI, the IMEI is stored inside the phone and not on the SIM card and cannot be swapped out.
offer the most advanced security features to date, and CTIA members are proud that security features in 3GPP networks improve release over release.

CTIA agrees with commenters that raise concerns with the FAA about using Part 15 broadcast connections for Remote ID, which are inherently not secure and not reliable.\textsuperscript{18} Conveying Remote ID information over secure connections is necessary because the FAA does not want to trade one security problem for another. The FAA recognizes as much through its clear preference for using secure wireless networks and devices to enable Remote ID, which is mentioned more than 20 times in the NPRM.

B. CTIA Supports Leveraging the NIST Cybersecurity Standards for Remote ID.

CTIA supports the FAA’s proposal to utilize the NIST standards “to ensure compliance with [Remote ID] requirements and guidelines where appropriate.”\textsuperscript{19} The communications and aviation sectors are among the sixteen sectors included in the NIST Critical Framework for Cybersecurity (the “NIST Framework”), a longstanding public-private partnership focused on sharing information related to cybersecurity and responding to evolving cybersecurity threats at the network, device, and application layers. The NIST Framework expands on significant

\textsuperscript{18} See, e.g., Comments of Edward Mitchell, FAA Remote ID NPRM, at 2 (filed Feb. 14, 2020) (“FAA’s proposed use of FCC Part 15 spectrum will cause interference and crashes. . . . This is not how Part 15 bands are intended to be used, [and] will cause interference to residential consumer devices and licensed services, and may lead to receiver desense and loss of flight control signals.”); Comments of Ray Meyer, FAA Remote ID NPRM, at 1 (filed Jan. 16, 2020) (“Wi-Fi can and often degrades or interferes with the control link of the UAS when used.”); Comments of Robert Meade, FAA Remote ID NPRM, at 4 (filed Feb. 19, 2020) (“This is an ill-conceived design goal with no basis in practicality. . . . [Unlicensed bands] are saturated with network and data link traffic as well as control link and video signals for UAS. Any effective and viable operation of a transponder service in this frequency range would have no greater reach than a control link to a UAS operator. . . . Operation at higher power levels would become a wifi (sic), cellular, Bluetooth, and UAS communications jammer.”).

\textsuperscript{19} FAA Remote ID NPRM at 72485.
industry efforts by CTIA members to collaborate on standards and guidance for cybersecurity protection of the wireless networks.

CTIA agrees with the FAA proposal that “[r]emote ID USS and UAS producers would be responsible for ensuring that UAS remote identification data and connections would be protected against cyber-attacks.”\textsuperscript{20} It is worth noting, however, that all potential access points in the Remote ID ecosystem must be secured. To that end, CTIA recommends that the FAA rely on the NIST cybersecurity standards for the transmission and broadcast connections for Remote ID as well.

C. The FAA Should Not Impose Its Own Internal Security Standards on Third-Party USS.

The FAA should not require adherence to the security standards used for FAA information systems—FAA Order 1370.121, the “FAA Information Security and Privacy Program & Policy”—for Remote ID USS. Those policies were not written with the requirements of Remote ID in mind, and include a number of features that apply specifically to the Department of Transportation and the FAA, such as behavioral rules and telework policies. Instead, the FAA should follow through with relying upon consensus-based NIST standards to secure all components of the Remote ID system, including the transmission and broadcast functions.

IV. TO THE EXTENT THE FINAL REMOTE ID RULE INCLUDES THE SECONDARY BROADCAST FUNCTION, THE FAA SHOULD REFINE THE REQUIREMENTS TO INCLUDE ANY SPECTRUM BAND THAT CAN SATISFY THE TWO ESSENTIAL “BROADCAST” FEATURES.

As noted above, CTIA is aware that many commenters are questioning the necessity of the broadcast function, and are raising security concerns related to Part 15 broadcasts. There is

\textsuperscript{20} Id.
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. CTIA applauds the FAA for recognizing this. CTIA also supports the FAA building flexibility into the Remote ID framework in order to ensure its long-term functioning for the UAS industry. To that end, if the FAA determines in the final rules to require the secondary broadcast function for standard UAS, it should refine the requirements as detailed below and include specification of any spectrum band that can satisfy the two essential requirements of the broadcast function: (1) use of a non-proprietary broadcast specification; and (2) delivery of Remote ID message elements to off-the-shelf wireless devices.21

A. A Part 15 Limitation Contradicts Other Parts of the NPRM and Will Unnecessarily Restrict the Usefulness of the Broadcast Function.

The Part 15 reference in Section 89.310 seems at odds with other Remote ID rules and statements in the NPRM, and would, in any event, be too limiting. As an initial matter, references to Part 15 fail to encompass all unlicensed bands, including the Part 18 Industrial Scientific and Medical (“ISM”) bands. More importantly, however, such references fail to include use of licensed bands that are capable of satisfying the two essential components of the broadcast function. CTIA does not believe it was the intention of the FAA in the NPRM to limit the broadcast function to “Part 15” spectrum—nor should it, as doing so would restrict the effectiveness of the broadcast Remote ID requirement.

Use of Part 15 spectrum is not included in the definition of “broadcast” contained in the NPRM at Section 89.1. There, the term “broadcast” is defined to mean “to send information

21 See, infra, Section IV.E, for further discussion.
from an unmanned aircraft using radio frequency spectrum.”22 Moreover, the NPRM characterizes the broadcast function in a flexible manner, stating that it must ensure “in real time during the whole duration of the flight, the direct periodic broadcast from the unmanned aircraft using an open and documented transmission protocol of the following data, in a way that they can be received directly by existing mobile devices within the broadcasting range.”23 In other words, the NPRM and the definition of “broadcast” from the proposed Remote ID rules do not limit the broadcast function to use of Part 15 spectrum.

In fact, the FAA is clear to the contrary, stating: “The FAA is not, however, proposing a specific frequency band. Rather, the FAA envisions industry stakeholders would identify the appropriate spectrum to use for this capability and would propose solutions through the means of compliance acceptance process.”24 As noted herein, there are many spectrum solutions that are appropriate for the broadcast capability, including licensed wireless bands that can transmit using a non-proprietary specification and can send messages to off-the-shelf wireless devices. All options for the broadcast function should be embraced by the FAA.

B. Commercial Wireless Networks Incorporate Licensed and Unlicensed Bands and Can Satisfy The Two Essential Requirements of the Broadcast Capability.

The commercial wireless networks operated by CTIA members can satisfy the essential requirements of the broadcast capability by using both licensed and unlicensed bands, operating according to non-proprietary specifications, and sending broadcast ID messages to off-the-shelf wireless devices. Today’s commercial wireless networks are heterogeneous—i.e., they rely upon use of both licensed and unlicensed spectrum. 3GPP is working on a globally harmonized, non-

22 FAA Remote ID NPRM at 72461.
23 Id. at 72456.
24 Id. at 72476.
proprietary Remote ID broadcast specification for all cellular networks. Thus, commercial wireless bands will be able to satisfy the broadcast function, both inside and outside of the network. For example, LTE-Direct technology functions over wireless spectrum both inside and outside of network coverage, and can provide reliable broadcast of Remote ID messages outside of network coverage, with low latency, high reliability, and superior security. Satisfying the broadcast function over LTE-Direct also offers advanced security capabilities such as authentication of the user. As the FAA is aware, IMSI/IMEI-based technology is highly capable and secure, whereas Wi-Fi technologies do not mandate authentication and are sub-optimal for outdoor use cases.


It is worth noting as well that the FAA should not limit the broadcast function to Part 15 frequencies because of the limited range of such spectrum. The FAA proposes that broadcast devices using Part 15 spectrum should “maximize the range” at which the broadcast can be received,25 stating that “[m]aximizing the broadcast range would ensure that remote identification information would be available to the largest number of potential receiving devices within the limits permitted by law.”26 The FAA is well aware, however, that Part 15 spectrum has severely limited range due to FCC-imposed power limitations. To provide context for the viable ranges of broadcast transmissions over licensed spectrum versus unlicensed spectrum, consider the following: Using LTE-Direct over licensed spectrum for the broadcast function can provide reliable Remote ID messages at ranges of up to 500 meters, whereas Wi-Fi Direct or Bluetooth Low Energy technology can only provide broadcast transmissions up to the tens of

25 Id. at 72520.
26 Id.
meters. Moreover, the FCC’s Technological Advisory Council (“TAC”), which is studying options for UAS communications, found in a recent report that, except in very sparsely populated areas, Wi-Fi and Bluetooth technologies are not likely to reliably satisfy Remote ID capabilities.\textsuperscript{27} The TAC found that Remote ID technologies over Wi-Fi and Bluetooth are only potentially reliable in truly rural and remote areas with populations of less than 10,000 people per square mile.

D. Relying on Broadcasts Over Part 15 Spectrum and Using Bluetooth and Wi-Fi Technologies Will Result in the Remote ID Capability Not Functioning in Many Scenarios, Contrary to the FAA’s Intent.

Finally, requiring Remote ID broadcasts to operate exclusively in Part 15 spectrum would result in Remote ID information being unavailable in large parts of the country, which serves no stakeholder interest, particularly law enforcement. As noted by the TAC, restricting the broadcast function to Part 15 spectrum will result in many instances in which the broadcast function will not be available due to technology limitations. Even beyond that, interference and congestion in Part 15 bands also will contribute to Remote ID not functioning. As the NPRM notes, Part 15 spectrum is entitled to no protections.\textsuperscript{28} It may not be possible to mitigate interference or congestion to these bands, resulting in the unavailability of the broadcast function. In order to ensure, to the greatest extent possible, that broadcast transmissions of Remote ID messaging are actually transmitted and received, the FAA should not rely on Part 15 spectrum alone.

In addition, as the FAA knows, unlicensed spectrum has unlimited users and must be shared with users in the air and on the ground in controlled or uncontrolled environments. There


\textsuperscript{28} FAA Remote ID NPRM at 72476.
are no protocols or etiquette in the unlicensed bands that would prevent any user or group of
users from monopolizing the spectrum and crowding out UAS users in the air, risking safety and
preventing critical Remote ID information from being shared with Remote ID USSs and law
enforcement. Relying solely on Part 15 spectrum would thus negatively impact the operational
performance, reliability, and security of Remote ID. For example, there may be unpredictable
instances during which Remote ID and tracking information will not be available to a Remote ID
USS or law enforcement because the unlicensed solution is overcrowded or experiencing
interference. It would be impossible for law enforcement to ascertain why the information is
unavailable, if the UAS is non-cooperative, and if it must be taken out of the sky.

Conversely, providing reliable, secure, verifiable, and authentic Remote ID information
using licensed wireless networks for the broadcast function will ensure that Remote ID
messaging is actually useful for Remote ID USS systems and law enforcement. Cellular
networks and devices offer many advantages. First, nearly all LTE devices today have a number
of sensors to track speed, location, direction, movement, and height above sea level, and LTE
Location Based Services and features such as OTDOA (Observed Time Difference of Arrival)
and eCID (Enhanced Cell ID) are continuously evolving. These developments indicate location
technologies offered by cellular technologies have significantly progressed and can offer location
accuracy and validation to law enforcement and Remote ID USSs. Second, when 5G technology
is widely deployed, studies suggest that location accuracy will be improved to sub-meter level
position accuracy. Third, Global Navigation Satellite Systems ("GNSS") receivers are integrated
in most LTE modules, which improve the availability and accuracy of position information using
network assistance, including cell signal triangulation. Those GNSS receivers can independently
confirm drone location information and share that useful information with Remote ID USSs and
law enforcement. Fourth, licensed wireless spectrum in today’s wireless networks also leverages unique IMEI. A Remote ID USS could use IMEI numbers to identify a UAS. Fifth, existing SIM technology also could provide independent verification. SIM card technology can easily identify and independently verify the identity of the registered UAS owner. And finally, SSL/TLS certificates provide an additional layer of encrypted transmission security. Simple Wi-Fi and Bluetooth technologies, if that is what the FAA means by use of “Part 15 spectrum,” do not require the use of any of the foregoing capabilities.

E. The FAA Should Refine the Requirements for Any Broadcast Function Adopted to Include Specification of Any Spectrum Band.

For all the reasons detailed above, the FAA should not limit the broadcast function to Part 15 spectrum. Instead, CTIA recommends that the FAA modify its remote ID rule to make clear that its requirements for the broadcast function for standard UAS can be achieved via any spectrum band—whether unlicensed or licensed—that uses a non-proprietary broadcast specification and can deliver Remote ID message elements to off-the-shelf wireless devices.

Currently, proposed rule Section 89.310 states that standard UAS:

must be capable of broadcasting the message elements . . . using a non-proprietary broadcast specification and using radio frequency spectrum in accordance with part 15 of title 47, Code of Federal Regulations, where operations may occur without an FCC individual license that is compatible with personal wireless devices.  

As written, the two essential features of the broadcast function are: (1) that a non-proprietary broadcast specification is used; and (2) that the Remote ID message elements are capable of delivery to off-the-shelf wireless devices. The purpose of these requirements is clear: to ensure that Remote ID broadcast information is available as widely as possible. To better satisfy this

29 Id. at 72520 (emphasis added).
goal, the final Remote ID rule should remove the reference to Part 15, which will limit, not expand, the availability of broadcast Remote ID messaging. The FAA also should substitute the language “personal wireless devices” with “commonly available consumer cellular phone, tablet, or other wireless devices,” as stated elsewhere in the NPRM.30

Combining these modifications, CTIA suggests the following specific changes to proposed Section 89.310:

a standard UAS “must be capable of broadcasting the message elements . . . using a non-proprietary broadcast specification and using radio frequency spectrum that can be received by commonly available, interoperable, consumer cellular phones, tablets, or other wireless devices capable of receiving that broadcast.”

At a minimum, if the FAA chooses not to modify Section 89.310 as suggested above, it should provide in the advisory circular, “Means of Compliance Process for Remote Identification of Unmanned Aircraft Systems,” that UAS with an embedded wireless connection (e.g., a 4G or 5G modem) can satisfy the broadcast function through this method, which serves as an alternate means of compliance.

V. THE FAA SHOULD RECONSIDER THE REQUIREMENT TO MAKE ALL REMOTE ID MESSAGE ELEMENTS AVAILABLE TO THE GENERAL PUBLIC.

In order to provide a better balance between the public’s right to know and the privacy rights of UAS operators, CTIA urges the FAA to reconsider its proposal in the NPRM that “any message element that is broadcast would be publicly available.”31 While CTIA agrees that all

30 Id. at 72485. This clarification will honor the FAA’s desire, as stated in the NPRM, to use “existing commonly available and 47 CFR part 15 compliant devices, such as cellular phones, smart devices, tablet computers, or laptop computers, to receive these broadcast messages.” This substitution will ensure that only devices that are interoperable with other off-the-shelf wireless devices are used for receiving Remote ID message elements.

31 Id. at 72485.
message elements should be made available to law enforcement, certain information—such as the transmission of UAS serial number and controller location information—is particularly sensitive and should not be made available to the general public.

First, the FAA should consider the purpose of sharing “all” Remote ID message elements with the public, including “the identity of the UAS (serial number or Session ID), the latitude and longitude [of the control station and UAS], barometric pressure and altitude of the control station and UAS, the time mark, [and] an indication of the emergency status of the UAS, which could include lost-link or downed aircraft.”32 CTIA appreciates the need for law enforcement to have all of this information, but the practical scope of the information that will be useful to the general public is likely limited to whether there is a cooperative UAS in the area, the location of the aircraft, and whether that aircraft has been registered to fly through a Remote ID USS as indicated by an authenticated USS-provided session ID. It also would be appropriate to inform the public if there is an emergency status associated with a UAS.

Second, broadcasting or transmitting via the internet the manufacturer-provided serial number should not be required, as it compromises security and the privacy of the UAS operator, potentially giving away too much personally identifiable information if the serial number and owner are matched and opening up opportunities to retrieve the “permanent” serial number and spoof the UAS identity. Instead, CTIA recommends use of a USS-provided “session ID,” one of the options offered by the FAA. A temporary session ID would not only provide necessary, authenticated identity information to law enforcement that cannot be spoofed, but it also would protect the privacy of the UAS operator.

32 Id. at 72465.
The “UAS serial number (SN),” as defined in the ANSI/CTA 2063 standard and labeled on the UAS, can also incorporate a 15-digit IMEI number as the manufacturer’s serial number. Using the IMEI can offer additional device security and can be registered within the CEIR (Central Equipment Identity Register) or IMEI DB (database). Such a database would provide services such as tracking lost or stolen UASs (blacklisted UAS) and enabling enhanced recordkeeping of UAS flight activities.

The FAA also should not make available to the general public the location information for a UAS controller. This is essential information for law enforcement to know, but the FAA should work to ensure that it does not create a scenario in which the safety of a UAS controller is compromised by providing to the public the location of that controller/operator.

Finally, the FAA should consider requiring, for all Remote ID information that is broadcast, an interoperable encryption and authorization mechanism.

VI. CONCLUSION.

CTIA appreciates the thoughtful approach taken by the FAA in proposing rules for Remote ID. With a few simple modifications as discussed herein, the framework set by the FAA will serve as a firm foundation for Remote ID regulations that will help to assuage the concerns of the security community with respect to UAS use.
Respectfully submitted,

/s/ Kara Graves
Kara Graves
Assistant Vice President, Regulatory Affairs

Thomas C. Power
Senior Vice President and General Counsel

Scott K. Bergmann
Senior Vice President, Regulatory Affairs

Jennifer L. Oberhausen
Director, Regulatory Affairs

Raj Sengupta
Director, Wireless Technology

CTIA
1400 16th Street, NW, Suite 600
Washington, D.C. 20036
(202) 736-3200

March 2, 2020