April 15, 2019

BY ELECTRONIC SUBMISSION

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: FEDERAL AVIATION ADMINISTRATION
ADVANCE NOTICE OF PROPOSED RULEMAKING
SAFE AND SECURE OPERATIONS OF SMALL UNMANNED AIRCRAFT SYSTEMS
(DOCKET NUMBER FAA-2018-1086)

Ladies and Gentlemen:

CTIA\(^1\) provides these comments in response to issues raised by the Federal Aviation Administration ("FAA") in the above-referenced Advance Notice of Proposed Rulemaking ("ANPRM") pertaining to safe and secure operations of small unmanned aircraft systems ("sUAS").\(^2\) Although sUAS is the focus of this proceeding, commercial wireless technology is well-suited to support unmanned aircraft systems ("UAS") beyond sUAS. As a consequence, these comments refer not just to sUAS, but also UAS more broadly.

\(^1\) CTIA-The Wireless Association® (www.ctia.org) represents the U.S. wireless communications industry and the companies throughout the mobile ecosystem that enable Americans to live a 21st century connected life. The association’s members include wireless carriers, device manufacturers, and 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.

As the representative of the U.S. wireless communications industry, CTIA brings a unique perspective to this proceeding. As the FAA is aware, safe and secure communications links are necessary to the functioning of UAS. A critical feature of the FAA’s definition of sUAS is the “communication links and the components that control” the sUAS.\textsuperscript{3} Additionally, FAA is aware that there is not enough aviation-protected spectrum available today to satisfy the communications links needed by UAS.\textsuperscript{4} Obtaining future spectrum allocations for UAS is uncertain and building new networks could take many years—time the United States cannot afford if the UAS opportunity is to flourish domestically.

Over the past five years, the FAA and Federal Communications Commission (“FCC”) have embraced 4G and 5G commercial wireless technology for safe, secure and reliable UAS communications links. These comments detail substantial progress in recognizing commercial wireless networks as a significant and necessary option for UAS communications. Continued FAA action is necessary, however, to ensure that unmanned aviation policy supports these solutions.

In these comments, CTIA makes the following points in response to the ANPRM:

(I) Commercial wireless technology provides the features necessary for UAS communications needs, and the industry is working with the FAA and FCC to address UAS integration issues;

(II) The FAA should establish reasonable, risk-based design requirements for safety-critical elements of UAS systems, such as communications links. Today’s commercial wireless technology offers authentication and security, quality of service, reliability, redundancy and interoperability;

\begin{enumerate}
\item \textsuperscript{3} 14 C.F.R. §107.3.
\item \textsuperscript{4} In 2012, the World Radio Conference (“WRC”) recommended the 5030-5091 MHz band for allocation to aviation mobile radio service (“AM(R)S”) on a primary basis in order to support line-of-sight control links for UAS. The Federal Communications Commission (“FCC”) allocation of this band is complete, but service rules are needed. The Aviation Industry Association (“AIA”) filed a Petition for Rulemaking requesting service rules in this band, which remains pending. Similarly, WRC-07 recommended allocation of the 960-1164 MHz band for UAS-based AM(R)S. There are many government radars in the band, at least in the U.S., bringing into question what portions of this band, if any, can be used to support UAS. Similar to the 5030-5091 MHz band, the FCC allocation of 960-1164 MHz is complete, but there are no service rules.
\end{enumerate}
The FAA’s implementation of a UAS Traffic Management (“UTM”) system must include information to remotely identify and track UAS. Commercial wireless technology can supply this information in a manner that is superior to other solutions;

The FAA must guard against the risk and potential harm to critical infrastructure, including communications facilities, from malicious or negligent UAS operations near such facilities by establishing stand-off distances for UAS operations; and

The FAA should expand payload restrictions to prohibit technologies that could damage or disrupt commercial wireless networks.

I. COMMERCIAL WIRELESS TECHNOLOGY PROVIDES THE FEATURES NECESSARY FOR UAS COMMUNICATIONS, AND THE INDUSTRY IS WORKING WITH THE FCC AND FAA TO ADDRESS UAS INTEGRATION ISSUES.

Drones present transformative opportunities for the U.S. economy, and CTIA and its members are excited to play a key role in these opportunities. CTIA members build, operate and manage commercial wireless networks, manufacture communications components, devices and network equipment, and manufacture UAS and their components. CTIA members play many roles in the UAS ecosystem, including as providers of essential communications networks that support safe and secure UAS operations, as operators of UAS, and as operators of Low Altitude Authorization and Notification Capability (“LAANC”), the precursor to UTM. CTIA is engaged with the FAA, the FCC, the Department of Homeland Security (“DHS”), and the National Aeronautics and Space Administration (“NASA”) on various initiatives addressing UAS integration issues.

Safe UAS operations will depend on use of reliable, secure and protected communications over licensed spectrum. Communications links are needed to satisfy command and control, remote identification and tracking, payload communications and collision avoidance. Because there is not enough aviation-protected spectrum to satisfy these functions, and

---

5. CTIA and its members have participated in the FAA’s UAS Identification and Tracking Aviation Rulemaking Committee (“ARC”); the FCC Technological Advisory Council (“TAC”) working group for Communication Strategies for UAS; the UAS Integration Pilot Programs; the NASA UAS Traffic Management (“UTM”) Pilot Program; and the DHS Critical Infrastructure Partnership Advisory Council (“CIPAC”).
aviation networks for UAS are largely nonexistent today, the FAA has two options—rely on licensed commercial wireless networks, or rely on unlicensed bands. The FAA and FCC should rely on next-generation commercial wireless infrastructure to enable advanced UAS operations, including beyond visual line-of-sight flights and flights over people. The FAA should reject use of unlicensed, unprotected bands for command and control, remote identification and tracking, and collision avoidance—particularly for operations over people and beyond visual line-of-sight—because of reliability, security and interference issues discussed herein.

Validation for using commercial wireless networks has come from many quarters, including the following authorities:

- Qualcomm Study, LTE Unmanned Aircraft Systems, Trial Report;\(^6\)
- International Telecommunications Union (“ITU”) presentation “Potential spectrum and telecom technologies for small UAS,” at the International Civil Aviation Organization’s Drone Enable conference;\(^7\)
- Report of the FAA Drone Advisory Committee (the “DAC Report”);\(^8\)
- Recommendations of the FAA Remote ID and Tracking ARC;\(^10\) and

---


Perhaps the most persuasive source of validation was a presentation given by Nikolai Vassiliev, Chief of the ITU’s Terrestrial Services Department, at Drone Enable. Vassiliev examined the use of unlicensed bands, licensed bands and aviation-protected spectrum for low-altitude UAS. After weighing the pros and cons of each, he recommended commercial wireless technology for low-altitude UAS communications, elevating it above unlicensed spectrum and aviation-protected spectrum. He noted the robust coverage of networked cellular technology, which can enable operations beyond visual line-of-sight, the potential for tracking UAS using wireless technology, the harmonization of commercial wireless bands, which will assist in trans-border operations, and the evolving nature of 5G wireless technology, which will provide even better coverage and dynamic data traffic management in the future.

In contrast, Vassiliev noted that unlicensed bands have no interference protection and, as such, quality of service is not ensured. Unlicensed bands are mainly for recreational UAS usage within line-of-sight and may be not suitable for beyond line-of-sight communications and commercial UAS operations. He also noted that unlicensed bands are not globally-harmonized. With respect to aviation-protected bands, he noted that these bands are exclusive and protected from interference, but limited in capacity and intensively used by existing aviation licensees. Aviation-protected bands are or will be congested, posing an additional challenge for use of this spectrum.

As Vassiliev explained, commercial wireless technology offers many advantages for safe and secure UAS operations, including the following features:

- **Authentication and Security.** The wireless industry has a long history of working to protect its customers, networks, and technology from cyber threats. Commercial
wireless networks are equipped with a variety of security approaches, including authentication technologies that validate and authorize users seeking to access the networks. These technologies help to protect network users—including UAS operators. As discussed below, the communications and aviation sectors are among the sixteen sectors included in the National Institute for Standards & Technology’s (“NIST”) Critical Framework for Cybersecurity (the “NIST Framework”), a longstanding public-private partnership focused on innovation, collaboration, sharing information related to cybersecurity, and responding to evolving cybersecurity threats at the network, device and application layers. The NIST Framework expands on significant industry efforts to collaborate on standards and guidance for cybersecurity protection.

- **Quality of Service.** Commercial wireless technology offers quality of service, with the coverage, performance, and latency required to support safe and secure UAS communications, both within and beyond visual line-of-sight. Commercial wireless networks today match the operational need for UAS, covering 99.7% of the U.S. population in areas where UAS are likely to fly. Given this robust coverage, commercial wireless networks can readily connect with UTM systems to provide reliable and timely situational awareness for the entire UAS ecosystem.

- **Reliability and Redundancy.** The reliability of commercial wireless technology will minimize and mitigate the risk of “lost link” with a ground station or UTM. Cellular networks include overlapping, adjacent cell sites that minimize the possibility of connection issues to the UAS. The FAA DAC Report cited the reliability of networked cellular as a positive factor in supporting beyond visual line-of-sight missions as follows: “Cellular networks in the US are engineered for massive volumes and cover more than 99% of Americans at approx. 300 million people. 56% of US population resides inside mode C veil. High-risk areas are populated and located in proximity to

---


17 See id. at 7 for a discussion of such industry efforts.

transport infrastructure (e.g. airports). Cellular networks are designed to serve these populated areas with high capacity and high reliability/coverage.19

- **Interoperability.** Through 3GPP, the commercial wireless industry has developed technology standards for 4G LTE and 5G. 3GPP standards are global and based on industry consensus, not proprietary to a particular company or entity. UAS and UTM can leverage the global adoption of harmonized wireless industry, providing the consistency and interoperability needed to allow vendors and manufacturers to take advantage of economies of scale, thus ensuring a vibrant, global UAS ecosystem.

Last month, the FCC TAC received a presentation from its 2018 UAS working group. The group found that “3GPP technology”20 satisfies the expected communications requirements for low altitude UAVs.21 The working group recommended that the FCC: (1) consult with involved federal agencies including the FAA as necessary regarding the use of technology for UAVs in the terrestrial mobile bands;22 and (2) re-assess the technical basis for prohibiting use of certain terrestrial mobile frequency bands above ground level.23 The report went on to state that “3GPP Technologies meet all expected communications requirements for supporting low flying UAVs . . . As with all technologies, additional development is required to support UTM or broadcast ID, but similar capabilities already exist within 3GPP technologies.”24 The FCC TAC Working Group identified the following “advantages of 3GPP Technologies”: (1) leverages already deployed network infrastructure; (2) employs mass produced communications hardware; (3) can meet the varying communications requirements of different mission types;

---

19 DAC Report at 67. The DAC Report highlighted additional reasons why using commercial wireless networks is the right approach for safe and secure UAS operations. These include the proximity of many UAS operations to areas with robust LTE coverage, the high reliability and security of commercial wireless technology, the availability of LTE coverage for many UAS operations, including both command-and-control, remote identification and payload, and the low cost of entry for commercial wireless equipment.

20 The 3rd Generation Partnership Project (“3GPP”) is a partnership among seven major standards development organizations from around the world that develops technical specifications for mobile systems. See About 3GPP, https://www.3gpp.org/about-3gpp.


22 The references to “terrestrial mobile bands” and “3GPP Technologies” both refer to commercial wireless technology.

23 See id at slide 25.

24 Id. at slide 51.
and (4) extensive security and privacy support. This important work of the FCC TAC confirms conclusions reached by prior working groups, industry leaders and international regulators concerning use of commercial wireless networks to support UAS communications.

Existing commercial 4G LTE networks already support initial drone deployment, and further optimization after wide-scale testing will expand the capabilities. 5G wireless technology will enable safe and secure UAS deployments on a larger scale and will offer reduced latency, providing UAS with an even faster and more reliable communications platform.

II. THE FAA SHOULD ESTABLISH REASONABLE, RISK-BASED DESIGN REQUIREMENTS FOR UAS SYSTEMS THAT ARE CRITICAL TO SAFETY OF FLIGHT, INCLUDING COMMUNICATIONS LINKS.

The ANPRM asks if the FAA should establish design requirements, including redundancy, for systems critical to safety of flight, particularly for UAS contemplated to fly beyond the remote pilot’s visual line-of-sight and/or over people. The FAA also asks if it should consider public safety and national security in connection with these requirements.

The FAA should collaborate with industry and international standards setting bodies, such as 3GPP, to establish reasonable design requirements for UAS systems that are critical to safety, including communications links. Such requirements should be risk-based, and should take into consideration the safety case of each proposed concept of operations, including the autonomy level of the aircraft. These factors may impact evaluation of communication links for safety-related functions.

3GPP’s global standards for wireless network support of UAS will provide a helpful blueprint for satisfying UAS communications needs. In a recent agenda item, 3GPP released its work

---

25 Id.


27 See ANPRM at 3737.

28 See id.

on requirements and key performance indicators ("KPIs") for UAV applications over wireless networks, including the following: (1) communication latency, reliability KPI, and mobility requirements for UAV applications (e.g. mapping navigation, photographs and videography), including to the UTM or cloud servers; (2) UAV applications (e.g., security surveillance) that require very high uplink data rate for air to ground communication; (3) consideration of potential usages of network slicing; (4) KPIs for command and control between UAV and UAV controller; and (5) discovery between UAV controller and UAV for the UAV applications. This 3GPP study also included a description of UAS communications functions that can be supported over 4G LTE, the functions that will be enhanced when 5G is deployed, and recommended future work for the standardization of UAS enhancements. Additionally, the 3GPP study considered a number of use cases for wireless support of UAS.

The wireless standards-setting process is studying, testing and proving out the viability, safety, and security of using wireless technology to support UAS. This work by 3GPP is playing out in a global forum that can provide interoperable, international standards that will ensure success of the global UAS market.

---

30 “Network slicing” is a type of virtual networking architecture that allows multiple virtual networks to exist atop a shared physical infrastructure. These virtualized “slices” can be dedicated to a particular application, such as UAS, to ensure safe and secure operations.

31 See Abstract to 3GPP TR 22.829 v.1.0.0, Study on Enhancement for Unmanned Aerial Vehicles, SP-190089 (March 2019).

32 Use cases considered in the 3GPP study include the following: video live broadcast, command and control (C2) communication, simultaneous support of UAV data transmission for enhanced mobile broadband users, autonomous UAVs controlled via artificial intelligence, isolated deployment of radio access through UAV, service experience assurance, and UAV swarms in logistics. 3GPP also included a framework for steering UAS KPIs, and for potential new requirements needed to support additional use cases and service level requirements.
III. THE FAA’S IMPLEMENTATION OF UTM SHOULD REQUIRE INCLUSION OF INFORMATION THAT REMOTELY IDENTIFIES AND TRACKS UAS, INFORMATION THAT CAN READILY BE SUPPLIED BY COMMERCIAL WIRELESS TECHNOLOGY.

The ANPRM asks what information a UTM system should share in order to improve safety.\(^{33}\) CTIA agrees that sharing remote identification information must be a priority.\(^{34}\) Remote identification and tracking is an essential UTM building block, and must be communicated in a manner that is reliable, secure, verifiable and authentic.

Although less robust solutions (solutions enabled with unlicensed spectrum, including Bluetooth) may be sufficient for sharing remote identification and tracking information in limited visual-line-of-sight operations, such solutions will not be sufficient when fleets of UAS are operating in more complex environments. UTM will require solutions that can scale rapidly, and reflect the future end state of UAS integration. As the ARC Report pointed out, “[g]iven the built-out nature of cellular networks today, there would be no infrastructure costs for this solution . . .” to UTM needs.\(^{35}\)

Safe and secure operations require the use of licensed spectrum solutions for remote identification and tracking information, ensuring that the information supplied to the UTM and law enforcement is reliable, secure, verifiable, and authenticated. As the ARC Report noted, licensed spectrum is protected from interference, which affords security, reliability, and a higher quality of service than unlicensed spectrum.\(^{36}\) Apart from networked cellular and satellite, most of the solutions studied by the ARC proposed to utilize unlicensed spectrum solutions (over Wi-Fi or Bluetooth), or over-shared spectrum bands such as Automatic Dependent Surveillance-Broadcast, a technology that is unencrypted and overcrowded.

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 are no protocols

---

33 See ANPRM at 3735-36.
34 See ANPRM at 3733 (explaining that the FAA plans to initiate a separate rulemaking on remote identification and “does not intend to promulgate the Operations of Small UAS over People final rule until the remote identification rulemaking is finalized.”).
36 See id. at 17-18.
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 identification and tracking information from being shared with the UTM and law enforcement.\textsuperscript{37} Utilizing unlicensed spectrum and solutions such as Bluetooth will negatively impact the operational performance, reliability, and security of any remote identification and tracking technology. For example, there may be unpredictable instances during which remote identification and tracking information will not be available to a UTM 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, whether the UAS operation is authorized, and whether it must be taken out of the sky. These problems would not occur over protected, commercial wireless networks.

In addition to providing reliable, secure, verifiable, and authentic information, commercial wireless networks can provide UTM systems and law enforcement with valuable data that verifies the accuracy of identification and tracking information transmitted by a UAS. LTE solutions must meet E-911 location requirements, and therefore include tracking data such as current position, speed and direction. Similarly, Global Navigation Satellite Systems ("GNSS") receivers are integrated in most LTE chipsets, improving 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 information with the UTM system through the commercial wireless networks.\textsuperscript{38}

Commercial wireless technology leverages existing unique International Mobile Equipment Identity numbers ("IMEI"), which are used for wireless devices. A UTM system could use IMEI numbers to identify a UAS. Existing SIM technology could also be used for independent verification. SIM card technology can easily identify and independently verify the identity of the UAS owner. SSL/TLS certificates provide an additional layer of identity validation.\textsuperscript{39}

\textsuperscript{37} See id. at 18.

\textsuperscript{38} See id. at 25.

\textsuperscript{39} See id. at 28.
As indicated above, CTIA was a voting member on the FAA’s ARC, which studied remote identification and tracking solutions. Since release of the ARC Report, the foundation for low-altitude traffic management concepts has started to take shape in the form of LAANC. During the early stages of the LAANC rollout, the commercial wireless networks have proven ideal for providing and retrieving data from both UAS operators and FAA users. Policymakers can leverage lessons learned from LAANC and implement them in remote identification and UTM solutions, enhancing the safety and security of UAS operations.

IV. THE FAA SHOULD IMPOSE STAND-OFF DISTANCES FOR UAS OPERATIONS AROUND CRITICAL INFRASTRUCTURE, INCLUDING THE COMMUNICATIONS NETWORKS.

CTIA agrees with the suggestion in the ANPRM that the FAA should establish stand-off distances with respect to people or objects to reduce hazards to public safety and national security. In particular, stand-off distances should be established for UAS operating around critical infrastructure.

As recognized by Presidential Policy Directive – Critical Infrastructure Security and Resilience, the communications sector is one of sixteen critical infrastructure sectors. UAS operators without knowledge of the potential impact of UAS operations to critical communications infrastructure could cause unintended harm or damage to the communications network, or people, objects, or structures near the network. Given the critical role of wireless networks to national security, it is essential to protect these networks from UAS with reasonable stand-off distances. Communications networks provide a lifeline for law enforcement, helping them do their jobs to protect and serve.

The FAA should establish reasonable and appropriate stand-off distances for UAS operations that are not authorized by a communications network owner/ operator, or by the owner/operator of related infrastructure such as towers. It is important that any stand-off requirements are flexible enough to allow mobile network operators and tower owners to use

---

40 See ANPRM at 3734.

UAS technology to maintain and repair wireless infrastructure. The FAA could incorporate education regarding stand-off distances around critical infrastructure into the standard Part 107 remote pilot training documents and the Part 107 certificate test.

V. THE FAA SHOULD EXPAND PAYLOAD RESTRICTIONS TO INCLUDE TECHNOLOGIES THAT KNOWINGLY DAMAGE OR DISRUPT COMMERCIAL WIRELESS COMMUNICATIONS NETWORKS.

As DHS has recognized, communications networks provide a mission-critical lifeline for America’s first responders. Illegal jamming of communications systems – including jamming of Global Positioning Systems, radio and wireless systems – poses a threat to law enforcement and public safety across the country. Jammers may interfere with public safety communications and can leave responders without vital communications and critical situational awareness.42 As the FAA considers safe and secure UAS operations, it should consider reinforcing that any UAS payload that is intended to damage, disrupt or interfere with the wireless communications network, or unlawfully wiretap information on the wireless networks, including personally identifiable, proprietary, or other sensitive information from the wireless network, is prohibited.43

VI. CONCLUSION.

CTIA looks forward to continuing its collaboration with industry, the FAA and the FCC to address UAS integration policy issues and the essential role to be played by commercial wireless technology to supply safe and secure communications links for UAS.

In support of safe and secure operations, CTIA urges the FAA to work with industry and CTIA to establish reasonable, risk-based design requirements for using commercial communications links to support UAS. The important work of 3GPP can help address the safety case for UAS


43 See 47 U.S.C. §333 (“No person shall willfully or maliciously interfere with or cause interference to any radio communications of any station licensed or authorized by or under [the Communications] Act or operated by the United States Government.”); 18 U.S.C. § 2511(b) (prohibiting the use of “any electronic, mechanical, or other device” to intercept communications when “such device transmits communications by radio, or interferes with the transmission of such communication.”).
communication links. The FAA should include remote identification and tracking information in the initial implementation of any UTM system, and it should rely on existing secure commercial wireless technology to supply these capabilities. The FAA should consider stand-off distances for critical infrastructure in order to guard against risk and potential harm, including to communications facilities, from malicious or negligent UAS operations near such facilities. Finally, the FAA should expand payload restrictions to prohibit technologies that could damage or disrupt commercial wireless networks.

Today’s commercial wireless technology offers the authentication and security, quality of service, reliability, redundancy, and interoperability with global standards that the UAS industry needs. CTIA and its members remain committed to working with the FAA to foster the safe and secure integration of UAS in the national airspace system, and stand ready to work with the FAA as it resolves the important questions raised in the ANPRM.

Respectfully submitted,

By: /s/ Jackie McCarthy
    Jackie McCarthy
    Assistant Vice President, Regulatory Affairs