ctia™
Everything Wireless

December 3, 2018

BY ELECTRONIC SUBMISSION

National Highway Traffic Safety Administration
1200 New Jersey Ave., S.E.
W12-140
Washington, DC 20590
ATTN: Finch Fulton, Deputy Assistant Secretary for Transportation Policy

Re: *Preparing for the Future of Transportation: Automated Vehicles 3.0 (Docket No. DOT-OST-2018-019)*

Dear Deputy Assistant Secretary Fulton,

CTIA[1] respectfully submits these comments in response to the Department of Transportation's ("Department") Notice of Request for Comments on Automated Vehicles 3.0 ("AV 3.0"). CTIA applauds the Department's efforts to establish a multi-modal federal policy that paves the way for automated vehicle ("AV") research, testing and deployment.

The wireless industry, including wireless carriers, device manufacturers and application developers, has helped create significant and widely beneficial changes in society, allowing for increased connectivity, productivity and the spread of information. 5G wireless networks will pave the way for a host of transportation innovations that will increase safety, efficiency and access to personal mobility. Self-driving cars could save almost 22,000 lives and $447 billion

[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, 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.

each year.[2] Wireless connectivity will enable these benefits by allowing vehicles and road infrastructure to share data and apply its insights. Vehicles can relay information about road conditions and congestion, and to nearby infrastructure like traffic signals. As AV 3.0 acknowledges, both Cellular Vehicle-to-Everything ("C-V2X") and Dedicated Short-Range Communications ("DSRC") will provide connectivity for AVs, road users and transportation infrastructure. As AV 3.0 suggests, cybersecurity of automated and connected vehicles requires a cooperative approach that includes both industry and policymakers.

I. 5G WIRELESS NETWORKS WILL PROVIDE SPEED, CAPACITY AND RELIABILITY FOR AUTOMOTIVE APPLICATIONS.

All U.S. national wireless carriers have announced 5G network deployments, some of which began this year. 5G networks will be 100 times faster than today's 4G LTE networks, providing significant potential for automotive applications. Additionally, 5G networks will support 100 times more devices than 4G networks. This improvement will address the vast increase in connected transportation infrastructure, not only from vehicles, but from traffic management and parking applications, and from road users' vast increase in mobile data usage. There are now more wireless connections in the U.S. than there are Americans, and over the past two years, U.S. mobile data usage has more than doubled. There are now 126 million data-only devices on U.S. wireless networks, representing a 147% increase in two years. Finally, 5G networks will be five times more responsive than 4G networks. This significant reduction in latency has powerful consequences for AVs. By way of example, it would take 4.6 feet for a car with 4G connectivity to apply its brakes while traveling 50 mph; it would take just 1 inch for a car with 5G connectivity to do so.[3]

[2] *See Wireless Connectivity Fuels Industry Growth and Innovation in Energy, Health, Public Safety and Transportation*, Deloitte at 3 (Jan. 2017) (the "Deloitte 5G Report"), *available at:* https://www.ctia.org/docs/default-source/default-document-library/deloitte_20170119.pdf .

[3] *See Huawei, 5G Vision: 100 Billion Connections, 1 ms Latency and 10 Gbps Throughput, available at:* http://www.huawei.com/minisite/5g/en/defining-5g.html .

II. CONNECTIVITY OF VEHICLES TO EACH OTHER, TO NEARBY ROAD USERS, AND TO TRANSPORTATION INFRASTRUCTURE WILL EXPAND THE POTENTIAL FOR AV BENEFITS.

Since NHTSA released its previous AV policy, stakeholders have tested various versions of auto connectivity. As AV 3.0 acknowledges[4], the wireless industry has advanced C-V2X standards that cover a variety of use cases. The Third Generation Partnership Program ("3GPP") issued a C-V2X standard in its Release 14 in 2017. Building on existing 4G standards, C-V2X provide for both direct and network-based communications.[5] Additionally, automakers have announced DSRC deployment commitments and work with wireless carriers to extend, target and authenticate basic safety messages.[6] CTIA applauds the Department's technology-neutral approach to vehicle connectivity, and agrees with the Department that all transportation stakeholders should "continue developing technologies that leverage…5.9 GHz spectrum for transportation safety benefits…."[7] Our members are committed to providing robust communications that leverage autonomy for societal benefits.

III. WORKING WITH ITS AUTOMOTIVE PARTNERS, THE WIRELESS INDUSTRY STANDS READY TO SECURE AUTOMOTIVE AND COMPONENT CONNECTIVITY.

America's wireless industry, including carriers, device manufacturers, operating system developers and applications providers, apply a comprehensive, evolving approach to ensuring data and networks are secure. This includes standards-

[4] *See AV 3.0* at 14.

[5] *See 3GPP Release 14, available at*: http://www.3gpp.org/news-events/3gpp-news/1798-v2x_r14

[6] *See AV 3.0* at 16. *See also, General Motors Ex Parte, ET Docket No. 13-49* (July 13, 2018), *available at:* https://ecfsapi.fcc.gov/file/107132653414467/GM%20Ex%20Parte%20Letter%20ET%20Docket%20No.%2013-49.pdf (outlining General Motors' automated assistance features and connectivity deployment timelines); *AT&T, Delphi and Ford Debut V2X Advanced Vehicle Communications* (Jan. 4, 2017), *available at:* https://about.att.com/story/att_debuts_v2x_advanced_vehicle_communications.html (describing how one carrier enhanced vehicle communications in a proof of concept with Ford and Delphi).

[7] *AV 3.0* at 16.

based encryption, authentication features, redundancies, and back-up power options and access controls.[8] Recently, CTIA introduced an Internet of Things ("IoT") Cybersecurity Certification Program, which began accepting devices including transportation components for certification in October.[9] Building on CTIA's 25-year history of developing and managing certification programs, CTIA developed the IoT Cybersecurity Certification Program with collaboration from wireless operators, technology companies, security experts, and test labs. This program establishes baselines for IoT device security and privacy. It builds upon recommendations from the National Institute of Standards and Technology, global standards and wireless industry certifications to support a variety of use cases and device sophistication.[10] Additionally, CTIA and its members participate in efforts to share information about cybersecurity threats and responses in the connected vehicle ecosystem, through Information Sharing and Analysis Centers ("ISACs"), both within the Communications ISAC and with the Automotive ISAC. As AV 3.0[11] recognizes, an effort to collaborate across industry and government is required to address evolving cybersecurity threats in the expanding ecosystem of mobility services.

IV. CONCLUSION

As the steward of our nation's transportation infrastructure, the Department has a unique opportunity to ensure continued U.S. leadership in automotive innovation focused on AVs' benefits for safety, efficiency and inclusion. AV 3.0 establishes the framework for these goals, and the wireless industry will continue to provide the

[8] *See Protecting America's Wireless Networks* at 3 (April 2017), *available at*: https://www.ctia.org/docs/default-source/default-document-library/protecting-americas-wireless-networks.pdf .

[9] *See CTIA IoT Cybersecurity Certification Program Begins Accepting Devices for Testing* (Oct. 30, 2018), *available at*: https://www.ctia.org/news/ctia-iot-cybersecurity-certification-program-begins-accepting-devices-for-testing .

[10] For more information on the CTIA IoT Cybersecurity Certification Program, including procedures and a Test Report Template, *see IoT Cybersecurity Certification Program Management Document Version 1.0* (Oct. 2018), *available at*: https://api.ctia.org/wp-content/uploads/2018/10/ctia_IoT_cybersecurity_pmd_ver-1_0.pdf .

[11] *See AV 3.0* at 17.

network, device and component resources critical to achieving the full promise of automated vehicles.

Respectfully submitted,

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

CTIA
1400 Sixteenth Street NW, Suite 600
Washington, DC 20036
(202) 785-0081

CC: Nathaniel Beuse, National Highway Traffic Safety Administration Associate Administrator for Vehicle Safety Research