ctia™
Everything Wireless

April 12, 2017

BY ELECTRONIC SUBMISSION
(www.regulations.gov)

Ms. Rebecca Yoon
Office of Chief Counsel
U.S. Department of Transportation
National Highway Traffic Safety Administration
1200 New Jersey Avenue SE
Washington, DC 20590

Re: *Notice of Proposed Rulemaking on NHTSA Federal Motor Vehicle Safety Standards; V2V Communications, Docket No. NHTSA-2016-0126*

Dear Ms. Yoon:

CTIA[1] respectfully submits these comments on the National Highway Traffic Safety Administration's ("NHTSA" or the "Agency") Notice of Proposed Rulemaking seeking comment on a new Federal Motor Vehicle Safety Standard (FMVSS), No. 150, to "mandate vehicle-to-vehicle [("V2V")] communications for new light vehicles and to standardize the message and format of V2V transmissions."[2]

I. INTRODUCTION AND OVERVIEW

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. Its members are actively involved in the connected vehicle ecosystem and the

[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.

[2] *Notice of Proposed Rulemaking; Federal Motor Vehicle Safety Standards; V2V Communications, Docket No. NHTSA-2016-*0126, 82 Fed. Reg. 3854 (Jan. 12, 2017)(the "NPRM").

development and implementation of emerging automotive technologies, providing connectivity technologies that make driving safer and more efficient.

We agree with NHTSA that connected vehicle technologies, along with smart transportation infrastructure, will increase road safety and efficiency. We respectfully disagree, however, with NHTSA's characterization of the reliability, security and privacy protections offered by commercial wireless networks as they relate to V2V deployments. In reality, wireless carriers have invested heavily to ensure that reliability, security, and privacy are built into all layers of the mobile broadband ecosystem, an investment that can benefit V2V communications.

Since 2010, wireless providers have spent $150 billion in network improvements to deliver 4G LTE mobile broadband nationwide to U.S. consumers, making the U.S. the world leader in 4G LTE deployment.[3] According to one recent study by Accenture, wireless operators will invest a projected $275 billion over the next decade to deploy real-time, faster, and higher capacity 5G technology that will unlock smart communities, promote better management of vehicle traffic, and support wireless-operated self-driving cars that could save up to 21,700 lives.[4]

This level of investment is directed in large part to ensuring that wireless networks can support V2V and other communications reliably, safely and securely. Indeed, wireless carriers, device manufacturers and app providers ensure that privacy and security are central elements of wireless service. These industry stakeholders are working to evolve security methods addressing a broad variety of Internet of Things ("IoT") use cases, including connected transportation.

The industry also strongly supports a performance-based authentication proposal as an alternative to a mandated authentication solution.[5] Rather than establishing an entirely new approach to authentication, a performance-based approach will allow the use of

[3] *See The Next Generation of Wireless: 5G Leadership in the U.S.* CTIA at 3 (Feb. 9, 2016) ("5G White Paper"), *available at:* http://www.ctia.org/docs/default-source/default-document-library/5g_white-paper_web2.pdf.

[4] *See How 5G Can Help Municipalities Become Vibrant Smart Cities,* Accenture Strategy at 1-2, 8 (Jan. 12, 2017) ("Accenture Smart Cities Report"), *available at:* http://www.ctia.org/industry-data/press-releases-details/press-releases/accenture-economic-societal-impact-investing-5g-infrastructure; *Wireless Connectivity Fuels Industry Growth and Innovation in Energy, Health, Public Safety, and Transportation*, Deloitte at 11(Jan. 2017) *available at:* http://www.ctia.org/docs/default-source/default-document-library/deloitte_20170119.pdf.

[5] *See NHTSA Vehicle-to-Vehicle Security Credential Management System Request for Information*, 79 Fed. Reg. 61, 927 (Oct. 15, 2014) (the "SCMS Request for Information").

commercial authentication solutions already in the marketplace, and will increase scalability and security in a Security Credential Management System ("SCMS").

II. THE DEPLOYMENT OF 5G WIRELESS NETWORKS WILL SIGNIFICANTLY INCREASE NETWORK CAPACITY AND RELIABILITY OF ALREADY-ROBUST EXISTING 4G LTE NETWORKS.

CTIA recognizes the significant automotive safety and other societal benefits that V2V communications in new light vehicles will bring to the U.S. automobile market. CTIA supports NHTSA's premise in this rulemaking, as it has in prior comments, that connected vehicle technologies, combined with smart transportation infrastructure, will make U.S. roadways safer and make ground transportation more efficient. However, CTIA respectfully disagrees with NHTSA's assessment of the reliability of cellular networks for vehicle-based communications. These conclusions misapprehend the current state of wireless network capacity and reliability. Wireless carriers have already deployed innovative and densified 4G LTE networks. These networks now reach 99.7 percent Americans, and 95.9 percent of all Americans can choose from three or more 4G LTE providers.[6] Additionally, 4G LTE latency rates are low: "roughly 10 milliseconds over the air."[7] 5G latency rates will be even lower, "targeted to be five to ten times lower."[8]

In other words, 5G speeds will result in a "10x increase over existing 4G network speeds."[9] This means that, operating on a 5G network, a self-driving car travelling at roughly 60 mph will move *just over 1 inch* (as opposed to 4.6 feet under the same conditions operating on a 4G LTE network) to execute a braking command once an obstacle is detected.[10] 5G can also address vehicle efficiency. The Accenture Smart Cities Report details how vehicle convoys using 5G to communicate road conditions could reduce drag by 20-60%, resulting in a 25% fuel savings.[11] Thus, 5G will enable vehicle safety and efficiency capabilities and, "with its device density and real-time capabilities, has the potential to advance V2V features."[12]

[6] *Implementation of Section 6002(b) of the Omnibus Reconciliation Act of 1993*, Nineteenth Report, 31 FCC Rcd 10534, ¶ 39, Chart III.A.2 (2016).

[7] 5G White Paper at 10.

[8] *Id.*

[9] CTIA Comments on NTIA's paper, *Fostering the Advancement of the Internet of Things* (the "NTIA Green Paper")(March 13, 2017) at 2, *available at:* https://www.ntia.doc.gov/files/ntia/publications/ctia_comments_ntia_iot_green_paper_3.13.17.pdf

[10] *See* 5G White Paper at 10-11.

[11] *See* Accenture Smart Cities Report at 8.

[12] *Id.*

5G is not aspirational. In fact, the FCC itself has recently declared that deployment of 5G wireless network by as early as 2020 is a "national priority." Since 5G infrastructure, particularly small cell sites and fiber connectivity, will be built close to roadways, it will be readily available to support the full range of V2V and vehicle-to-infrastructure ("V2I") communications at low latency, especially in high-density areas with great demands for data throughput from large numbers of users.[13]

Authorizing 5G for V2V communications would also be consistent with trends internationally, in which foreign carriers are upgrading their networks by making significant spectrum investments now to support 5G, IoT and V2I communications in densely populated, smart communities.[14] This global investment in 5G will enhance the capabilities and scope of wireless technology applications generally –including by improving speed, reliability and capacity essential to grow the Internet of Things and V2V-- but also as a driver of economic growth in building smart communities.[15] With 5G's "device density and real-time capabilities" supporting smart transportation and the Internet of Things, there can be an important role for 5G to support V2V communications.[16] . At the same time, manufacturers are already incorporating 5G technologies into their connected vehicle platforms.[17]

[13] Still, the evolution to 5G networks, and indeed all V2X deployments that require communications to/from fixed locations, depend on timely and efficient access to wireless infrastructure, particularly for "small cell" sites that are placed on existing structures like light and utility poles. Comments of CTIA, *Streamlining Deployment of Small Cell Infrastructure by Improving Wireless Facilities Siting Policies,* FCC WT Docket No. 16-42, at 9-10. (March 8, 2017).

[14] Korean carriers have announced 5G trials at the Winter Olympics in 2018, and Japanese carriers plan to demonstrate 5G at the 2020 Summer Olympics in Tokyo, capitalizing on improved 5G speed, especially in densely populated areas, greater connectivity of devices, and new applications and services that 5G offers. The European Union has committed 700 million Euros to 5G research and development. 5G White Paper at 2. Singapore's recent General Spectrum Auction, concluded on April 4, 2017, raised $1.14 billion Singapore dollars, the highest amount ever paid for spectrum in Singapore, for 175 MHz of spectrum in the 700 MHz, 900 MHz and 2.5 GHz frequency bands. Singtel Consumer Singapore's CEO, whose company was the biggest winning bidder, states that "[t]his investment puts us in a strong position to support the growth of IoT (Internet of Things) and 5G initiatives in the future." *"Expect faster mobile surfing speeds after airwave auction,"* The Straits Times at A1, A8 (April 5, 2017)¸*available at:* http://www.straitstimes.com/singapore/expect-faster-mobile-surfing-speeds-after-airwave-auction

[15] *"The Next Generation of Wireless: 5G Leadership in the U.S."*, Thomas K. Sawanobori, SVP and Chief Technology Officer, CTIA at 13 (Feb. 9, 2016)(5G White Paper), *available at:* http://www.ctia.org/docs/default-source/default-document-library/5g_white-paper_web2.pdf.

[16] *Id.* at 11.

[17] For example, it was recently reported that one foreign OEM is planning to equip its electric vehicles with 5G mobile connectivity and cellular vehicle-to-everything communication standards as it prepares to offer full autonomous driving functionality. The OEM reportedly decided against

III. PRIVACY AND SECURITY ARE INTEGRAL TO WIRELESS NETWORKS AND DEVICES IN THE EMERGING CONNECTED VEHICLE ECOSYSTEM.

The NPRM's claim that commercial wireless networks would introduce security risks ignores the level of cybersecurity protections embedded in wireless networks and the singular, coordinated focus of the wireless industry on cybersecurity issues. Indeed, based on industry reports, the U.S. enjoys one of the lowest mobile malware infection rates in the world—in 2012, mobile infection rates were less than 2% in the U.S. compared to more than 40% in China and Russia.[18]

This is not happenstance. The wireless industry has invested hundreds of millions of dollars to enhance the security of its networks, software, hardware and devices. Carriers, applications providers, operating system and platform providers address cybersecurity holistically, and have engaged in unified, focused efforts to deliver "effective cybersecurity and ensuring the entire interdependent mobile ecosystem delivers sustained, high-value security for all users."[19] As CTIA recently observed:

> [T]he wireless communications industry -- although fiercely competitive — has always been united in the core belief that security is absolutely critical. Developing and deploying advanced cybersecurity solutions to manage risk both maintains consumer confidence, and is the best defense to stay ahead of cybercriminals and hackers. It is this simple reality that drives the industry to spend hundreds of millions of dollars every year on cybersecurity measures — a level of investment that will continue to grow over the years.[20]

DSRC, which requires the deployment of its own dedicated infrastructure, in contrast to commercial mobile networks. According to a company official, "All future solutions for individual mobility rely on the ability to handle large amounts of data inside and outside the car. . . 5G is the key enabling technology to accommodate big data, enhance the user experience and transform the transportation system as a whole." *See, e.g., VW EVs will debut 5G connectivity service* (Automotive News Europe, Jan. 23, 2017), *available at:* http://europe.autonews.com/article/20170123/ANE/170119950/vw-evs-will-debut-5g-connectivity-services.

[18] *See* Lookout Mobile Threats Made to Measure: The Specialization of Mobile Threats Around the World, Lookout Mobile (Feb. 20, 2014), *available at:* https://www.lookout.com/static/ee_images/Mobile_Threats_Made_to_Measure_Lookout_Report_2013.pdf .

[19] CTIA, "Today's Mobile Cybersecurity – Protected, Secured and Unified" at 3, *available at:* http://files.ctia.org/pdf/CTIA_TodaysMobileCybersecurity.pdf .

[20] *Id.* at 24.

Wireless networks benefit from the security architectures of a variety of standards organizations, including the 3rd Generation Partnership Project ("3GPP"), the Alliance for Telecommunications Industry Solutions, the Institute of Electrical and Electronics Engineers ("IEEE") and the Internet Engineering Task Force. The relevant works of these organizations include 3GPP standards for over-the-air encryption and IEEE 802.11i, implemented as WPA2, and FIPS-14-2 for encryption, authentication and key management.[21] Through CTIA's Cybersecurity Working Group and other industry touchpoints, the entire mobile industry ecosystem engages in ongoing research and dialogue according to the NIST Cybersecurity Framework to address cybersecurity threats collectively and with impacted industries.[22]

The communications sector, of which the wireless industry is a part, was one of the first to establish an industry Information Sharing & Assurance Center ("ISAC") through the Communications Sector Coordinating Council ("CSCC"), established in 2005. The major automobile manufacturers, led by the Alliance of Automotive Manufacturers ("Auto Alliance") and the Association of Global Automakers ("Global Automakers") and with NHTSA's encouragement, developed and launched the automotive industry ISAC (the "Auto ISAC") in September 2015 to enable and promote the exchange of significant threat information, and countermeasures, in real time.[23] The CSCC and Auto ISAC collaborate on cross-sector threats and responses.

As recently reported by the Washington Post, a new wave of suppliers of "connected car" components are now recognizing the importance and value of information-sharing about vulnerabilities. At least 25 such suppliers have recently joined the Auto ISAC, furnishing additional data into its collaborative approach to cybersecurity system.[24] Because specifications for the automotive industry are created years ahead of actual vehicle production and vehicles are becoming more and more complex, fixes can require massive and expensive recalls. That reality creates ample incentives for information-sharing and cooperation through the Auto ISAC among automotive

[21] CTIA, "Today's Mobile Cybersecurity – Blueprint for the Future" at 8, *available at:* http://www.ctia.org/industry-data/press-releases-details/press-releases/u-s-wireless-industry-maps-its-blueprint-for-tomorrow-s-mobile-cybersecurity)

[22] *Id.* at 5

[23] Vehicle Electronics Report at 18; *see also Cybersecurity -- An industry-wide effort to identify emerging threats and potential adversaries*, *available at:* http://www.autoalliance.org/auto-issues/cybersecurity ("Auto Alliance Cybersecurity Site").

[24] "Behind Booz Allen's effort to get carmakers to work together against hackers", Washington Post, Capital Business (March 19, 2017), *available at:* https://www.washingtonpost.com/business/capitalbusiness/behind-booz-allens-effort-to-get-carmakers-to-work-together-against-hackers/2017/03/19/a4e9a146-0b4f-11e7-b77c-0047d15a24e0_story.html?utm_term=.1cf7b779e595

manufacturers and suppliers by sharing threat information, including information received from U.S. government agencies.[25]

These security initiatives complement cross-industry efforts to ensure consumer privacy. In 2014, participating members of the Auto Alliance and Global Automakers established Consumer Privacy Protection Principles (the "Privacy Principles") regarding data retrieved from vehicles.[26] These principles include notice and choice, transparency, respect for context, and data de-identification and security to protect Covered Information against unauthorized access or use. These elements of the Privacy Principles are consistent with the wireless industry's own principles for consumer privacy protection, as exemplified by the CTIA Best Practices and Guidelines for Location Based Services.[27] The Privacy Principles apply to new vehicles manufactured no later than the 2017 model year, and for Vehicle Technologies and Services subscriptions begun or renewed after January 2, 2016.[28]

In an effort to assist the auto industry with the development of its Privacy Principles, CTIA's Privacy Working Group shared the wireless industry's own efforts to advance and protect consumer privacy. In addition, CTIA is in discussions with the Alliance and Global Automakers regarding how the Privacy Principles compare with the wireless industry's own privacy protections (e.g., CTIA's Location-Based Services).

Wireless networks provide necessary data security and privacy protections necessary to play a key role in V2V communications. As in other sectors of the economy, NHTSA should rely on industry collaboration and information sharing to address cybersecurity and privacy concerns, in contrast to prescriptive government mandates.

IV. A TECHNOLOGY NEUTRAL APPROACH TO V2V MESSAGE AUTHENTICATION WILL PROMOTE THE SCALABILITY AND INTEROPERABILITY OF A SECURE CONNECTED VEHICLE COMMUNICATIONS SYSTEM.

The NPRM discusses two alternate proposals for standardizing and authenticating basic safety messages between vehicles, regardless of the V2V communication technology "potentially used." First, it proposes an SCMS via public key infrastructure, including a

[25] *See Id.*

[26] *See*, November 12, 2014 joint letter of Auto Alliance and Global Automakers to FTC Chairwoman Edith Ramirez re: "Consumer Privacy Protection Principles for Vehicle Technologies and Services," *available at:* http://www.autoalliance.org/auto-issues/automotive-privacy/letter-to-the-ftc.

[27] *See* CTIA, Best Practices and Guidelines for Location-Based Services, *available at:* *http*://www.ctia.org/policy-initiatives/voluntary-guidelines/best-practices-and-guidelines-for-location-based-services.

[28] *See* Auto Alliance Privacy Principles for Vehicle Technologies and Services, *available at:* http://www.autoalliance.org/auto-issues/automotive-privacy/principles.

date range for message validity and a digital signal from a certificate authority.[29] As an alternative approach, the NPRM proposes a "performance-based approach" that does not mandate a specific authentication solution or architecture, allowing vehicle manufacturers to validate the contents of a basic safety message to confirm that it originated from "a single valid V2V device" and the message was not modified in transmission.[30] This technology-neutral alternate proposal is an important way to establish a scalable, effective authentication solution that leverages existing authentication services and can reflect rapid evolution of authentication technologies.

As CTIA commented in the SCMS Request for Information,[31] the security functions necessary for a successful SCMS, and for V2V security generally, are similar to those necessary for the larger, growing machine-to-machine ("M2M") communications ecosystem that supports the Internet of Things. Creating an authentication infrastructure leveraging existing commercial wireless services would reduce costs, expedite deployment, and further interoperability. It would also ensure that V2V security systems are compatible going forward with the larger M2M ecosystem. Such "future-proofing" of V2V security functions is critical to the deployment of connected vehicle technologies that extend beyond V2V systems, allowing for scalable V2M systems. Beyond traditional telematics, V2M systems and technologies incorporate vehicles into the IoT ecosystem to provide convenience, reliability, scale and security.

V2V authentication systems should leverage this experience. The security standards eventually adopted for the V2V SCMS should be compatible with similar global standards to ensure that automobile manufacturers and their connectivity partners can use the same SCMS protocols across the globe, as well as across sectors—for example, V2M communication in connection with home automation. Other groups have set and are developing additional, relevant standards that already provide the framework for SCMS administration for wireless systems.[32]

As a result of these collective efforts, the wireless industry has developed robust authentication and security protocols that scale to provide nationwide coverage for devices and networks. While certificates and Resource Public Key Infrastructure ("RPKI") frameworks are commonly used security standards, our V2V framework should use existing commercial wireless network authentication and security protocols to

[29] NPRM at 3857.

[30] *Id.*

[31] See CTIA to SCMS Request for Information (Dec. 15, 2014).

[32] For example, (3GPP, http://www.3gpp.org/), which originally set global specification for 3G and has expanded its work to 4G and 5G, already provides the framework for SCMS administration for wireless systems. In addition, other industry stakeholders, such as ATIS, IEEE and IETF address standardization and interoperability issues that are applicable in the V2V SCMS context.

complement the proposed use of Dedicated Short-Range Communications, as well as other wireless transmission technologies that may be incorporated into V2V. As such, CTIA suggests that NHTSA not dictate a particular authentication solution.

Adopting a technology-agnostic approach to V2V authentication and encryption as part of the SCMS would ensure secure communications and global applicability, as well as avoid locking the V2V SCMS into potentially dated technology. Regardless, CTIA supports NHTSA's consideration of privately-managed SCMS and authentication architectures. The wireless industry stands ready to work with its automotive partners to ensure the delivery of reliable and secure V2V communications, increasing traffic safety and efficiency on our nation's roads and highways.

Respectfully submitted,

CTIA

By: */s/ Jackie McCarthy*
Jackie McCarthy
Assistant Vice President, Regulatory Affairs
1400 16th Street, NW, Suite 600
Washington, D.C. 20036
202-736-3200