Before the
BUREAU OF INDUSTRY AND SECURITY
Washington, D.C. 20230

In the Matter of	)	
	)	
Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles	)	Docket No. 240919-0245

COMMENTS OF THE
TELECOMMUNICATIONS INDUSTRY ASSOCIATION

I. INTRODUCTION

The Telecommunications Industry Association ("TIA") appreciates the opportunity to provide input regarding the Bureau of Industry and Security Office of Information and Communications Technology and Services' ("OICTS") Notice of Proposed Rulemaking on Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles. TIA is a U.S.-based trade association that represents more than 400 trusted, global manufacturers of telecommunications equipment and services. TIA members design, produce, market, and manage the information communications technology ("ICT") equipment and services that connect Americans to high-speed broadband networks, whether they are in their cars, their homes, or anywhere in between. Given the growing security vulnerabilities in this space, we are keenly aware of how supply chains – particularly those intersecting China and Russia – impact security; and we support the use of equipment from trusted vendors on national security grounds. For this reason, we provided input in successive rounds of comment regarding the underlying rules supporting OICTS' mission, urging the agency to be focused and targeted in

its rulemaking to be as effective as possible and avoid adopting rules or regulations that would inject unnecessary regulatory uncertainty into commercial transactions.[1]

II. The NPRM is Targeted, Phased, and Focuses on Vehicle Connectivity

We believe the agency has successfully hit that balance in this rulemaking. By focusing on specific types of technologies – in this case Vehicle Connectivity Systems ("VCS") and Automated Driving System ("ADS") software – that pose national security risks and creating a multi-year timeframe for companies to come into compliance, OICTS is taking reasonable steps to accommodate the needs of automotive original equipment manufacturers ("OEMs") as they transition to more secure technologies. TIA believes that Vehicle Connectivity Systems specifically are important given their ability to facilitate data exfiltration and download potentially damaging over-the-air updates. To the extent that OICTS applies similar scrutiny to other connectivity applications in the future, we would urge the Office to engage with OEMs in those industries in advance to determine what the minimum, reasonable length of time for those industries to come into compliance might be.

III. Cybersecurity Can Be Enhanced by Use of Telecommunications Security Standards

Regarding Cybersecurity Best Practices, TIA recommends that OICTS also consider how standards developed for use in adjacent industries – such as the telecommunications sector – may help BIS address risks in the supply chain. These standards are relevant to the discussion around connected vehicles given that VCS technologies essentially enable vehicle telecommunications. One such relevant standard is TIA's SCS 9001, a process-based standard that is intended to

[1] TIA Comments in the Matter of Securing the Information and Communications Technology and Services Supply Chain, Docket No. 210113-0009 (March 22, 2021) https://tiaonline.org/wp-content/uploads/2021/03/TIA-Comments-on-ICTS-SCS-IFR.pdf.

address risks in the telecommunications supply chain, and which includes specific mechanisms to address concerns regarding supply chain security and transparency.[2] SCS 9001 includes measures promoting the use of Software Bills of Materials, and it also has a section requiring transparency around business practices and the extent to which vendors can operate independently of governments in the jurisdiction in which they are headquartered.

IV. Regulating Auto OEMS is the Most Administrable Pathway

TIA supports OICTS focusing on regulating the automotive OEMs as the most logical and administrable approach. Automotive OEMs are the enterprises who ultimately integrate, test, and market products to consumers; and while they may not have perfect visibility into downstream suppliers, they are best positioned to mandate additional transparency from these suppliers as a part of their purchasing process. Additionally, the OEMs themselves are fewer in number and can be regulated in a way that the countless Tier 1 and Tier 2 component suppliers, many of which are headquartered in other countries, cannot.

V. Vendors on the FCC's Covered Entity List are Active in the VCS Market

Regarding the landscape of market participants in the VCS market, it is worth noting that there are several companies that have been found by the FCC to pose unacceptable risks to U.S. national security who are active participants in the connected vehicles market. These include the following:

[2] Mike Regan, TIA's SCS 9001 Cyber and Supply Chain Security Standard – Update, NIST (January 24, 2023), https://csrc.nist.gov/csrc/media/Presentations/2023/tia-quest-forum-scs-9001-update/images-media/Jan-24-2023-ssca-regan.pdf.

FCC Covered Entity	*OEM Partner*
Huawei	Changan[3], BYD[4], Audi[5], BAIC,[6] Volvo,[7] CFMoto[8]
ZTE	Chery[9], SAIC[10]
Datang	Ford[11]

TIA has long held that companies on the FCC's entity list pose a significant risk to U.S. national security and have no place in U.S. networks.[12] Action by OICTS to block transactions relating to these vendors in the context of connected vehicles would further enhance action by BIS, the FCC, and other agencies to protect U.S. national security.

---

[3] *Huawei to move smart car operations to new joint company with Changan,* Reuters (Nov. 26, 2023) https://www.reuters.com/business/autos-transportation/chinas-huawei-changan-auto-form-joint-auto-systems-venture-2023-11-26/

[4] China's BYD to Use Huawei's Advanced Autonomous Driving System in Off-Road EVs, Reuters (Aug. 27, 2024), https://www.reuters.com/business/autos-transportation/chinas-byd-use-huaweis-advanced-autonomous-driving-system-off-road-evs-2024-08-27/.

[5] Manufacturing Industry Digital Transformation with Huawei ICT, Huawei, https://e.huawei.com/th/ict-insights/global/ict_insights/201810190908/manufacturing/201901191459 (last visited Oct. 28, 2024).

[6] *China's Huawei, BAIC Motor Launch First Jointly Developed EV*, Reuters (Aug. 6, 2024), https://www.reuters.com/business/autos-transportation/chinas-huawei-baic-motor-launch-first-jointly-developed-ev-2024-08-06/.

[7] *Volvo's First Car with Huawei's HMS for Car, IoT Automotive News*, https://iot-automotive.news/volvos-first-car-with-huaweis-hms-for-car/ (last visited Oct. 28, 2024).

[8] 春风动力亮相 2022 华为开发者大会，携手打造智能骑行新生态 (*CFMOTO debuts at the 2022 Huawei Developer Conference, working together to create a new smart motorcycle ecosystem*), Sohu (June 12, 2022), https://www.sohu.com/a/604852851_121119177.

[9] *ZTE, Chery to Form 5G Vehicle Joint Venture*, Yicai Global (May 30, 2023), https://www.yicaiglobal.com/news/zte-chery-to-form-5g-vehicle-joint-venture.

[10] SAIC Motor forms tie-up with ZTE for 'software-defined' vehicles, China Association of Automobile Manufacturers, http://en.caam.org.cn/Index/show/catid/2/id/1785.html (last visited Oct. 28, 2024).

[11] *Ford and Datang Trial C-V2X Connected Car Technology in Shanghai to Support Global Connectivity Initiative* https://media.lincoln.com/content/fordmedia/fap/cn/en/news/2018/03/29/Ford_and_Datang_Trial_C-V2X_Connected_Car_Technology_in_Shanghai_to_Support_Global_Connectivity_Initiative.html

[12] See TIA Comments in the matter of Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs , WC Docket No. 18-89, (June 1, 2018). Available at: https://tiaonline.org/wp-content/uploads/2018/06/TIA-Comments-to-FCC-on-USF-Security-6-1-18.pdf

VI. Conclusion

As stated previously, TIA represents the trusted manufacturers and suppliers of telecommunications equipment. Insecure telecommunications equipment has no place in U.S. networks – particularly in high-risk applications like motor vehicles – and this rule will have an impact in reducing supply chain threats from countries of concern. TIA looks forward to partnering with OICTS as it pursues further investigations going forward. Please let us know as you have any questions.

Signed:

Melissa Newman
Senior Vice President, Government Affairs

Colin Andrews
Senior Director, Global Policy

TELECOMMUNICATIONS INDUSTRY ASSOCIATION
1310 N. Courthouse Road
Suite 890
Arlington, VA 22201
(703) 907-7700

Filed: October 28, 2024