

May 2, 2016

The Honorable Mark R. Rosekind, Ph. D.
Administrator
National Highway Traffic Safety Administration
1200 New Jersey Ave SE
Washington, DC 20590

RE: [Docket No. NHTSA-2016-0040] Request for Comment on NHTSA Enforcement Guidance Bulletin 2016-02: Safety-Related Defects and Emerging Automotive Technologies

COMMENTS OF THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION

I. INTRODUCTION

The Telecommunications Industry Association (“TIA”) hereby submits comments to the National Highway Traffic Safety Administration (“NHTSA”) in the above-referenced docket on proposed enforcement guidance for safety defects involving emerging automotive technologies.¹ TIA recognizes that as the automotive technology landscape evolves there is a need for NHTSA’s safety guidance and policies to address new developments to ensure continued driver safety and security. We appreciate the opportunity to provide comment on this issue.

TIA represents hundreds of information and communication technology (“ICT”) manufacturer, vendor, and supplier companies and organizations in standards, government affairs, and market intelligence. Many TIA member companies are developing ICT equipment and devices that are part of the emerging electronic automotive technology ecosystem. In the comments that follow, TIA encourages NHTSA to limit its enforcement

¹ Request for Public Comment on NHTSA Enforcement Guidance Bulletin 2016-02: Safety-Related Defects and Emerging Automotive Technologies, 81 Fed. Reg. 18,935 (Apr. 1, 2016) (“RFC”).

guidance to automotive electronic technology built into the vehicle consistent with its statutory authority. TIA also expresses its strong concerns with NHTSA's proposal to regulate software in the vehicle, which would have negative implications for innovation in the automotive technology arena.

II. TIA ENCOURAGES NHTSA TO LIMIT THE SCOPE OF ITS GUIDANCE TO THE APPLICATION FOR EMERGING AUTOMOTIVE TECHNOLOGY SPECIFICALLY WITHIN ITS STATUTORY AUTHORITY.

TIA fully supports NHTSA's safety-of-life directive to ensure "the safety of the driving public against unreasonable risks of harm that may occur because of the design, construction, or performance of a motor vehicle or motor vehicle equipment."² Thus, we understand that as automotive technology and equipment advances, NHTSA must ensure that its policies and guidance consider, and are responsive to, new vehicle systems that may have safety implications. Nonetheless, we are concerned that NHTSA's proposed guidance would potentially bring a broad range of technologies under the agency's enforcement authority beyond what is intended by the governing statute.

In the proposed enforcement guidance, NHTSA seems to interpret its authority under the Safety Act³ in an overly broad manner that would allow it to enforce regulations on a wide swath of new and emerging automotive technologies including electronic systems that may have tangential, rather than primary, safety uses in the vehicle. The RFC states "[w]ith respect to new and emerging technologies, NHTSA considers automated vehicle technologies, systems, and equipment to be motor vehicle equipment, whether they are offered to the public as part of a new motor vehicle (original equipment) or as an after-

² RFC, 81 Fed. Reg. at 18,935.

³ See National Traffic and Motor Vehicle Safety Act, as amended, 49 U.S.C. 30101 *et seq.* ("Safety Act").

market replacement of or improvement to original equipment.”⁴ Later in the guidance, NHTSA discusses electronic systems like “hardware, software, sensors, global positioning systems (GPS) and vehicle-to-vehicle safety communications systems” as being major aspects of emerging automotive technology.⁵ TIA and its members are concerned by the breadth and scope of devices that NHTSA’s guidance seems to attempt to bring within the scope of its authority.

NHTSA’s guidance takes an overly broad view of the agency’s authority, which is fundamentally about addressing *vehicle safety* matters.⁶ The guidance is unclear about distinguishing the treatment of and authority to regulate devices and related software that are built into the vehicle or for later vehicle installation from those brought in by the driver. This differentiation is necessary as NHTSA’s authority related to motor vehicle equipment does not extend to items such as smartphones or wearables that may have vehicle-related applications. There are numerous types of devices and systems that could technically fit within the umbrella of emerging technology and may be used in the vehicle without vehicle or driver safety being its intended purpose.

The ICT industry believes that neither mobile devices nor third party software fall within NHTSA’s jurisdiction. Therefore, we encourage NHTSA to clarify its guidance by making sure to restrict the application to emerging automotive technologies that are within its statutory authority to address motor vehicle or motor vehicle equipment safety.

⁴ RFC, 81 Fed. Reg. at 18,937.

⁵ *Id.* at 18,938.

⁶ See Safety Act, 49 U.S.C. § 30101 (explaining that the purpose of the statute is to prescribe safety standards for motor vehicles and motor vehicle equipment).

III. NHTSA SHOULD NOT USE THIS GUIDANCE AS A MEANS TO REGULATE SOFTWARE IN VEHICLES THAT ARE NOT A PART OF THE CRITICAL SAFETY SYSTEM.

Throughout the RFC, NHTSA asserts its belief that software is within its enforcement authority. In the guidance, NHTSA explicitly says it considers “software and after-market software updates to be motor vehicle equipment.”⁷ Additionally, the agency explains that software that allows a device to connect to the motor vehicle could in some circumstances be considered motor vehicle equipment.⁸ This statutory interpretation by NHTSA is overly broad and would be a significant change to the current understanding of what is considered motor vehicle equipment.

TIA is concerned by this approach and encourages NHTSA not to adopt policies that involve software unrelated to vehicle systems or vehicle components which control a motor vehicle’s critical safety systems. It would be an overreach to attempt to use this RFC as an avenue to broadly regulate all software which may be used “in or on” a vehicle. As TIA has said previous comments to NHTSA,⁹ efforts to extensively regulate software may be a disincentive to market innovation and R&D investments in the automotive electronics space. NHTSA expresses its interest in facilitating the development and deployment of emerging technologies but its proposed guidance may have the opposite effect by stifling innovation and hampering market growth. We ask that NHTSA consider the negative affect

⁷ *Id.* at 18,937.

⁸ *See id.* (explaining that NHTSA interprets its authority to potentially cover “software that enables devices not located in or on the motor vehicle”).

⁹ *See* TIA Comment, Docket No. NHTSA-2014-0108, filed Dec. 8, 2014, *available at* https://www.tiaonline.org/sites/default/files/pages/Automotive_Electronic_Systems_Security_Comment_Final.pdf.

on the broader Internet of Things ecosystem that may result from it applying a rigid, sector-specific approach to any software that may enable users to connect to a car or mobile equipment but may have other uses unrelated to vehicle operations.

To the extent that NHTSA determines that it has jurisdiction over software “installed *in or on* a motor vehicle”¹⁰, TIA believes this should be limited to those applications which directly affect and control a motor vehicle’s critical safety systems (i.e., systems encompassing critical control functions such as braking, steering, or acceleration). For “software located outside the motor vehicle (i.e., portable devices with vehicle-related software applications)”, TIA believes that NHTSA should clearly exclude software that is self-installed by a vehicle owner or an authorized third party from the definition of “motor vehicle equipment”, unless such applications are marketed or described in a manner that indicates the provider’s clear intent to affect and control a motor vehicle’s critical safety systems.

Furthermore, NHTSA’s authority to require safety-related defect or noncompliance reporting applies *only* to “manufacturer[s] of a motor vehicle or replacement equipment,” not to original equipment suppliers (*See* 49 U.S.C. § 30118). Thus, for critical safety software applications built into the vehicle, NHTSA should require that all software vulnerability and safety impact assessments be coordinated with the vehicle’s original equipment manufacturer (“OEM”) before reporting to NHTSA. Only the vehicle manufacturer has a total picture of the vehicle’s architecture and whether a particular software vulnerability poses “an unreasonable risk to safety” that would constitute a safety-related defect. For this reason, reporting of safety defects due to software

¹⁰ *See* 81 Fed. Reg. at 18,937 (emphasis added).

vulnerabilities should be solely the obligation of the vehicle OEM, and not encompass the vehicle manufacturer's equipment or software suppliers.

IV. NHTSA RECOMMENDATIONS SHOULD CONSIDER THE GLOBAL ECOSYSTEM TO AVOID COUNTRY- AND SECTOR-SPECIFIC APPROACHES THAT MAY INHIBIT INNOVATION.

TIA urges NHTSA to consider the larger ecosystem for emerging, connected technologies and not adopt an approach that places sector-specific obligations on technologies and systems that may have at most tangential vehicle-safety uses. Emerging electronic systems hold great potential for uses in a variety of industry sectors and the broader global marketplace.

TIA and its members encourage NHTSA to harmonize its vehicle safety efforts with international standards for security of the Internet of Things and Cyber Physical Systems. Without a harmonized policy and standard approach, NHTSA risks creating an environment that inhibits technological growth and places U.S. manufacturers at a disadvantage. As NHTSA continues the important task of ensuring driver safety, we encourage the agency to take heed of the broader landscape and not operate in a vacuum on safety and security matters.

V. CONCLUSION

TIA and its members appreciate the opportunity to provide input on the proposed safety guidance and urge NHTSA to appropriately limit the scope of its policies to technologies specifically within its motor vehicle safety authority.

Respectfully submitted,

By: /s/ James Reid

James Reid
Senior Vice President, Government Affairs

Avonne Bell
Senior Manager, Government Affairs

TELECOMMUNICATIONS INDUSTRY ASSOCIATION
1320 North Courthouse Rd
Suite 200
Arlington, VA 22201
United States
1 (703) 907-7000