

December 8, 2014

The Honorable David J. Friedman
Deputy Administrator
National Highway Traffic Safety Administration
1200 New Jersey Ave SE
Washington, DC 20590

RE: [Docket No. NHTSA-2014-0108] Request for Comment on Automotive Electronic Control Systems Safety and Security

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, towards fulfilling the statutorily mandated examination of the need for safety standards with respect to electronic systems in passenger motor vehicles. TIA recognizes the sensitive position NHTSA is in as it tries to balance the need for safety and security standards with respect to vehicle electronic systems with affording manufacturers flexibility in designing systems, and appreciates the opportunity to provide comment on this Request for Comment (“RFC”).¹ To this point, TIA urges NHTSA to allow industry-led, open, voluntary, consensus-driven processes to develop global standards.

TIA represents approximately 500 information and communication technology (“ICT”) manufacturer, vendor, and supplier companies and organizations in standards, government affairs, and market intelligence. TIA is accredited by the American National Standards Institute (“ANSI”) and has developed over two thousand ICT standards, through the input and

¹ Request for Comment on Automotive Electronic Control Systems Safety and Security, 79 Fed. Reg. 60574 (Oct. 7, 2014) (“RFC”).

engagement of member companies. As a standards-development organization, TIA recognizes the importance of technical standards particularly in areas of safety and security. Additionally, many TIA member companies are developing ICT equipment and devices that are part of the electronic systems installed in motor vehicles. NHTSA should encourage industry to collaborate in open participation global standardization efforts to develop technological best practices and standards.

In the comments that follow, TIA discusses its strong concerns with NHTSA's seeming intention to regulate software in the vehicle, which would be an unnecessary overreach that would stifle innovation in the US vehicle technology marketplace. In addition, TIA believes that NHTSA's focus in the RFC on a narrow set of security and safety design standards is similarly inappropriate; this is not a proper role for government. Finally, while we urge NHTSA not to take any cybersecurity risk management actions, if it nevertheless acts, it must ensure any regulation is technology-neutral and aligns with existing cybersecurity efforts, such as those by the National Institute of Standards and Technology ("NIST") rather than pursuing separate automotive industry-specific requirements.

Given the ICT industry's significant experience with developing voluntary, open, consensus-driven global standards and best practices, including in cybersecurity, NHTSA can learn much from ICT stakeholders as it works to identify practices that will continue to allow for innovation while keeping American drivers safe. With the ICT industry's rapidly increasing and essential role in the automotive and intelligent transportation sector, we look forward to working with NHTSA as it continues its investigation.

II. NHTSA Should Not Use This Examination as a Means to Try to Regulate Software in Vehicles.

In the RFC, NHTSA states that electronic system anomalies “including those related to software programming . . . may not leave physical evidence, and hence are difficult to investigate without a record of data from the electronic systems.”² And, in multiple places throughout the RFC, NHTSA identifies software systems as a component of vehicle electronic systems that potentially affect safety, thereby presumably signaling an intention to regulate software in vehicles,³ rather than allowing industry and the competitive marketplace to determine best software solutions.

TIA strongly urges NHTSA not to pursue any regulatory action with respect to software in vehicle systems or components. Indeed, NHTSA would be overreaching to attempt to use this RFC as an avenue to regulate the software running on electronic components and/or systems in vehicles. Moreover, such action would unnecessarily stifle innovation and hamper marketplace competition, ultimately causing the U.S. to lag behind its global competitors. Government attempts to regulate ICT such as software and hardware increasingly cannot keep pace with the rapidly advancing technology ecosystem. Attempts to impose regulation on software in automotive electronic systems or components would de-incentivize market innovation and research and development investments, thereby having a negative effect on safety by causing market stagnation.

² RFC, 79 Fed. Reg. at 60, 576.

³ See *e.g.*, *id.* at 60, 575 , 60, 577.

III. NHTSA Should Encourage Industry to Determine Technical Design Standards Through an Open, Voluntary, Consensus-Based Process.

NHTSA, in the RFC, states that “[f]unctional safety assurance of modern automobiles requires a thorough understanding of electronic control systems’ design” and that to achieve this purpose the agency is conducting studies that apply specific design standards like ISO 26262 and System Theoretic Process Analysis. TIA believes that NHTSA should not impose any of these technical design standards or attempt to apply them to vehicle electronic systems. NHTSA’s focus on this narrow set of security design standards is inappropriate and would have a negative effect on market growth and innovation in the U.S. vehicle electronics technology industry. Rather, NHTSA should encourage industry to adopt global technical design standards through an open, voluntary, consensus-based process.

Should NHTSA, nonetheless, deem it necessary to act and *be able to legally justify its action*, performance-based guidelines for automakers are preferable. This would allow market participants to define standards and a method for achieving compliance with those standards by establishing benchmarks and allowing flexibility in selecting appropriate standards.

IV. Any NHTSA Cybersecurity Risk Management Efforts Should Align with Existing Public-Private Cybersecurity Activities, Like NIST’s Cybersecurity Framework, Rather Than Establishing Automotive-Specific Requirements.

In the RFC, in accordance with section 31402 of MAP-21,⁴ NHTSA seeks comment on the security needs to prevent unauthorized access to electronic components, encompassing cybersecurity in the context of road vehicles.⁵ The RFC also states that the introduction of new, emerging technologies in vehicle electronics has led to increasing system complexity and

⁴ Moving Ahead for Progress in the 21st Century Act, § 31402 (“MAP-21”).

⁵ See RFC, 79 Fed. Reg. at 60, 580.

challenges concerning “the ability of these systems to remain free of unauthorized access or malicious attacks.”⁶ TIA is cognizant of the potential challenges that the intersection of ICT and vehicles present, and we urge NHTSA to not promote any technology(ies) without first resolving security concerns to the greatest extent feasible.

Indeed, it is imperative that NHTSA include the ICT industry as a valued stakeholder in these discussions. This would allow NHTSA to leverage the ICT industry’s significant experience and expertise with cybersecurity matters, and ensure alignment with, and leveraging of, existing public-private cybersecurity risk management efforts.

TIA strongly encourages NHTSA to align its cybersecurity risk management efforts with ongoing research and guideline development being conducted through public-private efforts. Cybersecurity is an area that requires uniform, global consideration and thus, industry-specific standards will only hinder technology development. In the RFC, NHTSA identified NIST’s Cybersecurity Framework⁷ (“Framework”) as one potential cybersecurity safeguarding principle “that can potentially be examined and adapted for use in the automotive industry.” TIA believes adoption of the Framework may be a viable option as the ICT industry is working collaboratively with NIST on this effort. Additionally, if NHTSA decides to apply the Framework to the automotive industry, we urge the agency to include language affirming the Framework’s *voluntary* nature and reiterating President Obama’s commitment that the Framework is not intended to function as a regulation.⁸

⁶ See *id.* at 60, 576.

⁷ NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0 (Feb. 12, 2014), *available at* <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf>.

⁸ Executive Order No. 13636, 78 Fed. Reg. 11739 (2013) (calling for a “voluntary program to support the adoption of the Cybersecurity Framework”).

In addition to the Framework, NIST is currently leading an effort to define and shape research and standards with respect to cyberphysical systems,⁹ which includes a working group that focuses on cybersecurity. NHTSA should utilize industry's expertise and work in collaboration here with NIST, rather than trying to develop automotive-specific rules. Indeed, effective approaches to cybersecurity risk require uniformity, flexibility, and global applicability.

In the RFC, NHTSA also seeks comment on “the potential for voluntary safety process standards to help address challenges introduced by expanding use of electronics in automotive applications.”¹⁰ The ICT industry strongly supports an industry-led, *voluntary* approach to cybersecurity in all sectors (including automotive), rather than regulations that would stagnate the marketplace and hinder the ability and incentive of industry to innovate; regulation will fail to contemplate or keep pace with an ever-more complex threat environment. This model has been adopted with much success in the technology space, as industry has the incentives and expertise necessary to protect their systems from cyber-attacks.

V. Other Issues

TIA urges NHTSA to take into consideration the larger global perspective as it examines the safety and security implications of automotive electronic systems. The ICT industry as well as the auto industry operates in a global marketplace. Thus, to the extent NHTSA must adopt standards, it should do so in an international context to ensure standards are globally harmonized and U.S. manufacturers are not placed at a disadvantage in the marketplace. NHTSA should not operate in a US vacuum on issues of safety and security.

⁹ “Cyberphysical system” refers to interacting networks of physical and computational components including those in vehicles.

¹⁰ RFC, 79 Fed. Reg. at 60,582.

VI. Conclusion

TIA and its member companies appreciate the opportunity to provide comments in this RFC and urge NHTSA to support voluntary, industry-led, open standards processes with global harmonization.

Respectfully submitted,

TELECOMMUNICATIONS INDUSTRY ASSOCIATION

By: /s/ Danielle Coffey

Danielle Coffey
Vice President & General Counsel, Government
Affairs

Avonne Bell
Senior Manager, Government Affairs

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

December 8, 2014