Motor & Equipment Manufacturers Association

Comments to

U.S. Department of Transportation
National Highway Traffic Safety Administration

RE: Request for Comments; Cybersecurity Best Practices for the Safety of Modern Vehicles; Draft 2020 Update

Docket No. NHTSA-2020-0087

March 15, 2021

The Motor & Equipment Manufacturers Association (MEMA) submits the following comments pursuant to the National Highway Traffic Safety Administration's (NHTSA) Request for Comments on the 2020 draft update of the document titled *Cybersecurity Best Practices for the Safety of Modern Vehicles* (Best Practices or BPs).[1]

Introduction

MEMA represents more than 1,000 companies that manufacture original equipment (OE) and aftermarket motor vehicle parts, components, systems, and materials for use in passenger vehicles and commercial trucks.[2] Vehicle suppliers provide 907,000 direct jobs, making it the nation's largest manufacturing sector with jobs in all 50 states and contributing 2.5 percent of U.S. GDP.[3]

Our members lead the way in developing advanced technologies that enable safer, smarter, and more efficient vehicles. Vehicle suppliers conceive, design, and manufacture the OE components and systems that make up two-thirds of the value in every vehicle. Additionally, vehicle suppliers also manufacture aftermarket parts and materials for the maintenance and repair of the 290 million vehicles on the road. Suppliers are critical in the ongoing refinement and implementation of advanced safety technologies, such as advanced driver assistance systems (ADAS) and automated driving systems (ADS), which are the building block systems necessary to enable highly automated vehicles (AVs) to reach their full potential.

MEMA welcomes the opportunity to provide input to NHTSA's first update of the Cybersecurity Best Practices document. MEMA supports the voluntary guidelines approach to address foundational cybersecurity protocols in addition to other industry recommended standards, other industry best practices, and other key procedures and methods developed by organizations (such as the AutoISAC, SAE International, and the International Organization for Standardization). In fact, MEMA was one of the first strategic partners of the Auto-ISAC and continues to encourage vehicle suppliers to join and be part of that very important industry community. The draft 2020 Best Practices reflects NHTSA's research and information gathering as well as the steps the automotive and commercial vehicle industry has taken over the years. MEMA commends the agency's overall

[1] 86 Fed. Reg. at 2481

[2] MEMA represents its member companies through its four divisions: Automotive Aftermarket Suppliers Association (AASA); Heavy Duty Manufacturers Association (HDMA); MERA - The Association for Sustainable Manufacturing; and, Original Equipment Suppliers Association (OESA).

[3] In addition, direct, indirect, and induced vehicle supplier employment accounts for over 4.8 million U.S. jobs. U.S. Labor & Economic Impact of Vehicle Supplier Industry, MEMA and IHS Markit. February 2021.

support for the key industry standards, like the ISO/SAE 21434 "Road Vehicles –Cybersecurity Engineering" and a range of best practices documents from the Auto-ISAC.

MEMA Comments on NHTSA's 2020 Draft Cybersecurity Best Practices

In response to specific sections and titles noted in the guidelines, MEMA offers the following comments and observations for NHTSA's consideration. Additionally, MEMA's aftermarket segment division – the Automotive Aftermarket Suppliers Association (AASA) – will submit separate comments regarding the automotive aftermarket sections of the 2020 draft BPs.

1. Purpose of This Document

First, MEMA reiterates our support of a voluntary guidelines approach. NHTSA recognizes that different manufacturers will apply this guidance as it is appropriate "to their unique systems" and applications. On that point, MEMA would like to note that a vehicle supplier may create and develop a component or system independent of their vehicle manufacturer customer or they may create and develop a component or system collaboratively either with their customer and/or with another supplier. Similarly, a supplier may provide one module in a large network of modules but may not have information on either the network architecture or other modules that may or may not be on that network. Whichever the scenario, vehicle suppliers do consider these factors during product development with a risk-based approach, as recommended in the NTHSA BPs.

Second, MEMA offers a general remark about the frequency of review and updates of the NHTSA BPs. When the first BPs were published in 2016, the agency noted its intention for this to be a living document that would be periodically updated. However, there was a four-year interval between updates of the agency's BPs. Considering how quickly cybersecurity and related issues can evolve, MEMA encourages NHTSA to consider more frequent updates of their voluntary best practices.

2. Scope

MEMA appreciates that NHTSA includes a wide scope of entities encompassed by the BPs by including "all motor vehicles" as defined by 49 U.S.C. § 30102(a)(7). There is indeed broad applicability, and the agency recognizes that implementation will vary. However, there are some aspects of the overall BPs that cannot be a "one-size fits all" for all sectors. NHTSA almost exclusively uses the term "automotive industry" throughout the draft BPs but does not address any unique considerations for the heavy-duty commercial vehicle industry in its scope. MEMA raised this issue in our 2016 comments as well.

The AutoISAC recognizes the importance of including the commercial vehicle industry segment and, soon after its formation, opened membership to manufacturers of commercial vehicles and equipment. Certainly, a majority of the draft 2020 BPs can be applied to both the light, passenger vehicles and heavy, commercial vehicles segments. However, the commercial vehicle segment has a more closed-loop ecosystem of customer-supplier-fleets/owners-service relationship that is much different than the consumer passenger market. Moreover, many commercial vehicles are heavily customized (e.g., fleet specifications, service applications, etc.), which may add to cybersecurity complexity. When finalizing the next edition of the BPs, NHTSA must recognize these differences in its scope. NHTSA should provide a more tailored focus or strategy relative to the commercial vehicle sector based on the increased risk associated with such vehicles due to several factors, including, but not limited to, product lifetime, service applications, physical size, and standardization. Therefore, MEMA recommends that NHTSA include references to other standards developing activities that are specific to commercial vehicles and equipment in its Cybersecurity

Best Practices, for example, the SAE J1939 "Network Security" issued by its Truck Bus Control and Communications Network Committee.

Due to the ever-increasing connectivity of vehicle architectures, information technology protections are also important and should be included in the scope. As such, MEMA recommends the scope include information technology systems in addition to equipment and software. Industry standards similarly address the priority of these interrelated systems (e.g., ISO/SAE 21434).

4. General Cybersecurity Best Practices

MEMA supports the agency's overarching recommendations on a layered approach to vehicle cybersecurity that is rooted in the National Institute of Standards and Technology (NIST) Cybersecurity Framework. NHTSA must remain at the forefront of vehicle-related cybersecurity matters and interface with NIST to apply elements of that framework where it is practicable.

As an additional general comment, MEMA urges NHTSA to seek alignment with international norms (e.g., UN Regulation No. 155[4]) in two key areas – documentation/testing and implementation. As MEMA has noted in other comments, alignment to existing protocols and standards, whenever practicable, is critical for both industry and government to reduce duplication of resources to achieve the same objective. MEMA would like to emphasize those incompatible implementations, which may bring about different sets of components or software for vehicles in different regions, may impact security due to the increased complexity.

4.1 Leadership Priority on Product Cybersecurity

MEMA supports the recommendations in this section. We do recommend, however, that NHTSA add language that encourages vehicle manufacturers to directly submit to NHTSA their product security roadmaps, with confidential business information protections as appropriate.

4.2.1 Process

Regarding [G.3] product development process, MEMA suggests NHTSA add a footnote reference to ISO/IEC/IEEE 15288 "Systems and software engineering – System life cycle processes."

4.2.4 Unnecessary Risk Removal

Existing cybersecurity standards address risk. To enhance the BPs, MEMA recommends that NHTSA include a reference to the ISO/SAE 21434 "Road vehicles – Cybersecurity engineering" as well as how to manage risks (e.g., "avoiding," "reducing," "sharing (transferring)," or "retaining (accepting)").

4.2.6 Inventory and Management of Software Assets on Vehicles

Regarding [G.10], while MEMA can appreciate why NHTSA would make this recommendation, MEMA does have concerns with some potential negative consequences. A vehicle supplier's software bill of materials (SBOM), in most cases, belongs solely to the supplier. Although this can be a joint area of responsibility between the supplier and the vehicle manufacturer, it is essential that the supplier maintains control over its software catalog. MEMA is concerned that this guideline infers that a supplier would have to

[4] UN Regulation No. 155, Cyber security and cyber security management system

relinquish its entire software catalog over to their vehicle manufacturer customer(s). Not only is this a significant risk to a supplier's intellectual property, but also could potentially expose multiple vehicle manufacturers.

5. Education

MEMA supports NHTSA's encouragement of the vehicle industry to enhance skills development and education in the field of cybersecurity. Motor vehicle parts suppliers rely on a strong technical workforce innovating and manufacturing the transformative vehicle technologies needed to enhance future mobility. For the supplier industry to continue to innovate safely and securely, companies rely on workers with the right skills and training necessary for product and systems development. MEMA applauds endeavors like the agency's recent announcement about its project with the AutoISAC to develop a new training curriculum for vehicle cybersecurity professionals.

6. Aftermarket/User Owned Devices

Broadly, MEMA agrees with NHTSA's recommendations in this section and supports the [G.41] statement in the draft BPs. As noted in the introduction, our aftermarket division AASA is submitting separate comments sections of the draft BPs that are specific to the automotive aftermarket and serviceability matters.

Conclusion

MEMA continues to support NHTSA's efforts in the realm of vehicle cybersecurity in the proposed next edition of its Cybersecurity Best Practices. Voluntary guidance, using a risk-based approach, is appropriate especially as vehicle technologies and cybersecurity protections continue to evolve. MEMA encourages NHTSA to find ways to address sector-specific elements for commercial vehicles and equipment in its document. MEMA appreciates NHTSA's consideration of our comments and suggestions. Please contact MEMA Chief Technology Officer Brian Daugherty or Vice President of Regulatory Affairs Leigh Merino with any questions or request more information.