Automotive Aftermarket Suppliers 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 Automotive Aftermarket Suppliers Association (AASA), a division of 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]

Background

AASA represents aftermarket suppliers that provide vehicle parts, components, tools, and technologies for use in the light vehicle aftermarket industry. Aftermarket suppliers ensure that quality parts and service choices are available to the drivers of the 279 million passenger vehicles on our nation's roads. Suppliers are the foundation of a vibrant aftermarket industry, which employs more than 4 million Americans across manufacturers, motor vehicle repair facilities, and distribution and service providers. Furthermore, the independent aftermarket currently services over 70 percent of motor vehicle repairs in the United States. The aftermarket industry is committed to servicing vehicles in a safe and cybersecure environment. Access to vehicle telematics data is, and will continue to be, essential to making many of those repairs.

AASA welcomes the opportunity to provide input to the National Highway Traffic Safety Administration's (NHTSA) first update of the Cybersecurity Best Practices document. The original Best Practices document, published in 2016, showed a commitment to ensuring that that authorized alternative third-party repair services remain an option for consumers.[2] The aftermarket is a trusted partner in the service, repair, and maintenance of consumers' vehicles, including protection of vehicles against cybersecurity threats. Access to vehicle data is necessary to preserve consumer choice and prevent excessive automotive repair costs.

In the wake of the voters' approval of the Massachusetts Question 1 Right to Repair ballot initiative, we understand that the agency is receiving questions from Congress and other entities about the potential implications of that referendum. Some parties are erroneously stating that vehicle safety and cybersecurity are at risk by expanding access to appropriate repair and maintenance data transmitted wirelessly by motor vehicles.

AASA member companies, many of which are also original equipment suppliers of safety-critical components and systems, are committed to maintaining the safe and secure operation of vehicles.

---

[1] 86 Fed. Reg. at 2481

[2] National Highway Traffic Safety Administration. (2016, October). Cybersecurity best practices for modern vehicles. (Report No. DOT HS 812 333).

The aftermarket has a long history in safely servicing Americans' cars and trucks while protecting vehicle cybersecurity and owner privacy. Our industry has repaired electronics, software, and safety systems – effectively – for decades. We have dealt with private, secure data, such as key codes giving access to vehicles, effectively and cooperatively with automakers, for decades. We have well-established training and certification systems. As many technology leaders among our members can attest to, the technology solutions are available to ensure both cybersecurity and vehicle repair.

NHTSA must support aftermarket maintenance and serviceability of vehicle systems and component technologies. This will foster innovation and safety while providing the vehicle owner and the owner's designee the ability to access data generated, recorded, stored, and collected by the vehicle.

In response to specific sections noted in the guidelines, AASA offers the following comments and observations for NHTSA's consideration. Additionally, AASA's parent organization, MEMA, will submit broader comments addressing other sections of the 2020 draft Best Practices.

AASA appreciates NHTSA's consideration of these comments. For more information, please contact Brian Daugherty, MEMA chief technology officer at 248-430-5966 or bdaugherty@mema.org or Catherine Boland, MEMA vice president of legislative affairs at 202-312-9241 or cboland@mema.org.

Section 5. Education

AASA agrees that continuing education for the current and future workforces is critical to protect the cybersecurity of vehicles. For a vehicle to operate safely, it must be maintained and regularly serviced, and repairs must be completed in a timely fashion. The automotive repair industry, including service and repair technicians, have unique needs in education and credentialing. AASA urges NHTSA to strengthen the education requirements and recognize that aftermarket professionals have access to the appropriate and necessary training in order to maintain vehicles in a cybersecure fashion. This should be done in coordination with appropriate licensing schemes.

Section 6. Aftermarket/User Owned Devices

AASA agrees that third party devices when connected to the vehicle should be considered as possible vulnerabilities, and any devices themselves must be properly secured.

Section 7. Serviceability

AASA encourages NHTSA to clarify that the independent aftermarket must be able to access the same tools, equipment, service information, and training to be able to service vehicles as effectively as OEM dealers in a cybersecure fashion. This can be accomplished by requiring that any third-party repair service professionals authorized by the vehicle owner have access to vehicle data if the professional is properly credentialed and licensed. Additionally, these professionals must adhere to and observe the latest vehicle cybersecurity best practices.

As part of ensuring serviceability for vehicles, open access for properly credentialed and licensed repair professionals is critical. At the same time, this open access must be granted in a uniform process with cybersecure protections. AASA welcomes the opportunity to collaborate with

NHTSA and other stakeholders in the development of a self-governance structure that would allow open access to real-time bidirectional repair, maintenance, and service data.

Section 8. Technical Vehicle Cybersecurity Best Practices

Access rights to a vehicle owner or the owner's designee is critical to allow consumers to continue to have the ability to choose where to seek vehicle repair. To ensure that this is conducted in a cybersecure fashion, AASA encourages the inclusion of a best practice to create a self-governance structure for the aftermarket. Such a self-governance structure would create policies that would enable legitimate repair professionals to have access rights to vehicle data and be governed by polices that grant open access.