March 15, 2021

Dr. Cem Hatipoglu
Associate Administrator for Vehicle Safety Research
National Highway Traffic Safety Administration
1200 New Jersey Avenue SE
West Building, Ground Floor, Room W12-140
Washington, DC 20590-0001

Via: https://www.regulations.gov

Re: Docket No. NHTSA-2020-0087: Request for Comment on Cybersecurity Best Practices for the Safety of Modern Vehicles

Dear Associate Administrator Hatipoglu:

The Specialty Equipment Market Association (SEMA) appreciates this opportunity to provide comments on the Agency's updated draft best practices document, *Cybersecurity Best Practices for the Safety of Modern Vehicles*. SEMA is supportive of cybersecurity best practices for vehicles that maintain the legal right of vehicle owners to access the data, hardware and software in order to repair or modify their vehicle.

SEMA represents the $46 billion specialty automotive industry comprised of 7,500 mostly small businesses nationwide, that manufacture, retail, and distribute custom parts and accessories for motor vehicles. The industry produces performance, restoration, and enhancement parts for use on passenger cars and trucks, collector vehicles, racecars, and off-highway vehicles. Products range from wheels and tires to engines, exhaust systems, lighting equipment, suspensions, truck caps, leather seating, mobile electronics, and more.

SEMA appreciates NHTSA's outreach to the automotive community for feedback as the agency updates its cybersecurity best practices. The document is an important guide as stakeholders grapple with the challenge of addressing cybersecurity vulnerabilities.

The use of software in vehicles has expanded and become increasingly more complex in recent years. Computer chips are now as vital to the automobile as tires and wheels. Further, the explosion of data communications is not limited to the vehicle itself. Vehicles are now connecting with other vehicles (v2v) and the surrounding infrastructure (v2i), and all types of cybersecurity exposures need to be confronted.

SEMA's comments focus on Sections 6 and 7, Aftermarket/User Owned Devices and Serviceability. As aftermarket products become more digital and interface with motor vehicle software, it is necessary to reinforce consumer rights to lawfully gain or authorize access to their vehicle for purposes of repair or modification. NHTSA recognizes that this could present a unique cybersecurity challenge. It is not a new challenge. In fact, availability to onboard

diagnostic (OBD) system service information provides an analogy in which the law sought to protect the consumer's right to have the vehicle independently serviced and repaired and to make vehicle modifications.

The issue of access is not limited to electronic products. Cybersecurity controls on the motor vehicle must still permit the installation of aftermarket parts, both replacement and specialty equipment, from oil filters and brakes to suspension kits and more.

It is of vital importance that cybersecurity concerns not infringe upon vehicle owners' and independent shops' right to repair or modify vehicles. For example, in Massachusetts, voters overwhelmingly supported the "right to repair" ballot initiative in 2020 that updated the 2012 law to ensure consumers maintain the right to access their vehicle's wireless digital data. Top information security experts wrote in a letter to the editor in the Boston Herald that this initiative "in no way increases the risk of identity theft, cyber stalking or vehicle hacking."[1] The concerns of safety and cybersecurity surrounding motor vehicles and motor vehicle equipment are legitimate, but there is a way to balance this with the freedoms of vehicle owners to legally modify and repair their vehicles how they see fit.

NHTSA acknowledges the issue SEMA is raising in these comments within the Section 7 Serviceability section when it states, "NHTSA recognizes the balance between third party serviceability and cybersecurity is not necessarily easy to achieve. However, cybersecurity should not become a reason to justify limiting serviceability. Similarly, serviceability should not limit strong cybersecurity controls."

- SEMA recommends that Section 6 be expanded to include any type of aftermarket part, not just insurance dongles, mobile phones or other digital devices.

- SEMA recommends that Section 7 include reference to "vehicle modifications" to confirm consumer rights to modify vehicles in addition to having the vehicle serviced.

Guaranteeing consumer access within the cybersecurity framework is a complex challenge that requires collaboration within industry, government agencies and industry standard-setting organizations. SEMA appreciates NHTSA's updated cybersecurity best practices document as an important contribution to that effort.

Feel free to contact me if you have any questions.

Sincerely,

Daniel Ingber
Vice President, Government and Legal Affairs
202-792-4446; danieli@sema.org

1) "Letter: Scare tactics have nothing to do with car repair" Boston Herald Letter to the Editor, September 25, 2020. https://www.bostonherald.com/2020/09/25/letter-scare-tactics-have-nothing-to-do-with-car-repair/