

**Via electronic delivery**

March 15, 2021

U.S. Department of Transportation

National Highway Traffic Safety Administration (NHTSA)

1200 New Jersey Avenue SE

Room W12-140

Washington, D.C. 20590

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

To Whom It May Concern in the National Highway Traffic Safety Administration:

The Automotive Recyclers Association (ARA) appreciates the opportunity to submit the following comments for consideration by the National Highway Traffic Safety Administration (NHTSA) to assist in the agency’s evaluation of its updated *Draft 2020 Cybersecurity Best Practices for the Safety of Modern Vehicles* (2020 Cybersecurity Best Practices).[[1]](#footnote-1) ARA encourages NHTSA to update its 2020 Cybersecurity Best Practices document to better address the key areas of “Serviceability.”[[2]](#footnote-2)

Since 1943, the Automotive Recyclers Association has represented professional automotive recyclers, a vibrant and thriving part of the automotive supply chain. ARA’s mission is to advance the automotive recycling industry and promote its beneficial effects on society. ARA and its members are dedicated to the efficient removal and re-utilization of ROE-Recycled Original Equipment® which are genuine original equipment manufacturer (OEM) automotive parts – and the safe disposal of inoperable motor vehicles.

Automotive recyclers process over 12 million vehicles per year, making automobiles the most recycled item in the world. The automotive recycling industry is in the top 20 largest in the U.S., valued at an estimated $32 billion dollars annually. Professional automotive recycling facilities play an important role in the economic marketplace, providing a counterbalance to more expensive new replacement parts and ensuring competition in the motor vehicle replacement parts market. By being a primary source for cost effective and consumer friendly motor vehicle replacement parts, automotive recyclers provide vehicle owners with the ability to repair their vehicles in cases where it would normally be cost prohibitive.

In addition to the critical role they play in the automotive supply chain and motor vehicle replacement parts market, professional automotive recyclers play a valuable role in the efficient, environmentally friendly disposal of inoperable motor vehicles. Automotive recycling preserves natural resources, reduces the demand for scarce landfill space, and plays an important role in reducing air and water pollution.

As noted by NHTSA in its federal register notice, “*Automotive technology has developed to such an extent that today’s vehicles are some of the most complex computerized products available to consumers*.”[[3]](#footnote-3) Motor vehicles are becoming increasingly complex as they become ever increasingly connected digital devices and the data generated and used by vehicles throughout their lifecycles is becoming more important to the upkeep and use of vehicles. In formulating its 2020 Cybersecurity Best Practices, NHTSA focused on safety aspects of cybersecurity and tailored its focus on “*cybersecurity issues that impact the safety of motor vehicles throughout the lifecycle of design, operation, maintenance and disposal*.”[[4]](#footnote-4) NHTSA demonstrated its commitment to ensuring that cybersecurity impacting motor vehicle safety was addressed for the entire lifecycle of a vehicle by including sections on and Serviceability of its 2020 Cybersecurity Best Practices document. ARA strongly agrees with the guidance provided in the 2020 Cybersecurity Best Practices document that recognizes the need for automotive manufacturers to consider the serviceability of vehicle components and systems by individuals and third parties and that automotive manufacturers should not unduly restrict access by third-party repair services while providing cybersecurity protections.[[5]](#footnote-5)

While NHTSA included sections within the 2020 Cybersecurity Best Practices document that addressed the issues of serviceability, NHTSA did not go far enough in providing those within the vehicle manufacturing industry guidance on this issue. Serviceability issues must be addressed in the development of effective cybersecurity policy as it relates to motor vehicles due to the fact that vehicle owners will own their vehicles over the course of many years and that they will likely need to repair a vehicle past its original warranty. The interests of vehicle owners as well as a recognition of how motor vehicle owners interact with their vehicles on a daily basis over the course of many years must be considered in a successful cybersecurity policy. ARA would like NHTSA to take a more comprehensive look on the need for vehicle owners to control their property and the vehicle they own, which inevitably involves data access.

Therefore, ARA recommends that as vehicle owners have been historically able to choose when, how, and at what cost to repair their vehicles, that these principles be applied and recognized in future NHTSA policy. Without controlling the data, a vehicle owner will not be able to control the repair options. This will eventually restrict the ability of any party (other than the automobile manufacturer) from being able to perform repairs on a vehicle owners’ vehicle. Therefore, data generated and used by modern vehicles must remain the property of the vehicle owner and not unduly restrict their ability to effectively access and control the data that they own. This should extend to vehicle owners being able to designate who can access vehicle generated data.

Vehicle owners must also be provided with access to the data generated by their vehicles because of the associated safety risks. If vehicle owners do not have a choice where to have their vehicle repaired and can only use new equipment manufactured parts and original equipment manufactured service, vehicle owners may be unable to afford to repair their vehicle. By not being able to choose where to have their vehicle repaired, vehicle owners may drive their damaged vehicles under dangerous conditions due to not being able to afford replacement parts and repair services.

ARA recommends that NHTSA update its 2020 Cybersecurity Best Practices document to reflect the reality that vehicle owners need to have the ability to choose where and when to have their vehicle repaired and that this can only be accomplished so long as vehicle owners have access to their vehicle’s data.

Sincerely,

Sandy Blalock

Sandy Blalock

Executive Director

(505) 228-0401

sandy@a-r-a.org

1. National Highway Traffic Safety Administration (NHTSA), *Cybersecurity Best Practices for the Safety of Modern Vehicles* (Draft 2020 Update). <https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/vehicle_cybersecurity_best_practices_01072021.pdf> [↑](#footnote-ref-1)
2. National Highway Traffic Safety Administration (NHTSA), *Cybersecurity Best Practices for the Safety of Modern Vehicles*, 11, 12 (Draft 2020 Update). [↑](#footnote-ref-2)
3. Cybersecurity Best Practices for the Safety of Modern Vehicles, 86 Fed. Register 2482 (January 12, 2021). [↑](#footnote-ref-3)
4. *Id*. [↑](#footnote-ref-4)
5. National Highway Traffic Safety Administration (NHTSA), *Cybersecurity Best Practices for the Safety of Modern Vehicles*, 12 (Draft 2020 Update). [↑](#footnote-ref-5)