autocare ASSOCIATION
Independence drives us.

7101 Wisconsin Avenue
Suite 1300
Bethesda, MD 20814
www.autocare.org

T: 301.654.6664
F: 301.654.3299
info@autocare.org

October 19, 2015

Congressman Michael Burgess
Chairman
Subcommittee on Commerce, Manufacturing & Trade
2125 Rayburn House Office Building
Washington, DC 20515

Congresswoman Jan Schakowsky
Ranking Member
Subcommittee on Commerce, Manufacturing & Trade
2322A Rayburn House Office Building
Washington, DC 20515

RE: Discussion Draft to Provide Greater Transparency, Accountability, and Safety Authority to the National Highway Traffic Safety Administration

Dear Chairman Burgess and Ranking Member Schakowsky:

The Auto Care Association, on behalf of our 3,000 member companies representing more than 150,000 independent auto care businesses, are encouraged by the efforts to address the role of the National Highway Traffic Safety Administration (NHTSA) in order to further the passage of a long-term national transportation bill. The current discussion draft attempts to tackle the most complicated issues surrounding vehicle safety in our modern day with new sections on data privacy, hacking and cybersecurity. However, the current draft language under-values the role of the auto care industry in new and developing automotive technologies in a manner that could cripple the industry moving forward. We urge the subcommittee to revisit these critical sections of the discussion draft before proceeding.

The Auto Care Association is a national trade association representing the independent businesses within the supply chain of the $328 billion vehicle maintenance and repair industry. The auto care industry contributes more than 2.2 percent to the U.S. gross domestic product and employs more than 4 million people. Following expiration of a new car warranty, over 75 percent of car owners patronize independent repair shops rather than new car dealers.

The proliferation of software, firmware, and hardware into the operating functionality of motor vehicles means mechanical functions of vehicles are being partially performed by electronic systems. These systems are functionally integrated with, and as a practical matter, inseparable from physical engine parts. Whereas in the past a repair shop or car owner could diagnose an issue impacting emissions and safety solely by mechanical adjustments, today they require access to the vehicles' control software using laptop computers and sophisticated diagnostic tools and software.

However, section 302 of the Committee's discussion draft states that it is "unlawful for any person to access, without authorization, an electronic control unit (ECU) or critical system of a motor vehicle, or other system containing driving data for such motor vehicle, either wirelessly or through a wired connection." It should be noted that the ECU is the brain of a vehicle and therefore for a service facility to repair a vehicle system, they will need access to that ECU for both the diagnosis and repair. The language in the draft is extremely vague and could be interpreted to provide the car company with full control over who has access to key vehicles systems many of which are needed for repair purposes. Such action could have severe anti-competitive impacts on our industry and car owners who depend on independent repair shops for about 80 percent of post warranty repairs.

The Auto Care Association believes that when a consumer purchases a vehicle, they own not only the sheet metal and mechanical parts, but the software as well. While the design of the software might be the property of the developer, ownership and therefore access to that software should be controlled by the owner of that vehicle and not by the vehicle manufacturer. Therefore, it is important that in generating any measures to

protect cyber security, that the ability for car owners to be able to obtain competitive service or for that matter to be able service the vehicle themselves must be taken into account.

Furthermore, it has been promoted by academics and motor vehicle manufacturers, alike, that the aftermarket is a critical ally in accelerating the adoption of advanced vehicle technologies that have proven safety benefits. Add-on devices for lane departure warning, location services, collision warnings, and other technologies are being developed not solely by motor vehicle manufacturers, but auto care companies and aftermarket divisions of motor vehicle equipment companies. These companies outnumber motor vehicle manufacturers by far and provide just as much of a necessary perspective on the development of best practices for data and systems security. However, the current discussion draft grossly limits their ability to be present during the development of policies and practices surrounding the security of motor vehicle equipment. Specifically, limiting the presence of aftermarket representation on advisory committees determining policies on cyber security, advanced vehicle technologies, and other critical systems to one or even no members potentially cripples these policies from being effective and consistent across the automotive technology spectrum.

The Auto Care Association, on behalf of the auto care industry, strongly urges the subcommittee to review and redraft portions of the current discussion draft published October 13, 2015 with regards to electronic vehicle systems, data, hacking, advanced vehicle technologies, and cyber security.

Sincerely,

Aaron Lowe
Senior Vice President, Regulatory and Government Affairs
Auto Care Association