The Center for
Auto Safety
1825 Connecticut Ave. NW Suite 330 Washington, DC 20009
www.autosafety.org

June 13, 2018

Chairman John A. Barrasso
U.S. Senate Committee on Environment
and Public Works
410 Dirksen Senate Office Building
Washington, DC 20510

Ranking Member Tom Carper
U.S. Senate Committee on Environment
and Public Works
410 Dirksen Senate Office Building
Washington, DC 20510

RE: Hearing on Innovation and America's Infrastructure: Examining the Effects of Emerging Autonomous Technologies on America's Roads and Bridges

Dear Chairman Barrasso and Ranking Member Carper:

The Center for Auto Safety ("the Center") wants to express our appreciation for the Committee holding this important hearing today. Despite the ceaseless hype and hyperbole by some industries and investors interested in short term profits, the era of driverless vehicles is in its infancy. Accordingly, this is exactly the moment to conduct a holistic review of the future these technologies and examine how to ensure it coincides with the maintenance of our existing roads and bridges as well as any new projects. How and when our nation's infrastructure will be prepared to accommodate autonomous technologies for passenger and commercial traffic is a question best answered in concert with – and not separate from – the legal, regulatory, and safety issues that surround these early developmental days for driverless cars and trucks. Such a potentially revolutionary change requires careful planning at the local and national level and is unlikely to be best served from a rush-to-market philosophy.

The Center, founded in 1970, is an independent, non-profit consumer advocacy organization dedicated to improving vehicle safety, quality, and fuel economy not only for our members, but all drivers, passengers, and pedestrians in rural and urban areas alike. On behalf of those 310 million Americans who use our nation's roads and bridges daily, we urge the Committee to recognize that it may be decades until deployment of truly autonomous passenger vehicles is realized at levels beyond small geofenced areas. Therefore, while driverless cars may represent an exciting future, and generate headlines, in the here and now Americans are buying twice as many *used* cars and trucks every year instead of the technically advanced new vehicles. The annual death toll of 37,000, and more than 2 million serious injuries, from traffic crashes will not be waved away by a magic wand called "autonomy" any time soon, because conventional vehicles will dominate our roadways for decades to come. Our infrastructure plans should bear this in mind.

V2X

Vehicle-to-Vehicle, (V2V) Vehicle to Infrastructure, (V2I) Vehicle to Pedestrians, (V2P) and Vehicle to Network, (V2N) technology is often referred to collectively as "V2X." This connectivity has the potential to significantly improve traffic safety by giving drivers an early warning of yet-unseen crash hazards posed by other vehicles. V2X could enable drivers to obtain advance warning of other potential road hazards, and could improve pedestrian and cyclist safety as well. Such communication has the potential to make everyone's lives more efficient and convenient. For example, V2I and V2N could allow for an offramp's traffic camera to inform a vehicle's GPS of backed-up traffic and offer a reroute that gets the vehicle's occupant to her destination more quickly and with the use of less fuel or electricity. Put simply, V2X has great potential for safety advancements if it is an integrated feature of driverless vehicle and infrastructure development – and not an after the fact add-on.

Yet, it is exactly this integration that presents significant challenges in developing and implementing effective and reliable V2X communications systems, and in taking them from the closed testing environment to the open road. These include technological challenges, such as message congestion and gaps in GPS coverage; security challenges, such as vulnerability to hacking; and potential privacy issues.[1] In other words, for V2X to be a successful feature – and not simply a luxury infotainment system – it will require the intervention of regulating bodies, be they Congress or the Department of Transportation.

To begin with, all new vehicles will need have V2V and V2I as a standard feature, because the value of the connectivity is in its ubiquity. Also, V2X must have a common language, not only from manufacturer to manufacturer, but from state to state, and even city to city. Finally, safety messaging and traffic information must be separate from and primary to infotainment. This is important not only from a cybersecurity standpoint, but from a primacy of purpose view as well. Dedicated Short- Range Communication (DSRC) can accomplish this last item right away.

The Center maintains that moving forward with a safety focused DSRC rule that maximizes the spectrum previously set aside for this purpose, as contemplated by the V2V rulemaking undertaken in January 2017 by DOT,[2] is the fastest way to get this lifesaving technology deployed on today's vehicles. Unfortunately, that rulemaking has come to a complete halt because of what appear to be commercial interests advocating for technologies that could prioritize entertainment over safety. After a complete review it may well be that DSRC can be improved upon when it comes to delivering on the potential for connected vehicles and roads in terms of both safety and economic utility. Yet, instead of having that debate on the way to a safety rule, the process to require V2V communications has been ground to a halt with no movement in sight. It is exactly this kind of conflicting motive that can only be overcome by a nationwide plan that builds safety into the infrastructure from the start.

[1] Yet another reason using Dedicated Short- Range Communication is a good idea. https://consumerfed.org/press_release/consumer-auto-safety-groups-call-non-commerical-use-auto-safety-spectrum-strong-privacy-security-protections/

[2] https://www.regulations.gov/document?D=NHTSA-2016-0126-0009

Cybersecurity

As discussed above, the measured and planned development of V2X technologies are likely to play a key role in the success of driverless vehicles achieving their maximum utility from both a safety and commercial standpoint. V2X technologies have the potential to dramatically improve highway safety and traffic situational awareness for both conventional and driverless vehicles.

Unfortunately, these technologies also provide multiple opportunities for bad actors to interfere with individual vehicle operation, and potentially interfere with operation of the entire transportation system. The presence of safety-critical software in conventional automobiles (SAE autonomy levels 0-2) and the complete dependence of driverless vehicles (SAE autonomy levels 3-5) on extensive safety-critical software demand the establishment and enforcement of software safety standards for all elements of the technology. The reliance on safety critical software is what led the Department of Defense[3] and the Federal Aviation Administration (FAA)[4] to recognize the absolute need for cybersecurity in these types of applications and to respond by promulgating enabling requirements and regulations. These guidelines have been successful in protecting the security of military assets and the public safety of commercial aircraft operations.

While fully driverless vehicles may be years away from widescale deployment, or public acceptance, the time to plan for such occurrences is prior to their arrival. This is especially the case when it comes to the difficult and time-consuming task of creating usable process and performance standards for the cybersecurity of the hundreds of millions of driverless vehicles that may one day be operating across the country. Unfortunately, neither of the major bills currently under consideration in Congress regarding driverless vehicle technology require cybersecurity standards – either for the vehicles or infrastructure. What makes this lack of standards particularly puzzling is that analogous standards exist, such as RTCA DO-178C,[5] which are required to be met by the FAA prior to aircraft certification and commercial use.

As has been demonstrated in the of context a moving vehicle, the threats of cyber intrusion for autonomous cars and trucks are real.[6] Moreover, at a moment when massive

[3] DOD 5000.02, January 7, 2015, section 3h, Information Technology;

> "(1) All IT that receives, processes, stores, displays, or transmits DoD information will be acquired, configured, operated, maintained, and disposed of consistent with applicable DoD cybersecurity policies, standards, and architectures.
>
> "(2) Risks associated with global sourcing and distribution, weaknesses or flaws inherent in the IT, and vulnerabilities introduced through faulty design, configuration, or use will be managed, mitigated, and monitored as appropriate.
>
> "(3) Cybersecurity requirements must be identified and included throughout the lifecycle of systems including acquisition, design, development, developmental testing, operational testing, integration, implementation, operation, upgrade, or replacement of all DoD IT supporting DoD tasks and missions."

[4] FAA Advisory Circular AC No. 20-115C, Subject: Airborne Software Assurance, specifies acceptability of RTCA DO-178C, "Software Considerations in Airborne Systems and Equipment Certification," dated December 13, 2011.

[5] https://www.faa.gov/aircraft/air_cert/design_approvals/air_software/

[6] https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

cyber-breaches of major corporations or government entities seem to be announced on a weekly basis, to undertake the mass deployment of hackable multi-ton vehicles that can travel 100 mph without mandatory, demonstrable, security protocols is not only foolhardy – it presents a potential national security concern. The time is now to determine whether it is better to use an existing standard and adapt it to the ground transportation needs for V2X, or whether a new protocol must be developed.

Finally, from a fiduciary perspective, addressing these issues and implementing solutions on the front end is likely to be far less expensive than attempting to close the barn door after the proverbial horses have already escaped. All of us who believe in the importance of auto safety must work together to encourage the development of safety-critical software requirements or regulations in response to these emerging threats in order to mitigate, and ideally eliminate, automotive vehicle and related infrastructure cyber vulnerabilities.

Crash Data

As recent on-road crashes involving semi-autonomous (level 2) vehicles have demonstrated, the interaction between infrastructure and next generation vehicle technology can have tragic consequences.[7] In fact, the Tesla operating on "Autopilot" in the fatal Mountain View, California crash was reported to have veered into a guardrail – in a spot it had done so previously.[8] In another instance, Tesla had two separate vehicles using the "Autopilot," mode crash in essentially the same highway location approximately one year apart.[9]

One of the key issues raised in any crash involving cars with autonomous or semi-autonomous technology, including the one involving an Uber that killed a pedestrian in Tempe, Arizona, is how to understand what happened.[10] Two of these incidents resulted in deaths, two involved injuries. Ideally, each crash helps prevent the next one, but after each of these incidents there were conflicting media reports, and in some instances, conflicting police reports. How can national policy makers and the public be sure they are getting the facts? How can local authorities understand whether the infrastructure is to blame or the vehicle is at fault?

Today, when the National Transportation Safety Board (NTSB) undertakes a crash investigation of semi-autonomous vehicles, the agency has to work with manufacturers to access any data available to assist in an accurate evaluation of the crash. Unlike aviation, railroad, and ship accidents, when it comes to driverless vehicles, investigators are dependent upon the manufacturer to interpret the data and provide an accurate account of all relevant data available to the vehicle's recording systems.

[7] Drew Harwell, Experts Worry Tesla is using consumers as guinea pigs, Washington Post, June 11, 2018

[8] http://abc7news.com/automotive/i-team-exclusive-victim-who-died-in-tesla-crash-had-complained-about-autopilot/3275600/

[9] https://www.upi.com/Self-driving-Tesla-car-crashes-in-same-California-location-as-2017-accident/1131527692147/

[10] Uber – Tempe, AZ, March 18, 2018, resulting in a death; Tesla – Mountain View, CA, March 23, 2018, resulting in a death; Waymo – Chandler, AZ, May 4, 2018, resulting in an injury to the test driver; Tesla – South Jordan, UT, May 11, 2018, resulting in an injury to the driver.

Yet, there are no uniform parameters for driverless vehicle data recorders to allow crash investigators to compare information across manufacturers to help understand whether different autonomous systems might react the same or differently to the same stretch of road. Making things even more difficult in the context of several of these incidents, the manufacturers publicly disclosed information about the crash, prior to any official announcements, thwarting long-established policies of cooperation that are critical to conducting independent crash investigations.

Current event data recorder (EDR) requirements focus exclusively on the milliseconds prior to a crash with enough impact to cause airbags to deploy (among other factors). To properly evaluate driverless technology, investigators must be able to see far more time and data than on conventional vehicles. They must have access to pre-crash and post-crash data to be able to accurately evaluate the performance of the driverless vehicle. Otherwise, it will be next to impossible to answer such questions as whether a sensor malfunctioned or was simply not good enough; whether there was a data processing, communications, or software problem; whether a safety driver or the machine was in control; or whether the fault lies with a conventional driver. Current EDR rules mean the public and policy makers will have to rely on the *least* objective party involved to provide the information: the manufacturer. As the Committee with jurisdiction over public roads, highways, and bridges, it is vital for your oversight purposes to be sure that enough objective, unbiased information will be available to crash analysts to reduce or eliminate unnecessary deaths, injuries, and property damage.

Conclusion

While it is our current position that driverless cars should remain on test tracks and in controlled environments until they have demonstrated sufficient levels of safety to be allowed into our neighborhoods, it is our hope that this will not always be the case. At some point in the coming decades, driverless vehicles are likely to be deployed on public roads. These vehicles and infrastructure must work together to maximize safety for everyone on the road. Undertaking that process simultaneously is the best chance for all of us to reach that future as safely as possible.

On behalf of the Center for Auto Safety and our members, thank you for your attention to this important matter.

Sincerely,

Jason Levine
Executive Director