CVTA
COMMERCIAL VEHICLE
TRAINING ASSOCIATION

June 12, 2017

Mr. Larry Minor
Associate Administrator for Policy
Federal Motor Carrier Safety Administration
United States Department of Transportation
1200 New Jersey Avenue SE
Washington, DC 20590

RE: FMCSA Motor Carrier Safety Advisory Committee Task 17.1 (Highly Automated Commercial Vehicles)

Dear Associate Administrator Minor:

The Commercial Vehicle Training Association is the largest association of commercial truck driver training schools in the United States. Our membership represents nearly 200 locations in 42 states that collectively graduate around 50,000 commercial drivers annually. As educators and trainers of the next generation of truck drivers, our members will have a critical role in ensuring future drivers are trained on how to operate highly autonomous vehicles. Therefore, we appreciate the opportunity to comment on MCSAC Committee Task 17.1 and hope the Committee will consider the following comments.

Highly Autonomous Technology Should Not Replace Driver

Highly autonomous commercial vehicle (HACV) technology will greatly improve highway safety and efficiency of freight movement. To account for the existence of HACV technology, the FMCSA will need to modify existing Federal Motor Carrier Safety Regulations (FMCSRs). As the FMCSA begins to consider regulatory changes necessary to conform to new technology, we believe that the FMCSA should have two fundamental requirements. First, it should require a qualified commercial vehicle operator in the vehicle in the event of a technological malfunction. Second, the FMCSA should require all Commercial Motor Vehicles be equipped with steering, braking, and acceleration controls to allow the driver to assume full control of the vehicle at any time. We believe these are prudent and sensible policies to ensure highway safety.

Automation in transportation is not a new concept. The motor carrier industry has the luxury of looking to other modes for guidance on how automated technology can be implemented. For example, highly sophisticated automated technologies can be found in rail and aviation systems, yet the role of the conductor and the pilot remains paramount. While braking and speed control systems on trains require fewer inputs from conductors, the conductor is required to monitor the train’s systems and assume control when necessary. Even though an airline pilot can be relatively hands-off while a plane is flying at cruising altitude, he or she must constantly monitor airplane systems and be prepared to assume control of the plane in the event of a systems malfunction. Furthermore, pilot input is required during the highest-risk phases of flight where complicated maneuvers are required, such as take-off and ascent, descent and landing, and taxiing to and from the gate. We anticipate similar circumstances for HACV, where a driver may be hands-off for some of the time, but encounter situations which require them to take control over a vehicle.

Technology Malfunction, Cybersecurity, and Highway Safety

Any technology or machine is subject to damage, failure, or tampering. HACVs are no different. For these reasons, CVTA believes requiring a qualified, well-trained driver to remain in the cab of a CMV is sensible step in avoiding disasters of when technology fails, breaks, or gets hacked. There have been a number of cases where SAE Levels 1 passenger vehicles were hacked in a controlled environment, and the hackers were able to assume control of the vehicles' braking, steering, and acceleration functions.[1] In fact, cybersecurity researchers have determined it can actually be *easier* to electronically usurp a truck's acceleration and braking functions via cyber hacking. [2] With a recent uptick in criminal and terrorist attacks involving passenger and commercial vehicles both in the United States and abroad,[3] [4] [5] [6] there is a possibility that an AV or HACV would be a high value target for malicious state or non-state actors seeking to maximize damage upon our nation. Additionally, normal wear and tear, or other damage caused by physical tampering, weather, or roadway debris could impact HVACs and render its automated functions inoperable. MCSAC has a responsibility to call attention to these potential threats and limitations. Any policy regarding HACV should address the danger posed by technological failure, hacking, or other concerns with technology that could result in complete loss of control of vehicle functions that put public safety at risk. Again, CVTA's policy recommendation is to mandate a driver have the capability to override system of a HACV.

Entry-Level Driver Training Moving Forward

The Entry-Level Driver Training (ELDT) Final Rule has recently entered its implementation phase. By the time this rule is fully implemented, the FMCSA will likely have to again approach revamping the required curriculum and behind the wheel training to account for this technology in the very near future. While we believe this technology will enhance drivers' ability to perform their job, not replace them, we do recognize that the skills needed for this profession will change. This change will also happen very soon. As AV technology becomes more commonplace in the critical functions of commercial motor vehicles, CVTA recognizes that training providers may need to modify their curriculums to reflect these changes. Therefore, the FMCSA should consider a nimble process to accept recommendations and proposed changes to the required curriculum and behind the wheel training. It may want to consider whether a HACV endorsement for the commercial driver's license (CDL) would be more appropriate than an across-the-board requirement for proficiency in HACV technology.

Conclusion

CVTA offers itself as a resource to MCSAC and FMCSA as the industry continues the discussion on the future of technology in truck driving and the central role the driver will continue to play in the safe and efficient movement of U.S. freight. Please contact Mark Valentini, CVTA Director of Government

[1] Greenberg, Andy. "The Jeep Hackers Are Back to Prove Car Hacking Can Get Much Worse." *Wired,* August 1, 2016. https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/

[2] Greenberg, Andy." Hijackers Hijack A Big Rig Truck's Accelerator and Brakes. *Wired,* August 2, 2016. https://www-wired-com.cdn.ampproject.org/c/s/www.wired.com/2016/08/researchers-hack-big-rig-truck-hijack-accelerator-brakes/amp

[3] Greenberg, Andy. "The Jeep Hackers Are Back to Prove Car Hacking Can Get Much Worse." *Wired,* August 1, 2016. https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/

[4] "London Attack: Seven Killed in Vehicle and Stabbing Incidents." *BBC News,* June 4, 2017. http://www.bbc.com/news/uk-40146916

[5] Masters, James. "Stockholm Truck Attack Kills 4; Suspect Held on Suspicion of Terror." *CNN World,* April 8, 2017. http://www.cnn.com/2017/04/07/europe/stockholm-truck-crash/index.html

[6] "Death Toll from France Truck Attack Rises to 85." *BNO News,* August 4, 2016. http://bnonews.com/news/index.php/news/id4998

Affairs, at (703) 642-9444 or mark.valentini@cvta.org should you want to learn more about CVTA's efforts on HACV technology, or have any questions or concerns.

Thank you for your consideration.

Sincerely,

Don Lefeve,
President & CEO