**Owner-Operator Independent Drivers Association**

**National Headquarters: 1 NW OOIDA Drive, Grain Valley, MO 64029**
**Tel: (816) 229-5791 Fax: (816) 427-4468**

**Washington Office: 1100 New Jersey Ave. SE, Washington, DC 20003**
**Tel: (202) 347-2007 Fax: (202) 347-2008**

March 9, 2026

The Honorable Brett Guthrie
Chairman
House Committee on Energy and
Commerce Committee

The Honorable Frank Pallone
Ranking Member
House Committee on Energy and
Commerce Committee

**RE: Opposition to H.R. 7390, SELF DRIVE Act of 2026**

Dear Chairman Guthrie and Ranking Member Pallone:

The Owner-Operator Independent Drivers Association (OOIDA) is the nation's largest trade association representing the views of small-business truckers and professional truck drivers. OOIDA's mission is to promote and protect the interests of its members on any issues that might impact their economic well-being, working conditions, and the safe operation of commercial motor vehicles (CMVs) on our highways.

We write to express our opposition to H.R. 7390, the SELF DRIVE Act of 2026, since it fails to ensure the safe operation of driverless trucks or provide adequate transparency about their performance and capabilities.

A recent crackdown from the Federal Motor Carrier Safety Administration (FMCSA) demonstrates the importance of oversight and enforcement of critical safety regulations. On February 18, FMCSA announced it was revoking the authority of over 550 Commercial Driver's License (CDL) training schools for failing to meet federal safety standards, and in some cases, perpetrating outright fraud. We applaud FMCSA for this action since ensuring compliance with basic training and licensing standards is foundational to road safety. This action makes clear that regulatory verification and enforcement are critical to upholding safety standards.

Instead of holding autonomous vehicles to similar standards, H.R. 7390 would permit the operation of driverless 80,000 pound trucks based on the unverified assertions of companies with a vested financial interest in their deployment. While companies would be required to develop a "safety case" describing how the vehicle would operate safely, there is no requirement that the federal government verify these plans. In fact, companies would not need to provide these cases to the government before deployment, or possibly even at all. These cases must only be submitted to DOT upon request. This amounts to self-certification for the use of heavy-duty trucks on our nation's roads. Under these circumstances, there is no way for the public to know whether these vehicles will operate safely.

The use of "self-certification" has already proven to have serious shortcomings in multiple areas across the trucking industry, and taking this approach with autonomous CMVs would be the most disastrous use yet.

To take one example, the Electronic Logging Device (ELD) mandate requires that heavy-duty trucks be equipped with a device, hardwired into the engine control module, that tracks the truck's location and uptime, among other information. When issuing this regulation, FMCSA established only "minimally compliant" security standards, and no requirement for third-party validation or testing prior to self-certification.[1] As a result, we have seen numerous reports of ELDs that are vulnerable to cybersecurity attacks and could allow hackers to, "take control of, steal data from, or even disrupt entire fleets by spreading malware unnoticed between vehicles."[2] In 2019, the FBI issued a security bulletin that highlighted the ability of cyber criminals to exploit ELD vulnerabilities due to a lack of certified security practices. Specifically, they noted that "this poses a risk to businesses because ELDs create a bridge between previously unconnected systems critical to trucking operations."[3]

Similar to the implementation of the ELD mandate, H.R. 7390 contains only vague and insufficient cybersecurity requirements that fail to ensure the safety and integrity of automated vehicle operations. The bill merely requires manufacturers to maintain a written cybersecurity policy outlining how they would "detect and respond to cyber attacks, unauthorized intrusions, and false vehicle control commands," without defining specific technical standards such a policy must meet. This lack of specificity raises questions if these policies would actually prevent or mitigate cyber-attacks, or whether manufacturers could even execute their stated plans since the bill does not require them to prove compliance or verify cybersecurity protections are functioning as intended.

Equally troubling, H.R. 7390 includes no requirement for public disclosure of cyber intrusions, nor any mandate that companies suspend operations or take vehicles offline in the event of a cyber incident. As written, the legislation grants manufacturers significant discretion while offering the public little transparency or assurance that cybersecurity threats are being addressed promptly or appropriately.

Although H.R. 7390 attempts to provide additional cybersecurity oversight by requiring a review of the Department of Commerce's previously issued rule, "Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles," CMVs would not be included in this review since they were specifically excluded from the rule's scope. The Department of Commerce omitted CMVs because the complex nature of this sector and national security concerns require special attention. **Specifically, the Department highlighted that vehicle connectivity systems for CMVs, "pose a significant national security risk when designed, developed, manufactured, or supplied," by Chinese or Russian entities, and these risks would likely require a separate rulemaking to address this significant threat.[4]** This alone should be reason enough for the committee to recognize additional work is needed to address cybersecurity concerns for CMVs and it would be premature to permit their deployment under H.R. 7390.

---

[1] https://www.federalregister.gov/d/2015-31336/p-630
[2] https://engr.source.colostate.edu/researchers-highlight-potential-cybersecurity-threats-to-trucking-industry-supply/
[3] https://landline.media/wp-content/uploads/2020/07/Electronic_Logging_Devices_Cybersecurity_and_Best_Practices_PIN_20200721-001.pdf
[4] https://www.federalregister.gov/d/2025-00592/p-87

We also believe that this legislation fails to adequately address outstanding questions about how current safety regulations and licensing requirements will apply to heavy-duty trucks operating with automated driving systems (ADS). In 2019, FMCSA issued an Advanced Notice of Proposed Rulemaking (ANPRM) regarding the deployment of autonomous commercial motor vehicles (FMCSA-2018-0037-0131). This ANPRM raised numerous questions about how autonomous CMVs could be deployed, what safety measures should be in place, and in particular, what sort of CDL qualifications or requirements should be required of operators of these CMVs. To date, many of these questions remain unanswered.

We are concerned that this legislation doesn't directly address qualifications for remote operators for CMVs, or how an ADS would meet current Federal Motor Carrier Safety Regulations (FMCSRs) and qualifications for CMV drivers. Whether a vehicle is operated directly by a driver behind the wheel or by a remote assistant monitoring and potentially assuming control, the individual performing that function must hold a valid CDL. The CDL framework is built on decades of safety experience and ensures that operators understand the fundamental dynamics, risks, and responsibilities associated with CMV operation. For these reasons, all autonomous and remotely operated CMVs must remain fully subject to FMCSRs. The need for thorough inspections, hours-of-service limitations, drug and alcohol testing requirements, and physical qualification standards remains just as relevant—if not more—when technology may disengage unexpectedly or require a human to rapidly assume control. Until ADS-equipped CMVs have demonstrated safety performance equal to or exceeding that of human drivers, they should be held to the same, or more stringent, regulatory oversight.

Despite pronouncements from autonomous trucking companies that full deployment is just around the corner, we still have not seen any independent, verifiable evidence that AV trucks are safe and ready. As we have advocated for years, measures to advance automated technology should be met with mandatory data transparency from AV companies. This will help educate consumers, the industry, lawmakers, and regulators about the actual reliability of autonomous technology. Regrettably, H.R. 7390 falls short on this aspect as well. Instead of requiring proactive reporting of safety data and performance, this legislation only requires companies to report information after a crash. Our members make their living on the road, and they shouldn't have to wait until something goes wrong to learn more about the safety of the driverless vehicles they're sharing the road with.

We urge the Committee to reject H.R. 7390 and instead pursue a framework that prioritizes adherence to proven safety requirements, independent validation, and full transparency before allowing driverless heavy-duty trucks onto our nation's roads. Small-business truckers and professional drivers have a direct stake in the outcomes of these decisions, and they deserve policies rooted in rigorous oversight, not assumptions or unverified assurances from industry. We stand ready to work with you to develop responsible, data-driven approaches that genuinely enhance roadway safety while preserving the integrity of the trucking profession and safeguarding the motoring public.

Thank you,

Todd Spencer
President & CEO
Owner-Operator Independent Drivers Association, Inc.

Cc: Members of House Energy and Commerce Committee