Small Business in Transportation Coalition

September 27, 2021

PETITION

Mr. R. Ryan Posten,
Associate Administrator for Rulemaking
USDOT NHTSA
1200 New Jersey Avenue SE.
Washington, DC 20590

Re: PETITION FOR NEW & AMENDED MOTOR VEHICLE SAFETY STANDARDS & PETITION FOR A DEFECT INVESTIGATION.

Dear Mr. Posten,

This is a petition for new/amended motor vehicle safety standards and a request for investigation of the Society of Automotive Engineers (SAE) J1939 data bus standard. As you know, you currently maintain motor vehicle safety standards for buses, including school buses, and semi-trucks in terms of their accelerator control systems (49 CFR § 571.124 - Standard No. 124; Accelerator control systems) and braking systems (49 CFR § 571.105 - Standard No. 105; Hydraulic and electric brake systems & § 571.121 Standard No. 121; Air brake systems.). Many of these types of commercial motor vehicles across various manufacturers use the SAE J1939 standard.

BACKROUND

As you know, we previously petitioned the Secretary twice over the past two years for motor vehicle standards regarding Electronic Logging Devices (ELDs). By letter of September 9, 2021, you finally denied our request after failing to respond to our petitions within the 120 statutory period, and generally, contrary to the Administrative Procedure Act *(5 U.S. Code § 555).* You took the position that our request did not conform to a bona fide petition for motor vehicle standards because ELDs are a matter of a MAP-21 requirement. Presumably, you took this position to defend against our lawsuit against the Department, but this position leaves public safety at risk. You referred us back to the FMCSA, whom we have dealt with for years to no avail.

Comes now, the SBTC to request new and amended motor vehicle safety standards and a steering and acceleration defect investigation for all trucks and buses manufactured using the SAE J1939 standard.

First, we note that, while the Moving Ahead for Progress in the 21st Century Act (MAP-21) required all then-existing commercial motor vehicles manufactured after 2000 to be equipped with ELDs as of December 2017, ELDs are now installed at the time a vehicle is manufactured. We point to Exhibit A (Volvo's factory-fit telematics device is coupled with Geotab's ELD application). Notwithstanding FMCSA regulations, as we understand it, your agency has promulgated no motor vehicle safety standards on manufacturers' installation of these telematic devices to date. 49 U.S.C. § 30102 defines "motor vehicle safety standard" as "a minimum standard for motor vehicle or motor vehicle equipment performance." An ELD falls under the definition of "motor vehicle safety standard" insofar as an ELD is commercial "motor vehicle equipment" mandated by law.

Second, for the reasons shown in the following section, we are concerned that your current standards that pertain to accelerator control systems and braking systems are out of date due to the fact that factory-installed unencrypted telematics equipment are known to be vulnerable to hacking.

SUMMARY OF RESEARCH

In 2016, University of Michigan researchers Yelizaveta Burakova, Bill Hass, Leif Millar, and Andre Weimerskirch published the attached report entitled: *"Truck Hacking: An Experimental Analysis of the SAE J1939 Standard"* (Exhibit B). Quoting from the summary of the study:

> *We test our attacks on a 2006 Class-8 semi tractor and 2001 school bus. With these two vehicles, we demonstrate how simple it is to replicate the kinds of attacks used on consumer vehicles and that it is possible to use the same attack on other vehicles that use the SAE J1939 standard. We show safety critical attacks that include the ability to accelerate a truck in motion, disable the driver's ability to accelerate, and disable the vehicle's engine brake. We conclude with a discussion for possibilities of additional attacks and potential remote attack vectors.*

Indeed, there has been much research and media coverage of this matter.

Earlier this month, as you know, we marked the twentieth anniversary of 9/11 in which airplanes were used to attack and murder American citizens.

Given the truck attacks in Europe over the past decade at the Christmas Market in Berlin and Nice on Bastille Day in 2016, we contend it's only a matter of time until some terrorist hacks into a vulnerable ELD system, takes control of a hazmat truck's acceleration and/or steering, and remotely wipes out a school bus filled with children or drives it into a city's water supply. Coordinated attacks across the country simultaneously reminiscent of the 9/11 four hijacked planes are our worst fear.

This risk goes back to 2011 when the New York Times reported: *"Researchers Hack Into Cars' Electronics."*

While we believe FMCSA recklessly ignored the risk and side-stepped the issue with self-certification of ELD products, we now appeal to you with respect to new vehicle equipment.

See "Investigative: KeepTruckin fights NTSB bid to remove its ELD technology in wake of crash" - FreightWaves

Clearly, hacking risk exposure is getting worse as of 2019:

See "Car Hacking Danger Is Likely Closer Than You Think" (caranddriver.com)

And in terms of where we are going with autonomous vehicles, if they can hack a self driving car, then they will be able to hack a self driving truck and wreak absolute havoc.

See "How to hack a self-driving car" – Physics World

We note fleets are especially in danger...

See "Securing the Weakest Link in Connected Cars: Telematics Data Servers" (upstream.auto)

The insurance industry is really worried about their risk exposure:

See "Hackers infiltrate telematics technology" | Insurance Business Australia (insurancebusinessmag.com)

Truck media knows it's all about lack of encryption. These companies rushed products to market to capitalize on the mandate and quickly cash in:

See "How Secure is Your ELD?" - Fleet Management - Trucking Info

FMCSA will point to their 'best practices' document (Cybersecurity Best Practices for Integration/Retrofit of Telematics and Aftermarket Electronic Systems into Heavy Vehicles | FMCSA (dot.gov)), but they recklessly released all of these uncertified ("self-certified") products into the market in 2017. Worse, they failed to release the information they promised to release to the industry like "summary description of malfunctions" on their website, which would have enabled truckers and fleets to properly vet the products they had to choose from.

If NHTSA does not set motor vehicle standards related to telematics and their integration with acceleration, steering and braking, we are concerned our member carriers and independent owner-operators will ultimately be sued for using faulty equipment mandated by Uncle Sam when the inevitable happens in America.

FBI & AN NTSB BOARD MEMBER SHARE SBTC'S CONCERNS ABOUT HACKING

The FBI issued the attached Private Industry Notification in 2020 (Exhibit C) stating:

> The ELD mandate does not contain any cybersecurity or quality assurance requirements for suppliers of ELDs. As a result, no third-party validation or testing is required before vendors can self-certify their ELDs. Businesses choosing an ELD to use on their networks must therefore conduct due diligence themselves to mitigate their cyber risk and potential costs in the event of a cyber incident.

In it, the FBI suggests that once a cyber-criminal gains access, he can install malware, such as ransomware, to prevent the ELD, the vehicle, or connected telematics services (such as dispatching or shipment tracking) from operating until the ransom is paid. We all remember the May 2021 Colonial Pipeline ransomware attack and its effects.

Previous to that, in 2016, your own agency issued a joint PSA with FBI (Exhibit D).

That notice invited the public to:

> *3. Contact the National Highway Traffic Safety Administration*
>
> *In addition to contacting the manufacturer or authorized dealer, please report suspected hacking attempts and perceived anomalous vehicle behavior that could result in safety concerns to NHTSA by filing a Vehicle Safety Complaint.*

We do so now through this petition.

Furthermore, Michael Graham, NTSB Board Member, said during the recent Westfield Transport hearing that FMCSA's review process for ELDs was "perilously close to very little or no certification" at all. "It works, and it works because I say it works," Graham said. "That's not a very robust system."

PETITION

The SBTC hereby files a **threefold** petition:

1. We request with respect to new manufactured vehicles that you please adopt a motor vehicle standard on the installation of ELDs that takes into consideration the hacking vulnerability and encryption concerns expressed by other government agencies, industry, and the public. As you know, new vehicles are well within your purview and you have authority if not a duty to promulgate same.

   As an aside here, we note you also accept "complaints" regarding after-market equipment. https://www.nhtsa.gov/report-a-safety-problem#equipment Without conceding they were not originally 49 U.S. Code §30162 petitions as we properly characterized them to be, **we therefore now request you now accept our previous December 2019 and March 2021 49 U.S. Code §30162 petitions for ELD motor vehicle standards as "aftermarket complaints"** insofar as a lack

of encryption and vulnerability to hacking is concerned. They are incorporated here by reference. If you accept after-market complaints from the public through your website, we would hope you will not discriminate against us and reject an after-market complaint about a lack of ELD encryption and hacking vulnerability from us.

2. We request that with respect to your aforementioned currently existing motor vehicle standards for accelerator control systems and braking systems, you please address our suggestion that there is a need to modify these standards to ensure against telematics hacking and you should address, through amendment, the impact factory connection of telematics devices has on accelerator control systems and braking systems.

3. Lastly, with respect to 49 CFR § 554.6, Opening an investigation, in the interest of the identification and correction of safety-related defects in motor vehicles in terms of being susceptible to hacking as evidenced in the University of Michigan study, we request you please investigate defects in the 2006 J1939 databus that was the subject of the aforementioned hacking that enabled the accelerator to be hacked, taking into consideration the researchers' suggestion that remote hacking is also possible.

Pursuant to § 552.13, we understand from your letterhead that your office is now on New Jersey Avenue at USDOT Headquarters and we presume the address in the regulation (400 Seventh Street, S.W., Washington, DC 20590) has yet to be updated.

This letter is written in the English language.

I, JAMES LAMB, am the petitioner as Executive Director of the Small Business in Transportation Coalition (SBTC). Our address is on this letterhead.

In terms of setting forth in full the data, views and arguments of the petitioner, we offer the aforementioned University of Michigan researchers' report and FBI Private Industry Notifications that highlight ELD/telematics hacking vulnerabilities.

We make no request to have any information withheld from public disclosure and we make no request for confidential treatment.

We request you please set the requested effective dates as you deem just and proper in accordance with law.

REQUEST FOR DUE PROCESS

Pursuant to **49 CFR § 552.15 Processing of petition**, we ask that you please notify us **within 30 days** if there is any discrepancy in terms of this being a bona fide, fully compliant complete petition and not wait up to 21 months as was the case with our two previous petitions to the Secretary. We also request the petition be processed timely **within the statutory 120 days** as echoed in your regulation and the **Administrative Procedure Act** generally, and that either a timely *Notice of Proposed Rulemaking* or a timely notice denying the petition be published in the **Federal Register.**

We again point to APA statute *5 U.S. Code § 555 - Ancillary matters* that states:

(b)...With due regard for the convenience and necessity of the parties or their representatives and within a reasonable time, each agency shall proceed to conclude a matter presented to it (emphasis added)... and

(e) Prompt notice shall be given of the denial in whole or in part of a written application, petition, or other request of an interested person made in connection with any agency proceeding. Except in affirming a prior denial or when the denial is self-explanatory, the notice shall be accompanied by a brief statement of the grounds for denial.

Please advise if you require additional information in accordance with 49 CFR § 552.15. Thank you for your consideration of this important matter as it relates to highway safety.

Sincerely,

/s/ JAMES LAMB
SBTC Executive Director