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 20001
Tel: (202) 347-2007 Fax: (202) 347-2008

November 22, 2022

The Honorable Robin Hutcheson
Federal Motor Carrier Safety Administration
U.S. Department of Transportation
1200 New Jersey Avenue, SE
Washington, D.C. 20590

Re: Docket # FMCSA-2022-0062, "Unique Electronic Identification of Commercial Motor Vehicles"

Dear Administrator Hutcheson,

"It was a bright cold day in April, and the clocks were striking thirteen." The Owner-Operator Independent Drivers Association (OOIDA) does not support the erosion of privacy, nor the destruction of identity through surveillance and control. To ask for more surveillance and control in the name of safety on our highways is to venture into what George Orwell would call "doublespeak". The term "Big Brother" has come to signify government control of and intrusion into truckers' individual lives.

OOIDA and our members oppose this proposal in the strongest possible terms. Our members have been extremely clear that this concept is an unwarranted intrusion into their privacy, as well as an overly costly and burdensome requirement that does nothing to improve their efficiency or safety. Due to the absence of any research demonstrating how the use of unique electronic identifier (UEI) technology would improve safety, the motivation for pursuing this rulemaking appears to be nothing more than adding convenience for enforcement agencies. In fact, truckers have expressed serious concerns the implementation of this proposal would negatively affect highway safety if enforcement officers begin prioritizing roadside inspections based on potentially unreliable data, instead of observable safety hazards.

The Commercial Vehicle Safety Alliance's (CVSA) petition contends a UEI mandate would allow their members to better focus their enforcement efforts on high-risk carriers. OOIDA believes the systems currently used to determine high-risk carriers is critically flawed, such as the Compliance, Safety, Accountability (CSA) program, diminishing any perceived safety benefits of the proposal. We note the number of fatal crashes in the 5 years leading up to the start of CSA showed a steady decline. Following implementation, a steady increase in both fatal and non-fatal crashes occurred. In total, in the 5 years following CSA's introduction there was a 20% increase in fatal crashes and a 55% increase in crashes that resulted in injuries, further eroding

highway safety.[1]Additionally, many truckers have expressed frustration that CVSA member agencies fail to report clean inspections, which was promised when CSA was established. This has not facilitated confidence in the system and its ability to help identify high-risk carriers.

CVSA also contends UEI will provide incentives for motor carriers to operate at a higher level of compliance and safety. There is no research or data to support this claim. Motor carriers are already incentivized to run in the most compliant and safe manner, because it protects drivers' safety and promotes business success.

Perhaps the most concerning aspect of this proposal is FMCSA's failure to address the shortcomings and security risks associated with previous technology-based regulations, including the electronic logging device (ELD) mandate. There is insufficient recognition of the concerns motor carriers and drivers have continuously expressed about privacy and data security and no indications FMCSA has taken any meaningful steps to alleviate these concerns. Barreling forward with a new mandate involving the transmission of sensitive information only intensifies concerns involving identity theft, cargo theft, security threats, and more.

The proposed UEI mandate expands upon the warrantless search activities of both the federal government and its state partners. The Fourth Amendment to the U.S. Constitution (as well as similar provisions in most state constitutions) requires law enforcement officials to secure a warrant before searching private property unless the government can show that its search falls within a recognized exception to this warrant requirement. Courts have recognized such an exception where the government uses inspections to enforce an administrative scheme governing a "pervasively regulated" industry. *See, e.g.*, *New York v. Burger*, 482 U.S. 691, 702 (1987). Because participants enter into such industries with the knowledge that they will be subject to extensive regulation, they hold a decreased privacy expectation, and enforcement officials need not secure a warrant to search their premises for compliance with the administrative scheme. *See id.* Interstate trucking has been held to be a "pervasively regulated" industry subject to this exception.

Importantly, however, merely because an industry qualifies as "pervasively regulated" does not mean that industry participants lose all constitutional privacy protections. And just because the government may have established constitutional warrantless search activity in a pervasively regulated industry for some purposes, does not excuse the government from establishing the constitutional legitimacy of the expansion of its warrantless search activities into new areas.

Under federal law, these administrative searches must satisfy three requirements: (1) the warrantless inspection must advance a "substantial" government interest; (2) it must be shown that *warrantless* inspections are necessary to advance the government's interests; and (3) the inspection regulations must serve as a substitute for a warrant by sufficiently limiting officer discretion and the scope of inspections. *See id.* at 702-03. This standard defines the extent of the Fourth Amendment's privacy protections, but some states have held that their constitutions provide more protection for the privacy rights of individuals in pervasively regulated industries. *See, e.g., People v. Scott,* 79 N.Y.2d 474, 492-93 (1992).

[1] FMCSA Large Truck and Bus Crash Facts

Any proposed inspection scheme must comply with the applicable federal and state administrative search standards. The agency's proposal demonstrates that there remains much work to be done to ensure that any new inspection/identification scheme protects individual privacy rights in accordance with the Constitution. Many of the questions asked by the agency reveal that it is far from a forgone conclusion that warrantless UEI searches can be justified under the Constitution, as OOIDA details below.

In particular, the Notice does not discuss the need for a UEI search to have a defined scope – in the data that could be collected from UEI or the persons qualified to access them. The agency's questions suggest the agency is considering whether UEI transmit an expansive set of data to many different interested parties.

The proposal discusses the desire for the UEI search to improve safety in very general terms, but the Constitution demands that government searches, warrantless or not, be limited to discovering information that is relevant to determining violations of the law. The agency must make that connection to the law rather than generally to "safety."

OOIDA asks the agency to examine each of the questions posed in the proposal, as well as the comments submitted in response from the public, in the context of whether the UEI search would be permitted by the U.S. Constitution.

OOIDA submits the following comments and suggestions on this proposal, but reminds the agency we are adamantly opposed to advancing this rulemaking. We encourage the agency to abandon it entirely:

1. General

a. Should a device capable of transmitting an electronic ID be permanently affixed or removable/transferrable to CMVs currently in operation? Would FMCSA's rule need to specify?

> FMCSA has not provided any research demonstrating how the use of devices capable of transmitting an electronic ID would improve highway safety. The agency has proposed to include information for transmission that is already readily available to enforcement agencies. Therefore, OOIDA questions whether the purpose of this rulemaking is to advance the agency's mission or simply improve convenience for enforcement agencies.

b. What data should be included as part of the electronic ID (*e.g.*, carrier name, carrier contact information, vehicle ID number, license plate number, USDOT number, and gross vehicle weight rating)?

> Currently, all this information is readily available to enforcement agencies. It's transmission through a UEI is not necessary to ensure compliance with federal regulations or enhance highway safety. Additionally, law enforcement has already developed methods to automatically capture this information from moving vehicles. This proposal would only burden carriers with additional costs to provide records they are already required to make easily accessible.

Should the information be limited to non-PII information? If not, why not?

> We oppose any of this information being required in a UEI, but including PII is even less defensible for the reasons addressed below.

Should it include information specific to the driver (*e.g.,* hours of service, Commercial Driver's License compliance, and medical certification)?

> Absolutely not! Devices must not, under any circumstances, include information related to individual drivers. Again, this information is currently available to enforcement agencies, negating any need for it to be transmitted.
>
> Drivers are concerned about the scope of information that third-parties and enforcement agencies can already access. Having this information transmitted by a device has only increased these concerns, garnering universal opposition to this proposal among OOIDA members.
>
> Can the agency confirm this information can *only* be accessed by enforcement officers while a CMV is in operation? We have serious concerns about who may be able to access this information and what could potentially be done with it. The Federal Bureau of Investigation (FBI) has warned about information security problems related to ELDs, which also record and transmit sensitive information, but the agency has done little to resolve these issues. As a result, it's premature for FMCSA to move forward with another mandate that will further expose motor carriers and drivers to privacy and cybersecurity threats.

Should it also include information that may vary from trip to trip (*e.g.,* axle weight, pre-trip inspection date and time, and GPS coordinates and time when requested)?

> These factors do not help mitigate imminent safety hazards or identify high-risk carriers, and are therefore entirely unnecessary for real-time transmission to enforcement agencies. Furthermore, having to enter this information would create a new regulatory burden for motor carriers and drivers. Inclusion of this information would only add compliance work that takes away from their focus on safe operations.

Depending on how you answer the above questions, should the electronic ID be transferrable in the event of a CMV sale?

> The agency is considering including information specific to motor carriers and individual drivers for transmission. We have serious concerns about what happens to this data if the device is transferred to a new owner of a CMV. Can the devices be wiped of all information? Are motor carriers or drivers capable of doing this? What assurances would drivers have that their individual information has been removed by motor carriers?

Depending on how you answer the above questions, who should be responsible for providing the data set (see question 1.b.) associated with the electronic ID for a CMV (*i.e.*, driver, carrier, third party)?

> Drivers are already responsible for complying with too many regulations that have nothing to do with improving highway safety. It is absurd to consider holding them responsible for providing this data. If the device will be transmitting information unique to the driver, assurances must be made that this information is protected when being provided by a motor carrier or third party.

c. Depending on the scope of the data you believe is necessary in 1.b., how should the data be transmitted and received?

> Information should continue to be gathered through existing means, such as license plates, DOT numbers, and CDLs. Enforcement agencies already have access to this information, rendering this proposal wholly unnecessary.

Can existing technology (*e.g.*, ELDs) be used to collect and transmit the electronic ID data and receive a response from enforcement officials?

> No. Based on much of the information the agency is considering including in transmittable records, OOIDA believes this would represent an unreasonable departure from the authorized scope of the ELD mandate, which is solely permitted to determine compliance with hours-of-service requirements. 49 U.S.C. §31137(e)(3). We do not believe FMCSA has the authority to take this step.

How far in advance (time, distance) does a state need to gather the electronic ID information to positively ID a vehicle and message the vehicle whether further inspection is required?

> This question amplifies OOIDA's concerns that, under this proposal, the transmission of records will supersede observable safety hazards as the determining factor for conducting roadside inspections. We have serious concerns this will lead to an over-reliance on technology among enforcement officers. Rather than waiting for information to be transmitted, enforcement officers should continue to prioritize imminent safety hazards related to the condition of vehicle/equipment and driver behavior when deciding if a roadside inspection is warranted.

Should FMCSA propose a standard for the method of data transmission, and, if so, what should it be, or do you believe a voluntary standard can be developed?

> To truly improve highway safety, FMCSA should focus its resources on better identifying and mitigating imminent safety hazards on our roads. But generally speaking, the agency should implement more stringent security and certification standards for any technologies carriers are required to use. The failure of ELDs to fully protect sensitive information from cybersecurity threats and ensure basic compliance in some cases shows that self-certification does not work. Voluntary standards will allow device

manufacturers to implement features that go well beyond assessing compliance and allow for the collection and sale of additional motor carrier and driver data. We've already seen technology manufacturers, such as Google, be successfully sued for misleading customers into believing they had disabled location tracking when the provider continued to collect sensitive information. These concerns must be fully addressed before the agency considers moving forward with this rulemaking.

d. Are there reports or studies not already referenced above available regarding the use of electronic devices to identify CMVs that FMCSA may find useful in finding a technically sound, cost-effective, long-term means to identify CMVs at roadside? If so, please provide the references in your responses.

The reports and studies already associated with this proposal do not demonstrate how it would improve highway safety. CVSA's petition is largely built on assumptions, not the results of sound research. We are not aware of any additional research that would help justify the agency moving forward with mandating the use of UEI.

e. Should the electronic ID be limited only to CMV power units (*e.g.*, motorcoaches, truck-tractors) or also include trailers?

The more the agency broadens the scope of this proposal, the more costly, burdensome, and untenable it becomes. Is the agency suggesting a second device be installed on trailers or will a single device connected to the power unit include information for all equipment? Because trailers are often used by multiple drivers and in tandem with multiple power units, this creates serious concerns about who is responsible for providing and maintaining this information.

f. How would an electronic ID apply to rented or leased vehicles that are operated by different carriers or parties throughout the course of the year?

As we stated above, the complexity of factors like these render the proposal untenable. We envision the agency receiving multiple exemption requests, which will consume time and resources that could be better used advancing proposals with proven safety benefits.

g. How would or should an electronic ID be tied to States' CMV record keeping (*e.g.*, International Registration Plan registration, Performance and Registration Information Systems Management (PRISM))?

Compliance with these registration programs does not indicate whether a CMV or its driver poses an imminent threat to safety, which would necessitate a roadside inspection. Their inclusion in the transmission of records is wholly unnecessary.

h. Are there privacy, health, or coercion concerns FMCSA should consider in a future proposal?

Motor carriers and drivers have consistently expressed concerns about the use, transmission and retention of personal information or information related to their business when technology is involved, primarily because FMCSA has not taken the necessary steps to ensure privacy and security protection when implementing other technology-based mandates.

Additionally, we believe the mandated use of UEI will worsen driver retention problems within the trucking industry, which has correctly been a major concern for this administration. OOIDA members have expressed universal opposition to this proposal, believing it is yet another costly and burdensome regulation they will be forced to comply with despite the lack of any research demonstrating how these devices will improve safety, especially their own, or efficiency. The federal government can't keep piling on unnecessary regulations, especially ones that potentially involve the digital transmission of driver-specific information to anyone capable of receiving it, while claiming to be working to improve driver retention. If the administration truly cares about improving retention, it must listen to truckers about what is driving them from the industry.

2. Functionality

a. Should the electronic ID framework be flexible so that functionality could be added later, as new safety and other vehicle technologies emerge?

Absolutely not. This will further reduce the importance of identifying imminent safety hazards on our roads. Additionally, we envision this creating a scenario in which drivers are held responsible for technology malfunctions and deficiencies beyond their control. Furthermore, the functionality of technology may not be a determining factor in the safe operation of a CMV.

b. What operational and/or technical processes should be in place for handling situations where messages or data concerning the electronic ID do not send or receive correctly?

Even with a comprehensive certification process in place, it may be difficult for enforcement agencies and FMCSA to determine if a UEI has malfunctioned or if a driver is non-compliant. For example, if an enforcement officer "pings" a truck but doesn't receive a response, how will they determine if it was a device malfunction or failure to have the UEI engaged?

Furthermore, motor carriers and drivers should not be held responsible for any device malfunctions. Truckers are not technology experts or software developers.

c. How quickly can malfunctions in any electronic ID system be located and corrected?

Will drivers and/or owner-operators need to be trained to identify and remedy malfunctions in devices? Will drivers and/or owner-operators be expected to diagnose and fix any problems that arise with devices? How would time spent fixing problems be recorded for HOS compliance? Under the ELD mandate, if drivers experience a device

malfunction, they are required to use paper log as a substitute. How would drivers demonstrate compliance in the case of a UEI malfunction? Has there been any research to show where qualified software technicians who are capable of fixing malfunctions are located?

Drivers and owner-operators are not technology experts and should not be held responsible for malfunctioning devices. Because these devices have no connection to improved safety, requiring motor carriers and drivers to locate and correct malfunctions will dilute their focus on safely operating a CMV.

d. What cybersecurity issues (*e.g.,* "spoofing," and interference) should FMCSA consider in a future electronic ID proposal? Compare and contrast such concerns with the current electronic ID systems.

FMCSA must learn from its mistakes implementing earlier technology-based requirements, such as the ELD mandate, when determining how to address legitimate cybersecurity concerns related to UEI. The agency has failed to take legitimate concerns involving ELD security seriously, which resulted in the FBI issuing a Private Industry Notification (PIN) outlining numerous security issues with the devices. Specifically, the FBI noted:

"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."

The agency must assess and resolve all cybersecurity concerns related to similar technology-based mandates before taking any steps to mandate the use of UEI. This must include the establishment of a comprehensive certification process that prioritizes assessing and mitigating all cybersecurity concerns.

Additionally, does the agency plan to require that UEI only be "readable" by enforcement officers, or would device manufacturers be given discretion to allow other entities, such as truck stop operators, shippers, receivers, etc., to "ping" these devices? We imagine other businesses will have an interest in accessing this information, which raises even more privacy and security concerns.

e. How could tampering be prevented if some or all data entry or transfer is performed manually?

Drivers must not be responsible for manually entering or transferring data.

3. Populations Affected

a. What is the population of trucks that already have a type of electronic ID technology (*e.g.*, PrePass, Drivewyze)?

> While some motor carriers may use similar technology, such as PrePass, it is important to remember these programs are entirely voluntary. OOIDA members who made the decision to utilize these platforms are doing so because they believe it will improve their efficiency. The agency should be cautious to assume the use of these technologies would make UEI more palatable among motor carriers. Furthermore, we discourage the agency from relying on any data involving the safety records of motor carriers utilizing systems such as PrePass, as they often require a certain level of safety to participate, which would skew the universe of carriers studied.

b. What is the percentage of carriers that are not identified through current electronic screening capabilities? Please provide any supporting studies or reports.

> Enforcement agencies are currently capable of identifying all motor carriers through existing means. For example, in Kentucky, law enforcement has already implemented systems that can:
>
> *Capture images of the vehicle, the license plate, the USDOT and KYU numbers, and the inside of the cab. These images are fed to the Kentucky Automated Truck Screening (KATS) system where officers can quickly identify the vehicle and decide whether to send the vehicle for inspection. With the addition of the Driver Focus Camera, officers can now see the image of the driver in KATS along with all the vehicle's information, providing important safety data that was not captured before. Officers can use the image to flag the driver for further inspection or as evidence of a violation during a regular inspection.* [2]
>
> Given that enforcement agencies already have these capabilities, the agency's UEI proposal is duplicative and overreaching.

4. Cost/Benefits

a. What are the current and potential future safety benefits of electronic IDs?

> OOIDA is unaware of any research demonstrating how implementation of a UEI mandate would improve safety. CVSA has claimed, without providing any evidence, that this proposal would incentivize motor carriers to engage in safe and legal operations. We disagree with this unfounded claim. Motor carriers, especially small fleets and owner-operators, are already incentivized to operate safely and legally because it is good for their business and personal safety. FMCSA assumes the incentive for motor carriers would include avoiding unnecessary roadside inspections, but these possible benefits are far outweighed by concerns involving privacy, cybersecurity, cargo theft, driver

[2] HOW OBSERVING DRIVER BEHAVIOR IS IMPROVING SAFETY AND EXPEDITING PROCESSING FOR ONE KENTUCKY WEIGH STATION, Perceptics.com. https://perceptics.com/insights/46/how-observing-driver-behavior-is-improving-safety-and-expediting-processing-for-one-kentucky-weigh-station/

retention, and more. We strongly discourage the agency from advancing costly, burdensome, and wildly unpopular mandates based on nothing more than flimsy assumptions involving potential safety benefits.

We are also concerned this proposal may lead enforcement officers to focus too closely on records when determining if a roadside inspection of a CMV is warranted, rather than continuing to prioritize observable safety hazards.

Are there studies or reports that provide data to support the benefits of electronic IDs?

OOIDA is unaware of any research demonstrating this proposal would improve highway safety or efficiency.

Would implementing an electronic ID requirement lower crash rates, if so, how?

OOIDA is unaware of any research demonstrating this proposal would lower crash rates.

b. How would requiring an electronic ID impact the overall effectiveness of State CMV inspection programs?

When determining the need for a roadside inspection, this proposal would shift too much focus away from observing imminent safety hazards to assessing records. We note none of the ten most common factors leading to a fatal crash involving a CMV that FMCSA has identified are addressed within this proposal. CVSA claims this rulemaking would allow them to better target high-risk carriers for roadside inspections, when enforcement agencies should instead conduct inspections based on imminent safety hazards, including vehicle/equipment conditions and driver behavior. Furthermore, OOIDA questions the validity of the processes in place to determine supposed high-risk carriers. Since their inception, these systems have failed to decrease crash rates, indicating they are incapable of identifying carriers and drivers that are at the highest risk of crashing.

c. How much time would compliant motor carriers save if an electronic ID were to be required?

This question is impossible to answer. For one, how is the agency defining “compliant”? Additionally, if this proposal were to be adopted, are we to understand that enforcement agencies would never conduct an inspection on a carrier with “compliant” data? Finally, given that motor carriers range from single-truck operators to fleets of thousands of CMVs, it is meaningless to try to make a general statement about how much time a carrier would save.

Furthermore, it is equally important to consider how much time would be wasted inspecting supposed “high-risk” carriers that did not demonstrate any imminent safety concerns, as well as the time taken to program and update the information in the device, and fix any malfunctions. This mandate would likely cost small carriers more time to ensure compliance than would be saved.

d. What is the cost of adding electronic ID technology by type (*e.g.*, transponder, wireless, software, etc.)?

> Additional technology requirements always come at a cost, which is especially difficult for small carriers and owner-operators. Purchase, installation, maintenance and service of devices would increase operating costs for all motor carriers, without any proven benefit to efficiency or safety. Truckers are already experiencing elevated operating costs. There's absolutely no reason to raise those costs even higher.

e. What is the cost of electronic ID equipment for States, carriers, and drivers?

> This question is concerning, as it implies the agency is considering holding drivers responsible for the purchase and use of UEI. This would impose new costs and burdens on individual drivers at a time when inadequate driver compensation and increasingly difficult working conditions are contributing to poor retention across our industry, which this administration has correctly identified as a serious concern.

f. What is the cost of maintaining/operating electronic ID equipment (*e.g.*, internet connection, inspection, repair, third party contracting fees, etc.)?

> Because these devices do nothing to improve efficiency or safety, motor carriers will only see their costs increase. Requirements and costs continue to rise without positively affecting highway safety, and this proposal will only compound these problems.

g. What is the additional administrative burden (time and costs not already associated with vehicle or carrier registration) for registering the electronic ID and updating the registration as necessary to ensure that it is associated with the current motor carrier responsible for safety?

> Given the lack of specificity in this proposal and the wide range of possible requirements, it is difficult to estimate the burden, but for a small trucking business or owner-operator, administrative expenses for registering and updating a UEI will be especially high. Within this proposal, the agency has considered holding both motor carriers and/or drivers responsible for UEI compliance. Owner-operators are both the owner of a trucking business and the operator of a CMV, meaning they would be required to comply with requirements imposed on both motor carriers and drivers.

5. Other

Is there any other information associated with electronic IDs that FMCSA should consider? Please describe.

> Many states require an enforcement officer to use the probable cause statute before stopping a vehicle, including a CMV. Probable cause means an officer has sufficient reason, based upon known facts, to believe a crime has been committed or that certain property is connected with a crime. Where has the agency established that a motor

carrier's safety record can itself be sufficient probable cause to justify the search of a vehicle or driver? Even if receiving information from a UEI could be used to establish probable cause, such information must be reasonably calculated to determine whether or the law has been violated. One important component of that standard would be that the information transmitted from the device is accurate. To date, we are unaware of any tests or certifications that would prove that the information enforcement officers can access is correct. In fact, we know that some of the data the agency is proposing for transmission from a UEI have been found to be inaccurate on a regular basis. Having an officer sitting on the side of the road or at a facility utilizing UEI could represent a violation of the driver's fourth amendment rights.

Thank you for your consideration of these comments and suggestions. We encourage FMCSA to immediately abandon this proposal. We plan to vigorously oppose any subsequent steps the agency takes to mandate the use of UEI.

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