To whom it may concern,

Recently a story broke that the Pentagon is doing an investigation on an exercise tracker with GPS capabilities. Evidently, the Pentagon has a concern for the safety of their personnel and their ability to win future battles when their soldiers can easily be tracked. Who can blame them?

The truck drivers of the United States have a similar concern. The Federal Government forces trucking companies to install telematics devices with GPS and wifi capabilities. They feel that criminals of organized crime may have the ability to track trucks with high value freight and shut down the truck at their convenience to commandeer the vehicle. They may use a GPS jammer (illegal to use in the U.S. but easily purchased) to prevent the truck from being tracked any further. The FBI states that freight theft is a 30 billion dollar a year business for organized crime. What will it be by the end of this year with these tracking devices in every truck? If that's not bad enough, what happens if terrorist decide to override the computer system in a truck and use it as a form of attack in big cities? Such as the one that happened on July 14, 2016, in Nice, France.

Enclosed is the **Report on the Risk Of Cyber Security Threats From Electronic Logging Devices.** I hope that you will take this issue seriously because it is a great concern for the American truck driver.

Sincerely,

The American Truck Drivers

Truckers Report On The Risk Of Cyber Security Threats From Electronic Logging Devices

Report on the Risk Of Cyber Security Threats From Electronic Logging Devices

The warnings came, regarding the vulnerability to remote takeover, as early as 1999, in a book by Furnelb & Warren , 1999 - In which they warn: "Cyber terrorists operate with a political agenda which means that these types of attacks, using telematics, will be more specifically targeted and aimed at more critical systems."

In 1998, Werner Transportation, in conjunction with FMCSA, installed an early form of telematics elds. I don't believe in coincidences, do you? Nineteen years later, we have a whole nation being crisscrossed by 3 Million telematic targets.

During eld hearings, on FMCSA's own website in 2011, an independent testing laboratory wrote: that "ELDs are too expensive and too open to takeover via the two way signal they use to operate. The lab recommended the flash drive/ USB device and the DOT enforcement community concurred."

A major manufacturer replied: "Given availability of more secure transmission mechanisms such as transmitting electronic driving records via a central server (telematics) we see no practical reasons why FMCSA should allow transmitting electronic driving records via wired USB connections." Seven years later, we have 3 million telematic targets cruising our highways.

In April 3, 2014 - https://www.roanoketrade.com/cyber-liability-risks-transportation-logistics-companies/ In a recent report by PricewaterhouseCoopers, "Transportation & Logistics 2030, Volume 4: Securing the Supply Chain," Data via web-based applications, (telematics) are vulnerable to hackers and CAN ALSO ATTRACT CARGO THIEVES. Twenty months later, 3 million telematic targets roam the nation.

In 2016, this same manufacturer that wrote of the "more secure transmission" of telematics, admitted: "Now consider the complexities of a vehicle network and telematics devices that essentially connect the vehicle to the Internet and you start to the potential safety and security threats to a vehicle." http://www.fleetequipmentmag.com/hack-heavy-duty-truck/

Two years later, we share the road with 3 million of their telematic customers.

As you can see, in the interim between 1999 and now, the warnings of telematic danger have only increased in their insistance that we are putting our nation at risk with these hackable devices. Yet now, all we can do is hold our collective breaths, waiting for the first truck to draw the short straw, to become a suicide bomber, on a highway near us.

We first were alerted to the dangers of telematics from reading an article in a trucking magazine, in August of 2016, about the University of Michigan Transportation Research Department's published study of their successful hacking of the telematics of a semi. This study was a computer class project at the University, where the students took only two months to devise a way to hijack the truck's brakes, system controls and engine. -/www.wired.com/2016/.../researchers-hack-big-rig-truck-hijack-accelerator-brakes. The U of M researchers were keen to delve into the likelihood of carrying out the same type of hack, remotely via the telematics links.

Being properly horrified at this doomsday scenario, I took to doing my own research, online. Everything I will present to you is freely available to anyone. The most surprising discovery of my numerous discoveries, was how all this vital information was systematically ignored by our own DOT and the manufacturers of these telematic devices.

In August 2016: Following the use of a heavy-duty truck in a terrorist attack in Nice, France, in July, Assistant U.S. Attorney General John Carlin told Trucks.com that the federal government was worried that an increasing array of autonomous driving features, which is the installation of telematics, in trucks could turn them into terrorist weapons.

Dec 12, 2016 – Nearly a year after the mandate was published, NHTSA warns of this: www.encompassrisksolutions.com/2016/12/27/nhtsa-updated-cyber-security-guidelines-are-you-protected Cyber-attacks pose significant risks for both employers and employees. For example, successful cyber-attacks can TAKE COMMAND OF VEHICLE CONTROLS.

Sept 2017 – Three months before the final imposition of elds,

http://tanktransport.com/2017/09/cyber-attacks-threaten-trucking/ "It's not far-fetched to imagine cyber terrorists causing a driver to lose control of the safety-critical functions of his 80,000-pound truck as the result of a cyber attack. Such a scenario could potentially have devastating results. Attacks on a truck's physical systems pose a costly threat to the transportation industry not only in terms of physical equipment and goods, but more importantly,

human lives."

www.fleetowner.com/blog/data-breaches-it-s-4-million-incident-problem-now-0

We know that criminals are starting to use jammers to carry out crimes. For example, in Italy gangs have been targeting shipments of scrap metal. They hijack a truck, force the driver to pull over, hold the driver captive and then use a GPS jammer so the cargo can't be tracked as they drive off with it." In fact, industrial vehicles that often include telematics systems for fleet management may be easier to hack remotely than consumer vehicles.

Incidents are starting to be reported in that the eld can suddenly malfunction just from a hidden glitch within it, or when the device is remotely upgraded.

"Owner-operator Chris Guenther knows what it feels like to lose some control over a truck's electronics. Last summer, his Omnitracs telematics began switching log statuses flickering on and off. "My dashboard started popping all kinds of engine and re-gen codes," Guenther says. "The truck then de-rated" slightly, but he was many miles away from a good place to get service or even pull off. Guenther called the shop that had just worked on the truck and was referred to Omnitracs, when the MCP50 shut down, so did my engine – 5 times." If a simple malfunction or a remote reboot can shut just the engine down, just imagine what a well organized attack could accomplish.

The same computer chips that are in elds, are also used in the military.
www.theguardian.com/technology/2012/may/29/cyber-attack-concerns-boeing-chip
Researchers claim chip used in military systems and civilian aircraft has built-in function that could let in hackers. "The real issue is the level of security that can be compromised through any back door, and how easy they are to find and exploit," Woods said, "a back door is an additional undocumented featured deliberately inserted into a device for extra functionality" – in effect, a secret way to get into the chip and control it." Telematics need this back door to operate. But we do not need this defective device in order to safely operate commercial motor vehicles.

I don't claim to be a lawyer or a policy maker, but I do know that by ignoring all these public warnings, our government has put us in grave danger. Recently, on January 11 of this year, FBI Director Christopher Wray, gave another speech on the FBI's increased concern on cyber attacks at Fordham University. In March 18, 2016 - The FBI says car hacking is a real risk - Help Net Security The FBI stated that it considers ... hacking a real and present danger, and so should the general public and vehicle manufacturers. ... with the Telematics Gateway Unit (TGU). This device can leak sensitive data, and the FBI has posited that the VEHICLES THEMSELVES PERHAPS CAN BE MANIPULATED VIA THE DEVICE.

The risk of injury or death from telematics far exceeds the estimate of lives supposedly saved by this defective device. FMCSA estimates 26 lives will be saved. Just one telematics hijacking in the Holland Tunnel will exceed this toll.

The risk will be amplified in the very near future as carriers rush to the autonomous trucks to save wages. Since autonomous trucks will only work using the same defective telematics, the perfect storm of tragedy is now poised to take us all down.