AMERICAN TRUCKING ASSOCIATIONS
950 N. Glebe Road ★ Suite 210 ★ Arlington, VA ★ 22203-4181
www.trucking.org

NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION
U.S. DEPARTMENT OF TRANSPORTATION
DOCKET # NHTSA-2020-0087

Request for Comments:
Cybersecurity Best Practices for the Safety of Modern Vehicles

SUBMITTED BY:
American Trucking Associations
950 North Glebe Road, Suite 210
Arlington, VA 22203

March 15, 2021

Primary Contact:
Ross Froat
ATA
Director of Technology & Engineering Policy
rfroat@trucking.org

The American Trucking Associations, Inc. (ATA) submits these comments to the National Highway Traffic Safety Administration (NHTSA) in response to the January 2021 notice of request for comments[1] on the Agency's updated draft cybersecurity best practices document, *Cybersecurity Best Practices for the Safety of Modern Vehicles* ("2020 Best Practices").[2]

As the national representative of the trucking industry, ATA has a strong interest in matters affecting commercial motor vehicle (CMV) design, security, maintainability, and the cybersecurity posture on which our Nation's businesses rely. Employing more than 7.9 million people and moving nearly 12 billion tons of freight annually,[3] trucking is the industry most responsible for moving America's economy. Approximately 37 million trucks (all commercial classes) move more than 80 percent of our Nation's domestic freight and are considered critical infrastructure assets in the safety and security of our nation's roadways.

As these statistics demonstrate, trucking is an integral component of our Nation's transportation system and economy. The industry has a substantial stake in best practices regarding cybersecurity for transportation safety and stakeholder business productivity. Directly and through our affiliated organizations, ATA's united federation of motor carrier and allied members, state trucking associations,

[1] 86 Fed. Reg. 2481. (Jan. 12, 2021).
[2] NHTSA. (2020). *Cybersecurity Best Practices for the Safety of Modern Vehicles*. Washington, DC. USDOT. Found in Doc. NHTSA-2020-0087.
[3] ATA. (Aug. 2020). *American Trucking Trends 2020.* Arlington, VA. Found at https://www.trucking.org/news-insights/ata-american-trucking-trends-2020.

and national trucking conferences and councils represent nearly 40,000 industry stakeholders in the United States – encompassing nearly every type of business that supports trucking. Our allied members include original equipment manufacturers, supply chain and logistics companies, retail corporations, and technology firms – all engaged in improving industry cybersecurity and defending against cyber threats and attacks.

ATA is committed to improving highway freight transportation cybersecurity and commends NHTSA for taking action in updating the Agency's 2016 cybersecurity best practices document, *Cybersecurity Best Practices for Modern Vehicles* ("2016 Best Practices").[4] NHTSA's 2016 Best Practices supports industry-led efforts that improve the cybersecurity posture of automotive companies and stakeholders. It provides perspective on how to develop and apply risk-based cybersecurity management processes during the vehicle's lifecycle. ATA supports the latest 2020 Best Practices draft and offers the following supportive and constructive comments.

I. 2020 Update of Cybersecurity Best Practices

NHTSA's 2020 Best Practices builds upon agency research and industry progress since 2016, including emerging voluntary industry standards and best practices structured around five key areas: (1) General Cybersecurity Best Practices, (2) Education, (3) Aftermarket/User Owned Devices, (4) Serviceability, and (5) Technical Vehicle Cybersecurity Best Practices. In addition, the notice and draft update reference supporting ISO/SAE 21434 *Road Vehicles—Cybersecurity Engineering;* best practice guides developed by the Automotive Information Sharing & Analysis Center (Auto-ISAC), and findings from NHTSA research and workshops. ATA supports ISO/SAE 21434 and views its focus throughout the 2020 Best Practices to be an industry priority. ATA and the Auto-ISAC are strategic partners through ATA's Fleet CyWatch program and work together to improve the cybersecurity posture of all vehicle manufacturers and operators, reporting incidents and preventing the spread of cyber threats. ATA is also pleased with the Agency's continued partnership in providing the Vehicle Cybersecurity Workshops that raise industry awareness through resources and education.

A. ATA Fleet CyWatch, General Cybersecurity Best Practices & Education

Fleet CyWatch is an ATA Technology & Maintenance Council (TMC) and Transportation Security Council-supported[5] program that assists members in reporting trucking-related internet crimes and cyber-attacks. The program's purpose is to alert industry of potential cyber threats and serving as an information sharing and analysis organization (ISAO). In 2016, the FBI tasked ATA with initiating an ISAO that would coordinate federal and industry activities and provide a mechanism for stakeholders to exchange information about potential and actual cyber threats and incidents. In response to the FBI's request, ATA launched the Fleet CyWatch program[6] to assist members in reporting cybercrime, direct

[4] NHTSA. (Oct. 2016). *Cybersecurity Best Practices for Modern Vehicles*. Washington, D.C. USDOT. Found in Doc. NHTSA-2016-0104.
[5] ATA's councils are divisions of the ATA Federation focused on motor carrier issues at a granular level producing industry solutions to its particular areas of expertise.
[6] ATA. (February 2018). *ATA Fleet CyWatch*. Arlington, VA. Found at https://www.trucking.org/fleet-cywatch.

best practice solutions, and maximize relevant cybersecurity awareness through bimonthly information sharing notifications.

Fleet CyWatch coordinates with private and federal efforts to provide manufacturers and motor carriers with information and recommendations in the areas of cybersecurity awareness, prevention, and mitigation methods. The 2020 Best Practices sections *4) General Cybersecurity Best Practices* and *5) Education* list 38 *General best practices* ATA supports and actively promotes with trucking industry stakeholders through Fleet CyWatch and TMC. ATA's TMC[7] is a prime example of how industry comes together to face trucking equipment issues. In many ways, cybersecurity is becoming increasingly important as vehicle design, operation, aftermarket onboard technologies, and serviceability become more connected and technologically sophisticated. TMC has incorporated cybersecurity into many of its Recommended Practices[8] and leads company-based practices in its Cybersecurity Issues Task Force. Many of these practices are also applied in training at TMCSuperTech, where technicians demonstrate their skills at the "CyberTech" skills station.[9] Other commercial vehicle cybersecurity activities include the CyberTruck Challenge[10] and the National Motor Freight Traffic Association's heavy vehicle cybersecurity workshops.[11] As the Agency updates its cybersecurity best practices, it should identify existing best practices and educational resources for the trucking industry and note the impact of programs like Fleet CyWatch.

B. Aftermarket/User Owned Devices & Serviceability

The 2020 Best Practices sections *6) Aftermarket/User Owned Devices* and 7*) Serviceability* list five *General best practices* that ATA supports, but emphasizes the importance of vehicle-generated data ownership and serviceability. Commercial vehicles generate data from onboard and off-board systems regarding information that may involve vehicle performance, cargo status, and navigation connectivity that can be used for system diagnostics, identifying freight, and an intelligent transportation network. ATA supports government and industry initiatives to ensure that vehicle ownership conveys the following rights of access and control to the vehicle's owner and owner's designees:

- Direct access to data collected, generated, recorded or stored by the vehicle.
- Access to and use of operator data which may be personally attributable or identifiable, including driver behavior data and geolocation data, and right to grant or limit access to this data by other parties.
- A dependable, low-risk means of interfacing with the vehicle to retrieve data.

---

[7] TMC is a diverse group of industry professionals who work together to improve truck equipment and technology. TMC's priority is to provide industry-recognized best practices for fleet managers to specify and maintain vehicles, and provide guidance to manufacturers in the design of their equipment. Found at https://tmc.trucking.org/.
[8] TMC. (2020). *TMC 2020-2021 Recommended Practices Manual*. Arlington, VA. ATA.
[9] TMCSuperTech is the trucking industry's annual national event for state competitions, technicians, and students.
[10] The CyberTruck Challenge is a Michigan event that tests heavy vehicle cybersecurity vulnerabilities and develops talent to address those issues. Found at https://www.cybertruckchallenge.org/.
[11] NMFTA works to educate the industry on potential cyber threats to connected vehicle fleets. NMFTA hosts industry workshops exploring cyber security issues. Found at http://www.nmfta.org/pages/HVCS.

To foster safety and innovation, the U.S. Department of Transportation (DOT) should support and not restrict aftermarket maintenance and serviceability of vehicle systems and component technologies. ATA supports motor carriers' freedom of equipment maintenance and serviceability through both manufacturer and aftermarket solutions providers. NHTSA should support the development and harmonization of industry-recognized standards and best practices – such as those developed or adopted by TMC – to assist in the safety, design, performance, and maintainability of CMV equipment.

C. Technical Vehicle Cybersecurity Best Practices

The 2020 Best Practices section *8) Technical Vehicle Cybersecurity Best Practices* list 23 *Technical best practices* that ATA supports and commends the Agency for remaining non-binding, providing voluntary cybersecurity best practices to stakeholders. ATA is pleased with the research findings of DOT's *Cybersecurity Research Considerations for Heavy Vehicles*[12] and *Cybersecurity Best Practices for Integration/Retrofit of Telematics and Aftermarket Electronic Systems into Heavy Vehicles*.[13] Collectively, DOT has established a solid foundation that guides the design, manufacture, and operations of CMVs. This signifies our shared goals in improving transportation safety and freight delivery productivity.

II. Conclusion

ATA thanks NHTSA for the opportunity to provide feedback on this request for comments. Seeing the Agency request industry feedback on vehicle cybersecurity underscores NHTSA's continued commitment to safety and transportation security. ATA looks forward to working with the Agency to educate manufacturers, motor carriers, and the supplier industry about these best practices once finalized. We welcome future opportunities to provide feedback. If you have additional questions, please feel free to contact me by phone at (703) 838-7980 or at rfroat@trucking.org.

Sincerely,

Ross Froat
Director of Technology & Engineering Policy
American Trucking Associations

[12] NHTSA. (Dec. 2018). *Cybersecurity Research Considerations for Heavy Vehicles.* Washington, DC. USDOT. Report No. DOT HS 812 636.
[13] FMCSA. (May 2020). *Cybersecurity Best Practices for Integration/Retrofit of Telematics and Aftermarket Electronic Systems into Heavy Vehicles*. Washington, DC. USDOT. Report No. FMCSA-RRT-19-013.