BEFORE THE

NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION

UNITED STATE DEPARTMENT OF TRANSPORTATION

COMMENTS OF THE

NATIONAL MOTOR FREIGHT TRAFFIC ASSOCIATION, INC.
1001 NORTH FAIRFAX STREET, SUITE 600, ALEXANDRIA, VA 22314

IN RESPONSE TO NHTSA'S REQUEST FOR COMMENT ON

CYBERSECURITY BEST PRACTICES FOR THE SAFETY OF MODERN VEHICLES
Draft 2020 Update

[Docket No. NHTSA-2020-0087]

March 11, 2021

I. INTRODUCTION

These comments are submitted on behalf of the National Motor Freight Traffic Association, Inc., (NMFTA) in response to a request by the National Highway Traffic Safety Administration (NHTSA) for comments on January 12, 2021, entitled "Request for Comment on Cybersecurity Best Practices for the Safety of Modern Vehicles", Docket No. NHTSA-2020-0087.

II. STATEMENT OF INTEREST

NMFTA is a nonprofit membership organization headquartered in Alexandria, Virginia, whose mission is to promote, advance and improve the welfare and interests of its members and the motor carrier industry. NMFTA's current membership is comprised of approximately 500 motor carriers operating in interstate, intrastate and foreign commerce, primarily specializing in the movement of less-than-truckload quantities of freight (LTL). NMFTA's member carriers operate a combined total of more than 190,000 power units.

NMFTA has an ongoing cybersecurity program focused on the identification of vulnerabilities impacting heavy vehicles. The program also offers cybersecurity-specific education and training opportunities, as well as producing white papers directed to our membership and industry that outline potential vulnerabilities and offering recommendations for medium- and long-term actions meant to expand security protocols and more effective responses to attacks.

NMFTA hosts semi-annual conferences for the heavy vehicle industry, including OEM manufacturers, tier-one suppliers, cybersecurity companies, trucking companies, U.S. and Canadian federal government agencies, U.S. military, and university-based researchers focusing on ground vehicle cybersecurity issues.

II. COMMENTS

NMFTA has reviewed NHTSA's 2020 draft version of its *Cybersecurity Best Practices for the Safety of Modern Vehicles* and offers the following comments:

Section 4.1 – Leadership Priority on Product Cybersecurity

> [G. 2] [a] Combining the validation of product cybersecurity measures and vulnerabilities ill-defines the focus of the organization. These should be separate measures, i.e. vulnerabilities are not implemented. The guidance could be better framed as the organization having a vulnerability disclosure program. We suggest deleting 'and vulnerabilities' from [a] and adding a new '[d] Implementing a Vulnerability Disclosure Program (VDP)…'. For further details of good VDPs we suggest consulting and referring to CISA BOD 20-01 https://cyber.dhs.gov/bod/20-01/.

Section 4.2.1 – Vehicle Development Process with Explicit Cybersecurity Considerations, Process

[G.3] This wording unintentionally conflates security and safety; security requires different approaches than safety.

Section 4.2.3 - Vehicle Development Process with Explicit Cybersecurity Considerations, Sensor Vulnerability Risks

[G.6] The inclusion of machine learning false positives excitation along with sensor spoofing is a conflation of different concepts This should be an [a] and [b] guideline. Active safety or other sensor-based systems do not need to use machine-learning. The phrasing of this guideline implies that manufacturers could focus on any one of the list ("OR excitation of …) whereas the manufacturers should focus on both sensor issues and machine learning issues.

Section 4.2.5 – Vehicle Development Process with Explicit Cybersecurity Considerations, Protections

[G.9] Recommend clear cybersecurity _requirements_ (as opposed to the current 'standards' recommended – which do not yet exist) be communicated to suppliers and that these requirements be backed up by informative outward references.

Section 4.2.7 - Vehicle Development Process with Explicit Cybersecurity Considerations, Penetration Testing and Documentation

[G.14] The draft language "…highly incentivized to identify vulnerabilities" intuits financial incentives for finding bugs rather than focusing on a holistic quality assurance process that includes cyber as an integral part of the process.

[G.15] "Disposition of the vulnerability" is not appropriate for non-technical recommendations. The guidance can simply explain the need for analysis to indicate the degree to which the known vulnerability can be exploited in the current software implementation and configuration.

Section 4.2.11 - Vehicle Development Process with Explicit Cybersecurity Considerations, Industry best practices

[G.23] While the Auto-ISAC has produced good best practices, it is not a standards development organization and should not be characterized as one. We also suggest adding participation in SAE and ATA TMC.

Section 4.4 – Security Vulnerability Reporting Program

[G.26] Add a reference to CISA BOD 20-01 is a good directive for creation of a high-quality vulnerability disclosure program

Section 4.5 – Organizational Incident Response Process

[G.29] Disposition of the “vulnerability" is not appropriate for non-technical recommendations. The guidance should simply explain the need for analysis to indicate the degree to which the known vulnerability can be exploited in the current software implementation and configurations.

Section 5 – Education

[G.38] Section should include references to the SAE CyberAuto Challenge and the CyberTruck Challenge as exemplar events that promote education and community. [https://www.sae.org/attend/cyberauto] [https://www.cybertruckchallenge.org/]

Section 6.1 – Aftermarket/User Owned Devices, Vehicle manufacturers

[G.40] The authentication should be present. However, delegation of trust of the authentication and of the subsequent authorization must be under the control of the vehicle owner or long-term lessee. This is very important because without these provisions the resulting vehicle network protections will result in protection of the vehicle bus access from the owners of the vehicle. i.e. it would violate G.43.

The final document should clearly define the range of third-party devices that are connected to a vehicle to which the guidelines will apply. The final document should also clearly state if this requirement will encompass yet to be identified future devices that may be added as a result of technological advancement.

NMFTA also suggests that the authentication authority be named as the current owner or lessee of the vehicle.

Section 7 – Serviceability

This section is focused almost exclusively on passenger vehicles. NMFTA suggests it be expanded to include consideration of both heavy vehicle and trailer service lifetimes.

Section 8.2 – Technical Vehicle Cybersecurity Best Practices, Cryptographic Credentials

NMFTA suggests that the need for cryptographic resilience and obsolescence be explicitly stated.

Section 8.4 - Technical Vehicle Cybersecurity Best Practices, Diagnostic Tools

[T.8] Similar to comments above on [G.38], this guideline may conflict with the “right to repair” and our fleet interests. i.e. G.43. This guideline should clearly state that ultimate trust for the authentication authority be named as the current owner or lessee of the vehicle.

Section 8.5 – Technical Vehicle Cybersecurity Best Practices, Vehicle Internal Communications

[T.9] The document has already defined third-party devices and access previously. NMFTA suggests that be used here instead of using “external vehicle interfaces"

[T.10] NMFTA recognizes the importance of message authentication, however, requiring Message Authentication Codes (MAC) to the vehicle network (without also requiring the authentication authority be the vehicle owner or lessee) will result in excluding vehicle bus access from the owners of the vehicle, i.e. it would violate G.43. Furthermore, message authentication does not mitigate the risk of remote message spoofing because an ECUs whose code is compromised would be capable of creating messages which are ‘authenticated’ using the Message Authentication Code.

Section 8.9 – Technical Vehicle Cybersecurity Best Practices, Over-the-Air (OTA) Software Updates

NMFTA suggests a deeper explanation of, as well as resources on, over-the-air software updates be provided in the document. We also recommend referring to the UPTANE [https://uptane.github.io/] design for secure OTA.

III. CONCLUSIONS

This document, while providing guidance on the critical step of establishing internal processes and strategies to mitigate cyber risk, relies heavily on ISO/SAE 21424. We suggest the guidance be expanded to address the real-world conditions impacting vehicle cybersecurity across their entire lifecycle. NMFTA strongly believes that ultimate authentication and authorization control be vested in the vehicle owners and long-term lessees, rather than equipment suppliers. The vehicle owners and long-term lessees have day-to-day control of the operation of these vehicles and are often responsible for maintenance. The recommendation to add message authentication to the vehicle networks adds more complexity than benefit, as well as introduces impediments to legitimate diagnostics and the customization of vehicle networks.

Also, we recommend the inclusion in Section 4.1 of an additional reference on vulnerability disclosure systems:

- Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) CISA Binding Operational Directive (BOD), BOD 20-01.

Respectfully submitted,

National Motor Freight Traffic
Association, Inc.

Paul G. Levine
Executive Director

Urban Jonson
Chief Technology Officer