NMFTA
National Motor Freight
Traffic Association, Inc.

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 MODERN VEHICLES

NHTSA-2016-0104

November 28, 2016

I. INTRODUCTION

These comments are submitted on behalf of the National Motor Freight Traffic Association, Inc., (NMFTA) in response to a request for comments on October 28, 2016, entitled “Request for Comment on Cybersecurity Best Practices for Modern Vehicles," NHTSA-2016-0104.

II. STATEMENT OF INTEREST

NMFTA is a nonprofit membership organization headquartered at 1001 North Fairfax Street, Suite 600, Alexandria, VA 22314. Its membership is comprised of approximately 550 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’s mission is to promote, advance and improve the welfare and interests of its members and the motor carrier industry in general. NMFTA presents its members’ position in relevant judicial, regulatory and legislative proceedings.

II. COMMENTS

NMFTA initiated a project on the cybersecurity vulnerabilities of heavy vehicles in January 2015 in response to its members’ concerns of the potential cyber weaknesses in their vehicles. A white paper entitled *A Survey of Heavy Vehicle Cyber Security* was issued on September 21, 2015 outlining potential vulnerabilities and consequently their potential impact on its members’ operations. The white paper also includes recommendations for medium and long-term actions that could encourage better product security and more effective responses to attacks. Since December 2015, NMFTA has hosted three conferences for members of the heavy vehicle industry, including OEM manufacturers, tier one suppliers, cybersecurity companies, trucking companies, U.S. and Canadian federal government agencies, and the U.S. military to get together to discuss vehicle cybersecurity issues. NMFTA is also sponsoring research on this subject at two major universities. At the recently concluded heavy vehicle cyber security meeting, the group reviewed NHTSA's Cybersecurity Best Practices for Modern Vehicles and came up with the following recommendations:

- NHTSA's recommendations appear to be primarily directed to the passenger car and light truck segments of the automotive industry. These vehicles are almost always completely constructed by their original equipment manufacturers with a limited number of optional components and usually do not have additional devices connected to the vehicle CAN bus post-manufacture. Conversely, the manufacturers of heavy vehicles offer an extremely wide variety of components, the vehicles are often completed by outside parties, and additional components, such as electronic logging devices (ELDs), are often added to the vehicle CAN bus by these outside parties or the fleet owners themselves.
- The second bullet in section 5.1 states "Provide for timely detection and rapid response to potential vehicle cybersecurity incidents in the field." With light vehicles, the dealer or manufacturer is involved in installing or pushing out software updates to vehicles. With heavy vehicles, such maintenance is often handled by the fleet owners themselves so timely distribution of software patches to these entitles should be included in the recommendation. It should

be noted that heavy vehicle fleet operators will often delay implementation of software patches and updates until they can be tested to confirm that no conflicts occur with components that were added to the vehicle after delivery from the OEM.

- 6.3 Information Sharing—reference is made to the Auto ISAC. Due to the differing nature and use of heavy vehicles, the industry is seriously considering the creation of a Commercial Vehicle ISAC. It is anticipated that the CV ISAC and Auto ISAC would work closely together on issues of common concern, such as intelligence sharing and development of cyber-incident responses.
- 6.7.1 Limit Developer/Debugging Access in Production Devices—we suggest physically removing connectors and pins used only for developer access.
- 6.7.5 Limit Ability to Modify Firmware—we recommend digital signing in accordance with the most recent version of FIPS 140.
- 6.7.6 Control Proliferation of Network Ports, Protocols and Services—heavy vehicles use a variety of network interfaces; i.e. Bluetooth, satellite, and cellular. Whatever is not needed should be turned off by default. Furthermore, these network interfaces should not be routed, bridged or otherwise connectable.

The group further recommended that SAE J 3010 be referenced. This standard defines a common set of requirements for security to be implemented in hardware-protected security for ground vehicle applications.

Supply chain procurement should follow best practices when acquiring components. The cybersecurity of suppliers of components that plug into the vehicle CAN bus should be verified before they are installed in the vehicles.

III. **CONCLUSION**

Heavy vehicles differ from passenger cars and trucks in their design, function and operation. Heavy vehicle operators need the ability to connect additional equipment into the vehicle CAN bus beyond what is installed by the factory. Manufacturers of the vehicles and components should be encouraged to validate the cybersecurity of the components they purchase from their suppliers. For these reasons, we request that the suggested changes shown above be included in NHTSA's Cybersecurity Best Practices for Modern Vehicles.

Respectfully submitted,

National Motor Freight Traffic
Association, Inc.

Paul G. Levine

Paul G. Levine
Executive Director