National Motor Freight Traffic Association, Inc.
1001 North Fairfax Street, Suite 600
Alexandria, VA 22314
(703) 838-1810

Heavy Vehicle Cyber Security Bulletin

Bulletin Name	Issue Date	Last Updated	Version
Heavy Vehicle Cyber Security Bulletin	September 8, 2016	May 30, 2018	1.5

In 2013 there were approximately 10.6 million heavy vehicles registered in the US. It is estimated that class 8 trucks, which constitute the heaviest of these vehicles, have a service life of 7-8 years, with approximately 150,000 new class 8 trucks added to the fleet each year.

Heavy vehicles – while having some obvious material differences – are substantially similar in network architecture to light vehicles. Therefore, there is no reason to believe that heavy duty vehicles are less vulnerable to cyber security threats than the average automobile. The difficult part of hacking vehicles is gaining access, ideally *remote* access. Indeed, while passenger vehicles are just now becoming "connected" through telematics systems such as OnStar, SYNC, Uconnect, etc., heavy vehicles have been more pervasively "connected" through satellite and cellular communications linking to telematics, fleet management, and engine management applications, for quite some time. Consequently, heavy vehicles currently have more avenues for remote access than light vehicles.

With hundreds and sometimes thousands of virtually identically configured vehicles, commercial truck fleets have a high level of electronic homogeneity that can enable an adversary to economically develop viable exploits that could attack large numbers of vehicles simultaneously.

Therefore, we are encouraging motor carriers to maintain awareness of potential issues and threats that can impact the safety and security of their vehicle fleets.

How can motor carriers help minimize heavy vehicle cyber security risks?

There are several actions that can be taken to potentially mitigate the risks associated with the technological features of heavy vehicles.

Develop a Cyber Security Program

Create an internal program to address cyber security with high-level organizational support, which includes people and policies, to assess and respond to cybersecurity issues. The nature and composition of the program and team will vary by the type and size of organization. A good starting point is the National Institute of Standards and Technology (NIST) Cybersecurity Framework (https://www.nist.gov/cyberframework). Center for Internet Security (CIS) also offers a good starting point in their controls for effective cyber defense (https://www.cisecurity.org/critical-controls.cfm).

Protect Your Networks

An easily targeted access point is office networks and those computers that are used to communicate with the vehicles. Attacks can include malicious websites, email attachments as well as access by a rogue contractor or disgruntled employee. Companies should employ basic network and computer security protocols.

Separate Networks	Segregate networks where computers have remote access to vehicle systems from those utilized for routine business functions (email, browsing the internet, working on office documents etc.).
Network Security	Protect your networks that communicate with vehicles with well configured firewalls, intrusion detection/prevention systems (IDS/IPS), as well as vulnerability management tools to help ensure your environment has the latest patches and is configured properly.
Lock Down Internet Access	Restrict internet access on all systems and computers that communicate with vehicles and consider removing internet browsers, PDF readers, and email clients etc. If outbound internet access is required, make sure to restrict internet access to a known set of safe destinations.
Change Default Passwords	Change the default passwords for all network and connected equipment from vendor supplied defaults.
Two Factor Authentication	Ensure all systems that give remote access to vehicle communication and features are accessible only via two factor authentication, which prevents password sharing, phising, and brute force password attacks.
Disaster Plans and Backups	Establish disaster recovery plans with backup processes and procedures which include offsite and "offline" backups, i.e. "air gapped." In the event of a incident such as fire, ransomeware, or malware the impacted system(s) could be restored.

Protect Your Vehicles

While short term solutions to vehicle computer designs are limited, there are a number of steps to take to reduce the risks.

Vendor Communication	Establish communication and notification avenues with manufacturers and third party product/service integrators to ensure that you are notified of any critical security issues or updates to your equipment and service.
Established Maintenance Plans	Establish documented maintenace plans for the vehicles which include requirements to ensure that the latest firmware and software patches/upgrades are applied to the vehicles systems within 30 days of release.
Customizations and Add-ons	Make sure that any modifications or additions to your vehicle such as third party tracking and telematics systems do not compromise the security of your vehicle or bridge networks which have been separated by the OEM.
Reduce Attack Surface	Disable and remove unused features that are not critical to the use and functionality of the vehicle, especially those that enable remote access.
Update Vehicle Pre-Trip Inspection	Add cybersecurity items to the pre-trip inspection check list and include cyber security training for CDL drivers. Drivers need to be aware of cyberthreats and looking for foreign devices mounted to accessable parts of the vehicle that can connect to the CAN bus.

How can motor carriers prepare for a cyber security attack?

Given the increasing odds of a security breach, it is necessary to develop a plan to ensure you know how to recover and survive a breach or attack. A standard part of system security is an incident response plan. This plan outlines the process and procedures to follow in the event of an incident. It is highly recommended that all motor carriers immediately start working with heavy vehicle manufacturers and telematics providers, and associated third parties to develop a plan on how to recover.

Incident Response Plan

The following generic steps have been identified for responding to a major incident. Many steps can occur in parallel depending on the nature of the situation, e.g. multiple attack vectors or vulnerabilities, carriers, etc.

Preparation	Create team Establish communication plan and crisis management structure Conduct exercises
Identification	Identify if attack has occurred or is ongoing Identify the impacted assets
Assessment	Assess the scope, impact and risk of the incident Investigate the cause and establish first course of action Collect forensics and critical data for next steps Create profile of affected units
Containment	Minimize and isolate the damage or risk Use profile to strategically contain affected units Implement contingency plans to maintain continuity of business
Eradication	Determine the root cause Conduct analysis on forensics data collected and assets Restore / rebuild systems affected
Recovery	Implement irrevocable corrective actions Restore normal operations
Follow-up	Lessons learned collected and incident response plan is updated Identify other units with similar vulnerability and create remediation plans

Educate

Raise awareness within your company and the industry. Educate all the different stakeholders as to the issues and potential impact regarding heavy vehicle cyber security. Additional information and resources are available through National Motor Freight Traffic Association, Inc. (customerservice@nmfta.org).

How can motor carriers help?

Incorporate Security in OEMs/Vendor Selection	Start including security evaluations as part of the product selection criteria. Ask questions to sellers. Does this product undergo adversarial security testing? Does it come with a field kit to or offer any other assistance in recovery in the event of a incident? If not, why not?
Get Involved	Participate in industry meetings and conferences on cybersecurity for transportation. Carrier participation is critical to the hardening of our nation's transportation infrastructure.

How do I report a cybersecurity incident?

The Internet Crime Complaint Center (IC3) is a reporting mechanism to submit information to the Federal Bureau of Investigation (FBI) concerning suspected Internet-facilitated criminal activity and to develop effective alliances with law enforcement and industry partners. The information reported is analyzed and disseminated for investigative and intelligence purposes to law enforcement and for public awareness. The FBI's IC3 offers annual reports and multiple self-help documents for effective cyber defense. https://www.ic3.gov

Credits and Acknowledgements

This document was developed as a collaborative effort by NMFTA staff and a large number of other companies, associations, universities, and federal agencies. While we are not able individually recognize everyone involved, we are extremely appreciative of their assistance and continued involvement. Thank you for your support of the transportation community.

Disclaimers

The information contained in this document is subject to change without notice. The information contained in this document is presented in good faith, and is believed to be correct, but correctness and completeness is subject to the limitations of an expedited research and writing cycle. The information contained in this document is for information purposes only. NMFTA disclaims all warranties, express or implied.

Trademarks

ClassIT, NMFC, SCAC, and National Motor Freight Classification are a registered trademarks of the National Motor Freight Traffic Association, Inc. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.