7101 Wisconsin Avenue
Suite 1300
Bethesda, MD 20814
www.autocare.org

T: 301.654.6664
F: 301.654.3299
info@autocare.org

Comments Submitted by the Auto Care Association

RE: Cybersecurity Best Practices for the Safety of Modern Vehicles
Docket Number: NHTSA-2020-0087

March 12, 2021

About the Auto Care Association

The Auto Care Association represents the more than 4.7 million people employed coast to coast by the auto care industry. Our businesses include independent aftermarket part manufacturers, distributors, auto part retail stores, and independent auto repair shops. Our members help Americans obtain affordable, convenient and effective auto repair.

We appreciate NHTSA including serviceability and the cybersecurity of aftermarket tools and equipment in its "Cybersecurity Best Practices for the Safety of Modern Vehicles" 2020 draft guidance ("Guidance"). As the voice of the independent aftermarket, we are providing comments to the Guidance that will uphold the intended purpose of strengthening cybersecurity while ensuring that the independent aftermarket industry continues to be able to service vehicles and produce high quality aftermarket components that keep auto repair and insurance costs affordable.

Our industry is actively involved with emerging automotive technology. The association's Emerging Technology Team tracks the evolving transportation ecosystem including Advanced Driver Assistance Systems, connected and automated vehicles, and automotive embedded systems. These technology experts have reviewed the Guidance and provided recommended edits and background information that will provide NHTSA with an understanding of how the auto care industry wants to work with the automotive industry to ensure continued vehicle cybersecurity.

Introduction

In general, the association agrees with provisions included in the guidelines that "the automotive industry should consider the serviceability of vehicle components and systems by individuals and third parties." In fact, vehicle owners and the automotive aftermarket should not, and do not need to be, denied direct access to vehicle maintenance data nor should vehicle owners concede their right to choose who repairs their vehicle or their right to determine who can directly access the vehicle data generated due to cyber security concerns. As demonstrated in our comments below, proven technologies and international industry standards exist that support safe, secure, standardized and direct access to vehicle data with the authorization of vehicle owners.

Importance of International Standards Toward Ensuring A Cyber Secure Transportation System

The new draft guidelines document makes frequent reference to the ISO/SAE 21434 draft standard which defines the cybersecurity lifecycle of a vehicle and the roles of various organizations in maintaining a safe vehicle state. This draft standard is a valuable reference in the context of general guidelines and best practices for the industry. As the vehicle is part of a larger connected transportation system and is but one entity in the transportation ecosystem, there are other ISO standards that prescribe detailed cybersecurity

autocare ASSOCIATION
Independence drives us.

7101 Wisconsin Avenue
Suite 1300
Bethesda, MD 20814
www.autocare.org

T: 301.654.6664
F: 301.654.3299
info@autocare.org

standards for all connected entities in the transportation ecosystem. Aftermarket experts have been active participants with OE engineers in the development of these ISO standard. This group of standards are informally referred to as the Secure Vehicle Interface (SVI) (a description of SVI and how it maps to NHTSA's cybersecurity best practices is included in separate addendum to these comments). These standards support the implementation of a safe, secure, direct and standardized interface to connected vehicles and provides vehicle owners privacy and choice with regard to sharing their vehicle's data. The Auto Care Association recommends the inclusion of the following standards in an appendix to the NHTSA guidelines document.

- ISO/SAE 21177: ITS station security services for secure session establishment and authentication between trusted devices
- ISO/SAE 21184: Cooperative intelligent transport systems (C-ITS) — Global transport data management (GTDM) framework
- ISO/SAE 21185: Intelligent transport systems — Communication profiles for secure connections between trusted devices
  ISO/SAE 21217: Intelligent transport systems (ITS) — Station and communication architecture

Section by Section Comments on the Revised Guidelines

4.2.1 Vehicle Development Process

ISO/SAE 21434 defines a detailed process for vehicle and component design which includes a comprehensive cybersecurity risk assessment for each communications interface. A goal for the industry should be to apply the same level of careful design to aftermarket parts, diagnostic and repair tools and the corresponding connected infrastructure. The achievement of this goal would be facilitated by the development of a common set of assumptions about shared interfaces. Specifically, the cybersecurity assumptions made by vehicle manufacturers that any port or interface within a vehicle will be made available to aftermarket developers for use in designing and supporting new technology that extends or enhances the vehicle's capabilities.

4.2.3 Sensor Vulnerabilities and Risks

The new guidelines appropriately recognize that vehicle sensors are a critical component in the safe operation of vehicles. Guidance G.6 calls attention to the risk of sensors being spoofed or jammed as a potential threat against vehicle safety systems. The draft document is silent on the importance of calibration and testing of these sensors over time. Additional guidance encouraging manufacturers to share calibration data and procedures with aftermarket repair facilities to ensure accurate testing and sensor calibration would affirm the importance of this role in vehicle safety.

Manufacturers should offer access to the in-vehicle data and technical details required by aftermarket repair facilities to support ongoing calibration and testing for all safety-critical sensors over the lifetime of the vehicle. Design of safety systems should account for the need to maintain and replace advanced sensor systems over time.

autocare ASSOCIATION
Independence drives us.

7101 Wisconsin Avenue
Suite 1300
Bethesda, MD 20814
www.autocare.org

T: 301.654.6664
F: 301.654.3299
info@autocare.org

4.2.6 Inventory of Management of Software Assets on Vehicles

Section 4.2.6 discusses the value of maintaining an inventory of all software and systems in a vehicle. This data should be made available to after-market repair facilities and tool vendors to assist in safely diagnosing and repairing vehicle systems. It is further recommended that a copy of this inventory be securely available through a direct interface within the vehicle, rather than as a data feed or download from the manufacturer.

Ideally, vehicle software identification and version data should be made available through a direct interface in the vehicle. Authorized after-market tools should have the ability to securely update the vehicle history log with any updates or changes that have been applied as specified by the vehicle manufacturer.

4.3 Information Sharing

Aftermarket service providers could play a valuable role in identifying and reporting malicious behavior and identifying new cybersecurity threats. Ideally, these experts should be encouraged to participate in the Auto-ISAC, and aftermarket diagnostic tools should have the technical capabilities to collect and report log data of suspect activity to that organization. The automotive aftermarket services over 70% of post-warranty vehicles and ignoring this group represents a missed opportunity to improve the overall security of the transportation networks.

6 Aftermarket Devices

The safe and effective use of aftermarket devices requires collaboration between the device designers and the vehicle manufacturers. Section 6 of the guidelines represents this relationship as independent and isolated. The general recommendation is that vehicles and devices need to provide independent protections. This should be extended to recognize the value in sharing information and defining standard methods for authentication and authorization pursuant to ISO 21177. We believe vehicle manufacturers should provide technical data about in-vehicle networks so that after-market designers can make informed decisions about security assumptions and protections.

In the current environment, there is no standard way for after-market services to receive telematic data from vehicles. The use of add-on telematic devices has created significant innovation in new services that have made driving more valuable and safer for consumers and fleet operators. The adoption of secure, standards-based methods for delivering telematic data to this growing array of applications will deliver value and enhance safety and reliability for vehicle owners. NHTSA support for standards-based delivery of telematic data directly to third party applications would help to continue the progress of mobility innovation while ensuring safety and protecting the privacy of drivers.

autocare ASSOCIATION
Independence drives us.

7101 Wisconsin Avenue
Suite 1300
Bethesda, MD 20814
www.autocare.org

T: 301.654.6664
F: 301.654.3299
info@autocare.org

7 Serviceability

Ongoing cybersecurity protection and serviceability of vehicles should be treated as an integrated activity. Over the life of a vehicle, vehicle owners and authorized repair technicians selected by the owner should have access to vehicle status and history related to software versions and update history and security relevant diagnostic logs. This will enable the broader community to provide ongoing security monitoring and response over the full life span of the vehicle.

Conclusion

Auto Care strongly supports efforts by NHTSA to ensure cyber security protection for motor vehicles. As we have stated above, extensive international standards are in place to protect critical vehicle systems from cyber intrusions while still ensuring that car owners can have access to competitive and innovative services. We urge the Agency to adopt our suggested revisions and to work toward adoption of these standards by motor vehicle manufacturers. Please feel free to reach out to Aaron Lowe (aaron.lowe@autocare.org) should you have any questions or would like additional information on the issues raised in our comments.