March 15, 2021

By regulations.gov
National Highway Traffic Safety Administration (NHTSA)
Docket Management Facility
West Building, Room W12-140
1200 New Jersey Avenue, SE
Washington, DC 20590-0001

Re: Cybersecurity Best Practices for the Safety of Modern Vehicles; Doc. No. NHTSA–2020–0087

Ladies and Gentlemen:

The National Automobile Dealers Association (NADA) represents more than 16,000 franchised automobile and truck dealers who sell new and used motor vehicles and engage in service, repair and parts sales. Together they employ over 1,000,000 people nationwide, yet the majority are small businesses as defined by the Small Business Administration.

Earlier this year, NHTSA issued a notice requesting comment on a revised draft cybersecurity best practices document, titled *Cybersecurity Best Practices for the Safety of Modern Vehicles* (*Draft 2020 Update*).[1] The *Draft 2020 Update* builds on a cybersecurity best practices document first published in 2016. NADA's members sell and securely service on-road motor vehicles and are particularly concerned about potential risks to the driving public, the dealership employees, and others that can result from insufficient motor vehicle cybersecurity. In response to NHTSA's request, NADA offers the following comments and suggestions.

I. Introduction

As suppliers and manufacturers incorporate ever more advanced technologies into motor vehicles, it is incumbent upon NHSTA to help ensure that cybersecurity is a high priority, even if it means that certain features, attributes, or systems might have to be limited or delayed. This requires adherence to certain principles, including the following:

- Security must be a nonnegotiable fundamental against which convenience, efficiency, and consumer demand must be measured.
- Systems must be designed to allow flexibility, but third-party access must be limited as necessary to ensure security.

[1] 86 Fed. Reg. 2481, *et seq.* (January 12, 2021)

- Appropriate training must be built into all levels of system and security design and operation, including the sales and service of vehicles.
- Security of the vehicle and the data it contains must be optimized by ensuring that the entire vehicle ownership ecosystem is secure.

NHTSA should adopt a broad view of the vehicle lifecycle and ecosystem to ensure that modern, high-technology vehicles are safe to operate. NADA is encouraged that the Draft 2020 Update addresses the cybersecurity implications of service and remediation on connected vehicles, but more is needed.

Broad cybersecurity frameworks like the National Institutes of Standards and Technology's (NIST) ("Identify, Protect, Detect, Respond, and Recover") framework are important starting points for addressing cybersecurity. But it is critical that NHTSA continue to engage with, if not lead the efforts of, such independent standards setting organizations (such as the International Standards Organization (ISO)/SAE International (SAE)) and on targeted efforts such as ISO/SAE 21434,[2] to leverage the work done by such organizations in conjunction with a broad range of industry and other stakeholders.

For now, voluntary guidelines and industry consensus standards appear to be working. However, NADA recognizes that in the future NHTSA may need to consider the adoption of mandatory cybersecurity requirements. Of course, crafting mandatory requirements applicable to all vehicle types would present considerable challenges. However, given the ever-increasing technical complexity of on-road motor vehicles, a baseline of mandatory requirements may prove necessary to ensure vehicle safety.

In addition to NHTSA, governments and agencies around the world are working to address vehicle cybersecurity.[3] And useful analogs already exist under U.S. law. For example, the Gramm-Leach-Bliley Act (GLBA) contains cybersecurity requirements for financial institutions and the GLBA Safeguards Rule, in effect for nearly 20 years, has worked well to address financial sector cybersecurity issues.[4] Importantly, the Safeguards Rule has been effective in part because it addresses cybersecurity without being overly prescriptive. Such a regime - stringent, yet flexible and self-modernizing – works well in the quickly evolving world of cybersecurity and could serve as a reasonable model for NHTSA.[5] A goal of all cyber incidents may be appropriate, but the reality is that perfect security is not possible in any context. Instead, NHTSA should continue to strive for guidelines and requirements with clear-cut, well validated cybersecurity benefits. NHTSA's focus should be on ensuring that motor vehicles (and vehicle ecosystems) meet the highest cybersecurity standards, while allowing entities the flexibility necessary to meet those standards.

II. Security Vulnerability Reporting Program

NADA concurs that a security vulnerability reporting program is important. Other industries have used reporting programs to their benefit and the automotive industry is no different. NADA has for many years been a supporter and strategic partner in the Auto-ISAC. Given that they are on the front line of

[2] 6 ISO/SAE 21434:2020: www.iso.org/standard/70918.html
[3] E.g.: UN WP.29/2020/79: https://unece.org/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf
[4] 16 CFR Part 314
[5] See also the HIPAA Security Rule; 45 CFR Part 160.

interaction with the motoring public, dealers and service facilities are critical components of any cyber-vulnerability reporting program and NHTSA should take care to include them.

III. Cybersecurity Through the Lifecycle of the Vehicle

NADA agrees that, "Cybersecurity considerations encompass the full lifecycle of the vehicle, which includes conception, design, manufacture, sale, use, maintenance, resale, and decommissioning."[6] The average age of motor vehicles on the road today is 11.9 years – certainly longer than the average "smart" phone or other computer. In just 2020, over 37 million used vehicles were sold[7] and the average motor vehicle has more than three owners over its lifetime. Given that far more used motor vehicles are sold each year than new, ignoring the cybersecurity posture of used motor vehicles would pose an immense risk to their owners and operators, to the motoring public, and to others. Used motor vehicle purchasers should be able to benefit from the same cybersecurity protections new vehicle purchasers do. This means that NHTSA's cybersecurity framework, and associated administration, should aim to ensure cybersecurity over the multi-owner lifetime of motor vehicles.

Lifecycle cybersecurity is critical to ensuring that motor vehicles can be operated safely as a cyber-compromised vehicle is a threat to road safety no matter its age. Thus, NHTSA's cybersecurity framework must address the risks and vulnerabilities of both newly designed systems *and* motor vehicles with older software and hardware. Software updates, warranty protections, restrictions on software tampering and access should all be part of NHTSA's focus.

IV. Aftermarket Devices

As mentioned in the *Draft 2020 Update*, vehicle manufacturers (OEMs) should support cybersecurity throughout a motor vehicle's lifecycle. OEMs should be encouraged to limit or exclude aftermarket devices from accessing vehicle systems when necessary to maintain vehicle cybersecurity. When an OEM discerns a legitimate cybersecurity risk due to an aftermarket device, it must be able to disable the device and make necessary changes to its cybersecurity software. The *Draft 2020 Update* stresses the need for penetration testing[8], but such testing is of limited use if aftermarket devices are given unfettered rein to access vehicle systems.

Dealers often see first-hand the harm that can result from aftermarket and consumer vehicle modifications. In fact, consumers or unprofessional shops cause damage to vehicles through inappropriate modifications via computerized systems, those vehicles often end up in dealerships for repair. Unfortunately, such modifications can void or limit OEM warranty coverage. Or worse, such modifications can undermine a vehicle's safety or emissions performance. Consequently, to maintain vehicle cybersecurity and safety performance, OEMs must be able to appropriately restrict unfettered access to critical vehicle systems.

[6] *Draft 2020 Update* 4.2 Vehicle Development Process with Explicit Cybersecurity Considerations.
[7] IHS Markit.
[8] *Draft 2020 Update* 4.2.7 Penetration Testing and Documentation.

V. Serviceability

NHTSA correctly recognizes that there must be "a balance" between vehicle serviceability and cybersecurity.[9] The greater the access to a motor vehicle's systems, the greater the number of individuals who could *potentially* service them. At the same time, the greater the access to amotr vehicle's systems, the greater the risk of a serious cybersecurity breach. Given these competing interests, NADA agrees with NHTSA that the "Safety of vehicle occupants and other road users should be of primary consideration when assessing risks."[10] To protect vehicle occupants and road users, cybersecurity concerns must be paramount. Consequently, NHTSA must adopt limitations on third party vehicle system access consistent with its cybersecurity protocols. Specifically, third-party access to motor vehicle systems must be:

- Segregated: access should be permitted only to those systems that are necessary to complete required repairs or service. Allowing access to all vehicle systems poses unnecessary cybersecurity risks.
- Authorized: only trusted servicers authorized by both a motor vehicle's owner and its OEM should be permitted service access.
- With consent: both the OEM and a vehicle's owner must consent to servicer access; and
- With proper training: the servicer must have adequate training to properly access vehicle systems in order to avoid undue cybersecurity risks.

VI. Over the Air Updates (OTAs)

Physical access to computerized systems present risks that must be controlled, but remote access to such systems will likely raise broader cybersecurity risks and attack vectors. Dealers understand the potential promise of "over the air" ("OTA") software updates and other remote access means of updating motor vehicle software. But they also recognize the potential cybersecurity risks associated with remote access. OTA updates of infotainment and other noncritical systems are not the same as those to systems involving critical vehicle functions such as braking, steering, and acceleration. Of greatest risk is the potential for significant harm resulting from a successful malicious or negligent third into an OTA system.[11] No software system is completely secure if it can be accessed by third parties, and OTA systems necessarily involve risks of virtually universal access. In short, NHTSA's *Draft 2020 Update* should focus special attention on the inherent cybersecurity risks posed by OTA systems.[12]

Secure physical service access points likely are critical to ensuring that security measures implemented by motor vehicle OEMs are consistently applied during vehicle servicing. In addition, in many instances they may be critical to applying updates after a security breach. When systems are compromised, dealerships they may need to be physically re-flashed. Moreover, consumers who have experience a cybersecurity incident are likely to prefer to obtain additional updates directly from their dealer.

---

[9] *Id.* at 7. Serviceability

[10] *Id.* 4.2.2 Risk Assessment [G.5]

[11] See Greenberg, Andy, *Hackers Remotely Kill a Jeep on the Highway—With Me in It*, Wired (2015); www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

[12] See UN WP.29/2020/80 on vehicle software updates. https://undocs.org/ECE/TRANS/WP.29/2020/80

VII. Education

Franchised automobile dealers are vital to consumer cybersecurity education given their interaction with new and used motor vehicle purchasers. Vehicle purchasers and operators will need better cybersecurity information and an awareness of possible threats, including from aftermarket devices, phone interfaces, etc. Education on cybersecurity is important not only at the time of sale, but also over time as events change. NHTSA's educational guidelines should recognize the critical role dealers can and will continue to play with respect to providing consumers with information on how to minimize cybersecurity risks.

VIII. Conclusion

NHTSA's *Draft 2020 Update* is a significant improvement over its 2016 cybersecurity guidelines. NADA looks forward to working with NHTSA as it moves forward with addressing motor vehicle cybersecurity issues that are of critical importance to the safety of the motoring public. On behalf of NADA, I thank you for the opportunity to comment on this matter.

Respectfully submitted,

Douglas I. Greenhaus
Chief Regulatory Counsel - Environment, Health & Safety
National Automobile Dealers Association