The Center for
Auto Safety
4400 Jenifer Street, NW Suite 331 | Washington, DC 20015
www.autosafety.org

March 15, 2021

Office of the Administrator
c/o Steven Cliff, Deputy Administrator

National Highway Traffic Safety Administration
Docket Management Facility
U.S. Department of Transportation
1200 New Jersey Avenue SE
West Building, Ground Floor, Room W12-140
Washington, DC 20590-0001

Submitted electronically via www.regulations.gov

RE: **Cybersecurity Best Practices for the Safety of Modern Vehicles; Docket No. NHTSA-2020-0087**

The Center for Auto Safety, appreciates the opportunity to provide comments on the January 7, 2021, Request for Comment by the National Highway Traffic Safety Administration ("NHTSA" or "agency") regarding Cybersecurity Best Practices for the Safety of Modern Vehicles ("NHTSA 2020 Cyber Practices").[1] The Center, founded in 1970, is an independent, member supported, non-profit consumer advocacy organization dedicated to improving vehicle safety, quality, and fuel economy. In 2020, we celebrated 50 years of advocacy for automotive safety and consumer protection.

In the history of the automobile, the wide-spread adoption of connected vehicles remains a relatively new phenomenon. Accordingly, in the course of their development there may have been a time for an aspirational cybersecurity best practice guide and set of ideas. Yet, 2021 is no longer that time. It is past-time for NHTSA to seize its role as the public's vehicle safety agency and provide real-world leadership by doing everything in its power to make Americans safe and secure in connected vehicles.

The best practices compiled in the NHTSA 2020 Cyber Practices are useful in theory but are of questionable value without complementary requirements for design, validation, and maintenance. It is NHTSA's responsibility to provide minimum cybersecurity performance requirements for automakers and suppliers and to enable validation of design approaches that assure long-term cybersecurity effectiveness and vehicle safety throughout a connected vehicle's life cycle. To enable developers to achieve vehicle cybersecurity, NHTSA should continue to research and make available to developers validated best practices to support their designs and potentially vehicle maintenance.

[1] Cybersecurity Best Practices for the Safety of Modern Vehicles, hereinafter "NHTSA 2020 Cyber Practices," https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/vehicle_cybersecurity_best_practices_01072021.pdf

NHTSA is uniquely equipped to fill the role of overseeing the threat definition, regulatory, verification, and maintenance protocols necessary to provide adequate cybersecurity for connected vehicles. NHTSA has failed to lead the way for connected vehicle cybersecurity, and issuance of the NHTSA 2020 Cyber Practices does not remediate this failure. On behalf of all drivers, passengers, or pedestrians sharing the road with a connected car today, or a self-driving car in the future, the Center recommends that NHTSA take a more complete look at vehicle cybersecurity. NHTSA's goal should be to turn the included best practices (and others) into effective tools to prevent and mitigate vehicle cyberintrusions, thereby enhancing the safety of everyone interacting with connected vehicles.

I. A Document Limited By Exclusions

The NHTSA 2020 Cyber Practices refers to several purported "best practices, culled from voluntary standard documents written by several automotive standard setting organizations.[2] It is far from clear, however, that it is a sufficiently comprehensive source for developers that has evaluated all potential applicable sourced and vetted asserted 'best practices' for practicality and efficacy. That other equally well-regarded best practice documents were omitted raises doubts about the scope of the NHTSA 2020 Cyber Practices. One omitted applicable voluntary standard, UL 4600, including extensive additional provisions for assuring connected vehicle cybersecurity, was published in 2020.[3] Additionally the UNECE WP29 Automotive Cybersecurity Regulation standard, also published in 2020, is set to become an actual requirement for vehicles sold in Europe in the near future.[4] The agency's failure to include these in the NHTSA 2020 Cyber Practices, or explain their omission, raises questions as to whether "Best" is an appropriate name for the compiled practices.

Importantly, the experience of the the Federal Aviation Administration (FAA), a sister agency within the Department of Transportation (DOT), that has been issuing cybersecurity guidelines for decades does not appear to have been incorporated into the NHTSA 2020 Cyber Practices. In fact there is no evidence that lessons learned in the aviation industry, many of which are clearly applicable to modern motor vehicle cybersecurity, have been included. Despite FAA's relative success NHTSA chose to rely exclusively on hand-picked auto industry voluntary standards. The lives of modern vehicle occupants are no less vulnerable nor less valuable than those of airplane occupants.

Lessons from the aviation industy's experience are relevant to the auto industry because of the success of cybersecurity measures for aviation to date, the similarity between avionics and modern vehicle control electronics and data processing designs, and the dependency of human life on the successful outcome of cybersecurity measures.

[2] ISO/SAE 21434:2020 Road Vehicles – Cybersecurity Engineering: https://www.iso.org/standard/70918.html, Auto ISAC BEST PRACTICES available at https://automotiveisac.com/best-practices/ ,
NIST 8151, https://csrc.nist.gov/News/2016/NIST-Announce-the-Release-of-DRAFT-NISTIR-8151

[3] ANSI/UL 4600 Standard for Safety for the Evaluation of Autonomous Products, , https://www.shopulstandards.com/ProductDetail.aspx?productid=UL4600

[4] UNECE WP29 Automotive Cybersecurity Regulation, http://www.unece.org/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf

A report by the General Accounting Office, (GAO) in 2020, on the FAA noted "[t]o date, extensive cybersecurity controls have been implemented (in aircraft) and there have not been any reports of successful cyberattacks on an airplane's avionics systems."[5] The FAA's experience goes beyond best practices and provides applicable and analogous regulations for examination by NHTSA.[6] The NHTSA 2020 Cyber Practices, inexplicably, does not include discussion of the adaptability of these successful avionics cybersecurity measures to connected vehicles.

While no set of practices can ever be deemed perfect, the same or equivalent demonstrably successful cybersecurity standards and their implementation should be included in the baseline for connected vehicles. Yet, even after accounting for FAA's success, additional best practices documented by the GAO to reinforce aviation cybersecurity that are equally applicable to connected vehicles were excluded from the NHTSA 2020 Cyber Practices, including:

> (1) assessing its oversight program to determine the priority of (connected vehicle) cybersecurity risks,
> (2) developing a cybersecurity training program,
> (3) issuing guidance for independent cybersecurity testing,
> (4) including periodic testing as part of its monitoring process,

In the words of the GAO, "Until FAA strengthens its oversight program, based on assessed risks, it may not be able to ensure it is providing sufficient oversight to guard against evolving cybersecurity risks facing avionics systems in commercial airplanes."[7] Considering the current cybersecurity track record of FAA and aviation far outpacing that of NHTSA and the auto industry, NHTSA and its far less mature connected vehicle cybersecurity program should heed GAO's advice.

Further, that the NHTSA 2020 Cyber Practices's failed to include the Department of Defense (DoD) or any other US government cybersecurity best practices or lessons learned, other than those provided by NIST, is highly problematic. The DoD has tremendous experience with cyber defense, including defense against intrusions into operational systems analogous to modern vehicles in terms of both complexity and mission. In addition to reliance on NIST cybersecurity publications, NHTSA should evaluate and collaborate with the FAA, DoD, DHS, and other government assets relevant to vehicle cybersecurity and advocate or mandate those practices proven effective as applicable to modern vehicles. For just one example, the Cybersecurity Maturity Model Certification (CMMC) process is applicable to, and should be incorporated into, modern vehicle cybersecurity, wherever lapses could degrade the safety of vehicle occupants, other vehicles, or vulnerable road users.[8] The NHTSA 2020 Cyber Practices should, but does not, include CMMC processes as a recommended best practice.

[5] AVIATION CYBERSECURITY - FAA Should Fully Implement Key Practices to Strengthen Its Oversight of Avionics Risks, https://www.gao.gov/products/GAO-21-86

[6] IATA, Compilation of Cyber Security Regulations, Standards, and Guidance Applicable to Civil Aviation Edition 1.0, August 2020, https://www.iata.org/contentassets/4c51b00fb25e4b60b38376a4935e278b/compilation_of_cyber_regulations_standards_and_guidance_1.0.pdf

[7] AVIATION CYBERSECURITY – FAA, *supra* at FN 5.

[8] CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)Version 1.0 | January 30, 2020, https://www.acq.osd.mil/cmmc/docs/CMMC_Model_Main_20200203.pdf

Issuance of the NHTSA 2020 Cyber Practices falls short of even NHTSA's own goals as provided in its 2016 whitepaper, *NHTSA and Vehicle Cybersecurity*, which suggested the agency "be ahead of potential vehicle cybersecurity challenges, and seek ways to address or avoid them altogether."[9] In evaluating the whitepaper and NHTSA's roles and responsibilities for assuring vehicle cybersecurity, the GAO noted NHTSA's lack of cybersecurity planning:

> NHTSA has not yet formally defined and documented the agency's role and responsibilities in the event of a real-world vehicle cyberattack and how the agency's response actions would be coordinated with other federal agencies. Given that NHTSA and selected industry stakeholders we spoke with generally agreed that the threat of a vehicle cyberattack will increase as autonomous and connected-vehicle technologies are deployed in the coming years, such a response plan may be particularly important for NHTSA to develop proactively, before the threat environment significantly changes.[10]

Critically, this lack of proactive measures continues today, as NHTSA once again takes comments on an incomplete and inadequate catalogue of vehicle cybersecurity "best practices." Five years later, instead of simply asking for additional comments it is time to take steps to ensure that NHTSA and the DOT have methods and means in place to prevent and respond to vehicle cyberattacks in America.

Recent events demonstrate that even supposedly secure computer systems and networks are susceptible to malicious penetration by a determined actor despite a developer's access to recommended best practices.[11] Consequently, there can be no promise that voluntary or even mandatory incorporation of the best practices discussed in the NHTSA 2020 Cyber Practices will in fact provide cybersecurity for modern vehicles. Instead, the best that can be hoped for by its use alone as a reference for vehicle developers is a false sense of security, belying assertions of vehicle safety. Public safety demands more than a fig leaf. The GAO has noted,

> Several industry stakeholders we spoke with—including automakers and industry associations—told us that this type of guidance [a NHTSA document that provides a framework and educates the industry on the methodology NHTSA uses and the factors it considers when assessing risks associated with cybersecurity vulnerabilities in order to make safety defect and recall determinations] would be helpful and is needed. For example, representatives from one industry association told us that absent guidance, automakers could monitor NHTSA's actions and recall decisions over time to get clarity on what factors NHTSA considers important in making safety defect determinations; however, conducting such monitoring of

[9] NHTSA and Vehicle Cybersecurity, https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/nhtsavehiclecybersecurity2016.pdf

[10] GAO-16-350, VEHICLE CYBERSECURITY -DOT and Industry Have Efforts Under Way, but DOT Needs to Define Its Role in Responding to a Real- world Attack, pg 41, www.gao.gov/assets/680/676064.pdf

[11] As Understanding of Russian Hacking Grows, So Does Alarm, New York Times, 1/2/21, https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html; Florida water treatment facility hack used a dormant remote access software, sheriff says, Cnn, Feb. 10, 2021, https://www.cnn.com/2021/02/10/us/florida-water-poison-cyber/index.html

> NHTSA's actions is not efficient. In addition to being helpful to the industry, such guidance could also help NHTSA respond to identified vulnerabilities more consistently.[12]

NHTSA should not be expected to reinvent the wheel when it comes to identifying vulnerabilities and sharing information, but is responsible for making sure such threats are shared quickly and effectively, and not merely on a voluntary basis. History demonstrates that, generally speaking, the sharing of learned experience throughout an organization, or even a corporate sector, can improve results and productivity for all involved and save time, and money. In the proper context, such information sharing can also support effective cybersecurity maintenance.

While it is important that the auto industry continue to participate in collective activities such as Auto ISAC, the voluntary model provides little confidence that participation is sufficiently robust, comprehensive, or transparent to protect public safety. The DOT and NHTSA must work cooperatively with automakers and suppliers to incentivize the adoption of a coordinated vulnerability disclosure policy and practice. These policies and practices should allow manufacturers a reasonable period of time to confirm and remediate a vulnerability, but fundamentally must assure that all relevant information is promptly made available to all who can use it to promote public safety, regardless of the source of that vulnerability. Further, we recommend the Secretary create an internal process at DOT which is designed to quickly and effectively communicate to all relevant parties in the event of an intrusion, including the public when necessary, and assure expeditious distribution of remediation to affected vehicles. The Secretary should seek the advice of, and collaborate with. the Cybersecurity & Infrastructure Security Agency (CISA) at the Department of Homeland Security (DHS). There is little doubt that wide adoption of connected vehicles subject to cyber-intrusions is the equivalent of a potential critical infrastructure breach that CISA is designed to address.

At the same time, NHTSA should develop cybersecurity rules, validation means, and remediation distribution requirements for connected vehicles today with a long-term view towards an AV-focused Federal Motor Vehicle Safety Standard for cybersecurity validation. Reliance on safety recalls to accomplish equivalent results is not commensurate with the need to provide an immediate response in the face of cyberattacks of any size.

Finally, the NHTSA 2020 Cyber Practices provides no guidance for a minimum set of best practices with sufficient scope to allow for the design and delivery of a cybersecure vehicle. Industry standards may be an important and valid source for industry cybersecurity best practices, but NHTSA has not provided any insights into how best practices incorporated into the draft document were selected for inclusion, were vetted for efficacy, nor how a developer can use the document as a sufficient source for its design basis. If NHTSA has not made such a determination, the document should clearly state its limitations. Without guidance of sufficient scope, the NHTSA 2020 Cyber Practices is inadequate to remediate current industry efforts to develop effective voluntary cybersecurity standards.

NHTSA should instead identify a way for developers to assure safety by using its best practices guide, perhaps in combination with a definitive approach to penetration testing as discussed

[12] *Supra* FN 10 at GAO-16-350

below. In the interest of public safety, NHTSA should promulgate minimum mandatory cybersecurity requirements for modern vehicle developers that include some objective measures of their effectiveness so that risks to the public can be evaluated.[13]

II. Specific Shortfalls in the NHTSA 2020 Cyber Practices Document

Leaving aside the NHTSA 2020 Cyber Practices's implicit endorsement of potentially incomplete voluntary vehicle cybersecurity standards in a manner that turns public roads into an open source test track, there are other specific defects in the guidelines.

Best practices that are omitted from the 2020 Cyber Practices include:

- Define Attack Surface[14]
  - The cybersecurity attack surface including all vulnerabilities must be identified and documented.
- Define Cybersecurity Risk Criteria
  - Risk criteria, risk criticality, risk mitigation plans, and processes to retire risks must be identified, documented, and included in development plans.
- Cybersecurity Validation
  - Methods, technology, and test plans to validate cybersecurity against all threats identified in the vehicle's Attack Surface throughout a vehicle's life cycle must be identified, documented, and executed.[15]
- Domain Separation
  - The vehicle digital design shall assure that the vehicle operational controls disallow unauthorized communications.

NHTSA writes in the 2020 Cyber Practices, "This (layered) approach (to vehicle cybersecurity) should eliminate sources of risks to safety-critical vehicle control systems where possible and feasible,"[16] without prescribing what 'should' happen where eliminating the source of risk is not possible or feasible, nor providing any usable definition of 'feasible.' It would appear that NHTSA is implying that developers and the public merely accept such risks in vehicles when addressing the source is inconvenient.

Similarly, 4.2.4 – Unnecessary Risk Removal states, "Any unreasonable risk to safety-critical systems should be removed or mitigated to acceptable levels through design, and any functionality that presents an unavoidable and unnecessary risk should be eliminated where possible."[17] While the title refers to 'unnecessary risk,' the definition refers to 'unreasonable risk' which is quite a different concept. Unfortunately, the NHTSA 2020 Cyber Practices does

[13] NHTSA suggested it would do just this in 2016: *Supra* FN 10 at GAO-16-350, pg. 38, "Although NHTSA has taken some steps to examine the need for safety standards for electronic control systems as required by MAP-21, which could include government standards related to vehicle cybersecurity, officials informed us the agency's examination is still ongoing. As part of its examination, NHTSA is considering establishing process standards, which would prescribe specific processes for developing vehicle electronic systems."

[14] NIST Computer Security Resource Center, https://csrc.nist.gov/glossary/term/attack_surface

[15] *Supra* FN 1, NHTSA 2020 Cyber Practcies, 4.27, Penetration Testing and Documentation, suggests penetration testing and documentation as optional activities, and do not reference any requirements related to scope of testing.

[16] *Supra* FN 1, at pg 3.

[17] *Supra* FN 1.

not define what risks are either necessary or reasonable, nor how mitigation of an unnecessary or unreasonable risk can make it either necessary or reasonable. Neither does it provide guidance on how to manage a 'necessary' or 'reasonable' risk. These gaps are unacceptable in a technical guidance document. Omitting these considerations is a tragically inadequate, dangerous, and unacceptable approach to vehicle safety. At a minimum, a guide to cybersecurity must define what is necessary and what is reasonable, how to assess, evaluate and retire such risks, and what to do if an identified risk is neither necessary nor reasonable. A de minimus best practice would require developers to demonstrate a supportable rationale for accepted risks that includes analysis of their impact on vehicle safety.

III. New Technology Needs

NHTSA should develop cybersecurity regulations and requirements that define a test environment, protocols, and practices to identify and eliminate or mitigate residual safety threats in vehicles susceptible to cyberattack, validating the cybersecurity design. Defensive cybersecurity, protecting the vehicle and its passengers, is the principle concern and responsibility of developers. A preponderance of NHTSA energy to date has been focused on defensive capabilities, principally focused on design. But defensive design practices are only one aspect of connected vehicle cybersecurity. Equally important to avoiding cybersecurity challenges altogether is availability of 'white hat' offensive connected vehicle cybersecurity validation capabilities that can only be provided by an objective third-party, such as NHTSA. The agency should use its unique perspective and resources to research and develop benign and comprehensive 'white hat' offensive cybersecurity test capabilities sufficient to validate cybersecurity over the full life cycle of connected vehicles. Offensive cybersecurity capability development, or the ability to verify and validate the sufficiency and safety of a developer's defensive cybersecurity implementation, is a proper and vital role for NHTSA.

It is appropriate and would be beneficial for NHTSA to provide equal focus to cybersecurity validation capabilities, such as helping define the threats and using that information to enable comprehensive penetration testing for design validation and periodic testing. The effectiveness of cybersecurity measures can only be validated by testing. The problem with NHTSA's taking the position that: "Manufacturers should also pursue product cybersecurity testing, including using penetration tests, as part of the development process,"[18] is that voluntary compliance does not assure sufficient validation. Moreover, it is not clear that any, much less every, private developer in the connected vehicle supply chain could deploy penetration test protocols that include the full scope of threat definitions available only to the government.[19] Adequate threat definition and penetration testing to validate a developer's cybersecurity implementation would ideally both identify and catalog known threats with updates provided by collaborative government assets (including classified sources) that have already developed sophisticated cyber penetration test capabilities unavailable to private developers. As noted above, such an approach would be consistent with GAO recommendations for the FAA, which are also applicable to connected vehicles. NHTSA should enable itself - or qualified test facilities through development of test

[18] *Supra* FN 1 at pg 6.

[19] Nor is it clear that the government could or should reveal the full scope to private developers without appropriate security clearances.

standards and specifications - to test and validate cybersecurity capabilities developed and embedded in vehicles offered to the public.

NHTSA and DOT have access to applicable government research into malicious actors both foreign and domestic, which is not available to developers. Moreover, providing an objective third-party point of view to validate cybersecurity is a role that only NHTSA can fulfill, either directly or by working with an independent third-party.

To provide connected vehicle cybersecurity validation leadership, NHTSA should lead an effort to marshal federal and state government resources to confirm vehicle protections by applying cybersecurity confirmation test practices, and not merely tag along behind industry cybersecurity best practices development. Such an effort might include model standards, techniques, and/or cyber configuration confirmation technology validated by itself and other government agency experience, and employable during vehicle safety inspections (part of vehicle life cycle cybersecurity maintenance) to verify continued cybersecurity. Means to validate continued cybersecurity should be shared with appropriate state agencies responsible for vehicle safety inspections. Customary recommended vehicle maintenance programs need to include the expectation that vehicle software and logic-bearing devices conform to approved configurations and be periodically examined to determine they have not been breached or altered.

Instead of reliance on a voluntary accommodation of best practices with uncertain utility and acceptance of unquantified risk, NHTSA should insist upon digital architectural approaches that optimize safety. For example, if safe reversion to human control is not an option, vehicles should incorporate an isolated supervisory controller that is truly independent of external inputs and guarantees reversion to a safe vehicle state if the vehicle deviates from a safe operating envelope. Such a system would be the cyber analog of a dual diagonal braking system, once revolutionary but now standard equipment on all cars, assuring a safe stop even in the event of catastrophic failure of one braking system. Such a supervisory controller for modern vehicles could similarly provide reversion to an acceptable safe state protecting vehicle passengers if there were a catastrophic failure of the primary controls regardless of whether the failure was the result of malicious intrusion.

It may never be possible to implement 100% effective prophylactic cybersecurity measures, thus NHTSA should endeavor to promote full life cycle vehicle cybersecurity. In other words, in order to assure sufficient information for post-incident forensic analysis and the ability to share lessons learned with the entire connected vehicle community, including the public, a robust data set will be required. NHTSA should mandate that vehicle software, logic-bearing devices, sensors, and data processing equipment configuration are embedded in vehicle data records in the event of a successful attack causing a life-threatening or deadly incident.

IV. Conclusion

NHTSA is uniquely positioned to command the resources necessary to assure connected vehicle cybersecurity through a combination of research, mobilization of governmental cybersecurity resources, requirements, test protocols, standards, and regulations. No individual or collection of manufacturers, developers, or participants in their supply chains has the necessary access to threat information, insight into cybersecurity validation expertise, and comprehensive overview of industry best practices to accomplish the task.

The argument that such NHTSA capabilities do not currently exist does not absolve NHTSA of its legal duty to act in the face of clear threats to vehicular safety. In the words of Abraham Lincoln, "As our case is new, so we must think anew, and act anew."[20] The need to address connected vehicle cybersecurity is new and NHTSA's response to that need must also be entirely new.

NHTSA is in a central position to determine the needed scope and means of testing to enhance public safety. And only NHTSA can make certain that the auto industry is enabled to realistically validate their cybersecurity designs, that capabilities have been validated, and that validation results are available to the public. In the future, the Center expects that the results of cybersecurity testing and validation will be incorporated into the information available to consumers to assist their evaluation of various modern vehicle offerings.

Thank you for the opportunity to present our views on this notice regarding Cybersecurity Best Practices for the Safety of Modern Vehicles. The Center is grateful that NHTSA is addressing this important topic and looks forward to a successful implementation of cybersecurity design, performance, test standards, and reporting that provide for public safety while using modern vehicles.

cc: Honorable Pete Buttigieg, Secretary, U.S. Department of Transportation

[20] A. Lincoln, Annual Address to Congress, 12/1/1862., http://www.abrahamlincolnonline.org/lincoln/speeches/congress.htm