DEPARTMENT OF TRANSPORTATION

National Highway Traffic Safety Administration

[Docket No. NHTSA-2020-0087]

Cybersecurity Best Practices for the Safety of Modern Vehicles

AGENCY: National Highway Traffic Safety Administration (NHTSA), Department of Transportation (DOT)

ACTION: Request for comments.

SUMMARY: NHTSA invites public comment on the Agency's updated draft cybersecurity best practices document titled *Cybersecurity Best Practices for the Safety of Modern Vehicles*. In 2016, NHTSA issued its first edition, *Cybersecurity Best Practices for Modern Vehicles,*[1] which described NHTSA's nonbinding guidance to the automotive industry for improving vehicle cybersecurity. With this document, NHTSA is docketing and soliciting public feedback on a draft update based on the knowledge gained through prior comments,[2] continued research, motor vehicle cybersecurity issues discovered by researchers, and related industry activities over the past four years. To emphasize NHTSA's safety mission, recommendations in the document

[1] National Highway Traffic Safety Administration (2016), *Cybersecurity Best Practices for Modern Vehicles*, announced via Federal Register document, 81 FR 75190 (Oct. 28, 2016), available at https://www.nhtsa.gov/document/cybersecurity-best-practices-modern-vehicles.

[2] 81 FR 75190, available at https://www.federalregister.gov/documents/2016/10/28/2016-26045/request-for-comment-on-cybersecurity-best-practices-for-modern-vehicles

focus on cybersecurity best practices that have safety implications for motor vehicles and motor vehicle equipment.

DATES: Written comments are due no later than [INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: Comments must refer to the docket number above and be submitted by one of the following methods:

• *Federal eRulemaking Portal*: Go to *http://www.regulations.gov*. Follow the online instructions for submitting comments.

• *Mail*: Docket Management Facility, M-30, U.S. Department of Transportation, West Building, Ground Floor, Room W12-140, 1200 New Jersey Avenue S.E., Washington, D.C. 20590.

• *Hand Delivery or Courier*: U.S. Department of Transportation, West Building, Ground Floor, Room W12-140, 1200 New Jersey Avenue S.E., Washington, D.C., between 9 a.m. and 5 p.m. Eastern time, Monday through Friday, except Federal holidays. To be sure someone is there to help you, please call (202) 366-9322 before coming.

• Fax: 202-493-2251.

Regardless of how you submit your comments, you must include the docket number identified in the heading of this document.

Note that all comments received, including any personal information provided, will be posted without change to *http://www.regulations.gov*. Please see the "Privacy Act" heading below.

You may call the Docket Management Facility at 202-366-9322. For access to the docket to read background documents or comments received, go to *http://www.regulations.gov* or the

street address listed above. To be sure someone is there to help you, please call (202) 366-9322 before coming. We will continue to file relevant information in the Docket as it becomes available.

Privacy Act: In accordance with 5 U.S.C. 553(c), DOT solicits comments from the public to inform its decision-making process. DOT posts these comments, without edit, including any personal information the commenter provides, to *http://www.regulations.gov*, as described in the system of records notice (DOT/ALL-14 FDMS), which can be reviewed at *https://www.transportation.gov/privacy*. Anyone can search the electronic form of all comments received into any of our dockets by the name of the individual submitting the comment (or signing the comment, if submitted on behalf of an association, business, labor union, etc.).

FOR FURTHER INFORMATION CONTACT:

For technical issues, please contact Mr. Robert Kreeb of NHTSA's Office of Vehicle Safety Research at 202-366-0587 or robert.kreeb@dot.gov. For legal issues, contact Ms. Sara R. Bennett of NHTSA's Office of Chief Counsel at 202-366-2992 or sara.bennett@dot.gov.

SUPPLEMENTARY INFORMATION:

The evolution of automotive technology has included an increasingly expanded use of electronic systems, software, and wireless connectivity. While this development began in the late 1970s, the pace of technological evolution has increased significantly over the past decade. Automotive technology has developed to such an extent that today's vehicles are some of the most complex computerized products available to consumers. Enhanced wireless connectivity and continued innovations in electronic control systems introduce substantial benefits to highway transportation safety, mobility, and efficiency. However, with the proliferation of computer-based control systems, software, connectivity, and onboard digital data communication networks,

modern vehicles need to consider additional failure modes, vulnerabilities, and threats that could jeopardize benefits if the new safety risks are not appropriately addressed.

Connectivity and safety technologies that can intervene to assist drivers with control of their vehicles (e.g., automatic emergency braking) could also increase cybersecurity risks, and without proactive measures taken across the vehicle lifecycle, risks could result in negative safety outcomes. As such, motor vehicle cybersecurity remains a top priority for NHTSA. NHTSA is engaged in research and industry outreach efforts to support enhanced reliability and resiliency of vehicle electronics, software, and related vehicle control systems, not only to mitigate safety risks associated with failure or potential cyber compromise of such systems, but also to ensure that affected parties take appropriate actions and such concerns do not pose public acceptance barriers for proven safety technologies.

NHTSA's work in this area seeks to support the automotive industry's continued improvements to motor vehicle cybersecurity reliability and resiliency. The Agency also expends resources in understanding and promoting contemporary methods in software development, testing practices, and requirements management as they pertain to robust management of underlying safety hazards and risks across the vehicle life-cycle. These activities include close collaboration with industry to promote a strong risk management culture and associated organizational and systems engineering processes.

Background

In October 2016, NHTSA issued its first best practices document focusing on the cybersecurity of motor vehicles and motor vehicle equipment.[3] *Cybersecurity Best Practices for Modern Vehicles* ("2016 Best Practices") was the culmination of years of extensive engagement

[3] *Cybersecurity Best Practices for Modern Vehicles*, announced via the Federal Register, 81 FR 75190 (Oct. 28, 2016).

with public and private stakeholders and NHTSA research on vehicle cybersecurity and methods of enhancing vehicle cybersecurity industry-wide. As explained in the accompanying Federal Register document, NHTSA's 2016 Best Practices was released with the goal of supporting industry-led efforts to improve the industry's cybersecurity posture and provide the Agency's views on how the automotive industry could develop and apply sound risk-based cybersecurity management processes during the vehicle's entire lifecycle.

The 2016 Best Practices leveraged existing automotive domain research as well as non-automotive and IT-focused standards such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the Center for Internet Security's Critical Security Controls framework. NHTSA considered these sources to be reasonably applicable and appropriate to augment the limited industry-specific guidance that was available at the time. At publication, NHTSA noted that the 2016 Best Practices were intended to be updated with new information, research, and other cybersecurity best practices related to the automotive industry. NHTSA invited comments from stakeholders and interested parties in response to the document.

Below is a high-level summary of comments received and how NHTSA integrated those comments into the 2020 draft *Cybersecurity Best Practices for the Safety of Modern Vehicles*.

Summary of Public Comments Received in Response to NHTSA's 2016 Best Practices

NHTSA received comments from government agencies, regulated entities, trade associations, advocacy groups and organizations, and individuals.[4] Key topic areas, and how such comments are reflected in NHTSA's revised 2020 *Cybersecurity Best Practices for the Safety of Modern Vehicles* are listed below.

[4] Comments on the 2016 *Cybersecurity Best Practices for Modern Vehicles* can be found at https://beta.regulations.gov/document/NHTSA-2016-0104-0001/comment.

- *Guidance vs. Rules*. Many commenters noted that cybersecurity is a constantly evolving discipline and that best practices may need frequent updating, and most commenters suggested that NHTSA's cyber best practices should remain non-binding and voluntary. NHTSA agrees with these commenters, and adoption of any of the provisions listed in the 2020 *Cybersecurity Best Practices for the Safety of Modern Vehicles* remains voluntary.
- *NHTSA's cyber best practices should be aligned with industry initiatives*. Commenters noted that industry initiatives were under development at the time of the 2016 Best Practices publication. NHTSA believes that the specific best practices outlined in today's 2020 revision reflect a strong linkage to key industry cybersecurity-related initiatives and efforts by organizations such as SAE International (SAE), the International Organization for Standardization (ISO), NIST, and the Automotive Information Sharing and Analysis Center (Auto-ISAC)—and are, in general, consistent with guidelines, standards, and best practices developed by these organizations.
- *Focus on Safety.* Several commenters noted that NHTSA's best practices should focus squarely on safety aspects of cybersecurity. NHTSA agrees. The best practices presented in this revision are tailored to focus on cybersecurity issues that impact the safety of motor vehicles throughout the lifecycle of design, operation, maintenance and disposal. This emphasis is reflected throughout the document, including with a title change: *Cybersecurity Best Practices for the Safety of Modern Vehicles.*
- *Consideration of cybersecurity as part of software development process*. Multiple commenters recommended greater and more formal consideration of cybersecurity as part of the software development lifecycle process. NHTSA's revised best practice outlined today reflects a need to include cybersecurity considerations along the entire software

supply chain and throughout the lifecycle management processes of developing, implementing and updating software-enabled systems.

- *Additional cybersecurity terminology, definitions*. Commenters noted that the document would benefit from providing expanded definitions for certain terms to add precision and clarity to the recommended best practices. NHTSA has provided several additional definitions for key terms used throughout the document.

The comments received, combined with continued research, outreach to stakeholders, learnings from motor vehicle cybersecurity issues discovered by researchers, and related industry activities over the past four years have served as the foundation for the 2020 update. A description of other important information that guided the changes included in the 2020 *Cybersecurity Best Practices for the Safety of Modern Vehicles* is included in the following section.

2020 Update of Cybersecurity Best Practices

NHTSA is docketing a draft update to the agency's 2016 Best Practices,[5] titled *Cybersecurity Best Practices for the Safety of Modern Vehicles* (2020 Best Practices) for public comments. This update builds upon agency research and industry progress since 2016, including emerging voluntary industry standards, such as the ISO/SAE Draft International Standard (DIS) 21434, "Road Vehicles – Cybersecurity Engineering."[6] In addition, the draft update references a series of industry best practice guides developed by the Auto-ISAC through its members.[7]

---

[5] The 2016 guidance is titled *Cybersecurity Best Practices for Modern Vehicles* and is available at: https://www.federalregister.gov/documents/2016/10/28/2016-26045/request-for-comment-on-cybersecurity-best-practices-for-modern-vehicles. The 2020 update has a modified title that emphasizes the document's focus on, and NHTSA's commitment to, cybersecurity as an aspect of safety in motor vehicles and motor vehicle equipment.
[6] ISO/SAE 21434:2020 *Road Vehicles – Cybersecurity Engineering*, available at: https://www.iso.org/standard/70918.html.
[7] See https://automotiveisac.com/best-practices/

The 2020 Best Practices also reflect findings from NHTSA's continued research in motor vehicle cybersecurity, including over-the-air updates, encryption methods, and building our capability in cybersecurity penetration testing and diagnostics, and the new learnings obtained through researcher and stakeholder engagement. Finally, the updates included in the 2020 Best Practices incorporate insights gained from public comments received in response to the 2016 guidance and from information obtained during the annual SAE/NHTSA Vehicle Cybersecurity Workshops.

As with the 2016 Best Practices, NHTSA's updated draft, *Cybersecurity Best Practices for the Safety of Modern Vehicles,* is intended to serve as a resource for the industry as a whole and covers safety-related cybersecurity issues for all motor vehicles and motor vehicle equipment. As such, it is applicable to all individuals and organizations involved in the design, manufacture, and assembly of a motor vehicle and its electronic systems and software. These entities include, but are not limited to, small and large volume motor vehicle and motor vehicle equipment designers, suppliers, manufacturers, and modifiers. What follows is a listing of each new best practice, and an explanation of why NHTSA believes the inclusion is necessary in this update.

- *[G.6] Manufacturers should consider the risks associated with sensor vulnerabilities and potential sensor signal manipulation efforts such as GPS spoofing,*[8] *road sign*

[8] DefCon 23 – Lin Huang and Qing Yang – *Low cost GPS Simulator: GPS Spoofing by SDR* (2015). Video of the talk available at: https://media.defcon.org/DEF%20CON%2023/DEF%20CON%2023%20video/

modification,[9] Lidar/Radar jamming and spoofing,[10] camera blinding,[11] or excitation of machine learning false positives.[12]

This best practice recommends that industry consider "sensor vulnerabilities" as part of their risk assessment (examples: GPS spoofing, road sign modification, Lidar/Radar jamming and spoofing, camera blinding, or excitation of machine learning false positives). NHTSA added it to reflect the new research that shows that technology behavior could be influenced via sensor spoofing, which differs from traditional software manipulation-based cyber issues.

- *[G.7] 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.*

This best practice recommends "removal of risk" to be considered as part of the development process. NHTSA included this best practice to align with the National Traffic and Motor Vehicle Safety Act's prohibition of manufacturers selling motor vehicles and motor vehicle equipment that may contain unreasonable risks to safety. This is a common practice element of sound risk-based approaches. The 2016 Best Practices recommended assessing and appropriately mitigating risks to acceptable levels. While the 2016 documents implicitly included G.7 in cases where risks could not be mitigated with known tools and for a given architecture appropriately, this document makes the best practice explicit.

---

[9] McAfee Labs, *Model Hacking ADAS to Pave Safer Roads for Autonomous Vehicles* (2020), available at: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/model-hacking-adas-to-pave-safer-roads-for-autonomous-vehicles/.

[10] Mark Harris, IEEE Spectrum Sept 4, 2015, *Researcher Hacks Self-driving Car Sensors.*

[11] Petit, J. et al., "Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR" (2015), available at: https://www.blackhat.com/docs/eu-15/materials/eu-15-Petit-Self-Driving-And-Connected-Cars-Fooling-Sensors-And-Tracking-Drivers-wp1.pdf.

[12] Tencent Keen Security Lab, *Experimental Security Research of Tesla Autopilot* 2019, available at: https://keenlab.tencent.com/en/whitepapers/Experimental_Security_Research_of_Tesla_Autopilot.pdf.

- *[G.9] Clear cybersecurity expectations should be specified and communicated to the suppliers that support the intended protections.*

Vehicles are produced in a complex supply chain, and cybersecurity roles and expectations need to be clarified and coordinated among involved parties to support the cybersecurity goals of the manufacturers. ISO/SAE 21434 Clause 15 discusses customer-supplier relationships and provides various recommendations for how to manage cybersecurity risks among these entities. Such recommendations extend, among other aspects, to the interactions, dependencies, and responsibilities between customers and suppliers for cybersecurity activities.

- *[G.10] Manufacturers should maintain a database of operational software components[13,14] used in each automotive ECU, each assembled vehicle, and a history log of version updates applied over the vehicle's lifetime; and [G.11] Manufacturers should track sufficient details related to software components,[15] such that when a newly identified vulnerability is identified related to an open source or off-the-shelf software,[16] manufacturers can quickly identify what ECUs and specific vehicles would be affected by it.*

Through engagement in organized exercises, such as CyberStorm,[17] the Agency recognized that the ability to identify whether an issue with one component would affect a single or multiple makes and models is critically important to determine the potential scope of risk. Further, being

[13] This is also referred to as a software bill of materials (SBOM), which is a list of components in a piece of software, including assembled open source and commercial software components.
[14] Multistakeholder Process on Promoting Software Component Transparency, 83 Fed. Reg. 110 (June 4, 2018).
[15] These details could include: the licenses that govern those components, the versions of the components used in the codebase, and their patch status.
[16] A good example would be the vulnerability associated with the Transport Layer Security(TLS) implementations in OpenSSL 1.0.1 before 1.0.1g in the Heartbleed vulnerability: https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2014-0160.
[17] https://www.cisa.gov/cyber-storm-securing-cyber-space

able to recognize which software version is installed on individual vehicles or items of equipment and differentiate between versions is critical to respond to incidents quickly. The Food and Drug Administration and National Telecommunications and Information Administration developed detailed guidance around the same concept, and NHTSA believes such guidance to be of value to the automotive industry.

- *[G.12] Manufacturers should evaluate all commercial off-the-shelf and open-source software components used in vehicle ECUs against known vulnerabilities.*[18,19]

This best practice highlights the importance of making informed decisions about using open source and off-the-shelf software with respect to documented vulnerabilities. This is a common practice in other domains. NIST established a national database to facilitate such action.[20]

- *[G.22] Best practices for secure software development should be followed, for example as outlined in NIST 8151*[21] *and ISO/SAE 21434.*[22]

This best practice provides further detailed resources for companies to consider for implementation, as appropriate. Comments received on the 2016 Cybersecurity Best Practices requested that NHTSA incorporate current industry guidance and standards.[23] Pointing to such resources is helpful for all companies, but particularly for companies with less mature cybersecurity programs.

---

[18]MITRE Common Vulnerabilities and Exposures (CVE) may be found at: https://cve.mitre.org/.
[19] NIST's National Vulnerability Database may be found at: https://nvd.nist.gov/.
[20] *See* https://nvd.nist.gov/.
[21]Black P., Badger M., Guttman B., Fong E., NISTIR 8151 *Dramatically Reducing Software Vulnerabilities: Report to the White House Office of Science and Technology Policy.*
[22] ISO/SAE 21434 clause 10 discusses software development practices.
[23] *See* public comments in response to the 2016 Best Practices, such as NHTSA-2016-0104-0969, and NHTSA-2016-0104-0998.

- *[G.23] Manufacturers should actively participate in automotive industry-specific best practices and standards development activities through Auto-ISAC and other recognized standards development organizations.*

Industry standards, such as ISO/SAE 21434, are more broadly adopted when entities actively participate in their establishment and ensure their unique needs are considered and addressed. NHTSA's encouragement of industry involvement in standards development organizations is long standing.

- *[G.30] Commensurate to assessed risks, organizations should have a plan for addressing newly identified vulnerabilities on consumer-owned vehicles in the field, inventories of vehicles built but not yet distributed to dealers, vehicles delivered to dealerships but not yet sold to consumers, as well as future products and vehicles.*

During a validated incident, the ability to address the issue for the impacted population could vary for vehicles in different stages of distribution. A plan that considers these stages can facilitate a more effective organizational response. This addition also reflects Clause 7 of the ISO/SAE 21434 standard.

- *[G.40] Any connection to a third-party device should be authenticated and provided with appropriate limited access.*

During the life-cycle of a vehicle, consumer devices (*e.g.,* mobile phones, insurance dongles) or repair/maintenance tools may be connected to the vehicle systems. These systems could enable wireless connectivity to the vehicle interface and may not feature adequate cyber controls on them. For example, research on an insurance dongle inserted into the OBDII port during operation found that it did not employ techniques, such as digital signing, that would prevent a

cyber attacker from reprogramming firmware.[24] A similar issue is described by Argus Cybersecurity on a connected car service.[25] Accordingly, this best practice recommends that vehicle systems should treat such devices as untrusted and control their access to safety critical systems.

- *[T.7] The use of global symmetric keys and ad-hoc cryptographic techniques for diagnostic access should be minimized.*[26]

This best practice discourages the use of global symmetric keys or unproven cryptographic techniques, which can result in a false sense of security for manufacturers and the consumer. This addition is also responsive to a comment from a diagnostic tool manufacturer to the 2016 Best Practices. Further, research shows the ineffectiveness of symmetric keys (see footnote in T.7).

- *[T.8] Vehicle and diagnostic tool manufacturers should control tools' access to vehicle systems that can perform diagnostic operations and reprogramming by providing for appropriate authentication and access control.*[27]

This best practice responds to research demonstrating the ability to leverage diagnostic tools to reverse engineer and implement vulnerabilities in vehicle systems.

- *[T.12] Such logs that can be aggregated across vehicles should be periodically reviewed to assess potential trends of cyber-attacks.*

---

[24] See https://jalopnik.com/progressive-insurances-driver-tracking-tool-is-ridicul-1680720690.
[25] See Argus Cyber Security, "A remote attack on an aftermarket telematics service" (Nov. 7, 2014), available at: https://argus-sec.com/remote-attack-aftermarket-telematics-service/#:~:text=Zubie%20is%20a%20leading%20connected,II%20port%20of%20your%20car.
[26] Hogan G., *Flashing ECU Firmware Updates from a Web Browser*, Talk at DefCon 27: Car Hacking Village, Las Vegas. Video of the talk may be found at: https://media.defcon.org/DEF%20CON%2027/DEF%20CON%2027%20villages/ . Mr. Hogan describes reverse engineering enciphered firmware updates.
[27] ISO/SAE 21434 requirement [RQ-05-15] states that "Tools that can impact the cybersecurity of an item, system or component shall be managed."

Information aggregated across multiple vehicles in a manufacturer's fleet can highlight trends and help a manufacturer recognize a cybersecurity attack more quickly, and potentially prior to a successful breach, than focusing on only a single vehicle or compartmentalized information. This approach is common in the enterprise information technology domain,[28] and applies to the automotive realm. T.12 purposefully limits the recommendation to logs that can be aggregated.

- *[T.13] Manufacturers should treat all networks and systems external to a vehicle's wireless interfaces as untrusted and use appropriate techniques to mitigate potential threats.*

This is a common approach taken by the stakeholder community and NHTSA. Various forms of "man-in-the-middle" cyber attacks seen with wireless interfaces suggest that information outside the wireless interfaces of vehicles should not be trusted until appropriately authenticated for intended uses. NHTSA added this best practice to reflect learnings from demonstrated man-in-the-middle attacks.

- *[T.22] Maintain the integrity of OTA updates, update servers, the transmission mechanism and the updating process in general.*[29,30]

OTA updates are updates to vehicle or equipment software that are pushed remotely to the vehicle. The OTA update process should not introduce cybersecurity vulnerabilities in the process, through either the update itself or through the updating process. NHTSA added this best practice to reflect learnings discussed in the Agency's Cybersecurity of Firmware Updates research report.[31]

---

[28] See Chapter 4: Network based intrusion detection and protection systems in NIST 800-94, available at https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf

[29] Bar R., *Hacking into Automotive Clouds*, talk at DefCon 27 Car Hacking Village, Las Vegas 2019. Video of the talk: https://media.defcon.org/DEF%20CON%2027/DEF%20CON%2027%20villages/.

[30] Rodgers M., Hahaffey K., *How to Hack a Tesla Model S*, talk at DefCon 23, Las Vegas 2015. Video of the talk: https://media.defcon.org/DEF%20CON%2023/DEF%20CON%2023%20video/.

[31] https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/cybersecurity_of_firmware_updates_oct2020.pdf

- *[T.23] Take into account, when designing security measures, the risks associated with compromised servers, insider threats, men-in-the-middle attacks, and protocol vulnerabilities.*

This best practice provides more granular recommendations with respect to risk considerations in T.22. As with T.22, NHTSA added this to reflect learnings discussed in the Agency's Cybersecurity of Firmware Updates research report.[32]

Public Comment

NHTSA is seeking public comments on the 2020 Best Practices and additional ways to improve its usefulness to stakeholders. The updated draft document is structured around five key areas: (1) General Cybersecurity Best Practices, (2) Education, (3) Aftermarket/User Owned Devices, (4) Serviceability, and (5) Technical Vehicle Cybersecurity Best Practices, and NHTSA seeks comments on all areas.

NHTSA will further update and refine this draft document over time, based on public comments received, the experience of NHTSA, manufacturers, suppliers, consumers, and others, as well as from further research findings and technological innovations. The updated draft document is available in PDF format under Docket No. NHTSA-2020-0087.

Economic Analysis for *Cybersecurity Best Practices for the Safety of Modern Vehicles*

NHTSA is seeking comment on its Cybersecurity Best Practices for the Safety of Modern Vehicles (2020 Best Practices), which is non-binding (i.e., voluntary) guidance provided to serve as a resource for industry on safety-related cybersecurity issues for motor vehicles and motor vehicle equipment. As guidance, the document touches on a wide array of issues related to safety-related cybersecurity practices, and provides recommendations to industry on the

[32] https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/cybersecurity_of_firmware_updates_oct2020.pdf

following topics: (1) General Cybersecurity Best Practices, (2) Education, (3) Aftermarket/User Owned Devices, (4) Serviceability, and (5) Technical Vehicle Cybersecurity Best Practices.

NHTSA has made a good faith effort to assess the potential costs that companies in the automotive industry might bear if these companies decide to integrate the recommendations in the 2020 Best Practices into their business practices. The following is a summary of the considerations that NHTSA evaluated for purposes of this section.

First, although, as guidance, the 2020 Best Practices is voluntary, NHTSA expects that many entities will to conform their practices to the recommendations endorsed by NHTSA. NHTSA believes that the Cybersecurity Best Practices for the Safety of Modern Vehicles serve as means of facilitating common understanding across industry regarding best practices for cybersecurity.

Second, the diversity among the entities to which the 2020 Best Practices apply is vast. The recommendations found in Cybersecurity Best Practices for the Safety of Modern Vehicles are necessarily general and flexible enough to be applied to any industry entity, regardless of size or staffing. The recommendations contained within the best practices are intended to be applicable to all individuals and organizations involved in the design, manufacture, and assembly of a motor vehicle and its electronic systems and software. These entities include, but are not limited to, small and large volume motor vehicle and motor vehicle equipment designers, suppliers, manufacturers, and modifiers. NHTSA recognizes that there is much organizational diversity among the intended audience, resulting in a variety of approaches, organizational sizes, and staffing needs. NHTSA also expects that these entities have varying levels of organizational maturity related to cybersecurity, and varying levels of potential cybersecurity risks. These expectations, combined with NHTSA's lack of detailed knowledge of the organizational maturity

and implementation of any recommendations contained within the guidance, make it difficult for NHTSA to develop a reasonable quantification of the per-organization cost of implementing the recommendations.

Third, any costs associated with applying the 2020 Best Practices would be limited to the incremental cost of applying the new recommendations included in the document (as opposed to those in the 2016 Best Practices). The updated Cybersecurity Best Practices for the Safety of Modern Vehicles document highlights a total of 65 enumerated best practices, 16 of which could be considered "new" relative to the first version published in 2016.

Fourth, costs could be limited by organizations who have implemented some of the recommendations prior to this request for comment. NHTSA is unaware of the extent to which various entities have already implemented NHTSA's recommendations, and determining the incremental costs associated with full implementation of the recommendations is effectively impossible without detailed insight into the organizational processes of every company.

Fifth, many of NHTSA's recommendations lean very heavily on industry standards, such as Draft International Standard SAE/ISO 21434. Three of the 16 "new" best practices simply reference the SAE/ISO 21434 industry standard. Since many aspects of NHTSA's recommendations are mapped to an industry standard, costs would also be limited for those companies who are adopting SAE/ISO 21434 already. Thus, it would be impossible to parse whether a company implemented SAE/ISO 21434 or whether it had decided to adopt NHTSA's voluntary recommendations. While the 2020 Best Practices have some recommendations[33] that cannot be mapped to an industry standards document at this time, most of those

[33] For example, G.6 in Section 4.2.3 recommends consideration of sensor vulnerabilities as part of risk assessment; and G.9 and G.10 in Section 4.2.6 recommend tracking software components on vehicles in a manner similar to hardware components.

recommendations involve common vehicle engineering and sound business management practices, such as risk assessment and supply-chain management. For these recommendations, NHTSA's inclusion in the 2020 Cyber Best Practices serve as a reminder.

Regarding benefits, entities that do not implement appropriate cybersecurity measures, like those guided by these recommendations, or other sound controls, face a higher risk of cyberattack or increased exposure in the event of a cyberattack, potentially leading to safety concerns for the public.

Implementation of the best practices can, therefore, facilitate "cost prevention" in the sense that failure to adopt appropriate cybersecurity practices could result in other direct or indirect costs to companies (i.e., personal injury, vehicle damage, warranty, recall, or voluntary repair/updates). A quantitative analysis would require present value estimation of future benefits, or a comparison of two similar sample groups, one of which is implementing the recommendations and the other is not. This comparison would illustrate the differences in groups in a way that would allow the benefits attributable to implementation of the best practices to be calculated. However, neither is possible at this time.

The best practices outlined in this document help organizations measure their residual risks better, particularly the safety risks associated with potential cybersecurity issues in motor vehicles and motor vehicle equipment that they design and manufacture. Further, it provides a toolset of techniques they can utilize commensurate to their measured risks, and take appropriate actions to reduce or eliminate them, and in doing so lower the future liabilities these risks represent in terms of safety risks to public and business costs associated with addressing them.

In addition, quantitatively positive externalities have been shown to stem from vehicle safety and security measures (Ayres & Levitt, 1998). The high marginal cost of cybersecurity

failures (crashes) extend to third parties. Widely accepted adoption of sound cybersecurity practices limits these potential costs and lessens incentives for attempts at market disruption (i.e., signal manipulation, GPS spoofing, or reverse engineering).

How do I prepare and submit comments?

Your comments must be written and in English. To ensure that your comments are filed correctly in the docket, please include the docket number of this document in your comments. Your comments must not be more than 15 pages long (49 CFR 553.21). NHTSA established this limit to encourage you to write your primary comments in a concise fashion. However, you may attach necessary additional documents to your comments. There is no limit on the length of the attachments. Please submit one copy (two copies if submitting by mail or hand delivery) of your comments, including the attachments, to the docket following the instructions given above under ADDRESSES. Please note, if you submit comments electronically as a PDF (Adobe) file, NHTSA asks that the documents submitted be scanned using an Optical Character Recognition (OCR) process, thus allowing the Agency to search and copy certain portions of your submissions.

How do I submit confidential business information?

If you wish to submit any information under a claim of confidentiality, you should submit three copies of your complete submission, including the information you claim to be confidential business information, to the Office of the Chief Counsel, NHTSA, at the address given above under FOR FURTHER INFORMATION CONTACT. In addition, you may submit a copy (two copies if submitting by mail or hand delivery), from which you have deleted the claimed confidential business information, to the docket by one of the methods given above under ADDRESSES. When you send a comment containing information claimed to be confidential

business information, you should include a cover letter setting forth the information specified in NHTSA's confidential business information regulation (49 CFR part 512).

Will the Agency consider late comments?

NHTSA will consider all comments received before the close of business on the comment closing date indicated above under **DATES**. To the extent possible, the Agency will also consider comments received after that date. Given that we intend for the guidance document to be a living document and to be developed in an iterative fashion, subsequent opportunities to comment will also be provided necessarily.

How can I read the comments submitted by other people?

You may read the comments received at the address given above under COMMENTS. The hours of the docket are indicated above in the same location. You may also see the comments on the Internet, identified by the docket number at the heading of this document, at *http://www.regulations.gov*.

Issued in Washington D.C. under authority delegated in 49 CFR 1.95 and 501.8.

_____

Cem Hatipoglu
Associate Administrator for Vehicle Safety Research