BEFORE THE
NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION

CYBERSECURITY BEST PRACTICES FOR THE SAFETY OF MODERN VEHICLES
DOCKET NO. NHTSA–2020–0087

COMMENTS OF THE CONSUMER TECHNOLOGY ASSOCIATION

Jamie Susskind
Vice President, Policy and Regulatory Affairs

Mike Bergman
Vice President, Technology & Standards

Mitchell Kominsky
Director of Government Affairs

Consumer Technology Association
1919 S. Eads Street
Arlington, VA 22202

Megan L. Brown
Katy J. Milner
Charles S. Farlow
Wiley Rein LLP
1776 K St. NW
Washington, DC 20006

Counsel to Consumer Technology Association

March 15, 2021

TABLE OF CONTENTS

I. INTRODUCTION AND SUMMARY

The Consumer Technology Association ("CTA"),[1] which represents thousands of members that encompass the $422 billion U.S. consumer technology industry—including leaders in vehicle technology—welcomes this opportunity to engage with the National Highway Traffic Safety Administration ("NHTSA") on the significant issue of cybersecurity for all types of vehicles. This update to the first edition of NHTSA's *Cybersecurity Best Practices for Modern Vehicles* is timely, as much has changed in the automotive and cybersecurity landscape since the document's initial 2016 release.[2] This guidance is especially significant as cybersecurity is key to protecting mission-critical systems. CTA and its members agree that a proactive approach to addressing vehicle cybersecurity threats will improve automotive safety and benefit all Americans.

CTA welcomes NHTSA's efforts to complement ongoing automotive industry efforts by updating the best practices. Experience has shown that best practices, developed with well-informed input by the automotive industry and based on international standards, can help reflect and promote innovation. Such documents are most effective and useful when the guidance is non-binding and voluntary and practices can be adapted as new products and services are rolled out. While the draft helpfully lays out standards, guidelines and other references to international best practices for vehicle cybersecurity, certain aspects of the draft can be refined to provide a more solid foundation for proactive, risk-based approaches to vehicle cybersecurity challenges.

[1] As North America's largest technology trade association, CTA® is the tech sector. Our members are the world's leading innovators—from startups to global brands—helping support more than 18 million American jobs. CTA owns and produces CES®—the most influential tech event on the planet.

[2] NHTSA, Request for Comments, Cybersecurity Best Practices for the Safety of Modern Vehicle, Docket No. NHTSA–2020–0087, 86 Fed. Reg. 2481 (Jan. 12, 2021) ("Draft Best Practices").

Specifically, NHTSA should:

- ensure that the best practices incorporate the key principles of flexibility and adaptability;
- clarify recommendations that can be read as prescriptive rather than illustrative;
- refrain from adopting recommendations where the issues are still being analyzed and solutions evaluated, such as software issues;
- strengthen the draft by adding discussion of the role of end users and the concept of recovery, as well as incorporating foundational resources and standards; and
- avoid transforming information sharing and vulnerability disclosure practices into rigid requirements or mandates.

With these changes, NHTSA can promote industry implementation and help the technology and automotive sectors continue to secure vehicles and protect users across the U.S.

II. THE TECH SECTOR, INCLUDING THE AUTOMOTIVE SECTOR, ADDRESSES CYBERSECURITY IN SEVERAL WAYS.

CTA and its members, individually and collectively, are advancing cybersecurity in the automotive sector. ***First***, they allocate resources to innovation and technology development. CTA is a leader in advocating for innovation in transportation, and many of CTA's members are developing self-driving technologies and components, in addition to assisted driving technology aftermarket solutions to increase automotive safety for the over 276 million vehicles already on the road today. In particular, automotive sector companies are using innovative solutions to improve cybersecurity, including defense-in-depth, security by design, increasing system and component resilience, and aggressively managing vulnerabilities, including through "bug bounty" programs.[3] The automotive sector uses a multi-pronged approach to cybersecurity, with

[3] *See, e.g.*, Caleb Watney and Cyril Draffin, R Street Institute, Research Report, *Addressing New Challenges in Automotive Cybersecurity* at 6-7 (Nov. 1, 2017) *available at* https://www.jstor.org/stable/resrep19133.

research and development, internal teams that address cyber risk, third-party experts, field testing, government partnerships and state-of-the art cybersecurity protections.[4]

Second, the automotive industry helps develop effective cybersecurity practices for connected devices generally and for vehicles in particular. For example, CTA's pioneering work includes collaborating on the Council to Secure the Digital Economy's C2 Consensus on IoT Device Security Baseline Capabilities[5] and publishing a standard on Baseline Cybersecurity Standard for Devices and Device Systems,[6] CTA-2088, which provides a clear, unambiguous list of cybersecurity capabilities that any connected consumer device should have. While rooted in guidance from the Internet of Things ("IoT") landscape, in many cases these standards and recommendations are flexible enough to be adapted for the automotive industry.[7] Other resources address the unique characteristics of the automotive industry, such as guidance and reports published by the US Auto Information Sharing and Analysis Center ("Auto-ISAC"). The NHTSA best practices should draw on these efforts, and NHTSA may wish to clarify where the unique needs of the automotive industry have led to specialized approaches.[8]

---

[4] *See, e.g.* Global Automotive OEM Cyber Security Layout Report 2020: OEMs are Vigorously Seeking External Collaborations on Vehicle, Communication, Platform, Data, and Applications, https://www.prnewswire.com/news-releases/global-automiotive-oem-cyber-security-layout-report-2020-oems-are-vigorously-seeking-external-collaborations-on-vehicle-communication-platform-data-and-applications-301223020.html (Feb. 5, 2021).

[5] Council to Secure the Digital Economy, The C2 Consensus on IoT Device Security Baseline Capabilities *available at* https://securingdigitaleconomy.org/wp-content/uploads/2019/09/CSDE_IoT-C2-Consensus-Report_FINAL.pdf ("CSDE C2 Baseline").

[6] ANSI/CTA-2088, Baseline Cybersecurity Standard for Devices and Device Systems, https://shop.cta.tech/collections/standards/products/baseline-cybersecurity-standard-for-devices-and-device-systems-cta-2088.

[7] Another CTA member collaboration, CTA-CEB37, *Recommended Practice on Proper Use of the OBD-II Port* is automotive specific.

[8] In this regard, NHTSA could clarify that the unique security considerations of the connected vehicle and the unique structure of the automotive industry lead to different approaches from general IoT categories. The automotive industry may borrow from such general IoT category standards but should rely more on domain-centric international and industry standards (such as International Organization for Standardization ("ISO")/SAE International ("SAE") Draft International Standard (DIS) 21434 and UNECE WP.29 regulatory frameworks). NHTSA appropriately incorporates these domain-specific standards in this draft, using the broad stakeholder input

Third, the auto industry collaborates to address cybersecurity threats. Vehicle cybersecurity requires input and collaboration among many stakeholders, from original equipment manufacturers ("OEMs") to software developers, hardware suppliers, aftermarket integrators, dealers and more. These distinct stakeholders each play a role and can bolster each other's efforts in countering cyberthreats. One example of effective industry collaboration is participation in the Auto-ISAC, which encourages meaningful interaction among automotive companies to share updates and discuss strategies.

Fourth, the auto industry is engaged on international standards, which are key to addressing cybersecurity in a harmonized fashion and provide the foundation for developing and implementing best practices. NHTSA's draft recognizes the value of industry-led, voluntary standards and notes that the best practices are intended to build on standards such as the International Organization for Standardization ("ISO")/SAE International ("SAE") Draft International Standard (DIS) 21434, "Road vehicles – Cybersecurity engineering," which is nearing finalization.[9] This document specifies requirements for cybersecurity risk management regarding engineering for concept, development, production, operation, maintenance, decommissioning and end of cybersecurity support for road vehicle electrical and electronic (E/E) systems, including their components and interfaces. Industry recognizes that the ISO/SAE 21434 standard provides the foundation for UNECE WP.29 cyber security regulation,[10] and work

---

that is part of such standards. More general IoT Security requirements in development (such as NISTIR 8259D) are excluded from the current draft, as is appropriate.

[9] Draft Best Practices at 2, Section 3. ISO/SAE 21434, "Road vehicles – Cybersecurity engineering," *available at* https://www.sae.org/standards/content/iso/sae21434.d1/. The final version of this document is expected in the second quarter of 2021.

[10] "UN Regulation on uniform provision concerning the approval of vehicles with regards to cyber security and cyber security management system" (UN Regulation No. 155) available at http://www.unece.org/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf.

is underway on the ISO 24089 standard that supports UNECE WP.29 software updates regulation.[11] NHTSA's best practices should draw on these well-sourced resources to ensure that its guidance is based in real-life practices and appropriate for effective implementation by the automotive industry.

III. NHTSA'S BEST PRACTICES SHOULD BE GUIDED BY THE PRINCIPLES OF FLEXIBILITY AND ADAPTABILITY.

NHTSA, CTA, and the automotive industry share the same goal—understanding, preventing and resolving cybersecurity vulnerabilities that could impact safety. NHTSA can most effectively advance this goal by establishing voluntary, flexible best practices as guideposts for industry. Non-binding, adaptable best practices will encourage industry to continue taking a proactive approach and will support innovation in this fast-moving space. Regulation—and even guidance—will always lag behind real world developments. Binding the industry to specific practices could impede innovation and cyber threat responses, particularly where novel issues are presented.

CTA appreciates NHTSA's desire for a flexible document, easily adaptable for entities of any size playing any role in the automotive industry,[12] and urges NHTSA to preserve this concept in the final version. The final version should explicitly state that the best practices are meant to be used flexibly by the automotive industry, as appropriate to each industry segment and organization, based on their individualized risk assessments, rather than one uniform policy applied to all systems. The best practices should underscore the importance of establishing a

[11] For example, UNECE WP.29 on Cybersecurity regulation for connected vehicles (R155) is a valuable resource based on industry input. In parallel, work is underway on ISO 24089 on software updates for road vehicles, which provides foundational support for UNECE WP.29 Software update regulation for connected vehicles (R156).

[12] *See, e.g.* 86 Fed. Reg. at 2485 ("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.").

culture of security throughout the organization, be it a small business or global corporation.[13] In addition, given how much the landscape has changed since the Best Practices were released in 2016 and the unceasing pace of innovation, NHTSA should focus on making the updated best practices durable over time. Additionally, NHTSA should strive for a balanced approach between security and safety. While cybersecurity is important to ensure safety, an approach to cybersecurity that is too rigid or inflexible could lead to unintended consequences that actually impact safety.[14]

In a few areas, the best practices can be read as prescriptive rather than illustrative; these instances should be revised and clarified. For example, the draft calls on manufacturers to consider and address enumerated risks, noting a concern about manipulation of vehicle sensor data, such as GPS spoofing.[15] GPS spoofing is an area of ongoing research, both in terms of possible attacks (likelihood and severity) and mitigations; no conclusions or one-size-fits-all solutions exist that lend themselves to incorporation in motor vehicle industry best practices at this time. For now, NHTSA should ensure that its guidance focuses on encouraging vehicle manufacturers to stay abreast of all threats and include them in appropriate risk analyses.

Other new technologies will likewise require careful and iterative consideration. As CTA has explained, "Prominent displays and app integration are key components in [automotive

[13] For example, Section 4.1 of the draft discusses the need to "emphasis[e] the importance of cybersecurity from the leadership level down to the staff level." Draft Best Practices at 4.

[14] For example, if a two-factor authentication check is activated while the vehicle is in motion, there may be driver distraction or even the locking up of an important function, creating a hazardous situation. Another example might be a subsystem refusing to perform its function because a certificate expired overnight. Generally, designers will avoid such risky system architecture choices and policy should be flexible enough to permit them to do so.

[15] *See, e.g.* Draft Best Practices at 5.

evolution]. But now, those are complemented by more inconspicuous tech, including in-cabin sensors for detecting a driver's or passenger's mood and human-machine interfaces (HMIs)."[16]

The use of artificial intelligence ("AI") in vehicles[17] and the rise of connected and autonomous vehicles are also generating substantial investment and innovation and may raise complex issues.[18] Biometrics are promising and may lead to innovation, including in security.[19] For example, AI-based machine vision innovations have led to improvements addressing problems such as "infants and children accidentally left in the car, drivers falling asleep, and distracted driving."[20] Industry needs flexibility to harness new technology and nimbly manage security in new contexts. NHTSA should ensure its document promotes flexibility to explore and anticipate new challenges and avoids focusing on discrete risks that are likely to evolve. Doing so will make the document more durable, practical, and implementable.

IV. THE BEST PRACTICES MAY BE OVER COMPLICATED BY ATTEMPTING TO ADDRESS SOFTWARE ISSUES.

NHTSA has done an impressive analysis of the challenges facing industry in addressing cybersecurity, and offers practical, clear and effective cybersecurity practices. Many of the topics addressed in the draft are well understood by the automotive industry; some recommendations are already implemented, while other topics raise complex issues that require continuing

---

[16] CTA, R. Calem, *The Car Cockpit of the Future* (Jan 3, 2020), available at https://www.cta.tech/Resources/i3-Magazine/i3-Issues/2020/January-February/The-Car-Cockpit-of-the-Future

[17] Innovation abounds in AI-enabled driver assistance, sensors, telematics, fleet monitoring and more from companies like Nvidia, Panasonic Automotive, Lytx, and others.

[18] *See* "Cybersecurity Challenges in the Uptake of Artificial Intelligence in Autonomous Driving" (https://www.enisa.europa.eu/publications/enisa-jrc-cybersecurity-challenges-in-the-uptake-of-artificial-intelligence-in-autonomous-driving) and "ENISA Good Practices for Security of Smart Cars" (https://www.enisa.europa.eu/publications/smart-cars).

[19] *See, e.g.* Robert E. Calem, CarSmarts: the Future of Vehicle Tech, ITIS Innovation, (Dec. 11, 2018) *available at* https://www.cta.tech/Resources/i3-Magazine/i3-Issues/2018/November-December/Car-Smarts-The-Future-of-Vehicle-Tech

[20] Tech Briefs, AI-Based Machine Vision & the Future of Automotive In-Cabin Technologies (May 1, 2020) *available at* https://www.techbriefs.com/component/content/article/tb/supplements/pit/features/articles/36873

collaboration and consensus before being ripe for inclusion in the NHTSA best practices. The topic of software in particular raises challenges. Because this topic involves cooperation and buy-in among many automotive sector participants at varying points in the vehicle development, component sourcing, production, and lifecycle, a light touch approach will be particularly important. NHTSA should not rush and dilute otherwise actionable efforts by adopting best practices regarding software.

Cybersecurity related to software is being analyzed by the automotive industry on a company-by-company basis and collectively in several fora. While the draft offers suggestions on managing software cybersecurity considerations,[21] the automotive industry is evaluating this issue through participation in standards development and with best practices developed by stakeholders other than NHTSA. For example, the automotive industry is working on development of ISO/SAE 21434, a consensus standard regarding cybersecurity through the vehicle lifecycle, as well as ISO 24089 on software updates for road vehicles.[22] In addition, BSA The Software Alliance has developed a comprehensive framework for secure software[23] that maps to the U.S. National Institute for Standards and Technology ("NIST") "Secure Software Development Framework."[24] These are all useful tools to help stakeholders in the software industry address security risk. NHTSA should not duplicate efforts or issue potentially

[21] *See, e.g.* Draft Best Practices at 16-17.

[22] ISO CD 24089, "Road vehicles — Software update engineering," *available at* https://www.iso.org/standard/77796.html.

[23] BSA The Software Alliance, BSA Framework for Secure Software, https://www.bsa.org/reports/updated-bsa-framework-for-secure-software.

[24] NIST, Computer Security Resource Center, White Paper, Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework, https://csrc.nist.gov/publications/detail/white-paper/2020/04/23/mitigating-risk-of-software-vulnerabilities-with-ssdf/final.

conflicting guidance. Further, if best practices are adopted at this time or in the future, NHTSA should ensure that its guidance is linked to these foundational industry efforts.

Work also continues on specific software-directed efforts. The tech industry continues to explore cybersecurity solutions related to a software bill of materials ("SBOM") and work toward laying the groundwork for implementation in the future. While the National Telecommunications and Information Administration's ("NTIA") multi-stakeholder process has made excellent progress, NHTSA should be cautious about indicating that SBOM is a readily available solution. More, solutions may include use of a software composition analytic tool to identify components and verify associated vulnerabilities; these types of innovations and solutions are still being assessed.[25] NHTSA should avoid rigid or prescriptive guidance on software or SBOM at this time and be mindful of the evolution of industry-developed practices and standards as it continues to consider this topic.

V. KEY REFINEMENTS AND ADDITIONS

CTA offers suggestions for modifications to the draft intended to boost its utility for the automotive industry and help encourage adoption.

A. *The Draft Does Not Discuss the Role of End Users.*

As NHTSA acknowledges, the automotive ecosystem is vast and includes "small and large volume motor vehicle and motor vehicle equipment designers, suppliers, manufacturers, modifiers, and alterers," and "all individuals and organizations involved in the design,

[25] NTIA is also working with stakeholders on addressing SBOM. *See* NTIA Software Component Transparency, https://www.ntia.doc.gov/SoftwareTransparency (Jan. 13, 2021). However, NITA has acknowledged the unique challenges for SBOM in the automotive space, including the longer supply chain, greater number of players, and more lead time, and concerns about public disclosures. NTIA, SBOM: An Update on Efforts for Transparency in the Software Supply Chain, Presentation by Allan Friedman PhD, https://www.automotiveisac.com/wp-content/uploads/2020/05/2020_05_12_Friedman_AutoISAC_SBOM_CommunityCall.pdf (May 12, 2020).

manufacturing, and assembly of a motor vehicle have a critical role to play with respect to vehicle cybersecurity."[26] However, the draft omits discussion of one critical segment of the ecosystem—the role of drivers and end users. CTA has deep experience working with companies *and consumers* on these issues and urges NHTSA not to overlook this critical part of vehicle cybersecurity.

Security is often referred to as "team sport" and requires end users to do their part. Sometimes security information needs to be communicated to users (here, drivers and passengers) and others. The draft does not address this part of the ecosystem for connected vehicles, perhaps missing an opportunity to at least highlight this important area. This is in stark contrast to work at other agencies, such as the Food and Drug Administration, which is looking at the complexities in communicating security information to consumers.[27] Other resources have considered what consumers should know about their devices and any accompanying cybersecurity risks.[28] The best practices should acknowledge the differing roles of stakeholders, including users, and delineate the work-split where possible.

CTA acknowledges that consumer engagement may be complicated in the automotive sector because consumers may have robust—or little—contact with responsible entities. Consumers may also have different levels of sophistication and interest in modern vehicle components. For example, consumers may love or not use mobile management software,

---

[26] Draft Best Practices at 1-2.

[27] *See, e.g.* FDA, Patient Engagement Advisory Committee, Communicating Cybersecurity Vulnerabilities to Patients: Considerations for a Framework, Discussion Paper and Request for Feedback (Oct. 2020), https://www.fda.gov/media/143000/download.

[28] *See, e.g.* ENISA Baseline Security Recommendations for IoT at Annex A, End-of-life support *available at* https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot; FTC, Mobile Security Updates: Understanding the Issues, at 31-32, 71-73 https://www.ftc.gov/system/files/documents/reports/mobile-security-updates-understanding-issues/mobile_security_updates_understanding_the_issues_publication_final.pdf (Feb. 2018) (noting complexities of mobile device security updating, particularly with respect to consumer education and information disclosures).

infotainment solutions, and aftermarket products and services. Resale and warranty issues may likewise be complex. NHTSA should add discussion of the role of consumers with respect to cybersecurity to the best practices and may want to seek more information on how to address this particular segment – possibly in a future proceeding or guidance document.

B. *The Draft Should Better Use Third-Party Standards and Resources.*

NHTSA is right to center the document on voluntary, industry-led, international consensus standards but should explicitly encourage agility to use future standards. CTA is a proponent of voluntary, consensus-based standards for several reasons. Standards can enable cost-effective introduction of new technologies while helping drive competition. Standards can move at the speed of innovation, rather than at the speed of regulation. And reliance on standards also helps ensure consistency across global manufacturers.

The standard cited throughout the draft, ISO/SAE 21434, supports foundation of the best practices as it draws on expert recommendations from companies and nations around the globe on automotive cyber risk assessment and analysis. The standard is applicable to NHTSA's guidance regarding appropriate corporate processes and is written in a technology agnostic manner to cover rapid industry evolution. There are also useful standards in place for vulnerability disclosure (ISO/IEC 29147:2018); vulnerability handling (ISO/IEC 30111:2019 and subsequent amendments), and information security incident management (ISO/IEC 27035-1:2016), among others. Existing standards should be leveraged to support evolving auto industry best practices. These include relevant standards and best practices for the embedded and hardware sectors, which may raise unique considerations.[29] However, NHTSA best practices

[29] *See e.g.*, Center For Cybersecurity Policy And Law, Improving Hardware Component Vulnerability Disclosure White Paper (2019), https://static1.squarespace.com/static/5acbb666f407b432519ab15e/t/5cc86f37c830251f28d258fc/1556639544235/T

should not be too wedded to any one standard, as industry will move quickly and evolve. There is no one right way to mitigate cybersecurity risk, and NHTSA should acknowledge that there are many ways to reasonably address cybersecurity.

Further, for enterprise-level security, industry already has a useful starting point for addressing cybersecurity risk management in the NIST Cybersecurity Framework.[30] CTA has championed use of the NIST Cybersecurity Framework and urges NHTSA to reference it, other NIST documents and other valuable resources[31] in the final draft to ensure maximum compatibility and consistency with related workstreams.

C. *The Draft Should Refine Some Concepts, Like "Recovery."*

Finally, NHTSA should elaborate on the concept of cybersecurity "recovery" in the draft. The draft notes the NIST Cybersecurity Framework is "structured around the five principal functions 'Identify, Protect, Detect, Respond, and Recover.'"[32] While NHTSA addresses the first four elements in some detail, the draft does not discuss what it means to "recover" or include a section on "recovery." As NIST has identified, recovery is a critical element of cybersecurity and therefore the concept merits expansion in the draft. Here too, however, NHTSA should employ a light touch and take care to not bind companies to an overly rigid definition, as companies will

---

he+Center+for+Cybersecurity+Policy+and+Law_Improving+Hardware+Component+Vulnerability+Disclosure_April+2019.pdf.

[30] NIST, Cybersecurity Framework Version 1.1. https://www.nist.gov/cyberframework/framework (last updated Oct. 2, 2020) ("NIST Cybersecurity Framework"). The NIST Cybersecurity Framework provides general guidance to all critical infrastructure sectors and is focused at the enterprise or organization level.

[31] For example, CTA supports the work of the Cloud Security Alliance and The Open Web Application Security Project.

[32] Draft Best Practices at 3, G.1.

need flexibility to define recovery based on their own organization and make risk-based determinations on how to proceed in a given situation.[33]

VI. NHTSA SHOULD ENSURE THAT ITS BEST PRACTICES DO NOT BECOME INFORMATION SHARING OR REPORTING MANDATES.

NHTSA should tread carefully in developing best practices about information sharing and vulnerability reporting. Sharing cybersecurity information among industry and with government is vital, and that is why the automotive sector works with government. In recognition of the value of this component of managing cyber risk, NIST, NTIA, the Department of Homeland Security, and other agencies regularly examine how to improve information sharing, and policymakers are looking at ways to promote supply chain information sharing.[34] However, there are complex practical and legal issues associated with information sharing, and NHTSA's best practices should avoid binding directives and recognize that sharing must be left to individual organizations.

Information sharing is common across the automotive sector in certain contexts with appropriate protections. For example, the Auto-ISAC facilitates industry's cybersecurity-related information sharing among its members.[35] NHTSA can encourage continued participation in this well-functioning, voluntary process by amending best practice G.30 to add a suggestion that the response process include reporting incidents, exploits, and vulnerabilities to the Auto-ISAC as

---

[33] For example, the NIST Cybersecurity Framework offers a definition of "Recover" and identifies categories of action under that function for individual entity consideration. *See* NIST Cybersecurity Framework Section 2.1, Framework Core.

[34] *See, e.g.*, NIST, SP 800-150, *Guide to Cyber Threat Information Sharing* (2016), https://csrc.nist.gov/publications/detail/sp/800-150/final; National Telecommunications and Information Administration, Notice, *Request for Public Comment, Promoting the Sharing of Supply Chain Security Risk Information Between Government and Communications Providers and Suppliers*, Docket No. 200609–0154, 85 Fed. Reg. 35919 (June 12, 2020).

[35] Executive Order 13691, Promoting Private Sector Cybersecurity Information Sharing (Feb. 13, 2015).

soon as possible. The final best practices should also encourage companies to become members of Auto-ISAC, as the draft does in G.24(a).

But there can be risks in sharing cybersecurity information, as Congress knew when it enacted the Cybersecurity Information Sharing Act of 2015. As industry has seen, third parties have tried to seek disclosure of shared cybersecurity information, which threatens to chill beneficial cooperation.[36] In addition, there are other risks in poorly executed information sharing, such as in premature vulnerability disclosure. Disclosures can be counterproductive if made prior to a remediation being publicly available, which is why NTIA, ISO and others have devoted time to considering how best to manage multi-party vulnerability disclosure.[37] As CTA has long advocated to the federal government, while discovering and addressing vulnerabilities are important elements of cybersecurity risk management, there are inherent challenges, particularly in multi-party coordinated vulnerability disclosure which "involves numerous entities with different roles, and sharing information among them is not straightforward."[38] In light of these concerns, every organization should determine for itself whether, what, and how to share.

---

[36] *See e.g.,* Cybersecurity, Information Sharing and Partnership, Hearing Before Subcomm. on Oversight and Investigations of the H.Comm. on Energy and Commerce (Apr. 4, 2017) (Testimony of Denise Anderson), https://docs.house.gov/meetings/IF/IF02/20170404/105831/HHRG-115-IF02-Wstate-AndersonD-20170404.pdf (describing subpoena to Auto-ISAC, noting "the concern is that if courts were to allow broad sweeps for information and using ISACs as one stop shops to accomplish it, such actions would effectively kill information sharing").

[37] For example, several broadly adopted industry best practices also suggest implementing sharing rules to help prevent dissemination of information that, if improperly disclosed, could have adverse consequences for an organization or its customers. *See, e.g.* NIST SP-800-150, Guide to Cyber Threat Information Sharing, at 9-12 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf (Oct. 2016). For example, an entity may determine it needs to limit the disclosure to those entities essential to the remediation process (*e.g.*, those engaged in mitigation development), aiming to reduce the risk for end-users due to premature disclosure.

[38] *See, e.g.* CTA Comments on NIST Draft 2 of Version 1.1. of the Framework for Improving Critical Infrastructure Cybersecurity (filed Jan. 19, 2018). Indeed, these efforts may not be led by the original vendor.

That said, many companies have found ways to balance these concerns and embraced vulnerability disclosure programs,[39] and incentivized public crowd-sourced research programs ("bug bounties") including those provided by third party vendors like HackerOne and Bug Crowd. These participants have reported meaningful improvements in cybersecurity as a result. Approaches in this space are not uniform or one-size-fits all, and NHTSA should not mandate participation in information sharing, vulnerability disclosures, or bug bounties.

Finally, there may be several workable options for vulnerability sharing and the determination of which tools to engage must fall to the individual organization. CTA's work on the CSDE C2 Baseline reflects the importance of voluntary vulnerability submission and handling processes, but also notes that organizations need to have their own processes and prioritizations. These processes may include participation in threat sharing programs, working directly with third parties or other initiatives.[40] In light of the need for customization and flexibility, too much "specificity" on information sharing in these best practices may be counterproductive to the goal of securing vehicles against cyber threats. NHTSA should enable industry to navigate these complex considerations on an individual entity basis.

VII. CONCLUSION

CTA thanks NHTSA for the opportunity to comment on the draft best practices. Risk-based best practices can be integral to approaching and addressing cybersecurity challenges, but best practices must be voluntary, adaptable and fluid to promote utility and effectiveness. CTA and its members are committed to working with NHTSA and standards bodies and on this and

[39] Examples include: GM https://hackerone.com/gm?type=team; Toyota https://hackerone.com/toyota?type=team; Ford https://hackerone.com/ford?type=team; Stellantis https://bugcrowd.com/stellantis; Telsa https://www.tesla.com/about/security; and Mercedes Benz https://www.mercedes-benz.com/en/whitehat/.

[40] *See* CSDE C2 Baseline Section 5.2.1.

other industry-led collaborative efforts to identify strategies to ensure vehicle systems are safe and secure.

Respectfully submitted,

CONSUMER TECHNOLOGY ASSOCIATION

By: */s/ Jamie Susskind*

Jamie Susskind
Vice President, Policy and Regulatory Affairs

Mike Bergman
Vice President, Technology & Standards

Mitchell Kominsky
Director of Government Affairs

Consumer Technology Association
1919 S. Eads Street
Arlington, VA 22202

Megan L. Brown
Katy J. Milner
Charles S. Farlow
Wiley Rein LLP
1776 K St. NW
Washington, DC 20006

Counsel to
Consumer Technology Association

March 15, 2021