aws

March 15, 2021

Via Electronic Submission Only

Dr. Steven Cliff
Acting Administrator
National Highway Traffic Safety Administration
U.S. Department of Transportation
1200 New Jersey Ave, SE, West Building
Washington, DC 20590

Re: Docket No. NHTSA-2020-0087
Federal Register: 86 Fed. Reg. 2481 (January 12, 2021)
Request for Comments

Dear Acting Administrator Cliff,

Amazon Web Services, Inc. ("AWS") welcomes this opportunity to comment on the National Highway Traffic Safety Administration's ("NHTSA" or the "Agency") Request for Comments, *Cybersecurity Best Practices for the Safety of Modern Vehicles*.[1]

AWS is a Cloud Service Provider ("CSP"). Among other things, our comments reflect our experiences providing commercial cloud services to a global customer base and adhering to the highest international security standards, including compliance within existing applicable certifications and accreditations. AWS provides highly reliable, low-cost cloud services that power hundreds of thousands of businesses in 190 countries around the world. AWS also provides a full suite of service in the automotive industry to support Advanced Driver Assistance Systems ("ADAS") and autonomous vehicle development and deployment. Thus, AWS has a strong interest in this matter.

AWS strongly supports NHTSA's continued commitment to address cybersecurity challenges - through a voluntary, best practices approach - that have safety implications for motor vehicles and equipment.

As the Agency states in its Federal Register notice, its "recommendations … focus on cybersecurity best practices that have safety implications for motor vehicles and motor vehicle equipment."[2] While AWS applauds the Agency for taking action to address the safety implications that may be created by cybersecurity vulnerabilities, as it has in past initiatives, the

[1] *Cybersecurity Best Practices for the Safety of Modern Vehicles*, 86 Fed. Reg. 2481 (Jan. 12, 2021) ("Request for Comments").
[2] *Id.*

Agency should continue to strike an appropriate balance between ensuring motor vehicle safety and supporting and enhancing innovation in the industry.

Further, the Agency should ensure that its cybersecurity best practices are aligned with existing internationally recognized standards. In doing so, the Agency may promote collaboration among industry stakeholders, address additional areas to improve vehicle cybersecurity, and ensure that motor vehicles and equipment are "designed free of unreasonable risk to motor vehicle safety,"[3] consistent with the Agency's objectives.

I. NHTSA Should Ensure Further Integration of Proposed Cybersecurity Best Practices to Existing Internationally Recognized Security Standards.

The Agency expressed in various parts of the Request for Comments that NHTSA is committed to aligning its Cybersecurity Best Practices "to key industry cybersecurity-related initiatives and efforts by organizations such as SAE International ("SAE"), the International Organization for Standardization ("ISO"), the National Institute of Standards and Technology ("NIST"), and the Automotive Information Sharing and Analysis Center ("Auto-ISAC"),"[4] and that the proposed best practices are generally "consistent with guidelines, standards and best practices developed by these organizations."[5] Specifically, the Agency referenced "ISO/SAE Draft International Standard (DIS) 21434, Road Vehicles- Cybersecurity Engineering" and Auto-ISAC best practices as being the bases for the Agency's proposed cybersecurity beset practices.[6]

The Agency's specific proposed best practices should fully reflect these considerations. For example, best practice G.1 found in Section 4 of the Proposed Cybersecurity Best Practices currently provides:

> The automotive industry should follow the National Institute of Standards and Technology's (NIST's) documented Cybersecurity Framework, which is structured around the five principal functions "Identify, Protect, Detect, Respond, and Recover," to build a comprehensive and systematic approach to developing layered cybersecurity protections for vehicles.[7]

As drafted, proposed best practice G.1 in the Proposed Cybersecurity Best Practices only relies on NIST's cybersecurity framework as a reference for a general guidance for the automotive industry. But elsewhere, in proposed best practice G.23, NHTSA states:

[3] National Highway Traffic Safety Administration, "*Cybersecurity Best Practices for Modern Vehicles*," (October 2016) at 5 available at https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/812333_cybersecurityformodernvehicles.pdf (Last accessed March 8, 2021 ("2016 Best Practices").

[4] Request for Comments at 2482.

[5] *Id.*

[6] *Id.* at 2483. *See also* https://automotiveisac.com/best-practices/

[7] *Cybersecurity Best Practices for the Safety of Modern Vehicles, Draft 2020 Update*, Docket No. NHTSA-2020-0087 (Jan. 11, 2021) ("Proposed Cybersecurity Best Practices").

> Manufacturers should actively participate in automotive industry-specific best practices and standards development activities through Auto-ISAC and other recognized standards development organizations.

With this context, proposed best practice G.1 should be revised to acknowledge that industry stakeholders can and should be encouraged to develop their cybersecurity programs consistent with all applicable internationally recognized security standards, as appropriate.

The Agency should also incorporate existing internationally recognized standards developed by the industry and standard developing organizations in internet of things ("IoT") security and secure device component configuration into its Proposed Cybersecurity Best Practices. For example, Cloud Security Alliance Controls and ISO, among other organizations, have various standards applicable to IoT and secure device component configuration.[8]

Furthermore, the Proposed Cybersecurity Best Practices should implement a differentiation between cybersecurity of the overall ecosystem (i.e., the various companies and stakeholders within the cybersecurity landscape) and technical component standards applicable to individual components and/or pieces of equipment. As drafted, the Proposed Cybersecurity Best Practices commingle requirements that would apply equally to the broader ecosystem and to individual components. Separating the requirements would allow for manufacturers to focus on secure component development, while allowing downstream OEMs and integrators to focus on the security of the overall ecosystem.

AWS also believes that the Proposed Cybersecurity Best Practices would benefit from further alignment with internationally recognized standards concerning remote software updates and wireless security. While the Agency addressed various issues in the Proposed Cybersecurity Best Practices, including over-the-air software updates, the Agency should align its principles concerning remote software updates and wireless security with existing software security design principles, such as the Open Web Application Security Project. The Agency should also include vehicle owners in the applicable update/awareness processes.

Further, the Agency should consider segmentation of best practices applicable to critical safety operational systems and consumer environment, similar to the standards applicable to the aerospace industry. By allowing for a consumer environment, NHTSA can foster innovation in consumer technology in an appropriate way. Indeed, this approach is consistent with NHTSA's previous views on consumer-oriented technologies. As NHTSA opined in various public documents, the National Traffic and Motor Vehicle Safety Act, as amended, requires manufacturers to "ensure that systems are designed free of unreasonable risks to motor vehicle safety, including those that may result due to existence of potential cybersecurity

[8] *See, e.g.*, ISO/IEC 21823-1:2019 Internet of things (IoT) — Interoperability for IoT systems — Part 1: Framework available at https://www.iso.org/standard/71885.html#:~:text=ISO%2FIEC%2021823%2D1%3A2019(E)%20provides,for%20interoperability%20for%20IoT%20systems.&text=This%20document%20provides%20a%20common,the%20various%20entities%20within%20them (Last accessed March 8, 2021) ; CSA IoT Security Controls Framework v2 available at https://cloudsecurityalliance.org/artifacts/csa-iot-security-controls-framework-v2/ (Last accessed March 8, 2021)

vulnerabilities."[9] NHTSA also has emphasized over time, in various public documents, that it is committed to striking an appropriate balance between legitimate public concerns and supporting innovation in emerging technologies.[10]

Consistent with NHTSA's prior teachings, the Agency should therefore ensure that all cybersecurity systems are designed free of unreasonable risks to motor vehicle safety, while also providing for sufficient flexibility for the industry to remain innovative and competitive in consumer technology, while at the same time being able to tailor applicable cybersecurity requirements to the appropriate level of risk. Such an approach would not only promote cybersecurity, but also help preserve flexibility, innovation and open integration.

II. NHTSA Should Foster Collaboration Across the Industry to Recognize Vehicle Cybersecurity Throughout the Vehicle Lifecycle.

In the Request for Comments, the Agency states, at various parts, that it is important to address cybersecurity with "proactive measures taken across the vehicle lifecycle."[11] Similarly, NHTSA recognizes the importance of developing best practices that "include cybersecurity considerations along the entire software supply chain and throughout the lifecycle management processes of developing, implementing and updating software-enabled systems."[12]

AWS agrees. Cybersecurity in the automotive context is an ongoing effort beginning with component manufacturers and extending throughout the service life of the vehicle. Thus, the Proposed Cybersecurity Best Practices should provide sufficient flexibility in design requirements to enable the Agency's cybersecurity best practices to evolve over time to include new technologies and address evolving security threats.

To address this issue and provide appropriate additional flexibilities, the Agency should develop secure design principles that are open and accessible to any automotive industry participant. The Auto-ISAC, which is intended to "facilitate industry's cybersecurity-related information sharing among its members,"[13] can play a key role in achieving a mechanism to engage the industry and allow for such promotion of innovation.

Additionally, as the Agency well-knows, the Auto-ISAC provides a venue to exchange threat information, but does not currently facilitate safety-related security vulnerability disclosure. Accordingly, NHTSA should also consider a program such as the Aviation Safety

[9] 2016 Best Practices at 5.

[10] *See e.g.*, Ensuring American Leadership in Automated Vehicle Technologies, Automated Vehicles 4.0 (January 2020) ("AV 4.0") ("The USDOT is actively preparing for emerging technologies by engaging with new technologies to address legitimate public concerns about safety, security, and privacy without hampering innovation."); Preparing for the Future of Transportation, Automated Vehicles 3.0 (October 2018) ("AV 3.0") at 5 ("Governments at all levels should not unnecessarily impede … innovation.").

[11] Request for Comments at 2482. *See also Id.* "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."

[12] *Id.*

[13] Proposed Cybersecurity Best Practices at 8.

Reporting System facilitated by NASA on behalf of the FAA. Vulnerability disclosure is a key element of security, but confidentiality is critical to incentivizing disclosures.

III. NHTSA Should Consider the Vehicle Owners and Consumers as Beneficiaries of the Cybersecurity Best Practices and Engage in Additional Consumer-Oriented Activities.

Ensuring that motor vehicles and equipment are manufactured free of potential cybersecurity vulnerabilities is critical for the Agency and all industry stakeholders. In order to address this critical issue, the Agency released the Proposed Cybersecurity Best Practices as a "resource for the industry as a whole and covers safety-related cybersecurity issues for all motor vehicles and motor vehicle equipment."[14]

The scope of Proposed Cybersecurity Best Practices should reflect the general understanding that consumers are also an important part of the applicable regulatory landscape. While the application of the Agency's best practices will clearly benefit the whole industry, including the vehicle owners and consumers, the scope of Proposed Cybersecurity Best Practices is limited to "individuals and organizations designing and manufacturing vehicle electronic systems and software."[15] With this context, the Agency should expand this scope to recognize vehicle owners and consumers as beneficiaries of these best practices, especially in the context of information sharing related to sensor data and personal data collected, balancing consumers' potential exposure to cybersecurity risks with the rewards flowing from robust information collection and sharing.

The Agency should also consider creating consumer-facing education and awareness on vehicle cybersecurity risks, Agency best practices and integration into other personal digital technologies. As the Agency recognized, there are various scenarios where the vehicle owners can create cybersecurity vulnerabilities.[16] Similarly, the Proposed Cybersecurity Best Practices reflect these concerns regarding vehicle owners.[17] The Agency should play a key role in educating consumers and creating awareness on cybersecurity related threats.

IV. NHTSA Should Update Off-Vehicle Data Processing and Security to Recognize Cloud Technologies.

In the Proposed Cybersecurity Best Practices, at Section 8.7.4 in connection with communication to back-end servers, the Agency states:

[14] Request for Comments at 2483.

[15] Proposed Cybersecurity Best Practices at 1-2.

[16] *Characterization of Potential Security Threats in Modern Automobiles – A Composite Modeling Approach* in Docket No. NHTSA-2014-0071 (Sept. 2014) at Appendix A (identifying various scenarios which can create potential cybersecurity vulnerabilities, including the owner installing "an after-market radio purchased from a third party, which may come with an on-board malware that can access a vehicle data bus.")

[17] Proposed Cybersecurity Best Practices at 12, G. 39 ("The automotive industry should consider the incremental risk that could be presented by [aftermarket devices] when connected with vehicle systems [by consumers] and provide reasonable protections.")

[T.19]: Manufacturers should use appropriate encryption and authentication methods in any operational communication between external servers and the vehicle.[18]

This best practice should be reframed to recognize cloud computing, including communications, data integrity and data processing servers, which are crucial for modern vehicles. The Agency itself recognized the importance of cloud technologies in the development autonomous vehicles.

For example, in AV 4.0, the Agency advised manufacturers of autonomous vehicles to take a NIST publication for manufacturers of IoT devices, which necessarily require utilization of cloud technologies, as a basis that can be used to understand cybersecurity risks and to develop cybersecurity measures "for potential IoT devices embedded in AVs."[19]

In other words, the Agency recognizes and foresees that IoT devices will be part of modern vehicles and naturally these devices will require cloud computing as part of their functionality. The Agency should therefore reframe T.19 of Proposed Cybersecurity Best Practices to address sharing of information and communication between cloud servers and the vehicle.

AWS also believes that the Agency should develop a shared responsibility model among component manufacturers, OEMs, and service providers that recognizes vehicle ownership and supply chain responsibilities. Further, the Agency should consider a risk-based model to facilitate the transfer of ownership along the supply chain and in the context aftermarket vehicle sales.

V. AWS's Additional Comments on Proposed Cybersecurity Best Practices.

In addition to general considerations set forth above, AWS also believes the Proposed Cybersecurity Best Practices would benefit from inclusion of several additional considerations.

Outcomes-Based Framework: NHTSA should apply a framework of outcomes, control objectives and security requirements in its Proposed Cybersecurity Best Practices. The Proposed Cybersecurity Best Practices in its current form are focused on a "best effort" for each subject area, which could potentially lead to over-prescriptive outcomes. By using an outcomes-based framework, NHTSA can effectively set the bar for performance, while leaving open design and innovation to meet the requirement.

Governance of Suppliers and Component Manufacturers: Section 4.1 in Proposed Cybersecurity Best Practices provides over-prescriptive measures for the governance of suppliers and component manufacturers. Product security should be addressed with standards focused

[18] Proposed Cybersecurity Best Practices at 16, T.19.

[19] AV 4.0 at 23. *See also* NISTIR 8259 Foundational Cybersecurity Activities for IoT Device Manufacturers, (May 2020) at 12 ("Other systems and services that may or may not be acting on behalf of the manufacturer can provide the technical means (e.g., a cloud-based service that securely stores data for each IoT device, internet service providers and other infrastructure providers).") available at https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259.pdf (Last accessed March 8, 2021).

around secure product development, including supply chain integrity, pen testing and failover, among others.

While the Proposed Cybersecurity Best Practices address various issues concerning supply chain, such as communication of "clear cybersecurity standards … to the suppliers that support the intended protections,"[20] NHTSA should incorporate additional principles of secure product development and supply chain integrity. For example, recognizing that the scope of the standard is applicable to physical supply chain integrity of goods, AWS believes that the standards set forth in ISO 28000:2007, *Specification for security management systems for the supply chain*, can serve as a guide, as appropriate, for supply chain aspects of the Proposed Cybersecurity Best Practices.[21]

Zero Trust Architecture: While the current best practices in Proposed Cybersecurity Best Practices, such as T.14 set forth in Section 8.7.2, are focused on perimeter security and network segmentation, the best practices should be built around zero trust architecture for component interconnectivity. This will help ensure that the cybersecurity vulnerabilities are minimized.

Data Access Advisory Committee: The Agency should establish an industry/government data access advisory committee to provide a forum to discuss the information or data that vehicles collect, generate, record, or store in an electronic form that is retrieved from an highly automated vehicle or automated driving systems.

Risk Reduction and Data Asset Management: The Agency should also encourage emphasis on data asset management and risk reduction before acquisition of information and security technologies. The Agency should also encourage selection of appropriate countermeasures and investments in security, compliance and risk management.

Cybersecurity Simulator: The Agency could also benefit from developing a cybersecurity simulator that can facilitate identification of vulnerabilities and risk mitigation strategies. An example of a cybersecurity simulator was employed by the Federal Aviation Administration.[22] The simulator would serve as a complimentary source to supplement industry-developed and self-exercised cybersecurity standards.

On-Board Diagnostics Protocol: The Agency should also ensure the development of cybersecurity countermeasures within the on-board diagnostics protocol with sufficient flexibility as not to interfere with repair and maintenance procedures and serviceability of motor vehicles and equipment.

Intrusion Detection and Incident Response: The Agency should encourage industry collaboration to identify attempted and successful exploitations and attacks not previously considered in the design and assessment phases. To that end, AWS supports proposed best

[20] Proposed Best Practices at 6, G.9.

[21] ISO 28000:2007, Specification for security management systems for the supply chain available at https://www.iso.org/standard/44641.html (Last accessed March 11, 2021).

[22] NHTSA, A Summary of Cybersecurity Best Practices (Oct. 2014) at 10, available at https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/812075_cybersecuritybestpractices.pdf (Last accessed March 8, 2021).

practices G.18 and G.26, which provides that manufacturers should collect information on potential attacks, that this information should be analyzed and shared with industry through the Auto-ISAC, and that automotive industry members should create their own vulnerability reporting policies and mechanisms.

Again, AWS appreciates the opportunity to comment on this matter.

Blair Anderson
Director, Public Policy