March 15, 2021

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

National Highway Traffic Safety Administration
US Department of Transportation
1200 New Jersey Avenue, SE
Washington, DC 20590

Dear Mr. Kreeb:

SAE International, a global voluntary consensus mobility standards development organization, appreciates this opportunity to respond to the request for comments. Advancing the safety and security of mobility is a priority of SAE members. On behalf of the subject matter experts of SAE International's Vehicle Cybersecurity Systems Engineering Committee, the following comments are in response to the NHTSA request.
.
The National Technology Transfer and Advancement Act (NTTAA) directs Federal agencies to adopt voluntary consensus standards wherever possible, thus avoiding development of unique government standards. OMB Circular A-119, revised by the Office of Management and Budget (OMB) in January 2016, spells out the government strategy for standards development promoting agency participation with standards bodies. SAE standards committee members have a long history of developing voluntary consensus standards that have been incorporated by reference into legislation, rulemaking documents, and regulations. SAE ground vehicle standards are cited in the US DOT's National Highway Traffic Safety Administration's and Federal Motor Carrier Safety Administration's regulations.

SAE committees include experts from industry, academia, research organizations, and government. The resources and input each sector provide are beneficial to both the process and the products. Having NHTSA and other government participation in the subject area of cybersecurity, in the standards committees, is encouraged by the SAE membership.

Overall, the committee preference is for this NHTSA document to be more prescriptive. For example, the Original Equipment Manufacturer (OEM) / Aftermarket, Serviceability and Diagnostic Tool sections are very significant. We welcome additional concrete recommendations on how to provide stronger cybersecurity protections. The best practices are fundamentally focused on cybersecurity as it relates to safety. Cybersecurity influences not just the safety of a vehicle, but overall security including property, financial, and privacy. The NHTSA should consider this where applicable throughout the document (e.g., proposed changes in rows 3,7, & 39 in table below).

The document indicates the automotive industry should follow the five principal functions “Identify, Protect, Detect, Respond and Recover”. We were unable to locate content of the “recover” guidance. Additional material, such as the following could be provided:

- Examples of recovery solutions (update lessons learned, training and awareness)
- Requirements for recovery (guidance on duration and thresholds)

There are multiple references to ISO/SAE 21434 which is outstanding; however, NHTSA supplied a hyperlink to access the document only via the ISO webpage. We request that NHTSA add www.saemobilius.sae.org for stakeholders to obtain the document through an alternative source. In addition, specific requirements and clauses are referenced that have changed in the final release of the ISO/SAE 21434 Final Draft International Standard (FDIS). Either it must be clear that those references are for the 21434 Draft International Standard (DIS) release or more generic references to Clause Titles and/or the 21434 standard are used. Otherwise, the NHTSA best practice document, if not edited, will become outdated.

SAE followed NHTSA’s identification structure to identify where proposed changes are suggested. “General best practices” are enumerated using the convention [G.n] and [T.n] for “Technical best practice” elements.

In the interest of brevity, bold text within the “Comment” column of the following table recommends adding this new text to the specified best practice. Entries leading with “Revise”, “Replace”, “Remove” are suggestions for NHTSA from the subject matter experts. Following the table are details of SAE’s current and planned professional development offerings regarding Cybersecurity and Certificate Programs (reference G.38).

Thank you for your consideration of SAE International’s Vehicle Cybersecurity Systems Engineering Committee committee’s comments.

Sincerely,

S. William Gouse

S. William Gouse
Director, Federal Program Development
SAE INTERNATIONAL
901 15th Street, NW, Suite 520
Washington, DC 20005
M: +1.202.281.5844
E: S.William.Gouse@sae.org
www.sae.org

Table of SAE Committee Comments

Identification Number	Reference	Comment
1	Scope (Footnote 4)	SAE believes the scope does not include mobile apps, APIs, backend infrastructure, Remote Vehicle Operation, and Service Tools. May want to add a footnote to contrast ISO/SAE 21434 and ISO 24089 scopes.
2	G.1	See General section above
3	G.2 part [c]	Remove the end of the sentence "within the vehicle safety design process".
4	G.2 Footnote 10	Call out Organizational Cybersecurity Management of ISO/SAE 21434 as reference. The RQ numbers are different between DIS and FDIS, so specific requirement numbers should be refrained and just the section titles mentioned instead.
5	G.4 (4.2.2)	Reword: This process should include **continual** cybersecurity risk **assessments** that **are** appropriate and reflects mitigation of risk for the full **lifecycle** of the vehicle11. **(see Continual cybersecurity activities in ISO/SAE 21434)**
6	G.6	This seems to put an artificial emphasis on sensor manipulation. The task is larger and following the NIST Cyber risk management process should prioritize the assets of a system and determine attack feasibility of those assets by any means. The specific attack outlined in DefCon 23 or the other research cited should not be used to illustrate an implied prioritization. Instead principles of least privilege, defense in depth, end to end security and zero trust should be recommended. Recommendation is to move this item as a further example within Section 8.
7	4.2.4	Reword: **Risk Treatment**
8	G.7	Reword: Any **uncontrolled** risk to vehicle systems should be removed or mitigated.
9	G.8 (footnote 17)	Remove Footnote 17 or provide a more correct reference to Defense In Depth principles.
10	G.9 (footnote 18)	Industry needs more guidance on what is meant by G.9 (Standards, requirements, expectations, processes…)? Possibly change "standards" to "processes" and it will read better and be less ambiguous. It would also be more encompassing.

11	4.2.6	Retitle: **Inventory and Management of Assets on Vehicles**
12	4.2.6	Add a reference to NTIA.
13	G10 and G11	Include inventory management of hardware, software, firmware, etc., with appropriate data relationships established. Software inventory management alone is not sufficient.
14	4.2.7	Retitle: **Cybersecurity Testing and Vulnerability Identification**
15	G.13	Reword: Manufacturers should also pursue product cybersecurity testing **(**including, penetration tests, **API vulnerability checks …)** as part of the development process.
16	4.2.8	Retitle: **Monitoring and Containment**
17	G.17	Reword: **When a cyber-attack is detected it shall be entered into the security log and used to establish future mitigations.**
18	G.18	There are various forms of sharing information. Remove the words, "through the Auto ISAC". That is just one example.
19	G.19	Reference should be made to ISO/SAE 21434, specifically the cybersecurity plan, cybersecurity case and cybersecurity assessments.
20	4.2.11	Remove reference to **NIST 8151** and instead reference **NIST White Paper: Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF)** **https://csrc.nist.gov/publications/detail/white-paper/2020/04/23/mitigating-risk-of-software-vulnerabilities-with-ssdf/final**
21	4.2.11	Auto ISAC is not a standards development organization. Could add as example along with SAE and ISO.
22	G.23	Reword: Manufacturers should actively **apply** automotive industry-specific best practices and **participate in** standard development activities.

23	4.3	Reword sentence before G.24 **NHTSA recommends:**
24	4.5	Reword paragraph before G.31: Additionally, the response process should include reporting **relevant** incidents, exploits, and vulnerabilities **identified during post-production to the Auto ISAC in a timely manner…**
25	4.6	Reword: **Automotive industry** should be changed to **Automotive Manufacturer** throughout section.
26	G.34	Reword: Further, such documents should be retained through **the end of cybersecurity support. See ISO/SAE 21434 clause End of Cybersecurity Support and Decommissioning.**
27	G.37	Reword: The automotive industry should consider carrying out **periodic** organizational and product cybersecurity audits. **See ISO/SAE 21434 clause Organizational and Project Cybersecurity Management**
28	G.38	Add the following link for guidance as to areas of training development needed to ensure workforce is prepared for their roles. Also, see section following this table. **https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf**
29	G.39	Reword: Change **automotive industry** to **automotive manufacturers**. Change **these devices** to **user owned or aftermarket devices**. Delete the word "incremental". **Apply defense in depth protections.**
30	G.40	Reword: Any connection to a third-party device should be **authorized** and provided with appropriate limited access. **See SAE 3138 Data Link Security.**
31	G.40	Add an additional best practice after G.40: **G.4x Any external device allowed access should be firewalled from safety-critical systems.**

32	G.41	Add an additional best practice after G.41: **G.4x OEMs should implement defense-in-depth protections against potential vehicle cybersecurity compromises from aftermarket devices.**
33	G.42	The following is an example where this might not happen: Given the highly proprietary nature of AV systems, it is unlikely that those elements will be serviceable by outside parties. Reword: The automotive **manufacturer** should **design to allow the** serviceability of vehicle components and systems by individuals and third parties where such activities do not violate existing laws.
34	G.43	Reword: The automotive **manufacturer** should provide strong vehicle cybersecurity protections that do not **unreasonably** restrict access by **qualified** third-party services authorized by the vehicle owner.
35	T.2	Reword: **If developer access is necessary to perform forensics, then any action taken shall render the device ineligible for continued operational use.**
36	T.3	Reword: Cryptographic credentials that provide an authorized, elevated level of access to vehicle computing platforms should be protected from **unauthorized** disclosure or modification.
37	T.7	Reword: The use of global symmetric keys and *ad hoc* **cryptography** should be **prohibited**.
38	T.7	Add best practice after T.7: **T.x Only cryptographic techniques providing sufficient strength for diagnostic access and international standard cryptographic techniques should be utilized.** Add reference to NIST SP 800-131a **https://csrc.nist.gov/publications/detail/sp/800-131a/rev-2/final**
39	T.10	More criteria needed. Reword: **Employ best practices for communication of critical information over shared and possibly insecure channels. Limit the possibility of replay, integrity compromise, and spoofing. Physical and logical access should also be highly restricted.**

40	T.21	Add best practice after T.21: **T.x Controls should be implemented to prevent rollback attacks.**
41	T.21, T.22, T.23	Add additional references such as UPTANE and ISO 24089. **https://uptane.github.io/** **https://www.iso.org/standard/77796.html**
42	Appendix-Terms and Descriptions	The following terms need to be defined: **Automotive Industry** **Automotive Manufacturer**

Additional Reference Material for Item 28 / G.38:

Please see the links below to access the current list of SAE's cybersecurity offerings.

Managing Cybersecurity Risks Using ISO/SAE DIS 21434 PD532013

Introduction to Car Hacking with CANbus C1857

Introduction to Automated Vehicle Safety: Multi-Agent, Functional, SOTIF, and Cybersecurity C1950

Formal Methods for Functional Safety and Security in Cyber-Physical Systems C1876

Introduction to the Secure Microkernel, seL4 C1874

Introduction to Cyber Security for Commercial Aviation C1881

SAE Three-Level Certification Program:

SAE is in the process of developing a training and certification program that enables organizations to gain competency in key automotive cybersecurity skills, processes, and tools. These include mastery of the ISO/SAE 21434 standard and the UN ECE vehicle regulations for Cybersecurity Management Systems and Software. It awards a certification upon successful completion and mastery on an assessment. The program will enable customers to define cybersecurity policies and processes, manage cybersecurity risk, implement a cybersecurity management system, and foster a cybersecurity culture. The product is a three-level certification program, please see specific breakdown below.

- Level One – Basic Module -- 1-Day covering the basics of cybersecurity in automotive.
- Level Two – Advance Modules – 3-Day course covering the basics (Level One) plus threat and risk analysis and protection concepts and implementation, verification, and validation in the development phase.
- Level Three-Expert – 4-Day course covering the basics (Level One), advanced topics (Level Two) and automotive cybersecurity engineering over the lifecycle.

End of SAE International's Comments:Docket No. NHTSA-2020-0087