TOYOTA

TOYOTA MOTOR NORTH AMERICA, INC.
Sustainability & Regulatory Affairs
325 Seventh Street, NW #1000 Washington, DC 20004

March 15, 2021

Dr. Cem Hatipoglu
Associate Administrator for Vehicle Safety Research
National Highway Traffic Safety Administration
1200 New Jersey Avenue, SE
Washington, DC 20590

RE: Cybersecurity Best Practices for the Safety of Modern Vehicles – Request for Comments [Docket No. NHTSA-2020-0087]

Dear Dr. Hatipoglu:

Toyota Motor North America, Inc., on behalf of Toyota Motor Corporation (collectively, "Toyota"), is pleased to provide these comments to the January 12, 2021 *Federal Register* notice on the Cybersecurity Best Practices for the Safety of Modern Vehicles ("Best Practices") Request for Comments. These comments supplement the comments submitted by the Alliance for Automotive Innovation.

General Comments

While NHTSA includes modifiers and alterers in the Scope of this Best Practice, NHTSA does not offer best practices directed at third-party modifiers and alterers that would address issues unique to this stakeholder group. To align with ISO 21434, NHTSA should provide guidance to repair shops to ensure cybersecurity is maintained through repairs. This should include items such as ensuring use of replacement parts and service tools that conform to ISO 21434.

NHTSA should also clarify that the use of the term "Manufacturers" in the best practices themselves refers to the broad group of stakeholders identified in the Scope of the document.

Line Edit Suggestions

Toyota provides the following line edit suggestions for the Best Practices document. Please note the edits in red font.

[G.2][a] *Allocating dedicated resources within the organization focused on researching, investigating, implementing, testing, and validating product cybersecurity measures and ~~vulnerabilities~~ threats;*
Reason: It would be more comprehensive to say threats, rather than vulnerabilities.

[G.6] We recommend striking this best practice and include this topic as part of the "emerging risks" section proposed in the comments submitted by Auto Innovators.
Reason: Sensor spoofing and manipulation is an area that needs further research to further understand the vulnerabilities and identify mechanisms to address those risks.

[G.12] *Manufacturers should evaluate ~~all~~ critical commercial off-the-shelf and open-source software components used in vehicle ECUs against known vulnerabilities.*
Reason: It is impracticable to evaluate all commercial off-the-shelf and open source software components due to the large number and dynamic nature of these components. The necessity to evaluate each component would also vary depending on system design. This language also provides consistency with UN-R 155.

[G.13] *Manufacturers should ~~also pursue~~ consider utilizing product cybersecurity testing, including using penetration tests, as part of the development process.*
Reason: The use of the term "pursue" is very broad and unclear. The revision makes it clear that manufacturers should consider product cybersecurity testing as a part of the development process, as appropriate.

[G.16] (footnote 27) *Described in clause ~~7~~ 13 of ISO/SAE DIS 21434, "~~Continuous Cybersecurity Activities~~ Operations and Maintenance."*
Reason: [G.16] is discussing incident detection and remediation, which is specifically addressed in sub-clause 13.3, Cybersecurity Incident Response.

[G.17] We recommend striking this best practice and include this topic as part of the "emerging risks" section proposed in the comments submitted by Auto Innovators.
Reason: This area is not yet mature as there are no related standards for near-real-time remediation.

[G.20] *All related work products should be traceable ~~within~~ using a robust ~~document version control system~~ mechanism that is appropriate for the manufacturer.*
Reason: This edit makes it clear that the intent of this recommendation is not to require a specific method or type of system (e.g. electronic system) for tracing documents but that a company can decide on the appropriate method for traceability of the related work products.

[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.*
Reason: Auto-ISAC has developed best practices in the past when standards and best practices were not yet developed or mature yet. Industry should focus on collaborative developments through standards organizations.

[G.37] *The automotive industry should consider carrying out organizational and product cybersecurity audits ~~annually~~ periodically.*
Reason: This would help align these best practices with ISO 21434 RQ-05-17 Note 4.

6.1 Vehicle manufacturers

We recommend combining [G.39] and [G.40] to read as follows:
The automotive industry should consider the incremental risks that could be presented by these devices when connected with vehicle systems and provide reasonable protections~~.~~, which may include authentication, as appropriate.

Reason: [G.40] as written creates conflict with cybersecurity countermeasures. We feel this alternative provides a clearer recommendation.

[G.43] *The automotive industry should provide strong vehicle cybersecurity protections that do not unduly restrict access by approved alternative third-party repair services authorized by the vehicle owner.*
Reason: It is reasonable to provide strong protection and provide access to approved third-party repair services; however, providing strong protection and anticipating any possible third-party repair service creates a conflict with the cybersecurity goal.

8.1 Developer/Debugging Access in Production Devices
Recommend the proposed edit to the last sentence in this section:
Merely physically hiding connectors, traces, or pins intended for developer debugging access ~~should~~ would not be considered a sufficient form of protection.
Reason: We suggest this word change to make clear that this is providing additional context for the related best practices.

[T.7] Provide clarification by defining “global symmetric keys”.

[T.9] *When possible, critical safety signals should be securely transmitted. ~~transported in a manner inaccessible through external vehicle interfaces.~~*
Reason: There are safe and secure methods for protecting safety-critical messages.

[T.20] *Manufacturers should consider planning for and creating~~e~~ processes that could allow for quickly propagating and applying changes in network routing rules to a single vehicle, subsets of vehicles, or all vehicles connected to the network.*
Reason: This edit provides more flexibility for each stakeholder to apply the appropriate mechanism to address threats.
Also, please provide clarification as to what exactly “changes in network routing rules” refers to.

8.9 Over-the-Air Software Updates
We recommend that this section reference ISO 24089 – Software Updates for Road Vehicles.

Throughout the document, NHTSA should consistently include “DIS” in the references to ISO standards.

Should you and/or your staff have any questions, please contact me or Jade Hill, Toyota’s Program Manager for active safety regulations, at jade.s.hill@toyota.com or (202) 463-6836.

Sincerely,

Tom Stricker
Group Vice President
Sustainability & Regulatory Affairs