BOSCH

Robert Bosch LLC
38000 Hills Tech Dr.
Farmington Hills, MI 48331
Tel 1 (248)876-2627
Fax 1 (248)719-2092
www.bosch.us

March 15, 2021

Mr. Cem Hatipoglu
Associate Administrator for Vehicle Safety Research
National Highway Traffic Safety Administration
Department of Transportation
1200 New Jersey Avenue S.E.,
West Building Washington D.C. 20590-0001

Re: Request for Comments on Cybersecurity Best Practices for the Safety of Modern Vehicles, Docket No. NHTSA-2020-0087, 86 Fed. Reg. 2481

Dear Associate Administrator Hatipoglu,

Robert Bosch LLC ("Bosch") appreciates the opportunity to provide its perspective concerning the proposed update to NHTSA's Cybersecurity Best Practices for the Safety of Modern Vehicles ("Best Practices"). Bosch welcomes NHTSA's efforts to revise the Best Practices document and to ensure that its contents and recommendations are concurrent with the evolution of cybersecurity technology. As Bosch stated in its 2017 response to the original Best Practices document, it is essential that this be maintained as a living document which will be regularly amended to represent the industry's feedback as well as ongoing threats and developments within the U.S. market.

Bosch believes that cybersecurity is a priority issue for the automotive and commercial vehicle industries and strongly supports a layered approach to vehicle cybersecurity. We have espoused this principle in the development of our own products and in our engagement with customers.

<u>General Best Practices:</u>

Concerning best practice [G.1], Bosch notes that one of the recommendations is phrased as follows "Design-in methods and processes to facilitate rapid recovery from incidents when they occur." Bosch supports this overall recommendation but wishes to note that the appropriate means for "recovery" are dependent on each situation. Therefore, Bosch would urge the addition of this bullet point under [G.1].

"Consider a sophisticated, holistic, balanced, and sustainable approach to recovery taking into account the risks of making changes to complicated vehicle systems. The best possible solution may include disabling features, blocking traffic in gateways, or even not taking any action at all."

Leadership Priority on Product Cybersecurity:

Bosch supports the points raised in this section. NHTSA may also want to consider requesting an annual confidential consultation with the vehicle manufacturers concerning their company security roadmap.

Vehicle Development Process with Explicit Cybersecurity Considerations:

Concerning best practice 4.2.6 "Inventory and Management of Software Assets on Vehicles," Bosch views this critical activity as being an area of shared and joint responsibility between the supplier and the vehicle manufacturer. Suppliers must maintain appropriate control and management of their catalogue of proprietary software. It is not advisable or preferred for suppliers to disclose their catalogue of software to other entities. This trend would increase the potential disclosure of sensitive and safety-critical information through an attack or unauthorized breach. It would also raise concerns over the protection of valuable commercial assets and intellectual property.

Consequently, Bosch requests that the language be amended to read as follows:

- *[G.10] Suppliers and vehicle manufacturers should work collaboratively to maintain a database of operational software components used in each automotive ECU, each assembled vehicle, and a history log of version updates applied over the vehicle's lifetime.*

Concerning best practice 4.2.7 "Penetration Testing and Documentation," Bosch requests additional clarification from NHTSA. Bosch supports the overall intent of this section of the document but it should be made clear that these expectations do not apply to proprietary software. NHTSA could also encourage the use of software composition and analysis tools which enable the analysis of open-source and off the shelf software components. Such mechanisms provides lists of common vulnerabilities. Proprietary software is different and distinct and will require specialized tools.

Concerning [G14], Bosch respectfully requests that NHTSA clarify the use of the term "test stages". This is not in alignment with the common nomenclature used by the industry. Bosch recommends that NHTSA consider utilizing the term "penetration testing." In addition, we propose that NHTSA clarify that penetration testers should be dedicated security testers, not the same staff members or associates who designed the product or conducted the validation engineering. Bosch notes that there may be penetration experts embedded within the development team, but that these individuals should not also be in the position of conducting the actual penetration test.

Concerning [G.15], Bosch welcomes this text as a good recommendation. However, in some cases, "each known vulnerability" may prove to be too much to consider. For example, some of the common tools that would be used to fulfil [G.12] may yield a list of known vulnerabilities in excess of 5,000 for a single ECU because it is prone to many false positives. Analysis of each case is not appropriate, however it is appropriate to analyze groups or subsets of known vulnerabilities.

Bosch recommends that [G.15] be amended to read as follows:

- *[G.15] "A vulnerability analysis should be generated for relevant known vulnerabilities assessed or newly identified relevant vulnerabilities with significant impact to cybersecurity which have been identified during security testing. The disposition of the vulnerability or group of vulnerabilities and rationale for how to manage risk related to the vulnerabilities should be documented."*

Turning to 4.2.9 "Data, Documentation, Information Sharing" and specifically best practice [G.18], Bosch notes that NHTSA should also acknowledge the modified MITRE ATT&CK Framework proposed by the Auto-ISAC and encourage its use. This framework would enable the sharing of cyber incidents to generate a heat map of the most common automotive cybersecurity attacks. This mechanism could assist the industry in sharing information and identifying the top ten cyberattacks from the wild.

Bosch requests that NHTSA expand the references included in 4.2.11 "Industry Best Practices." Specifically, Bosch supports the language in [G.22] relative to industry standards and best practices (e.g. ISO/SAE 21434); however, NHTSA should also consider the J1939 task force activities related to cybersecurity for commercial vehicles and the Cybersecurity Requirements for Telematics Systems developed by the National Motor Freight Traffic Association (NMFTA).

Although the overall document is intended to encompass all vehicles, Bosch believes that NHTSA should specifically highlight best practices and recommendations for commercial vehicles. Commercial vehicles have unique facets that should be addressed and considered relative to cyber protection.

Information Sharing:

Bosch respectfully requests that NHTSA amend the language in [G.25] to clarify that the Auto-ISAC is not a standards-setting organization.

Bosch concurs with NHTSA that vehicle manufacturers and suppliers should be encouraged to join the Auto-ISAC, share timely information and collaborate. This recommendation should be extended to all industry members. Bosch understands the value of the Auto-ISAC and has been an active member since December 2016.

Security Vulnerability Reporting Program:

Bosch supports best practice [G.26]. Bosch continues to enable effective communication with other Bosch entities, external parties, including researchers. In 2016, a Product Security Incident Response Team (Bosch

PSIRT) was established to serve as the central point of contact for external security researchers, partners or customers to report security information related to Bosch products. The PSIRT interface provides a clear and accessible means for external parties to communicate and ensures that all submissions will be reviewed and considered. This mechanism enables an assessment of the validity of vulnerability notifications and allows for a quick and appropriate action. The Bosch PSIRT webpage (psirt.bosch.com) includes a list of existing Security Advisories.

Bosch wishes to re-iterate its prior position that, to the extent possible, NHTSA should ensure that the Best Practices document and all future communications from the Agency encourage and support the use of a coordinated disclosure process so as to minimize potential risks to public safety. In the case of a coordinated disclosure, the external party notifies us in advance of a vulnerability. We collaborate with the relevant party and address the concern. The vulnerability then remains confidential to those parties required to address the vulnerability ("need-to-know principle") until the appropriate time.

Education:

Concerning best practice [G.38], Bosch applauds NHTSA for encouraging collaboration amongst the industry, universities and other stakeholders. Bosch is currently supporting workforce development in automotive cybersecurity, offering several internship, thesis and PhD positions. In addition, Bosch has a number of associates that teach at universities which offer related cybersecurity programs.

Aftermarket / User Owned Devices:

Bosch supports best practice [G.41] concerning the need for aftermarket device manufacturers to employ strong cybersecurity protections on their products. Bosch maintains this as a core principle, but is aware that this is not the situation across the aftermarket sector. The current situation is such that third-party devices should be considered possible vulnerabilities when they are connected to the vehicle.

Serviceability:

Bosch strongly concurs with best practices [G.42] and [G.43] and appreciates NHTSA's clear affirmation that the industry should not only provide strong vehicle cybersecurity protections, but also enable access by alternative third-party repair services as authorized by the vehicle owner.

However, the Best Practices document does not provide further guidance on how the vehicle should be secured as it relates to third party connected devices. Bosch is in agreement with NHTSA that the SAE and ISO guidelines are relevant but urges NHTSA to meet with all relevant stakeholders and work towards a uniform standard and clear definition on what constitutes secure access.

8.3 Cryptographic Credentials:

Concerning technical best practices [T.3] and [T.4], Bosch concurs that any credential obtained from a single vehicle's computing platform should not provide access to multiple vehicles. Promoting the use of unique credentials reduces the risk of fleet-wide attacks.

8.6 Event Logs:

In its 2017 response to NHTSA during the formulation of the initial Best Practices document, Bosch described the future of automotive cybersecurity as encompassing intrusion prevention and detection. Bosch is actively developing components and systems to support vehicle manufacturers in developing vehicles that are safe and secure. Intrusion detection systems and real-time response and recovery are an option for core automotive modules. In-vehicle networks and connected services produce data that can support detection of unauthorized attempts to access vehicle computing resources.

Concerning [T.11] and [T.12], Bosch agrees that these statements are directionally correct but would appreciate clarification relative to a few central points. Bosch is concerned that an event log may be of limited use if it is not coupled with an Intrusion Detection System (IDS).

An IDS may detect anomalous behavior but not have sufficient information to reveal the nature of a cybersecurity attack.

- Is it intended that these logs be generated by an IDS or a complete log of all network traffic?
- Is this intended to steer the industry towards host-based vs. network-based IDS strategies?
- Are these logs related to or generated by an IDS?
- Does NHTSA intend to have OEMs collect real-time data and transmit it to a back end for analysis or just store the data for the next time the vehicle goes in for service?
- Is the intent to transmit meta-data surrounding anomalous behavior to a remote location for analysis?

Further, Bosch requests that NHTSA provide more definition around the types of events that should be logged (i.e. reprogramming, diagnostic access requests, anomalous behavior detection).

Terms and Descriptions:

Bosch applauds NHTSA for considering ISO/SAE 21434 for the development of the overall document and would recommend that the Agency consider harmonizing related definitions to ensure consistency within the industry.

Commercial Vehicles:

[redacted]

[redacted]

[redacted]

[redacted]

Conclusion:

Bosch appreciates this opportunity to help advance vehicle safety and we welcome NHTSA's review and consideration of our feedback. We would be pleased to answer any questions or provide additional information.

Please do not hesitate to contact Ana Meuwissen at 202/815-7645 or Ana.Meuwissen@us.bosch.com if we can be of further assistance.

Yours sincerely,

Digitally signed by pki, BOSCH, US, T, I, Tim.Frasier
Date: 2021.03.12 12:12:05 -05'00'

Tim Frasier
Regional President
Cross Domain Computing Solutions
Robert Bosch LLC

pki, BOSCH, US, A, N, Ana.Meuwissen

Digitally signed by pki, BOSCH, US, A, N, Ana.Meuwissen
Date: 2021.03.12 17:08:53 -05'00'

Ana M. Meuwissen
Director, Federal Government Affairs
Robert Bosch LLC

pki, BOSCH, US, R, O, Robert.Kaster

Digitally signed by pki, BOSCH, US, R, O, Robert.Kaster
Date: 2021.03.12 17:17:21 -05'00'

Robert Kaster
Chief Technical Expert
Robert Bosch LLC