Before the
DEPARTMENT OF TRANSPORTATION
Washington, DC 20230

In the Matter of	)	
	)	
Document Number 2020-25930: National Highway Transportation Safety Administration's Cybersecurity Best Practices for the Safety of Modern Vehicles Voluntary Guidance.	)	Docket No. NHTSA-2020-0087

COMMENTS OF
BLACKBERRY CORPORATION

BlackBerry Corporation[1] respectfully submits these comments in response to the National Highway Transportation Safety Administration (NHTSA) request for comments on the Cybersecurity Best Practices for the Safety of Modern Vehicles. The rapid innovation within modern consumer, commercial, and military automobiles is unique in the history of technology and motor vehicles alike. Advanced software, machine learning, advanced sensors, machine-to-machine interface, and multiple means of communication are becoming standard in most vehicles, making them processing nodes in a wider network. A focus on cybersecurity is vital as vehicles become connected with critical infrastructure and a compromised vehicle could pose a threat to life, property, capital, and even national security. **BlackBerry applauds the efforts, diligence, and foresight of NHTSA for taking a position of cybersecurity leadership**. Our

[1] BlackBerry Corporation has provided secure communications to the world governments and the largest businesses for over 35 years. From secure devices, we have shifted that technology to build some of the worlds most advanced cybersecurity technologies, utilizing Artificial Intelligence (AI) and Machine Learning (ML) to ensure zero-trust environments for some of the most critical operations. This combined with BlackBerry's work on secure real-time operating systems that power everything from 175 million vehicles worldwide, to vital observation equipment on the international space station, places our company in a unique position as a software provider that offers operational effectiveness with security into the very design of our products and services.

company agrees with the new and existing best practices, as well as the choice of ISO/SAE 21434 as the primary industry standard as the foundation for the best practices.

In general, BlackBerry agrees with the standards and best practices presented within Document Number 2020-25930: *Cybersecurity Best Practices for the Safety of Modern Vehicles*[2]: hereafter referred to as *the document*; and BlackBerry appreciates the relative exploratory challenge cybersecurity presents to the automotive industry, in contrast to safety and safety regulation. In general, we encourage continued examination into **mandatory** cybersecurity regulation, standardization, and certification to ensure the safety of citizens; the security of private data; the protection of critical infrastructure; and continued consumer trust in the safety and security of vehicles.

To that end, BlackBerry supports many of the findings of the Cyberspace Solarium Commission's (CSC) final report[3] - and with reference to the present discussion, particularly the findings of Pillar 4 - *Reshape the Cyber Ecosystem toward Greater Security*, focused on driving down vulnerabilities across the cyber ecosystem by shifting the burden of security away from end users to operators, developers, and manufacturers who can more effectively implement security solutions at the appropriate scale. We strongly agree with CSC that in some cases, where market forces are either not present or do not adequately address cyber risk, the U.S. government must explore executive action, investment, legislation, and regulation. We would suggest including CSC Pillar 4 recommendations as a reference and guidance for a *commonsense* approach to incentivizing greater cybersecurity regulation and practices in the market. Listed below in Section I and II are comments expressing our concerns with the voluntary guidance. In

[2] https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/vehicle_cybersecurity_best_practices_01072021.pdf

[3] Pillar 4 in pp. 71-94 of CSC Final Report

Section III we recommend use of a software composition analytic tool for verification and assurance of automotive complex supply chain to enhance NHTSA best practice and reiterate importance of ISO/SAE 21434 as the foundation for automotive cybersecurity.

I. Comments on the Voluntary Nature of the Document

The purpose and scope of *the document* clearly states that it is intended to be only a voluntary guidance for automakers. While voluntary cybersecurity guidance may have been appropriate a couple years ago, the recent (and unfolding) large scale supply chain attack, as well as the CSC Pillar 4 findings referenced above, are a strong indication that voluntary cybersecurity guidance will no longer meet the nation's cybersecurity needs in the future. This is particularly true as transportation, mobility and infrastructure become increasingly connected (e.g., connected vehicles, vehicle-to-infrastructure connectivity; etc.) and as sophisticated threats proliferate. When viewed in combination with the lessons still being learned from the recent cyberattacks on US Governmental systems that were perpetrated by threat actors who gained access to supply-chain build systems, we must ask ourselves whether a voluntary approach is enough. Therefore, BlackBerry encourages NHTSA to consider recommendations put forward in CSC Pillar 4, taking into account the frequent absence of sufficient market forces to incentivize and drive industry actors to implement high cybersecurity standards.

It should be noted that the Department of Defense classifies cyberspace as an *Operational Domain of Warfare*[4]; meaning that much like the land, sea, and air, it is a domain that is vital to the national security of the United States. Allies and adversaries of the United

[4] *Summary of the 2018 National Defense Strategy*, (2018) United States Department of Defense, Page 6

States regularly utilize cyberspace as a means of exerting national power. As the Department of Homeland Security pointed out in their 2019 public-private report,[5] transportation, and specifically modern vehicles, have several use cases in this domain. As we face malicious nation state actors in cyberspace possessing the ability to apply human, electronic, and cyber intelligence targeting our system's weaknesses, our cyber defense capabilities must extend beyond technical design protections alone. This requires a high-level of threat intelligence, constant monitoring, secure software development lifecycle management, and supply chain protection. Rarely does the market reward features that they cannot prescribe a value, creating a market failure. Examples of the government's protection from market failure abound in the history of NHTSA; seat belts, air bags, and back-up cameras all are mandatory because companies that take on the extra cost of providing these items as a standard, were not rewarded by the market; and the *public good* was protected through NHTSA regulation. We recommend NHTSA to consider legislation or regulatory approach to drive industry to meet sufficiently high cybersecurity standards.

II. Comments on Self-Assessment and Certification

Self-assessment is an excellent tool in preparing for certification inspections and audits. BlackBerry believes, however, that self-assessments, in line with industry guidelines and best practices, may not offer sufficient protection against common cyber threats and vulnerabilities. In fact, from the standpoint of critical infrastructure, an exclusive reliance on self-certification could lead to unintentional and disastrous outcomes. As discussed above, the motivations for nation state actors to infiltrate, manipulate, and disrupt the U.S. ground transportation system are

[5] *Commodification of Cyber Capabilities: A Grand Cyber Bazaar*, (2017), United States Department of Homeland Security, Page 28

very high. In addition, with the inclusion of in-car payments and the exchange of personal data, criminal elements will see automobiles as attractive targets. It is nearly impossible for a firm that is not focused on national security and cyber security to internally track and adapt to these active threats. Although, security is critical to safety, it is very different than safety in its nature. Security changes as the adversary changes its tactics, techniques, and procedures. Companies that focus on outside auditing can provide recommendations and changes to internal procedures that will maintain safety within the vehicle. The incentive for a company which is not focused on security auditing, to find and adapt to vulnerabilities in procedure and product due to changes in the threat landscape is heavily countered by the cost of such changes. Outside auditors provide an objective assessment and will ensure that all manufactures meet the same standards and incur the same costs. For the reasons mentioned above, BlackBerry recommends NHTSA to consider alternative approach to encourage outside cybersecurity auditing.

III. NHTSA Best Practices and Supporting Standards

A. Software Bill of Material and securing supply chain

BlackBerry agrees with NHTSA on including best practices G10, G11, and G12 that support production of a software bill of materials, and which recommend that for each identified operational software component there should also be regular cross-checking of databases to search for vulnerabilities. BlackBerry recommends that OEMs should also acquire the capability to independently verify software bill of material (SBOM) information that is provided by their suppliers through use of a software composition analysis tool that works on binary images provided by their suppliers. Such a tool can also be used by an OEM to either create a software inventory, or to augment an existing inventory. The tool should also report vulnerability information associated with the software inventory. Such a capability enables an OEM to maintain a link between the known SBOM for a given software version and the set of

ECUs and vehicles that uses this version; and manage software update and risks more effectively. An example of where and how the software is deployed affects the risk profile is as follows. Contrast the case where a serious vulnerability is only associated with a test vehicle as opposed to a large number of passenger vehicles on the road, emergency or commercial vehicle handling dangerous goods.

As well as identifying open source components within the supplied software, such a tool can also be used to provide software quality KPIs that an OEM can use to drive cybersecurity improvements throughout the supply chain. OEMs should be encouraged to also apply such verification as part of software update processes. Suppliers should also be encouraged to make use of such static analysis tools during their build processes to ensure that any cybersecurity weaknesses are addressed throughout the development lifecycle, to drive improvements in software quality KPIs and to verify their SBOM prior to releasing it to the next downstream company. Section 2.5.3 of Auto-ISAC's 'Threat Detection, Monitoring and Analysis' best practice guidance similarly highlights the need for OEMs to maintain inventories of assets, so that the OEMs can better understand the root causes for any incidents and so that supply chain partners can be contacted where necessary. In addition, BlackBerry recommends that automation should be used wherever possible, for example an OEM may monitor vulnerability databases. When monitoring determines that a new vulnerability has been registered against any open source software that is in the vehicle, this can be used to populate the database of an OEM-local vulnerability tracking system. Registering a vulnerability can also trigger the sending of a request-for-information to the potentially impacted supplier, who can then respond to the OEM with information such as whether or not the vulnerability is exploitable and, if so, any mitigations that need to be applied.

To summarize, BlackBerry suggests that the best practice should recommend use of a software composition analysis tool by both OEM and suppliers, both for the purposes of verifying and/or creating the software bill of materials and for the purposes of assessing and verifying use of secure software coding. This should include use of a tool that works on the binary image of the actual built code that will be deployed on the vehicle, and which can additionally check that good security practice has been followed during compilation.

B. Protection from Supply Chain Attacks

Whilst SBOMs are useful in providing protection against certain classes of attacks on supply-chain provided software components, there are other supply-chain related cybersecurity measures that NHTSA may wish to emphasize in the guidance. Specifically, following the recent attacks on US Governmental systems that were perpetrated by threat actors who gained access to supply-chain build systems, and in-line with the spirit of President Biden's recent executive order on supply chain integrity, NHTSA may wish to provide guidance to encourage automotive suppliers and OEMs to protect against compromises of this type and of similar types. Such guidance should encourage suppliers to implement cybersecurity management systems and processes to ensure integrity of: source code, source code repositories, build systems, development environments and deployment of release builds. Whilst there are many measures that can be taken, it's worth highlighting that some improvements could also incorporate use of static analysis and malware scanning of binaries both by suppliers and OEMs to search for unexpected changes introduced during development and/or build.

C. Considerations for safety critical functionality

Since the focus of the best practice is on cybersecurity measures directed at ensuring safety of vehicle occupants and other road users, it is worth highlighting that because safety and security are both emergent properties of the system there is benefit in considering the two aspects

of safety and cybersecurity risk management together. It can for example, be the case that OEMs and suppliers need to make trade-offs between safety and cybersecurity, since a solution for an issue in one domain, may cause problems in the other. Equally, whilst there can be tensions in fulfilling the requirements for safety and cybersecurity there are also multiple synergies that can be exploited, for example in identifying potential sources of harm and their potential impact. Co-assurance of safety and cybersecurity can prove useful. These overlaps in the fulfillment of safety and cybersecurity requirements and the need to ensure accountability for both safety and cybersecurity can impact the ways in which OEMs design and develop their organizations, processes and culture. Some of the techniques for assessing risk such as Fault Tree Analysis and System Theoretic Process Analysis (STPA)[6] that have often been used in safety engineering can be useful ways by which both safety and cybersecurity experts can collaborate to better understand risks and possible sources of harm.

One of the tensions between cybersecurity and safety engineering is the desire in cybersecurity engineering to quickly patch discovered vulnerabilities, whilst in contrast in the safety engineering world the modus operandi is to only make updates after careful, and therefore often time consuming, consideration of the possible safety impacts. BlackBerry recommends that system designers give consideration to this problem during system design and consider how it can be managed through the appropriate use of modularity in software design. Modularity can help in reducing the amount of safety analysis that needs to be done because in some instances it is possible to reason about the impact on the patched module alone, rather than having to consider the impact of the change on a much larger piece of monolithic (less well modularized) code. NHTSA may wish to consider making reference to some of the work that has been done

[6] STPA handbook; N.Leveson, J. Thomas, https://psas.scripts.mit.edu/home/materials

in jointly considering the problems of safety and cybersecurity risk management, for example the IET and UK NCSC's 2021 'Code of Practice: Cybersecurity and Safety'[7].

D. Supporting standards

BlackBerry strongly support NHTSA on referencing to the automotive industry standard of ISO/SAE 21434 throughout their recommendations. Citing of an industry-agreed standard for automotive cybersecurity is seen as extremely beneficial to the automotive community as it will universally align OEMs and suppliers, which is especially important for suppliers located outside of the US.

BlackBerry kindly informs NHTSA that the next draft version of ISO/SAE 21434, known as Final Draft International Standard (FDIS), has been agreed by the technical committees in charge of its development and will soon be made public (expected March/April 2021). It should be noted that some clauses have been moved and therefore some referenced sections and referenced requirements will need to be corrected due to a change in their numbering.

Following on from ISO/SAE 21434, there is likely to be further work undertaken by the aforementioned technical committees, the exact details of which are not yet finalized, but at time of writing are expected to cover at least the following: enhanced definition and application of the Cybersecurity Assurance Levels (CALs), further guidance for assessing the feasibility of attacks, and further definition of verification and validation methods, to name just a few of the more popular topics under discussion. BlackBerry strongly supports this further work, as it will benefit the automotive industry in providing clearer and more precise best practice cybersecurity to the

[7] https://electrical.theiet.org/guidance-codes-of-practice/publications-by-category/cyber-security/code-of-practice-cyber-security-and-safety/

industry, and in the case of CALs, will encourage competition between suppliers for higher levels of product cybersecurity.

Also, BlackBerry would like to raise to the attention of NHTSA the upcoming standard for software updates, ISO 24089 (currently at Committee Draft (CD) stage), and the upcoming best practice guidance for performing technical audits for road vehicles in ISO PAS 5112 (soon to enter CD stage, expected around March 2021). Referencing of ISO 24089 is seen as beneficial to recommendations G.10, G.11, G.30, T.21, and T.22. Referencing of ISO PAS 5112 is seen as beneficial to recommendations G.36 and G.37.

IV. Conclusion

BlackBerry Corporation commends this effort and its purpose, and we are grateful for the opportunity to comment on this vital effort. We agree with the updated best practices, standards, and references utilized within *the document*. And we encourage a more active role of regulation and compulsory requirements above voluntary guidance.

Respectfully submitted,

BLACKBERRY CORPORATION

By: Takashi Suzuki
Takashi Suzuki
Senior Director, Standards

March 12, 2021