March 15, 2021

Dr. Cem Hatipoglu
Associate Administrator for Vehicle Safety Research
National Highway Traffic Safety Administration
U.S. Department of Transportation
1200 New Jersey Ave S.E., Washington, D.C. 20590

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

Dear Dr. Hatipoglu,

Continental is pleased to submit these comments in response to the notice published in the Federal Register on January 12, 2021 requesting input on the Agency's updated draft cybersecurity best practices document titled *Cybersecurity Best Practices for the Safety of Modern Vehicles*.

We appreciate the agency's efforts to document cybersecurity best practices and make them available to our company and the industry at large. We also appreciate the extent to which the agency has sought to ensure that the document reflects ongoing cybersecurity-related initiatives and efforts by organizations such as SAE International (SAE), the International Organization for Standardization (ISO), NIST, and the Automotive Information Sharing and Analysis Center (Auto-ISAC). Going forward, we urge the agency to update its best practices document frequently (at least on an annual basis). To the extent industry is utilizing the document, failure to keep the document current could create confusion for stakeholders and negatively impact motor vehicle safety.

At Continental, we have many team members dedicated to the issue cybersecurity. In fact, in 2017, we added to our competency in this area by acquiring Argus Cyber Security, a global leader in automotive cyber security. Together with our subsidiary Elektrobit (a developer of embedded and connected technology products and solutions for the automotive industry), we offer multi-layered, end-to-end automotive cyber security solutions and services to protect connected vehicles from cyber-attacks.

In reviewing NHTSA's latest update to the best practices, we sought input from many cybersecurity experts residing within Continental. This included input from:

- Continental's Security & Privacy Competence Center
- Continental Autonomous Mobility and Safety Business Unit[1]

[1] Continental's Autonomous Mobility and Safety business area develops, produces and integrates active and passive safety technologies and controls vehicle dynamics. The product portfolio ranges from electronic and hydraulic brake and chassis control systems to sensors, advanced driver assistance systems, airbag electronics and sensorics as well as electronic air suspension systems all the way to windscreen washer systems and headlight cleaning nozzles.

- Continental's Vehicle Networking and Information Business Unit[2]
- Powertrain (Vitesco Technologies)[3]
- ARGUS Cyber Security

Below, the compiled input from our team of experts is summarized for your consideration.

GENERAL CYBERSECURITY BEST PRACTICES (G.1 – G.43)

G.1 ***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.***

Continental: There is no one entity responsible for the "automotive industry." Therefore, a term such as "vehicle manufacturers" should be used in order to reduce ambiguity. Alternatively, "automotive industry" should be defined.

G3 ***The automotive industry should follow a robust product development process based on a systems-engineering approach with the goal of designing systems free of unreasonable safety risks, including those from potential cybersecurity threats and vulnerabilities.***

Continental: There is no one entity responsible for the "automotive industry." Therefore, a term such as "vehicle manufacturers" should be used in order to reduce ambiguity. Alternatively, "automotive industry" should be defined.

Continental: Process guidance should also touch upon the organization's process landscape (policies, processes, procedures, etc.) when it comes to cyber-threat, vulnerability and attack monitoring, detection and response during production and post-production stages.

---

[2] Within Continental, the Vehicle Networking and Information units specializes in information management. It develops and produces network, information and communication solutions and services for cars and commercial vehicles.

[3] Formerly the Continental Powertrain Division, Vitesco Technologies provides innovative, efficient electrification technologies for all types of vehicle. Its portfolio includes 48-volt electrification solutions, electric drives, and power electronics for hybrid and battery-electric vehicles.

G.6 ***Manufacturers should consider the risks associated with sensor vulnerabilities and potential sensor signal manipulation efforts such as GPS spoofing, road sign modification, Lidar/Radar jamming and spoofing, camera blinding, or excitation of machine learning false positives.***

Continental: In addition to G.6 language as drafted, please consider including the following: *In addressing such risks, manufacturers should consider the use of robust sensors which, by design, minimize the impact of a manipulation of sensoric perception. Furthermore, manufacturers may consider adopting mitigation strategies to address sensor vulnerabilities at the vehicle architecture level.*

Continental: G.6 could be integrated into section 4.2.2 "Risk Assessment" rather than have a separate section for a particular type of recommended risk evaluation which may lead some to making conclusions about NHTSA's risk priorities (i.e., that sensor vulnerabilities and manipulation efforts are more important than other risks according to NHTSA).

G.7 ***Any unreasonable risk to safety-critical systems should be removed or mitigated to acceptable levels through design, and any functionality that presents an unavoidable and unnecessary risk should be eliminated where possible.***

Continental: In addition to G.7 language as drafted, please consider the following points:

- The overall vehicle system should detect and react to intrusions.

- Each manufacturer may have a different interpretation of what is "unreasonable"; therefore, it would be helpful for NHTSA to provide guidance about what is and is not an acceptable safety risk due to a cyber threat / vulnerability. Such guidance could be criteria with which to evaluate a given risk.

- It would make more sense if unavoidable risks from unnecessary functions were always removed (unless there is clear justification for keeping the unnecessary function(s)); while unavoidable risks for necessary functions should be "eliminated where possible."

- NHTSA should consider integrating G.7 into the following sections:

    - 4.2.2 "Risk Assessment" – if the section name changed from Risk Assessment to "Risk Assessment & Management"

    - 4.2.5 "Protections" – so as to have all activities related to identified risk consolidated into a single provision.

G8 ***For remaining functionality and underlying risks, layers of protection that are appropriate for the assessed risks should be designed and implemented.***

Continental: To support the wider effort of protecting the fleet, vehicle manufacturers should establish and maintain monitoring, analysis, and response measures and, at a minimum, the ability to collect and analyze vehicle data.

G.9 ***Clear cybersecurity expectations should be specified and communicated to the suppliers that support the intended protections.***

Continental: We agree. We suggest that NHTSA frequently update its guidance to ensure that manufacturers have a common understanding of latest expectations. This will help ensure that state-of-the-art measures are being deployed.

G.11 ***Manufacturers should track sufficient details related to software components, such that when a newly identified vulnerability is identified related to an open source or off-the-shelf software, manufacturers can quickly identify what ECUs and specific vehicles would be affected by it.***

Continental: We think that it is not enough to be able to quickly identify relevant vulnerabilities. It should be recommended that OEMs also have a response plan and infrastructure in place to address new cyber threats, vulnerabilities and/or attacks in the field. Moreover, guidance should indicate that the response time should be sufficient to ensure that consumers are not exposed to safety critical vulnerabilities for many months or years.

NHTSA should consider clarifying that G.11 is directed toward "vehicle manufacturers."

G.12 ***Manufacturers should evaluate all commercial off-the-shelf and open-source software components used in vehicle ECUs against known vulnerabilities.***

Continental: We suggest that G.12 specify that such evaluations should be conducted in accordance with ISO/SAE 21434. Further, we believe that such guidance should additionally recommend there be a process in place to address vulnerabilities/risks when identified.

G21 ***Companies should use a systematic and ongoing process to periodically re-evaluate risks and make appropriate updates to processes and designs due to changes in the vehicle cybersecurity landscape, as appropriate.***

Continental: In G.21, the word "designs" should be replaced with "protection" as it is more realistic for the manufacturer to be able to make adjustments / updates to measures / protections than it is for them to make changes to underlying designs.

G.27-33

Continental: Section 4.5 (Organizational Incident Response Process) should note that organizational processes related to cyber-risk management (including incident response) should be fully integrated within a process landscape and not operated or managed in silos.

G.30 ***Commensurate to assessed risks, organizations should have a plan for addressing newly identified vulnerabilities on consumer-owned vehicles in the field, inventories of vehicles built but not yet distributed to dealers, vehicles delivered to dealerships but not yet sold to consumers, as well as future products and vehicles.***

Continental: In future updates to G.30, NHTSA may look to UN Regulation No. 155 - *Cyber Security and Cyber Security Management* for more precise guidance in this area. UN Regulation No. 155 will apply to vehicles produced after July of 2022.

G.40 ***Any connection to a third-party device should be authenticated and provided with appropriate limited access.***

Continental: In future updates to G.30, NHTSA may look to UN Regulation No. 155 - *Cyber Security and Cyber Security Management* for more precise guidance in this area. UN Regulation No. 155 will apply to vehicles produced after July of 2022.

TECHNICAL VEHICLE CYBERSECURITY BEST PRACTICES (T.1 – T.23)

T.1 ***Developer-level access should be limited or eliminated if there is no foreseeable operational reason for the continued access to an ECU for deployed units.***

Continental: This guidance would also be true with regard to Programming sessions on CAN buses which can be reached in several ways using the car connectivity interfaces going through a gateway unit and/or the OBD port.

T.2 ***If continued developer-level access is necessary, any developer-level debugging interfaces should be appropriately protected to limit access to authorized privileged users.***

Continental: This guidance would also be true with regard to Programming sessions on CAN buses which can be reached in several ways using the car connectivity interfaces going through a gateway unit and/or the OBD port.

T.7 ***The use of global symmetric keys and ad-hoc cryptographic techniques for diagnostic access should be minimized.***

Continental: NHTSA should clarify that this requirement should be satisfied by employing state-of-the-art methods.

T.8 ***Vehicle and diagnostic tool manufacturers should control tools' access to vehicle systems that can perform diagnostic operations and reprogramming by providing for appropriate authentication and access control.***

Continental: NHTSA should clarify that this requirement should be satisfied by employing state-of-the-art methods.

T.10 ***Critical safety messages, particularly those passed across non-segmented communication buses, should employ a message authentication method to limit the possibility of message spoofing.***

Continental: NHTSA should define what constitute "critical safety messages" or otherwise remove the word "critical." T.10 might additionally note that deep packet inspection technology can be used to identify attacks within otherwise "authenticated" messages.

T.12 ***Such logs that can be aggregated across vehicles should be periodically reviewed to assess potential trends of cyber-attacks.***

Continental: Given the value of cross-fleet data analysis, we believe that T.12 should specify that, in the case it is technically feasible, all logs be aggregated across vehicles and periodically reviewed to assess potential trends of cyber-attacks.

T.13 ***Manufacturers should treat all networks and systems external to a vehicle's wireless interfaces as untrusted and use appropriate techniques to mitigate potential threats.***

Continental: NHTSA should clarify that this requirement should be satisfied by employing state-of-the-art methods.

T.21 ***Automotive manufacturers should employ state-of-the-art techniques for limiting the ability to modify firmware to authorized and appropriately authenticated parties.***

Continental: To the extent NHTSA is in a position to clarify what it regards as state-of-the-art, we urge it to do so.

T.22 ***Maintain the integrity of OTA updates, update servers, the transmission mechanism and the updating process in general.***

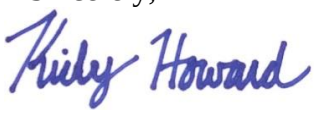
Continental: We suggest T.22 be revised to read as follows: *Vehicle manufacturers should maintain the integrity of OTA updates, update servers, the transmission mechanism, and the updating process in general.*

T.23 ***Take into account, when designing security measures, the risks associated with compromised servers, insider threats, men-in-the-middle attacks, and protocol vulnerabilities.***

Continental: We suggest T.23 be revised to read as follows: *In accordance with state-of-the-art techniques, take into account, when designing security measures, the risks associated with compromised servers, insider threats, men-in-the-middle attacks, and protocol vulnerabilities.*

Continental routinely provides substantive feedback to multiple State and Federal Agencies in collaboration with our customers, industry partners, and trade associations. We would like to thank NHTSA and Associate Administrator Hatipoglu for the opportunity to provide input on the agency's request for comment and welcome the opportunity to provide direct feedback during the review process. Should you have any questions or whish to discuss further, please do not hesitate to contact me by telephone at 202-440-1861 or by email at Kirby.Howard@Continental.com.

Sincerely,



Kirby Howard
Government Affairs
Continental AG
1101 K Street, N.W., Suite 1000
Washington, D.C. 20005