ZF North America, Inc.
12001 Tech Center Drive | Livonia | MI 48150

Docket Management Facility
US Department of Transportation
1200 New Jersey Avenue SE
West Building, Ground Floor, Room W12-140
Washington, DC 20590-0001

Department	Executive
From	Dr. Martin Fischer
Phone	734-855-2480
Email	m.fischer@zf.com
Date	March 8, 2021

Attention: Cem Hatipoglu
Associate Administrator for Vehicle Safety Research
National Highway Traffic Safety Administration

RE: Docket No. NHTSA-2020-0087

Dear Associate Administrator Hatipoglu:

ZF North America (ZF) appreciates the opportunity to respond to NHTSA's Request for Comments (RFC) regarding its draft update to *Cybersecurity Best Practices for the Safety of Modern Vehicles* (the "Draft Update"). As a leading producer of a diverse array of vehicle technologies that rely on robust cybersecurity measures to ensure safety and reliability, ZF is pleased to inform this process.

ZF North America is headquartered in Livonia, Michigan, and is a primary developer and producer of active, passive, and integrated safety systems, as well as electromobility solutions, serving all major vehicle manufacturers. We proudly design and produce many of these technologies and products here in the United States.

ZF is appreciative of this initiative by NHTSA to update and further promote consensus-based best practices regarding vehicle cybersecurity. This is – and we believe, should continue to be – an iterative process to adapt and improve defenses to evolving threats to vehicles that are increasingly reliant on software and electronic infrastructure. In the comments below, ZF provides feedback regarding various sections of the Draft Update.

Highlights of ZF Comments:

- Language in the scope of this Draft Update could be amended to explicitly mention information technology in parallel with the mentions of motor vehicle equipment and software, as these three areas are increasingly interconnected and interdependent.
- At several points in the document, further definition of "vehicle lifecycle" would enable greater clarity for the industry and, hopefully, stronger vehicle cybersecurity protections.
- To promote greater uniformity in confronting common cybersecurity threats, where possible, NHTSA could consider aligning with existing cybersecurity best practices, including those developed by SAE/ISO.
- The development of best practices or guidance regarding the cybersecurity event vehicle data NHTSA urges the industry to collect would be beneficial.

ZF's full comments are provided on the following pages. Again, ZF appreciates this opportunity to share our perspective with NHTSA. We stand ready to provide further clarification and insights regarding this feedback, as needed.

Best regards,

Dr. Martin Fischer
President
ZF North America, Inc.

ZF Response to NHTSA-2020-0087: Draft Update to *Cybersecurity Best Practices for the Safety of Modern Vehicles*

The *Cybersecurity Best Practices for the Safety of Modern Vehicles* is a useful tool for industry stakeholders to review and incorporate recommended best practices into their cybersecurity processes. ZF appreciates the changes included in this Draft Update and is pleased to provide further comment to inform the iteration of this document moving forward. Below is ZF's feedback regarding specific sections of the Draft Update.

General Questions:

2. Scope:

The scope of these Best Practices is stated as applying to motor vehicle equipment (including software), but it is important to ensure information technology protections are similarly prioritized. With increasingly connected vehicle architecture, the security of production IT systems cannot be disassociated from the cybersecurity of vehicles on the road. We therefore suggest an explicit mention that these three areas – equipment, software, and IT – are increasingly inextricably linked in automotive systems and should be collectively defended. Models for the concurrent defense of these interrelated systems include IEC/ISA 62443 and ISO 27000, as well as ISO/SAE 21434.

4. General Cybersecurity Best Practices

NHTSA should consider UNECE R155 as instructive, as it is based on current automotive best practices. Particularly useful is the UNECE R155 requirement that a cybersecurity management system (CSMS) be leveraged to promote security in the vehicle production process.

4.1 Leadership Priority on Product Cybersecurity

We recommend that NHTSA highlight the importance of leadership support for the full vehicle lifecycle, as the potential cybersecurity threats to vehicles extend beyond the R&D phase. For example, we suggest amending the following text as indicated in italics:

> [G.2][c] Enabling an independent voice for vehicle cybersecurity-related considerations within the *full vehicle lifecycle, including vehicle design, manufacturing, and post-production support processes.*

4.2 Vehicle Development Process with Explicit Cybersecurity Considerations

Multiple definitions of lifecycle exist among standards organizations, so it would be helpful for NHTSA to explicitly define the meaning of "lifecycle" within the context of the Draft Update and to explain the rationale for that usage based on consideration of cybersecurity risks. While we recommend that definition align with the amendment suggested for [G.2][c], if not, [G.2][c] should also be amended to reflect the "lifecycle" definition ultimately used.

[G.3]

NHTSA might consider referring to ISO 15288 as an example of a robust product development process described in this section.

[G.7]

We recommend that NHTSA consider aligning its risk considerations to those used in existing cybersecurity standards. This could include ISO/SAE 21434, which outlines the management of risk through risk treatments, including *avoiding*, *reducing*, *sharing* (transferring) or *retaining* (accepting) risk.

[G.17]

Intrusion detection systems, while promising, have not yet been proven to substantively enhance security. This topic merits further research.

4.5 Organizational Incident Response Processes

[G.27]

We believe there is a typo in [d]: "[G.26 [a]-[c]]" should read "[G.27[a]-[c]]."

[G.30]

It is important that "in the field" be understood to reflect the broad post-development lifecycle, including time spent in maintenance. While this could be interpreted from the terminology used, we recommend being more specific in defining the scope of this term.

8.6 Event Logs

We recommend NHTSA provide guidance, in coordination with the U.S. Federal Trade Commission, regarding how best to maintain privacy protections while collecting data necessary for cybersecurity event logs.