



March 15, 2021

USG 5018

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 (January 12, 2021)

Dear Mr. Hatipoglu:

General Motors LCC (“GM” or “General Motors”) welcomes the opportunity to provide input to the National Highway Traffic Safety Administration (“NHTSA”) in response to its request for public comments on the updated draft cybersecurity best practices document titled *Cybersecurity Best Practices for the Safety of Modern Vehicles* (“Cybersecurity Best Practices”).

GM has made substantial investments in the cybersecurity of its products and services via its dedicated Product Cybersecurity organization, the first-of-its-kind in industry. Product Cybersecurity is one of six cybersecurity-related domains that comprise a Global Cybersecurity organization which reports to the CEO and Board of Directors, ensuring C-suite awareness, engagement, and direction.

GM contributes to an enterprise commitment to customer safety through a robust product cybersecurity strategy. Our three-pillar approach prioritizes defense-in-depth, monitoring and detection, and incident response, all of which are enhanced by our commitment to proactive information sharing.

We welcome the opportunity to share more about how we secure our systems and protect our customers.

### **Defense-In-Depth**

Product Cybersecurity implements a risk-based approach to secure GM vehicles. The approach starts at the component level by assigning security controls commensurate with hardware and software attributes and their associated attack surfaces. Next, security engineers perform a threat analysis to identify sub-system and system-level attacks and assign appropriate goals. Finally, when required, GM’s security engineers assign additional security controls to support these goals and create a layering of security controls. This layering results in a defense-in-depth, designed to thwart the successful completion of an attack and to frustrate an attacker.

---

**general motors**

Product Cybersecurity adheres to a Security Development Lifecycle to synchronize supplier engagement and maximize security requirement compliance success, often culminating with a penetration test managed and/or executed by our internal Testing Team.

### **Monitoring and Detection**

The second pillar encompasses multiple activities to monitor for and detect the introduction and/or exploitation of vulnerabilities that could compromise customer safety. Some of the activities include:

- Evaluating customer reports via our service centers and OnStar call center
- Managing a Security Vulnerability Disclosure program on HackerOne
- Sharing and consuming cyber threat reports via the Auto-ISAC
- Proactive monitoring of open source information sources by the GM Cyber Defense team
- Attending nationally and internationally-recognized cybersecurity conferences
- Performing software composition analysis scans on supplier-provided firmware and GM-produced source code to identify and remediate known vulnerabilities before production
- Performing or managing the penetration testing of key vehicle components, subsystems, and systems
- Implementing security controls in the vehicle, telematics channels, and back office and monitoring for anomalous activity

### **Incident Response (IR)**

The final pillar represents GM's IR-related activities, which are invoked from overt indicators of an in-progress or imminent vehicle attack or as a result of a detailed vulnerability management process that includes assessment and investigation phases with leadership reviews between the phases and prompts to invoke safety and IR processes as required. Additionally, GM deliberately engages in IR tabletop and no-notice exercises as well as IR info sharing and awareness engagements within and external to GM. Finally, GM tracks and reports IR maturity using a tailored NIST Cybersecurity Framework.

### **Information Sharing**

GM collaborates with experts in the defense and aerospace industries, government organizations, academia, and industry consortiums on best practices and key learnings. GM is an active participant in industry-wide efforts to enhance automotive cybersecurity resilience, including the Auto-ISAC, currently chaired by Kevin Tierney, GM's VP of Global Cybersecurity.

Further, GM continues to collaborate with industry technical consortia and standards bodies, including recent collaborative efforts between SAE International and ISO to develop ISO/SAE 21434 – Road Vehicles – Cybersecurity Engineering, and has introduced a risk modeling framework that is fundamental 21434 compliance and UN Regulation 155 – Cybersecurity type approval.

### **Cybersecurity Best Practices Recommendations**

With respect to the update to the Cybersecurity Best Practices, General Motors expresses support for NHTSA's approach to vehicle cybersecurity.

#### **Continue NHTSA's Longstanding Self-Certification Approach**

With the constantly evolving cybersecurity threat landscape, it is important that automakers and governments alike deploy multi-layer defense systems and remain agile to respond to rapid and dynamic evolving cyber threats. We encourage NHTSA to continue to update this foundational best practice document to keep pace with the rapidly evolving threat landscape, as well as to incorporate important cybersecurity-related work and actions by industry, standards bodies, and other stakeholders. Further, we support NHTSA in its approach to vehicle cybersecurity through the issuance of best practices, as opposed to type-approval regulations that could quickly become obsolete.


#### **Harmonization**

Globally, there are disparate efforts focused on automotive cybersecurity. To the extent possible, we encourage NHTSA to help ensure alignment and harmonization between its Cybersecurity Best Practices and ongoing work underway in international standards bodies and regulatory agencies.

Specifically, we encourage NHTSA to explore opportunities to enhance alignment between the Cybersecurity Best Practices, industry standards, and the recently adopted UN regulations for automotive cybersecurity and over-the-air updates. As the party leading the translation/implementation of the UN regulations to the 1998 Agreement, NHTSA has an opportunity to help shape this process in a manner that offers the greatest opportunity for international alignment and harmonization on automotive cybersecurity.

General Motors appreciates the opportunity to comment on the updates made to the Cybersecurity Best Practices. We look forward to continuing to work with NHTSA and federal partners on this important topic.

Sincerely,



Alfred Adams  
Chief Product Cybersecurity Officer  
General Motors