ALLIANCE FOR AUTOMOTIVE INNOVATION

Submitted via Email at cyberframework@nist.gov

November 6, 2023

Katherine MacFarland
Applied Cybersecurity Division
National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, Maryland 20899-2000

RE: Public Draft: The NIST Cybersecurity Framework 2.0

The Alliance for Automotive Innovation ("Auto Innovators") welcomes the opportunity to provide input to the National Institute of Standards and Technology ("NIST") on the draft Cybersecurity Framework ("CSF" or "Framework") 2.0. Auto Innovators appreciates that NIST intends the CSF to be a living document that is updated over time with stakeholder input.

Auto Innovators represents the manufacturers that produce most of the cars and light trucks sold in the U.S., original equipment suppliers, technology companies, battery manufacturers, and other value-chain partners within the automotive ecosystem. Representing approximately 5 percent of the country's GDP, responsible for supporting 10 million jobs, and driving $1 trillion in annual economic activity, the automotive industry is the nation's largest manufacturing sector.

The automotive industry reflects the evolving cybersecurity landscape, as the integration of vehicles into a broader ecosystem of connected infrastructure and innovative vehicle technologies provides consumers with new ways of interacting with and engaging in personal mobility and spurs new business models, products, and services. These shifts also have the potential to unlock societal benefits related to safety, fuel efficiency, and transportation equity. However, this transformation can present new cybersecurity threats and risks, including connections and external stakeholders that extend beyond the vehicles themselves. The automotive industry continues to build in cybersecurity, identifying and mitigating cybersecurity risks throughout the connected digital ecosystem and related supply chains.

The CSF serves as a key resource in automotive cybersecurity. It helps to inform automotive industry standards and best practices, as well as regulatory guidance. For example, SAE International and the Automotive Information Sharing and Analysis Center ("Auto-ISAC") reference the CSF in their

industry cybersecurity-related standards (*e.g.*, ISO/SAE 21434)[1] and cybersecurity best practices,[2] respectively. In its voluntary guidance to industry, the National Highway Traffic Safety Administration ("NHTSA") specifically recommends that the automotive industry follow the CSF.[3] The references to, or incorporation of, the CSF into industry standards, industry best practices, and regulatory guidance point to the commonalities between the CSF and other private and public sector resources.

Auto Innovators supports several changes made in the draft CSF 2.0, such as the inclusion of the Govern function to emphasize cybersecurity governance, the addition of implementation examples to provide notional examples of action-oriented processes to achieve CSF subcategories, and the synthesis of cybersecurity supply chain risk management as a new Category. To further improve the CSF 2.0, we suggest that NIST:

- Add "Managing existing vulnerabilities" to (GV.SC);
- Modify (ID.RA-01) as follows: "Vulnerabilities in assets are identified, validated, recorded, and monitored;
- List common risk responses (*e.g.*, mitigate, accept, avoid, share) in (ID.RA-06);
- Add "Handling of identified risks with chosen risk response option is verified" to (PR.PS);
- Add "Analyzing protection against monitored vulnerabilities" to (PR.PS);
- Add "Monitored vulnerabilities are included in incident analysis" to (DE.AE); and
- Add "Cybersecurity supply chain risks are monitored" to (DE.CM).

The automotive industry looks forward to the release of the CSF 2.0 early next year. We appreciate that NIST continues to solicit multistakeholder input on technical and policy questions to ensure that the CSF remains a key resource for automotive cybersecurity.

Sincerely,

Tara Hairston

Tara Hairston
Senior Director, Technology, Innovation, & Mobility Policy

---

[1] ISO/SAE 21434:2021, *Road vehicles – Cybersecurity Engineering*

[2] Automotive Information Sharing and Analysis Center, *Automotive Cybersecurity Best Practices* [online]. Available at: Best Practices — Automotive ISAC.

[3] National Highway Traffic Safety Administration ("NHTSA"), *Cybersecurity Best Practices for the Safety of Modern Vehicles, 2022 Update* [online]. Available at: Cybersecurity Best Practices for the Safety of Modern Vehicles, Updated 2022 (nhtsa.gov).