ALLIANCE FOR AUTOMOTIVE INNOVATION

Submitted via Email at cyberframework@nist.gov

March 17, 2023

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

RE: NIST Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework

Dear Ms. MacFarland:

The Alliance for Automotive Innovation ("Auto Innovators") welcomes the opportunity to share its input to the National Institute of Standards and Technology ("NIST") on its Concept Paper that outlines significant potential changes that NIST is considering in developing 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 on proposed structural and directional changes.

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 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. This approach enables the realization of the safety, privacy, environmental, and societal benefits of vehicles with advanced and connected technologies.

Since 2014, the CSF's flexibility, simplicity, and ease of use have contributed to its use as a resource by the automotive industry. Its five functions – Identify, Protect, Defend, Respond, Recover – have provided companies with a common tool to communicate internally regarding ongoing cybersecurity activities, respond to cybersecurity threats, assess cybersecurity investments, and incorporate lessons learned. Companies have also used the CSF for external communications purposes, articulating their cybersecurity risk management expectations to suppliers and other business partners, as well as contextualizing their cybersecurity posture to customers and end users. As NIST notes in the Concept Paper, "The CSF has been adopted voluntarily and in governmental policies and mandates at all levels around the world, reflecting its enduring and flexible nature to transcend risks, sectors, technologies, and national borders."[1]

In addition to aligning internal and external communications, the CSF informs automotive industry standards and best practices, as well as regulatory guidance. 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)[2] and cybersecurity best practices,[3] respectively. The National Highway Traffic Safety Administration ("NHTSA") recommends that the automotive industry follow the CSF.[4] 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. NIST publications often serve as a baseline to develop more targeted risk management approaches for specific use cases and industries, and the CSF is yet another example for the automotive industry.

Auto Innovators offers the following perspectives on behalf of the automotive industry:

- **Explicit Recognition of CSF's Broad Applicability:** Auto Innovators supports NIST's efforts to change the CSF's formal title to reflect its intended use by all organizations; to ensure that the CSF is helpful to organizations regardless of sector, type, or size; to prioritize exchanges with foreign governments and industries to facilitate international collaboration and engagement on CSF 2.0's development; and to engage strategically in the work of international standards developing organizations.

---

[1] National Institute of Standards and Technology, *NIST Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework* [online], pg. 3. Available at: NIST Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework.

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

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

[4] 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).

- **Retention of Framework Format:** Auto Innovators agrees that maintaining the CSF's flexibility, simplicity, and ease of use will enable it to remain scalable and adaptable for different organizations and multiple sectors. We also support NIST's plans to reference other Frameworks as guidance in CSF 2.0 or in companion materials; move toward the use of online, updatable references; work with the community to encourage and enable the production of mappings; and review the CSF to ensure that its broad outcomes can be used by organizations employing information technology ("IT"), Internet of Things ("IoT"), operational technology ("OT"), and/or cloud computing services. Linking the CSF and other NIST risk management frameworks could reveal opportunities to improve integration and alignment of NIST resources to better equip organizations. We further encourage NIST to partner with other U.S. federal agencies to map their guidance documents (*e.g.*, NHTSA Cybersecurity Best Practices for the Safety of Modern Vehicles – 2022 Update[5]) to the CSF and other NIST risk management resources.

- **Updating and Expanding Guidance for Framework Implementation:** NIST should develop action-oriented, notional implementation examples that can help organizations better account for the evolving nature of cybersecurity threats, organizational capabilities, mitigation technologies and techniques, the state of cybersecurity education, and current cybersecurity workforce needs. Clarifying the meaning and intent of each CSF Subcategory will help organizations utilize the CSF. Using the examples to highlight possible differences in implementations for platforms such as IT, IoT, OT, and cloud computing will also be useful in helping organizations adapt the CSF across all these domains. Auto Innovators recommends adding implementation examples to the CSF directly since that is likely the resource most known to organizations seeking to improve their cybersecurity risk management posture.

- **Adding Govern as a CSF Function:** Cybersecurity governance will be a useful addition to support the other CSF Functions and is consistent with the approach NIST has taken with its Privacy and Artificial Intelligence Risk Management Frameworks. As a cross-cutting Function, Govern can help organizations assess cybersecurity risks and impacts, understand cybersecurity roles and responsibilities, establish cybersecurity procedures and policies, and determine cybersecurity risk tolerances. Auto Innovators recommends that NIST make clear that governance outcomes inform "the prioritization and implementation of each of the current Functions."[6] This will help organizations apply cybersecurity risk governance to all stages of their cybersecurity risk management activities.

- **Addressing Cybersecurity Supply Chain Risk Management:** In CSF Version 1.1, NIST acknowledged the importance of supply chain risk management, the complexity and

---

[5] *Ibid.*

[6] *NIST Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework* [online], pg. 10-11.

interconnectedness of supply chains, and the importance of communicating cybersecurity risk among stakeholders throughout supply chains. Identifying, assessing, and managing both first- and third-party supply chain risks are critically important, and Auto Innovators supports the inclusion of additional guidance in CSF 2.0 to address both sets of risks. NIST should leverage its extensive supply chain risk management resources and help organizations streamline the adoption of their important aspects. In addition, NIST should work with the community to further discuss supply chain-related attestations and integrity checks that could relate to the CSF and its supply chain risk management resources. The further integration of cybersecurity supply chain risk management outcomes throughout the CSF Core across Functions should be sufficient to emphasize the importance of cybersecurity supply chain risk management.

- **Advancing Measurement and Assessment:** Auto Innovators agrees with NIST that there is no single approach to measure and assess the CSF. Auto Innovators recommends that NIST include examples of how organizations have used the CSF to assess and communicate their cybersecurity capabilities to better assure flexibility in how organizations implement the Framework. Such examples should note that assessments and related metrics can be qualitative, quantitative, or semi-quantitative.

Auto Innovators appreciates the opportunity to provide the automotive industry's perspectives on potential significant updates to the CSF. We look forward to continued engagement with NIST as it moves forward.

Sincerely,

Tara Hairston

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