April 25, 2022

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

RE: Request for Information on Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management

Dear Ms. MacFarland:

The Alliance for Automotive Innovation ("Auto Innovators") is pleased to submit comments to the National Institute of Standards and Technology ("NIST") in response to its request for information to assist in evaluating and improving its cybersecurity resources. Auto Innovators appreciates the opportunity to share the automotive industry's perspectives on the Framework for Improving Critical Infrastructure Cybersecurity ("CSF") and to contribute to the National Initiative for Improving Cybersecurity in Supply Chains ("NIICS").

Auto Innovators is the singular, authoritative, and respected voice of the automotive industry. Focused on creating a safe and transformative path for personal mobility, Auto Innovators represents the manufacturers that produce nearly 98 percent of cars and light trucks sold in the United States, original equipment suppliers, technology companies, and other value-chain partners within the automotive ecosystem. The automotive industry is the nation's largest manufacturing sector, representing 5.5 percent of the country's GDP and responsible for roughly 10 million jobs.

Auto Innovators agrees with NIST that the cybersecurity landscape has changed since the 2018 update to the CSF. Such a shift has been impactful in the automotive space. The integration of vehicles into a broader ecosystem of connected infrastructure, devices, features, and stakeholders – combined with innovative vehicle technologies – has the potential to unlock a wide array of societal benefits related to safety, fuel efficiency, and transportation equity. This transformation in personal mobility also can provide consumers with new ways of interacting and engaging with vehicles, spurring new business models, technologies, and services.

However, these opportunities also present new cybersecurity threats and risks, including some that are no longer isolated to the confines of vehicles. The automotive industry continues to build cybersecurity proactively into the products and services that will define the future of transportation, but cybersecurity threats and risks can now extend to an ecosystem of connections and external stakeholders far more vast. Increased awareness and mitigation of cybersecurity risks throughout this connected and

digital ecosystem and related supply chains is critical to realizing the safety, privacy, environmental, and societal benefits of vehicles with advanced and connected technologies.

The CSF has served as a useful resource for the automotive industry since its inception in 2014. Its five functions – Identify, Protect, Defend, Respond, Recover – have provided companies with a common tool to communicate internally regarding ongoing cybersecurity activities, responses to cybersecurity threats, assessing cybersecurity investments, and lessons learned. Companies have also used the CSF to articulate their cybersecurity risk management expectations of suppliers and other business partners. As NIST notes, the CSF "is used widely by private and public sector organizations in and outside of the United States and has been translated into multiple languages, speaking to its success as a common resource."

In addition to internal company use, the automotive industry's utilization of the CSF extends to industry standards and best practices, as well as regulatory guidance. Both 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. The National Highway Traffic Safety Administration ("NHTSA") recommends that the automotive industry should follow the CSF as part of a "layered approach to vehicle cybersecurity, an approach that assumes some vehicle systems could be compromised, reduces the probability of an attack's success and mitigates the ramifications of unauthorized vehicle system access."[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. NIST publications often serve as a baseline to develop more targeted risk management approaches for specific use cases and industries, and the CSF for the automotive industry is yet another example.

Seeking information from stakeholders to evaluate and improve the CSF, as well as inform the direction of the NIICS, is a worthwhile endeavor. With regards to the Request for Information, Auto Innovators offers the following perspectives on behalf of the automotive industry:

- **Consider Profiles on Other Technology Uses:** NIST explains that the CSF "is applicable to organizations relying on technology, whether their cybersecurity focus is primarily on information technology (IT), industrial control systems (ICS), cyber-physical systems (CPS), or connected devices more generally, including the Internet of Things (IoT)." However, given its high-level and conceptual nature, it can be challenging to adapt the CSF across all these domains. Since automotive companies operate within all of these areas, we suggest that NIST consider the creation of profiles on the various technology uses the CSF acknowledges. Additional informative references beyond ISA/IEC 62443 to further articulate the applicability of the CSF to operational technology, industrial control systems, and cyber-physical systems would also be helpful.

---

[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, *Cybersecurity Best Practices for the Safety of Modern Vehicles, Draft 2020 Update* [online]. Available at: Cybersecurity Best Practices for the Safety of Modern Vehicles (nhtsa.gov).

- **Potential Adoption of Practice Guide Approach:** As NIST notes, much has changed in the cybersecurity landscape since the last iteration of the CSF in April 2018. However, frequent changes to the CSF could potentially impact the usability and backward compatibility of the CSF for organizations. Therefore, NIST should consider providing additional examples and practices to assist organizations in using the CSF to better account for the evolving nature of cybersecurity threats, organizational capabilities, mitigation technologies and techniques, the state of cybersecurity education, and the current cybersecurity workforce needs. One potential approach is producing a companion Practice Guide for the CSF such as that which NIST plans to develop in conjunction with the Artificial Intelligence Risk Management Framework, or AI RMF.

- **Include Industry-Specific Informative References:** The inclusion of informative references in the CSF is helpful for entities to map their organizational activities and capabilities (Functions) and discrete outcomes (Categories and Subcategories) to existing standards, practices, and guidance documents. The majority of informative references currently included in the CSF are industry-agnostic. For heavily regulated industries like the automotive industry, the inclusion of industry-specific standards, practices, and guidance documents would provide additional benefit to companies in aligning their current and target cybersecurity risk management practices with the CSF. While incorporating every industry-specific standard, practice, and guidance document into the CSF is likely to be cumbersome and make the document unwieldy, NIST should consider one or all of the following: 1) working with industry groups to develop exemplars that highlight their industry-specific documents; 2) incorporating guidance documents from other U.S. federal agencies (*e.g.*, NHTSA, Food & Drug Administration) into the next iteration of the CSF; or 3) developing a compendium of cybersecurity resources and best practices documents as an Appendix to the CSF.

- **Further Leverage OLIR:** NIST has utilized the National Online Informative References ("OLIR") Program to map the relationships between some of its other risk management resources and the CSF (*e.g.*, Risk Management Framework[4], Privacy Framework[5], and Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management[6]). The private sector has also used OLIR to map industry-specific guidance documents against the CSF and other NIST publications. Auto Innovators encourages NIST to also use OLIR to map the CSF to forthcoming publications on cybersecurity supply chain risk like the pending revision to NIST SP 800-161 Revision 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations.[7] Mappings between the CSF and other NIST risk management frameworks

---

[4] Joint Task Force (2018), *Risk Management Framework for Information Systems and Organizations – A System Life Cycle Approach for Security and Privacy* [online]. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37, rev. 2. Updated December 2018. Available at: Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy (nist.gov).

[5] National Institute of Standards and Technology (2020), *NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management, Version 1.0* [online] Available at: NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management, Version 1.0.

[6] Stein, Kevin et al. (2020), *Integrating Cybersecurity and Enterprise Risk Management* [online]. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8286. Released October 2020. Available at: Integrating Cybersecurity and Enterprise Risk Management (ERM) (nist.gov).

[7] Boyens, Jon et al. (2021), *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* [online]. (National Institute of Standards and Technology, Gaithersburg, MD), Draft (2nd) NIST Special Publication (SP) 800-161, rev.

could, in turn, reveal opportunities to improve integration and alignment of NIST resources. We also recommend that NIST partner with other U.S. federal agencies to map their guidance documents (*e.g.*, NHTSA Cybersecurity Best Practices for the Safety of Modern Vehicles – Draft 2020 Update[8]) to the CSF and other NIST risk management documents as well. To facilitate increased use of the Program, NIST could also hold a workshop session with private sector entities to discuss best practices on how to map industry-specific resources to NIST publications in OLIR.

- **Expand Cybersecurity Supply Chain Risk Management Focus Beyond the CSF:** In Version 1.1, NIST acknowledged the criticality of supply chain risk management as an organizational function, the complexity and interconnectedness of supply chains, and the importance of communicating cybersecurity risk among stakeholders throughout supply chains. Given the breadth and scope of NIST's supply chain risk management resources, the CSF could potentially help organizations streamline the adoption of important aspects of these resources as they incorporate cybersecurity supply chain risk management into their broader enterprise risk management approaches. In addition, NIST should work with its various stakeholders to further discuss supply chain-related attestations and integrity checks, beyond a self-assessment model, that could relate to the CSF and its supply chain risk management resources.

Auto Innovators appreciates the opportunity to provide the automotive industry's perspective to NIST on potential improvements to the CSF and priority supply chain-related cybersecurity needs for the automotive sector to inform the development of NIICS. We look forward to further engagement with NIST on this and other efforts.

Sincerely,

Tara Hairston

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

1. Updated October 2021. Available at: Draft (2nd) NIST SP 800-161 Rev. 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations.

[8] See footnote 3.