ALLIANCE FOR AUTOMOTIVE INNOVATION

September 29, 2022

SUBMITTED VIA ELECTRONIC MAIL at AIframework@nist.gov

Elham Tabassi
Chief of Staff, Information Technology Lab
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, Maryland 20899

RE: Request for Comment on Artificial Intelligence Risk Management Framework Second Draft

Dear Ms. Tabassi:

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 comments on the Artificial Intelligence Risk Management Framework ("AI RMF") Second Draft. Auto Innovators appreciates that NIST continues to seek and incorporate feedback to support the AI RMF's development.

Auto Innovators is the singular, authoritative, and respected voice of the automotive industry. 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. Representing approximately 5.5 percent of the country's GDP and responsible for roughly 10 million jobs, the automotive industry is the nation's largest manufacturing sector.

The automotive industry leverages the power of artificial intelligence to integrate driver support features, advanced safety technologies, and automated driving systems into consumer vehicles. These and other technological advances have the potential to protect vulnerable road users, reduce serious injuries and deaths, improve roadway safety, and provide environmental benefits. To improve transportation safety through the deployment of technology, including artificial intelligence, we need to cultivate public trust and responsible technology usage and practice as part of a proactive, comprehensive, holistic, and collective approach to risk management within the relevant contextual environment. The automotive industry supports NIST's clear intention that the AI RMF offer "approaches to minimize anticipated negative impacts of AI systems *and* identify opportunities to maximize positive impacts (emphasis in original)."

Incorporating the feedback of Auto Innovators and other stakeholders, the Second Draft includes several important changes compared to the Initial Draft. For example, the explicit inclusion of "pro-innovation" in the proposed attributes of the AI RMF acknowledges the

ongoing evolution in artificial intelligence products, services, and systems over time. The expansion of the AI RMF's intended audience to various artificial intelligence actors with their attendant artificial intelligence lifecycle activities reiterates the essentiality of "collective responsibility" for successful artificial intelligence risk management. Auto Innovators appreciates the Second Draft's inclusion of descriptions for each of the trustworthy artificial intelligence characteristics, their interrelationships, and their interdependencies; the reviews of how each characteristic may address potential artificial intelligence risks; and the guidance for addressing each characteristic. The additional details regarding the role of human factors in artificial intelligence risk management and oversight are also helpful.

Specific Comments:

As NIST continues its development of the AI RMF, Auto Innovators offers the following specific comments on the Second Draft:

- **Managing Bias:** NIST states that three major categories of artificial intelligence bias – systemic, computational, and human – must be considered and managed. Since artificial intelligence systems are comprised of both algorithms and data, it remains important to recognize that neither component is sufficient by itself to provide explainable or interpretable results. Balancing data sets to have output or target classes represented by the same number of input samples is important to present as many possibilities as possible. The AI RMF should encourage artificial intelligence actors, particularly in the design and development phases, to ensure training, validation, and holdout data sets are complete and then pair those data sets with algorithms to help facilitate bias-free outcomes. While training sets, in particular, are inputs that artificial intelligence actors can manage, it is only through the results of such pairing – the predictive outcomes – that success can be measured.

- **Safety:** NIST notes that transportation is a field that could inform artificial intelligence safety measures. To that end, Auto Innovators reiterates its previously stated position that the AI RMF should not group safety risks that do not pose a potential risk of serious injury or death with potential safety risks that do pose such risks. As the Second Draft recognizes, "AI systems are not inherently bad or risky, and it is often the contextual environment that determines whether or not negative impact will occur." Therefore, different types of safety risks may require tailored artificial intelligence risk management approaches based on context and the severity of potential risks presented. For example, "the ability to shut down or modify systems that deviate from intended or expected functionality" is not always possible in an automated vehicle or in some Advanced Driver Assist Systems ("ADAS"). Such a requirement could introduce unintended safety risks to the driver and other road users, particularly when the vehicle is in motion. Instead, the risk management best practice in this instance should be to reach a minimal risk condition.

- **Security:** NIST includes the traditional cybersecurity triad of confidentiality, integrity, and availability, through protection mechanisms that prevent unauthorized access and use, to describe secure artificial intelligence systems. Auto Innovators recognizes that

while these three attributes are often associated primarily with information technology ("IT"), they also apply to operational technology ("OT"). Nevertheless, we think it is important to specifically articulate OT-related security attributes such as safety, availability, and reliability in the discussion on secure and resilient artificial intelligence systems as well to communicate the applicability of the AI RMF to all artificial intelligence systems.

- **Transparency:** Auto Innovators agrees with NIST that data used to build artificial intelligence systems may not be "a true or appropriate representation of the context or intended use" of said systems. Sufficiently robust, diverse, and representative training data are critical to the safe, responsible, and trustworthy deployment of artificial intelligence, as well as to engender transparency with regards to the use of artificial intelligence systems. Transparency should also consider the human-machine interaction, *e.g.*, how a human operator or user will be notified when an artificial intelligence system detects a potential or actual adversarial attack. In addition to considerations related to training data and human-machine interactions, NIST should expand its review of transparency to include the importance of reproducibility given the AI RMF identifies concerns about opacity as an artificial intelligence-specific risk. Therefore, Auto Innovators asserts that NIST should account for these and other factors in its discussion on transparency and accountability.

Auto Innovators welcomes its ongoing collaboration with NIST on the development of the AI RMF. We appreciate NIST's continued commitment to this multistakeholder, consensus-driven process.

Sincerely,

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