U.S. Chamber of Commerce

1615 H Street, NW
Washington, DC 20062-2000
uschamber.com

September 29, 2022

National Institute of Standards and Technology
U.S. Department of Commerce
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

Re: Request for Information, National Institute of Standards and Technology; Artificial Intelligence Risk Management Framework Second Draft (August 18, 2022)

To Whom It May Concern:

The U.S. Chamber of Commerce's Technology Engagement Center ("C_TEC") appreciates the opportunity to submit feedback to the National Institute of Standards and Technology ("NIST") in response to its request for information about its "second draft" as well as its "Playbook" of an "Artificial Intelligence Risk Management Framework" (AI RMF).

C_TEC appreciates NIST's ongoing work to unite individuals and organizations associated with AI by creating a voluntary RMF. Also, we appreciate the opportunity to provide additional input to help further inform, refine, and guide the development of the AI RMF.

The Chamber has long recognized that "fostering public trust and trustworthiness in AI technologies is necessary to advance its responsible development, deployment, and use."[1] Furthermore, we agree with NIST's acknowledgment that "AI has led to a wide range of innovations with the potential to benefit nearly all aspects of society and our economy,"[2] and that "cultivating trust and communication about how to understand and manage AI Risks of AI system will create opportunities for innovation and realize the full potential for the technology."[3]

I. Following is our feedback on the questions posed regarding the "AI Risk Management Framework: Second Draft."

The ability for the RMF to be implemented successfully starts with ensuring that C-Suite level executives and others in the decision-making process provide the necessary resources and backing needed for effective execution. The RMF states that the primary audience includes those with "responsibilities to commission or fund an AI system and those who are part of the enterprise management structure governing the AI system lifecycle."[4] This shows the importance of having C-suite leaders and others in the chain of command

[1] https://www.uschamber.com/technology/us-chamber-releases-artificial-intelligence-principles
[2] https://www.nist.gov/system/files/documents/2022/08/18/AI_RMF_2nd_draft.pdf
[3] https://www.nist.gov/system/files/documents/2022/08/18/AI_RMF_2nd_draft.pdf
[4] https://www.nist.gov/system/files/documents/2022/08/18/AI_RMF_2nd_draft.pdf

informed and well-versed in the RMF. Therefore, we strongly recommend that NIST look to provide necessary resources and mechanisms to reach these groups as part of its publication and eventual promotion of the NIST AI RMF and Playbook. We would be happy to engage in conversations to help with this.

Furthermore, companies deploying artificial intelligence range from smaller, newer companies to more extensive, established ones. For this reason, we recommend that the RMF addresses the potential limitations that may accompany the ability of an organization, such as those companies that may be smaller and have fewer resources but are still utilizing the technology, to the ability to implement the RMF. We would appreciate input on how the RMF could be gradually phased throughout the AI lifecycle. We believe such guidance could help make incremental yet impactful progress toward robust AI governance. NIST notes that the voluntary AI RMF "can assist organizations, industries, and society in understanding and determining their acceptable levels of risk." We support organizations defining their own risk tolerance and establishing appropriate procedures according to their industries and AI use cases.

We encourage NIST to recognize explicitly in the AI RMF that there are many different AI transparency tools (e.g., system cards, model cards, etc.) and that these tools are currently in their infancy in terms of companies or organizations determining which approach for documentation is most useful (specific devices may be more appropriate in some cases than others and what is most useful may depend on the audience). Developers of AI systems should be encouraged to test different types of transparency tools in cooperation with AI deployers to ensure that AI systems are used as intended.

One of the critical benefits of AI is that it provides society with a tool that continues to help complement the workforce and provide efficiency and insights that have led to increased productivity and better outcomes. For this reason, it is essential that the RMF also consider this when it is framing risk. We recommend NIST address this by discussing the importance of the "human-baseline approach," which sets the bar against human legacy systems, not against vague AI-related risks without meaningful context. Furthermore, leaving out the human-baseline comparison within the framework could ultimately limit AI adoption.

Regarding NIST's question on "whether there are applications that may require future updates," C_TEC believes that Neuromorphic Computing and large language models will require iterative updates and more catered risk profiles.

Under the "*Manage"* section, NIST includes the sub-category of recognizing risks from third-party resources. We encourage NIST to continue working with stakeholders to develop further guidance on understanding risks from third-party resources, including vendors that contribute to comprehensive models. Furthermore, the AI RMF should explicitly acknowledge that AI risk management is a responsibility shared by developers, deployers, and users of AI systems.

"*Evaluators*" have been mentioned as essential stakeholders in the RMF. However, they are included within the scope of both categories – "AI Design" and "AI Deployment." This

creates confusion as it is unclear which AI Actor (developer or deployer) is responsible for the evaluation of the design of an AI application. Guidance needs to be provided, or principles need to be laid down defining the scope of obligations/responsibilities of evaluators and how the evaluation should be conducted.

Under the "*Operate & Monitor*" section, the framework has asked for continuous assessments of both intended and unintended impacts in AI applications. Asserting or assessing unintended consequences is a complicated task, and its scope has not been defined yet. We would ask NIST to provide further guidance or principles for AI Operators to assess the unintended impact, as this can prove to be a resource-intensive process with no concrete outcome.

Under the "*Transparent and Accountable* " section, the framework should make reasonable recommendations to reflect the extent to which transparency and accountability are feasible. Measures to enhance transparency and accountability should consider the impact on the implementing entity, including the level of staffing and monetary resources necessary, as well as the impact on innovation and market competitiveness.

Under the "*Explainability and interoperability*" section, the RMF has not clarified the critical points that need to be revealed to help a system achieve this objective. We would suggest providing guidance to ensure that only that information is disclosed to help understand the purpose and impact of an AI application instead of sharing such technical details/information that does not serve the purpose of an AI impact assessment.

Regarding the RMF's section on "*profiles*," we ask that NIST provide examples for entities' various AI approaches, including those that build and deploy their own models, use other vendors' models, or may utilize vendors for aspects of their model building processes. Furthermore, as AI continues to be implemented more widely, we encourage NIST to continue working with stakeholders to develop use-case profiles, including human resources and hiring, health benefits, public health services, synthetic drug development, lending & credit.

There are also different risk implications and considerations for AI that makes decisions and AI that supports human decision-making, which also varies by industry and uses case. We ask NIST to work with stakeholders to expand guidance considerations.

II. C_TEC looks to provide the following feedback on the questions posed regarding the "AI Risk Management Playbook."

First, the current Playbook is currently geared towards technologists. We highly encourage NIST to consider replicating the Playbook with different versions focused on different audiences—particularly one for legal experts and C-suite leaders, which will be critical to achieving the objectives of the governing section.

Second, the Playbook must provide clear recommendations for transparency and documentation targeted to address the suggested actions. Part of the Playbook would benefit from additional clarity. For example, in the Governance 1.1, the Playbook states that

"organizations can document…when auditing an AI system, has existing legislation or regulatory guidance been reviewed and documented." C_TEC believes NIST should clarify whether, or under what circumstances, auditing is intended. Furthermore, because of the current lack of standardization and robust technical standards around "auditing" we would encourage that you change the term to a more appropriate one such as "assessment." Additionally, in Governance 1.2, the Playbook states that "organizations can document… the characteristics of trustworthy AI are integrated into organizational policies and procedures." While C_TEC has long advocated for the development of trustworthy AI, we believe that NIST needs to provide further clarification on the section, as some information may not be appropriate to be printed and made available as it's not firmly tied to concrete risk-management goals.

Conclusion

C_TEC appreciates NIST's ongoing efforts to improve the risk management framework for individuals, organizations, and AI-associated by creating a voluntary RMF. This effort holds significant promise in creating an innovative environment for Artificial Intelligence, which is why we urge NIST to continue working closely with stakeholders to ensure innovation is not stifled. We thank you for considering these comments and would be happy to discuss any of these issues further.

Sincerely,

Director
Chamber Technology Engagement Center
U.S. Chamber of Commerce