U.S. Chamber of Commerce

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

April 29, 2022

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

Re: Artificial Intelligence Risk Management Framework Initial Draft

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 on its "initial draft" of an "Artificial Intelligence Risk Management Framework."

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

1. *Whether the AI RMF appropriately covers and addresses AI risks, including with the right level of specificity for various use cases.*

C_TEC strongly agrees with the principle that the "AI RMF provides the opportunity for organizations to specifically define their risk thresholds and then manage those risks within their tolerances.[4]"

However, the AI RMF does not fully cover specificity for various use cases and could encourage further specificity in the soon-to-be-published companion document, as there is no mechanism for how to detangle impact. Furthermore, the current draft's focus on the characteristics of a system (technical, sociotechnical, guiding principles) can obscure the specific risks that a system does or does not pose. Without practical guidance, it is unclear whether this approach works out.

[1] https://www.nist.gov/system/files/documents/2022/03/17/AI-RMF-1stdraft.pdf
[2] https://www.nist.gov/system/files/documents/2022/03/17/AI-RMF-1stdraft.pdf
[3] https://www.uschamber.com/technology/us-chamber-releases-artificial-intelligence-principles
[4] https://www.nist.gov/system/files/documents/2022/03/17/AI-RMF-1stdraft.pdf

Within section five, AI risk and trustworthiness, the AI RMF should update the technical characteristic term to "predictive accuracy," which would allow for the appropriateness of metrics with the model to be considered. We also recommend evaluating the use of "accuracy" throughout the document and considering the change to "predictive accuracy," correctness, or usefulness depending on the intended outcome. This will ensure clarity between all stakeholders.

Finally, there should be a more stronger connection between the NIST Cybersecurity Framework and the NIST Privacy Framework. As you have indicated in the initial draft, the AI RMF "aims to fill the gaps related specifically to AI[5]" and not related to "cyber security" and "privacy." For this reason, we believe a better connection on how the cybersecurity and privacy frameworks fit into the AI Risk Management Framework is necessary.

2. *Whether the AI RMF is flexible enough to serve as a continuing resource considering evolving technology and standards landscape.*

C_TEC strongly supports the Framework's flexibility and asks NIST to continue to allow flexibility to encourage collaboration and use of all relevant information as AI developments continue. We urge NIST to ensure that the draft does not stray too far and make policy judgments, which would impact how the RMF can be adopted and used by organizations as the policies and regulations around AI continue to develop. The Technical Characteristics, for instance, generally are policy considerations. As Figure 4 shows, the characteristics proposed by NIST do not align with existing policy instruments and regulatory proposals. The AI RMF should not seek to replicate policy and regulatory standards but instead, be sufficiently flexible so that organizations can plug the standards that develop through them into the RMF to conduct a risk management analysis.

3. *Whether the AI RMF enables decisions about how an organization can increase understanding of, communication about, and efforts to manage AI risks.*

C_TEC appreciates NIST's understanding that "small, medium-sized organizations face different challenges in implementing the AI RMF than large organizations[6]." While the AI RMF acknowledges significant differences between the company's size and its challenges, the AI RMF should explicitly acknowledge that AI risk management is a responsibility shared by developers, deployers, and users of AI systems, and NIST should clarify this throughout the document.

In addition, C_TEC would like to highlight concerns that the draft RMF may seek to include too broad an audience. While we agree that there are broad internal and external stakeholders relating to AI systems, the audience for (i.e., the users of) the RMF are the internal stakeholders that the RMF identifies as the "primary adopters" of AI, and the internal operators and evaluators. This aligns with established

[5] https://www.nist.gov/system/files/documents/2022/03/17/AI-RMF-1stdraft.pdf
[6] https://www.nist.gov/system/files/documents/2022/03/17/AI-RMF-1stdraft.pdf

risk management practices. For this reason, we ask for further clarification about the role that each stakeholder group should play in the risk management in future complementary resources.

4. *Whether the functions, categories, and subcategories are complete, appropriate, and clearly stated.*

Regarding the Map category, C_TEC strongly supports these categories and subcategories. We recommend that NIST consider these categories in relation to AI developers, deployers, and end-users. However, the NIST documentation assumes that all components are AI and used as standalone. Typically, solutions also have non-AI components that work in conjunction with AI components to create the final AI decision. We recommend NIST work with stakeholders to develop recommendations for evaluating components. The categories and subcategories help create a consistent baseline of recommendations for evaluating AI across the lifecycle.

Regarding the Measure category, under subcategory one, we recommend removing "accuracy," as this is misleading and could perpetuate problematic algorithms. Instead, we recommend replacing this "metric approved for use for the algorithm." When a developer chooses a metric, they should be able to defend it. Under subcategory two, we would like to highlight that risks are not the same for every model. Each model is built independently of the others. We recommend clarifying text to state that model risk should be evaluated as standalone.

Regarding the Manage category, under subcategory one recommendations, we would encourage both impact and scale to be defined. Furthermore, under subcategory two, we support disengaging or deactivating AI mechanisms that demonstrate outcomes inconsistent with the intended use. We recommend expanding this subcategory to include "create a contingency plan for the deactivation of the AI," as this is necessary to ensure there is no halt in services.

Regarding the Govern category, C_TEC recommends NIST continue stakeholder discussions on how these categories and subcategories tie to outcomes or would be demonstrated. Furthermore, we believe trade associations should be involved in processes for subcategory five.

C_TEC would like to clarify that making clear expectations and processes across a company will help to facilitate consistent standards and communication around identifying and mitigating AI risks. We support the creation and use of AI checklists and sound processes created by each organization and in alignment with industry requirements. We are setting clear policies and procedures for relevant algorithms and models, such as high-risk AI as defined by the company.

While we support sharing relevant details regarding the creation and use of algorithms, we also recommend that NIST and AI-related entities consider privacy, security, and intellectual property (IP) concerns. Considerations must be taken into account to prevent unintended consequences such as breaches or algorithm corruption by external parties.

5. *Whether the AI RMF is in alignment with or leverages other frameworks and standards such as those developed or being developed by IEEE or ISO/IEC SC42.*

C_TEC first appreciates NIST's coordination with "Singapore's industry aimed Minimum Viable Product for Testing Framework." C_TEC has continuously pushed for any work on this important issue to "be mindful of existing rules and regulations.[7]" As "governments should avoid creating a patchwork of AI policies at the subnational level and should coordinate across governments to advance sound and interoperable practices.[8]" To that end, it would be beneficial for NIST to explicitly detail how the RMF, once published, relates to ISO/IEC DIS 23894 AI Risk Management and IEEE 7000-2021 and ISO/IEC 5338 (which pertain to AI lifecycles and are already consistent with ISO/IEC/IEEE 12207 and 15288). The alignment of risk management frameworks internationally is key for businesses operating globally.

6. *Whether the AI RMF is in alignment with existing practices and broader risk management practices.*

A deep understanding is necessary to understand existing practices in each specific industry. C_TEC would like to thank NIST for its efforts to engage stakeholders throughout the process through workshops. NIST should continue leveraging public workshops and other feedback opportunities to support industry-specific groups in discussing best management practices.

7. *What might be missing from the AI RMF?*

C_TEC believes that it should be more explicit regarding allocating responsibilities to general-purpose tools that users develop into AI systems. The text should mention that when a user develops a general-purpose tool into an AI system for intended high-risk use, it is up to the user to comply with the requirements for high-risk systems.

A decommissioning phase is important for the AI lifecycle. We would encourage NIST to add "decommissioning" to the figure and offer baseline recommendations for consideration when removing AI from use.

C_TEC notices that the NIST RMF references "auditors" and "auditing." We believe that a disclaimer within the AI RMF is necessary to ensure that the RMF is law and regulation agnostic. We believe that the AI RMF must state deliberately that

[7] https://www.uschamber.com/technology/us-chamber-releases-artificial-intelligence-principles
[8] https://www.uschamber.com/technology/us-chamber-releases-artificial-intelligence-principles

companies may carry out internal audits of their AI systems and that "auditing" does not necessarily mean "external audit." We also believe it's important to highlight that audits are an evolving set of tools and vary in quality because consensus-based technical standards are still in development.

8. *Whether the soon-to-be-published draft companion document citing AI risk management practices is useful as a complementary resource and what practices or standards should be added.*

C_TEC recommends that AI RMF address the differences in responsibilities. We also believe it is important that the Practice Guidance that NIST is developing to accompany the AI RMF provides examples that demonstrate what these different responsibilities mean for AI providers, deployers, and users when implementing the Framework.

Conclusion:

C_TEC appreciates NIST's ongoing efforts to improve AI risk management, including by creating the voluntary Risk Management Framework, which has significant promise in creating an innovative environment for Artificial Intelligence, which is why we are eager to continue working with NIST to ensure that the AI RMF continues to support innovation and strengthen public trust in AI. We thank you for your consideration of these comments and would be happy to discuss any of these topics further.

Sincerely,

Michael Richards
Policy Director
Chamber Technology Engagement Center
U.S. Chamber of Commerce