U.S. Chamber of Commerce

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

September 9, 2024

The Honorable Dr. Laurie Locascio
Director
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

Re: NIST AI 800-1 Initial Public Draft, Managing Misuse Risk for Dual-Use Foundation Models.

Dear Director Locascio,

The U.S. Chamber of Commerce ("Chamber") appreciates the opportunity to provide comment to the National Institute of Standards and Technology ("NIST") request for feedback on the "initial public draft of the Managing Misuse Risk for Dual-Use Foundation Models" ("draft guidelines"). The Chamber has long been a staunch advocate of NIST's work in Artificial Intelligence ("AI") governance which include developing the Risk Management Framework (RMF), as well as corresponding efforts to provide critical resources to those fostering an ecosystem of responsible AI development and use.

The Chamber believes that such an ecosystem is important for the development and deployment of AI and that it is only possible through American leadership. The Chamber has stated that "The U.S. and its allies should be the ones developing and advancing ethical Artificial Intelligence technologies that align with our common democratic goals and values. Any effort to pause further innovation will leave us unable to advance these essential values as others move forward without us.[1]" For this reason, we believe it's vital that draft guidelines formulated in a way that ensures continued U.S. leadership. The Chamber offers feedback on the initial draft of draft guidelines.

I. Clarification of Draft Guidelines Needed

The Chamber believes that NIST needs to provide further clarification on the role of the draft guidelines. Executive Order 14110, the Safe, Secure, and Trustworthy

[1] Michael Richards. "The U.S. Should Lead not Pause AI." U.S Chamber of Commerce, 4-6-2024, https://www.uschamber.com/technology/artificial-intelligence/the-u-s-should-lead-not-pause-ai

Development of Artificial Intelligence, requires the establishment of "guidelines and best practices, to promote consensus industry standards,[2]" as well as to "establish appropriate guidelines (except for AI used as a component of a national security system), including appropriate procedures and processes, to enable developers of AI, especially of dual-use foundation models, to conduct AI red-teaming tests to enable deployment of safe, secure, and trustworthy systems." However, the draft guidance does not meet either of these requirements, as the initial guidance does not utilize "consensus industry standards" such as NIST SP 800-37, ISO 31000, NIST AI RMF, and SSDF or provides specific guidance on how to "conduct AI red-teaming test." Therefore, we would ask NIST to clarify the relationship between the draft guidance and the guidance required under EO 14110.

II. Entire AI Life Cycle Approach

The Chamber strongly supports NIST's rationale within the NIST AI 100-1 that "AI risks should not be considered in isolation. Different AI actors have different responsibilities and awareness depending on their roles in the lifecycle." The Chamber has long highlighted the importance of an encompassing approach to risk mitigation where roles and responsibilities differ between different AI actors. Sadly, the draft guidance as drafted, focuses entirely on the foundation model developers while leaving out essential actors throughout the AI life cycle. For this reason, the Chamber is concerned that the draft guidance puts unrealistic responsibilities on foundation model developers while not considering others' duties and responsibilities throughout the AI lifecycle. For this reason, we believe it's essential for the document to provide an entire AI Life Cycle approach to AI governance and not just for developers as NIST advocated previously. We would further encourage NIST to clarify roles and responsibilities for those throughout the AI life cycle to fine-tuning a model.

III. Need for Harmonization:

The Chamber believes harmonization of terms and concepts is essential in developing a thriving ecosphere. For this reason, the Chamber has concerns with NIST AI 800-1 as it does not look to harmonize with the National Telecommunications and Information Administration (NTIA) recent released report on "Dual Use Foundation

[2] President Biden, EO 14110, Safe, Secure, and Trustworthy Development of Artificial Intelligence, October 30th, 2024, FR Vol. 88 No. 210, https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/

Models with Widely Available Model Weights," which calls for a marginal risk standard. This standard is essential in not inadvertently stopping innovation, as it highlights the importance of addressing "risks that are unique to the deployment of dual-use foundation models with widely available model weights relative to risks from other existing technologies[3]." We are concerned that not utilizing the marginal risk standard, which has also been used by other AI Safety Institutes and U.S. Government agencies, will lead to unnecessary fragmentation.

IV. Risk-based approach:

The Chamber has long highlighted the importance of a risk-based approach to AI governance. In a previous response to NIST, the Chamber further highlighted the importance of taking a "human-baseline approach" to set "the bar against human legacy systems, not against vague AI-related risks without meaningful context.[4]" This ensures that the technology is not wrongfully restricted or held to a higher standard than other alternative technologies, which is further emphasized in our response above on the need for harmonization. For this reason, the Chamber would like to continue to echo the importance of a risk-based approach that is "specific, narrowly tailored to appropriate use cases, and weighed against the economic and social benefits forfeited by its enactment.[5]"

V. Implications for Open-Source Ecosystem:

The Chamber is concerned with draft guidance impact on the open-source AI ecosystem. The Chamber sees open-source technology as vital for the continued development and innovation of the technology. In our recent response to NTIA's RFI on dual-use technology, the Chamber highlighted that "Open-source technology allows developers to build, create, and innovate in various areas that will drive future economic growth. We already see innovation in marketing, communication, cybersecurity, and medicine, among other fields. Access model weights can be a boon to driving safety and security improvements to artificial intelligence by providing

---

[3] National Telecommunications and Information Administration, *Dual-Use Foundation Models with Widely Available Model Weights Report*, July 2024, https://www.ntia.gov/sites/default/files/publications/ntia-ai-open-model-report.pdf
[4]U.S. Chamber of Commerce, Re: Request for Information, National Institute of Standards and Technology; Artificial Intelligence Risk Management Framework Second Draft (August 18, 2022), September 29, 2022, https://www.nist.gov/system/files/documents/2022/11/16/U.S.%20Chamber%20of%20Commerce_Technology%20Engagement%20Center%20%28C_TEC%29.pdf
[5]U.S. Chamber of Commerce, *U.S. Chamber Releases Artificial Intelligence Principles*, September 29th, 2019, https://www.uschamber.com/technology/us-chamber-releases-artificial-intelligence-principles

greater transparency, allowing flaws to be quickly identified and patched.[6]" Sadly, the criteria set out in the draft guidance could stifle deployers' access to state-of-the-art open-source generative AI, which could stifle innovation and limit market access. We recommend that NIST conduct a crosswalk analysis of its draft guidance document and the NTIA final report on dual-use foundation models with open model weights to establish consistency in its approach to an open-source AI ecosystem.

VI. Transparency:

The Chamber supports the call for organizations to document best practices to provide "transparency" about potential misuse risks. However, we believe clarification is necessary that the guidance is not asking for these documents to be made public, as doing so could have significant safety and security implications by requiring organizations to share sensitive information about how they address and manage misuse risk.

Conclusion:

The Chamber would like once again to highlight our appreciation of NIST and its work. We look forward to working with NIST and other stakeholders on our concerns outlined in this letter and to advance U.S. leadership on a responsible AI ecosystem.

Sincerely,

Michael Richards

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

[6] U.S. Chamber of Commerce, U.S. Chamber Files Comments to NTIA on Dual Use Foundation Open Model, March 27th, 2024, https://americaninnovators.com/advocacy/u-s-chamber-files-comments-to-ntia-on-dual-used-foundation-open-models/