C_TEC

U.S. Chamber of Commerce
Technology Engagement Center

MICHAEL RICHARDS
Director

1615 H STREET, NW
WASHINGTON, DC 20062-2000
(202) 463-5518
MRichards@uschamber.com

August 25, 2021

National Institute of Standards and Technology
U.S. Department of Commerce
Gaithersburg, MD 20899

**Re: Trust and Artificial Intelligence (Draft NISTIR 8332)**

To Whom It May Concern:

The U.S. Chamber of Commerce's Technology Engagement Center ("C_TEC") appreciates the opportunity to submit comment to the National Institute of Standards and Technology's ("NIST") draft publication on "Trust and Artificial Intelligence." C_TEC appreciates NIST's ongoing efforts to advance understanding on AI and convene diverse sets of stakeholders to ensure U.S. leadership in trustworthy AI.

The draft publication addresses the importance of user trust in the development of AI systems and proposes an approach to assess a user's level of trust in an AI system. C_TEC agrees that understanding user trust in AI systems is desirable and helpful. However, the proposed approach also raises several questions, which are outlined below. Furthermore, C_TEC provides responses to several of the questions contained in the draft publication.

First, the draft publication noted the difference between technical trustworthiness and user trust, and that this draft publication focuses on the latter. Moreover, in discussing the nine characteristics for AI system trustworthiness, the draft publication states, while these characteristics are necessary from a technical perspective, they do not automatically equate to user trust. The draft publication explains "Ultimately, the user's perception of available technical information is what contributes to their trust." Given the observation, C_TEC seeks clarification from NIST on how it envisions the role of user trust regarding NIST's ongoing efforts on trustworthy AI statutory requirements such as the Section 5301 of the Fiscal Year 2021 National Defense Authorization Act.

Second, the draft publication does not consider the critical role of consumer trust with brands and the importance to businesses of maintaining that trust. Broadly, brands enable consumers and customers to not just develop familiarity with their particular business, but also build trust in their products. According to Edelman's Trust Barometer Special Report, 70% of consumers believe that brand trust is more important today than previously and 75% of consumers with high brand trust noted that they will purchase the brand even if a less costly alternative exists. However, despite the clear intersection between brands and trust, the draft publication does not consider the role of brands, and instead relies on utilizing a mathematical approach. Many AI applications are consumer-oriented and customer-facing. Consequently, the brand of a developer or deployer will likely be a crucial factor in whether a consumer or customer chooses to purchase or interact with the AI application. As NIST continues its work on AI and user trust, C_TEC urges NIST to consider the role of brands to establish and maintain user trust in AI applications.

Third, C_TEC notes that the draft publication does not outline a definition of AI in the context of AI and user trust. While there is no universal definition of AI, there are several definitions which could be applicable to this draft publication. These include the statutory definitions in the FY 2019 National Defense Authorization Act and Section of the FY21 National Defense Authorization Act, and the several technical definitions of AI included in the Appendix I of NIST's "*U.S. Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools*." While C_TEC understands that NIST may not have coalesced around a single definition, it would be beneficial for NIST to note which definition is being utilized for a particular draft publication. Furthermore, C_TEC emphasizes the need for that definition to be applicable across all industries and AI activities. Absent such clarification, the draft publication could be interpreted as having a broader scope and application than intended and might inadvertently conflict with other NIST initiatives.

Further, the paper seems to be focusing on machine learning, e.g. "No longer are we asking automation to do our tasks—we are asking it to do tasks that we can't. Asking the AI to perform the same task on two different occasions may result in two different answers as the AI has "learned" in the time between the two requests. AI has the ability to alter its own programming in ways that even those who build AI systems can't always predict". Not all AI meets these criteria. It would be helpful to clearly specify if the paper is focused primarily on machine learning, rather than other types of AI which do not 'learn'.

Fourth, C_TEC recommends consideration of how AI systems arrive at an answer when determining user trust potential (UTP). This could include but is not limited to trustworthy AI principles of explainability, transparency, reliability, and fairness. Also, C_TEC notes that if an AI system uses more personal, sensitive, and granular information, this may impact user trust potential and require additional trust-building. Furthermore, the draft publication primarily focuses on end recipients or users of an AI system, specifically on non-enterprise consumers. Given this context, NIST may also need to contemplate trust from other types of users, including internal users and enterprise customers. For both of these, the type of user and their level of interaction with the AI system may have different trust needs. Internal users would include users within a business or other entity that leverages AI for internal functions, such as back-office functions like payroll or invoicing. Enterprise customers may leverage AI services to help them best achieve their needs. In some circumstances, they may be willing to replace "trust" with certifications and audit reports produced by third-party firms (e.g. certifications and reports that provide these customers with defensible evidence that they've performed their due diligence on the "trustworthiness" of a service).

Fifth and finally, C_TEC offers the following considerations for user experience (UX), pertinence, and sufficiency regarding AI and user trust. First, UX) metrics might consider factors such as overall satisfaction, consumer effort necessary to get to their intended action or answer, and issue resolution, which may additionally influence user trust. There is a strong correlation that high UX relates to high user trust in products and services. Overall satisfaction is foundational for building an individual's confidence in a service or tool. Under the discussion of pertinence, NIST includes objectivity as a characteristic of AI system trustworthiness. We ask NIST to clarify if objectivity is intended as a proxy for transparency as a characteristic to evaluate pertinence generally, or if objectivity is intended to capture a different metric. C_TEC also recommends NIST consider timeliness as a measure of pertinence. An example includes sending a consumer a confirmation shortly after an online purchase, so they are assured their purchase is secure, safe, and received. Additionally, under sufficiency, C_TEC recommends NIST consider the variations of human oversight and intervention across AI technologies in the guidance. Differing levels of human-AI interaction may assist or alter overall trust building, including how a user considers each characteristic and contextual risk.

NIST has a critical role to play in convening stakeholders to advance trustworthy AI. The Chamber continues to support NIST's efforts on this topic and again appreciates the opportunity to submit comments on this draft publication. We look forward to collaborating with NIST on the next steps for this publication and on future AI-related activities.

Sincerely,

Michael Richards

Michael Richards
Director, Policy
Chamber Technology Engagement Center