February 2, 2024

Via regulations.gov
National Institute of Standards and Technology
100 Bureau Drive (Mail Stop 8900)
Gaithersburg, MD 20899-2000

Re: AI E.O. RFI Comments

CTIA[1] appreciates the opportunity to provide input to the National Institute of Standards and Technology ("NIST") on its Request for Information regarding assignments under sections 4.1, 4.5, and 11 of the Executive Order on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence ("AI").[2] NIST's commitment to meaningful collaboration with stakeholders – including in its foundational development of the AI Risk Management Framework ("AI RMF") and numerous directives under the AI E.O. – will help ensure the success of this guidance across the broad and diverse AI ecosystem. CTIA is proud to work with NIST in this effort.

As NIST undertakes these initial efforts to establish guidelines and best practices for trustworthy AI development and deployment and to advance responsible global technical standards for AI development, it should carefully consider how to tailor obligations to entities in the best position to identify and manage particular risks. To do so, NIST's standards and guidelines should:

1. Consider what responsibilities may be appropriate for *all* versus *particular* stakeholders in the value chain;
2. Avoid assumptions regarding risk that do not adequately reflect the AI ecosystem;
3. Ensure that AI deployers can rely on full and transparent information from AI developers in order to adequately manage risk; and
4. Align to globally recognized definitions to facilitate a harmonized, risk-based global approach.

We elaborate on these recommendations below.

I. NIST Should Consider What Responsibilities May Be Appropriate for All Versus Particular Stakeholders in the Value Chain.

In developing the standards and guidelines directed under E.O. 14110, NIST may identify responsibilities that all stakeholders in the AI value chain should share. For example, entities with a role in bringing AI-supported products to market – from the original model developer to AI systems integrators to

[1] CTIA —The Wireless Association® ("CTIA") (www.ctia.org) represents the U.S. wireless communications industry and the companies throughout the mobile ecosystem that enable Americans to lead a 21st century connected life. The association's members include wireless providers, device manufacturers, suppliers as well as apps and content companies. CTIA vigorously advocates at all levels of government for policies that foster continued wireless innovation and investment. The association also coordinates the industry's voluntary best practices, hosts educational events that promote the wireless industry and co-produces the industry's leading wireless tradeshow. CTIA was founded in 1984 and is based in Washington, D.C.

[2] *Request for Information (RFI) Related to NIST's Assignments Under Sections 4.1, 4.5 and 11 of the Executive Order Concerning Artificial Intelligence*, Request for Information, 88 FR 88368 (rel. Dec. 21, 2023) ("RFI"); Exec. Order No. 14110, 88 Fed. Reg. 75191 (2023) ("AI E.O.").

deployers – should be transparent regarding risk decisions, data use and protections, and intended or planned use cases for the AI system. NIST can facilitate more consistent communication across the value chain by clarifying expectations regarding testing – for both developers and deployers – including what type of testing entities should perform and how often it should be conducted.

At the same time, entities performing a particular role in the value chain may have unique obligations based on their insight and ability to manage risks related to that role. For example, AI developers – who design, code, or produce AI systems – should be expected to follow responsible practices, e.g., for acquiring, protecting, and using training data; conducting design evaluations; documenting and sharing pertinent risk information such as: (i) the intended purpose of the AI system; (ii) known limitations of the AI system; (iii) known, likely, and specific high risks that could occur and steps taken to mitigate those risks; (iv) data used to train the AI system; and (v) how the AI system was evaluated prior to sale or licensing. From a distinct vantage point, AI deployers – who use AI systems for a particular purpose – should conduct impact assessments of high-risk AI systems and document pertinent risk information, e.g., (i) the intended purpose of the AI system; (ii) transparency measures, including notices to impacted individuals regarding the AI system's use; (iii) how the AI system is evaluated, if applicable; (iv) known, likely, and specific high risks that could occur and steps taken to mitigate those risks; and (v) steps taken to monitor the AI system post-deployment and other user safeguards, if applicable.

NIST should also consider how obligations may shift as roles in the AI value chain become more diverse and complex – beyond simply the "AI developer," "AI deployer," and "end user" both before and after deployment. As stakeholders have already noted, a single organization may act as both a developer and a deployer (e.g., in the case of a cybersecurity company that develops AI software that monitors network traffic and customer transactions and then uses it on its own platform).[3] But we are also likely to see instances where an "AI deployer" may tailor an AI system designed and developed by a third party in order to meet bespoke needs. There may also be organizations that act as "integrators" that take AI systems developed by one or more organizations and build products for other companies to deploy. Accordingly, NIST should consider a sliding scale of responsibilities based on the actual functions an organization performs in the AI value chain.

II. Standards and Guidelines Should Avoid Assumptions Regarding Risk that Do Not Adequately Reflect the AI Ecosystem.

As NIST works with stakeholders to shape a risk-based approach to AI standards and guidelines, it should ensure this approach reflects the real and evolving landscape of AI-related risks and avoids overbroad generalizations that may not accurately reflect the diverse use cases to which this guidance will apply. For example, some stakeholders have suggested that "[r]egulators should focus their oversight on operators, the parties responsible for deploying algorithms, rather than developers, because operators make the most important decisions about how their algorithms impact society."[4] However, just because an AI deployer has direct contact with consumers does not mean that deployer can inherently manage all risk related to the AI system most effectively. Developers are likely to make many decisions (e.g., regarding training data, data security, and privacy controls) that will significantly impact end users

[3] *See e.g.,* BSA | The Software Alliance, *AI Developers and Deployers: An Important Distinction*, https://www.bsa.org/files/policy-filings/03162023aidevdep.pdf (last visited Jan. 31, 2024).
[4] Center for Data Innovation, Comments on NTIA AI Accountability Policy Request for Comment (June 12, 2023), https://www2.datainnovation.org/2023-ntia-comments-ai-accountability.pdf.

regardless of how a deployer uses the model. Rather than focusing risk management obligations on one set of stakeholders, AI standards and guidelines should reflect the shared responsibility of managing and communicating risk across the AI value chain as a whole.

III. Deployers Must Be Able to Rely on Full and Transparent Information from Developers in Order to Adequately Manage Risk.

As part of their shared responsibility in managing risk across the AI value chain, deployers should be expected to assess, manage, and transparently communicate the unique risks that may be associated with their particular use cases. To do so effectively, deployers need complete information from developers regarding the risk decisions they have made and passed along through their products. Developers should be expected to relay, for example, model cards and system cards that explain intended use, what data the model was trained on, and any other information that may bear on subsequent risk decisions made by integrators, deployers, and end users. When using an AI system, deployers must be able to rely on the completeness and accuracy of that information and integrate it into their own communication to end users and other relevant stakeholders.

IV. NIST's Guidance Should Align to Globally Recognized Definitions to Facilitate a Harmonized, Risk-Based Global Approach.

NIST should likewise champion these risk management goals in international discussions. To advance adoption of responsible global technical standards for AI development, NIST should consider grounding its work with internationally recognized definitions. For example, last year the Organization for Economic Co-operation and Development (OECD) adopted an updated definition of "AI system" to facilitate alignment across the international AI governance landscape.[5] Integrating this definition can help translate NIST's guidance for greater impact in the global AI value chain.

***

CTIA and its member companies appreciate the opportunity to provide this initial input and look forward to continued collaboration with NIST on the important work ahead.

Respectfully submitted,

/s/ David Valdez
David Valdez
Vice President, Privacy and Cybersecurity

Justin C. Perkins
Director, Cybersecurity and Policy
CTIA
1400 16th Street, NW, Suite 600
Washington, DC 20036
202-736-3200
www.ctia.org

[5] *See* Stuart Russell, Karine Perset, Marko Grobelnik, *Updates to the OECD's definition of an AI system explained*, OECD.AI (Nov. 29, 2023), Updates to the OECD's definition of an AI system explained - OECD.AI.