September 15, 2021

National Institute of Standards and Technology (NIST)
100 Bureau Drive, Gaithersburg, MD 20899
Via e-mail: AIframework@nist.gov

Re: Artificial Intelligence Risk Management Framework **(Docket No. 210726-0151; Document No. 2021-16176); Comments of CTIA**

To Whom It May Concern:

CTIA[1] appreciates the opportunity to comment on NIST's Artificial Intelligence ("AI") Risk Management Framework ("AI Framework") in response to the July 29, 2021 Request for Information ("RFI").[2] Congress directed NIST to develop—in collaboration with the public and private sector—"a voluntary risk management framework for trustworthy artificial intelligence systems."[3] Given the potential impact of NIST's work on technology, innovation, procurement, and beyond, broad public input will be critical for NIST to fulfill this statutory obligation. Considering its extensive work developing the Cybersecurity Framework[4] and the Privacy Framework,[5] NIST is the correct entity to take on this task.

Ultimately, in developing the AI Framework, NIST should be guided by the same principles that guided both the Cybersecurity and Privacy Frameworks, including making certain that the AI Framework is risk-based, scalable, and not overly prescriptive, and that the AI Framework is not "one-size-fits-all." These attributes—along with others highlighted in the RFI—are critical to ensuring that the AI Framework can support industry's efforts to manage AI risks while reaping its enormous benefits.

The AI Framework Should Facilitate Innovative and Beneficial Uses of AI, Building on Existing Practices.

AI promises a multitude of benefits, including network and consumer security advancements that contribute to fraud detection and prevention and real-time detection of network threats. For the wireless sector, AI is a promising tool for next-generation network operations.[6] A recent report from the Federal Communications Commission's ("FCC") industry-led Technological Advisory Council ("TAC") illustrates that AI has broad applicability across the telecommunications industry.[7] Major wireless providers and device manufacturers are using data and machine learning ("ML"), and their research and investments are leading the way on AI in everything from network design to customer service to application development. The benefits of this work are plain to see:

- AI and ML have generally played a key role in developments in Open Radio Access Networks.[8]
- AT&T explains that "AI and machine learning are woven into customer interactions, [its] software-defined network and [its] next-gen technologies[,]" and has developed its own AI Guiding Principles.[9]
- T-Mobile has been working with Ericsson to use AI to improve customer experience and order fulfillment,[10] as well as with Amazon Web Services to use machine learning to improve customer service.[11]
- Verizon has teamed with IBM on network design and enterprise services,[12] and is using AI to speed the deployment of its 5G network.[13]

These are just a few examples, but AI use cases in telecommunications alone demonstrate enormous complexity and diversity in application, and require care from NIST—indeed any government or third party—in developing AI governance frameworks.

CTIA urges NIST to keep AI's benefits top of mind to ensure that the AI Framework becomes a tool that will support and not stifle AI applications. In the RFI, NIST rightly recognizes the vast potential of AI, beginning with a discussion of how AI "is rapidly transforming our world" and generating "a wide range of innovations" that "are benefitting many parts of society and economy from commerce and healthcare to transportation and cybersecurity."[14] To build from this, and in order to best facilitate and promote AI, NIST should look to prior, industry-led AI work in developing the AI Framework. NIST should draw upon industry-led AI research, reports, and assessments—like the TAC AI Report. In doing so, NIST will be able to better understand and capture the vast benefits of AI across sectors, and thus allow further beneficial and innovative uses of AI to flourish.

NIST should also provide an unambiguous definition of what the Framework encompasses as "AI," in addition to providing more specific definitions of AI-related terms to help enable meaningful dialogue and understanding of AI within organizations, across sectors, and with policymakers. Already in the RFI, NIST explains that one of the Framework's attributes should be to "provide definitions and characterizations for aspects of AI risk and trustworthiness that are common and relevant across all sectors."[15] A clear definition of what AI encompasses within the Framework would avoid uncertainty and fragmentation in approaches and an uneven playing field. And clear definitions will support the open communication and sharing of knowledge between policymakers, industry, and academia.

NIST Should Model Its AI Work on the Development Processes and Principles for the Cybersecurity and Privacy Frameworks.

First, transparent and broad collaboration will yield the most usable document for widespread adoption. As illustrated with the Cybersecurity and Privacy Frameworks, collaboration is a cornerstone of NIST's success.[16] Congress recognized the value of this approach by requiring that the AI Framework be developed "in collaboration with other public and private sector organizations."[17] Already, NIST has been convening stakeholders and considering issues of trustworthy AI and AI risk management. CTIA is pleased that the RFI demonstrates NIST's ongoing commitment to meaningful collaboration on its AI efforts.[18] CTIA and its members look forward to engaging in this process and encourage NIST to be transparent in its planning. Doing so will encourage public participation and stakeholder dialogue, and it will help ensure that the AI Framework draws from ongoing work from industry and others.

Second, the AI Framework should eschew a one-size-fits-all approach. With the Cybersecurity and Privacy Frameworks,[19] NIST soundly rejected a one-size-fits-all approach, which it should also do here. In the RFI, NIST identifies several key attributes that the AI Framework should have, which CTIA supports.[20] In particular, CTIA emphasizes that a risk-based, scalable, flexible, and proportionate approach will be paramount to the AI Framework's success. AI has a multitude of diverse applications, making it ill-suited for a prescriptive, one-size-fits-all approach. The RFI appears to rightly acknowledge this.[21] Going forward, different applications and uses of AI will necessitate different governance approaches. NIST should account for this by developing a model that is scalable and flexible, so that users can apply it based on their own assessment of risk.

Third, the AI Framework should strive to help organizations identify and mitigate—not eliminate—risk. It is critical that the AI Framework make clear that different AI applications will raise different risks. For example, many promising uses of AI relate to the improvement of business processes and

operations, which present a low risk of harm to individuals.[22] NIST should develop the AI Framework as a value-agnostic tool for organizations to identify and assess the unique risk that any given AI application may raise for an organization, recognizing that risks and mitigations will vary widely.

To this end, the AI Framework should focus on potential risk identification and mitigation,[23] not the elimination of risk. The pursuit of trustworthy AI is not a matter of eliminating *any* risk; it is impossible, for example, to entirely eliminate risk of error or risks related to privacy or security. Rather, the goal of NIST's efforts should be to help organizations identify and address risks. Unfortunately, it appears that the RFI has set the unrealistic expectation that AI risk can be avoided, defining "responding" to AI risk to mean "***[a]voiding***, mitigating, sharing, transferring, or accepting risk."[24] NIST should be careful not to apply this concept of risk avoidance to its work moving forward, as avoiding risk is an infeasible metric for any technology, system, or program, and AI is no exception. The AI Framework should focus on responses that aim to mitigate AI risks, and the reasonable design, oversight, and monitoring that can achieve robust risk mitigation. Imposing a technically infeasible metric like "avoiding" risk or being free of errors will stymie, if not entirely quash, AI innovation.

Fourth, the AI Framework should be compatible with other risk management approaches in use and under development, while remaining policy neutral. The AI Framework should be structured to align with NIST's Cybersecurity and Privacy Frameworks to ensure consistency across AI, privacy, and cybersecurity, which have significant overlap in issues and governance processes.

Additionally, NIST should consider other global, risk-based approaches. CTIA agrees that the AI Framework should be interoperable and "law- and regulation-agnostic "[25] but cautions that the nascent regulatory landscape for AI could make it difficult for this attribute to come to fruition. For this reason, it is important that the AI Framework be adaptable—not just to different actors within the AI lifecycle—but also to global regulatory developments. To support this, NIST should be aware of and align with existing AI guidance and frameworks. For example, NIST should consider the Organisation for Economic Co-operation and Development's *Principles on Artificial Intelligence*[26] and Federal Trade Commission guidance on AI as it develops a scalable and interoperable approach to AI risk mitigation and management.

Finally, the AI Framework necessarily must take account of the risks associated with AI and consider issues such as explainability, auditability, accuracy, and bias. In each of these areas, standards and guidance are still being established, and many AI efforts by the private sector, academia, and government—including NIST's own efforts with respect bias, explainability, and security—remain ongoing. The AI Framework should not attempt to define requirements regarding these concepts, as doing so would be unhelpful, both in terms of deploying unworkable risk management solutions and in terms of influencing negative regulatory outcomes. Rather, NIST should develop an AI Framework that is policy neutral.

***

CTIA is proud to have worked with NIST on both the Cybersecurity and Privacy Frameworks and looks forward to another collaborative process here. As NIST moves forward with developing the AI Framework, it should focus on encouraging and facilitating innovative and beneficial AI uses, and embrace the same principles and processes it did in developing the Cybersecurity and Privacy Frameworks.

Respectfully submitted,

/s/ *Melanie K. Tiano*
Melanie K. Tiano
Assistant Vice President, Cybersecurity and Privacy

Thomas K. Sawanobori
Senior Vice President and Chief Technology Officer

John A. Marinho
Vice President, Technology and Cybersecurity

Avonne Bell
Director, Connected Life

---

[1] 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 carriers, 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] *See Artificial Intelligence Risk Management Framework*, 86 Fed. Reg. 40810 (July 29, 2021) ("RFI").

[3] *See* William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, § 5301(c) ("2021 NDAA").

[4] *See* NIST, *Framework for Improving Critical Infrastructure Cybersecurity* (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf ("Cybersecurity Framework").

[5] *See* NIST, *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management* (Jan. 16, 2020), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf ("Privacy Framework").

[6] *See, e.g.*, Sean Kinney, *AI and 5G go hand-in-hand for network operations*, RCR Wireless News (Aug. 3, 2018), https://www.rcrwireless.com/20180803/wireless/ai-5g-network-operations-tag17.

[7] *See* Technological Advisory Council, *The Importance of Artificial Intelligence and Data for the Telecommunications Industry and the FCC* at 5 (Jan. 14, 2021), https://www.fcc.gov/sites/default/files/fcc_aiwg_2020_whitepaper_final.pdf.

[8] *See* 5G PPP Technology Board, *AI and ML – Enablers for Beyond 5G Networks* (May 11, 2021), https://5g-ppp.eu/wp-content/uploads/2021/05/AI-MLforNetworks-v1-0.pdf.

[9] *See* AT&T Labs Research, Data Science & AI, https://about.att.com/sites/labs_research/ai (last visited Aug. 12, 2021).

[10] *See* Ericsson, *T-Mobile, improving customer experience with AI and IT Operations*, https://www.ericsson.com/en/cases/2021/tmobile-improve-customer-experience-with-ai, (last visited Aug. 12, 2021).

[11] *See* AWS, *Using Technology to Improve Personal Connections*, https://aws.amazon.com/machine-learning/customers/innovators/t_mobile/, (last visited Aug. 12, 2021).

[12] *See* IBM, *Q&A: Why IBM and Verizon Are Teaming on 5G, AI and IoT Industrial Solutions*, https://newsroom.ibm.com/Verizon-5G-QandA, (last visited Aug. 12, 2021).

[13] *See* Karen Schultz, *Verizon and Cellwize speed deployment of Verizon's 5G network, simplify development for the network*, Verizon (July 15, 2020), https://www.verizon.com/about/news/verizon-cellwize-speed-deployment.

[14] RFI at 40810.

[15] *Id.* at 40811.

[16] *See, e.g.*, Cybersecurity Framework at iv; Privacy Framework at 2.

[17] 2021 NDAA at § 5301(c).

[18] *See* RFI at 40811 ("The Framework's development process will involve several iterations to encourage robust and continuing engagement and collaboration with interested stakeholders. This will include open, public workshops, along with other forms of outreach and feedback.").
[19] *See* Cybersecurity Framework at 2 ("The [Cybersecurity] Framework is not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure."); Privacy Framework at 1 ("Finding ways to continue to derive benefits from *data processing* while simultaneously protecting individuals' privacy is challenging, and not well-suited to one-size-fits-all solutions.") (emphasis in original).
[20] *See* RFI at 40811-12 (explaining that the AI Framework should be "adaptable to many different organizations, AI technologies, lifecycle phases, sectors, and uses," "scalable to organizations of all sizes, public or private," and "risk-based," among other things).
[21] *See id.* at 40811 (expressing that the AI Framework "should provide a catalog of outcomes and approaches to be used voluntarily, rather than a set of one-size-fits-all requirements . . . .").
[22] For instance, the European Commission's draft Artificial Intelligence Act proposes that many AI applications present a low risk and therefore should benefit from a correspondingly light regulatory burden. *See Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, Explanatory Memorandum, § 2.3.
[23] *See* RFI at 40811 ("Among other purposes, the [AI Framework] is intended to be a tool that would complement and assist with broader aspects of enterprise risk management which could affect individuals, groups, organizations, or society.").
[24] *Id.* at 40811 (emphasis added).
[25] *Id.* at 40812.
[26] OECD, *OECD Principles on Artificial Intelligence*, https://www.oecd.org/going-digital/ai/principles/ (last visited Aug. 12, 2019).