Consumer Technology Association™

1919 S. Eads St.
Arlington, VA 22202
703-907-7600
CTA.tech

June 20, 2023

The Honorable John Hickenlooper
Chairman
Subcommittee on Consumer Protection,
Product Safety, and Data Security
United States Senate
Washington, D.C. 20510

The Honorable Marsha Blackburn
Ranking Member
Subcommittee on Consumer Protection,
Product Safety, and Data Security
United States Senate
Washington, D.C. 20510

Dear Chairman Hickenlooper and Ranking Member Blackburn,

The Consumer Technology Association® ("CTA")®[1] respectfully submits the following in response to questions in your letter of April 19, 2023, asking us to describe how our members are incorporating best practices from the National Institute of Standards and Technology ("NIST") Artificial Intelligence Risk Management Framework ("Framework" or "AI RMF") into their consumer products and services.

On January 26, 2023, NIST released the final version of the AI RMF[2] as the culmination of NIST's intensive drafting process over the last year that allowed interested stakeholders – including CTA – several opportunities to comment and provide input on working drafts of the AI RMF and NIST's companion AI RMF Playbook ("Playbook").[3] Throughout the process CTA supported NIST's effort to create a flexible and voluntary risk management framework that will help identify and address risks in the design, development, use, and evaluation of AI products and services across a wide spectrum of types, applications, and maturity of AI systems throughout the AI lifecycle. NIST developed its consensus-based approach to providing guidelines for trustworthy AI and continues to explore and draft guidance on issues such as AI explainability and interpretability. CTA was deeply engaged in the development of NIST's AI RMF and broadly supports NIST's voluntary, flexible, risk-based approach to developing trustworthy AI systems.[4]

---

[1] As North America's largest technology trade association, CTA® is the tech sector. Our members are the world's leading innovators—from startups to global brands—helping support millions of jobs. CTA owns and produces CES®—the largest, most influential tech event on the planet.

[2] National Institute of Science and Technology, AI Risk Management Framework, (rel. Jan. 23, 2023), https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.

[3] https://airc.nist.gov/AI_RMF_Knowledge_Base/Playbook

[4] *See* Comments of the Consumer Technology Association Comments, RFI - NIST AI Risk Management Framework, Docket No. 21076-01510 (filed Sept. 15, 2021), https://www.nist.gov/system/files/documents/2021/09/16/ai-rmf-rfi-0087.pdf; Comments of the Consumer Technology Association, NIST AI Risk Management Framework: Initial Draft, (filed Apr. 29, 2022), https://www.nist.gov/document/1st-draft-ai-rmf-comments-consumer-technology-association; Comments of the Consumer Technology Association, NIST AI Risk Management Framework: Second Draft, Docket No. 21076-01510 (filed Sept. 29, 2022).

The AI RMF also offers guidance for the development and use of trustworthy and responsible AI that is rights-preserving, non-sector-specific, and use-case agnostic, thus providing flexibility to organizations of all sizes and in all sectors. Specifically, NIST's AI RMF "offers a path to minimize potential negative impacts of AI systems, such as threats to civil liberties and rights, while also providing opportunities to maximize positive impacts."

Your letter also mentions the National Artificial Intelligence Initiative ("NAII") that partnered with the private sector to "identify, understand, and develop responses to the range of issues in the field of AI such as generated bias or limited transparency." We share your interest in developing AI and applications that are transparent, trusted and adopted by consumers. Our members' implementation of trustworthy and responsible AI will be a significant part of shaping AI's future, ensuring the United States' leadership in emerging technologies, and that "new innovations in AI are introduced to consumers in a deliberate and responsible manner."[5]

A. Efforts to Regulate or Legislate Emerging AI Technologies Require Due Deliberation and Caution

Significantly, NIST acknowledges the nascent nature of AI technology,[6] explicitly recognizes that risk mitigation frameworks must measure the benefits offered by AI systems, and that consideration of such benefits against risks is contextual, depending on "the values at play in the relevant context and should be resolved in a manner that is both transparent and appropriately justifiable."[7] NIST's measured and cautious approach is especially important given the public and private sector efforts to establish voluntary risk management frameworks that are tailored to potential risks while still allowing AI to be deployed in beneficial ways. Given the increased use of these voluntary risk management frameworks and the fast-moving pace of development of this technology, many companies have been actively working to ensure their systems conform with existing laws that regulate AI systems, such as privacy, consumer protection, and anti-discrimination regulations. Further development of AI tools and systems using AI and data should proceed without undue regulatory interference or the many benefits of AI available now, and in the future, may be lessened.[8]

Risk management is context specific, likely to change and adapt over time, and risk tolerances can be influenced by policies and norms established by AI system owners, organizations, industries, communities, or policy makers. Because there is no universally accepted concept of fairness, and because bias in AI systems cannot be eliminated in all circumstances, we believe the AI RMF will enable organizations to make contextualized decisions to ensure that steps taken to measure, map, and govern risks are reflective of unique circumstances presented in specific situations where those organizations deploy AI systems. NIST notes that "standards of fairness can be complex and difficult to define because perceptions of fairness differ among cultures and may shift depending on application.

[5] CTA also recognizes that Senate Majority Leader Chuck Schumer has come out in favor of legislating "a high-level framework that outlines a new regulatory regime for artificial intelligence…" https://www.democrats.senate.gov/newsroom/press-releases/schumer-launches-major-effort-to-get-ahead-of-artificial-intelligence

[6] AI RMF at 4.

[7] *Id*. at 37.

[8] For the same reason the National Security Commission on Artificial Intelligence's Final Report did not recommend regulation for AI technologies due, in part, to the "speed of technology development by the private sector . . . ." *See* Final Report, National Security Commission on Artificial Intelligence, at 449 (Mar. 19, 2021), *available at* https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf.

Organizations' risk management efforts will be enhanced by recognizing and considering these differences."[9]

Indeed, because decisions concerning potential bias may require tradeoffs between affected interests and intended goals of the system, developers and users of trustworthy AI systems must be empowered to take a contextual approach to risk assessment and management recognizing that acceptable risk will always be use-case specific. Similarly, because risk assessments are context specific, likely to change and adapt over time, and risk tolerances can be influenced by policies and norms established by AI system owners, organizations, industries, communities, or policy makers, organizations must be able to define reasonable risk tolerance, manage those risks, and document their risk management process. CTA's members are only at the beginning of deployment and risk assessment processes on a scale sufficient to determine the best approach to risk management. It is important to acknowledge that attempting to eliminate risk entirely can be counterproductive in practice – because incidents and failures cannot be eliminated – and may lead to unrealistic expectations and resource allocation that may ultimately exacerbate risk and make risk triage impractical. Instead, organizations should adopt "a risk mitigation culture" and allocate resources to align to the risk-level and impact of an AI system as deployed, recognizing that AI shortcomings and risks are an inevitable part of the AI development and deployment process.

In addition, we want to be sure that your Committee is aware of the multiple inquiries and initiatives directed at regulating AI technologies by the Federal Trade Commission,[10] NTIA,[11] and jointly by the DOJ, FTC, CFPB, and the EEOC.[12] The White House also announced several new initiatives to support the development of a National AI Strategy focused on not only increasing federal investment in AI research and development but also gathering information about mitigating risks and responding to the latest challenges posed by AI.[13] We mention these inquiries and initiatives to suggest that a unified and organized approach to regulating AI nationally and internationally is optimal, and in contrast to a fractured landscape of state and federal laws that will make it difficult for companies to effectively and timely deploy AI technologies.[14]

To illustrate the already complex patchwork of existing and proposed legislation that touches on AI, in the state of California alone, (1) the "Bot Disclosure Law," SB 1001, prohibits the use of undeclared bots to communicate or interact with another person in California; (2) the California Fair Employment and Housing Council has proposed draft regulations that seek to make unlawful the use of automated-decision systems that "screen out or tend to screen out" applicants or employees (or classes of applicants or employees) on the basis of a protected characteristic; (3) the California Privacy Protection Agency is considering draft regulations that would impose notice, opt-out, and transparency

[9] RMF 1.0.

[10] https://iapp.org/news/a/iapp-gps-2023-ftcs-bedoya-sheds-light-on-generative-ai-regulation/ and https://www.ftc.gov/business-guidance/blog/2023/03/chatbots-deepfakes-voice-clones-ai-deception-sale

[11] https://www.federalregister.gov/documents/2023/04/13/2023-07776/ai-accountability-policy-request-for-comment. CTA's comments to NTIA are attached as Exhibit A.

[12] https://www.ftc.gov/system/files/ftc_gov/pdf/EEOC-CRT-FTC-CFPB-AI-Joint-Statement%28final%29.pdf

[13] https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/23/fact-sheet-biden-harris-administration-takes-new-steps-to-advance-responsible-artificial-intelligence-research-development-and-deployment/

[14] For example, in the absence of any cohesive regulation of consumer privacy, ten states (soon to be 11) have legislated overlapping and oftentimes inconsistent provisions governing required notices to consumers and restrictions on processing data and deploying technologies that are critical to training, improving, and deploying AI.

requirements on AI systems that fall within defined "automated decision making" systems; and (4) Attorney General Bonita has launched an inquiry into racial and ethnic bias in healthcare algorithms.[15]

In addition, the Food and Drug Administration has already been active in addressing concerns related to using automated decision making in "Software as a Medical Device;"[16] the Equal Employment Opportunity Commission has published guidance on the Americans with Disabilities Act and its impact on the use of algorithms in the hiring process;[17] the FTC has stated that existing laws already apply to the use of AI in credit eligibility decisions under the Fair Credit Reporting Act and the Equal Credit Opportunity Act;[18] the Consumer Financial Protection Bureau ("CFPB") has published guidance for financial and credit institutions that use artificial intelligence;[19] a collection of federal financial regulators including the Board of Governors of the Federal Reserve, the CFPB, the Office of Comptroller of Currency ("OCC"), and the Federal Deposit Insurance Corporation ("FDIC") have issued a Request for Information relating to Financial Institutions' Use of Artificial Intelligence, Including Machine Learning;[20] and the Department of Transportation has published a comprehensive plan on autonomous vehicles.[21]

To avoid confusion and the potential for conflicting obligations for companies that operate in multiple states and throughout the world, any proposed legislation should not conflict with existing laws and policies. The U.S. also should work with international partners and policymakers.

B. Response to Questions on CTA Members' AI RMF Best Practices:

CTA developed and fielded a survey soliciting its members' perspectives on the utility of the NIST AI RMF, to explain to what degree the AI RMF is or will be implemented, and to further identify areas for potential improvement or revisions to the AI RMF in the future. The following incorporates our members' responses to your specific questions:

1. *How do you plan to build and deploy safe and transparent AI systems for consumers?*

---

[15] See Press Release of the Office of California Attorney General, dated Aug. 31, 2022, available at: https://oag.ca.gov/news/press-releases/attorney-general-bonta-launches-inquiry-racial-and-ethnic-bias-healthcare.

[16] *See* Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD) Action Plan, Food and Drug Administration (Jan. 2021), https://www.fda.gov/media/145022/download.

[17] *See The Americans with Disabilities Act and the Use of Software, Algorithms, and Artificial Intelligence to Assess Job Applicants and Employees*, Equal Employment Opportunity Commission (May 12, 2022), https://www.eeoc.gov/laws/guidance/americans-disabilities-act-and-use-software-algorithms-and-artificial-intelligence.

[18] Andrew Smith, *Using Artificial Intelligence and Algorithms*, FTC (Apr. 8, 2020), https://www.ftc.gov/business-guidance/blog/2020/04/using-artificial-intelligence-and-algorithms.

[19] Consumer Financial Protection Circular 2022-03: Adverse action notification requirements in connection with credit decisions based on complex algorithms, CFPB (May 26, 2022), https://files.consumerfinance.gov/f/documents/cfpb_2022-03_circular_2022-05.pdf.

[20] *Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, Including Machine Learning*, Request for Information and Comment, 86 Fed. Reg. 16837 (Mar. 31, 2021), https://www.federalregister.gov/documents/2021/03/31/2021-06607/request-for-information-and-comment-on-financial-institutions-use-of-artificial-intelligence.

[21] Automated Vehicles Comprehensive Plan, Department of Transportation (Jan. 2021), https://www.transportation.gov/sites/dot.gov/files/2021-01/USDOT_AVCP.pdf.

Many members responding to our survey both develop and deploy AI systems, with machine learning and image recognition models and systems being most commonly developed and deployed, while AI machine translation models and systems less so. The machine learning systems include computer vision-enabled applications and predictive analytics. Conversely, authentication and identity verification systems are not part of CTA members' anticipated AI offerings. The vast majority of members responding to our survey already have a risk management or governance framework in place for AI systems that are currently deployed or planned for deployment. The vast majority of respondents are familiar with the NIST AI RMF, and more than half of the survey respondents say they intend to implement some elements of the framework.

Because there will be many situations where an entity acquires and uses an AI system developed by a third-party developer, expectations will be different for different actors in the AI lifecycle. All parties involved should ensure the AI systems they develop and deploy as standalone or integrated components are trustworthy. Allocating responsibility, while important in all procurement contexts, may prove to be especially significant for developers of general AI systems and those that purchase such systems as components in larger AI systems. As transparency tools for AI systems and related documentation continue to evolve, our members as deployers of AI systems will test different types of transparency tools in cooperation with AI developers to ensure that AI systems are used as intended, a process we believe is consistent with NIST guidance.

2. *How does the AI RMF align with and support your AI development and deployment practices?*

CTA member survey respondents generally agree the AI RMF aligns with their organizations' AI development and deployment practices and that it will mitigate risks and biases associated with the development or deployment of AI systems. While only a few believe the AI RMF can be "easily" applied, aligning their internal risk management with the AI RMF, international standards, and production crosswalks is a high priority, along with providing guidance related to explainability and interpretability, and how to apply that guidance within the AI RMF. Another sector of respondents to the survey believes that developing case studies demonstrating how the AI RMF has been used by a single organization in context using tutorials and other resources to enhance multi-disciplinary and socio-technical approaches to AI risk management are a high priority for their organization.

Most of our members responding to the survey intend to implement some elements of the NIST AI RMF, but it is too early in the process for many to determine the degree or scope of implementation with reasonable precision. Risks and lifecycles are not the same for every algorithmic model created by a particular developer or generated for a particular purpose, since each model is built differently from others and based on different datasets.

There also are instances where risk cannot be measured. CTA respectfully notes that the absence of an ability to measure risk does not imply that an AI system poses high or infinite risk and should not automatically or necessarily result in halting the development or use of a technology. Additionally, it also should not lead to the implementation of misplaced or unnecessary mitigation measures under an incorrect assumption of high risk at a stage of the lifecycle where such measures would not be useful.

While there is no formal safe harbor protection associated with the AI RMF, adherence to the principles in the framework should be evidence that an organization has worked in good faith to mitigate potential

harms in such systems. Indeed, an express safe harbor could enhance AI system development and deployment.

3. *How could NIST continue to offer support to you in your efforts to deploy AI applications in the near-term?*

All our members that responded to the survey believe the AI RMF would benefit from further improvement, updates, or revisions, some of which are described above. Specifically, the process for framing risk, defining the appropriate audience, and evaluating the interplay bewteeen AI risks and trustworthiness are high on the list. Many also believe further enhancements to the process for measuring, managing, governing and mapping risks will help in the development and deployment of AI systems.

Currently, the AI RMF does not include recommendations that developers of AI systems which distribute their systems, either as finalized products or components of larger AI systems, design them to allow for further fine tuning using the acquirer's data. Similarly, while the NIST Playbook directs acquirers to establish policies related to the limitations of third-party AI systems, it does not contain any direction for purveyors to proactively provide information to acquirers regarding the limitations of the purveyors' AI systems (and need to fine tune them). Developers of AI systems should provide documentation regarding the limitations of the AI systems and the process to allow for those limitations to be mitigated. Developers should also be encouraged to test out different types of transparency tools and follow industry standards at the time a model is in use, and jointly collaborate to develop additional guidance for allocating risks, responsibilities, and obligations between these two groups.

As part of the effort to address AI trustworthiness characteristics such as "Secure and Resilient" and "Privacy-Enhanced," organizations may consider leveraging available standards and guidance that provide broad direction to organizations to reduce security and privacy risks, such as, but not limited to, the NIST Cybersecurity Framework, the NIST Privacy Framework, the NIST Risk Management Framework, and the Secure Software Development Framework.

4. *What plans do you have to contribute independently or jointly to case studies, AI profiles or tutorials that the AI RMF Roadmap outlines?*

A small percentage of our responding members intend to contribute to developing case studies demonstrating how the AI RMF has been used by a single organization or sector, context, or AI actor; and/or tutorials and other resources to enhance multi-disciplinary and socio-technical approaches to AI risk management. A larger share of survey respondents has not reached a conclusion on such contributions or have not ruled it out.

5. *What are the most effective ways to provide resources directly to consumers in consumer-facing products to help them understand and trust AI systems?*

Effectiveness will depend on developing educational materials for the general public, realizing that we have multiple audiences with multiple viewpoints (e.g., those who may mistrust technology and would need encouragement to use it, and others who may over trust and would need encouragement to carefully consider what their AI-enabled application is telling them).

Transparency and explainability are important to consumers' understanding that AI systems are reliable (*e.g.,* that models produce anticipated outcomes) and are also protected against bad actors. Ongoing audits and monitoring, at an appropriate cadence, will confirm that systems behave as intended, have not experienced unauthorized internal access or modification, and enjoy robust security to avoid adversarial attack. Additionally, consumers will benefit from receiving cybersecurity guidance so they understand that their data, as well as the models and algorithms, are protected from tampering or unsupervised changes. Cybersecurity guidance also should address privacy, security, and infrastructure considerations related to sharing data and models.

Conclusion

CTA appreciates your and the Committee's attention to the issues arising today for the development and deployment of responsible and trustworthy AI. CTA also recognizes the road to achieving that goal is beset on all sides with competing concerns for safety and efficacy, for accuracy and nondiscrimination, and for efficiency and effectiveness, although these goals may be inconsistent at times. As AI continues to become more integrated into many aspects of daily life, the importance of addressing potential biases, transparency, explainability, and possible flawed designs becomes increasingly critical. Congress and the Administration should recognize that voluntary, flexible, risk-based approaches to risk mitigation, like the NIST RMF, are the most effective tool to encourage the development of trustworthy AI while also ensuring that U.S. companies have the necessary flexibility to design and deploy products and services that will maintain the United States' current competitive edge in the global marketplace.

Respectfully submitted,

/s/ Douglas K. Johnson
Douglas K. Johnson
Vice President, Emerging Technology Policy

/s/ Michael Petricone
Michael Petricone
Sr. Vice President, Government and Regulatory Affairs

BEFORE THE
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION

In the Matter of **AI Accountability Policy Request for Comment**	RIN 0660-XC057

COMMENTS OF THE CONSUMER TECHNOLOGY ASSOCIATION IN RESPONSE TO THE NTIA'S REQUEST FOR COMMENTS ON AI SYSTEM ACCOUNTABILITY MEASURES AND POLICIES

The Consumer Technology Association® ("CTA") submits this response to the National Telecommunications and Information Administration ("NTIA") AI Accountability Policy Request for Comment ("Request for Comment"). CTA is North America's largest technology trade association. Our members are the world's leading innovators—from startups to global brands—helping support more than 18 million American jobs. CTA owns and produces CES®—the most influential tech event in the world.

In response to the NTIA's call for comments, CTA urges the NTIA to proceed with caution when considering whether, or what, new rules may be necessary to establish accountability within the ecosystem of entities developing and deploying artificial intelligence systems. Artificial Intelligence ("AI") as a category of technologies is not new, but generative AI systems and technologies such as machine learning that underlie AI systems are emerging technologies that are evolving rapidly. Indeed, a recent Federal Trade Commission ("FTC") report found that AI is nascent, varied, and not susceptible to one definition.[1] For example, AI

[1] *See* Combatting Online Harms Through Innovation, FTC, at 1 (June 16, 2022), available at https://www.ftc.gov/system/files/ftc_gov/pdf/Combatting%20Online%20Harms%20Through%20Innovation%3B%

systems may be used to inform a broader system, such as AI machine vision systems that are used to read stop signs in autonomous vehicles. Such applications have very different risk profiles as compared with generative AI tools that are connected to the Internet and interact with users directly. Industry leaders in the development of AI systems, including generative AI systems, have been actively working to ensure their systems comply with existing laws, such as privacy, consumer protection, and anti-discrimination regulations.

As such, before supporting or proposing policies that call for new rules in this area, the NTIA should ensure that it develops a robust record and undertakes sufficient deliberation and consideration of both the benefits and risks presented by AI systems and technology. Any new rules recommended by the NTIA should be part of a risk-based, flexible approach that accounts for different use cases and is narrowly tailored to avoid imposing undue burdens innovation.

In these comments, CTA outlines several factors the NTIA should consider as it collects information regarding methods of ensuring trustworthy and accountable AI systems. First, CTA describes the nascent development of AI technologies and the need for a flexible approach to regulation. Next, CTA provides responses to specific questions posed by NTIA in its Request for Comment.

I. New Efforts to Regulate Emerging AI Technologies Require Due Deliberation and Caution

AI offers tremendous potential for human and societal development: promoting inclusive growth, improving the welfare and well-being of individuals, and enhancing global innovation and productivity. A growing body of research demonstrates that AI can identify and mitigate

---

20Federal%20Trade%20Commission%20Report%20to%20Congress.pdf ("Combatting Online Harms Report") ("AI is defined in many ways and often in broad terms. The variations stem in part from whether one sees it as a discipline (e.g., a branch of computer science), a concept (e.g., computers performing tasks in ways that simulate human cognition), a set of infrastructures (e.g., the data and computational power needed to train AI systems), or the resulting applications and tools.").

bias in human decision making.[2] Perhaps the leading federal agency focused on AI governance and risk management, the National Institute of Science and Technology ("NIST"), has recently commented that "new AI-enabled systems are revolutionizing and benefitting nearly all aspects of our society and economy – everything from commerce and healthcare to transportation and cybersecurity."[3]

Further, CTA members help promote the development of responsible and trustworthy AI through leadership in the development of emerging practices that mitigate risks, such as the use of federated learning, a machine learning ("ML") approach that learns from a user's interaction with a given device while keeping all the training data on the device, so that the data does not need to be shared with a server. For example, Google recently published research on Entities as Experts AI, explaining how these systems are answering text-based questions with less data.[4] Google has also published guidance for regulators on how to most effectively regulate AI in its *Recommendations for Regulating AI* paper.[5] Indeed, CTA has supported efforts at the federal level to develop voluntary risk-based frameworks to address potential AI risks while enabling

---

[2] *See, e.g.*, Jon Kleinberg et al., *Discrimination in the Age of Algorithms*, 10 J. of Legal Analysis 113, 120 (2019), https://academic.oup.com/jla/article/doi/10.1093/jla/laz001/5476086; Cass R. Sunstein, *Algorithms, Correcting Biases*, 86 Soc. Rsch.: An Int'l Q. 499, 500 (2019), http://eliassi.org/sunstein_2019_algs_correcting_biases.pdf; Kimberly A. Houser, *Can AI Solve the Diversity Problem in the Tech Industry? Mitigating Noise and Bias in Employment Decision-Making*, 22 Stan. Tech. L. Rev. 290, 352 (2019), https://www-cdn.law.stanford.edu/wp-content/uploads/2019/08/Houser_20190830_test.pdf.

[3] Moreover, NIST recognizes that AI "is rapidly transforming our world. Remarkable surges in AI capabilities have led to a wide range of innovations including autonomous vehicles and connected Internet of Things devices in our homes. AI is even contributing to the development of a brain-controlled robotic arm that can help a paralyzed person feel again through complex direct human-brain interfaces." *Artificial Intelligence*, NIST, https://www.nist.gov/artificial-intelligence (last visited Oct. 1, 2022). *See also About Artificial Intelligence*, National Artificial Intelligence Initiative Office, https://www.ai.gov/about/ (last visited Oct. 1, 2022) (explaining that investments in AI technology "have led to transformative advances now impacting our everyday lives, including mapping technologies, voice-assisted smart phones, handwriting recognition for mail delivery, financial trading, smart logistics, spam filtering, language translation, and more. AI advances are also providing great benefits to our social wellbeing in areas such as precision medicine, environmental sustainability, education, and public welfare.").

[4] Eunsol Choi et al., *Entities as Experts: Sparse Memory Access with Entity Supervision*, Google Research (Oct. 6, 2020), https://arxiv.org/pdf/2004.07202.pdf.

[5] Recommendations for Regulating AI, Google, https://ai.google/static/documents/recommendations-for-regulating-ai.pdf (last visited Oct. 3, 2022).

stakeholders to maximize the benefits of this technology.[6] In recent comments to NIST concerning the development of that agency's AI Risk Management Framework ("RMF"), CTA applauded the agency's work to create a flexible and voluntary risk management framework for managing AI risks, including those that may be implicated by the use of AI tools and systems.[7]

Released in January of this year, NIST's AI RMF sets forth a voluntary framework to map, measure, manage and govern emerging AI risks.[8] Significantly, in the RMF, NIST acknowledges the nascent nature of this technology[9] and explicitly recognizes that risk mitigation frameworks must measure the benefits offered by AI systems, and that consideration of such benefits against risks is contextual and depends on "the values at play in the relevant context and should be resolved in a manner that is both transparent and appropriately justifiable."[10]

NIST's findings and decision to use a voluntary framework suggest it may be premature for the NTIA to move forward with broad restrictions on a nascent technology which offers the potential to dramatically improve consumer well-being. This is especially true given public and private sector efforts to establish voluntary risk management frameworks tailored to potential risks while still allowing AI deployment in beneficial ways. Given the increased use of these voluntary risk management frameworks and the fast-moving pace of development of this technology, NTIA should proceed with caution and avoid adopting overly prescriptive rules.

---

[6] *See, e.g.*, Consumer Technology Association Comments, RFI - NIST AI Risk Management Framework, Docket No. 21076-01510 (filed Sept. 15, 2021), available at https://www.nist.gov/system/files/documents/2021/09/16/ai-rmf-rfi-0087.pdf.

[7] Comments of the Consumer Technology Association, AI Risk Management Framework, at 2 (filed Sept. 29, 2022), available at 2 https://www.nist.gov/system/files/documents/2022/11/16/Consumer%20Technology%20Association%20%28CTA%29.pdf .

[8] National Institute of Science and Technology, AI Risk Management Framework, (rel. Jan. 23, 2023), available at https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf

[9] *Id*. at 4.

[10] *Id*. at 37.

Specific restrictions on AI tools and systems or on data necessary for those systems to function could undermine the many benefits of AI available now and in the future.

For the same reason, the National Security Commission on Artificial Intelligence's Final Report did not recommend regulation for AI technologies due, in part, to the "speed of technology development by the private sector . . . ."[11] Prescriptive rules would undermine the important work that has been done across the public and private sectors to focus on risk-based approaches. These findings counsel against the adoption of broad prescriptive rules at this time.

To that end, the emergence of flexible voluntary consensus-based international industry frameworks to enable trustworthy AI systems, such as NIST's AI RMF, should be fully leveraged before the NTIA (or other federal agencies) recommend the adoption of new prescriptive rules governing AI systems. At a minimum, NTIA should provide sufficient time for implementation of the AI RMF as organizations work to voluntarily identify and address AI risks and the relevant risk profiles and tolerances. It would be premature to suggest that AI needs onerous rules until such voluntary approaches are considered (particularly given that existing laws, including anti-discrimination laws, already apply when AI is used).

II. Response to Questions Framed by NTIA's RFC

A. Response to Question 1: What is the purpose of AI accountability mechanisms such as certifications, audits, and assessments?

Broadly speaking, the purpose of AI accountability mechanisms is to ensure the development of trustworthy AI systems without unduly hindering innovation and the development of new, beneficial technologies. Accountability mechanisms allow businesses to ensure the AI systems they develop operate consistent with responsible development and operational principles established to ensure trustworthiness.

[11] *See* Final Report, National Security Commission on Artificial Intelligence, at 449 (Mar. 19, 2021), *available at* https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf.

Question 1(e) specifically asks whether "AI accountability practices [can] have meaningful impact in the absence of legal standards and enforceable risk thresholds." In response, CTA notes that this question presumes an absence of legal standards or enforceable risk thresholds regarding AI systems. In fact, in the current regulatory environment, there are a number of extant laws and regulations creating legal standards and enforceable risk thresholds that apply to AI systems. AI tools used for employment decisions, for example, are subject to existing civil rights laws as well as unfair trade practices and privacy laws.

Moreover, where there are perceived gaps in existing laws and regulations, private companies, leading trade associations, government agencies, and civil society organizations are currently leading the way with additional policies, frameworks, standards, and technical mechanisms for developing and deploying trustworthy AI, with an eye towards meeting or exceeding legal standards. For example, CTA has published a set of "Guidelines for Developing Trustworthy Artificial Intelligence Systems" that is publicly available for businesses to use when developing AI systems. In addition, the NIST AI RMF, noted above, is the most significant among these mechanisms. The AI RMF is already driving an increase in the adoption of AI governance and risk management frameworks by CTA member companies and many other companies developing or deploying AI systems.

When considering potential mechanisms for ensuring AI accountability, the NTIA should consider both the significant body of law that already governs the development and use of AI systems, and the significant measures that industry leaders, trade associations, and governmental bodies have already taken to encourage the development of trustworthy AI.

B. Response to Question 3: AI accountability measures have been proposed in connection with many different goals. To what extent are there tradeoffs among these goals?

NIST recognized in its AI RMF that addressing characteristics of trustworthy AI individually is unlikely to be sufficient and that when "tradeoffs are [] involved, rarely do all characteristics apply in every setting, and some will be more or less important in any given situation." For example, regarding the characteristic of transparency, the AI RMF notes "a transparent system is not necessarily an accurate, privacy-enhanced, secure, or fair system." Indeed, highly transparent systems can create privacy risks and potentially offer bad actors greater ability to manipulate the system and generate unwanted results.

Similarly, the inclusion of "human alternatives" will not necessarily result in a reduction of potentially harmful bias. As noted above, AI systems have been developed precisely to identify and mitigate bias in human decision making.[12] Therefore, in some situations, reintroducing human alternatives into the decision making process may be counterproductive to efforts to minimize or eliminate harmful bias.

In addition, the use of "human alternatives" should be distinguished from "human fallbacks" because inserting human alternatives into a decisionmaking process may dampen innovation and increase the costs of implementing AI systems. However, in contrast, implementing a system of human fallbacks or review of decisions made primarily by AI systems may allow for some level of human involvement while maintaining the efficiency of the AI system.

[12] *See footnote 2.*

C. Response to Question 6: The application of accountability measures (whether voluntary or regulatory) is more straightforward for some trustworthy AI goals than for others. With respect to which trustworthy AI goals are there existing requirements or standards?

There are currently a plethora of federal, state, and local laws, rules, and regulations that already exist, or which governments have proposed, that cover the development and use of AI systems. Federal and state regulatory bodies have already invested significant time and resources in developing appropriate risk-based regulatory frameworks applicable to those entities using AI that are subject to the jurisdiction of these sector-specific regulators. Adopting broad, general-purpose rules that may conflict, or be inconsistent, with these sector-specific approaches could create significant uncertainty and confusion in these industries. As such, any regulation should seek to harmonize with existing federal sectoral statutes, rules or regulations, and other state AI or consumer privacy laws.

Considering the already complex patchwork of laws governing AI, NTIA should ensure that it is fully informed by a robust and complete record that reflects the new and emerging federal, state, and local rules and regulations applicable to AI-enabled systems. Any new rules that may be recommended by the NTIA should include express exclusions for entities that are subject to existing federal statutes, regulations, orders or decisions that clearly govern specific services, systems or practices.

To illustrate the already complex patchwork of existing and proposed legislation that touches on AI, in the state of California alone, (1) the "Bot Disclosure Law," SB 1001, prohibits the use of undeclared bots to communicate or interact with another person in California; (2) the California Fair Employment and Housing Council has proposed draft regulations that seek to make unlawful the use of automated-decision systems that "screen out or tend to screen out" applicants or employees (or classes of applicants or employees) on the basis of a protected

characteristic; (3) the California Privacy Protection Agency is considering draft regulations that would impose notice, opt-out and transparency requirements on AI systems that fall within the designation of "automated decision making" systems; and (4) Attorney General Bonita has launched an inquiry into racial and ethnic bias in healthcare algorithms.[13]

States outside of California with consumer privacy statutes have also already proposed or enacted rules related to the use of automated tools for "profiling." For example, the Colorado Privacy Act defines "profiling" as "any form of automated processing of personal data to evaluate, analyze, or predict personal aspects concerning an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements."[14] The recently finalized rules implementing the Colorado Privacy Act require companies that employ profiling "for a decision that results in the provision or denial of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health-care services, or access to essential goods or services" are required to provide consumers notice of:

1. the decisions that are subject to automated decision making,
2. the categories of data processed as part of the profiling,
3. a non-technical, plain language explanation of how profiling is used in the decision-making process,
4. whether the system has been evaluated for fairness and accuracy,
5. the benefits and potential consequences of the decision based on profiling, and
6. information about how a consumer may choose to opt-out of such decisions.[15]

The Colorado regulations also provide consumers the right to opt-out of profiling in

[13] See Press Release of the Office of California Attorney General, dated Aug. 31, 2022, available at: https://oag.ca.gov/news/press-releases/attorney-general-bonta-launches-inquiry-racial-and-ethnic-bias-healthcare.
[14] C.R.S. § 6-1-1303(20)
[15] 4 CCR 904-3; 9.03(A)

furtherance of decisions that produce legal or other "similarly significant" effects concerning a consumer, although businesses are not required to honor such requests if they employ "Human Involved Automated Processing"[16] and provide consumers with certain disclosures about the decision that incorporates the profiling process.[17]

Virginia's consumer privacy law, which came into effect on January 1, 2023, also requires companies to provide consumers the ability to opt-out of profiling in furtherance of decisions that produce legal or "similarly significant" effects concerning the consumer,[18] and also requires companies to conduct data protection assessments when they engage in "processing of personal data for purposes of profiling, where such profiling presents a reasonably foreseeable risk of (i) unfair or deceptive treatment of, or unlawful disparate impact on, consumers; (ii) financial, physical, or reputational injury to consumers; (iii) a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person; or (iv) other substantial injury to consumers."[19] Connecticut's consumer data privacy statute contains similar opt-out and impact assessment requirements.[20]

These state privacy laws also ensure that consumer opt-out and access rights regarding profiling do not extend to decisions that are only partially automated and incorporate human review within the decision-making process. For example, the profiling opt-out and access rights in Connecticut's consumer privacy act are restricted to "profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the

[16] Defined as the automated processing of Personal Data where a human (1) engages in a meaningful consideration of available data used in the Processing or any output of the Processing and (2) has the authority to change or influence the outcome of the Processing.
[17] 4 CCR 904-3; 9.04(C)
[18] Va. Code Ann. § 59.1-577(A)(5)
[19] Va. Code Ann. § 59.1-580(A)(3).
[20] *See* CT LEGIS P.A. 22-15, 2022 4(a), 8(a).

consumer."[21] Similarly, in Colorado, the AG recently finalized regs that create an exemption from the opt-out rules for profiling that is based on "human involved automated processing."[22] These restrictions incentivize companies to adopt innovative AI systems while still maintaining some human oversight of the process.

Federal sector-specific regulations also must be considered before advancing rules that may impact industries that are already highly regulated, such as healthcare and financial services. These industries face unique considerations that regulators with specialized knowledge would best address. For example, the Food and Drug Administration already has been active in addressing concerns related to using automated decision making in "Software as a Medical Device;"[23] the Equal Employment Opportunity Commission has published guidance on the Americans with Disabilities Act and its impact on the use of algorithms in the hiring process;[24] the FTC has stated that existing laws already apply to the use of AI in credit eligibility decisions under the Fair Credit Reporting Act and the Equal Credit Opportunity Act;[25] the Consumer Financial Protection Bureau ("CFPB") has published guidance for financial and credit institutions that use artificial intelligence;[26] a collection of federal financial regulators including the Board of Governors of the Federal Reserve, the CFPB, the Office of Comptroller of Currency ("OCC"), and the Federal Deposit Insurance Corporation ("FDIC") have issued a Request for Information relating to Financial Institutions' Use of Artificial Intelligence, Including Machine

[21] *See* CT LEGIS P.A. 22-15, 2022, Section 4(a)(5)(C).
[22] *See* CPA Rules, Rule 9.04(C)
[23] *See* Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD) Action Plan, Food and Drug Administration (Jan. 2021), https://www.fda.gov/media/145022/download.
[24] *See The Americans with Disabilities Act and the Use of Software, Algorithms, and Artificial Intelligence to Assess Job Applicants and Employees*, Equal Employment Opportunity Commission (May 12, 2022), https://www.eeoc.gov/laws/guidance/americans-disabilities-act-and-use-software-algorithms-and-artificial-intelligence.
[25] Andrew Smith, *Using Artificial Intelligence and Algorithms*, FTC (Apr. 8, 2020), https://www.ftc.gov/business-guidance/blog/2020/04/using-artificial-intelligence-and-algorithms.
[26] Consumer Financial Protection Circular 2022-03: Adverse action notification requirements in connection with credit decisions based on complex algorithms, CFPB (May 26, 2022), https://files.consumerfinance.gov/f/documents/cfpb_2022-03_circular_2022-05.pdf.

Learning;[27] and the Department of Transportation has published a comprehensive plan on autonomous vehicles.[28]

In addition, international organizations also have been actively developing guidelines and standards for trustworthy AI. For example, the ISO-IEC Joint Technical Committee has engaged in a broad scope of work regarding development of AI standards addressing foundational concepts, trustworthiness aspects, data management, and robustness.[29] These organizations also have developed sector-specific voluntary frameworks regarding AI which industry participants have adopted. For example, ISO 26262 is the leading safety standard for autonomous vehicles, and adoption of that standard contributes to the establishment of safe and trustworthy AI systems.

Clearly, there are existing policy frameworks in place for governing AI use, many of which create a patchwork of complex and challenging legal and regulatory duties. To avoid confusion and the potential for conflicting obligations for companies operating in multiple states, the NTIA should ensure that any new proposed rules do not conflict with existing federal and state laws.

D. Response to Question 10: What are the best definitions of terms frequently used in accountability policies, such as fair, safe, effective, transparent, and trustworthy?

The NIST AI RMF is widely seen as one of the most significant voluntary risk mitigation frameworks, and it clearly defines key terms and concepts necessary to develop accountability mechanisms supporting trustworthy AI. The RMF, in turn, relies in part on concepts and

---

[27] *Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, Including Machine Learning*, Request for Information and Comment, 86 Fed. Reg. 16837 (Mar. 31, 2021), https://www.federalregister.gov/documents/2021/03/31/2021-06607/request-for-information-and-comment-on-financial-institutions-use-of-artificial-intelligence.

[28] Automated Vehicles Comprehensive Plan, Department of Transportation (Jan. 2021), https://www.transportation.gov/sites/dot.gov/files/2021-01/USDOT_AVCP.pdf.

[29] ISO/IEC JTC 1/SC 42 Artificial Intelligence, ISO-IEC Joint Technical Committee (October 2022),

definitions from the well-established OECD AI principles and is compatible with other AI risk management guidance, such as the draft EU AI Act, ISO/IEC 23894 (AI Risk Management standard), and the White House Blueprint for an AI Bill of Rights. Moreover, to the extent that the RMF does not include definitions relating to emergent technologies that are necessary for policy development, NIST intends the RMF to be a living document that will continue to be iterated and revised to include new definitions. Accordingly, the NTIA should leverage the definitions and concepts developed by NIST that address key concepts such as fair, safe, effective, transparent and trustworthy AI systems.

E. Response to Question 14: Which non-U.S. or U.S. (federal, state, or local) laws and regulations already requiring an AI audit, assessment, or other accountability mechanism are most useful and why? Which are least useful and why?

Several state privacy laws require a privacy impact assessment when businesses use so-called "automated decision-making systems" or process "sensitive personal information." Further, New York City will soon begin enforcing Local Law 144 of 2021 relating to automated employment decision tools ("Law 144"). Although Local Law 144 targets employment decisions, its expansive definition of automated employment decision tools and extensive requirements to obtain third-party audits and publish the results will make compliance extremely difficult, especially for small and medium sized businesses, and it could raise security concerns. Although audits are not *per se* undesirable and can be an effective tool for minimizing harmful bias, inflexible and costly audits, including those that require results to be published publicly or provided to government agencies, may be overly burdensome, costly and ineffective in eliminating actual, or perceived, risks. For that reason, any proposal endorsing the use of audits should permit operational flexibility, proper scoping to avoid unnecessary compliance hurdles, and use of less costly or intrusive processes that may achieve the same goal – such as allowing

businesses to conduct internal self-assessments. Accordingly, CTA urges the NTIA to instead support efforts to incentivize adoption of voluntary, risk-based approaches to AI accountability, such as through adoption of the NIST RMF or other potentially applicable standards.

F. Response to Question 17: How should AI accountability measures be scoped (whether voluntary or mandatory) depending on the risk of the technology and/or of the deployment context? If so, how should risk be calculated and by whom?

Accountability measures that go above and beyond existing law should be scoped to include only decisions that are made solely by automated means and have high-risk or high-impact to individuals, including legal or similarly significant effects, such as decisions resulting in the provision or denial of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, and health-care services.[30]

G. Response to Question 30: What role should government policy have, if any, in the AI accountability ecosystem?

One-size-fits-all rules to regulate or discourage AI and algorithmic decision making would stifle innovation by discounting potential benefits and ignoring options for risk mitigation. Given widespread applications and uses of AI, regulation of AI is particularly ill-suited to a one-size-fits-all approach. Across applications and uses, there are substantial differences between the kinds of risks that consumers may face from mistakes or misuse of AI-enabled systems. For example, health care (e.g., robotic surgery) applications may be more high-risk than media or advertising uses. As explained above, there are significant federal regulations in place covering industry-specific application of AI. Prescriptive rules attempting to generally regulate AI technology itself, without accounting for sector-specific applications or actual risks to consumers, will stifle benefits without effectively addressing risks.

[30] NTIA should avoid overly broad definitions of decisions with legal or similarly significant effects, such as including decisions concerning the provision of broadband and telecommunications services.

When analyzing potential mechanisms of establishing accountability in the AI ecosystem, the NTIA should look to the NIST AI RMF which relies on flexible risk-based assessments and recognizes the importance of proceeding deliberatively to avoid unnecessary burdens on AI development and deployment. NIST solicited input from a wide array of stakeholders to develop its consensus-based approach to providing guidelines for trustworthy AI, and NIST continues to explore and draft guidance on issues such as AI explainability and interpretability. CTA was deeply engaged in the development of NIST's AI RMF and broadly supports NIST's flexible, risk-based approach to developing trustworthy AI systems.[31]

Respectfully submitted,

CONSUMER TECHNOLOGY ASSOCIATION

/s/ Douglas K. Johnson
Douglas K. Johnson
Vice President, Emerging Technology Policy

/s/ Michael Petricone
Michael Petricone
Sr. Vice President, Government and Regulatory Affairs

Dated: June 12, 2023

[31] *See* Comments of the Consumer Technology Association Comments, RFI - NIST AI Risk Management Framework, Docket No. 21076-01510 (filed Sept. 15, 2021), https://www.nist.gov/system/files/documents/2021/09/16/ai-rmf-rfi-0087.pdf; Comments of the Consumer Technology Association, NIST AI Risk Management Framework: Initial Draft, (filed Apr. 29, 2022), https://www.nist.gov/document/1st-draft-ai-rmf-comments-consumer-technology-association; Comments of the Consumer Technology Association, NIST AI Risk Management Framework: Second Draft, Docket No. 21076-01510 (filed Sept. 29, 2022).