U.S. Chamber of Commerce

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

June 12, 2023

Via Electronic Filing

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW
Washington, DC 20230

Re: National Telecommunications and Information Administration; AI Accountability Policy Request for Comment (88 Fed. Reg. 22,433-22,441, April 13, 2023)

Artificial intelligence (AI) is revolutionizing how businesses of all sizes and industries operate and how those companies will provide significant benefits and efficiencies for Americans to live and work. The U.S. Chamber of Commerce ("Chamber"), in a report released on March 9, 2023,[1] has advocated for developing a regulatory environment that uses risk-based models and gap filling of existing laws and regulations to foster trust in AI and its ethical deployment. These policies are necessary to maintain American leadership and to ensure the safe use of AI that is expected to add $13 trillion to the global GDP by 2030[2].

Recognizing these needs, the Chamber released AI principles in 2019. The first principle stated, "Trustworthy AI is a [p]artnership.[3]" This highlights the importance of fostering public trust in AI technologies, as it is necessary to advance its design, development, deployment, and use. Trustworthy AI encompasses transparency, explainability, fairness, and accountability. However, the speed and complexity of changes in AI technology mean that governments alone cannot promote trustworthy AI.

Governments must partner with the private sector, academia, and civil society when addressing issues of public concern associated with AI. Similar public-private partnerships, centered around standards and practices, have benefited consumers and businesses alike. The Chamber recognizes and commends existing partnerships that have formed in the AI community to address these challenges, including protecting against harmful biases, ensuring democratic values, and respecting human rights. A governance framework should be flexible and driven by a transparent, voluntary, risk-based, and multi-stakeholder process.

Valuing partnership, the Chamber appreciates NTIA's request for comment on AI Accountability in the agency's capacity as "the President's principal advisor on telecommunications and information policy issues."[4] However, concerns exist regarding the enormous scope of the questions posed within the request for comment. Furthermore, compounding these concerns is the number of government entities advising the President on AI and the number of government agencies requesting comment on various aspects of AI. This

[1] https://www.uschamber.com/assets/documents/CTEC_AICommission2023_Report_v6.pdf
[2] https://www.mckinsey.com/industries/public-and-social-sector/our-insights/the-potential-value-of-ai-and-how-governments-could-look-to-capture-it
[3] https://www.uschamber.com/technology/us-chamber-releases-artificial-intelligence-principles
[4] https://ntia.gov/sites/default/files/publications/ntia_rfc_on_ai_accountability_final_0.pdf

uptick of activities within multiple entities, while notable on a certain level, makes it difficult for the business community to relay important information on these essential issues within the federal government and raises doubts about the ability of relevant agencies to engage in coordinated and timely action. Without better coordination, this scenario could lead to a possible patchwork of guidelines that would inhibit development of A.I. and hinder the benefits that should accrue to the American economy and consumers.

The Chamber provides provide the following feedback on the following request for comment on the "AI Accountability Policy Request for Comment."

AI Accountability Objectives

1. What is the purpose of AI accountability mechanisms such as certifications, audits, and assessments?

The Chamber recognizes the purpose of certification, audits, and assessments as a means for organizations to utilize repeatable and standard methodologies to help them improve the explainability of an algorithm. It is important to highlight that many sectors already have sector-specific rules and associated reporting requirements that apply to artificial intelligence. Additionally, the context of AI deployment is critical for determining risk. For this reason, we believe that there is a strong need to use existing laws, rules, regulations and guidance, for the foundation of AI policy development, but that duplication should be avoided.

Furthermore, there are strong apprehensions regarding any *mandatory* third-party audit requirement. Further research, standardization, and economies of scale around best practices and the prevalence of practitioners are still needed in this space.

2. Is the value of certifications, audits, and assessments mostly to promote trust for external stakeholders or is it to change internal processes?

As stated above, the value of assessments is to reduce the risk of harm. Increased transparency can help both to demystify AI products and remove opportunities for adverse consequences. Assessments can identify areas of risk and enable corrections prior to deployment. In addition, a common set of values and language can shape the culture of AI, enabling these tools to be used and developed in inclusive ways for the benefit of all people.

3. AI accountability measures have been proposed in connection with many different goals

The development of best practices and guidelines for AI accountability measures continues to evolve and develop. This is why the Chamber has been a staunch supporter of the National Institutes of Standards and Technologies ("NIST") Artificial Intelligence Risk Management Framework ("RMF") The NIST AI RMF is a congressionally mandated voluntary framework that enables businesses and organizations to have a flexible framework to help mitigate issues within the entire AI lifecycle. In particular, the Chamber looks forward to NIST's adoption of "profiles," which "are implementations of the AI RMF functions, categories, and subcategories for a specific setting or application based on the requirements, risk tolerance, and resources.[5]"

[5] https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf

Developing best practices around specific use cases will be beneficial as new companies and organizations enter the market and seek to mitigate potential issues appropriately.

4. Can AI accountability mechanisms effectively deal with systemic and/or collective risks of harm?

Companies and organizations designing, developing, deploying, and using AI technologies have strong incentives to mitigate and avoid harm due to these activities' legal and reputational risks. Companies and organizations should look to frameworks, such as the NIST AI RMF, as a critical accountability resource to support their efforts to help address potential risks and harm.

It is essential for further development of the NIST AI RMF to address risks and harm. Other AI accountability mechanisms to consider include ISO 420010 and ISO 23894. Furthermore, because responsible AI heavily depends on good and sound data, the Chamber highlights the use of government data sets' vital role in addressing potential harms associated with using the technology.

5. Given the likely integration of generative AI tools such as large language models (e.g., ChatGPT) or other general-purpose AI or foundational models into downstream products, how can AI accountability mechanisms inform people about how such tools are operating and/or whether the tools comply with standards for trustworthy AI?

AI accountability mechanisms should provide meaningful transparency to ensure the accountability of foundation models. However, any accounting mechanism should be done based on the specific risk of the technology. Such clarity should be done in a way that the average person can understand, and could be something as straightforward as an "AI Service Cards" which provides (1) the type of data being used, (2) the purposes for which the AI is employed and; (3) the self-governance mechanisms embedded throughout the AI lifecycle that are implemented to mitigate negative impacts and harms.

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? Are there any trustworthy AI goals that are not amenable to requirements or standards? How should accountability policies, whether governmental or non-governmental, treat these differences?

Empowering organizations and companies to improve the trustworthiness of their AI requires implementing a culture that prioritizes defining roles, responsibilities, and effective risk-management incentive structures, to promote accountability. Regarding standardization, NTIA should look to entities such as NIST, ISO and IEEE grading AI standards.

7. Are there ways in which accountability mechanisms are unlikely to further, and might even frustrate, the development of trustworthy AI? Are there accountability mechanisms that unduly impact AI innovation and the competitiveness of U.S. developers?

There are many things that can negatively impact AI innovation and the competitiveness of U.S. developers. These include stringent compliance timelines and accountability mechanisms that are overly

prescriptive and fail to provide necessary flexibility. Regulators should take a regulation approach based upon precision and focus on the most harmful uses/impacts of AI.

8. What are the best definitions of and relationships between AI accountability, assurance, assessments, audits, and other relevant terms

The Chamber strongly believes that definitions must be precise and align with standards and terms developed by established entities such as federal agencies' guidance, standards development groups, and regulatory frameworks. Such an approach will create clearly identifiable guardrails.

The U.S. Chambers AI Commission highlighted in its recent report that "[t]o succeed in creating a regulatory framework for AI, the U.S. needs a clear legal definition of AI with precise legal certainty[6]." The Commission further highlighted the following recommendations:

- *The diversity of current AI applications paired with an unknown innovation trajectory may complicate efforts to build an "ideal" legal definition sufficiently broad enough to accommodate future changes. Any legal definition should be technology neutral and sufficiently flexible to accommodate technical progress, while precise enough to provide the necessary legal certainty.*
- *Overly prescriptive legal definitions may lead to unintended consequences that inhibit innovation by discouraging research and development outside specified applications.*
- *Definitions should not be overly broad, and they should focus on systems that learn and adapt over time.*
- *Definitions should focus on real AI, not non-AI enabled computer software that has been mistakenly assumed or perceived to be AI.*
- *Any legal definitions should be accessible to individuals at different levels of understanding.*
- *A legal definition should address AI's potential impacts on the public, such as AI discrimination or violations of consumer rights.*

Existing Resources and Models

9. What AI accountability mechanisms are currently being used? Are the accountability frameworks of certain sectors, industries, or market participants especially mature as compared to others? Which industry, civil society, or governmental accountability instruments, guidelines, or policies are most appropriate for implementation and operationalization at scale in the United States? Who are the people currently doing AI accountability work?

NIST released its AI Risk Management Framework earlier this year. The NIST AI RMF Is modeled on other successful and widely adopted materials from the agency, including its Cybersecurity Risk Management Framework. The AI RMF is less than a year old, and companies and organizations are still familiarizing themselves with how they can adopt the AI RMF. NIST's supplementary AI RMF Playbook[7] supports these

[6] https://www.uschamber.com/assets/documents/CTEC_AICommission2023_Report_v6.pdf
[7] https://www.nist.gov/itl/ai-risk-management-framework/nist-ai-rmf-playbook

efforts by suggesting **"ways to navigate and use the** AI Risk Management[8] Framework (AI RMF) to incorporate trustworthiness considerations in the design, development, deployment, and use of AI systems."[9] The Chamber highly encourages alignment with the NIST AI RMF, as the most appropriate framework for implementation and operationalization at scale throughout the U.S. This recommendation is consistent with the National Artificial Intelligence Advisory Committee, which calls for both supporting public and private adoption of the NIST AI RMF and internationalizing the NIST AI RMF in its May 2023 Report[10]. Additionally, companies within the financial services sector are utilizing the S-11-7/MRM[11] to help mitigate AI risks.

11. What lessons can be learned from accountability processes and policies in cybersecurity, privacy, finance, or other areas?

While many lessons have been learned regarding processes and policies for accountability in other subject matter areas, concerns continue to arise where processes are too prescriptive and do not provide the necessary flexibility to change and evolve along with the technology. Processes and policies around AI accountability should align with existing definitions, laws, and requirements (e.g., the HIPAA Materiality Standard, the NAIC cyber model, and the NY Cyber Model law on vendor oversight, and state fintech safe harbors and sandboxes). Within the financial sector, as stated before, there are risk frameworks such as SR-11-7/MRM to mitigate AI risks.

12. What aspects of the United States and global financial assurance systems provide useful and achievable models for AI accountability?

Financial institutions must participate in a complex and comprehensive regulatory framework that includes proactive supervision due to the risk associated with the use of technology within the sector. This model ensures that AI and other new technologies are implemented carefully and minimizes unintended consequences. Furthermore, financial institutions operate within a robust regulatory environment with strict compliance standards, paired with proactive regulatory supervision and examination to remediate risks *before* they can harm consumers.

Accountability Subjects

15. The AI value or supply chain is complex, often involving open source and proprietary products and downstream applications that are quite different from what AI system developers may initially have contemplated. Moreover, training data for AI systems may be acquired from multiple sources, including from the customer using the technology. Problems in AI systems may arise downstream at the deployment or customization stage or upstream during model development and data training.

The AI value chain is complex and evolving. Non-binding guidance or templates on developing contractual clauses on fairly sharing accountability efforts could be a valuable resource for the industry to

[8] https://www.nist.gov/itl/ai-risk-management-framework
[9] https://www.nist.gov/itl/ai-risk-management-framework/nist-ai-rmf-playbook
[10] https://www.ai.gov/wp-content/uploads/2023/05/NAIAC-Report-Year1.pdf#page=12&zoom=100,108,96
[11] https://www.federalreserve.gov/supervisionreg/srletters/sr1107.htm

draw upon. We would encourage NTIA to convene stakeholders through a multi-stakeholder process to help produce such model guidance or templates.

Accountability should also fall on those in the value chain that are responsible for and/or able to address the issues at the time they arise. Developers should not be able to completely shift the burden of accountability to deployers if the deployer is using the AI as intended and as instructed. Developers should be required to provide sufficient instructions on use to enable responsible use by deployer. Instructions must be sufficiently detailed to enable users to use the AI system appropriately, mitigate any known or reasonably foreseeable risks/bias (including appropriate techniques for processing data prior to ingestion to mitigate such bias), test for risk/bias, train individual users of the system, enable sufficient human oversight, and ensure continued compliance.

16. The lifecycle of any given AI system or component also presents distinct junctures for assessment, audit, and other measures. For example, in the case of bias, it has been shown that "[b]ias is prevalent in the assumptions about which data should be used, what AI models should be developed, where the AI system should be placed — or if AI is required at all." How should AI accountability mechanisms consider the AI lifecycle?

Companies and organizations should embed self-regulatory accountability mechanisms in all aspects of the AI lifecycle to measure and manage risks that arise at different stages within the lifecycle and implement appropriate risk mitigation measures. As previously indicated, it is vital to defer to different sectors as to the appropriate cadence for review. Each use case within each industry presents different levels of risk to consider.

Some industries already face explicit state statutory definitions of unfair discrimination, and regulators in those industries review conduct to ensure compliance with that standard. The McCarran-Ferguson Act enabled state insurance regulators to define unfair discrimination and prevents federal law from impairing, conflicting with or superseding that definition by creating a new legal standard.

Finally, to the extent that the federal and/or state governments consider algorithmic bias laws, they should encourage AI designers, developers, users, and deployers to test and mitigate disparities by including an affirmative defense where a defendant has self-tested and taken active steps towards remediation.

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?

The scope of risk should be focused on specific harm to individuals. The NIST AI Risk Management Framework sets an excellent example of how a model can be developed to guide and develop best practices around determining a calculated risk threshold.

18. Should AI systems be released with quality assurance certifications, especially if they are higher risk?

For higher-risk uses of the AI technology, it could be appropriate for the developer to release for out-of-package implementation some certification that explains the standards to which the entity that created the AI holds itself. Such certification would help promote explainability and minimize harmful impacts.

19. As governments at all levels increase their use of AI systems, what should the public expect in terms of audits and assessments of AI systems deployed as part of public programs? Should the accountability practices for AI systems deployed in the public sector differ from those used for private sector AI? How can government procurement practices help create a productive AI accountability ecosystem?

AI accountability looks different based on the sector in which it is implemented, and the specific use cases within each sector. It is vital to ensure that any accountability mechanisms created are flexible enough to support risk-based sector-by-sector and use case-by-use case approaches to compliance while still providing consistent consumer protections. Risk-based AI Accountability systems deployed as part of public programs should not differ from those used for private sector AI to maintain a broader ecosystem of trust in AI systems.

Accountability Inputs and Transparency

20. What sorts of records (*e.g.,* logs, versions, model selection, data selection) and other documentation should developers and deployers of AI systems keep in order to support AI accountability? How long should this documentation be retained? Are there design principles (including technical design) for AI systems that would foster accountability-by-design?

Specific to Generative AI uses, a list of inputs and outputs from the AI model can assist with accountability. Regarding Generative AI models, things such as the data sources, the algorithm's relative weights, changes to the model over time, and output results may all be essential records for organizations to keep for internal review. Such records and documentation may be helpful for critical internal reviews to ensure accountability. Conversely, data retention can potentially be problematic for companies and organizations, as holding onto such information can open them to data protection liabilities. Much of this information could be seen and likely be treated as propriety and not used for reporting requirements. Data retention can potentially be problematic for companies and organizations, as holding onto such information can open them to data protection liabilities. Also, data retention requirements under AI Accountability efforts may contradict data destruction and deletion requirements under current privacy laws.

21. What are the obstacles to the flow of information necessary for AI accountability either within an organization or to outside examiners? What policies might ease researcher and other third-party access to inputs necessary to conduct AI audits or assessments?

Potential problems for AI accountability within an organization include not having a full organizational buy-in on these accountability standards and processes. The Chamber highlighted in comments filed with NIST on their second draft of the AI Risk Management Framework that "[t]he ability for the RMF to be implemented successfully starts with ensuring that C suite level executives and others in the decision-making process

provide the necessary resources and backing needed for effective execution[12]." This comment highlights how important decision-makers at all organizational levels must be well-versed in frameworks such as the AI RMF, which can help mitigate potential issues.

Regarding inputs necessary for third-party access, industry stakeholders should engage with third parties and researchers on what specific requirements related to the disclosure of AI-driven systems may be needed, including, for instance, documentation of whether decisions were AI-generated and what information should not be shared with third parties to ensure proprietary information is protected.

22. How should the accountability process address data quality and data voids of different kinds? For example, in the context of automated employment decision tools, no historical data may be available for assessing the performance of a newly deployed, custom-built tool. For a tool deployed by other firms, there may be data a vendor has access to, but the audited firm itself lacks. In some cases, the vendor itself may have intentionally limited its own data collection and access for privacy and security purposes. How should AI accountability requirements or practices deal with these data issues? What should be the roles of government, civil society, and academia in providing useful data sets (synthetic or otherwise) to fill gaps and create equitable access to data?

Best practices for AI Accountability should be determined by industry stakeholders and adhere to industry-specific regulations and considerations. The requirements may include documentation, feasibility analysis reports, and a checklist for industry-specific considerations across the AI lifecycle.

Regarding data quality, the Chamber has long advocated for the government to prioritize access to government data and models. High-quality data is the lifeblood of developing new AI applications and tools, and poor data quality can heighten risks. Governments at all levels possess a significant amount of data that could be used to improve the training of AI systems and create novel applications. When the Chamber asked leading industry experts about the importance of government data, 61%[13] of respondents agreed that access to government data and models is essential. For this reason, the Chamber encourages policymakers to build upon the success of the OPEN Government Data Act by providing additional funding and oversight to expand the scope of the law to include non-sensitive government models as well as datasets at the state and local levels.

23. How should AI accountability "products" (*e.g.,* audit results) be communicated to different stakeholders? Should there be standardized reporting within a sector and/or across sectors? How should the translational work of communicating AI accountability results to affected people and communities be done and supported?

Many different sectors have their specific lexicon because each industry has explicit policies and laws which regulate it. This is one of the reasons why standardization and best practices at the sector-specific level may be necessary, as it is important to communicate such standardization in specific terms to allow that

---

[12] https://www.nist.gov/system/files/documents/2022/11/16/U.S.%20Chamber%20of%20Commerce_Technology%20Engagement%20Center%20%28C_TEC%29.pdf

[13] https://www2.deloitte.com/us/en/pages/consulting/articles/investing-in-ai-trust.html?nc=1

sector to adopt and comply. For this reason, if there is an overarching standard to be developed, it must be done flexibly to allow reporting to be done in a way that meaningfully translates to different specific sectors.

Barriers to Effective Accountability

25. Is the lack of a general federal data protection or privacy law a barrier to effective AI accountability?

C_TEC has strongly supported the need for a national data privacy law, as a 50-state patchwork is problematic and burdensome for the business community and consumers. A national data privacy law would help provide the business community with one set of rules and guidelines around data use. However, this is only the case if Congress looks to preempt state laws and provide one national standard.

Furthermore, a data privacy bill could have profound implications for effective AI accountability, as these systems are only as good as the data provided to them, so faulty data will lead to faulty algorithmic outputs. For this reason, we firmly believe that Congress must first enact a national privacy law before any legislative action is taken around AI, as such legislation will dictate many meaningful policies around artificial intelligence.

26. Is the lack of a federal law focused on AI systems a barrier to effective AI accountability?

AI Accountability is a nascent concept, but the business community and organizations have been at the forefront of creating AI accountability frameworks and addressing potential issues and will continue to manage and mitigate the potential impact associated with automated systems. Implementation of guidance from the NIST AI RMF is a critical resource to support these efforts. For this reason, it is important for Congress to fully fund NIST work around the AI RMF which will help support the agency's ability to work with the business community to develop specific guidance where there may be gaps in current law. We believe this provides the necessary consensus-based way to address and mitigate potential concerns.

27. What is the role of intellectual property rights, terms of service, contractual obligations, or other legal entitlements in fostering or impeding a robust AI accountability ecosystem? For example, do nondisclosure agreements or trade secret protections impede the assessment or audit of AI systems and processes? If so, what legal or policy developments are needed to ensure an effective accountability framework?

There is a robust discussion around what proprietary intellectual property ("IP") rights are involved with AI models and how those might need to be addressed in any AI accountability framework, including the U.S. Patent and Trademark Office's Proceeding on AI and Inventorship[1]. As noted earlier, multiple federal entities are engaged in processes to better understand and address challenges in the AI ecosystem. C-TEC encourages NTIA to engage with other federal entities and all relevant stakeholders to inform a streamlined, whole-of-government approach to considering these issues.

28. What do AI audits and assessments cost? Which entities should be expected to bear these costs? What are the possible consequences of AI accountability requirements that might impose significant costs on regulated

[1] https://www.federalregister.gov/documents/2023/02/14/2023-03066/request-for-comments-regarding-artificial-intelligence-and-inventorship

entities? Are there ways to reduce these costs? What are the best ways to consider costs in relation to benefits?

The entity that will end up bearing an AI audit or assessment cost will ultimately be the deployer and/or user of the system. While designers, developers, and/or vendors may be required to conduct audits and assessments before deploying them or making them available to clients for deployment, in the latter case, audit costs will be passed on to the client.

Audits and assessments can costs hundreds of thousands of dollars, which can be cost-prohibitive, especially for start-ups and small businesses that may not have the necessary capital and funding for such expenses. Such an inability to meet compliance costs may lead these organizations to merge with other companies or not enter the market, reducing the overall market size and potentially reducing innovation. For this reason, we continue to push for industry standards, which can assist in harmonizing responsibilities and reducing compliance costs.

AI Accountability Policies

30. What role should government policy have, if any, in the AI accountability ecosystem? For example: a. Should AI accountability policies and/or regulation be sectoral or horizontal, or some combination of the two?

As highlighted in a recent joint statement from the Department of Justice, Federal Trade Commission, Equal Employment Opportunity Commission, and the Consumer Finance Protection Bureau, OBJ many existing laws allow for necessary oversight to ensure the deployment of AI systems is accountable. It is essential for regulating agencies to act within the contours of the congressional authority they are afforded.

In addition to relying on existing laws where appropriate, the government can play a decisive role in the AI accountability ecosystem in multiple ways, such as supporting adoption of the NIST AI RMF and the evolution of the AI RMF as technology evolves, convening multistakeholder discussions, as well as developing and making available best practices and other voluntary resources to help mitigate potential issues around the deployment of AI. Furthermore, the government can play a crucial role in helping address the alignment of laws and cross-sectoral reporting requirements, to limit duplication, including with international laws. For this reason, we encourage reviews of such policies to reduce burdensome regulatory overlap.

31. What specific activities should the government fund to advance a strong AI accountability ecosystem? The federal government should take/play a leading role in strengthening the development and deployment of AI and encourage immediate action on the following recommendations:

- **First, the federal government should conduct fundamental research in trustworthy AI.** The federal government has played a significant role in building the foundation of emerging technologies through conducting and supporting fundamental research and development. AI is no different. A recent report from the U.S. Chamber Technology Center and the Deloitte AI Institute found significant support from U.S. business leaders for such public investment. Enactment of the CHIPS and Science Act was a positive step, as it authorizes $9 billion to NIST for Research and Development and advancing standards for “industries of the future,” including AI.

Furthermore, the Chamber has been a strong advocate for the National Artificial Intelligence Initiative Act, which developed the office of the National AI Initiative Office (NAIIO) to coordinate the Federal government's activities, including AI research, development, demonstration, and education and workforce development. The business community strongly urges Congress to appropriate these efforts fully.

- **Second, the Chamber encourages continued investment into Science, Technology, Engineering, and Math Education (STEM).** The U.S. Chamber earlier this year polled the American public on their perception of AI. The findings were clear; the more the public understands the technology, the more comfortable they become with its potential role in society. Education continues to be one of the keys to bolstering AI acceptance and enthusiasm as a lack of understanding of AI is the leading indicator for a push-back against AI adoption.

  The Chamber strongly supported the CHIPS and Science Act, which made many of these critical investments, including $200 million over five years to the National Science Foundation (NSF) for domestic workforce buildout to develop and manufacture chips, and $13 Billion to NSF for AI Scholarship-for-service. However, the authorization within the legislation is just the start; Congress should appropriate the funding for these important investments.

- **Third, the government should prioritize improving access to government data and models.** High-quality data is the lifeblood of developing new AI applications and tools, and poor data quality can heighten risks. Governments at all levels possess a significant amount of data that could be used to improve the training of AI systems and create novel applications. When the Chamber asked leading industry experts about the importance of government data, 61% of respondents agreed that access to government data and models is important. For this reason, the Chamber encourages agencies to open government data that can assist with the training.

- **Fourth, increase widespread access to shared computing resources**. In addition to high-quality data, the development of AI applications requires significant computing capacity. However, many small startups and academic institutions lack sufficient computing resources, which in turn prevents many stakeholders from fully accessing AI's potential. When the Chamber asked stakeholders within the business community about the importance of shared computing capacity, 42% of respondents supported encouraging shared computing resources to develop and train new AI models. Congress took a critical first step by enacting the National AI Research Resource Task Force Act of 2020. Now, the NSF and the White House's Office of Science and Technology Policy should fully implement the law and expeditiously develop a roadmap to unlock AI innovation across all stakeholders.

- **Fifth, enable open source tools and frameworks**. Ensuring the development of trustworthy AI will require significant collaboration between government, industry, academia, and other relevant stakeholders. One key method to facilitate collaboration is by encouraging the use of open source tools and frameworks to share best practices and approaches to trustworthy AI. An example of how this works in practice is the NIST AI RMF, which is a consensus-driven, cross-sector, and voluntary framework, akin to NIST's existing Cybersecurity Framework. Stakeholders can leverage the AI RMF as a best practice to mitigate risks posed by AI applications. Policymakers should recognize the

importance of these types of approaches and continue to support their development and implementation.

34. Is it important that there be uniformity of AI accountability requirements and/or practices across the United States? Across global jurisdictions? If so, is it important only within a sector or across sectors? What is the best way to achieve it? Alternatively, is harmonization or interoperability sufficient and what is the best way to achieve that?

The Chamber has long advocated for the need for industry-led, consensus-based standards that are at the heart of digital innovation, including AI technologies. The Chamber encourages policymakers to acknowledge and support the development of such measures in recognized international standards bodies and consortia. As for global companies, regulatory fractures across multiple jurisdictions created additional costs and reduced the ability for global companies to compete in these areas of emerging technologies, which is why we support harmonization with other regulatory frameworks, including promoting the NIST AI RMF internationally.

Conclusion:

In conclusion, the Chamber appreciates the opportunity to provide input on the AI Accountability request for comment issued by the National Telecommunications and Information Administration (NTIA). As an organization committed to fostering innovation, economic growth, and ethical practices the Chamber recognizes the importance of addressing the challenges and opportunities presented by AI. Fostering collaboration between industry, government, academia, and civil society can create an environment that encourages responsible AI development, deployment, and usage. The U.S. Chamber stands ready to engage in ongoing discussions and initiatives to advance AI accountability and ensure the United States remains at the forefront of AI innovation while upholding solid ethical principles.

Sincerely,

Michael Richards
Director, Policy
Chamber Technology Engagement Center