U.S. Senate AI Insight Forum: High Impact AI

Written Statement of
Jason Oxman
President and CEO
Information Technology Industry Council (ITI)

November 1, 2023

Leader Schumer, Senator Rounds, Senator Heinrich, Senator Young, and distinguished members of the U.S. Senate, thank you for the opportunity to discuss ITI's views on artificial intelligence (AI) that relate to high-impact uses and how our members are mitigating potential harms and risks associated with AI.

My name is Jason Oxman, and I am the President and CEO of the Information Technology Industry Council (ITI). ITI is the premier advocate and thought leader in the United States and around the world for the information and communications technology (ICT) industry. We represent leading companies from across the ICT sector, including hardware, software, digital services, semiconductor, network equipment, cybersecurity, Internet companies, and other organizations using data and technology to evolve their businesses. ITI's advocacy efforts help shape technology policy around the globe and enable secure innovation, competition, and economic growth, while supporting governments' efforts to achieve their public policy objectives. Our members stand at the forefront in developing and deploying consumer-facing, business-to-business, and government-focused AI solutions. In fact, AI is a priority technology area for nearly all ITI members as they leverage this technology to evolve their businesses and benefit consumers. As such, we are committed to the responsible development and deployment of AI technologies and have been deeply engaged with policymakers globally as they determine the most appropriate approach to AI governance and regulation.

ITI's WORK ON AI

AI's transformational impact is being felt across all sectors, including financial services and health care, and AI has increased U.S. economic growth, facilitated economic opportunities for businesses of all sizes, and enabled the U.S. to deepen cooperation with allies and remain competitive with other nations also spearheading AI development and deployment.[1] As the global trade association specializing in advocacy and public policy development on behalf of the technology sector, ITI has helped advance the international debate on how to promote and govern the responsible and transparent development and use of AI technologies. Examples of ITI's AI thought leadership and policy principles include:

- Policy paper entitled, *Understanding Foundation Models & The AI Value Chain: ITI's Comprehensive Policy Guide.* This policy paper outlines the role foundation models play in the AI ecosystem, how Large Language Models (LLMs) and generative AI relate to foundation models, and how policymakers and AI stakeholders can manage associated risks, among other areas.

[1] See McKinsey and Company, The Economic Potential of Generative AI: The Next Productivity Frontier (June 2023), which states that: "the total global economic benefits of AI in the years ahead, which now includes the impact of generative AI, range from $14 trillion to $25 trillion."

- Policy paper entitled, *Policy Principles for Enabling Transparency of AI Systems.* This policy paper underscores that transparency is a critical part of developing accountable and trustworthy AI systems and avoiding unintended outcomes or other harmful impacts. It offers a series of recommendations to policymakers seeking to develop legislative or regulatory approaches to transparency, encouraging them to consider the objective of transparency requirements, take a risk-based approach, and ensuring that any requirements keep in mind the need to protect sensitive IP and source code, among others.
- Written Testimony submitted to the U.S. Senate Committee on Commerce, Science & Transportation Subcommittee on Consumer Protection, Product Safety and Data Security. The September 2023 hearing entitled, *The Need for Transparency in Artificial Intelligence.* In his written testimony, ITI's Executive Vice President of Global Policy Rob Strayer identified the following areas of focus for Congress to support a pro-innovation agenda that harnesses AI's potential and mitigates risk:
    - Support AI innovation, investment, and industrial policy that builds off the success of *The CHIPS & Science Act* and other related laws.
    - Legislation should be risk-based, evaluate the existing regulatory landscape, and clearly delineate risk areas that are not adequately addressed.
    - How AI developers and deployers can help foster public trust in AI technology.
    - Rely upon globally-recognized international standards.
- ITI's written response to an April 2023 letter authored by Senators Hickenlooper (D-CO) and Blackburn (R-TN), which requested that ITI detail how companies are operationalizing the National Institute of Standards and Technology (NIST) AI Risk Management Framework (AI RMF).

ITI's RECOMMENDATIONS FOR HIGH-IMPACT USES

In seeking to advance a pro-innovation AI policy agenda, it is important that Congress work with stakeholders to clearly delineate the risks and negative impacts that need to be addressed within a regulatory framework. As AI will continue to evolve, any regulatory approach will need to be flexible and future-proof in order to address risks and impacts on individuals as they develop AI, while avoiding hindering the advancement of beneficial applications of AI. With that in mind, we offer the following recommendations to mitigate risk stemming from high impact uses:

1. Follow a risk-based approach that adequately covers "high-impact" use cases and applications – not entire classes of AI technology systems or sectors of the economy.

Risks need to be identified and mitigated in the context of the specific AI use. This will help policymakers determine use cases or applications that are of particular concern, avoiding overly prescriptive approaches that may serve to stifle innovation. Regulatory approaches that leverage an overly broad definition of AI, that do not take a risk-based approach, and that mandate overly prescriptive requirements will stymie innovation. Regulation that designates entire classes of technology as high-risk or high-impact, or that designates entire sectors of the economy as such, misses important nuance and may impact many low-risk and low-impact uses of the technology.

When scoping high-impact uses, below are suggestions of how Congress might appropriately capture these use cases without hindering future innovation:

- A baseline definition of "high-impact AI" or "high-risk AI" should cover uses wherein the outcome of an AI system's decision has the potential to cause harm or materially impact an individual's access to goods and services and other matters that pose a significant risk to fundamental human, civil, and constitutional rights.[2]

- When examining high-impact uses that apply to critical infrastructure protection, it is important to carefully consider how applicable U.S. statutes can inadvertently lead to blanketing entire sectors as high-risk. To avoid prescriptive risk classification for high-impact uses of AI that apply to the operation of critical infrastructure, we recommend tailored definitions that cover AI systems intended to be used as safety components in the management and operations of road traffic and the supply of water, gas, heating and electricity, since their failure or malfunctioning may put at risk the life and health of persons at large scale and lead to appreciable disruptions in the ordinary conduct of social and economic activities.

2. <u>Evaluate the existing legal, policy and regulatory landscape.</u>

As an initial step, policymakers should evaluate how the NIST AI RMF is being adopted and how it can be used to manage risk. The AI RMF provides companies with a comprehensive way to think about risk management practices, which is fundamental to fostering long-term public trust. With those risks identified, the next step is to consider the role for existing statutory and regulatory authorities to address discrete risk. We do not want layers of regulation that conflict with one another, create undue burdens on innovators, and slow advancement. Therefore, it is imperative that Congress review the existing regulatory landscape to assess gaps that may exist. There are existing laws and regulatory frameworks that can address AI-related risks, so it is critical to understand how those laws apply, and where they may not be fit-for-purpose, prior to creating new legislation or regulatory frameworks pertaining to AI.[3] Below are some examples of existing policies and frameworks that apply to the use of AI in the healthcare and financial services sectors:

- *Healthcare:* **<u>U.S. Food and Drug Administration (FDA) Risk Management Framework for Medical Device Equipment:</u>** By analyzing large amounts of data in real time, AI can help improve clinical and nonclinical decision making, reduce medical variability, and optimize staffing. The FDA is already regulating AI in medical devices effectively.[4] Specifically, the FDA ensures that the AI devices it reviews are safe and effective before they are released, and places requirements on manufacturers to track the products already on the market so they maintain safety and effectiveness. Examples include adverse

[2] However, to align with international AI legislation that is approaching the final stages of legislative consideration, we recommend that Congress consider legislating based on "risk" versus "impact." This approach will ensure greater harmonization for companies that develop, deploy and adopt AI technologies in global markets.

[3] For example, some of these relevant bodies of law and regulation, coupled with relevant potential AI-related harms, include: 1) intellectual property law, especially the Copyright Act of 1976, to address issues related to the use of copyrighted material in training data and questions regarding the IP rights in AI generated content; 2) the Federal Trade Commission Act to address unfair, deceptive or abusive practices related to AI-enabled misrepresentations or harmful content; 3) product liability common law to address potential safety issues related to products containing AI technology that may cause physical injury; 4) First Amendment jurisprudence and Section 230 of the Communications Decency Act to address issues related to AI-generated content and freedom of expression interests; 5) Title VII of the Civil Rights Act of 1964 and related laws to address issues related to bias, discrimination, or other civil rights harms; and 6) relevant federal sector-specific privacy provisions, such as in the Health Insurance Portability and Accountability Act, to address potential privacy harms related to AI that include the accuracy of data.

[4] See FDA Guidance entitled, *Factors to Consider Regarding Benefit Risk in Medical Device Product Availability, Compliance, and Enforcement Decisions* (Dec. 2016), available here.

event reporting, device tracking which helps identify and address any potential safety issue, post-market surveillance, and labeling.

- *Financial Services:* **The U.S. Federal Reserve (Fed) and Office of the Comptroller of the Currency (OCC) *Supervisory Guidance on Model Risk Management*:** Banks and other financial institutions have long relied on quantitative methods and modeling to produce statistical, economic, and financial analysis as mechanisms to assess the solvency of a financial organization. AI technologies are increasingly being adopted by financial institutions to aggregate financial models, forecasts, and vast amounts of data more efficiently and effectively. To keep pace with advances in financial modeling, the Fed and OCC jointly released the *Supervisory Guidance on Model Risk Management* (SR 11-7), a framework designed for use by banking organizations and supervisors as they assess organizations' management of model risk. Financial organizations that leverage AI for predictive modeling can align their risk management practices with SR 11-7.

3. Allocate responsibilities proportionately between different stakeholders in the AI value chain, including developers and deployers.

With the wide adoption and integration of foundation models into various deployments, including potential high-risk use cases, it is important to appropriately delineate responsibilities of developers and deployers in the value chain. In many instances, the developer of a foundation model will not have concrete insight into the ultimate use case of the model. At the same time, the deployer will often require documentation and tools from the developer in order to support their own understanding of and control of the model they seek to leverage. Moreover, AI developers and deployers play an essential yet distinct role in mitigating potential harms:

- **A developer** (sometimes also called a "producer") is the entity that is producing the foundation model. The developer of a foundation model is in control of certain information and decisions, e.g., how the model's training data is selected and used, what kind of testing and validation is performed on the model, etc. Accordingly, **developers are best positioned to manage model-level risks and understand the capabilities and limitations of a particular model**. In many instances, the foundation model can be built into other products that are then deployed by a different entity.
- **A deployer** (sometimes also called a "provider") is the entity that is deciding the means by and purpose for which the foundation model is ultimately being used and puts the broader AI system into operation. Deployers often have a direct relationship with the consumer, including a hospital or a bank. While developers are best positioned to assess, to the best of their ability, and document the capabilities and limitations of a model, **deployers, when equipped with necessary information from developers, are best positioned to document and assess risks associated with a specific use case.**

CONCLUSION

ITI and our member companies appreciate the Senate's continued attention to this matter and its work to convene educational forums for members of Congress to understand AI and its implications. We share the U.S. Senate's goal in equipping members of Congress with the tools and expertise needed to advance meaningful legislation that encourages future AI innovative and investment in the United States while mitigating real risks to consumers and businesses alike. This is a highly complex issue that impacts nearly every business sector, and the government's role should be limited to addressing critical risks in specific use cases. Where those risks are identified, Congress should evaluate the existing legal, policy and regulatory landscape, and clearly delineate risk areas that are not adequately addressed. Future requirements should be aligned with international consensus standards wherever possible to ensure that risk management is effective and to harmonize the global marketplace for technology.