Written Testimony of

Courtney Lang

Vice President of Policy, Trust, Data, and Technology

Information Technology Industry Council (ITI)

Before the

United States House Committee on

Energy & Commerce

Subcommittee on Communications and Technology

Hearing on

Leveraging AI to Enhance American Communications

November 14, 2023

Chairman Latta, Ranking Member Matsui, and Chairwoman McMorris Rodgers and Ranking Member Pallone, thank you for the opportunity to testify today.

My name is Courtney Lang, and I'm the Vice President of Policy for Trust, Data and Technology at the Information Technology Industry Council (ITI). I lead ITI's global Artificial Intelligence (AI) policy portfolio, where I focus on advancing the responsible development and use of AI globally. As a part of this, I direct ITI's AI Futures Initiative, which is a group comprised of ITI member company technical and policy experts that are focused on proactively addressing policy questions emerging around AI. I also manage our cybersecurity policy portfolio, including as it relates to AI and have been very engaged in international conversations around the cybersecurity implications of AI. 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. Our members stand at the forefront in developing and deploying consumer-facing, business-to-business, and government-focused solutions, including AI technologies that enable cybersecurity professionals to detect adversarial cyber threats and telecommunication operators to efficiently map broadband networks to unserved rural areas.

We are encouraged by the bipartisan efforts in Congress and the Energy and Commerce Committee to address the opportunities, as well as the challenges, related to AI. This Committee's jurisdiction over issues ranging from data privacy, spectrum availability, and network security gives you an important role to play in AI policy discussions. Congress and the Administration should work together to ensure any legislation or regulatory proposals encourage future innovation and investment in the United States and allied markets, protect consumers and businesses, mitigate foreseeable risks, and do not complicate or duplicate existing standards, laws, and sector-specific policies and frameworks. ITI looks forward to being a contributing stakeholder in those efforts.

I. ITI's Response to the Administration's Executive Order (EO) on Safe, Secure, and Trustworthy Artificial Intelligence

The Biden Administration's long-awaited AI EO takes a whole-of-government approach to advance a sector-specific vision of AI governance, which includes directives for sector-specific agencies and independent regulators to evaluate the use of AI within their sectors and to develop guidance as appropriate. We are supportive of the fact that the Administration attempted to balance the need to support innovation and competition with its desire to foster greater accountability. This balance is incredibly important to strike, especially because as of late, significant emphasis has been placed on accountability, with less focus on innovation. Both are needed to advance a realistic policy framework. While we are supportive of the Administration advancing responsible AI policymaking, Congress has an essential role to play in encouraging future innovation and investment in the United States, protecting consumers and businesses, and mitigating foreseeable risks. Regarding the EO's provisions and requirements, below are several sections that are of immediate relevance to ITI and its members:

- *National AI Research Resource* – We support the NSF's pilot program that would implement elements of the National AI Research Resource (NAIRR).

- *DOD & DHS Pilot Program* – The pilot program that DOD & DHS are directed to establish focused on using AI to detect and fix vulnerabilities in critical USG software and systems demonstrates the cybersecurity benefits that AI can enable.
- *International Leadership* – It is helpful that the EO recognizes the instrumental role that the U.S. can and should play in advancing a vision of responsible AI around the globe.
- *Use of Defense Production Act & Disclosure Obligations* – At the same time, we have questions regarding several of the areas in the Executive Order, including invoking the Defense Production Act to levy disclosure obligations directly on dual-use foundation model providers and owners (or potential owners) of computer clusters. The EO directs companies to provide specific types of information to the Federal Government, which may include sensitive and/or proprietary information about their technologies. However, as drafted, the EO leaves significant questions unaddressed, which we believe need to be answered in order to better understand the scope of the requirements, including who within the Commerce Department is collecting the information, for what purpose, and how the information will be protected.
- *Equating Compute Power with Risk* – By defining and levying obligations on dual use foundation models, the Executive Order suggests that models of a certain compute power/compute capacity are riskier than other types of models. It is not clear to us that compute power is necessarily an indicator of risk. We urge the Commerce Department, the agency tasked with promulgating the technical parameters for a dual-use foundation model, to further delineate what specific risks are that the obligations are seeking to address.

II. <u>Impact of AI in Telecommunications & Cybersecurity</u>

The development and adoption of AI technologies will help companies of all sizes that rely on cyber protections and communication networks become more effective and efficient, particularly at addressing business operations challenges, research and development, and software engineering.

In fact, an Accenture survey of 1,500 executives across all sectors found that 84 percent believed AI is critical to meeting their growth objectives and 73 percent said they risk going out of business if they cannot scale AI.[1] As a testament to AI's revolutionary impact, credible estimates of 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.[2] According to Allied Market Research, the global AI in telecommunication market size is projected to reach $38.8 billion by 2031.[3]

Today, the United States is leading AI development, deployment, and innovation. The United States employs the best and the brightest AI researchers and experts working to advance American leadership in AI innovation. Other nations have recognized the United States as the center for AI excellence and are

[1] See Accenture AI investment study (November 14, 2019), available at https://www.accenture.com/usen/insights/artificial-intelligence/ai-investments

[2] See McKinsey and Company study, *The Economic Potential of Generative AI: The Next Productivity Frontier* (June 2023), available at https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/the%20economic%20potential%20of%20generative%20ai%20the%20next%20productivity%20frontier/the-economic-potential-of-generative-ai-the-next-productivity-frontier-vf.pdf?shouldIndex=false

[3] Kashinath G, Vineet K, Allied Market Research study, *AI in Telecommunication Market Research, 2031* (September 2023)

working harder than ever to develop the next major technological developments in AI and to deploy AI in new use cases in their countries.

AI will play an essential role in future national security applications for the military and intelligence communities and in the cybersecurity defense of critical infrastructure and high-priority telecommunication networks. It is not an exaggeration to say that U.S. national security depends on continued U.S. technological leadership in AI. It is more important than ever that the United States considers how any new policy affecting AI will help it maintain its technological leadership. Regarding AI's role in the telecommunications sector and cybersecurity applications, below are some of the use cases that AI will empower:

- **Cybersecurity**
  - *Threat Mitigation*: AI and machine learning can be leveraged to improve cybersecurity. Indeed, defensive cybersecurity technology is embracing machine learning and AI as part of the ongoing battle between attackers and defenders. The threat landscape is constantly evolving, with cyberattacks becoming more complex and increasingly leveraging automation. Attackers continually improve their sophisticated and highly automated methods, moving throughout networks to evade detection. The cybersecurity industry is innovating in response: making breakthroughs in machine learning and AI to detect and block the most sophisticated malware, network intrusions, phishing attempts, and many more threats. AI is the best tool defenders have to identify and prevent zero-day attacks and malware-free attacks because AI can defeat novel threats based on behavior cues rather than known signatures. Leveraging these technologies is essential to meeting constantly evolving threats.
  - *Network Security*: AI can monitor network traffic, detect anomalies, and identify potential cybersecurity threats. AI algorithms can analyze patterns, identify malicious activities, and take immediate action to protect the network and customer data from cyberattacks.

- **Telecommunications**
  - *Broadband Mapping*: AI-based mapping systems can not only utilize US Census Bureau data, but can also convert satellite images into real-world features to develop a map of broadband serviceable locations that can help identify communities that previous mapping models missed. More accurate mapping strategies can also assist in network deployment, which helps in determining optimal tower locations, estimate coverage areas, and predict network capacity requirements; thus, enabling providers to make informed decisions during network expansion.
  - *5G and AI:* 5G is propelling the rapid proliferation of intelligent devices and services, with more than 1.5B connections globally. The rise of AI not only transforms mobile experiences, including improved camera quality and predictive texting, but also brings a unique opportunity to revolutionize the future of wireless communications. For future evolutions in cellular networks, AI can help optimize system energy saving, network load balancing and device mobility management.
  - *Spectral Efficiency:* One of the most interesting examples is an AI-powered feature to increase spectral efficiency. Spectrum is among the biggest asset expenses facing

communication service providers, and as such, increasing the efficiency of its utilization represents a very high value use case. Initial demonstrations of using AI to adapt the modulation and coding scheme, have shown gains in spectral efficiency of roughly 10 percent, depending on the scenario.

- *Self-Healing Networks:* These networks are equipped with inherent features designed to safeguard against disruptions by anticipating issues, offering solutions or alternatives, facilitating recovery, and averting future incidents The paradigm shift to software-defined infrastructure transformed network automation from basic redundancies and back-ups in the event of an outage to the ability to analyze traffic patterns, density, and sensor input from real time and historical data to enhance visibility and automate remediation of network problems. AI and ML technologies can also be paired with digital twins to test network changes before deployment. Self-healing capabilities enable networks to forecast whether latency service levels meet the criteria for autonomous vehicles to effectively monitor pedestrians and cyclists, ensuring seamless autonomous driving, or, in cases of insufficient conditions, trigger a return to driver control.
- *Spam/Fraud Detection:* AI can play a pivotal role in real time analysis of extensive data to identify and proactively thwart various types of fraudulent activities beyond call spoofing, including SIM-swapping, unauthorized network access, counterfeit profiles, and billing fraud. AI and machine learning can be used to identify unusual patterns and anomalous behavior to flag suspicious activity and identify fraud, possibly preventing consumer harm even before it starts.

As evidenced by the above examples, AI has the potential to significantly improve applications in both the telecommunications and cybersecurity contexts and play a transformative role for society more broadly. At the same time, ITI recognizes that there are key questions that are emerging in the AI policy conversation, including related to privacy, accountability and transparency, and that there is increasing interest on the part of legislators in figuring out how to best address risks related to AI. ITI's AI policy framework is therefore focused on both supporting innovation and investment, as well as mitigating risks. Below, I will discuss several key pillars of our AI policy approach, with a particular emphasis on how they apply in the telecommunications and cybersecurity context. Such pillars include: fostering innovation and investment in key sectors and applications, how a risk-based approach applies to cybersecurity and telecommunication sectors, ensuring security and privacy, and how the proportionate responsibilities allocated between AI developers and deployers will impact cybersecurity and telecommunication uses.

III. The United States and Congress should follow an approach to AI policy that balances innovation with risk management

a. The United States should ensure that its approach to AI policy appropriately recognizes and supports the role of innovation and investment in order to realize applications in both the telecoms and cybersecurity sector and advance key risk management practices.

While a significant part of the policy conversation has been focused on addressing risks, commensurate attention should be given to the ways in which policy levers can support innovation, advance helpful applications of AI, and progress the research and development needed to implement risk management practices. Congress and the U.S. government should advance efforts to stand up infrastructure needed to support high-performance computing, data centers, and other hybrid environments:

- We support efforts to establish opportunities and resources for companies of all sizes to partner with federal research centers focused on AI R&D, including the National AI Research Resource (NAIRR). Specifically, ITI supports H.R. 5077, the CREATE AI Act, bipartisan legislation that is supported by several members of this Subcommittee, as well as the Executive Order's direction to the National Science Foundation, in conjunction with other Federal agencies, to pilot the NAIRR, aligned with the recommendations of the NAIRR Task Force.[4]
- This infrastructure will be critical to advancing research and development (R&D) in the broader community, including related to applications in both telecommunications and cybersecurity.
- The United States also needs a forward-looking national spectrum strategy to unleash the benefits of next generation wireless networks, including AI applications. As a first step, we urge Congress to restore the FCC's spectrum auction authority, and we applaud the Committee's leadership in advancing legislation to reinstate this key tool for American spectrum leadership.

In order to supplement contributions by the private sector, **Congress and the U.S. government should provide the necessary resources and incentives for R&D activity, including that taking place at National Labs, in the private sector, and beyond.** Private sector stakeholders and academics are undertaking R&D to progress privacy enhancing technologies (PETs) and advance Academics and private sector stakeholders are conducting research and development to progress privacy enhancing technologies (PETs) and advance measurement science to test, evaluate, validate, and verify (TEVV) model performance. Testing and evaluation metrics are especially important in effectively and consistently implementing risk management practices across organizations. Innovations in measurement tools for AI will make risk management more concrete and objective and improve accountability and transparency. The National Institute of Standards and Technology (NIST) will play an increasingly important role in convening stakeholders to develop these metrics, guidelines, and best practices, especially in light of the recent Executive Order. For example, NIST is charged with developing a companion document to its AI Risk Management Framework focused on Generative AI, on developing a secure software development framework specific to generative AI and foundation models, creating

[4] H.R. 5077, the Creating Resources for Every American to Experiment with Artificial Intelligence Act of 2023, available here: https://www.congress.gov/bill/118th-congress/house-bill/5077; Sec. 5.2 *Promoting Innovation,* of Executive Order 14110 instructs that within 90 days of the EO, Federal agencies that the Director of NSF deems appropriate are directed to launch a pilot program to implement the National AI Research Resource (NAIRR) .

guidance to help with evaluating and auditing AI systems, and establishing red-teaming guidelines for foundation models. All of these activities are critical to operationalizing AI risk management activities.

As such, the U.S. government should fund additional R&D focused on supporting these activities to advance a strong AI accountability ecosystem. In its AI RMF Roadmap, NIST indicates that additional efforts are needed in this space in order to develop meaningful benchmarks to evaluate risk and trustworthiness.[5] Public-private research opportunities and AI pilot programs would also be valuable mechanisms for facilitating accountability, collaboration, transparency, and trust across the AI ecosystem, including in the telecommunications and cybersecurity contexts.

b. The United States should follow a risk-based approach to AI regulation, encouraging the adoption of risk-based governance frameworks.

A risk-based approach supports innovation. **Policymakers should work with stakeholders to determine concrete risks that they are hoping to address by instituting specific obligations**. Concrete, evidence-based risk assessments can serve to support the creation of thoughtful policy that is targeted at those uses that present the greatest risk, allowing innovation to continue in those areas that pose little or no risk.

Importantly, in the telecommunications and cybersecurity sectors, automation and machine-learning have been used for years (and in some cases decades) to perform certain tasks. The use of AI systems should therefore not be viewed as the introduction of entirely new technology, **but as an evolution of existing technology**. For example, cybersecurity risks are something that telecom operators are already considering with present networks and one of the reasons for the proliferation of basic encryption standards such as "https."

As AI is integrated more robustly into telecommunications networks, it is true that the AI system itself could become an additional target of an adversary, but this additional threat vector does not require an entire overhaul of existing cybersecurity risk management practices. Instead, it requires that operators integrate considerations around AI into existing risk management approaches.

Additionally, reliability is an important consideration in the context of critical infrastructure assets, including telecommunications networks. As such, the introduction of AI can introduce distinct risk in that a failure or disruption of the AI system could have widespread consequences with regard to both availability and reliability. However, properly maintained, protected and deployed AI can enhance reliability in instances where there is an outage caused by downed equipment or power stations. Additionally, in the same way that current telecom networks face supply chain risk, so will networks that incorporate AI systems or components.

In thinking through risks specific to the communications sector, Congress should keep the above in mind. **In crafting specific policy, we discourage classifying entire sectors as high-risk. Blanketing entire sectors with requirements is not proportionate and misses important nuance**. For example, there has been interest in designating AI used in "critical infrastructure" as high-risk, but this would be too broad and complicate the ability of critical infrastructure owners and operators, including in the

[5] National Institute of Standards and Technology. (2023, January 26). *Roadmap for the NIST Artificial Intelligence Risk Management Framework* (AI RMF 1.0). Retrieved from https://www.nist.gov/itl/ai-risk-management-framework/roadmap-nist-artificial-intelligence-risk-management-framework-ai

communications sector, to apply AI in many low-risk use cases. It is more appropriate to designate particular AI components used for safety functions in critical infrastructure as high-risk, than to classify entire critical infrastructure sectors as high-risk.

Second, **policymakers should evaluate the existing legal and policy landscape in the United States, taking into account existing laws that may already protect against identified risks**. 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. The Executive Order seeks to further this approach to some extent, directing individual agencies to assess the use of AI within their specific sectors and jurisdictions. **We believe a sector-specific approach is most appropriate, given agencies have unique expertise in their areas of jurisdiction and can most effectively understand the unique risks that may stem from the use of AI in their sectors.** For example, the Telephone Consumer Protection Act (TCPA) allows the FCC to address risks to consumers related to robocalls and robotexts.[6]

Third, **in seeking to support a risk-based approach Congress should encourage the adoption of risk-based governance practices and frameworks, such as NIST's AI Risk Management Framework.** The AI RMF provides companies with a comprehensive way to think about risk management practices, which is fundamental to fostering long-term public trust. It captures many of the outcomes and best practices that companies are already undertaking, such as framing and prioritizing risks and addressing AI trustworthiness characteristics (e.g., reliability, safety, explainability, privacy, fairness, accountability, and transparency). ITI and its member companies were active in the development of this Framework and are actively adopting it. We appreciate that NIST has also launched the AI RMF Playbook as a complement to the AI RMF. Indeed, this tool is instrumental to ensuring that the Framework is actionable and implementable, particularly for organizations that may be less familiar with the scope of guidelines and best practices that are available to them. We have previously encouraged the Administration to explore how the AI RMF might be integrated into federal contracts and encouraged the government to leverage the AI RMF in crafting OMB guidance.[7] Therefore, ITI and its members were pleased to see the AI RMF referenced throughout the recent Executive Order, as well as the continuing involvement of NIST in progressing the uptake of the AI RMF. In high-risk settings, it is reasonable to expect organizations to undertake a baseline set of practices aimed at mitigating risk, many of which are outlined in the AI RMF.

[6] Some of these relevant bodies of law and regulation, coupled with relevant potential AI-related harms, include: 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; the Federal Trade Commission Act to address unfair, deceptive or abusive practices related to AI-enabled misrepresentations or harmful content; product liability common law to address potential safety issues related to products containing AI technology that may cause physical injury; First Amendment jurisprudence and Section 230 of the Communications Decency Act to address issues related to AI-generated content and freedom of expression interests; 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 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. In our view, it makes sense to proceed with creating new legislation only if there is a specific harm or risk where existing legal frameworks are either determined to be insufficient or do not exist.

[7] See ITI's Response to Office of Science and Technology Policy *Request for Information on National Priorities for AI* (July 7, 2023), available here: https://www.itic.org/documents/artificial-intelligence/ITIResponsetoOSTPRFIonNationalAIPrioritiesFINAL%5B25%5D.pdf

c. **The United States should ensure that its AI policy approach appropriately reflects the roles of various stakeholders in the AI value chain, including developers and deployers of the technology.**

In seeking to advance a risk-based approach, Congress should ensure that legislation appropriately reflects the role of different stakeholders in the AI value chain. We explore this further in our paper on *Understanding Foundation Models and the AI Value Chain*.[8] There are multiple stakeholders in the AI value chain that each play a role in the development and deployment of AI in a responsible manner. In thinking through appropriate obligations and/or responsibilities in legislation, policymakers should ensure they are allocated among actors based on their role and function in the AI value chain and recognize that risk management is a shared responsibility. While we believe that all organizations in the value chain should adopt practices focused on driving accountability, specific tools, mechanisms, practices, or obligations should be scoped based on the level of risk posed and relevant context, as outlined above.

Further, with the wide adoption and integration of foundation models into various deployments, including 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. In some cases, the developer and the deployer will be the same organization. Moreover, AI developers and deployers play an essential yet distinct role in mitigating potential harms:

- A developer is the entity that is producing the foundation model, such as LlaMa 2 or GPT-4. 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 is built into other products that are then deployed by a different entity.

- A deployer is the entity that decides 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. 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.

To provide an illustrative example applicable to cybersecurity, a foundation model developer may create a model that is then integrated by a cybersecurity provider into their offerings. The developer should provide information to the deployer about the model – for example, its limitations and capabilities, and identified risks and mitigation steps – to allow the deployer to understand its functionality, perform fine-tuning, and make an informed decision about whether and how to leverage the model. The deployer

[8] Our policy paper *Understanding Foundational Models and the AI Value Chain* is available here: https://www.itic.org/documents/artificial-intelligence/ITI_AIPolicyPrinciples_080323.pdf

would then also undertake relevant risk management practices; for example, undertaking a risk or an impact assessment.

d. The United States' AI policy approach should seek to facilitate public trust in the technology.

The overarching goal of an AI policy or regulatory framework should be fostering public trust in AI technology. Fostering trust in AI systems requires AI model developers, deployers, and policymakers to collaborate. Transparency is a key means by which to achieve that trust. To support those efforts, ITI developed AI Transparency Policy Principles, which offer recommendations to policymakers on how best to think about transparency, including considering the objective of and intended audience for transparency requirements, targeting transparency requirements to level of risk, considering the role that disclosure plays.[9]

ITI members are actively taking steps to build and deploy safe and transparent AI systems. While transparency can take different forms, our companies are working to ensure that users understand when they are interacting with an AI system and, broadly, how that system works. For example, several of our member companies provide information about an AI system via model or system cards.

ITI members are also undertaking efforts to advance content authentication in light of concerns related to mis- and disinformation. Several of our members are engaged in C2PA, a consortium focused on developing technical standards to support content provenance.[10]

Innovation is key to advancing these efforts. Congress should therefore avoid creating rigid regulations that mandate the use of one technique over another, as techniques for AI content authentication are still evolving. While there are several promising methods of content authentication, additional R&D is needed before definitive recommendations can be made as to which one is most effective; it may be that multiple techniques are appropriate for a given AI output.

Consistent with our AI Transparency Policy Principles, we believe that consumer awareness of AI-generated content is important, but it is equally important that they are equipped with an understanding of the tools available for verification. **Congress should therefore work with industry and other stakeholders to support consumer education initiatives to enhance consumer digital literacy and allow the public to better determine when content is AI-generated.**

e. The United States should ensure that its AI policy approach protects privacy and bolsters cybersecurity.

Cybersecurity and privacy are fundamental to advancing the responsible development and deployment of AI systems and are key characteristics of trustworthy AI systems. There are several ways in which privacy and cybersecurity interact with AI. First, AI can enhance cybersecurity, as referenced above. Second, as the government considers its approach to AI, it should focus on supporting the deployment

[9] See ITI's Policy Principles for Enabling Transparency of AI Systems, https://www.itic.org/documents/artificialintelligence/ITIsPolicyPrinciplesforEnablingTransparencyofAISystems2022.pdf

[10] The Coalition for Content Provenance and Authenticity (C2PA) is a Joint Development Foundation project that brings together the efforts of the Content Authenticity Initiative (CAI) and Project Origin. Additional information is available here: https://c2pa.org/

of secure AI systems. Third, users need to trust that any personal and/or sensitive data used by AI systems is appropriately protected and handled.

In seeking to bolster cybersecurity, **Congress should ensure that a policy framework supports the use of AI for cybersecurity purposes and also reflects the need to develop and deploy secure AI.** As referenced above, the integration of AI will not necessarily require a wholesale change to cybersecurity risk management processes, but rather will require organizations to consider AI in their existing cybersecurity risk management processes and ensure that they are accounting for AI-specific risks. In this way, maintaining a commitment to secure-by-default practices is critical.

At the same time, there are unique risks that AI may present in a cybersecurity context, including related to data poisoning, prompt injection attacks, and the extraction of confidential information from training data. ITI is therefore pleased to see that as a part of the recent Executive Order, NIST has been tasked with developing a secure software development framework to focus on generative AI and foundation models, especially as NIST's existing Secure Software Development Framework (SSDF) has been an important tool for organizations in thinking through secure software development processes. Additional ongoing cybersecurity efforts pursuant to Executive Order 14028 and the National Cyber Strategy will also help continue to bolster software security, and therefore, AI security.

With regard to protecting users' sensitive data, there is a clear regulatory gap given the absence of federal privacy legislation. ITI testified before this Committee last year in support of your work on comprehensive federal privacy legislation, which we consider critical to protecting consumers from data related harms and a necessary complement to any potential AI legislation or regulation.[11] However, a privacy law is not the appropriate tool for addressing every potential harm from AI. Specifically, ITI expressed concerns about prematurely mandating prescriptive requirements to conduct algorithmic design evaluations and impact assessments, and that the scope of those requirements, which would have potentially covered all algorithms, were overbroad and would have swept in a vast array of technologies well beyond AI. Moreover, a singular focus on "algorithms" does not provide an accurate picture of potential harms or necessary mitigations. Addressing concerns about bias and discrimination requires an examination of an AI system, including inputs such as the data it was trained on and the context for its deployment. In order to appropriately evaluate potential bias, more work is needed to develop the technical standards that would undergird any such assessment.

Relatedly, high-quality data sets are an important precursor for accurate and robust outputs. In that vein, we believe it is crucial that organizations undertake activities that can help to ensure that input data is in fact, accurate, relevant, complete, and consistent, and that bias is mitigated to the extent possible. While data governance processes may vary across organizations, in high-risk scenarios it is important that organizations document and share information about the processes they are undertaking. In order to ensure sufficiently robust outcomes, it is important that high-quality data is relevant and available in machine-readable formats. In addition to access to the compute infrastructure referenced above, AI developers and stakeholders need access to large and diverse datasets to better target solutions, and meet the needs of individuals and society in unprecedented ways. More available data means more data with which to train systems, resulting in higher quality offerings. A U.S. approach

[11] Testimony of John Miller, Hearing on Protecting America's Consumers: Bipartisan Legislation to Strengthen Data Privacy and Security, Before the U.S. Energy and Commerce Committee (June 14, 2022) available at https://docs.house.gov/meetings/IF/IF17/20220614/114880/HHRG-117-IF17-Wstate-MillerJ-20220614.pdf

that prioritizes innovation should therefore **seek to support existing international data standards and promote the development of new standards for data quality, as well as make government data available in machine-readable formats, and curate widely available data.**

IV. Conclusion

To reap the benefits that AI will bring to the communications sector and to society more broadly and maintain U.S. leadership in the development and deployment of the technology, Congress has an important role to play. A U.S. AI policy framework should be risk-based, reflect the unique roles of different actors in the AI value chain, foster public trust in the technology, and uphold the tenets of security and privacy. It should also recognize the importance of global cooperation and seek to work with partners multilaterally, bilaterally, and in international standards organizations to progress a vision of responsible, trustworthy AI around the world. Above all, an approach that equally prioritizes efforts to advance innovation in important areas like red-teaming, content authentication, and model performance evaluation metrics will be critical to implementing risk management practices that will help to foster accountability moving forward.