**Before the**
**NATIONAL SCIENCE FOUNDATION**
**Alexandria, VA 22314**

| | |
|---|---|
| In the Matter of | ) |
| | ) |
| Request for Information on the | ) |
| Development of an Artificial Intelligence | ) |
| (AI) Action Plan | ) |

## COMMENTS OF USTELECOM – THE BROADBAND ASSOCIATION

USTelecom – The Broadband Association ("USTelecom")[1] is proud to collaborate with the Administration to unlock the transformative potential of AI and contribute to a forward-looking AI Action Plan.[2] The broadband industry has been at the forefront of AI innovation since its inception in the mid-20th century, making broadband providers among the earliest adopters of AI technologies.[3]

The rapid expansion of AI tools today marks a new frontier of human ingenuity, reminiscent of the early days of consumer internet access. As AI continues to drive economic security and prosperity in the U.S., its success is powered by a skilled workforce of engineers and data scientists. Leveraging the insights of our industry's experts and business leaders, USTelecom presents the following recommendations to fully harness AI's potential:

1. Cut Government Red Tape and Speed Up Broadband Deployment
2. Embrace Pro-Innovation AI Governance to Keep America Competitive
3. Ensure Balanced Assignment of Responsibilities Among AI Developers and Deployers
4. Reduce Barriers to AI Innovation and Market Entry
5. Strengthen the American Market-Driven Approach to Standards Development

---

[1] USTelecom is the nation's leading trade association representing service providers and suppliers for the telecom industry. USTelecom members provide a full array of services, including broadband, voice, data, and video over wireline and wireless networks. Its diverse member base ranges from large international publicly traded communications corporations to local and regional companies and cooperatives, serving consumers and businesses in every corner of the country and world.

[2] Development of an Artificial Intelligence (AI) Action Plan, Request for Information (rel. Feb. 6, 2025) ("RFI"), https://www.federalregister.gov/documents/2025/02/06/2025-02305/request-for-information-on-the-development-of-an-artificial-intelligence-ai-action-plan.

[3] The term "artificial intelligence" was coined in 1955 when Bell Telephone Laboratories and other organizations proposed a study on the topic. See McCarthy et al., A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence (1955), available at https://www-formal.stanford.edu/jmc/history/dartmouth/dartmouth.html.

## I. CUT GOVERNMENT RED TAPE AND SPEED UP BROADBAND DEPLOYMENT

AI is transforming everything from national security to the economy, but its future depends on something more fundamental: the strength of America's fiber broadband infrastructure. Without high-capacity fiber networks, AI can't function at scale, and the U.S. risks losing its competitive edge. Policymakers must recognize that investing in next-generation fiber networks is just as critical as advancing AI itself.

Following China's unveiling of Deep Seek—an AI model that exceeded many experts' expectations—David Sacks, the President's advisor on AI and cryptocurrency and head of the President's Council of Advisors on Science and Technology, underscored the importance of strengthening American infrastructure. He emphasized that expanding the nation's largest data centers remains a strategic advantage, stating, "If we scale the biggest data centers, it is still an advantage."[4]

To avoid a shortfall of broadband and fiber infrastructure to support AI, the U.S. should address deployment barriers that slow builds and add costs. A regulatory environment that prioritizes streamlined permitting, spectrum access, and investment-friendly policies for broadband and data centers will accelerate AI adoption and maintain U.S. competitiveness in the global AI race. As AI increasingly is integrated into devices used by consumers and businesses, robust broadband connectivity also is needed at the edge points.

Here are several reasons why broadband, specifically, is the key to America winning:

- **Broadband and fiber connectivity are essential to the AI data center transformation.** It is estimated that data centers running AI large language models will require 5x more *optical connectivity* than traditional data centers.[5] AI applications depend heavily on *symmetrical bandwidth*, which allows massive amounts of data in and out of a network simultaneously. Greater fiber capacity is needed to ensure AI can scale exponentially – fiber provides the symmetrical, *ultra-low latency, and scalability* that AI workloads require to function optimally.

- **AI networks face fiber networks capacity shortage.** The rapid growth of AI applications is driving unprecedented demand for robust fiber networks that are essential for connecting AI data centers, delivering high bandwidth and low latency. While the U.S. has significant backhaul fiber infrastructure for broadband, AI infrastructure demands much higher bandwidth, signaling a need for major network upgrades.

- **Spectrum availability fuels next-gen AI connectivity.** More licensed and shared spectrum for broadband providers supports the seamless, high-speed wireless

[4] Jason Plautz, *Energy is AI's barrier to entry. David Sacks knows it.*, E&E News by Politico (Feb. 11, 2025), https://www.eenews.net/articles/energy-is-ais-barrier-to-entry-david-sacks-knows-it.

[5] Corning, *AI is here, and it needs glass* (Dec. 2023), https://www.corning.com/worldwide/en/the-progress-report/crystal-clear/ai-is-here-and-it-needs-glass.

connectivity AI needs to function at scale, particularly for edge computing, IoT, and 5G-powered AI applications.

- **AI helps secure the homeland from cyber threats.** With the ability to sift through massive amounts of data at lightning speed, AI detects threats faster, predicts attacks before they happen, and automates responses to neutralize risks in real time. Unlike traditional methods, which often drown security teams in false alarms, AI hones in on real dangers with razor-sharp accuracy. This means fewer distractions, quicker decision-making, and a stronger, more resilient defense against ever-evolving cyber threats.

By prioritizing broadband expansion, policymakers can ensure the U.S. stays ahead in the AI revolution. The future of AI isn't just about smarter machines—it's about smarter infrastructure decisions today.

## II. EMBRACE PRO-INNOVATION AI GOVERNANCE TO KEEP AMERICA COMPETITIVE

As Vice President J.D. Vance stated recently, "Now at this moment, we face the extraordinary prospect of a new industrial revolution, one on par with the invention of the steam engine or Bessemer steel, but it will never come to pass if overregulation deters innovators from taking the risks necessary to advance the ball…."[6] And as many have observed, we are locked in a geopolitical AI arms race with numerous rivals including – though not limited to – the Chinese Communist Party.

With this in mind, USTelecom offers the following recommendations to ensure a pro-innovation AI governance framework, which recognizes opportunities—not just risks.

### 1. Existing laws already address most harms that may result from the use of AI.

As a number of agencies—including the Department of Justice ("DOJ") and the Federal Trade Commission ("FTC")—have acknowledged, existing laws already protect against many of the potential harms that may result from AI. For example, the FTC Act (Section 5) and other consumer protection laws apply regardless of whether a human acts alone or uses technology to commit an act in violation of those statutes.

Existing legal frameworks are designed to be flexible and adaptable to new technologies and contexts. These frameworks have been tested and refined through years of legal interpretation and application, thereby offering greater degrees of consistency and predictability.

Existing laws may better protect against harms they were designed to address than AI-specific laws. This is because the existing laws are focused on the harm, rather than the technology, and will not depend on how AI is defined or whether the technology evolves. The existing laws also have a long history of implementation and enforcement, and there are existing legal and regulatory frameworks already in place to enforce them.

---

[6] Remarks by Vice President J.D. Vance at the Artificial Intelligence Action Summit in Paris, France (Feb. 11, 2025), *available at* https://www.presidency.ucsb.edu/documents/remarks-the-vice-president-the-artificial-intelligence-action-summit-paris-france.

We encourage policymakers to evaluate the extent to which existing laws apply to AI systems and to work to better understand how existing laws can be leveraged to foster trustworthy and safe AI systems.

2. **To the extent regulation is required to address high risk uses of AI, USTelecom supports a risk-based approach that fosters trustworthy AI while maintaining U.S. leadership in innovation.**

In pursuing trustworthy AI, policymakers should avoid a prescriptive approach to regulation that stifles innovation while failing to keep pace with the dynamic nature of a technology that continues to rapidly evolve. While ethical and responsible deployment are critical, striking the right balance that keeps the United States from falling behind other countries that invest heavily in AI innovation, including foreign adversaries, is essential.

At this early stage of AI development, the voluntary framework outlined by NIST is appropriate for most AI applications. To the extent regulation is required, however, policymakers should endorse a risk-based regime that is consistently based on NIST's framework.

While the government may, in appropriate contexts, consider additional laws or regulations, AI should not be held to unreasonable legal standards that hamper technological innovation and growth, and which may be ineffective for achieving the stated policy goals.

3. **Policymakers should seek to avoid a patchwork of state laws that creates uncertainties and implementation challenges for developers and deployers.**

Currently, there is no federal law in the United States that preempts state-level regulation of AI. As such, there is a substantial risk that AI innovation could be hampered by a patchwork of inconsistent state-level regulations. Indeed, dozens of state AI laws have been enacted and hundreds of AI bills have already been introduced in recent years.

To avoid inconsistent state laws that hamper innovation, the U.S. should take action to preempt state-level fragmentation efforts and ensure U.S. policy on AI is harmonized at the national level. The Administration should work with Congress on federal legislation that preserves a national framework for AI and avoids a patchwork of state regulation.

4. **Third-party audits across all AI risk categories is unnecessary and could create significant security and other risks.**

USTelecom supports a risk-based framework for managing AI systems. Not all AI use cases present the same level of potential harm and oversight measures should be commensurate with the level of risk. Consistent with that view, we believe independent third party audits should not be required of most AI systems. Creating such a requirement would unnecessarily stifle AI innovation and increase the risk of security, privacy, IP, and trade secret risk.

For uses that are not considered extremely high risk, self-certification is an effective oversight mechanism and is also more efficient from a financial and administrative perspective for small to medium sized firms.

Requiring independent third party audits for AI use that does not present considerable risk to human safety has a number of downsides. First, there is no credentialing system for independent auditors of AI systems, so it is possible that companies setting themselves out as AI

auditors could have ties to foreign adversaries, have poor security systems, and lack an appropriate mechanism for protecting privacy and trade secrets, among other things. Second, there is no government accepted, normative standard—like PCI DSS in the payment card data security context—for a third party auditor to use to conduct such an audit. As a result, industry and government could be faced with "apples to oranges" comparisons when trying to compare audit results from different companies doing similar AI development work. For example, each algorithm developed for use in AI has differing value preferences. Because there is no "correct" answer as to how the values—such as privacy, safety, objectivity, accuracy—should be balanced, a third-party audit cannot guarantee a "better" or "more objective" investigation and risks introducing value preferences that are not tailored to the specific use case. Finally, requiring external audits for medium to low risk AI use could create a barrier to entry for small companies looking to innovate in this space.

## III. ENSURE BALANCED ASSIGNMENT OF RESPONSIBILITIES AMONG AI DEVELOPERS AND DEPLOYERS

In general, responsibility in AI governance should be proportionate to the level of control an entity has over the technology. AI deployers—businesses, individuals, or institutions that implement AI models in their workflows—should not bear liability for issues stemming from the design, training, or fundamental flaws in the AI model that they neither created nor have the capacity to alter. Holding deployers accountable for failures they cannot anticipate or rectify would not only be unjust but would also stifle innovation by discouraging AI adoption. Instead, liability frameworks should clearly distinguish between developers, deployers, and infrastructure providers, ensuring that obligations align with decision-making power. This approach fosters a balanced ecosystem where each stakeholder plays a role in mitigating risks without being unfairly burdened.

### 1. Policymakers should recognize key differences between developers and deployers.

**Developers research, design, code, and produce AI systems** for use by deployers and end users.[7] More specifically, a "Developer" is a natural or legal person, public authority, agency or other body that provides the initial infrastructure, or substantial modification to, an AI system, including model building and interpretation tasks, that involve the creation, selection, calibration, training, and/or testing of models or algorithms. Developers of AI systems and models most often have sole knowledge of the code used to develop an AI system. Developers also have control over any and all related data used to train the AI, the training methods, and guardrails for ensuring models delivered to deployers are safe, secure, legal, effective, and trustworthy, and that they minimize the potential for bias and discrimination. While developers generally do not have control over subsequent uses of an AI system by a deployer, the developer is the only entity that can specify the intended uses of AI systems for deployers and policymakers, and that can

[7] *See* AI Developers and Deployers: An Important Distinction, BSA - The Software Alliance (Mar. 16, 2023); *see also* NIST RMF 1.0 at 35 ("AI Development actors provide the initial infrastructure of AI systems and are responsible for model building and interpretation tasks, which involve the creation, selection, calibration, training, and/or testing of models or algorithms.").

take the steps in model development, data selection, and guardrail implementation that are appropriate for those intended uses.

**In contrast, deployers use an AI system produced by a developer.** Deployers may modify or adjust AI systems to maximize or tailor the system to their business purposes, but "do[ ] not generally have control over design decisions made by another company that developed the AI system."[8] Deployers may use AI systems internally, or they may use them to engage with consumers or end users. In those instances where deployers are using AI systems directly with consumers, they will need to rely substantially on the information provided by, and decisions made by, the developers. Absent regulatory or contractual transparency obligations for developers, deployers will have little understanding of what comprises an AI system or the universe of expected outcomes from the use of a particular AI system.

As a result, policymakers must recognize the different roles and responsibilities of developers and deployers of AI systems and align regulatory obligations with the information available to each stakeholder and at relevant points in the AI life cycle. This approach is critical to ensuring regulatory obligations are tailored to an organization's role in the AI marketplace, and that both are held to responsible AI practices.

**2. A fair, risk-based approach is essential, placing responsibility on those best positioned to manage AI-related risks.**

Three key policy questions to address in the context of this issue are: (1) What are the appropriate upfront obligations for developers and deployers? (2) What is the appropriate structure for liability on the backend? (3) When does a deployer become a developer, when is a developer also a deployer, and who is the responsible party when the lines are blurred? The regulatory construct for upfront obligations, backend liability, and how these roles are defined should be approached thoughtfully and with continued industry input.

**Upfront Obligations**. With regard to the appropriate upfront obligations for developers and deployers, particularly in higher-risk applications of AI, policymakers should recognize that developers have the most insight into how an AI is trained, what the AI can and cannot do, and what safeguards were put in place to mitigate bias, discrimination, and other negative outcomes.

**Developers**. Given the significant–and asymmetrical–access to information developers have about the inner functioning of AI systems, upfront obligations for developers should include extensive transparency requirements to deployers in the form of a detailed model/system card and any additional contextual information around what uses are considered on-label and off-label. Developers of AI systems should be held responsible for ensuring the systems meet those specifications. Model/System cards provided to deployers should include at a minimum:

- Model Details – A brief narrative explaining what the model does, any outputs, proof of concept, date, version, model type, and underlying licenses.
- Use Cases – What uses are intended and not intended, and any mitigation controls put in place to prevent unintended outcomes for intended uses.
- Limitations & Risks – Developers should flag any known limitations. They should also highlight any known, likely, and specific high risks for using an AI system and appropriate steps for risk mitigation.
- Training – Data sources, data strategy, and permission to use.

[8] AI Developers and Deployers: An Important Distinction, BSA - The Software Alliance (Mar. 16, 2023).

- Analyses – Evaluation metrics, fairness, and known recommendations.

**Deployers**. With regard to deployers, upfront obligations may include a requirement to notify the developer in instances where the deployer wants to use the AI system in a way that was not contemplated in the original commercial agreement. Deployers should also be responsible for post-deployment monitoring and relevant safeguards put in place for AI systems deployed for the purpose of direct consumer engagement.

**Responsible Party**. In some cases, an entity will act both as a developer and deployer. Under those circumstances, the entity should observe the responsibilities of both, executing its role-specific obligations based on the context.

There may be times when a deployer modifies an AI system substantially and in a way that is prohibited by, or outside the boundaries of, the model/system card provided by the developer to the deployer. Under those circumstances, the deployer assumes the obligations of a developer with respect to its modifications. The standard for when a deployer assumes the obligations of a developer through substantial modification to an AI system should be fairly high. For example, deployers should not incur developer obligations by training or using an AI on their own data or making predictable and/or necessary modifications to AI systems as required to carry out or optimize the expected functioning of the AI. (Predictable modifications include re-training and scoring, for example.) The legal discourse surrounding what constitutes a predictable modification to an AI system is expected to evolve.

A developer acts as a deployer any time it uses AI systems that it developed itself for its own internal business operations or to engage with consumers or end users directly.

**Backend Liability**. There will likely be some level of shared liability depending on a number of contributing factors, e.g., the level of harm resulting from an AI malfunction, whether the AI use was an intended use, if the resulting harm was predictable/ascertainable by the developer and whether adequate measures were put in place before the AI system was provided to deployers. These theories of liability stem from historical product liability or tort principles. Based on the discussion above, however, there is a need for certain protections to be put in place. A deployer should be protected from liability if it makes AI systems available to end users as intended and as described in the documentation provided by the developer and the AI malfunctions in a way that could have been prevented by the developer, or when a deployer relies on a model/system card provided by a developer to the deployer's detriment.

### 3. Broadband providers are not "AI regulators" and should not be expected to monitor, regulate, or assume liability for AI applications running over their networks.

Broadband providers play a fundamental role in enabling America's digital economy, providing the high-speed connectivity that fuels innovation, commerce, and communication. However, while these companies are sometimes developers or deployers of AI technology in their own right, their core function remains providing infrastructure—not monitoring or regulating the vast array of applications and services that run over their networks. Placing them in the role of AI enforcers or internet gatekeepers would be a misalignment of responsibility that undermines both technological progress and fundamental principles of a free and open internet.

Indeed, requiring broadband providers to monitor and regulate AI on behalf of the government would blur the lines between private enterprise and state control, creating a system where internet access is contingent on compliance with government-mandated oversight. This

would open the door to broader forms of content moderation and surveillance that could threaten free expression and innovation. History has shown that once private entities are pressured to enforce government directives, the scope of that enforcement tends to expand over time, raising concerns about privacy, overreach, and the unintended consequences of deputizing network providers as regulators.

Moreover, imposing this burden on broadband providers would distort their role in the marketplace and divert resources away from their core mission—delivering fast, reliable, and secure internet service to American businesses and consumers. Compliance costs associated with AI monitoring would not only drive up operational expenses but could also lead to reduced investment in broadband expansion and innovation. The result would be a slower, more cumbersome digital infrastructure at precisely the time when global competitiveness depends on accelerating America's technological leadership.

## IV. REDUCE BARRIERS TO AI INNOVATION AND MARKET ENTRY

As Vice President J.D. Vance observed, "AI will have countless revolutionary applications in economic innovation, job creation, national security, health care, free expression, and beyond. And to restrict its development now would not only unfairly benefit incumbents in the space, it would mean paralyzing one of the most promising technologies we have seen in generations."

Put simply, AI technologies have yet to realize their full potential; overly burdensome regulatory barriers may hamper innovation and should be avoided.[9]

A pro-innovation framework will support additional development of nascent uses of new AI technologies, increase business investment, and build the public and consumer trust necessary for the success of an innovation economy. In addition to hampering innovation, extensive or overly prescriptive regulatory requirements could hinder competition due to increased compliance costs that could create barriers to entry for small and medium sized businesses— A regulatory framework that creates barriers to entry will negatively impact the United States' leadership role in AI on the global stage.

### 1. AI regulations should not unfairly single out specific industries.

AI regulations should be designed to foster innovation and competition across all sectors without imposing undue burdens on specific industries. Policies that disproportionately target broadband providers while allowing more flexibility for IT firms could create an uneven playing field, stifling fair competition and limiting consumer choice. For instance, if broadband providers face stricter oversight when deploying AI-driven services such as chatbots—while IT companies offering similar solutions operate under more lenient rules—this discrepancy could hinder their ability to innovate and compete effectively. A balanced regulatory approach should apply consistent standards across industries, ensuring that all players have equal opportunities to leverage AI advancements while maintaining consumer protections and ethical safeguards.

[9] Remarks by Vice President J.D. Vance at the Artificial Intelligence Action Summit in Paris, France (Feb. 11, 2025), *available at* https://www.presidency.ucsb.edu/documents/remarks-the-vice-president-the-artificial-intelligence-action-summit-paris-france.

### 2. Overly broad opt-out requirements can undermine AI benefits.

Overly broad opt-out requirements will hamper innovation by disincentivizing adoption of new AI systems. To operate in a fair and equitable way, AI systems depend heavily on vast amounts of diverse and representative data to learn and make accurate predictions. Overly broad opt-out requirements would make little sense in many contexts, and can lead to data scarcity and lower quality training sets, hampering the AI system's ability to perform well in real-world scenarios. Imposing broad opt-out requirements also increases the risk of bias, by removing diverse data sets from AI models, if certain groups disproportionately opt out of the use of AI in a particular context.

In addition, overly broad opt-out requirements would undermine many consumer benefits of consumer-facing AI use cases. For example, more accurate diagnoses in healthcare, personalized financial advice, or optimized transportation networks. Such requirements would also be impracticable to implement because AI will be embedded in so many aspects of commerce in the future; attempts to impose the requirements would likely lead to inconsistent enforcement and confusion among consumers and businesses alike.

### 3. The government should not let anticompetitive behaviors deny innovators market access.

To maintain a dynamic and competitive marketplace, the government should actively monitor for potential anticompetitive behaviors that could disadvantage innovative American companies, including broadband providers. Ensuring fair competition is essential for fostering innovation, consumer choice, and economic growth. Dominant players in the technology ecosystem must not be allowed to use their market power to restrict access, impose unfair contractual terms, or create artificial barriers that prevent emerging competitors from offering AI-driven and other advanced services.

By enforcing fair competition policies, policymakers can promote a level playing field where businesses of all sizes can thrive, ultimately benefiting consumers through greater innovation, improved services, and more competitive pricing.

## V. STRENGTHEN THE AMERICAN MARKET-DRIVEN APPROACH TO STANDARDS DEVELOPMENT

Standards development activities for AI and other emerging technologies provide the foundation for transforming innovation into products and services that change the world. The architectural models, features, and capabilities that are defined by standards and specifications are essential to technological creativity, interoperability, and the establishment of global platforms for innovation and value creation. When developed through industry-driven, transparent, and voluntary development procedures, collaboration between different technology developers is enabled. Contributors submit their ideas in a consensus building process that, following robust debate and review, enables technology that promotes interoperability, unlocks greater functionality, and generates network effects—value that is greatly beyond the sum of the individual parts.

The industry-driven model heretofore has been a crucial component to innovation in, and the development of, the global digital economy, which has made enormous contributions in

improving quality of life around the world. To ensure that U.S. technology firms continue to be able to compete on a global scale, U.S. industry and government should work together to promote and preserve the widespread use of the industry-driven model.

As USTelecom noted when helping NIST define a standards strategy for AI and other critical and emerging technologies,[10] technology standards are beneficial for many reasons, including the following:

- **Competitiveness and Innovation.** Because standards are critical to product design and to cross-border acceptance, a nation's strength in setting standards is part of its of economic competitiveness. As NIST notes, standards are the technical foundation enabling competitiveness and innovation.[11]
- **Cybersecurity/National Security.** Cybersecurity is a difficult practice. Standards distill the knowledge and expertise of skilled industry practitioners. Industry standards are developed in a transparent process. This openness leads to greater scrutiny and technical engagement.
- **Economic Efficiency.** Standards that reflect the consensus of all interested stakeholders drive significant economies of scale. Efficiency gains enabled through global standards are a key driver of economic growth.

### 1. Promoting the American, market-driven approach to standards development globally is essential.

There has been a growing perception by some that the United States is either falling behind or being outflanked through the global standards and specification development process, particularly by China. As observed by numerous associations across both the communications and technology sectors, these perceptions tend to underestimate the strength of rules-based, consensus-driven standards development organizations to prevent inordinate influence by any actor.

Nonetheless, speaking hypothetically, decreased U.S. industry participation (particularly in the industry-led venues) would have a significant impact on U.S. economic competitiveness and empower rivals such as China. And even absent credible evidence of the U.S. falling behind, bolstering U.S. company participation should be a national priority to promote globally the U.S. private sector led approach to standards.

The U.S. approach, which has been extremely successful in establishing the U.S. as a global technology leader is market-driven and generally ensures a level playing field where technologies can rise and fall on their own merits. Standardization is led by privately empowered standards organizations, with NIST and ANSI providing crucial roles and serving as important conveners for stakeholders.

---

[10] Comments of USTelecom, *Implementation of the United States Government National Standards Strategy for Critical and Emerging Technology*, NIST, Docket No. 230818-0199 (Nov. 13, 2025).

[11] *Setting the Standards: Strengthening U.S. Leadership in Technical Standards* (testimony of James Olthoff), NIST (Mar. 17, 2022) [hereinafter NIST Testimony], https://www.nist.gov/speech-testimony/setting-standards-strengthening-us-leadership-technical-standards.

Overwhelmingly, industry prefers, and consumers benefit from this market-driven approach, whereby consensus is developed on a voluntary basis and a higher degree of transparency promotes the integrity of standards. While this approach is not perfect, governments are less able to put their thumbs on the scale at the expense of integrity.

In contrast, China's approach to standardization is shaped by party-state influence and lends itself more easily to political influence overtaking market and technologically driven interests. This increases the likelihood of a state exerting undue influence in government-led standards organizations, where governments get a formal vote on standards, enabling national self-interest or one country's influence over others to outweigh market-based criteria. Even in the government-driven International Telecommunication Union Telecommunication Standardization Sector (ITU-T), where membership is open to industry, we have repeatedly observed the specter of government, rather than market consensus or technical expertise, forming the basis of *policy proposals*. This speaks to the need to address ITU governance issues, even if policy proposals do not entail success with respect to *technical standards contributions*.

Another problem with government-led standards organizations is the diminished role of industry experts who can provide meaningful perspectives from the companies developing and deploying emerging technologies. This can result in standards that are divorced from or not optimized for the operational, economic, or security realties that industry experts are familiar with because of their direct experience.

For these reasons, the U.S. government should actively promote and continue to support the globally accepted, market-driven, voluntary approach to standards development.[12] Stakeholders from all countries should be welcome to participate in the market-driven model. This market-driven approach encourages users of AI platforms to choose their preferred systems without political influence, fostering innovation and supporting growth. It allows the industry to develop AI models that benefit the user community while utilizing existing intellectual property protections. This is a crucial factor in the successful development and incubation of AI technology. NIST is the agency most suited to coordinate U.S. government efforts to support this model, due to NIST's many years of close partnership with industry and established, trusted relationships.

**2. The U.S. government should create financial incentives to help offset the costs of participating in standards bodies and increase U.S. participation.**

To strengthen U.S. leadership in global standards, more private-sector organizations must actively contribute as standards members. One of the biggest barriers to U.S. company participation in standards-setting is cost. On average, it costs companies approximately $300,000 per engineer annually to engage in standards development,[12] with the process of developing a single standard often spanning multiple years and costing millions.

To mitigate these financial challenges, the U.S. government should consider targeted support measures, such as grants for companies that find costs prohibitive and tax incentives to encourage broader participation among U.S. businesses. Small and medium-sized enterprises (SMEs) face particularly steep financial barriers, making their increased involvement essential. However, given that many standards are primarily developed by larger corporations and will

[12] Jeanne Whalen, *Government Should Take Bigger Role in Promoting U.S. Technology or Risk Losing Ground to China, Commission Says*, Washington Post (December 1, 2020), https://www.washingtonpost.com/technology/2020/12/01/us-policy-china-technology.

continue to be, it is crucial to avoid restrictive policies—such as capping the maximum number of employees a company can have to qualify for funding. Instead, financial support should be accessible to companies of all sizes to enhance U.S. competitiveness.

Beyond direct support for companies, the U.S. government should also provide incentives or subsidies to North American standards organizations, such as the Alliance for Telecommunications Industry Solutions ("ATIS") and the American National Standards Institute ("ANSI"), to facilitate the domestic hosting of standards meetings.

**3. The U.S. government should invest in research and development, as well as education to increase the future talent pool of standards experts.**

Ensuring the United States maintains and secures its place as a global leader in standards development requires a forward-looking vision that goes beyond immediate returns on investment. For instance, investing in research and development will drive and accelerate the release of future international standards. This is because standards depend upon peer reviewed and often innovative, experimental research. In recent years, China has devoted substantial resources to ensuring its own competitiveness on the world stage. The U.S. government should consider ways that it can incentivize and unleash private sector innovation, to ensure the country does not fall behind.

Part of ensuring U.S. long-term standards leadership is investing in the talent pool for standards development. China is actively recruiting university graduates. In comparison, U.S. universities generally place a lower priority on promoting standards. The U.S. government should look for ways to enhance the STEM talent pool and support educational programs that equip the next generation of experts to sustain the economic security of the United States.

**4. The U.S. government should promote industry-led standards for post-quantum cryptography.**

As the United States accelerates its leadership in artificial intelligence, it must also prioritize investment in other foundational technologies, such as post-quantum cryptography ("PQC"). AI is driving advancements across industries, including broadband, enhancing network efficiency, customer interactions, and digital services. However, to fully harness AI's potential, the underlying infrastructure must be equipped with state-of-the-art security standards that support long-term technological progress. Quantum computing represents a generational leap in computing power, requiring new encryption methods to ensure that all industries, including broadband, can continue to innovate with confidence. Developing and adopting PQC standards now will future-proof digital infrastructure, ensuring that AI-driven advancements are built on a secure and resilient foundation.

A forward-thinking national strategy should view AI, PQC, and broadband as complementary pillars of technological leadership. Just as policymakers and industry leaders are working together to shape AI governance, the same collaborative approach should be applied to establishing PQC standards. By proactively investing in post-quantum security, the U.S. can ensure that its digital infrastructure remains globally competitive and that broadband providers have the tools they need to deliver secure, AI-enhanced services. Prioritizing PQC alongside AI is not just about mitigating future risks—it is about creating the conditions for sustained

innovation, ensuring that American companies remain at the cutting edge of the global digital economy.

## VI. CONCLUSION

USTelecom appreciates the opportunity to contribute to the United States' AI Action Plan, and we stand ready to work closely with the Administration on its implementation.

Respectfully submitted,

*/s/ Paul Eisler*
Paul Eisler
Vice President, Cybersecurity

**USTelecom – The Broadband Association**
601 New Jersey Avenue, NW
Suite 600
Washington, DC 20001
(202) 326-7300

March 14, 2025