TECHNET
THE VOICE OF THE INNOVATION ECONOMY

1420 New York Avenue NW, Suite 825
Washington, D.C. 20005
www.technet.org | @TechNetUpdate

March 11, 2025

National Science Foundation
Attn: Faisal D'Souza
2415 Eisenhower Avenue,
Alexandria, VA 22314

Re: TechNet Comments on the Development of an Artificial Intelligence (AI) Action Plan

To Whom It May Concern:

TechNet appreciates the opportunity to respond to the National Science Foundation request for information on the development of an AI Action Plan. Our members represent many of the leading artificial intelligence (AI) and automated systems developers, deployers, users, and researchers.

TechNet is a national, bipartisan network of technology CEOs and senior executives that promotes the growth of the innovation economy by advocating a targeted policy agenda at the federal and 50-state level. TechNet's diverse membership includes dynamic American businesses ranging from startups to the most iconic companies on the planet and represents more than 4.5 million employees and countless customers in the fields of information technology, e-commerce, the sharing and gig economies, advanced energy, cybersecurity, venture capital, and finance.

AI is a transformational technology that is revolutionizing how Americans live and work and developing solutions to the most significant challenges of our time. AI can enhance productivity, democratize and expand access to important services, and improve product innovation. It has the potential to create significant value across every sector and, according to recent estimates, is poised to contribute up to $20 trillion to the global economy through 2030.[1] This presents an immense opportunity to improve the lives of all Americans, including by strengthening public health through early disease detection and personalized medicine; improving education with customized learning tools; bolstering public safety through smart surveillance and disaster prediction systems; and bridging communication and language barriers through real-time translation.

[1] Clemmons, Elisabeth, et all, "The Global Impact of Artificial Intelligence on the Economy and Jobs: AI will Steer 3.5% of GDP in 2030," IDC, September 17, 2024.

In recognizing AI's enormous potential, President Donald J. Trump launched the American AI Initiative through Executive Order 13859 in February 2019 to secure America's leadership in this critical technology. As a result of the Trump administration's critical early investments in AI research and development (R&D) and efforts to remove barriers to AI innovation, the United States currently holds the largest share of the global AI industry, which is valued at roughly $758 billion.[2] However, our international competitors and adversaries are working quickly to overtake our lead. China set a goal to become the global leader in AI by 2030, creating a new AI investment fund and pouring billions into AI research and development. Chinese models are already challenging American dominance with Alibaba's Qwen model rising to the top of open LLM leaderboards at the end of last year and surpassing U.S. model performance measurements.[3]

Industry and government must now work together to ensure our nation remains the global leader of AI. To achieve that end, TechNet recommends the administration's AI Action Plan build on the five key lines of effort established in President Trump's Executive Order 13859 – including setting AI technical standards, increasing AI research investment, building America's AI workforce, unleashing federal AI computing and data resources, and engaging with international allies – and includes the following principles and priorities.

Adopt a Risk-Based, Sector-Specific Regulatory Approach and Leverage Existing Laws

TechNet believes that AI systems should be developed, deployed, and used responsibly, enabling the United States to maintain its competitive edge and innovation leadership. Designers, developers, deployers, and users of AI systems are working to ensure appropriate oversight and accountability and protect against malicious activity. Any AI regulations should focus on mitigating known or reasonably foreseeable risks and designating responsibility and liability appropriately across the AI value chain.

As policymakers consider if new regulations for AI are necessary, it is important to note that there are already existing rules, regulations, and laws that prohibit unlawful behavior, including those perpetuated through AI. Such laws and regulations, which benefit from existing well-developed regulatory and enforcement frameworks, focus on preventing and providing recourse against the prohibited conduct rather than the means by which the conduct was accomplished. Government agencies should consider using existing statutory authority to issue sector-specific policy statements, guidance, or regulatory clarity. In many cases,

[2] Precedence Research, "Artificial Intelligence (AI) Market Size, Share, and Trends 2025 to 2034," Last updated, February 10, 2025. https://www.precedenceresearch.com/artificial-intelligence-market#:~:text=The%20global%20artificial%20intelligence%20(AI,19.20%25%20from%202025%20to%202034.
[3] Hugging Face Open LLM Leaderboard, https://huggingface.co/spaces/open-llm-leaderboard/open_llm_leaderboard#/

existing legislation already provides a way to more effectively regulate the safe use of AI.

When seeking to adopt new regulations for AI, policymakers should follow an incremental and collaborative approach to AI governance that is risk-based and sector-specific, accounts for changes in technology, and allows for innovation. Policymakers should assess the different applications or types of AI and ensure that any new AI-focused laws or regulations target AI-specific harms that could result from gaps in existing law where there is a high risk of demonstrable and tangible harm to individuals.

The AI ecosystem is diverse, with developers, deployers, and users all playing a role in the development and deployment of AI. We believe it is crucial to differentiate responsibilities between developers, deployers, and users, and these responsibilities should align with their specific positions in the AI system lifecycle. Careful consideration must be given to delegating regulatory responsibility that aligns with the roles and interactions of these entities. To implement effective regulatory policies, it is important for all of these actors to work together and have clear roles to maintain responsible and secure AI systems.

It is also important to note the role of the AI startup ecosystem and small and medium-sized enterprises in maintaining America's competitive edge in the economy, and they deserve to have a voice in determining a regulatory approach. The administration should give consideration to the potential implications of any proposed regulatory policies for all businesses, but particularly for small and medium-size businesses with the goal of supporting and accelerating the adoption of AI by such businesses.

Promote Technical Standards Based on Industry Frameworks and Best Practices

To promote innovation and adapt to technological changes, we encourage the use of industry frameworks and evidence-based regulatory tools like safe harbors, which allow the industry to test and share best practices.

TechNet believes the administration should promote technical standards and codes of conduct developed through industry-led processes that can help AI stakeholders signal to users that the platform utilizes trustworthy AI systems. Currently, many AI developers and deployers utilize internal processes to assess their AI systems, including internal auditing and impact assessments, which can involve monitoring an AI system for unfair bias, errors, and other issues that could compromise an AI system's reliability and accuracy – and, ultimately, its trustworthiness. In addition, throughout the development of AI systems, AI developers work to review the data that is used to train and test their AI models, which can help identify any potential biases or errors in the data. These internal audits should be used to improve and update the AI systems accordingly.

Many AI stakeholders are applying the NIST AI Risk Management Framework (RMF) to examine and assess their systems for determining and addressing risk throughout a system's lifecycle. The NIST AI RMF supports AI developers and other stakeholders in this effort by providing a risk-based, voluntary approach to incorporate trustworthiness and accountability benchmarks into the entire lifecycle of an AI system. In addition, the NIST AI RMF appropriately recognizes that the level of risk among different AI use cases can vary significantly. NIST developed its AI RMF in collaboration with key AI researchers, developers, and the broader technology industry. The public-private partnership fostered by NIST and the transparent development process ultimately led to a strong and forward-looking document. We advise that any future AI regulations or standards incorporate the NIST AI RMF, or a similar widely accepted set of voluntary standards, as a model for policy development.

Many leading AI developers are continuing to research and improve how best to explain the output of AI systems. We encourage the administration to support continued research and development to improve the measurement of frontier model capabilities in national security areas while developing narrowly tailored requirements that outline appropriate standards for such models. Any oversight and risk management framework must be carefully targeted, focusing exclusively on models most likely to present significant national security risks and should apply only to high-risk applications that lack existing regulatory structure.

Incentivize Private Sector Implementation of Responsible AI

To further incentivize responsible AI implementation in the private sector, the administration should employ a multi-faceted approach that combines financial incentives with resource support and opportunities for collaborative partnerships. For example, the federal government could offer tax credits, deductions, or grants for companies that invest in AI safety research, develop responsible AI frameworks, promote transparency, and implement bias detection and mitigation tools. These financial incentives should be extended to companies participating in voluntary AI safety testing or investing in robust transparency and accountability frameworks, including efforts to explain AI practices to consumers. The government could also allow for accelerated depreciation expensing for investments in state-of-the-art AI infrastructure – particularly when such investments include tools for data security and compliance monitoring – to help reduce upfront costs and encourage innovation while ensuring that deployment aligns with public interest and safety standards. Additionally, targeted grants could be made available to research institutions and startups focused on developing safe and secure AI applications, enabling them to scale responsibly. Government contracts and partnerships should also give preference to companies that demonstrate a commitment to the responsible implementation of AI, including those that have existing MOUs with the government to advance third-party testing of AI systems for national security risks. Such incentives create a competitive advantage for companies that prioritize testing and transparency, continuous monitoring, and bias mitigation.

Additionally, TechNet recommends adopting a voluntary partnership between the federal government and the private sector where the two agree to share learnings and access, where appropriate, on national security threats and risk mitigation in exchange for an agreement on federal guardrails that would preempt restrictive state-based regulations that bog down innovation.

For example, policymakers should prioritize maintaining public-private partnership initiatives such as the FCC's Technical Advisory Committee (TAC) and its work on AI's positive impacts on the U.S. telecommunications infrastructure. As AI continues to shape the future of connectivity, ensuring that AI/ML methods are effectively leveraged for spectrum utilization and network optimization is essential for maintaining the U.S.'s leadership in telecommunications. The TAC's focus on applying AI to enhance spectrum administration, improve network security, optimize performance, and address interoperability challenges is a critical step in modernizing digital infrastructure. By fostering collaboration between government and industry experts, policymakers can accelerate the deployment of AI-driven solutions that improve wireless and wired network efficiency, reduce congestion, and enhance cybersecurity.

The AI Action Plan should integrate efforts such as this to help streamline AI adoption, ensuring AI models can be deployed swiftly and effectively in the communications sector. AI-enabled networks can optimize complex network behaviors, predict failures, and enable proactive corrective actions, enhancing national infrastructure resiliency. By investing in these types of initiatives, the administration can advance its AI strategy, drive innovation, and create a competitive edge.

Set Federal Guardrails to Preempt State Regulation

In 2024, nearly 700 AI bills were introduced in state legislatures. Many companies developing and deploying AI systems do not operate within the boundaries of any one state. However, the AI bills introduced are not uniform or interoperable with one another, contain different definitions of AI and related terminology, and require different disclosures for engineering content. This developing patchwork makes compliance burdensome for businesses and confusing for consumers. A well-scoped federal approach would help prevent fragmented state-level regulation that increases regulatory burdens on AI developers and deployers.

To this end, we believe it is important for the administration to continue federal efforts to advance measurement science and collaborate with private industry to develop responsible safety practices and harmonize national standards around AI testing and evaluations. A unified federal approach to managing the risks of AI models and systems, including the most powerful AI frontier models, would help address compliance burdens with varying state regulations while still making room for states to address concerns related to high-risk consumer-facing applications where clear gaps have been identified and no existing regulation is applicable. Furthermore, given the rate at which we are seeing overregulation at the state

level, the federal government should look to impose a moratorium on state legislation related specifically to the development of frontier AI models until national standards are adopted.

Increase Federal Investment in Basic Research, R&D, and Workforce Development

America has long been the global leader in foundational technology research and development. AI tools can enhance scientific research to achieve insights and results within hours instead of months or years, helping us to achieve scientific breakthroughs that will define the next generation. As nations like China work to outcompete America in AI and emerging technologies, it is critical that we strengthen our investments not only in AI research and development (R&D) but also basic research and the broader scientific ecosystem. This includes funding national research infrastructure to provide AI researchers and students with greater access to complex resources, data, and tools needed to develop AI. It also requires robust funding for programs such as the Department of Commerce's Economic Development Administration's Regional Innovation and Technology Hubs Program, the National Institute of Standards and Technology's (NIST) laboratories, and the Department of Energy's Office of Science, which will ensure innovation, workforce development, and economic development are catalyzed and spread throughout the entire country. In addition to strengthening domestic AI research and development, the government should work with trusted partners to foster stronger international AI research collaborations that will help the U.S. maintain its competitive edge while ensuring that AI ecosystems remain anchored in the United States.

For the United States to remain the global leader in AI, we must also strengthen our domestic STEM talent pipeline. According to the House China Select Committee, the Chinese Communist Party has invested heavily in STEM education and is producing more research on AI and as many as five times the number of STEM graduates as the U.S. American students and adults need high-quality, widely accessible STEM and workforce education and training programs at all levels to give them the tools they need to succeed. Federal, state, and private investments in computer science, core STEM competencies, and related programs from early childhood through high school and beyond will produce immense returns for American technological innovation.

The National AI Research Resource (NAIRR) developed materials to support educators to ensure that they have readily available options for incorporating AI tools and training materials that support student learning in AI. We encourage the administration to utilize these best practices and continue to invest in the development of educational materials that will allow students to gain new and early exposure to AI tools and methodologies that transform their understanding; increase their interest in AI and other science, technology, engineering, and mathematics (STEM) fields; and broaden engagement across the full pool of talent to build a strong and diverse future AI innovation ecosystem. Many TechNet members are currently providing upskilling opportunities for individuals looking to

enter the technology economy, and we would like to remain partners with federal and state governments to design effective workforce programs.

TechNet has also been a longtime supporter of the creation of a National Digital Reserve Corps. A National Digital Reserve Corps aims to bridge federal government needs and private sector capabilities by establishing a federal program to manage a reserve of individuals with the credentials to address the digital and cybersecurity needs of Executive Agencies across the federal enterprise both before and when cyber incidents arise. We believe this kind of creative thinking and public-private partnership can buttress the U.S. government's workforce needs and address our ongoing modernizing needs.

Invest in Infrastructure to Support AI Development

Policymakers have taken important steps to increase our domestic manufacturing capabilities of critical technologies, enhance our R&D capabilities, and strengthen supply chains, and this work must continue to preserve our competitive advantage. To continue this progress, we recommend prioritizing and streamlining investments in AI infrastructure and supply chains, including by encouraging domestic manufacturing of semiconductor chips, modernizing energy grids, and updating energy policies to ensure adequate energy for data centers.

Incentivizing the further buildout of domestic manufacturing capacity, particularly in leading-edge chips, is critical to national security and to maintaining U.S. technology leadership, including in AI. The administration should work with Congress to promote long-term American competitiveness and ensure an even playing field for semiconductor fabrication in the United States by extending advanced manufacturing investment credits under the *CHIPS and Science Act*, which have already led to more than 90 new projects across the U.S., totaling more than $500 billion in private investment and creating more than 58,000 direct jobs in America. As a result of these new investments, U.S. production of the advanced logic chips needed to power AI has finally begun. Extension of the advanced manufacturing investment credit past its current December 31, 2026, expiration date will be needed to secure further growth in domestic advanced chip manufacturing. Additionally, the administration should ensure that trusted foreign companies that are investing domestically have fair access to data center capacity and energy infrastructure to further encourage global AI firms to invest in the United States.

Modernizing energy grids, updating U.S. energy policy, and streamlining related environmental and energy permitting regulations will also be required to meet the increasing demand for AI-related energy consumption. Within five years, training a leading AI model is projected to consume around five gigawatts of power.[4] However, data centers are facing long delays connecting to power grids due to

[4] Tim Fist and Arnab Datta, *How to Build the Future of AI in the United States*, Institute for Progress, October 23, 2024. https://ifp.org/future-of-ai-compute

availability constraints and lengthy and complex permitting processes. Federal agencies should be tasked with streamlining permitting processes by accelerating reviews, enforcing timelines, and promoting interagency coordination to remove bureaucratic obstacles. The administration should grant greater authority to federal agencies to site and permit interstate transmission lines and work with state and local governments to reduce permitting burdens in order to streamline the approval process and prevent discriminatory state practices where necessary to support data centers and other AI infrastructure needs. The administration should also incentivize the development of additional energy sources, including domestic nuclear power and small modular reactors (SMRs), and leverage federal funding for strategic energy infrastructure projects.

On top of this, the administration should seek to further reduce the energy load on the grid as a key strategy to meet the country's near-term AI energy demands. For example, initiatives such as EPA's ENERGY STAR leverage AI driven efficiency in consumer application to reduce overall electricity consumption, ease grid stress, and lower energy demand at the consumer level to allow for more power to be allocated to AI data centers.

TechNet also recommends the development of AI Economic Zones, created by local, state and the federal government together with industry. These zones would offer incentives for the creation of AI research hubs and significantly speed up the permitting processes for building AI infrastructure. These zones could include specialized infrastructure and regulatory frameworks, preferential land-use policies in strategic locations, and partnerships with local utilities to ensure sustainable power supplies. Further incentives could include research funding for innovative cooling technologies and energy management systems that optimize data center operations. Such zones could also facilitate the offtake of meaningful amounts of compute by public universities to scale the training of a homegrown AI-skilled workforce.

Develop AI Ready Data

TechNet supports the government development of "AI Ready Data." The U.S. federal government is one of the biggest producers of data in the world, and these important datasets are already fueling innovation in the public and private sectors. As we move to greater deployment of AI systems, ensuring this data is well-organized will allow these modern tools to deliver faster, cost-effective, and more accurate insights. We encourage NIST and other agencies to make datasets public, when appropriate, to increase AI research and development.

It is essential that the administration protects access to publicly available data and avoid restrictions on the processing of public data that is needed to train AI models and is foundational to model quality and functionality. Additionally, the fair use of text and data mining exceptions through balanced copyright rules are an important mechanism for enabling innovation while supporting rightsholders and are critical to enabling AI systems to learn from prior knowledge and publicly available data.

Standardize Definitions and Terminology

We want to encourage the use of a consistent and clear definition for artificial intelligence. In legislation and policy guidance, policymakers have utilized different definitions of AI, leading to legal uncertainties and ambiguity around implementation. We advise the use of the NIST AI RMF's definition[5] of an AI system for two reasons: 1) the RMF was developed through close coordination with experts from the AI community, and 2) it was adapted from existing AI industry definitions. Adopting the NIST AI RMF definition across the government will help provide greater clarity for the public's understanding of AI systems.

Adopt a National Privacy Standard

We also want to take this opportunity to highlight the need for a comprehensive federal privacy standard, which would allay many of the concerns about the harm to consumer privacy from the use of AI. By having a clear national privacy framework, we can help build trust in AI systems deployed across the United States, utilizing the same standards when it comes to consumer privacy.

TechNet believes that congressional action is the best approach to a federal privacy law because Congress can expressly preempt state laws and ensure that authorities with relevant expertise are responsible for enforcement. The House Energy and Commerce Committee is working to develop such legislation, recently issuing a request for information from industry for insights on a data privacy framework.[6] However, short of congressional action, we urge the administration to develop a uniform, coherent national privacy framework. A federal privacy standard will help consumers understand their rights relating to the data used to inform automated systems and will assist developers in knowing their liability when managing large datasets. It will also help avoid the confusion resulting from differing policies state-to-state, which make it difficult for more comprehensive deployment of AI across the United States.

Support Public-Private Collaboration on Security

Efforts to promote America's AI leadership will be meaningless if adversaries can steal sensitive intellectual property such as AI model weights or proprietary technology or launch attacks against critical AI infrastructure. As AI capabilities advance, China and other adversaries will have increased incentives to undermine these advancements through cyberattacks or simply steal these capabilities. The administration should partner with industry to substantially increase security

[5] The NIST AI RMF refers to an AI system as an engineered or machine-based system that can, for a given set of objectives, generate outputs such as predictions, recommendations, or decisions influencing real or virtual environments. https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf

[6] https://energycommerce.house.gov/posts/chairman-guthrie-and-vice-chairman-joyce-issue-request-for-information-to-explore-data-privacy-and-security-framework, issued February 21, 2025.

protocols at AI laboratories, data warehouses, and data centers to ensure security throughout the AI stack. This could include establishing enhanced security protocols for infrastructure and developing technical solutions for confidential computing technologies to protect model weights and user data to prevent adversaries from exploiting the most powerful AI models. The government should also collaborate more closely with industry to track adversarial activities and capabilities and create communication channels to share information and warn of national security threats. This includes strengthening collaboration in monitoring traditional cyber threats, as well as disinformation campaigns or other information operations, malicious use of models, and energy usage by foreign malign actors.

Improve Federal AI Procurement and Government Utilization

TechNet supports expanded government utilization of AI to improve access to important services, enhance efficiency and cost savings, and ensure data-driven decision-making. This will require improving federal IT procurements by moving away from cost plus contracting, encouraging modular procurement that allows agencies to procure AI components and services separately, utilizing flexible procurement mechanisms such as Other Transaction Authority to attract non-traditional vendors, and leveraging the use of cloud-based AI services to reduce infrastructure costs and improve scalability. In particular, the government should simplify the accreditation process for cloud-based AI tools. A faster, criteria-based approach would allow agencies to test real use cases sooner while maintaining rigorous security oversight. AI vendors should also be required to meet FedRAMP continuous monitoring requirements before full accreditation, enabling ongoing security assessments and reducing deployment timelines by an average of 12 months. Finally, the administration should prioritize interoperability requirements and foster collaboration between agencies, industry partners, and academic institutions to help keep procurement practices aligned with rapidly evolving AI technologies and best practices.

Lead International Coordination

To protect America’s competitive edge in AI, it is critical that the administration lead international efforts to establish shared understandings of frontier AI risks and coordinate on standards and security best practices. The United States must drive global consensus in support of a U.S.-led framework for international AI standards and definitions that enables regulatory coherence and global adoption. This includes working closely with trusted partners and allies to harmonize AI standards and regulations to ensure that misaligned regulatory frameworks do not create unnecessary barriers to AI adoption, increase compliance costs, or slow innovation. American competitiveness relies on U.S. companies having the freedom to expand, compete, and integrate AI solutions globally without facing unnecessary regulatory barriers. However, the emergence of inconsistent and overly restrictive AI regulations in various countries creates significant challenges for American innovation. These disparate regulatory approaches increase development costs, complicate deployment, and ultimately restrict U.S. companies' ability to fully

participate in international markets. The resulting limitations on American AI products and services in global markets threaten to undermine U.S. dominance in digital innovation and weaken our competitive position against strategic rivals who are aggressively advancing their own AI capabilities. A harmonized international regulatory approach will allow AI developers and deployers to operate more efficiently across jurisdictions while maintaining high safety and security standards.

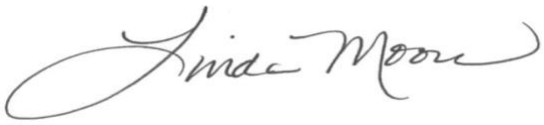
The administration should actively engage foreign nations, particularly in the EU, to push back against harmful and overreaching regulations, prevent non-tariff trade barriers on AI models, and ensure foreign markets are open to American business. This international engagement strategy should protect U.S. market access and promote an innovation-oriented approach, including advocating for adherence to international consensus-based technical standards, the use of existing regulatory frameworks where possible, and AI-specific rules only where gaps exist. It should also promote innovation-enabling policies like open government data and cross-border data flows while opposing forced data localization and protecting AI's algorithmic and source-code integrity.

As the world demands more and more technology, the administration should harness the power of America's technology sector by partnering with industry to provide better solutions abroad. This could include official government programs for exporting U.S. AI and technology solutions that come with certain incentives and expectations attached, including safety and security standards. Through such technology diplomacy, the United States will continue to underpin the global AI ecosystem and support American AI interests.

Conclusion

We applaud the administration for its inclusive approach in gathering diverse stakeholder perspectives to shape the administration's emerging AI policy framework and collaborating with industry on best practices for its AI Action Plan. By pursuing an AI Action Plan that favors flexible regulatory oversight and a risk-based approach rather than restrictive controls, the United States can unlock unprecedented technological advancement and economic growth. Moving forward, we remain eager to collaborate with the administration in developing balanced AI policies that safeguard public interests while ensuring the U.S. maintains its global leadership and continues to foster AI innovation. This balanced approach will be crucial in maintaining America's competitive edge in the rapidly evolving AI landscape.

Sincerely,



Linda Moore
President and CEO