A Framework for America's AI Future:

A Roadmap for Responsible Innovation, Opportunity, and Security

Mark WARNER
U.S. SENATOR FOR VIRGINIA

table of contents

BUILDING AI INFRASTRUCTURE RESPONSIBLY

As companies race to build the infrastructure powering artificial intelligence, communities are increasingly being asked to shoulder the costs—in higher energy demand, increased water consumption, and growing strain on local infrastructure. The United States needs clear rules to ensure this buildout happens responsibly. That means greater transparency, stronger accountability, and federal policies that reward efficient, sustainable development rather than subsidizing projects that externalize their costs onto communities and taxpayers.

The legislative solution:

DATA CENTER TAX ACCOUNTABILITY AND DISCLOSURE ACT OF 2026

As the proliferation of artificial intelligence has accelerated hyperscale data center development in Virginia and across the nation in recent years, states, localities, and residents have raised legitimate concerns regarding the energy and water needs of these facilities and the impacts they may have on their communities – including rising costs and depleted natural resources.

States, localities, and residents need to have accurate information about the electricity and water needs of data centers to make the best decisions for their communities. To do business in states and localities, data center developers and operators should be fully transparent regarding their energy and water needs.

In addition, federal tax policy is supporting continued investment in AI infrastructure and equipment, including the compute systems and data center equipment that enable large-scale AI deployment. To continue accessing certain lucrative tax benefits like bonus depreciation, data centers should be required to meet high efficiency and sustainability standards that reduce burdens on states and communities.

Bonus Depreciation/LEED Certification:

- This legislation incentivizes AI data centers to maximize the efficiency and sustainability of their facilities while significantly reducing their consumption of energy, water, and other natural resources by preventing companies from accessing bonus depreciation unless their AI data centers meet the Platinum or Gold level of Leadership in Energy and Environmental Design (LEED) certification for data centers.

- LEED is a globally recognized green building certification program and provides a framework for constructing, designing, operating, and certifying environmentally responsible and resource-efficient buildings. It is the world's first green building rating system that explicitly addresses data centers.

- By tying bonus depreciation to LEED Platinum and Gold certification, data centers will be incentivized to build more responsibly and sustainably – including by consuming less energy and water, fewer natural resources, and reducing the overall impact of development on the communities in which they are located.

Data Center Disclosures:

- Requires data center operators and developers to provide detailed reports on energy usage and water consumption at their facilities, including the total energy and water consumed at each facility, to the states in which they operate.

- Directs prospective data centers to report their estimated electricity and water consumption no later than 180 days before they commence operations.

- Requires states to provide the data center reports collected to the Department of Energy and Environmental Protection Agency, where the information will be compiled in an annual report and publicly released.

- Allows the Department of Energy and Environmental Protection Agency to fine data center owners and operators that fail to comply or provide false information.

PROMOTING COMPETITION, SAFETY, AND CONSUMER TRUST

The benefits of artificial intelligence will depend not only on what the technology can do, but on the rules that govern how it is deployed and who it serves. Congress has a responsibility to establish clear rules of the road that preserve competition, protect consumers, and encourage innovation without allowing powerful companies to dictate the future of the technology unchecked. By promoting interoperable markets, setting baseline safety expectations, and establishing accountability for high-risk uses of AI, these proposals seek to build public confidence while ensuring responsible innovators can thrive.

The legislative solutions:

ARTIFICIAL INTELLIGENCE ACCESS, GATEKEEPER EXCHANGE, AND NONDISCRIMINATORY TRANSFER ACT

An artificial intelligence agent is a system that can perceive its environment, can act autonomously or according to preestablished rules or objectives, and make decisions with minimal human oversight in service of a defined goal. AI agents are being deployed for research assistance, in cybersecurity and software development, scheduling and email management, customer service and support, and more.

As AI agents become more widespread and consumer-facing, it is critical that customers, whether they be individuals or businesses, have real choices in a marketplace. In order to avoid a market dominated by a few major players and encourage innovation and small business growth, there needs to be real competition. To really work, that consumer choice has to be balanced with reasonable privacy, cybersecurity, and reliability mechanisms – ensuring that consumer-facing AI agents aren't abusing consumers' trust or subjecting them (or services they access) to privacy or security risks. An AI agent that has access to a user's most sensitive data and access rights – including email, e-commerce accounts, and credit cards – must behave in a fiduciary-like manner to protect users.

With the *AI AGENT Act,* agentic AI startups will be able to compete on equal terms with the biggest tech companies – creating new opportunities to tilt the balance back towards consumers. Investment capital and human talent will have more opportunities to grow businesses. Users will be empowered through trusted custodial agents acting on their behalf in a variety of online contexts, such as e-commerce, social media, online personal finance, and travel booking.

Summary

The *AI AGENT Act* opens digital markets up to competition from consumer-empowering digital intermediaries, establishing a framework for an online and connected ecosystem where:

- AI agents are able to openly and securely access a range of online platforms.
- AI agents act with a duty of loyalty to their user.
- AI agents strictly protect user data and privacy, with restrictions on monetizing or otherwise commercially using user data beyond what's strictly necessary.
- Users are able to freely change AI agents and maintain access to certain online platforms, activities, or communities.

This bill will:

- Establish rights and responsibilities for guaranteed secure access by AI agents to certain large online platforms.
- Create a Federal Trade Commission registry of trusted, secure AI agents – with a regulatory environment swift enough to approve innovative user services or quickly curtail products that violate consumers' trust.
- Require AI agents protect users' privacy and user data and act transparently in a user's best interest and in a manner that makes clear to third-party websites and online service providers that an AI agent has valid authorization.
- Direct NIST to identify technical standards and open protocols to make online services more accessible to AI agents and to ensure consensus-based standards around critical mechanisms like authentication.
- Protect businesses, users, and online providers from AI agent abuse or misuse.

SAFEGUARDING AGAINST FABRICATED EXPLOITATION THROUGH ARTIFICIAL INTELLIGENCE (SAFE AI) ACT

Artificial intelligence models have made it easier, faster, and cheaper to generate photorealistic images that are nigh-indistinguishable from actual images. If those tools are used to create child sexual abuse material (CSAM) or non-consensual intimate images (NCII), people are harmed and Congress must act. Many AI model developers want to, and are attempting to, do the right thing and prevent their models from being used to produce CSAM or NCII, and the *SAFE AI Act* recognizes the need for metrics, testing, and robust and secure frameworks to train models against doing so, and a process to identify those models.

Furthermore, taxpayers expect that the U.S. Government will not do business with AI model developers that release AI models that can generate NCII and CSAM, and would ban federal funding for AI models that can generate CSAM and NCII.

Summary

The *SAFE AI Act* will build on existing efforts by industry, law enforcement, and advocates to combat AI-generated CSAM and NCII. The SAFE AI Act is designed so that:

- AI model developers may test their models to demonstrate that a model is incapable of generating CSAM or NCII.
- Federal agencies may not procure AI models that have the ability to generate CSAM or NCII.
- CSAM survivors may seek judicial relief when their likeness is misused in the creation of CSAM.

This bill will:

- Create a NIST-led process to establish a testing process and benchmarks to evaluate an AI model's ability to generate CSAM or NCII, establishing those models that cannot generate CSAM or NCII as verified models.
- Remove all untested AI models or unverified models from federal agencies' IT systems.
- Bar federal agencies from acquiring untested or unverified AI models.
- Prohibit the sale or creation of software designed to circumvent AI models' restrictions on generating CSAM.
- Establish a private right of action for child sexual abuse material survivors to seek judicial relief (including injunctive relief and statutory or liquidated damages) in certain instances where AI models are used to generate CSAM.

PREPARING AMERICA'S WORKFORCE FOR THE ECONOMY OF THE FUTURE

Artificial intelligence will reshape jobs across nearly every sector of the economy. America cannot afford to wait until workers have already been displaced to begin preparing for that transition. The gains from AI should be matched by investments in the people whose jobs and industries will be transformed by it. That means helping workers build new skills, supporting career transitions, strengthening the pipeline of homegrown talent in critical technologies, and ensuring the benefits of AI are shared broadly across the American workforce.

The legislative solutions:

THE NATIONAL WORKFORCE TRANSITION FUND ACT OF 2026

Artificial intelligence is rapidly transforming the American economy. Across industries, employers are deploying artificial intelligence systems that can automate tasks, redesign occupations, reshape hiring pathways, and alter demand for human labor. While AI adoption may increase productivity and create new economic opportunities, it may also contribute to worker displacement, occupational restructuring, reduced demand for some entry-level roles, and regional labor-market disruption.

At the same time, federal tax policy continues to support investment in AI infrastructure and equipment, including the compute systems and data center equipment that enable large-scale AI deployment. Federal workforce systems, however, remain under-resourced and often lack the flexibility, data, and accountability mechanisms necessary to respond to rapid technological change.

The *National Workforce Transition Fund Act* would rebalance federal AI policy by limiting accelerated tax treatment for covered AI infrastructure and dedicating the resulting revenue to worker retention, workforce transition support, labor-market modernization, and employer accountability.

The Fund would be temporary and targeted. It would provide time-limited support to help workers, employers, states, regions, and federal agencies respond to labor-market disruption associated with AI, emerging technologies, occupational restructuring, and related economic transitions.

The purpose of the Fund is not to slow innovation or discourage AI adoption. Rather, it is to ensure that the economic gains associated with AI-driven productivity growth are matched by investments in workers, communities, workforce systems, and labor-market resilience.

The *National Workforce Transition Fund Act* is designed around a simple principle: if federal policy supports the infrastructure enabling large-scale AI deployment, it should also support the workers, communities, and workforce systems navigating the resulting labor-market transition.

More specifically...

- For a period of five years, the bill would disallow bonus depreciation for the property contained within AI data centers and transfer those funds to the National Workforce Transition Fund.

- The National Workforce Transition Fund would be administered by a National Workforce Transition Board. The Board would be headed by the Secretary of the Department of Labor in consultation with the Secretaries of the Department of Education and the Department of Commerce. The Board's main purposes are to develop and publish an annual federal workforce transition plan, administer the use of funds, and publish an annual report assessing the effectiveness of the Fund. The Board would be made up of a tripartite structure, including one-third employer representatives, one-third labor representatives, and one-third government representatives.

- The Board would fund federal and state data modernization, individual training accounts, tuition assistance for in-demand fields, industry-led/sectoral workforce development grants, and employer retention and redeployment grants. The bill also provides flexibility for the Board to fund experimental pilot programs that test innovative workforce interventions and workforce transition support.

PROMOTING HIGH-SKILLED DOCTORAL (PHD) TALENT ACT

The United States is facing an alarming decline in its Ph.D. pipeline, with major universities accepting 15% fewer applicants to doctoral programs in fall 2026 compared to the previous year. A persistent shortfall in the number of domestic students enrolled in doctoral programs – especially in science, technology, engineering, and mathematics (STEM) fields – impedes the capacity of the United States for global leadership in research excellence and technology innovation.

This bottleneck in our domestic talent pipeline is particularly concerning as international competition for research talent and investment accelerates in critical technology fields like AI, cybersecurity, semiconductors, quantum computing, and more. China's research and development (R&D) investment has surpassed that of the United States , while other countries like Canada are investing in programs to attract foreign scientists. And while our domestic talent pool shrinks, recent data shows that China produced nearly 9,000 more STEM doctorates than the United States.

Institutions across the country have already implemented various accelerated degree programs. The United States must strengthen its pipeline of homegrown STEM talent by helping universities establish innovative, reliable pathways for students seeking STEM doctorate degrees in critical technologies.

Summary

- The bill is designed to increase the number of domestic STEM Ph.D.'s by establishing a competitive grant program at the Department of Energy's (DOE) Office of Science – the DOE Strategic Scientific Workforce – to provide funds for universities to establish accelerated doctoral programs in critical or emerging technology areas.

- Accelerated programs must meet certain requirements, such as incorporating structured professional development for each student that includes opportunities for engagement through research rotations at Federal agencies such as the DOE's National Laboratories.

- Accelerated programs must also include education, training, and research rotations designed to develop dual competency in both the student's primary STEM discipline and the application of AI, advanced computing, data science, machine learning, or related computational methods to research in that discipline.

- The grants may be used by universities to establish or support accelerated doctoral programs, as well as to cover not less than three years of the doctoral portion of the program.

- The DOE shall offer workshops that help universities design the curriculum for an accelerated program and develop processes to align course credit mechanism, financial aid, and academic policies for students.

- The bill authorizes the DOE to establish a pilot fellowship program for domestic students that can be replicated and expanded to the larger DOE Strategic Scientific Workforce grant program.

- Not later than one year after the date of enactment, and annually thereafter, DOE shall submit to Congress a report regarding the grant program, including longitudinal tracking of students participating in accelerated programs.

STRENGTHENING AMERICA'S NATIONAL SECURITY

Artificial intelligence will be central to the geopolitical competition of the twenty-first century and America's leadership will depend not only on developing the world's most advanced AI systems, but on ensuring they are secure, resilient, and protected from theft or exploitation by foreign adversaries. The United States must lead in innovation while safeguarding frontier AI technologies, strengthening cybersecurity, improving collaboration between government and industry, and maintaining America's technological edge against competitors like China.

The legislative solution:

SECURE ARTIFICIAL INTELLIGENCE DEVELOPMENT ACT

There are artificial intelligence models that are emerging and are capable of autonomously identifying and exploiting severe software vulnerabilities. These AI models are capable of working faster than humans at these tasks, increasing cyber-attack vectors and requiring significant resources to defend against. Currently, these capabilities are believed to be confined to a few known models, but as model capabilities increase, there must be a statutory structure in place purpose-built to address the need to determine a given model's capabilities prior to the model's public release.

Summary

The Secure AI Development Act will establish a pre-release testing of AI models, improve threat information sharing among industry and the government, and create databases of AI risks, incidents, and vulnerabilities – all to improve the safety of U.S. persons, secure government and critical infrastructure IT systems from national security threats, and protect U.S. industry.

This bill will:

- Create an NSA-led mandatory pre-deployment testing process for frontier models to determine risk.
- Establish a public database for the voluntary submission of AI security and safety incidents and risks, as well as a mechanism to determine the causes of those incidents or risks.
- Create a advisory committee to recommend metrics for evaluating advanced AI models' risk capabilities and to develop best practices for public disclosure of AI model capabilities, for securing access to AI models and AI model labs, and for guiding model developers' safety and security research practices.
- Establish a public registry of frontier artificial intelligence models that have been introduced into interstate or foreign commerce.
- Require an update of the CISA CVE Program and the NIST NVD to account for AI cybersecurity risks and vulnerabilities facilitated or exacerbated by the use of AI.
- Direct an interagency evaluation of the Vulnerabilities Equities Policy and Process focused on AI-related security vulnerabilities.
- Instruct CISA, NSA, and NIST, in collaboration with AI developers, to develop best practices to protect the AI supply chain from risks caused by foreign adversaries.
- Establish a pilot program to share threat information and intelligence with stakeholders to secure the AI supply chain.