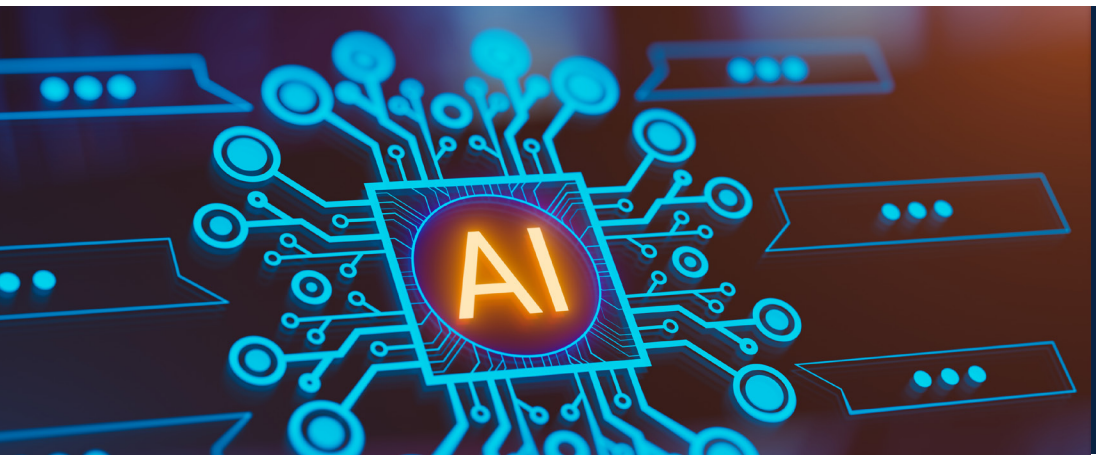
SOLUTIONS BRIEFS

CED



SUSTAINING CAPITALISM

A series focused on nonpartisan reasoned solutions in the nation's interest to the central challenges we face in order to provide prosperity for all Americans.

Principles for AI Guardrails in the US

Safety, Security, and Innovation

The rapid development of artificial intelligence (AI) has the potential to reshape society, the economy, and national security profoundly. The possibilities of AI are vast, with the potential to revolutionize the economy, and open new frontiers in scientific research and discovery. Yet the integration of these technologies into a growing number of applications also has the potential to introduce novel risks ranging from bias and inaccuracy to misuse, disinformation, and weaponization.

American companies lead in AI today. At the same time, to strengthen US technological leadership and national security, lawmakers should develop a policy framework that ensures responsible AI development and use, working to promote safety, security, and innovation simultaneously. The pace of change that AI promises demands that the US take a proactive approach to lead in this era. AI safety and innovation should act as complements, providing businesses and users the certainty to accelerate AI advances and adoption in a responsible manner. Only through collaboration between policymakers and business leaders will the US be able to develop the strategic framework necessary to support the growth of this sector, while establishing guardrails targeted towards the highest-risk AI applications.

This Solutions Brief explores the need for AI guardrails in the US to assure businesses and consumers of AI's safety and fortify US competitiveness. It lays out guiding principles for policymakers as they construct a framework that leverages the administration's ongoing work to review sectoral regulation and government uses of AI, while focusing on high-risk AI use cases and promoting continued innovation in the rapidly evolving AI sector.

Trusted Insights for What's Ahead™

- Prioritizing safety, security, innovation, and transparency will establish an environment that allows US companies to lead responsibly in AI.
- A risk-based approach can best address both needed oversight and continued innovation. Regulatory scrutiny should be calibrated according to the risk that AI poses in applications, particularly where the application would make decisions that impact individuals.
- The US will need to evaluate the applicability of existing US laws and regulations to AI applications in areas including data privacy, intellectual property, and consumer protection.
- The US must lead in developing global and regional standards as the EU, China, and other jurisdictions implement AI frameworks that may challenge US technological leadership and competitiveness.

Recommendations: AI Principles for Safety, Security, and Innovation

Establishing a national AI framework is essential for continued US leadership in the global AI race, ensuring the AI revolution can proceed safely and securely to benefit all Americans. Safety underpins this effort, but innovation and safety should not be in opposition. Rather, a strategic AI framework that can remain adaptive to new technological developments will expedite the path to AI advances and adoption, and societal gains. At the center of this effort should be a risk-based approach that identifies and addresses risks outside the scope of existing structures—and focuses on the context of the application in which AI systems are being used, rather than the technology itself.

1 US Should Aim to Lead in AI

- Commit to the initiatives necessary to lead the global AI race, promoting pathways for innovation and establishing a federal framework that can catalyze responsible development and deployment. Clear rules will provide innovators with the certainty to drive progress.

2 Promote Innovation

- Calibrate standards to promote innovation and not hamper US competitiveness, focusing on propelling advances in AI reliability, model testing, and risk assessment.

3 Prioritize Transparency

- Construct transparency responsibilities commensurate with the risk level of an AI application and each entity's role: AI developers should test and disclose information on their products based on standardized benchmarks, while AI deployers should be transparent to end users about the use of AI.

4 Apply Risk-Based Approach to Setting Standards

- Establish a classification system based on the risk associated with the application in which AI is deployed, with heightened transparency obligations targeting high-risk applications and minimal requirements for lower-risk use cases to preserve space for innovation.

5 Protect Data Privacy

- Handle sensitive personal data under heightened scrutiny and consider establishing an "unacceptable risk" tier that would prohibit activities such as dark pattern analysis or behavioral monitoring. For certain use cases, users should retain the right to control their data and have it deleted.

6 Clarify AI Intellectual Property Rights & Liability

- Add clarity on the treatment of copyrighted works collected or used for AI training, intellectual property rights of AI-generated content, and the extent of liability for AI developers and users.

7 Collaborate with International Allies

- Expand and lead international collaboration on AI principles, seeking framework interoperability with allied partners while leveraging broad cooperation and cutting-edge AI-powered solutions to address risks from malicious actors such as cyber, biochemicals, misinformation, and other weaponization.

8 Mitigate Environmental Impact

- Address the interconnection backlog of renewable energy resources to build grid capacity and resilience, while ensuring that AI research and deployment initiatives drive efficiencies that can offset AI's new capacity demands.

9 Invest in Workforce & Literacy

- Invest in a skilled and adaptive US workforce through expanding training and apprenticeship opportunities; reinvigorating science, technology, engineering, and mathematics (STEM) education; and promoting broad AI literacy.

How Should Policymakers Define AI?

As policymakers approach a US AI framework, it will be necessary to define the scope of AI. The term is used to describe a growing number of technologies, often including types long used in commercial products such as language processing, predictive analytics, and machine learning models. With the introduction of generative AI based on neural networks, these tools have become multimodal general platforms that can digest text, voice, and images from users to return increasingly advanced responses, analyses, images, and videos.

However, policymakers should recognize these tools fall into a continuum of technologies. They are in many ways an extension of the tools already in use but their increasingly broad capabilities open new applications where AI can be leveraged productively across a range of sectors.

As a result, a risk-based US framework should categorize tools according to the risk of how they are deployed, not the underlying technology or its complexity. When deployed for the same application, both simple algorithms and leading AI systems can raise similar risks of error and bias—irrespective of how each is developed and trained. This principle follows the White House Office of Management and Budget guidance to US departments and agencies, which stated that the same protections are required for generative AI as other AI tools, focusing on the potential harms associated with how a system is used.[1]

Today's framework should focus on how the current generation of technologies will be deployed, ensuring that current laws and regulations remain applicable in the context of all AI and automation tools, while constructing a risk-based categorization of the applications where these tools are deployed so that oversight and transparency standards can be appropriately targeted. Guardrails must ensure the framework's risk definitions and standards are as clear and consistent as possible, while avoiding conflicting guidelines.

Need for US Guardrails

The US must capitalize on the AI transition to harness its transformative benefits, including boosting economic growth and productivity, securing networks and data, promoting advances in manufacturing and health care, and opening new possibilities in education and climate resilience. Establishing a US framework of AI guardrails is essential to accelerate innovation while ensuring that AI development and use are safe, secure, and beneficial for society. Policymakers and business leaders should work collaboratively to construct a framework that calibrates existing regulations with AI, addresses the risks in high-risk use cases, and drives safe and secure development of AI systems while ensuring US technological leadership. This framework also must remain adaptable to keep pace with technology's rapid changes.

The administration's Executive Order on Safe, Secure, and Trustworthy AI issued in October 2023 was a necessary first step, providing guidance on AI use and capabilities across federal agencies, while directing agencies to review the applicability of existing regulations within their domains.[2] However, full implementation of a US AI framework will require legislation by Congress to codify the strategy's principles. While this framework must address safety, security, and innovation, a statement of guidelines will serve to mitigate risks and lay the foundation for continued progress.

From the perspective of business users, additional congressional and administration action would help spur further AI advances and adoption. As businesses strategize around AI in their sectors, 62% of firms say they are awaiting clearer AI-specific regulations before proceeding with full implementation.[3] Businesses are assessing how the landscape will evolve, including how AI will impact existing sectoral regulations, AI's profound implications for copyright and intellectual property, and potential liability related to their own and their employees' use of AI tools. Establishing a national framework—one that preempts the disparate AI policies developing across states—will provide clear guideposts to drive the responsible development and deployment of AI, allowing investment and innovation to accelerate.

A key priority is ensuring safety for consumers. The majority of Americans support US guardrails, with 77% of voters believing the government should be doing more to regulate AI and 67% reporting more concern over insufficient regulation of AI than over regulation.[4] AI systems present a number of risks, the severity of which frequently depend on the application. For example, AI models used to make networks or information systems more efficient and secure would present significantly lower risk to individuals' rights or privileges than an AI model used to make consequential decisions on access to housing, employment, or public benefits. While many advanced AI systems can reliably detect fraud, interpret medical scans, and thwart cyberattacks, some of today's most advanced generative AI systems are not 100% accurate and can return incorrect information, known as "hallucination."[5]

AI tools are generally meant to augment the work of humans. They will reshape the workforce, but maintaining human oversight is essential and should be clear in AI applications. To that end, ensuring that automated systems do not become a single point of failure in high-risk applications, such as the operation of critical infrastructure, is of supreme importance. Deployers of AI tools in high-risk situations must retain human oversight and the legal responsibility for actions taken by the systems they use, so long as users have abided by AI providers' instructions for use. Therefore, the framework should focus on AI deployed in high-risk use cases where incorrect AI results and actions pose significantly higher risks. Guardrails should prioritize ensuring safe AI deployment in sectors with significant impact on the rights and privileges of individuals or significant socioeconomic impact, including in health care, banking, employment, and law enforcement.

For example, AI has the potential to revolutionize access to quality health care, yet the deployment of AI technologies in health care settings presents substantial risks, including significant questions of patient privacy.[6] General AI models today are capable of passing medical licensing exams, AI's patient care has scored higher in empathy and quality compared to human physicians, and AI tools allow for earlier and more precise detection of abnormalities.[7] However, AI is not yet at the stage to take on medical diagnosis, procedures, or patient care without human oversight. As the technology evolves, regulators and medical professionals must consider it carefully to ensure safety and reliability, and address thorny issues such as a medical professional's potential liability for a diagnosis relying on AI.

A more immediate risk is the protection of patients' and consumers' data as AI tools streamline medical recordkeeping; priorities must include fortifying cyber defenses with AI-powered capabilities and seeking ways to adapt current legal protections, including those in the Health Insurance Portability and Accountability Act (HIPAA).[8] Addressing any underlying bias embedded in AI tools is also paramount to avoid false and disparate outputs in high-risk cases. As discussed below, existing laws and regulations governing health care are in place to address many of these issues, yet a framework that supports sectoral guidance and addresses any gaps legislatively would help effectively usher in these changes.

Supporters of the rapid deployment of AI must nevertheless acknowledge that the technology has risks. Further AI developments will continue to improve the reliability of these tools, yet the availability of AI tools to malicious actors expands the threat horizon

for the nation's security.[9] In 2023 a group of more than 600 US technology experts and scientists signed an open statement that warned "[m]itigating the risk of extinction from AI should be a global priority alongside other societal-scale risks such as pandemics and nuclear war."[10] It is clear that AI will scale and expand the sophistication of cyberattacks. At the same time, AI-powered cybersecurity capabilities can give defenders the upper hand against this rapidly evolving threat, giving essential sectors in critical infrastructure the ability to fight AI with AI.

The weaponization of AI is also a possibility, widening the potential for autonomous and biological weapons. Policymakers should take precautions against these potential threats, as well as consider secure-by-design principles that ensure businesses are securing every point in the AI development and deployment lifecycle. This should include securing AI supply chains and giving businesses the ability to detect what AI tools are running on their networks and what data is going into those models. Policymakers should also consider establishing an "unacceptable risk" tier for AI applications that could be strictly regulated or prohibited.[11] To face these challenges, US lawmakers must work internationally to expand global coordination with partner countries to promote common standards for security.

Guardrails, Not Regulation

The US has thus far taken a decentralized approach, acting first to produce AI guidance within government, and committing AI investments towards research and building federal AI talent. Issued in October, the Executive Order on Safe, Secure, and Trustworthy Development and Use of AI was a critical first step, providing a comprehensive set of directives to federal agencies to begin developing guidelines for safe AI development and deployment, including policies on procurement and contractors.[12] The order also established the first requirements for testing and disclosure of leading AI models, leveraging an interim solution tied to national security risks.

As Congress approaches legislation to formalize a national AI framework to prevent a patchwork of state regulations, it should continue its pro-innovation approach, fostering continued advances in AI technologies—which are still in early stages—while remaining alert to risks as they become clearer, and as AI-related technology develops and changes. US guardrails must focus on AI's use within the context of each application. While specific applications and use cases will present different levels of risk, many challenges can be addressed by updating existing laws and regulations that govern sectors where AI's impact is expected to be high.

Progress on updating current laws and regulations

The executive order was an important initial step, mandating that agencies review their authorities and existing rules and to consider whether additional rulemaking or legislative action is necessary. This work has proceeded in earnest, achieving all the goals outlined for completion within 180 days.[13] Last year, the Department of Justice, the Federal Trade Commission, the Consumer Financial Protection Bureau (CFPB), and the Equal Employment Opportunity Commission (EEOC) issued a joint statement reiterating the applicability and enforcement of existing rules on non-discrimination and consumer harm.[14]

In health care, the Food and Drug Administration outlined how it would assess AI tools in its medical product authorization process, and has announced the approval of more than 850 AI and machine learning-enabled medical devices.[15] The Department of Health and Human Services (HHS) issued a new rule clarifying non-discrimination principles apply to the use of AI.[16] While HHS notes that HIPAA rules still apply to patients' data privacy, policymakers have highlighted this as an area that should be revisited to ensure that rules reflect how technology-enabled tools alter considerations of data collection, encryption, and patient notification.[17] Other health care regulations are likely to be implicated as well.

In banking and finance, the CFPB issued guidance on credit denials from lenders using AI.[18] The primary US financial markets regulators, the Securities and Exchange Commission and Commodity Futures Trading Commission, have each outlined frameworks for addressing AI risks.[19] The Department of the Treasury issued guidance in March on managing AI-specific cyber risks in the sector.[20]

The Department of Housing and Urban Development and the EEOC each affirmed existing non-discrimination laws apply when AI is used in housing opportunities and employment.[21] Agencies that provide households food and income assistance have also issued guidance on their responsible use of AI.[22] Regarding larger threats, the Cybersecurity and Infrastructure Security Agency issued its first AI safety guidelines for critical infrastructure, while a separate cross-department effort has established a framework focused on mitigating AI risks in biological and chemical national security threats.[23]

On leading generative AI models, the National Institute of Standards and Technology (NIST) built on its AI Risk Management Framework to produce a Generative AI Profile for public comment focused on securely developing foundation models, expanding international standards development in AI, and reducing the risks posed by AI-generated content.[24] The US Copyright Office and the US Patent and Trademark Office are each working on reports on the impact of AI on copyright and intellectual property law.[25] To address AI misinformation, the Federal Communications Commission (FCC) adopted a ruling determining that AI-generated or voice-cloned robocalls are illegal under the Telephone Consumer Protection Act, while the Federal Election Commission is currently working through public comments on the potential regulation of deceptive AI use in political advertising.[26]

This initial work to assess the adequacy of existing laws and regulations for the age of AI will help regulators and Congress identify gaps and prepare rulemaking and legislative updates. Departments and agencies should be supported in this crucial step through to completion, with adequate funding and coordination across the government to ensure that sufficient resources are available to weigh the benefits and risks of AI-enabled products and provide predictable regulatory structures. In sectors where multiple regulators share oversight responsibilities—for example in banking and health care—agencies should work collaboratively in preparing AI guidance and standards to avoid companies having to navigate duplicative or conflicting rules. Still, US industry—both AI developers and users—needs a broader framework to ensure continued US leadership in AI.

Next steps

Much work remains, including how oversight of frontier general-purpose AI (GPAI) models could occur given that their range of applications falls outside traditional sector regulation. How should training of AI models consider data inputs that include personal information or content protected by copyright? Should generative AI providers be protected from liability for user interactions with their tools under Section 230 of the Telecommunications Act?[27] How can policymakers address misinformation through AI-generated content?

Some of these issues are working their way through US courts, including questions on copyright and liability for AI developers and deployers.[28] But Congress can craft a framework to add clarity to these important issues. Through initial work, policymakers have taken an appropriate caution towards regulation that could stifle the sector. Policymakers should prioritize addressing gaps in current sector frameworks, focusing on immediate risks to ensure the deployment of AI tools is done safely and securely.

Importantly, a national framework should, in some way, preempt the wave of state and local AI regulations that has arisen in the vacuum of federal legislation. Colorado was the first state to pass legislation regulating high-risk AI use cases; there are more than 600 active AI-related bills in total across 45 states.[29] Congress should lead a unified and strategic path to ensure responsible US leadership for AI.

Congress' framework should leverage the existing body of work by federal agencies that offered guiding principles to which the private sector has begun aligning. That includes NIST's AI Risk Management Framework that the agency is currently updating, the administration's AI Bill of Rights from 2022, and the October 2023 executive order.[30] As discussed below, the US has also led a growing number of international fora and working groups that can provide a broad outline to inform a US framework that shares common principles with allied and friendly countries, and promotes interoperable security measures.

As Congress approaches the issue, it should commit to fostering a competitive AI sector primed for innovation and dynamism. To achieve this, the framework must rely on principles rather than fixed technical standards that risk obsolescence as technology evolves. Because of the length of the regulatory process and limited regulatory capacity across government, policymakers must have the foresight to target risks selectively where oversight is most needed and embed flexibility that allows the framework to adapt over time so that regulation keeps pace with technology. Policymakers must also avoid picking winners through anticompetitive regulatory barriers that could insulate today's AI leaders from broader competition. For instance, proposals for a licensing regime for AI models could inadvertently stifle innovation, increase costs, and disadvantage smaller-scale and open-source developers. While there is tension between promoting innovation and safety, the goal of a framework should be for them to act as complements. Rules must be clear and consistent, without raising prohibitive compliance costs.

The evolving landscape of AI frameworks across the world underscores the need for the US to craft an alternative set of AI guardrails quickly and diligently. The EU and China are pushing ahead on AI frameworks, leaving US firms and the country as a whole at a

potential disadvantage. In this environment, congressional action to define clearly US guardrails would provide certainty to US AI leaders and American businesses—before other jurisdictions dictate how AI will be regulated.

If the US fails to produce its own guardrails, the US will again defer de *facto* authority to other jurisdictions, impacting US corporations. One example is the EU's General Data Protection Regulation (GDPR), a comprehensive law that set guidelines for the collection and processing of personal data.[31] In lieu of a US alternative, GDPR quickly became a global standard after taking effect in 2018 and applying to multinational companies with an EU presence.[32] As the world's first comprehensive privacy law, it influenced legislation adopted by US states. In the same way that California's 2018 privacy law mimics concepts from GDPR,[33] the growing number of AI bills at the state and local level borrow, to different degrees, from foreign policies in the void left by a lack of action at the national level.[34]

European Union

The EU has again outpaced the world in the space of AI regulation.[35] The EU's AI Act will be the first comprehensive AI law globally.[36] The AI Act is on track to enter into force later this year, with the majority of provisions taking effect within two years. The act classifies AI into risk levels within the context of the AI application, with activities deemed high risk required to fulfill new transparency obligations. High-risk AI will be required to register in a centralized EU database and undergo conformity tests monitored by the EU's new AI Office.[37] Importantly, the bloc recognizes certain beneficial AI use cases, including cybersecurity and fraud prevention, and exempts those capabilities from the definition of high risk. The AI Act also designed a specific regulatory framework for GPAI models under which developers are obligated to provide regulators with technical documentation on their AI training process and evaluation results. Developers must provide publicly a detailed summary of underlying content used to train models. These rules will apply to all AI developers and distributors operating in the EU market or leveraging EU users' data. The EU's framework also relies heavily on GDPR for data protection in the context of AI—a foundation that the US lacks.

United Kingdom

The UK's efforts have mirrored the US with a pro-innovation approach that focuses first on developing a framework for existing regulators to interpret and apply within their sector-specific domains.[38] Select UK regulatory agencies were required to publish their AI annual strategic plans in April, similar to the early work of US agencies.[39] The UK has prioritized initiatives outlined in its National AI Strategy from 2021, launching AI research programs, piloting a new AI Standards Hub to coordinate with global standardization, and updating cross-government standards for AI transparency.[40] However, without introducing new laws or regulation, the framework currently relies on voluntary safety and transparency measures for developers of highly capable AI models. UK officials stated in a follow-up response in February that if AI capabilities continue to expand exponentially, binding measures could be produced if voluntary commitments are deemed insufficient.[41]

Singapore, ASEAN, Japan, and South Korea

In addition to China, other Asian countries—including Singapore, Japan, and South Korea—have taken a range of approaches to AI. Singapore led the 10-country Association of Southeast Asian Nations (ASEAN) to an agreement on principles for AI governance in February[42] but spurned calls from EU officials to align ASEAN's framework with the AI Act's provisions on copyright and AI-generated content.[43] Japan, like the UK, has promoted agile non-binding governance, largely allowing the private sector to self regulate. Japan's 2021 white paper on AI governance remains the country's standard, acting as a comprehensive set of principles to guide AI development and deployment. In addition, Japanese officials maintain that "legally binding horizontal requirements for AI systems are deemed unnecessary at the moment".[44] Japan has also concluded its copyright laws would not be enforced in the case of training generative AI models.[45] In contrast, South Korea is pursuing its own comprehensive AI Act based on risk tiers and transparency reporting for high-risk AI applications. But South Korean officials have pledged wide accessibility to AI technology for all developers without government approval or licensing.[46]

United Arab Emirates

Other countries seeking to grow their technology leadership are also pushing ahead on defining their AI frameworks. The UAE became the first country to establish an AI Ministry in 2017 and produced its initial national AI strategy and ethics guidelines in 2018.[47] The country is promoting an AI-friendly ecosystem without strict requirements for AI developers, instead focusing on advancing research, and accelerating collaboration between public and private sectors. In 2022 the UAE launched an AI & coding license, which instead of acting as a oversight mechanism enables businesses to operate in the country's innovation hubs and facilitates the acquisition of Golden Visas.[48] In recent months the Dubai International Financial Centre also enacted updates to its data protection regulations in an effort to continue attracting foreign investment and companies.[49] Prioritizing competitiveness and innovation, the UAE is also exploring the use of regulatory sandboxes to experiment with AI and study developing global standards.[50] These initiatives have spurred domestic innovation: the Abu Dhabi-funded Technology Innovation Institute launched an open-source AI model, Falcon 2, along the lines of those offered by Google and Meta.[51]

Global agreements

Momentum towards aligning international AI efforts continues to grow as well. The UN and G-7 have each agreed on principles to guide responsible and secure AI development and deployment.[52] The US has also advanced collaboration in bilateral fora, signing a code of conduct within the US-EU Trade and Technology Council in May and announcing a partnership between the US AI Safety Institute and its UK counterpart.[53] A key area of focus for many governments is military use of AI. In November 2023 the Department of State published a declaration on responsible AI and autonomous systems in the military context; nearly 50 countries have signed the declaration.[54]

While the global community is coalescing around sets of shared principles, including on security and non-discrimination, the development of domestic AI policies across these

countries exposes divergent approaches. Further international agreement may prove difficult as countries turn their attention to more specific policy elements, including questions around copyright, data privacy, and surveillance. However, the growing number of international working groups and bilateral agreements can help US officials set and reinforce guidelines in establishing a US framework, one that will ultimately be most effective with greater global coordination and interoperability.

US Competitiveness

Congress should exercise caution towards following any single example from these international frameworks. The EU's framework could impede AI innovation because of several stringent requirements, including mandating registration of high-risk AI by the EU AI Office, which could erect barriers to a competitive AI market for smaller entities. Additionally, the AI Act outlines potentially onerous and wide-reaching requirements for companies that deploy AI tools in high-risk areas, which already must conform their use of AI to sector-based requirements and laws. Those companies must submit fundamental rights impact assessments before deployment, which require descriptions of how companies will use AI in line with developers' instructions; categories of persons that potentially could be affected and the specific harms AI usage could cause; and a summary of the implementation of human-oversight measures. Further, the act's abandonment of a tiered-risk approach for GPAI systems, even when GPAI is applied in otherwise low-risk scenarios, could hinder the development of and access to leading tools.

The US should place greater emphasis on the highest-risk AI uses that China's framework lacks in its exclusion of a defined unacceptable risk tier. Japan's decision that copyright provisions do not apply to AI training content is likely inapplicable in a US context and requires careful assessment given evidence of GPAI's ability to replicate copyrighted works in text and image.[55] US courts are beginning to hear AI-related copyright cases and will likely play a defining role in determining the applicability of copyright. The US Copyright Office is also working through guidance that may provide clarity in the short term, but legislative clarification of this issue could offer foresight on how the economy for artists, designers, musicians, and other creators should be shaped by these technologies.

Other emerging frameworks offer several promising examples for US guardrails. South Korea's consideration of transparency requirements roughly aligning to the EU framework without a full licensing and approval structure is one such example, as is the EU's regulatory exemptions for beneficial AI use cases. Efforts to solidify US AI leadership should also consider business-friendly policies that induce investment and operations of global firms that can spur further innovation. The UAE's prioritization of regulatory flexibility, innovation, and legislative reforms to immigration and data protection are intended to build a foundation for its AI sector to thrive—an important theme for US officials to consider.

While voluntary commitments in the US from AI companies are likely insufficient to mitigate some overarching risks, the US must forge its own framework that breaks from the rigidity of the EU's regulation in key aspects to maintain a truly risk-tiered

approach with calibrated oversight. A US framework would better target risks that should be mitigated after gaps have been identified in existing laws and regulations, while promoting innovation and continued advances. Policymakers should also leverage existing guidance from US agencies and, as appropriate, from globally agreed upon principles, which businesses are already using to manage AI risks before completed frameworks take effect. Efforts to align these standards and promote interoperability for global firms operating across jurisdictions would ease compliance and, done well, expedite adoption of best practices.

Principles for Responsible AI

1) US Should Aim to Lead in AI

The US should commit to the initiatives necessary to lead the global AI race, both in promoting pathways for innovation and in establishing a federal regulatory framework that can catalyze responsible development and deployment. Clear rules will provide innovators with the needed certainty to drive progress forward. The executive order on AI took an important first step to launch a government-wide review of existing laws and regulations to assess where rules and legislation may need to be updated. As Congress approaches formalizing a national AI framework it must work to promote further AI advances, ensure safety for users, and mitigate security and other risks.

Given AI technologies' rapid advances and potential disruption, policymakers should collaborate with business leaders to understand how these tools will be deployed and where more clarity is needed to accelerate progress. A US framework must prioritize making AI safe for all consumers, engaging with civil society to ensure the revolutionary benefits this technology offers are widely shared.

Safety and innovation should not be in opposition but rather work in a complementary fashion as technology advances. A strategic and clear AI framework that can remain adaptive will expedite the path to innovation, adoption, and societal gains from AI tools in a safe manner. A risk-based approach should be at the center of this effort, identifying and addressing risks outside the scope of existing structures. It should focus on the context of the application where AI systems are being used, rather than the technology itself. Gaps do exist in current frameworks for which Congress can provide needed clarity, including on liability and copyright standards.

2) Promote Innovation

AI standards should be calibrated to promote innovation and not hamper US competitiveness in the global AI race. While there is general agreement that issues of safety, privacy, and governance must be addressed, further developments are necessary to advance the reliability and trustworthiness of these technologies, including new ways of testing model performance, metrics for assessing risks, and methods for representing the knowledge and reasoning of AI systems. Applying overly restrictive rules to this nascent space threatens to stall the advances needed to understand these technologies better and preempt the potential economic and societal benefits AI promises in the future.

US legislation should promote a vibrant ecosystem of AI innovation and inclusive development of AI, including by codifying and supporting the National AI Research Resource pilot program.[56] These efforts can widen access to leading research tools and resources to ensure a broad range of individuals and organizations can participate in building the future of AI.

3) Prioritize Transparency

Transparency is the most significant pillar of any responsible AI framework, both now and in the longer term. While further technical developments will likely enhance AI model testing and explainability, a starting place is moving towards a system of baseline documentation and disclosure for AI systems used in areas deemed high-risk.

Each player in the AI ecosystem should have transparency responsibilities commensurate with their respective role in the development and deployment of AI, and transparency requirements will continue as AI continues to develop. For example, AI developers should test and disclose information on their products based on a set of standardized benchmarks. This could include technical documentation, compliance with copyright law, and detailed summaries about the data that was used for training the model. AI deployers should be transparent about the use of AI in certain circumstances and test any changes they have made to their model. Parties should be held accountable for violations of their respective responsibilities. Moreover, data is the fuel for developing and training models; fair, responsible, and trustworthy data will develop responsible and trustworthy AI models.

As AI becomes more ubiquitous, and as more and more software incorporates AI features, a key consideration should be establishing mechanisms to provide full disclosure to users when they are interacting with an automated system, when content has been AI-generated, and when commercial software incorporates AI capabilities. Taking action to identify materially deceptive AI-generated content for political and consumer purposes is particularly urgent as the use of generative AI in the creation of deep fake images and videos has proliferated. In cases where consumers interact with an AI system online, a disclaimer should be displayed to inform consumers. As a broad solution, the US should consider an approach to visually demonstrate that sites and products using AI are safe and trustworthy, similar to the FCC's US Cyber Trust Mark for labeling secure smart products.[57]

A centralized online resource that makes available all AI regulations, voluntary and mandatory standards, and standardized definitions of risk-based levels will ensure a common understanding, helping to harmonize standards across different industries and companies. A shared understanding of data models, model testing, and frameworks can help promote transparency, and drive acceptance and compliance. Given the pace of AI advances, as new forms of model evaluation and risk measurement are introduced, standards should be crafted to encourage adoption of best practices.

4) Apply Risk-Based Approach to Setting Standards

Establishing standards for AI model development and usage should depend on a risk-based classification system that differentiates treatment and oversight of AI applications according to their risk. Low-risk AI applications and smaller-scale research projects should face minimal, if any, regulatory hurdles to encourage innovation. The level of scrutiny should scale as potential risk rises, with the highest risk use cases facing the highest standards of risk mitigation and accountability. The definitions of different risk-based levels should be standardized, as it is crucial to ensure a common understanding that will harmonize the standard across the different industries and companies.

For instance, the EU's AI Act specifies a category of "unacceptable risk" and standards for AI systems classified as "high risk", largely defined as applications that impact the health, safety, or fundamental rights of individuals, including those related to employment, healthmcare, education, banking, and law enforcement where the socio-economic impact of AI applications could be significant. These areas have heightened transparency requirements because of the risks to consumers. The US might also consider developing a select list of applications categorized as "unacceptable risk". The "limited-risk" tier includes algorithmic systems that underlie online platform recommendations, targeted marketing, and customer service chatbots. In the EU these systems are subject to lighter obligations. Finally, AI uses of "minimal risk" comprise the majority of currently available AI tools, including those filtering spam and performing data analysis. Under the EU risk-based approach these applications will not face new regulations; instead, they are obligated to comply with general EU privacy and security rules. This tiered structure ensures adequate oversight of the highest-risk use cases while preserving space for innovation and experimentation for the majority of AI applications.

5) Protect Data Privacy

Data privacy is a foundational pillar of responsible AI development. However, the US currently lacks a federal statutory or regulatory framework governing the collection and usage of personal data. General terms of service may not be sufficient; today a patchwork of state regulations—and, to some extent, non-US regulations that companies with international operations must follow—tends to fill that void. Users and the public should be reasonably assured that online data collected to train AI models is limited to data that is necessary for the specific context (which clearly discloses prohibited data categories, such as biometrics), while users should retain the right to know about their data's use and, in certain cases, the right to have their data deleted. AI providers should adequately disclose the sourcing, necessity, and procedures for using personal data; and data collectors should inform users how they can control the reuse or transfer of personal data for any additional purpose. Personal data related to sensitive areas, including health, employment, finances, and criminal justice should be subject to heightened scrutiny, and indiscriminate surveillance monitoring should be prohibited. Data privacy principles also need to be flexible to accommodate the use of certain data for bias testing and other testing of AI models.

6) Clarify AI Intellectual Property Rights & Liability

The impact of intellectual property (IP) laws on the development and use of AI must be evaluated. First, IP laws should be reviewed to account for the use of data for training AI models that are protected under patent, copyright, or trademark. Second, IP law should clarify protections available to AI-generated content or other AI-enabled IP. It is essential that US agencies—the US Patent and Trademark Office in particular—have the technical expertise, training, and resources needed to expedite review of AI-related patent applications.

Jurisdictions outside the US have taken different tacks in categorizing the underlying data used to train AI models, with the EU explicitly stating that providers of GPAI models must comply with EU copyright law and are obligated to disclose publicly detailed summaries of the content used in training. Other countries, such as Japan, have thus far implicitly supported "fair use" of copyrighted content used for training; however, Japanese officials released draft guidance in December 2023 revisiting the possibility of certain AI training violating copyright laws.[58] Congress' efforts on a US framework should provide clarity on how existing legislation should treat emerging data-driven technologies.

Congress should also add clarity around liability in the AI space, determining whether or how Section 230 protections apply to generative AI providers. Proposals to strip this protection from AI platforms entirely must be reconciled with the potential that doing so could undermine algorithmic innovation by unleashing a flood of litigation. Legislation should understand the different roles of AI creators and deployers, holding them accountable for their role in either developing or deploying AI tools. It is essential to promote both innovation and accountability.

7) Collaborate with International Allies

AI policy benefits from a global vision. Development of the US AI framework should aim to be interoperable with standards of our allies and partners. This alignment will ease compliance to promote swift adoption of new standards, as well as open investment opportunities with friendly partners to expand the potential market for US firms operating globally.

The US participates actively in existing international fora and standard-setting organizations, each with workstreams reviewing AI standards and codes of conduct. The largest global fora—the UN, the Organization for Economic Cooperation and Development, and G-7—have each produced principles that should can help align of US policy efforts with those of partner countries.[59] The US must also continue advancing bilateral principles, such as through the joint EU-US Trade and Technology Council, and the growing UK-US partnership that combines the efforts of each country's AI Safety Institute.[60] The Department of Commerce tasked the new US AI Safety Institute with facilitating the development of US safety standards and working with institutions in partner nations to coordinate international alignment.[61]

The US must expand and lead these international efforts. Global collaboration and agreement on standards is the best way to address risks of bad actors leveraging the technology to expand disinformation, enhance cyberattacks, or develop other forms of weaponization.

8) Mitigate Environmental Impact

AI will require higher electricity capacity to power the growing fleet of data centers that will be used for training and processing user requests. Researchers estimate that AI's computational power will double every 100 days, with global AI-related energy demand increasing between 26% and 36% annually in the coming years.[62] Robust and reliable power infrastructure to meet this demand is essential.

In its 2023 *Long-Term Reliability Assessment,* the North American Electric Reliability Corporation underscored that US officials must address backlogs in transmission development and build resilience into the energy grid to meet the demands of new technologies and mitigate weather-related disruptions.[63] At the beginning of 2024 the US had nearly 12,000 projects awaiting approval for grid connection, with 95% comprising solar, wind, and battery storage projects.[64] Eliminating this backlog would add 2,600 gigawatts to America's grid—tripling current electricity capacity.[65]

AI also presents unprecedented opportunities for grid optimization and efficiencies throughout supply chains to help the US meet its energy and climate goals.[66] AI tools can allow businesses to optimize industrial facilities, electricity generation, and transmission and distribution assets.[67] Policymakers should expedite the permitting and interconnection of additional renewable energy resources to meet current and expected demand, while ensuring that AI research and deployment initiatives are targeted to drive efficiencies that can offset AI's new capacity needs.

9) Invest in Workforce & Literacy

Finally, investing in a skilled and adaptive US workforce is perhaps the most important key to a successful AI transition.[68] Ensuring that workers and students have the necessary skills to adapt today and lead in the future is critical both to maximizing AI's potential while mitigating its risks. Across K-12, community college, university, and training programs, STEM curricula that foster foundational technical skills must be reinvigorated. Policymakers must focus on expanding training programs and apprenticeship opportunities in technology, as well as in other in-demand fields such as health care where AI will be critical to future workforce success. Leveraging partnerships and guidance from business leaders is essential to these efforts to inform policymakers on in-demand skills and training curricula, with the aim of developing pipelines for local workforces.

Government, too, must upskill its AI workforce to build internal expertise. While the recent AI Talent Surge is a promising start, these efforts must continue as agencies become increasingly engaged with AI adoption, and as AI tools can improve government processes and delivery of public services.[69]

Digital and AI literacy are also becoming essential skills for everyone. We can start by ensuring AI use in the classroom is guided by best practices to prepare the next generation of workers whose careers will be shaped by these tools. We can also begin to explore the opportunities AI presents for expanding access to education and training by exploring the potential for individualized learning.

Conclusion

Swiftly establishing a comprehensive framework of guardrails for AI to protect the rights and privileges of individuals is crucial for maintaining US technological leadership, and mitigating the most immediate safety and security risks that AI applications pose. At the same time, US policymakers' caution toward erecting stringent AI regulation is warranted, as this nascent technology continues to develop.

Instead, the rapid evolution of AI technologies requires a comprehensive and agile approach that promotes innovation while addressing identifiable risks such as bias, misuse, and security threats. A risk-based regulatory framework that focuses on high-risk AI applications and prioritizes transparency, data privacy, and intellectual property rights will help reach this goal. A robust and strategically oriented US framework will foster trust, drive innovation, and safeguard societal interests to ensure the US can harness AI's transformative potential responsibly and sustainably.

Endnotes

1 Office of Management and Budget, *OMB Releases Implementation Guidance Following President Biden's Executive Order on AI*, November 1, 2023.

2 The White House, *Executive Order on the Safe, Secure, and Trustworthy Development and Use of AI*, October 30, 2023.

3 Jessica Apotheker et al., *From Potential to Profit with Generative AI*, Boston Consulting Group, January 12, 2024.

4 AI Policy Institute, *Overwhelming Majority of Voters Believe Tech Companies Should be Liable for Harm Caused by AI Models*, September 19, 2023; Michelle Faverio and Alex Tyson, *What the Data Says about Americans' Views of AI*, Pew Research Center, November 21, 2023.

5 Yue Zhang et al., *Siren's Song in the AI Ocean: A Survey on Hallucination in Large Language Models*, Cornell University, September 3, 2023.

6 Shuroug A. Alowais et al., *Revolutionizing Health Care: The Role of AI in Clinical Practice*, BMC Medical Education 23, no. 689, September 22, 2023.

7 Harsha Nori et al., *Capabilities of GPT-4 on Medical Challenge Problems*, Microsoft, March 2023; John W. Ayers et al, *Comparing Physician and AI Chatbot Responses to Patient Questions Posted to a Public Social Media Forum*, JAMA Network 183 no. 6 (April 28, 2023):589–596; Patrick Boyle, *Is it Cancer? AI Helps Doctors Get a Clearer Picture*, Association of American Medical Colleges, March 28, 2024.

8 Eren Bali, *More Personal Visits: Introducing AI-Enabled Hands-Free Charting*, Carbon Health, June 5, 2023; See: *Health Insurance Portability and Accountability Act of 1996*.

9 Daniel Colson, *Overwhelming Majority of Voters Believe Tech Companies Should be Liable for Harm Caused by AI Models*, the AI Policy Institute, September 19, 2023.

10 Center for AI Safety, *Statement on AI Risk: AI Experts and Public Figures Express Their Concern About AI Risk*, accessed May 12, 2024.

11 Christine Lai and Jonathan Spring, *Software Must Be Secure by Design and AI Is No Exception*, Cybersecurity and Infrastructure Agency, August 18, 2023.; Future of Life Institute, *High-level Summary of the AI Act*, February 27, 2024.

12 The White House, *Executive Order on the Safe, Secure, and Trustworthy Development and Use of AI*.

13 The White House, *Biden-Harris Administration Announces Key AI Actions 180 Days Following President Biden's Landmark Executive Order*, April 29, 2024.

14 Federal Trade Commission, *Joint Statement on Enforcement Efforts Against Discrimination and Bias in Automated Systems*, April 25, 2023.

15 Food and Drug Administration, *AI and Medical Products: How CBER, CDER, CDRH, and OCP are Working Together*, March 2024; Food and Drug Administration, *AI and Machine Learning (AI/ML)-Enabled Medical Devices*, May 13, 2024.

16 Department of Health and Human Services, *HHS Issues New Rule to Strengthen Nondiscrimination Protections and Advance Civil Rights in Health Care*, April 26, 2024.

17 Department of Health and Human Services, *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, March 18, 2024.; Federal Register, *H.R.3103: Health Insurance Portability and Accountability Act of 1996*, Public Law No. 104-191, August 21, 1996; Senator Bill Cassidy, *Request for Information on Safeguarding Patient Privacy*, September 7, 2023.

18 Consumer Financial Protection Bureau, *CFPB Issues Guidance on Credit Denials by Lenders Using AI*, September 19, 2023.

19 Securities and Exchange Commission Investor Advisory Committee, *Establishment of an Ethical AI Framework for Investment Advisors*, April 6, 2023; Commissioner Kristin N. Johnson, *Statement on the CFTC RFC on AI: Building a Regulatory Framework for AI in Financial Markets*, Commodity Future Trading Commission, January 25, 2024.

20 Department of the Treasury, *Managing AI-Specific Cybersecurity Risks in the Financial Services Sector*, March 2024.

21 Department of Housing and Urban Development, *HUD Issues Fair Housing Act Guidance on Applications of AI*, May 2, 2024; Equal Employment Opportunity Commission, *EEOC Releases New Resource on AI and Title VII*, May 18, 2023.

22 Department of Agriculture, *Framework for State, Local, Tribal, and Territorial Use of AI for Public Benefit Administration*, April 29, 2024; Department of Health and Human Services, *HHS Shares its Plan for*

Promoting Responsible Use of AI in Automated and Algorithmic Systems by State, Local, Tribal, and Territorial Governments in the Administration of Public Benefits, April 29, 2024.

23 National Science and Technology Council, *Framework for Nucleic Acid Synthesis Screening*, April 2024.

24 National Institute of Standards and Technology, *AI Risk Management Framework: Generative Artificial Intelligence Profile*, April 2024.

25 Federal Register, *US Copyright Office Notice of Inquiry on AI and Copyright*, August 30, 2023; Federal Register, *Patent and Trademark Office Request for Comments regarding the Impact of the Proliferation of AI on Prior Art, the Knowledge of a Person Having Ordinary Skill in the Art, and Determinations of Patentability Made in View of the Foregoing*, April 30, 2024.

26 Federal Communications Commission, *FCC Makes AI-Generated Voices in Robocalls Illegal*, February 8, 2024.; Federal Election Commission, *Comments Sought on Amending Regulation to Include Deliberately Deceptive AI in Campaign Ads*, August 16, 2023.

27 Federal Register, *S.652: Telecommunications Act of 1996*, Public Law No. 104-104, February 8, 1996; Legal Information Institute, *47 US Code § 230: Protection for Private Blocking and Screening of Offensive Material*, Cornell Law School, accessed May 10, 2024.

28 Michael Grynbaum and Ryan Mac, *The Times Sues OpenAI and Microsoft Over AI Use of Copyrighted Work*, New York Times, December 27, 2023; Rebecca Cahil, *OpenAI Defamation Lawsuit: The First of its Kind*, Syracuse Law Review, June 22, 2023.

29 Colorado General Assembly, *SB24-205: Consumer Protections for AI*, May 17, 2024.

30 National Institute of Standards and Technology, *AI Risk Management Framework (AI RMF 1.0)*, January 2023; The White House, *Blueprint for an AI Bill of Rights*, October 2022; The White House, *Executive Order on the Safe, Secure, and Trustworthy Development and Use of AI*.

31 European Parliament, *General Data Protection Regulation*, April 27, 2016.

32 Marco Luisi, *GDPR as a Global Standards? Brussels' Instrument of Policy Diffusion*, E-International Relations, April 9, 2022.

33 State of California, *The California Consumer Privacy Act of 2018*, Assembly Bill No. 375, April 28, 2018; Reece Hirsch and Kristin M. Hadgis, *California's New, GDPR-Like Privacy Law Is A Game Changer*, Bloomberg Law, August 2018.

34 Devika Kornbacher and Dessislava Savova, *EU and US AI Regulatory Push Overlaps Across Global Business*, Bloomberg Law, March 22, 2024.

35 Kelvin Chan, *Europe Agreed on World-leading AI Rules. How Do They Work and Will They Affect People Everywhere?*, Associated Press, December 11, 2023.

36 European Parliament, *AI Act*, March 13, 2024; Kelvin Chan, *Europe's World-first AI Rules Get Final Approval from Lawmakers. Here's What Happens Next*, Associated Press, March 13, 2024.

37 European Commission, *European AI Office*, May 14, 2024.

38 UK Office for AI, *A Pro-Innovation Approach to AI Regulation*, August 3, 2023.

39 UK Office of the Secretary of State for Science, Innovation and Technology, *Request for Regulators to Publish an Update on Their Strategic Approach to AI: Secretary of State Letters*, February 14, 2024.

40 UK Office for AI, *National AI Strategy*, December 18, 2022; UK Research and Innovation, *AI Research Resource Funding Opportunity Launches*, January 24, 2024; Alan Turing Institute, *About the AI Standards Hub*, accessed May 10, 2024; UK Office for AI, *A Guide to Using AI in the Public Sector*, October 18, 2019.

41 UK Department for Science, Innovation, and Technology, *Consultation Outcome: A Pro-innovation Approach to AI Regulation: Government Response*, February 6, 2024.

42 Association of Southeast Asian Nations, *ASEAN Guide on AI Governance and Ethics*, February 2024.

43 Fanny Potkin et al., *Exclusive: EU's AI Lobbying Blitz Gets Lukewarm Response in Asia*, Reuters, July 19, 2023.

44 Japan Expert Group on AI Principles Implementation, *AI Governance in Japan Version 1.1*, July 9, 2019.

45 Hiroyuki Omoto and Kaoru Yamada, *Japan Panel Pushes to Shield Copyrighted Work from AI Training*, Nikkei Asia, December 21, 2023.

46 Taeyoung Roh and Ji Eun Nam, *South Korea: Legislation on AI to Make Significant Progress*, Kim and Chang, March 6, 2023.

47 Omar Sultan Al Olama, *UAE AI Minister Omar Al Olama on the Era of AI*, Atlantic Council, April 19, 2024; UAE National Program for AI, *UAE National Strategy for AI 2031*, 2018; Smart Dubai Office, *AI Ethics Principles and Guidelines*, December 30, 2018.

48 Emirates News Agency WAM, *UAE Launches Ground-breaking AI and Coding License*, March 1, 2022.

49 Dubai International Financial Centre Commissioner of Data Protection, *Overview of DIFC Data Protection Law and Regulations*, April 30, 2024.

50 UAE Telecommunications and Digital Government Regulatory Authority, *Regulatory Sandboxes in the UAE*, February 1, 2024; Marissa Newman, *OpenAI's Altman Sees UAE as World's AI Regulatory Testing Ground*, Bloomberg, February 13, 2024.

51 Technology Innovation Institute, *Falcon 2: UAE's Technology Innovation Institute Releases New AI Model Series, Outperforming Meta's New Llama 3*, May 13, 2024.

52 European Commission, *Hiroshima Process International Guiding Principles for Advanced AI System*, October 30, 2023; UN General Assembly, *General Assembly Adopts Landmark Resolution on Steering Artificial Intelligence towards Global Good, Faster Realization of Sustainable Development*, March 21, 2024.

53 The White House, *US-EU Joint Statement of the Trade and Technology Council*, May 31, 2023; Department of Commerce, *US and UK Announce Partnership on Science of AI Safety*, April 1, 2024.

54 Department of State, *Political Declaration on Responsible Military Use of AI and Autonomy*, November 9, 2023; Department of State, *Inaugural Plenary Meeting of States Endorsing the Political Declaration on Responsible Military Use of AI and Autonomy*, March 19, 2024.

55 Omoto and Yamada, *Japan Panel Pushes to Shield Copyrighted Work from AI Training*; Grynbaum and Mac, *The Times Sues OpenAI and Microsoft*; Susan Abramovitch and Madison MacColl, *AI Image Generators: Drawing Infringement Claims, Not US Copyright Protection*, Gowling WLG, March 13, 2023.

56 National Science Foundation, *National AI Research Resource Pilot*, accessed May 12, 2024.

57 Federal Communications Commission, *FCC Creates Voluntary Cybersecurity Labeling Program for Smart Products*, March 14, 2024.

58 Copyright Research and Information Center, *Copyright Law of Japan*, accessed May 10, 2024; Omoto and Yamada, *Japan Panel Pushes to Shield Copyrighted Work from AI Training.*

59 UN General Assembly, *Seizing the opportunities of Safe, Secure, and Trustworthy AI;* European Commission, *Hiroshima Process International Guiding Principles for Advanced AI System*, October 30, 2023; Organization for Economic Cooperation and Development, *Recommendation of the Council on AI*, May 2024.

60 The White House, *US-EU Joint Statement of the Trade and Technology Council*, April 5, 2024; Department of Commerce, *US and UK Announce Partnership on Science of AI Safety*, April 1, 2024.

61 Department of Commerce, *At the Direction of President Biden, Department of Commerce to Establish US AI Safety Institute to Lead Efforts on AI Safety*, November 1, 2023.

62 Beena Ammanath, *How to Manage AI's Energy Demand—Today, Tomorrow, and in the Future*, World Economic Forum, April 25, 2024.

63 North American Electric Reliability Corporation, *2023 Long-Term Reliability Assessment*, December 2023.

64 Joseph Rand et al., *Queued Up: 2024 Edition Characteristics of Power Plants Seeking Transmission Interconnection*, Lawrence Berkeley National Laboratory, April 2024.

65 Lindsey Buttel, *America's Electricity Generation Capacity 2024 Update*, American Public Power Association, April 2024.

66 June Kim, *Four Ways AI Is Making the Power Grid Faster and More Resilient*, MIT Technology Review, November 22, 2023.

67 Alex Heil and Ivan Pollard, *Smart Power: Will AI Spike Electricity Demand or Reduce It Through Efficiencies?*, The Conference Board, May 30, 2024.

68 The Committee for Economic Development, *Future-Proofing the Workforce for the AI Era*, The Conference Board, April 15, 2024.

69 US Office of Personnel Management, *OPM Highlights Key Actions Supporting AI Talent Surge to Recruit and Hire AI Professionals*, May 20, 2024.

SUSTAINING CAPITALISM

Achieving prosperity for all Americans could not be more urgent. Although the United States remains the most prosperous nation on earth, millions of our citizens are losing faith in the American dream of upward mobility, and in American-style capitalism itself. This crisis of confidence calls for reasoned solutions in the nation's interest to provide prosperity for all Americans and make capitalism sustainable for generations to come. In 1942, the founders of the Committee for Economic Development (CED), our nation's leading CEOs, took on the immense challenge of creating a rules-based postwar economic order. Their leadership and selfless efforts helped give the United States and the world the Marshall Plan, the Bretton Woods Agreement, and the Employment Act of 1946. The challenges to our economic principles and democratic institutions now are equally important. So, in the spirit of its founding, CED, the public policy center of The Conference Board, releases a series of CED Solutions Briefs throughout the year. These briefs address today's critical issues, including health care, the future of work, education, technology and innovation, regulation, US global competitiveness, geo-economics, infrastructure, inequality, climate, energy and nature, and fiscal health.

THE CONFERENCE BOARD

THE CONFERENCE BOARD is the member-driven think tank that delivers Trusted Insights for What's Ahead™. Founded in 1916, we are a nonpartisan, not-for-profit entity holding 501 (c) (3) tax-exempt status in the United States.

WWW.CONFERENCEBOARD.ORG

THE COMMITTEE FOR ECONOMIC DEVELOPMENT (CED) is the public policy center of The Conference Board. The nonprofit, nonpartisan, business-led policy center delivers trusted insights and reasoned solutions in the nation's interest. CED Trustees are chief executive officers and key executives of leading US companies who bring their unique experience to address today's pressing policy issues. Collectively, they represent 30+ industries and over 4 million employees.

WWW.CONFERENCEBOARD.ORG/US/COMMITTEE-ECONOMIC-DEVELOPMENT

This is a Policy Statement of the Committee for Economic Development of The Conference Board (CED). The recommendations presented here are not necessarily endorsed by all trustees, advisers, contributors, staff members, or others associated with CED or The Conference Board.