AI COMPETITION CENTER

A Policy Framework for Powering America's AI Future

Table of Contents

Foreword by Chip Pickering

Since its founding in 1982, INCOMPAS has established itself as a prominent trade association in Washington, D.C., dedicated to promoting open networks, open markets, and the open Internet. Representing a broad tent of competitive communications and infrastructure leaders, as well as technology companies, INCOMPAS has a long and consistent history of championing policies that foster innovation, competition, and consumer choice. From its inception, the association has been instrumental in advocating for a fair and open telecommunications landscape, pushing back against monopolistic practices and ensuring that new entrants can thrive in a competitive market. This commitment has positioned INCOMPAS as a critical voice in the evolution of U.S. telecommunications and technology and telecommunications policy. Through the Artificial Intelligence Competition Center (AICC), INCOMPAS now continues its important policy development work, seeking to educate stakeholders on the implications of artificial intelligence (AI) and to chart a policy path forward.

The policy recommendations in this report are focusing squarely on our top priority: creating an AI framework that works for every American. Yet, we must also acknowledge the reality of the challenges and opportunities ahead, particularly as the geopolitical map becomes ever more complex and technology becomes more central to our national security. Consequently, this framework also recognizes that it is vital to protect and advance our competitiveness on the world stage.

As we begin, it is important to remember that when it comes to technology policy, the old adage that all that is past is prologue is certainly instructive. The AI policy debate and its associated governance requirements reflect a similar approach to the regulatory frameworks that shaped the early Internet in the 1990s. During this period, lawmakers crafted a series of foundational policies that laid the groundwork for the Internet as we know it today. That early framework did not come in one omnibus "Internet Act," but rather through a series of laws that required a resolute commitment to harnessing our country's innate culture of entrepreneurialism, innovation, and global competitiveness.

Specifically, these steps included landmark legislation like the Cable Act of 1992, the spectrum auction provisions in the 1993 budget, the Communications Assistance for Law Enforcement Act (CALEA), the Telecommunications Act of 1996 with its critical Section 230, and later, the Digital Millennium Copyright Act (DMCA) and the Children's Online Privacy Protection Act (COPPA) in 1998.

These were transformational laws, the broadly positive effects of which we are still enjoying today. Each of these pieces of legislation addressed different facets of the emerging Internet ecosystem, from infrastructure and competition to copyright and children's privacy. But, crucially, they had a spirit of bipartisanship and shared American principles at their core. They were also underpinned by a belief that technology, advanced through thoughtful policies, would ultimately lead to greater prosperity and well-being for the United States and its citizens.

Notably, these early Internet laws were products of a bipartisan consensus; they were not ideological or zero-sum. They were achieved through a spirit of cooperation that transcended political divisions to forge a path for the digital age. Despite a divided government, policymakers of the 1990s understood the need for a balanced approach to fostering innovation while addressing emerging challenges.

The AI policy framework recommended here seeks to replicate that balance, offering guidance that could ensure the responsible development of AI technologies while promoting competition and safeguarding fundamental rights. In this report, we approached the issues from three perspectives: the mission and founding principles of AICC, a general cross-cutting framework, and, finally, topic-specific AI pillars that feature findings and policy suggestions.

While the two latter perspectives will be elaborated upon later, I'd like to remind you of the AICC's core philosophy here. The mission of the AICC served as the foundation of our national policy framework:

"Our mission is to promote a competitive, trusted, and innovative AI ecosystem for the benefit of all Americans."

This mission not only serves U.S. national, geopolitical, and economic interests, but forms the basis of creating a policy framework that can secure far-reaching economic prosperity and well-being for U.S. citizens.

Just as the early Internet policy framework withstood the test of time, this AI framework aims to provide a durable and resilient yet iterative foundation, one that will support future innovations in an increasingly AI-driven world.

Executive Summary

Our research has provided us with both broad takeaways and topic-specific insights, which we have summarized below.

A Cross-Functional Framework

- The U.S. would benefit from a "whole of government" approach, with much greater coordination across agencies, to ensure consistency and clarity for the private sector and the public. Furthermore, the federal government will need to work closely with the private sector and civil society, as well as with its international allies, to tackle this momentous challenge.
- We believe in an "All of the Above" approach to AI policy whereby —– according to user needs —– both open source and closed AI models should advance to meet marketplace demands.

Economic Leadership & Innovation

- An open, competitive marketplace encourages entrepreneurship, innovation, technological advancement, and diffusion. Reforming procurement processes will expand opportunities for startups and SMBs to compete for government AI contracts, giving innovative smaller players an avenue for growth.
- The government can help build out regional growth by establishing regional tech hubs beyond traditional centers to drive nationwide innovation.
- Our workforce is a key asset that has been the cornerstone of American innovation and productivity. We call for an "AI Education for All" program that not only upskills and retrains existing workforces, but also revamps the education system to prepare a new generation of workers for the jobs and economic opportunities of the future.

Infrastructure Modernization

- The fundamental infrastructure to build out AI begins with inclusive broadband. In order to support broadband network availability, policymakers should break down existing barriers to fast and affordable deployment.
- Energy constraints present a significant challenge to scaling AI. We will need not only to build competitive electricity markets, but also resilient ones by acting quickly to invest and by thinking creatively to use technology and diversify energy sources.
- This critical juncture also presents us with an unmatched opportunity: America can take advantage of two major technology revolutions occurring simultaneously. Policymakers can act to ensure that the U.S. leads in AI and the energy revolution, promoting policies that drive cutting-edge innovation and investment in both sectors. Such an approach could create new jobs and position America to thrive in the world economy. The US now needs a comprehensive "all-of-the-above" energy strategy that pairs robust fiber networks with abundant data center capacity.

National Security

- The best way to lead and protect the world from bad actors and misuse of AI technologies will be to harness the American strengths of openness, innovation and entrepreneurial talent in the defense of our nation and for the security of our economy, businesses and all Americans.
- The U.S. must use and develop its resources wisely as part of a national security strategy. Education and workforce are also vital components of this. The U.S. will also have to be agile in organizing and integrating data as a key component of national security. Furthermore, the U.S. can be a leader in strengthening collaboration with like-minded allies to ensure that democratic values are integrated into AI systems across the world.

- On a tactical level, the broad, strategic strokes of national security should be fortified by granular efforts to strengthen AI cybersecurity. A consistent, national approach to security will not only lessen vulnerabilities but also make it easier for companies to navigate and implement policies, fostering competition. Policymakers will have to pay special attention to increasing cyber-attacks, especially on critical infrastructure.

Legal Framework and Consumer Protection

- Forward-looking and adequate legal protections are another key foundation for competitive AI. Federal privacy and liability laws would provide consumers and regulators with consistent standards while giving companies clear guidelines instead of forcing them to navigate a complex patchwork of jurisdictions. Liability regulation needs to clearly and appropriately delineate the various roles and obligations of actors in the AI value chain.

Introduction

With the advancement of AI, the world is on the cusp of groundbreaking and transformative economic, political, and social change. AI promises to deliver significant economic and societal benefits but also holds great geopolitical risks and potential social changes.

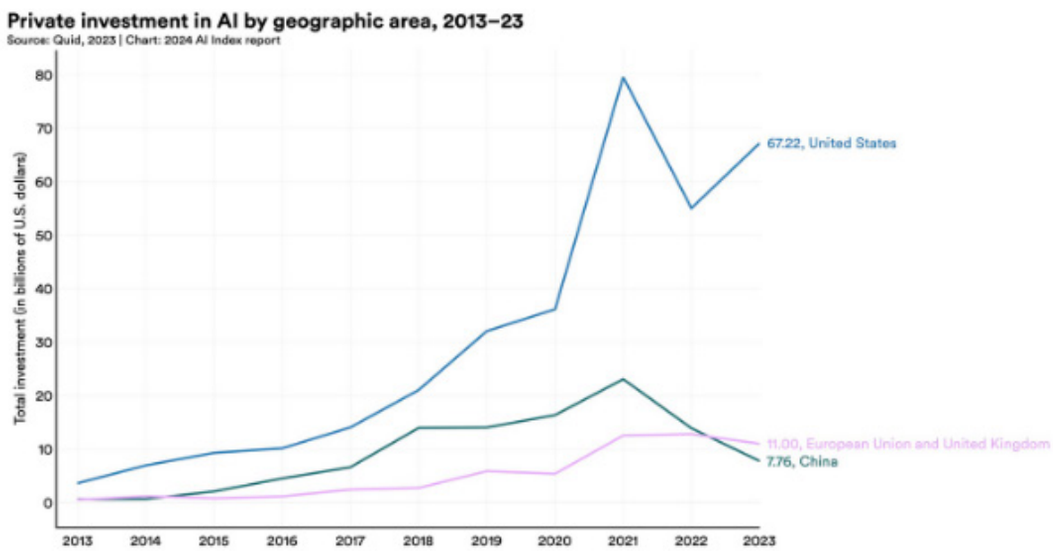
As we work to understand how to leverage its best qualities and develop a solid policy framework, AI is advancing by leaps and bounds. Its performance capabilities are progressing meteorically: OpenAI's GPT models went from outperforming 10% of those taking the U.S. bar exam to surpassing 90% of them within one year.[1] It is no wonder that companies are trying to integrate AI's extraordinary capabilities into their operations. A recent McKinsey Global Survey found that 65% of organizations are deploying generative AI to drive efficiency; this figure is double that of a previous survey conducted ten months prior.[2]

Concurrent with technological and market developments is a rising geopolitical challenge. After decades of increasing integration through globalization, the pendulum has swung back to a multipolar world, one that particularly places the U.S. and China at odds. Tech competition is, in fact, geopolitical competition, and nowhere is this more evident than in the battle for AI superiority. The U.S. is leveraging its strengths in its well-developed, dynamic technology sector and entrepreneurship ecosystem. China is taking advantage of its capacity for centralized planning– including a National Data Administration– and access to vast amounts of data.

Globally, an estimated $1 trillion of spending is expected across the AI sector, which will include investments in compute, semiconductor chips, data centers, energy, and other infrastructure.[3] Currently, the U.S. leads in private AI investment: AI investment in the

[1]Andrew McAfee, "Generally Faster: The Economic Impact of Generative AI," April 25, 2024, https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/Generally_Faster_-_The_Economic_Impact_of_Generative_AI.pdf.
[2]Alex Singla, Alexander Sukharevsky, Lareina Yee, Michael Chui and Bryce Hall. "The state of AI in early 2024: Gen AI adoption spikes and starts to generate value," May 30, 2024, https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai.
[3]Goldman Sachs, "Gen AI: Too Much Spend, Too Little Benefit," Global Macro Research, Issue 129, June 25, 2024,

U.S. was around $67 billion in 2023 — almost 9 times more than China, which is the second closest country to the U.S. in terms of investment. The United States experienced an increase of 22.1% in 2022, while private AI investment in China and the European Union declined by 44.2% and 14.1%, respectively.[4]



Source: The AI Index Report 2024

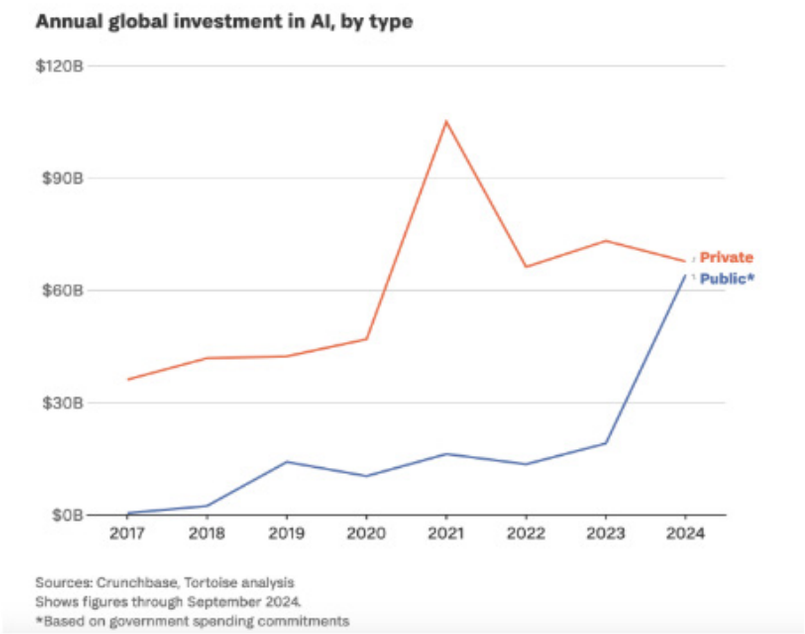
In addition, public AI investment is rising relative to private investment, and it is crucial that the U.S. government does not fall behind on this front. In its 2017 "Next Generation AI Development Plan," China determined that AI was a "strategic technology" and set forth a plan whereby it would lead global AI investments by 2030.

---

https://www.goldmansachs.com/images/migrated/insights/pages/gs-research/gen-ai--too-much-spend,-too-little-benefit-/TOM_AI%202.0_ForRedaction.pdf.

[4]Nestor Maslej, Loredana Fattorini, Raymond Perrault, Vanessa Parli, Anka Reuel, Erik Brynjolfsson, John Etchemendy, Katrina Ligett, Terah Lyons, James Manyika, Juan Carlos Niebles, Yoav Shoham, Russell Wald, and Jack Clark, "The AI Index 2024 Annual Report," AI Index Steering Committee, Institute for Human-Centered AI, Stanford University, Stanford, CA, April 2024,https://aiindex.stanford.edu/report/

[2]James Black, Mattias Eken, Jacob Parakilas, Stuart Dee, Conlan Ellis, Kiran Suman-Chauhan, Ryan Bain, Harper Fine, Maria Chiara Aquilino, Mélusine Lebret and Ondrej Palicka, "Strategic competition in the age of AI: Emerging risks and opportunities from military use of artificial intelligence," RAND Corporation, 2024, https://www.rand.org/pubs/research_reports/RRA3295-1.html



Source: Tortoise Media

Concurrently, the U.S. is leading in technology development: in 2023, 61 major AI models came from U.S. entities, a number significantly higher than the 21 originating from the EU and 15 from China.[6] Nevertheless, Chinese AI companies are also making inroads, and some seem to be catching up with U.S. capabilities.[7] Furthermore, China will also graduate almost double the number of U.S. STEM students by 2025 and is overtaking the U.S. in scientific article publications.[8] The imperative for continued investment in education and research is abundantly clear.

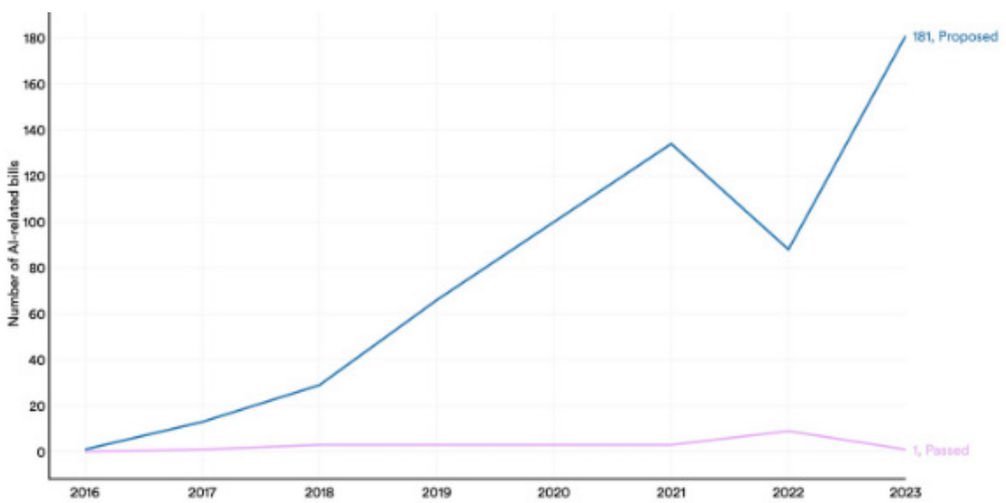
---

[6]Nestor Maslej, Loredana Fattorini, Raymond Perrault, Vanessa Parli, Anka Reuel, Erik Brynjolfsson, John Etchemendy, Katrina Ligett, Terah Lyons, James Manyika, Juan Carlos Niebles, Yoav Shoham, Russell Wald, and Jack Clark, "The AI Index 2024 Annual Report," AI Index Steering Committee, Institute for Human-Centered AI, Stanford University, Stanford, CA, April 2024, https://aiindex.stanford.edu/report/.

[7]Dohmen, Hannah, "Assessing China's AI development and forecasting its future tech priorities," The Atlantic Council, Strategic Insights Memo, September 18, 2024, https://www.atlanticcouncil.org/content-series/strategic-insights-memos/assessing-chinas-ai-development-and-forecasting-its-future-tech-priorities/.

[8]Shaun Narine, "Why the American technological war against China could backfire," The Conversation, December 17, 2023, https://theconversation.com/why-the-american-technological-war-against-china-could-backfire-219158.

In parallel to this activity, proposed AI-related regulations are also on the rise worldwide. Research from Stanford found that in the U.S., more than twice as many AI-related bills were proposed in 2023 at the federal level compared to the previous year.[9]



Source: The AI Index Report 2024

While both companies and governments recognize a need for thoughtful solutions to manage AI risks, there is still widespread disagreement on how this should be done. Part of it is due to the technology itself, which is evolving expeditiously and is not always readily understandable to the public or policymakers. Part of it is due to institutional legacy. Although each new technology presents its own set of challenges, AI has sounded the alarm bells more than any other technological development in recent memory. The responses have ranged from calls for a pause in development, recommendations to control the technology through strict regulation, or a wait-and-see approach rooted in fears that premature or overregulation could stifle innovation.

[9]Nestor Maslej, Loredana Fattorini, Raymond Perrault, Vanessa Parli, Anka Reuel, Erik Brynjolfsson, John Etchemendy, Katrina Ligett, Terah Lyons, James Manyika, Juan Carlos Niebles, Yoav Shoham, Russell Wald, and Jack Clark, "The AI Index 2024 Annual Report," AI Index Steering Committee, Institute for Human-Centered AI, Stanford University, Stanford, CA, April 2024, https://aiindex.stanford.edu/report/.

As we consider rules for this era of AI innovation, we can draw valuable lessons from the transformative period of Internet policymaking from the 1990s. We believe this U.S. approach is well-suited to today's challenges, recognizing that AI will evolve rapidly and play an increasingly central role in people's lives. Sensible policies with appropriate safeguards can ensure AI is integrated safely into the economy while maintaining a climate that encourages continuous innovation and investment. We seek the development of a robust and successful AI policy framework that will combine solutions from policymakers, civil society, and marketplace participants. We are confident that this is the path that will enable the U.S. to maintain its technological and economic edge.

We also believe that this is how we can bolster U.S. competitiveness, promote entrepreneurial market entry, ensure U.S. security, and help to prepare the next generation for the coming opportunities and global challenges. Vitally, it will also enable the development and proliferation of safe AI that reflects the values of our society: respectful of civil liberties, inclusive, and innovative. We now have a window of opportunity that we cannot miss.

General Framework

Although specific topics each have their own set of unique policy needs, we believe the most practical approach is to underscore key solutions that could guide an overall regulatory framework. These include the following:

Coordination Across Government

One of the key determinants of a successful U.S. AI policy framework is coordination. The passage of a single law, such as the EU AI Act, is both unlikely and unnecessary in the U.S. Existing statutes can be leveraged and used in conjunction with new laws that can fill in legislative gaps. While we respect states moving to take action on AI, we believe that for purposes of U.S. competitiveness and national security, federal-level legislation is ideal.

Furthermore, the U.S. would benefit from a "whole of government" approach, with much greater coordination across agencies, to ensure consistency and clarity for the private sector and the public. A December 2023 Government Accountability (GAO) report found that even among agencies implementing AI usage, their own internal requirements were incomplete.[10] While a sector-based approach can refine policies within areas of particular subject matter expertise, there should also be mechanisms in place to assess common, cross-sectoral risks and advance AI policy and innovation opportunities across government.

Collaboration and Input From Diverse Groups

The federal government should work closely with the private sector and civil society, not only to solicit input on potential AI policies, but also to work together to develop mechanisms to mitigate AI risks and harness its immense potential. Ensuring that experts with deep and relevant experience are at the table will enable the inclusion of different viewpoints to inform policymaking, and to build trust across the AI ecosystem.

Furthermore, the U.S. government will have to work closely with its allies to ensure the development and deployment of AI tools that are based on shared values and priorities.

[10] "Artificial Intelligence: Agencies Have Begun Implementation but Need to Complete Key Requirements," United States Government Accountability Office, Report to Congressional Addressees, Dec 12, 2023, https://www.gao.gov/assets/gao-24-105980.pdf.

While regulatory approaches may be different, alignment on key ethics and values is vital. Recent multinational initiatives, including the State Department's Global Partnership on AI (GPAI) and ongoing collaboration through the U.S.-EU Trade and Technology Council (TTC), demonstrate potential next steps.

From Energy Crunch to Potential Boom

Electricity demand is increasing because of the rising use of cloud services and AI, the onshoring of manufacturing, and electrification. Recent tech company sustainability reports are showing rising greenhouse gas emissions due to data center energy consumption. At the same time, AI provides the opportunity to improve energy system planning and increase the efficiency of existing generation and operations. Perhaps most vitally, it is also a moment in history whereby policymakers can modernize energy policy to ensure that carbon-free generation, energy storage, and transmission are able to be quickly deployed to ensure the reliability and resiliency of the grid. America has the opportunity to take advantage of two major technology revolutions occurring simultaneously.

"All of the Above AI"

We believe in a competitive landscape where — according to user needs — both open source and closed AI models should advance to meet marketplace demands.

The transparency of open source AI is a valuable attribute from both a security perspective and an economic perspective. Open source allows third-party access and can be audited more easily. There is less risk of biases as both inputs will be more diverse, and existing biases can be more easily pinpointed and rectified. Open source can also facilitate more innovation and promote entrepreneurial market entry and more open competition. Open source offerings may also use less data and energy and offer more niche, tailored services.

Closed models will also undoubtedly have a prominent place in the ecosystem. The major investments and financial bets that the largest tech companies are placing on proprietary model AI approaches is evidence of the marketplace building to scale based upon anticipated demand. Such models will have attributes that are different from open source offerings but may meet important customer needs.

Optimizing Our Country's Resources

We are on the edge of a new world, and we need to invest in capacity to be prepared for the challenges and opportunities that it will bring. If the U.S. invests now, it can continue to remain ahead in the long term. The U.S. will need to keep its scientific lead through top-notch AI research. Meanwhile, investments in infrastructure will be critical to both helping to develop AI further and ensuring its smooth operation at scale. One of the greatest resource challenges will be the education, recruitment, and retention of talent.

We are also cognizant of the colossal cost that many of these investments will entail. As such, policymakers will have to make hard decisions, and there will inevitably be trade-offs.

This general framework embodies the principles that we believe policymakers should be guided by. We have further focused on some of the key issues that policymakers will have to address in the coming months and years in the forthcoming sections.

AI Pillars

Economic Leadership & Innovation

Competition

Competition drives innovation, investment, and consumer choice. America's policy framework for AI should embrace and promote open and competitive markets across the AI value chain — from LLMs to applications.

Findings

- **Competition as a core advantage:** An open, competitive marketplace encourages entrepreneurial entry, fosters innovation, investment, and rapid technological advancement. Robust competition among all marketplace participants - both large and small - brings fresh ideas, agility, and the ability to challenge established practices, which drives progress across any industry. This competitive environment nurtures creativity, stimulates growth, and ensures that the future of AI in the United States remains dynamic and accessible to all innovators.
- **A synergistic system:** America's competitive edge in AI stems from its world-class talent pool, investments in R&D and infrastructure, and a vibrant startup ecosystem backed by strong venture capital networks. The U.S. benefits from significant AI research and development, with diverse AI applications across industries like healthcare, finance, and defense, further strengthening its position. This combination of technical expertise, entrepreneurial culture, and financial support ensures the U.S. remains a global leader in AI innovation and in international markets. Recent research from Accenture and Microsoft found that the potential uplift to labor productivity from generative AI could contribute $3.8 trillion to the U.S. economy by 2038.[11]

[11]"Unlocking the Economic Potential of the US Generative AI Ecosystem," Accenture and Microsoft, November 2024,

Policy Recommendations

- Support AI entrepreneurs: Entrepreneurs and startups have been the backbone of American innovation. That should not change now. Supporting AI startup ecosystems to flourish by funding accelerators, encouraging university partnerships, and making venture capital more accessible.
- Include smaller players in discussions: Although we are heartened by the U.S. government's convenings with AI companies, we should also encourage smaller AI companies to be present at the table.
- Policy on an as-needed basis: The UK and the EU have both recently passed digital markets legislation. Promoting competition in the AI ecosystem is an important goal that is advanced by existing legislation and the courts, and we encourage Congress to weigh the benefits of select policy interventions against the costs of enacting broad, systemic legislation similar to the UK and EU approaches.

American Innovation, Regional Development, and SMBs

AI offers an unprecedented opportunity for economic development across the United States. At its core lies the need to continue to innovate. Yet innovation must be sustainable.

Furthermore, policymakers at this juncture have the opportunity to guide innovation policies so that groups beyond the usual suspects have an opportunity to be included in this massive economic and social transformation. Uneven adoption will eventually lead to uneven growth and inequality. Targeted policies to develop regional hubs can expand employment opportunities and innovation. This will require comprehensive national strategies that can be smoothly implemented on the local level. Regional development can also help with workforce displacement.

Likewise, SMBs must not be disproportionately left behind; on the contrary, policies should help them take advantage of the shift to AI. A recent study found that, for the moment, large companies have the highest AI use, with over 60% of companies with more

---

https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/MSFT-US-Generative-AI-Ecosystem-WHITE-PAPER-FINAL-Nov-20-2024.pdf.

than 10,000 employees actively using it in their day-to-day operations.[12]

Findings

- **Shifting geopolitics:** U.S. innovation has always been cutting-edge and robust. But in recent years, the changing geopolitical landscape has meant the world has moved from globalization to a more localized approach, particularly with regard to strategic industries and key raw materials.
- **Existing policy levers:** Government must play a role in further promoting American industry and innovation. The CHIPS Act, Science Act, and export controls have been effective in their short-term goals. However, there will be insufficient policy levers to maintain U.S. advantage in an increasingly competitive and multipolar world. Some experts even believe that export controls have bolstered Chinese industrial policy and motivated Chinese firms to move faster. For example, Huawei and SMIC developed a semiconductor "with capabilities that U.S. export controls were intended to prohibit."[13]
- **Regional concentration:** AI affords an opportunity to guide regional economic development. However, AI adoption is concentrated among startups in "superstar" cities. Researchers predict that if this trend continues, there will be an "AI divide" whereby some geographies will continue to attract more of the high-growth startups that are already operating there.[14] Furthermore, new AI jobs also appear to be concentrated in the same locales.[15] Rather than technological and economic diffusion, this would seem to indicate even greater centralization and, eventually, greater inequality.

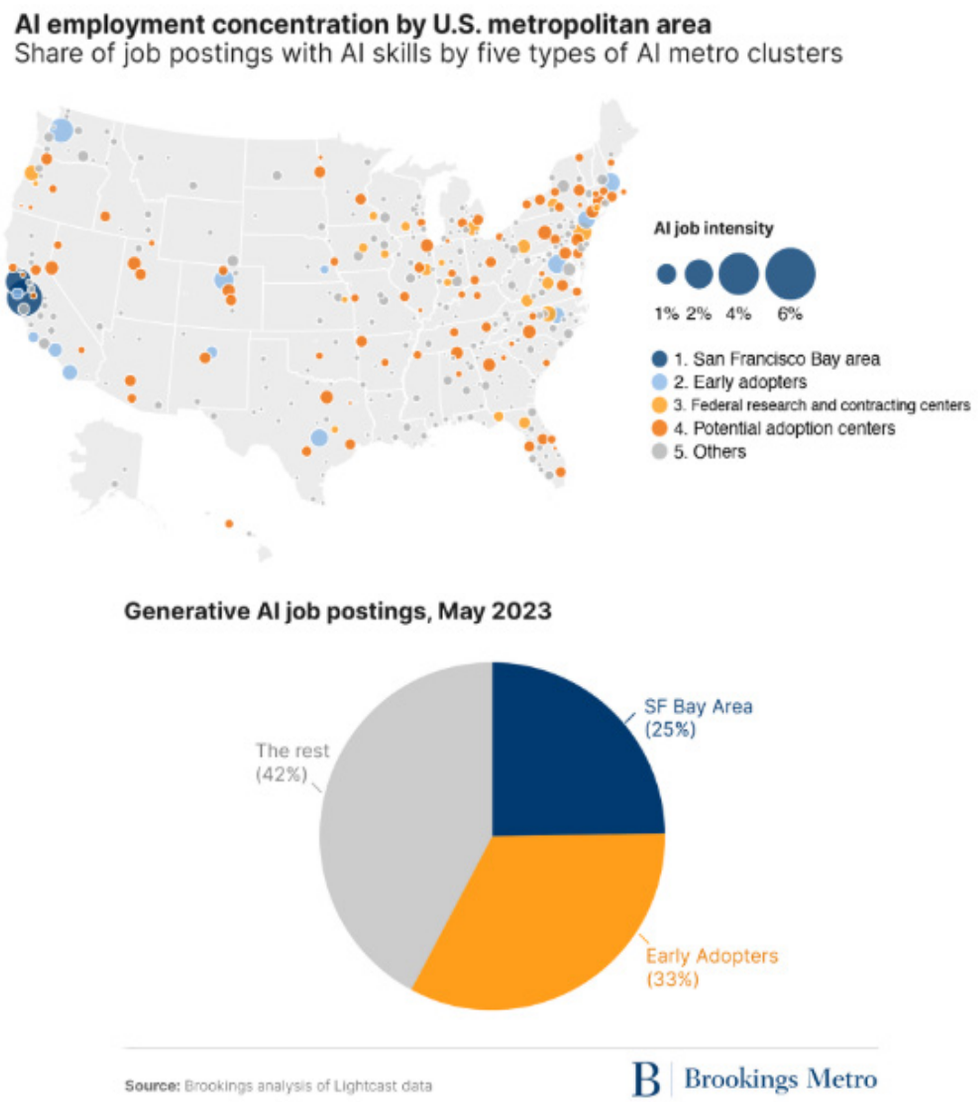
---

[12]Brian Eastwood, "The who, what, and where of AI adoption in America," MIT Sloan, Feb 7, 2024, https://mitsloan.mit.edu/ideas-made-to-matter/who-what-and-where-ai-adoption-america.

[13]Kirti Gupta, Chris Borges, and Andrea Leonard Palazzi, "Collateral Damage: The Domestic Impact of U.S. Semiconductor Export Controls" CSIS, July 9, 2024, https://www.csis.org/analysis/collateral-damage-domestic-impact-us-semiconductor-export-controls.

[14]Kristina McElheran, J. Frank Li, Erik Brynjolfsson, Zachary Kroff, Emin Dinlersoz, Lucia Foster, Nikolas Zolas, "AI adoption in America: Who, what, and where," The Journal of Economics & Management Strategy (JEMS), Volume 33, Issue 2, Special Issue on Artificial Intelligence and the Business Revolution, Summer 2024, Pages 375-415, https://doi.org/10.1111/jems.12576.

[15]Mark Muro, Julian Jacobs, and Sifan Liu, "Building AI cities: How to spread the benefits of an emerging technology across more of America," The Brookings Institution, July 20, 2023, https://www.brookings.edu/articles/building-ai-cities-how-to-spread-the-benefits-of-an-emerging-technology-across-more-of-america/.



Source: The Brookings Institution

- **Considering smaller players:** Small and Medium-Sized Businesses (SMBs) are the backbone of the economy and yet have few resources to adopt and integrate AI into their business practices. Research found that smaller businesses (with 5-100 employees) prefer financial assistance, while businesses with more than 100 employees prefer technical assistance.

Additionally, two-thirds of small business owners and executives were interested in Small Business Administration (SBA) loans to help with AI adoption.[16]

Policy Recommendations

- **More R&D:** Expedite and expand upon R&D initiatives set forth in CHIPS. In recent months, the CHIPS program has made numerous awards. These have generally been concentrated among larger firms. We would encourage diversifying the awards to companies of all sizes that possess the necessary technical capabilities as a means of supporting smaller, innovative firms in this space. In addition, the Defense Advanced Research Projects Agency (DARPA) will launch a domestic hub for prototyping advanced semiconductor fabrication techniques. There is room for even more investment to strengthen the U.S. semiconductor industry.[17] Furthermore, Congress should continue to support programs that prioritize U.S. semiconductor security and innovation.
- **Coordinated technology development strategy:** The U.S. government should facilitate increased investment and innovation in AI and other emerging and complementary technologies, such as robotics or quantum computing. The White House National Security Memo on AI recognizes this need, stating that relevant agencies should "use existing authorities to make public investments and encourage private investments in strategic domestic and foreign AI technologies and adjacent fields." and will also be given "new authorities."[18]

---

[16]Michelle Kumar and Justis Antonioli, "Small Businesses Matter: Navigating the AI Frontier," Bipartisan Policy Center, April 29, 2024, https://bipartisanpolicy.org/report/small-businesses-matter-navigating-the-ai-frontier.

[17]Sujai Shivakumar, Charles Wessner, and Thomas Howell, "A World of Chips Acts: The Future of U.S.- EU Semiconductor Collaboration," CSIS, August 20, 2024, https://www.csis.org/analysis/world-chips-acts-future-us-eu-semiconductor-collaboration.

[18]"Memorandum on Advancing the United States' Leadership in Artificial Intelligence; Harnessing Artificial Intelligence to Fulfill National Security Objectives; and Fostering the Safety, Security, and Trustworthiness of Artificial Intelligence"The White House, October 24, 2024, https://www.whitehouse.gov/briefing-room/presidential-actions/2024/10/24/memorandum-on-advancing-the-united-states-leadership-in-artificial-intelligence-harnessing-artificial-intelligence-to-fulfill-national-security-objectives-and-fostering-the-

- **Government-led signaling:** The U.S. government can use its purchasing power to guide the direction of AI development and to help drive adoption within the public sector, particularly to drive more efficiency. It can do so by better communicating its own needs and requirements to the market, reforming procurement practices, and making its own massive data assets available to the market in affordable ways. Directly signaling its needs can not only result in better-suited technology but can also promote and accelerate the advancement of specific clusters and subsectors as needed.

- **AI procurement reform:** Larger players are moving quickly into the government AI procurement market.[19] One risk is that startups and smaller firms — which are often the drivers of new technology– will face increasing difficulty competing with large vendors in government procurement contracts. This will stifle their ability to grow, invest further in their companies, and innovate. Congress should work with the relevant departments and the Office of Management and Budget (OMB) to create a program that allocates part of the procurement budget to purchases from qualified startups. Furthermore, the OMB can conduct outreach to help departments and agencies understand that the place of AI tools is separate and distinct from other software and that startups and midsize vendors are capable and well-positioned to provide these products. Given that the Department of Defense (DoD) is one of the largest buyers of these services, special attention should be paid to its role and its procurement practices. The White House National Security Memorandum (NSM) on AI calls for revised procurement processes for national security is a good step in this direction. We especially applaud the call to simplify "processes such that companies without experienced contracting teams" can compete meaningfully.

- **Public Dataset Availability:** The federal government can help the development of AI models by making its vast data resources available to developers and researchers. This information would include a variety of sources that contain valuable

---

Jacob Larson, James S. Denford, Gregory S. Dawson, and Kevin C. Desouza, "The evolution of artificial intelligence (AI) spending by the U.S. government," The Brookings Institution, March 26, 2024, https://www.brookings.edu/articles/the-evolution-of-artificial-intelligence-ai-spending-by-the-u-s-government/.

demographic, economic, and cultural data, enabling models to contain factually correct information covering a significant period of time. The Department of Commerce (DoC) has already established an "AI and Open Government Data Assets Working Group" aimed at developing guidelines to make DoC data available.[20] We encourage other agencies to similarly create working groups and guidelines to make their data available for AI training in affordable and easily accessible ways.

- **University support:** University research is a critical leg to continued U.S. innovation. University researchers, not constrained by a company's own agenda, are more free to pursue experimental or public good research. They are, however, limited by resources. The passage of the CREATE AI Act, which supports the foundation of The National Artificial Intelligence Research Resource (NAIRR), would be a positive development.
- **Expanding public sector expertise:** Protecting U.S. innovation will require that government officials and staff have specialized skills and knowledge, adequate experience, and sufficient expertise in making decisions related to AI and other emerging technologies. In addition to providing expert AI training to existing staff, the U.S. government should proactively recruit leading experts from academia and the private sector. Programs like the AI Talent Surge and U.S. Digital Corps should be expanded to meet this acute need.
- **Federal direction for regional initiatives:** Congress should work with local stakeholders to ascertain what additional geographic locations could benefit from what is needed to become a future hub. The government is starting to make some initial investments. The DoC announced $504 million for 12 Tech Hubs to give regions across the nation the resources and opportunities needed to lead in areas such as semiconductors, clean energy, biotechnology, AI, and quantum computing.[21]

---

[20]Oliver Wise, Sallie Ann Keller, and Victoria Houed, "Preparing Open Data for the Age of AI," Department of Commerce, January 18, 2024, https://www.commerce.gov/news/blog/2024/01/preparing-open-data-age-ai.

[21]Madeleine Ngo and Ana Swanson, "U.S. Awards $504 Million for 'Tech Hubs' in Overlooked Regions," NYTimes, July 2, 2024, https://www.nytimes.com/2024/07/02/us/politics/504-million-tech-hubs-overlooked-regions.html.

Congress could scale up place-based investments in emerging AI communities. The National Science Foundation (NSF) Regional Innovation Engines program and the DoC's Regional Technology and Innovation Hubs programs could be supported through more funding.[22]

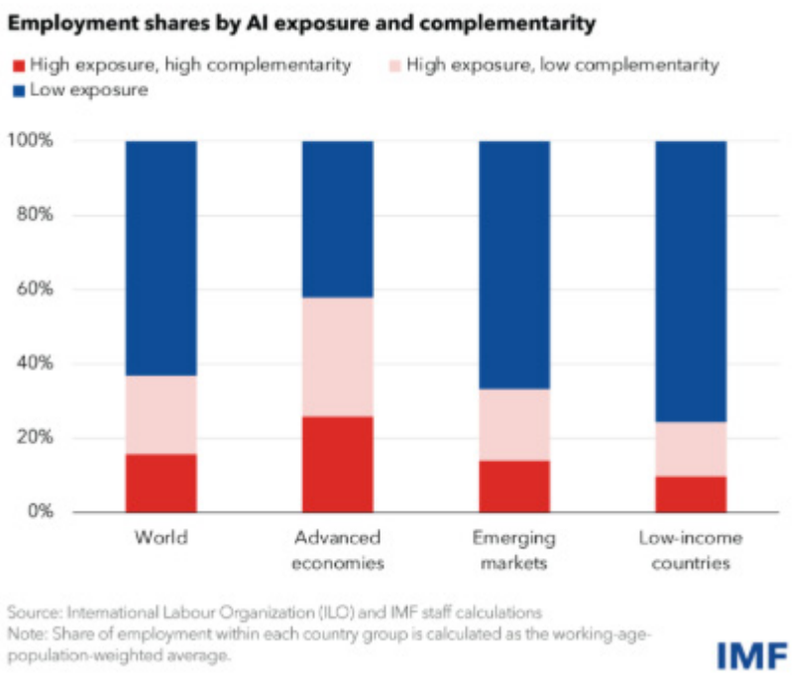
- **Small business support:** Small businesses will need extra support (either through access to know-how or funding) in order to take advantage of the many opportunities that AI can afford them.

Workforce Impact and "AI Education for All"

With the efficiencies that AI brings, our greatest hope as human beings is that AI will take care of mundane or repetitive tasks so that we can fully realize our creative and intellectual potential. It may even allow for the reconfiguration of work in such a way that society and individuals have ample time and opportunities to pursue other interests.

While AI promises astounding developments in innovation and productivity, it will unquestionably result in significant job displacement as well. It will create new sources of employment, while simultaneously eliminating some jobs —even among those that have historically been thought of as secure. As such, the challenge will be in benefiting from AI efficiencies while ensuring that policies promoting upskilling and the evolution of new job categories can help those that are displaced.

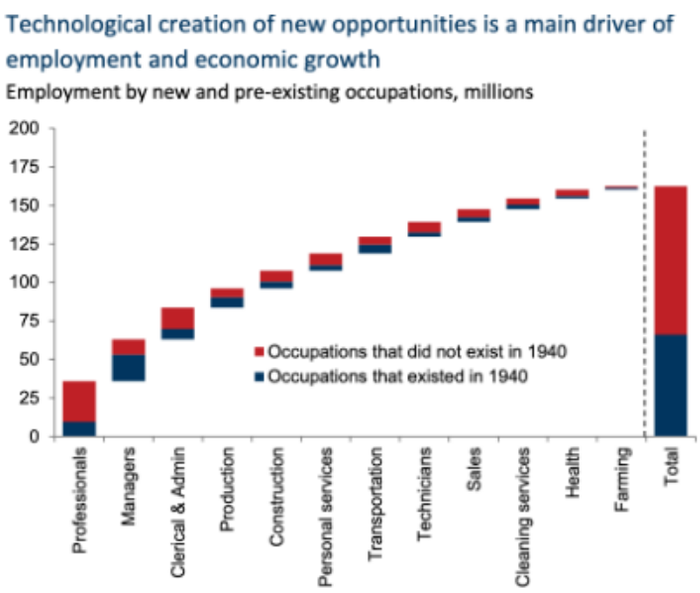
Mark Muro, Julian Jacobs, and Sifan Liu, "Building AI cities: How to spread the benefits of an emerging technology across more of America," The Brookings Institution, July 20, 2023, https://www.brookings.edu/



Source: IMF

Findings

- **Chance to bolster the middle class:** AI can help give rise to a new middle class with the right policies in place. The advent of computational power resulted in a hollowing out of the middle class due to the disappearance of many middle-skill jobs. AI, too, will also likely eliminate many job categories and displace many workers. Upskilling and retraining workers and revamping the education system to prepare for a new generation of workers will be critical to allowing the U.S. to remain competitive and prosperous.



Source: Autor et al. (2022), Goldman Sachs GIR.

A dearth of workers: Meanwhile, there is a projected deficit of workers and aging populations in many democracies. For example, in the semiconductor industry, the U.S. faces a frightening shortage of 67,000 technicians, computer scientists, and engineers by 2030. The U.S. will also face a gap of 1.4 million skilled workers throughout the broader U.S. economy.[23]

Productivity to improve: We have not yet realized the potential of productivity gains that AI can offer. So far, productivity gains from digital automation technologies and early AI have, to date, been limited. Researchers evaluated the use of generative AI tools used by customer service agents and found a roughly 14% improvement in productivity, most significantly among novice workers.[24]

---

[23]John Neuffer, "Two Years After CHIPS Enactment, Here's How to Sustain America's Budding Semiconductor Resurgence," Semiconductor Industry Association, Aug 08, 2024, https://www.semiconductors.org/two-years-after-chips-enactment-heres-how-to-sustain-americas-budding-semiconductor-resurgence/.

[24]David Autor, "AI Could Actually Help Rebuild The Middle Class," Noema Magazine, February 12, 2024, https://www.noemamag.com/how-ai-could-help-rebuild-the-middle-class/.

However, the acceleration is expected to be exponential, so resting on laurels is a strategic error governments should avoid — at all costs.

Policy Recommendations

More workforce impact research: Congress should work with relevant government departments and other stakeholders to study workforce impact across different industries, functions, and geographies — and over time. These parties should also work together to determine which new jobs will likely be created by AI and other emerging technologies. These analyses can then help determine specific education and upskilling policies based on skills needs.

Incentives for worker training: The growing use of AI, even if only for complementing workers, and the further reinvention of organizations around this new general-purpose technology imply a great need for worker training or retraining. Federal or local governments could provide this training or provide incentives for corporate training.[25]

Revamped curriculum: Critical thinking, problem-solving, and teamwork should be integrated as a key component of the K-12 curriculum. Computer science and AI literacy and education should also be included in the K-12 curriculum across the U.S., "AI Education for All," not unlike the "Internet for All" program in its goal of improving digital equity. Congress and the Department of Education can work together with state authorities to build programs that make additional STEM and technology learning opportunities available at the K-12 level. Furthermore, policymakers can work with industry and universities to identify and coordinate collaboration opportunities across the K-20 timeline.

Targeted immigration reform: Since 2000, half of all U.S. start-ups valued at $1 billion or more have been founded or co-founded by immigrants.[26]

---

[25]Erik Brynjolfsson, "The Turing Trap: The Promise & Peril of Human-Like Artificial Intelligence," Daedalus Journal of the American Academy of Arts & Science, Spring 2022, https://www.amacad.org/sites/default/files/publication/downloads/Daedalus_Sp22_19_Brynjolfsson.pdf.

[26]Graham Allison and Eric Schmidt, "The U.S. Needs a Million Talents Program to Retain Technology Leadership," Foreign Policy, July 16, 2022, https://foreignpolicy.com/2022/07/16/immigration-us-technology-companies-work-visas-china-talent-competition-universities/.

Specific immigration reforms can help the U.S. continue to attract and retain top talent in the country. The White House National Security Memo on AI, recognizing the critical importance of talent, sets forth strong and concrete steps by which the U.S. government should work to determine the available AI (and related sectors') talent pool in the U.S. and abroad and to create mechanisms to attract and vet those individuals to work in the U.S. Congress should also make it easier for graduates with relevant STEM and AI skills and qualifications to remain in the U.S. by streamlining processes to obtain green cards. Furthermore, Congress could raise the current cap on employment-based STEM visas. Immigration reform could also create a track to attract individuals with specialized AI or STEM skills as well as AI and STEM entrepreneurs.[27]

[27]Joel Burke, "National Security AI Entrepreneur Visa: Creating a New Pathway for Elite Dual-Use Technology Founders to Build in America," Federation of American Scientists, June 27, 2024, https://fas.org/publication/ai-entrepreneur-visa-legislative-sprint/.

Infrastructure Modernization

Broadband Infrastructure and Delivery of Communications Services

Broadband infrastructure is critical for AI development as it ensures high-speed Internet access that AI technologies require to function effectively. Current public policy development aims to expand broadband coverage, especially in underserved areas, and this – along with access to competitive compute resources and an enhanced electricity infrastructure – will help to enable widespread use of AI applications. Investments in broadband can also spur innovation in AI by providing the necessary network reliability for advanced research and development. Furthermore, AI can improve the delivery and security of communications services, including, for example, addressing unwanted illegal robocalls and robotexts. Promoting open Internet rules that allow consumers to access lawful online content and services without interference will ensure consumers can access AI applications.

Findings

- **Security issues:** One of the key risks for the broadband industry is related to the risk of sabotage by bad faith actors due to the connected nature of networks. Given the difficulty of controlling all access points the sector faces unquantifiable risks. AI has the potential to improve security but also create new security threats.
- **Network optimization:** AI is already delivering efficiencies to broadband providers by helping to optimize network traffic management with regard to timing, geography and other factors. In addition to providing a better customer experience, this could also lead to lower downtimes and lower costs, among other benefits.
- **Workforce efficiency:** Broadband providers are already seeing workforce efficiencies thanks to AI. While it is early days, call center productivity appears to be rising. This will allow employees to focus on higher cognitive tasks. Similar efficiencies have been observed with regard to technical staff. Technology is also helping to monitor potential problems in real-time and allowing for preemptive troubleshooting.

Limitations on physical access: Providers who are deploying their own broadband network to compete against broadband monopolies continue to face significant barriers when deploying their fiber and wireless networks. For example, railroads charge excessive rates for access to their rights-of-way, there are significant permitting delays in gaining access to the public rights-of-way, and there are continued restrictive access of multiple tenant environments (MTEs), largely due to commercial arrangements between service providers and building owners that inhibit competition.[28] These barriers to deployment slow down the process, increase costs, and often prevent providers from reaching underserved and unserved communities. We believe that market-based options, infrastructure sharing, and open access are emerging trends that should be encouraged.

Policy Recommendations

- **Net neutrality:** The principles of net neutrality, which ensured an even playing ground and equal access for all Internet traffic, enabled the democratic and competitive development of the Internet. These same principles are as relevant and critical to ensure that AI develops and is used fairly and equitably.
- **Improving physical access:** To support broadband network availability, policymakers should break down existing barriers to fast and affordable deployment. They should speed broadband providers' access to public rights-of-way ("ROW") by accelerating permit approval by implementing applicable shot clocks and charging reasonable fees.

---

[28]Angie Kronenberg, "Poles and Railroads: Breaking Down Barriers to Broadband Deployment," Medium, March 1, 2023, https://medium.com/@akronenberg/poles-and-railroads-breakingdownbarriers-tobroadband-deployment-d5eafda2c1ac.; Thomas Jones, "Re: Accelerating Wireless Broadband Deployment by Removing Barriers to Infrastructure Investment, WT Docket No. 17-79; Accelerating Wireline Broadband Deployment by Removing Barriers to Infrastructure Investment, WC Docket No. 17-84," Notice of Ex Parte, Wilkie Farr and Gallagher LLP, October 31, 2019, https://www.fcc.gov/ecfs/document/1031214319574/1.;
Angie Kronenberg, Christopher L. Shipley and Lindsay Stern,"In the Matter of Office of Economics and Analytics Seeks Comment on the State of Competition in the Communications Marketplace, Comments of INCOMPAS," FCC, June 6, 2024, https://www.fcc.gov/ecfs/document/106061459503586/1.

Policymakers should also ask state and local governments, utilities, and railroads to publicly disclose their fees and ensure that they are competitively and technologically neutral, non-discriminatory, and based on their actual, objectively reasonable costs for access to ROW, poles, and conduit. The Federal Communications Commission (FCC) and states should modernize their pole access rules to set timeframes for large deployments. Lastly, policymakers should examine unreasonable door fees and inside wiring disputes prevalent in commercial multi-tenant environments ("MTEs") while reaffirming the benefits of neutral host operations for MTE rooftops.

- **Collaboration with government and law enforcement:** Given the interconnected nature of the networks, improved and centralized cyber threat intelligence -sharing mechanisms between relevant government agencies and companies is key and the government must be an active participant in providing its own information to inform industry. To be effective, there must be a two-way flow of information.
- **AI-Powered Infrastructure Mapping and Deployment:** Use AI to create detailed, real-time maps of existing broadband infrastructure and identify areas with gaps in deployment. This can assist policymakers in targeting investments and incentivizing public-private partnerships for deploying broadband where it's needed most. This would streamline the planning and construction of broadband infrastructure, reducing costs and enabling more accurate, competitive investments in underserved regions. AI can also assist in predictive maintenance and optimizing network performance for new deployments. AI tools for infrastructure mapping could be utilized to deploy fiber networks more efficiently by analyzing geographic and demographic data.
- **AI to Reduce Regulatory Barriers for Small ISPs:** Use AI to simplify regulatory compliance and reduce the burden on smaller Internet service providers (ISPs) entering the broadband market. AI could automate reporting processes, predict potential regulatory violations, and ensure that smaller providers meet compliance standards without excessive administrative costs.

By lowering regulatory and compliance costs, AI can encourage more competition by enabling smaller ISPs to compete effectively with larger, established providers. This could accelerate broadband deployment in areas currently underserved by large providers. Automation tools in regulatory compliance can be explored to streamline processes for small businesses and startups in various industries.

Spectrum Policy

Spectrum is an invaluable resource in our nation's communications infrastructure. Maximizing the availability of spectrum and managing its allocation, licensing, and use effectively and efficiently can benefit the AI ecosystem. Moreover, AI applications may assist in the policy management of spectrum resources and the management and deployment of wireless networks alike.

Findings

- **Spectrum Management and Allocation:** AI can optimize the allocation and management of radio frequency spectrum, ensuring more efficient use of available bandwidth. By analyzing large datasets, AI can predict demand and dynamically allocate spectrum resources in real time, reducing interference and improving overall spectrum efficiency.
- **Interference Detection and Mitigation:** AI can help in identifying and mitigating harmful interference in spectrum use. Machine learning algorithms can detect patterns and anomalies in spectrum usage, allowing for quicker and more accurate identification of interference sources, which can then be addressed to maintain signal integrity.
- **Regulatory Compliance and Policy Enforcement:** AI can assist in monitoring spectrum usage to ensure compliance with regulatory policies. Automated systems can continuously analyze spectrum use, detect violations, and enforce policies, helping regulators maintain control over spectrum resources and ensuring that users adhere to established rules.

Policy Recommendations

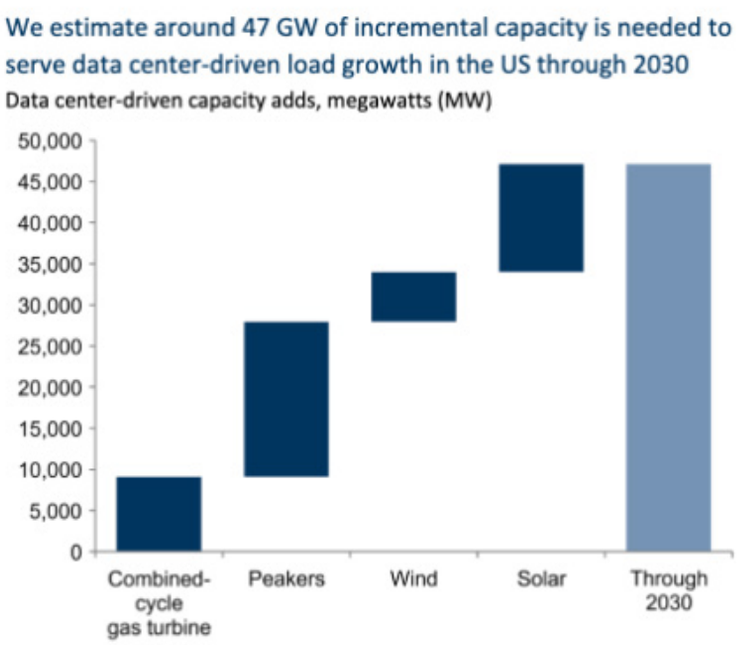
AI-Driven Spectrum Management and Allocation: Implement AI technologies to optimize spectrum management and allocation. By using AI to dynamically assess and manage spectrum usage, regulators can allocate broadband spectrum more efficiently, especially in rural or underserved areas. AI can identify underutilized spectrum in real-time, allowing for more flexible and competitive access. This would increase competition among ISPs, reduce entry barriers for smaller ISPs, and improve overall spectrum utilization for broadband services, particularly in high-demand areas. Countries like the United States and the UK are exploring AI for dynamic spectrum sharing to maximize the use of wireless infrastructure, which is key to broadband expansion.

AI-Enabled Dynamic Spectrum Sharing: Leverage AI for dynamic spectrum sharing, where multiple wireless operators or services can share the same spectrum bands based on real-time demand. AI can manage spectrum usage by continuously monitoring traffic patterns and adjusting allocations to avoid interference and maximize efficiency. This would allow for more efficient use of spectrum, especially in crowded urban areas or during peak usage times. It also opens up opportunities for smaller providers to access spectrum more flexibly, fostering wireless competition. The approach can reduce the need for static, exclusive spectrum licenses, enabling more dynamic and competitive wireless broadband deployments. Note that the FCC has experimented with dynamic spectrum sharing in the Citizens Broadband Radio Service (CBRS) band, where AI is used to manage spectrum access among different users.

AI to Automate and Optimize Licensing Processes: Implement AI tools to streamline and optimize the spectrum licensing process, making it more efficient and transparent. AI could analyze applications, predict spectrum needs based on usage trends, and recommend optimized license terms that consider current and future demand. By reducing bureaucratic delays and administrative overhead, AI-driven licensing could speed up the deployment of wireless broadband infrastructure, particularly for smaller providers that may struggle with lengthy regulatory processes. Automating parts of the licensing process can also help regulators allocate spectrum more fairly and efficiently, fostering greater competition in the wireless market. AI tools are already being explored in various regulatory settings to simplify complex application processes, and similar approaches could be applied to spectrum licensing.

Energy Infrastructure

The rise of AI will require a significant boost in energy resources. The IEA estimates that globally, electricity consumption from data centers, AI development, and the cryptocurrency sector could double by 2026.[29] U.S. electricity demand is expected to rise at a 2.4% compound annual growth rate between 2022 and 2030, with data centers accounting for about 90% of that growth.[30]



Source: Goldman Sachs GIR.

[29]"Electricity 2024: Analysis and forecast to 2026," IEA, https://www.iea.org/reports/electricity-2024, License: CC BY 4.0.

[30]Goldman Sachs, "Gen AI: Too Much Spend, Too Little Benefit," Global Macro Research, Issue 129, June 25, 2024, https://www.goldmansachs.com/images/migrated/insights/pages/gs-research/gen-ai--too-much-spend,-too-little-benefit-/TOM_AI%202.0_ForRedaction.pdf.

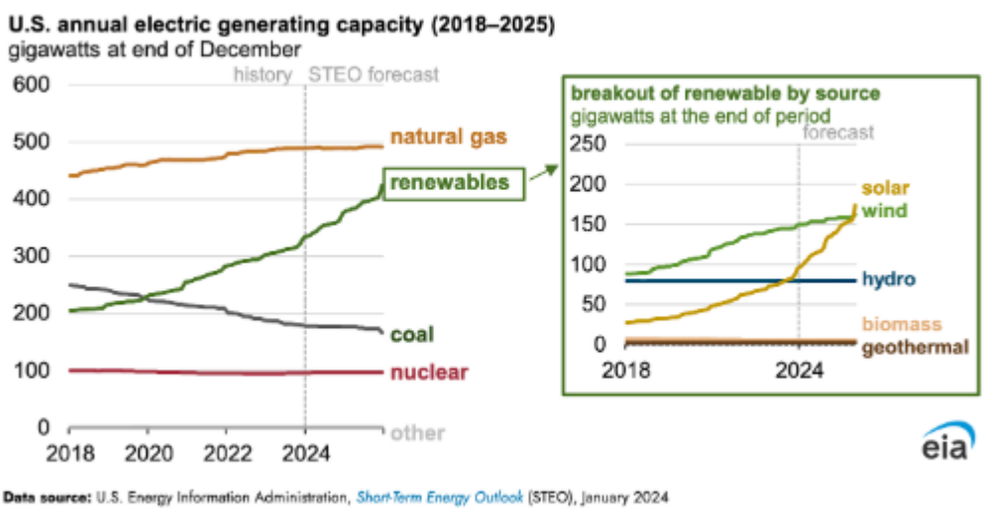
Furthermore, while companies are finding that AI is challenging their energy goals, they are also finding new ways to source energy that is compatible with their emissions goals. Thus, the challenge of AI and energy will not only be to source sufficient amounts but also to do so in a way that is compatible with emissions goals and ensuring environmental resilience.

Findings

- **Access to reliable energy is a barrier to AI growth:** Energy availability is one challenge to scaling AI. A reliable energy grid is important for local communities and economic development. In addition, ensuring electricity remains affordable is important for ratepayers.
- **Geopolitical challenge:** China has strong natural resources and energy production, controlling 60% of worldwide critical mineral extraction, 80% of the world's solar manufacturing capacity, and 60% of global wind power manufacturing.[31] To compete with this, the U.S. will have to think creatively, plan assertively, and transition quickly. It may be that the competition for AI dominance ends up expediting the clean energy transition.
- **Lead times and costs:** The timeline to build out energy infrastructure does not align with the pace needed to keep the U.S. lead in AI. Permitting and construction for this infrastructure can run 40-70 months and the interconnection queue growing nearly 30% last year will continue to cause delays. Some companies are investing in behind the meter solutions, but face the same regulatory challenges.

[31]Ben Bain, David Lin, PJ Maykish, Liza Tobin, Abigail Kukura, Jafer Ahmad, Nyah Stewart, Pieter Garicano, Brady Helwig, Linda Bachg, Olivia Armstrong, and Nayanee Gupta, " National Action Plan for U.S. Leadership in Next Generation Energy," The Special Competitive Studies Project, February 2024, https://www.scsp.ai/

Energy sources: Natural gas will continue to be the largest source of U.S. electricity generation; however, wind and solar energy are expected to lead growth in U.S. power generation for the next two years: U.S. solar power generation is expected to grow 75% from 2023 to 2025, and wind power generation will grow 11% by 2025.[32] Furthermore, nuclear energy last year supplied 48% of U.S. carbon-free electricity, and at the COP29 Summit, the U.S. announced new deployment targets set to increase triple capacity relative to 2020.[33]



[32]"Solar and wind to lead growth of U.S. power generation for the next two years," U.S. Energy Information Administration In Brief Analysis, January 16, 2024, https://www.eia.gov/todayinenergy/detail.php?id=61242#

[33]Office of Nuclear Energy, "5 Fast Facts About Nuclear Energy," U.S. Department of Energy, June 11, 2024, https://www.energy.gov/ne/articles/5-fast-facts-about-nuclear-energy; "Safely and Responsibly Expanding U.S. Nuclear Energy: Deployment Targets and a Framework for Action," The White House, November 2024, https://www.whitehouse.gov/wp-content/uploads/2024/11/US-Nuclear-Energy-Deployment-Framework.pdf.

Not just electricity: Increased water usage for data center cooling needs is also a significant issue. For example, in Virginia, water usage rose from 1.13 billion gallons to 1.85 billion, an increase of almost two-thirds between 2019 and 2023.[34]

Policy Recommendations

- **Visionary strategy:** At a high level, the federal government should convene a multidisciplinary group of technology, energy, and environmental experts to examine the dual goals of energy security and sustainability.
- **Integrate the environment:** Given the significant increase in energy usage the U.S. needs to consider environmental impact to local communities.
- **Grid modernization:** Grid modernization is important. Congress and the Administration should continue to identify ways to incentivize and accelerate the use of grid-enhancing technologies and grid expansion.
- **Minimize red tape:** Build out new sources of energy by reforming processes and making financing more accessible. Congress should work with the DoE, regional authorities, and utilities to understand and create new strategies to remove bureaucratic hurdles, fast-track permitting, and secure financing from both private and public sources. The White House National Security Memo on AI recognizes these hurdles and calls upon The Office of the White House Chief of Staff, DOE, and other relevant agencies to coordinate efforts to "streamline permitting, approvals, and incentives for the construction of AI-enabling infrastructure, "including "clean energy generation, power transmission lines, and high-capacity fiber data links."

[34]Kyle Wiggers, Demand for AI is driving data center water consumption sky high," TechCrunch, August 19, 2024, https://techcrunch.com/2024/08/19/demand-for-ai-is-driving-data-center-water-consumption-sky-high/.

- **Clean energy incentives:** The surge in AI energy needs offers an opportunity to jumpstart the U.S. transition to clean energy. Integration of renewables will also require updated grid infrastructure with better storage and management capabilities. It will also require access to the appropriate land. Inflation Reduction Act (IRA) clean energy tax incentives can continue to help support clean energy usage.
- **Continued support for nuclear:** Nuclear energy is undoubtedly a clean energy that is having a resurgence around the world. Nuclear energy will require significant investment and time to deploy, but it could be considered a longer-term, sustainable source of energy. In the medium term, repowering old plants could be one option, as well as converting coal to nuclear power. Nuclear fusion is also one technology that is garnering interest. Small Modular Reactors (SMRs) have been well-received for their safety features as well as opportunities to co-locate with data centers. The Administration should fully and quickly implement the ADVANCE Act. In addition, Congress should ensure that the nuclear incentives included in the Infrastructure Investment and Jobs Act (IIJA) and IRA are maintained.
- **Support efficient technologies:** The U.S. needs to become better at using existing energy sources by supporting the improvement of existing technologies and encouraging the development of new energy efficiency technologies. The development of energy-efficient technologies and practices, including a ramp-up in heat recycling, is critical. Providing grants and funding for new technologies, such as advanced cooling systems, energy storage, and AI solutions, is essential, too. Battery storage will be vital, particularly as renewable usage ramps up.

- **AI as a tool:** AI software can help drive energy efficiency grid management and offer other benefits. For example, the DoE has announced an AI testbed to bring together researchers, national labs, and the private sector to research energy-efficient and/or energy-flexible AI training and inference.[35] It is also already developing AI tools to improve the way such projects are sited and permitted at the federal, state, and local levels as part of its recently launched voltAIc Initiative.[36] Furthermore, the DoE notes that AI systems also have the potential to improve energy equity and has prioritized ensuring the benefits from clean energy solutions flow to disadvantaged communities.[37] More broadly, the DoE's Frontiers in Artificial Intelligence for Science, Security and Technology (FASST) program is a multi-purpose initiative leveraging the DoE's infrastructure to address issues including energy, national security, and workforce. Congress should allocate increased funding to help the DoE continue investments in AI.
- **Protecting infrastructure:** AI can be used to mitigate increased cybersecurity threats to energy infrastructure. The DoE has launched a number of efforts, including the establishment of the Energy Threat Analysis Center (ETAC), to build partnerships between the public and private sectors to mitigate cyber threats to energy infrastructure. The DoE also awarded $4.2 million to Georgia Tech to develop an AI grid security solution as part of $45 million in funding for 16 different cybersecurity solutions in the energy sector.[39] Cyberattacks will undoubtedly increase; Congress should continue funding to ensure these solutions are scaled and distributed across the U.S.

---

[35]"Recommendations on Powering Artificial Intelligence and Data Center Infrastructure," U.S. Department of Energy, Secretary of Energy Board, Presented to the Secretary of Energy on July 30, 2024,https://www.energy.gov/sites/default/files/2024-08/Powering%20AI%20and%20Data%20Center%20Infrastructure%20Recommendations%20July%202024.pdf.

[36]"How AI Can Help Clean Energy Meet Growing Electricity Demand," U.S. Department of Energy, Office of Policy, August 16, 2024, https://www.energy.gov/policy/articles/how-ai-can-help-clean-energy-meet-growing-electricity-demand

[37]Keith J. Benes,, Joshua E. Porterfield, and Charles Yang, "AI for Energy Opportunities for a Modern Grid and Clean Energy Economy," U.S. Department of Energy, April 2024, https://www.energy.gov/sites/default/files/2024-04/AI%20EO%20Report%20Section%205.2g%28i%29_043024.pdf

[38]"FASST Factsheet," U.S. Department of Energy, July 2024, https://www.energy.gov/sites/default/files/2024-07/FASST%20Handout%20%281%29_0.pdf.

[39]Zac Amos, "Protecting the Grid: Does AI Hold the Key to Cybersecurity?" EEPower, April 02, 2024, https://eepower.com/tech-insights/protecting-the-grid-does-ai-hold-the-key-to-cybersecurity/#.

National Security

Policymakers should explore policy proposals to harness AI to enhance national security, developing frameworks to prevent the misuse of AI in cyber warfare, espionage, and other threats. AI will compel the U.S. to rethink its national security strategy holistically to maintain primacy and compete with adversaries. This will require systems and processes that possess sufficient adaptability and agility, while having adequate controls. It will require specialized know-how.

Findings

- **U.S. global leadership and competitiveness:** The U.S. must maintain its position as a global leader. This requires ensuring the U.S. sets the standard in terms of values and ethics, especially within the context of increased geopolitical volatility and an erosion of democratic values abroad.
- **Emerging threats:** AI will give rise to new emerging threats including the development and use of AI in cyber attacks, as well as the risk of new autonomous, biological, and chemical weapons.
- **Spending is rising:** The U.S. has experienced a substantial increase in AI spending during the last year. The DoD, in particular, is investing in research, development, test and evaluation, and other initiatives to integrate AI into the department.[40]
- **Continued deficit of qualified personnel:** As far back as 2018, the DoD had identified an AI-proficient workforce as a focus area and priority. The National Security Commission on Artificial Intelligence found in 2021 that the continued AI talent deficit was a key impediment to the U.S. being AI-ready by 2025. A 2023 GAO assessment found that the DoD continued, for example, to lack human capital implementation actions and AI-related terminology.[41]

[40]Jacob Larson, James S. Denford, Gregory S. Dawson, and Kevin C. Desouza, "The evolution of artificial intelligence (AI) spending by the U.S. government," The Brookings Institution, March 26, 2024, https://www.brookings.edu/articles/the-evolution-of-artificial-intelligence-ai-spending-by-the-u-s-government/.
[41]Alissa H. Czyz, "Artificial Intelligence: Actions Needed to Improve DOD's Workforce Management Report to the Committee on Armed Services, House of Representatives," United States Government Accountability Office, December 2023, https://www.gao.gov/products/gao-24-105645.

- **Balancing open source and national security:** Research indicates that even in the realm of national security, open source can help to advance national interests.[42] Open source communities can help the U.S. stay ahead of geopolitical adversaries by allowing American firms and entrepreneurs to innovate rapidly and continually. Moreover, the open source AI community can help identify and resolve security vulnerabilities. The July 2024 National Telecommunications and Information Administration (NTIA) report on "Dual-Use Foundation Models with Widely Available Model Weights" concluded that given the ongoing evolution of open foundation model capabilities and limitations– as well as the difficulty of quantifying related benefits and risks–it would be difficult to recommend a specific policy path at the moment. As such, the report recommends expanding the government's ability to gather evidence, assess, and act accordingly, meanwhile supporting "openness in ways that enhance its benefits."[43] This support could include encouraging more research on these issues.[44]
- **Mindset change on approaching national security needed:** National security officials will need to develop a flexible mindset to adapt to an environment that will be increasingly automated and will continue to evolve. The nature of warfare itself is changing, and this will affect everything from procurement to tactics, as well as the laws of war. A culture that embraces constant iteration and adjustment will provide a strategic advantage.[45]
- **Data challenges:** Data will become an increasingly critical component in national security in order to conduct intelligence and information operations, build better models, and act as a strategic asset. The acquisition and processing of data through open source and AI promises to target operations more precisely and ultimately more effectively. Furthermore, AI will also make it easier to leverage narrative intelligence to follow and analyze disinformation campaigns and trends.

---

[42]Masao Dahlgren, "Defense Priorities in the Open-Source AI Debate," CSIS, August 19, 2024, https://www.csis.org/analysis/defense-priorities-open-source-ai-debate.

[43]"Dual-Use Foundation Models with Widely Available Model Weights," National Telecommunications and Information Administration, U.S. Department of Commerce, July 2024, https://www.ntia.gov/sites/default/files/publications/ntia-ai-open-model-report.pdf.

[44]Ibid.

[45]Statement before the Senate Select Committee on Intelligence "Addressing the National Security

The U.S. will, however, have to be extremely efficient and agile in organizing and using data. While authoritarian nations have much broader and centralized access to data, the U.S. approach must be consistent with protecting privacy and civil liberties. Furthermore, given the strategic importance of data, the U.S. will have to be especially diligent in protecting its data and data centers from adversaries.

Policy Recommendations

- **Values, ethics, and partnerships:** The U.S. should take leadership and work with its allies to ensure that AI systems are imbued with values consistent to the democratic world and to set a standard of ethics with regard to the use of AI in warfare.
- **Incorporating U.S. values:** Security should be aligned with American values and balanced with civil liberties. AI will increasingly be used in the context of national security and law enforcement. The Transportation Security Administration (TSA) will, for example, use AI-powered facial recognition technology. Congress, DHS, DoD, and other relevant organizations should work to determine strategies to ensure these technologies do not encroach upon civil liberties. The White House National Security Memo on AI, too, addresses this and calls on agencies to monitor, assess, and mitigate risks related to human rights, civil rights, and privacy in defense, intelligence, or law enforcement contexts. One additional idea could be the creation of a "Privacy and Civil Liberties Oversight Board" that could work independently and encompass civil rights-related considerations in AI used for national security purposes.[46]

Implications of Artificial Intelligence: People, Bureaucracy, and Data Infrastructure" Testimony by Dr. Benjamin Jensen, CSIS, September 19, 2023, https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-09/230919_Jensen_AddressingNationalSecurityImplications_ArtificialIntelligence.pdf?VersionId=pICjkTd.eXHY.x4PFB0PWQ08SwjGxzZK.

[46]Faiza Patel and Patrick C. Toomey, "An Oversight Model for AI in National Security: The Privacy and Civil Liberties Oversight Board," The Brennan Center for Justice, April 30, 2024, https://www.brennancenter.org/our-work/analysis-opinion/oversight-model-ai-national-security-privacy-and-civil-liberties.

- **Maintaining a robust system of checks and balances:** Similarly, there should be a system of checks and balances when high-risk AI is used for national security. Congress could put in place an AI framework statute to ensure multiple checks, including knowledge of Congress and approval of the president, are in place before certain types of technology are used.[47]
- **Education is a national security issue:** Much like in the post-WWII era, the U.S. government should consider education a national security issue. In line with this, the U.S. will need to create an approach that links national security to education and workforce evolution.[48]

Specific to national security, existing personnel should be equipped not just with technical skills but also a mindset conducive to thinking of warfare and security in the hybrid, cyber-physical context. Likewise, national security leaders that can think holistically, incorporating cyber and AI dimensions will be integral for resiliency. For this, the armed services could develop a technical leadership program within their academies.

While the DoD has been working on its AI workforce strategy, the GAO found in a December 2023 report that there are still gaps, including the additional steps necessary to fully define and identify DOD's AI workforce and the timeline for adoption of the steps necessary to fully define and identify the AI workforce.[49] National security organizations will need to expand upon recruitment pipelines, both in the short term and in the long term, from a variety of sources. As a positive step, the National Defense Authorization Act (NDAA) includes several AI provisions, including directing the DoD to identify individuals with AI expertise.

---

[47]Ashley Deeks, "Regulating National Security AI Like Covert Action?," Lawfare, July 25, 2023, https://www.lawfaremedia.org/article/regulating-national-security-ai-like-covert-action.

[48]Broader suggestions on developing the U.S. resiliency are detailed in the workforce section.

[49]Alissa H. Czyz, "Artificial Intelligence: Actions Needed to Improve DOD's Workforce Management Report to the Committee on Armed Services, House of Representatives," United States Government Accountability Office, December 2023, https://www.gao.gov/products/gao-24-105645.

- **Open source as an asset:** Open source communities can strengthen national security and reliability. Concerns over the confidentiality and reliability of foundation models remain concerns to the national security community. Supporting the open research community can serve to increase reliability.[50] Regardless, some assets will continue to need heightened security. The recently formed Testing Risks of AI for National Security (TRAINS) Taskforce can help to determine these risks and take steps to mitigate appropriately.
- **Crowdsourcing expert know-how:** DARPA's efforts to crowdsource expertise through challenges are reaping results and should continue to be supported by increased resources. It is spearheading programs to find new cybersecurity solutions for AI and AI edtech solutions to teach STEM subjects to adults.[51]
- **AI integration:** Utilizing AI to garner efficiency can serve to breed greater familiarity and comfort with the technologies while ensuring that the U.S. government is capitalizing on the efficiencies that AI can provide. Congress is currently debating a bill for the DoD to carry out a pilot program on using AI-enabled software "to optimize the workflow and operations of DoD depots, shipyards, and other manufacturing facilities."[52]
- **Emerging threats:** Mapping and mitigating risk will be critical, particularly with regard to the possible threats from new biological, chemical, and autonomous weapons that use AI. National security organizations and other relevant government agencies should be part of this effort and include relevant

[50]Masao Dahlgren, "Defense Priorities in the Open-Source AI Debate," CSIS, August 19, 2024, https://www.csis.org/analysis/defense-priorities-open-source-ai-debate.
[51]"AI-Enabled Tools Show Promise in Upskilling National Security Workforce," DARPA, July 25, 2024,
https://www.darpa.mil/news-events/2024-07-25
[52]Text of S. 4758, Introduced in Senate July, 24, 2024, https://www.congress.gov/bill/118th-congress/senate-bill/4758/text.

outside stakeholders.[53] In conjunction, the government must continue R&D and investment in new technologies. This includes allocating resources to identify and plan for investments in emerging technologies, such as quantum computing and advanced manufacturing, that work together with and can even amplify the power of AI.

Protecting critical infrastructure: National security organizations should seek to map and determine risk levels — not just for the physical aspects of critical infrastructure, but AI software and hardware tools.[54] Organizations should then determine security plans accordingly, while Congress should allocate resources to ensure critical infrastructure security based on these assessments.

Meanwhile, the use of AI to protect critical infrastructure also needs to be considered. DHS recently acknowledged that certain AI-enabled systems can provide new tools to protect critical infrastructure.[55] In coordination with all relevant departments, such as DoD and DoE, as well as private sector actors, DHS is well-positioned to be a convening and coordination center for the deployment of such tools.

Data management and optimization: As data is the key resource in the AI world, national security organizations will have to invest in systems to manage data collection and processing. In addition to resources allocated to compute, policies should be designed to assess sound data collection and processing methodologies. The DoD should continue its work to make sure that data silos are reduced, processes are streamlined to ensure data optimization, and AI is used to optimize critical analysis.

---

[53]Bill Drexel and Caleb Withers, "Catalyzing Crisis: A Primer on Artificial Intelligence, Catastrophes, and National Security," Center for New American Security, June 2024, https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/Catastrophic-AI_TECH-2024_Final.pdf.

[54]Chris Sledjeski, "Principles for Reducing AI Cyber Risk ın Critical Infrastructure: A Prioritization Approach," MITRE, 2023, https://www.mitre.org/sites/default/files/2023-10/PR-23-3086%20Principles-for%20 Reducing-AI-Cyber-Risk-in-Critical-Infrastructure.pdf.

[55]Alejandro N. Mayorkas, "Memorandum for Distribution: Srategic Guidance and National Priorities for U.S. Critical Infrastructure Security and Resilience (2024-2025)," U.S. Department of Homeland Security, June 14, 2024, https://www.dhs.gov/sites/default/files/2024-06/24_0620_sec_2024-strategic-guidance-national-priorities-u-s-critical-infrastructure-security-resilience.pdf.

Cybersecurity

Cybersecurity is a matter of U.S. competition because the ability to protect sensitive information and critical infrastructure is crucial for maintaining national security, economic stability, and technological leadership in an increasingly interconnected and adversarial global landscape. As AI develops, its potential use in attacks increases. Tactics become more sophisticated. However, AI can also be an important part of the solution, helping to move from a reactive to a more preventive approach. AI public policy should promote the development of standards and protocols to protect against data breaches, cyber threats, and the misuse of AI technologies. AI could also assist experts in better assessing and analyzing risks, organizing data, and optimizing decision-making and solutions more rapidly and efficiently.

One of the key debates on AI regulation is balancing security and innovation. However, it is becoming increasingly clear that without security, innovation will be short-lived, and trust will plummet. Ensuring AI security will entail developing new methodologies as the technology evolves. The foundation of effective cybersecurity will also be contingent upon the development and deployment of AI, which is safe and secure.

Findings

- **Fragmented approach:** A "patchwork" of regulation can result in inconsistencies and security gaps. States have already started debating and even passing their own AI laws. Yet, unified federal regulation is the most secure way of mitigating this risk while fostering more predictability, thus more competition. Furthermore, federal-level policy can also lessen compliance burdens upon companies and other institutions. Harmonization in the U.S. as well as internationally can also ensure that the U.S. AI industry retains its leading edge.
- **Standards and metrics as a baseline:** AI standards and metrics are not yet established. Without this critical starting point, many other risk mitigation efforts become difficult. For example, the absence of clear and uniform standards and metrics not only makes auditing difficult but it also could create inconsistent evaluations, which are, in and of themselves, risks.

- **Escalating attacks:** Cyber attacks are on the rise and will rise further, with both private and state actors among the culprits. It is very difficult for humans alone to respond to automated attacks. AI can help detect, alert, identify, and mitigate these attacks.

Policy Recommendations

- **U.S. AI Safety Institute:** Confirmation of the U.S. AI Safety Institute as the central contact for the private sector is a significant step to ensuring consistent and sound testing, development of standards and mitigation measures.
- **NIST funding:** Given NIST's increasing responsibilities and expansive programs, policymakers should provide it with commensurate funding to fulfill its new tasks to support American leadership.
- **Development of "brakes" for AI:** Permissive action links are used in nuclear weapons to prevent unintentional use. Some similar measures could be put in place to prevent accidents in the AI sector. Congress should establish a commission that can determine the types of safeguards that can be put in place together with industry.[56] Congress could mandate that high-risk applications run pre-deployment risk assessments in secure facilities.[57] The U.S. government could also engage in dialogue with adversaries on limiting the use of AI in certain fields and on developing "universal" security measures for dual-use technology in particular.[58]

[56]Henry A. Kissinger and Graham Allison, "The Path to AI Arms Control," Foreign Affairs, October 13, 2023, https://www.foreignaffairs.com/united-states/henry-kissinger-path-artificial-intelligence-arms-control.

[57]Ibid.

[58]Kevin Klyman and Raphael Pilliero, "AI and the A-bomb: What the analogy captures and misses," Bulletin of the Atomic Scientists, September 9, 2024, https://thebulletin.org/2024/09/ai-and-the-a-bomb-what-the-analogy-captures-and-misses/.

- **Lessons learned:** Congress could establish a database or hub of AI failures or incidences. This could be a repository of information about AI system failures, accidents, security breaches, and other potentially hazardous incidents with the federal government.[59] This could potentially be a resource to assist researchers and policymakers to pinpoint flaws and design mechanisms to ensure that things "go right."
- **"Persistent engagement:"** Establish protocols and work streams throughout the federal government that encourage "persistent engagement" with cyber threats.[60] This more proactive approach would be intended to help institutions understand and therefore counter risks in advance.
- **Cyber workforce:** The deficit of cybersecurity experts can be considered a national security vulnerability. We applaud the National Cyber Workforce and Education Strategy (NCWES)'s ecosystem approach that recognizes that no single stakeholder can fill this deficit. We look forward to the Office of the National Cyber Director (ONCD) cyber workforce and education ecosystem playbook. We also are encouraged by the ONCD "Service for America" program focused on cybersecurity experts.[61] Similar programs in other subject matter areas should be determined and executed.

[59]John Croxton, David Robusto, Satya Thallam, Doug Calidas, "Message Incoming: Establish an AI Incident Reporting System," Federation of American Scientists, June 25, 2024, https://fas.org/publication/establishing-an-ai-incident-reporting-system/.

[60]David Rand, "What Many Get Wrong About Persistent Engagement and Why It Matters to Business," May 8, 2023, Tanium, https://www.tanium.com/blog/what-many-get-wrong-about-persistent-engagement-and-why-it-matters-to-business/.

[61]"Initial Stages of Evaluation of the National Cyber Workforce and Education Strategy," The White House, June 2024, https://www.whitehouse.gov/wp-content/uploads/2024/06/NCWES-Initial-Report-2024.06.25.pdf?trk=public_post_comment-text; Marcus Law, "How the White House is Tackling the Cyber Skills Gap," Technology Magazine, September 9, 2024, https://technologymagazine.com/articles/how-the-white-house-is-tackling-the-cyber-skills-gap.

Legal Framework & Consumer Protection

Privacy & Consumer Protection

Privacy is vital to consumer well-being and consistency for market participantsPolicymakers will need to tackle personal data protection, the establishment of sensible privacy standards, and safeguarding against unauthorized data collection and misuse. In addition, policymakers should explore the real world consequences of bias and discrimination in AI results and formulate solutions.

Findings

- **Data is a key AI component:** Data is the fundamental ingredient of AI, and the federal government will likely need to address evolving data trends.
- **Voracious appetite for data:** This time, the stakes are higher as the scale of data usage is significantly higher.
- **Algorithmic bias:** AI systems can be skewed – either inadvertently or purposefully. Factors that can create biases in the models include data inputs used to train models, including training language, certain assumptions made by programmers, or even the interpretation of outputs by end users. These choices can have serious repercussions, including on essential civil rights political discourse and on issues as wide-ranging as healthcare, education, and employment. Not only can these outcomes create unfair outcomes for individuals, but over time, they have the potential to have a lasting and structural impact on society at large — eroding trust and abetting polarization.

Policy Recommendations

- **Federal privacy law:** We encourage the adoption of a federal-level privacy law. Privacy rules at the national level would provide consumers and regulators with consistent standards while giving companies clear guidelines instead of forcing them to navigate a complex patchwork of jurisdictions. Furthermore, it would also provide a greater sense of trust to consumers, knowing that their data was being treated consistently across the U.S.

Consumer Protection

- **Utilize existing laws:** Congress should examine existing laws to ensure civil rights are duly safeguarded in the AI ecosystem and other proposals that address discriminatory biases. The goal should be to maximize a competitive technology ecosystem that is consistent with existing legal frameworks and guided by a spirit of empowerment and wide adoption.
- **AI literacy:** Expanding AI awareness and literacy will be important to help consumers understand AI. We would encourage the passage of legislation that would develop and carry out the appropriate public awareness and literacy campaigns.
- **Public awareness campaign on privacy literacy:** Along with a general lack of AI literacy within the American population, low levels of data and privacy literacy are issues that could affect how citizens utilize and interact with AI systems.[62]
- **Consumer-oriented keys:** Easy to understand, consumer-oriented, and transparent legends to understand AI and privacy could be mandated by Congress. For example, "AI Nutrition Labels" are model cards that provide key information about an AI model's privacy level and design elements in a consistent and transparent format so that businesses and consumers can clearly understand the products. Similarly, an "AI Privacy Ladder" would show the type of data used by the model and whether the model is exclusively for your use or the use of multiple customers.

[62]Nicol Turner Lee, Joseph B. Keller, Cameron F. Kerry, Aaron Klein, Anton Korinek, Mark MacCarthy, Mark Muro, Chinasa T. Okolo, Courtney C. Radsch, John Villasenor, Darrell M. West, Tom Wheeler, Andrew W. Wyckoff, and Rashawn Ray, edited by Mishaela Robison, "Will the White House AI Executive Order deliver on its promises?," The Brookings Institution, November 2, 2023, https://www.brookings.edu/articles/will-the-white-house-ai-executive-order-deliver-on-its-promises./

Liability

A national AI public policy framework should focus on creating clear guidelines for liability to encourage innovation and competition while protecting the public. Liability policies related to AI address the question of who is responsible when AI systems fail or cause harm. Policies should address how liability is assigned, whether to the developers, users, or manufacturers of AI technologies. Policymakers may also explore the need for new legal frameworks to accommodate the autonomous nature of AI systems.

- **Two parameters of consideration in liability**: If developers fail to employ industry-leading safety practices, such as rigorous independent safety testing or the installation of robust safeguards against misuse, they may incur substantial liability exposure due to negligence. If courts or legislatures deem (certain) AI systems to be "products," product liability would apply. Not only is there uncertainty regarding developers' liability with regard to third parties, but existing legal provisions may also impact how liability is interpreted.[63]
- **State-specific tort liability:** Tort liability is primarily contingent on state law.[64] As such, there is a great deal of uncertainty for AI developers, who, depending on the state, may incur little or substantial tort liability.
- **Application of existing laws and standards**: Aspects of how existing laws will apply will be determined by the courts. However, regulatory agencies must also determine how existing laws and regulations apply to AI systems. In a joint statement, for instance, the FTC, the DOJ's Civil Rights Division, the Equal Employment Opportunity Commission, and the Consumer Financial Protection Bureau stated that "[e]xisting legal authorities apply to the use of automated systems and innovative new technologies just as they apply to other practices."[65]

---

[63]Ketan Ramakrishnan, Gregory Smith, Conor Downey, "U.S. Tort Liability for Large-Scale Artificial Intelligence Damages: A Primer for Developers and Policymakers," RAND Corporation, August 21, 2024, https://www.rand.org/pubs/research_reports/RRA3084-1.html.

[64]Ibid.

[65]"Liability Rules and Standards," NTIA, U.S. Department of Commerce, March 27, 2024, https://www.ntia.gov/issues/artificial-intelligence/ai-accountability-policy-report/using-accountability-inputs/liability-rules-and-standards.

Policy Recommendations

- **Consultation needed:** Congress and state legislatures will need to conduct research, with input from numerous parties — including those impacted–so as to inform policymakers on the role and implications of liability.[66]
- **Well-defined roles:** AI regulation needs to clearly and appropriately delineate the various roles and obligations of actors in the AI value chain. Such rules should also include safe harbors, as well as proportional obligations, to ensure that small start-ups and entrepreneurs are not unduly burdened with regulatory requirements that are more appropriate for larger players. Clear delineation of roles and responsibilities will help ensure that the wrong stakeholders are not inadvertently tasked with responsibilities they cannot meet while holding the appropriate stakeholders accountable. Congress should consider an 'AI Accountability Framework' that looks at the issue based on the role a stakeholder plays in the value chain. This should move beyond the developer/user delineation to create space for other intermediaries, for example, recognizing the "integrator" as a separate role.
- **Developing voluntary standards:** The creation and adoption of voluntary industry standards will help ensure clear accountability.
- **Safe harbor:** The U.S. should consider certain mechanisms to protect researchers conducting vital research from liability. Another option would be to create regulatory sandboxes for high-risk AI systems.[67]

---

[66]Ellen P. Goodman, "Artificial Intelligence Accountability Policy Report," NTIA U.S. Department of Commerce, March 2024, https://www.ntia.gov/sites/default/files/ntia-ai-report-final.pdf#clean_NTIA_v1-3_footnotes.indd%3A.120995%3A909.

[67]"Challenges in evaluating AI systems," Anthropic, October 4, 2023, https://www.anthropic.com/news/evaluating-ai-systems.

Conclusion

As the AICC, we believe that as AI reshapes our economy, security, and society, the United States must act decisively to maintain its competitive edge, ensure that the technology serves all Americans, and serve as a leader in global AI governance.

The U.S. would benefit from a "whole of government" approach, with much greater coordination across agencies, to ensure consistency and clarity for the private sector and the public. Furthermore, the federal government will need to work closely with the private sector and civil society, as well as with its allies to tackle this momentous challenge. We believe in "All of the Above AI" whereby —– according to user needs —– both open source and closed AI models should advance to meet marketplace demands.

The AICC presents four critical pillars for a comprehensive national framework to harness the potential of this transformational technology. With regard to the economy, policymakers should ensure we retain our edge by providing innovative entrepreneurs with access to resources and markets through more streamlined procurement processes. An "AI Education for All" program will not only focus on upskilling and retraining the existing workforce but also revamping the education system to prepare for a new generation of workers. Regional development programs will ensure that not just parts but the whole country can prosper.

Modern infrastructure is a prerequisite for AI advancement. Inclusive broadband serves as a foundation for AI development, while AI stands to provide flexibility and efficiency for spectrum management. There is a significant AI energy challenge that will need to be addressed through grid modernization and expanding access to diverse sources of clean energy.

The U.S. will have to use and develop its resources wisely as part of a national security strategy. National security leaders and personnel that have both technical skills and can think holistically will be key. The U.S. will also have to be agile in organizing and integrating data as a key component of national security. Furthermore, the U.S. can be a leader in strengthening collaboration with like-minded allies to ensure that democratic values are integrated into AI systems across the world.

AI cybersecurity is vital to national security. The AI Safety Institute's work to develop federal standards will be a good step to achieving this goal. Policymakers will have to ensure the safety of critical infrastructure and further expand upon the cybersecurity workforce.

Another key foundation for competitive AI is forward-looking and adequate legal protection. Federal privacy legislation will help provide consistency, while consumer-oriented measures and education can further protect Americans. Finally, liability frameworks will need to appropriately assign responsibility across the AI value chain.

Our National AI Policy Framework is in Beta

And that's okay. Any compelling national plan on technology policy will necessarily be in beta and should remain flexible to change with the pace of advancements. We encourage all participants with an interest in this debate — from civil society and academia, to industry and policy leaders — to provide feedback on our first draft here. This is a participatory process, and we welcome feedback.

Given the speed with which AI is progressing, policies developed today will likely require increased adaptation and evolution over time, allowing the U.S. policy framework to remain dynamic and flexible. This will be challenging for policymakers, who often deal with longer timelines in devising new policies. Yet, given the nature of technology, it will be imperative to act quickly and continuously adapt as technology and policy needs evolve.

This approach also harkens back to how the U.S. gained a critical advantage over the Internet in the 1990s through a path that built a policy framework through a series of laws. Rather than one sweeping piece of legislation, history has shown that a more flexible approach allows policy to keep pace with market developments.


COMPETITION
CENTER