MAY 2024

Driving U.S. Innovation in Artificial Intelligence

A ROADMAP FOR ARTIFICIAL INTELLIGENCE POLICY IN THE UNITED STATES SENATE



The Bipartisan Senate Al Working Group

Majority Leader Chuck Schumer Senator Mike Rounds Senator Martin Heinrich Senator Todd Young

Introduction

Early in the 118th Congress, we were brought together by a shared recognition of the profound changes artificial intelligence (AI) could bring to our world: AI's capacity to revolutionize the realms of science, medicine, agriculture, and beyond; the exceptional benefits that a flourishing AI ecosystem could offer our economy and our productivity; and AI's ability to radically alter human capacity and knowledge. At the same time, we each recognized the potential risks AI could present, including altering our workforce in the short-term and long-term, raising questions about the application of existing laws in an AI-enabled world, changing the dynamics of our national security, and raising the threat of potential doomsday scenarios. This led to the formation of our Bipartisan Senate AI Working Group ("AI Working Group").

From the outset, the AI Working Group's objective has been to complement the traditional congressional committee-driven policy process, considering that this broad technology does not neatly fall into the jurisdiction of any single committee. We resolved to bring leading experts into a unique dialogue with the Senate on some of the most profound policy questions AI presents. In doing so, we aimed to help lay the foundation for a better understanding in the Senate of the policy choices and implications around AI.

Our efforts began with three educational briefings on AI for senators in the summer of 2023, culminating in the first ever all-senators classified briefing focused solely on AI. These sessions made clear there is broad bipartisan interest in AI and emphasized the need for further policy discussions, acknowledging the complexity of the subject and the importance of well-informed deliberations. To address more specific policy domains, the AI Working Group then hosted nine bipartisan AI Insight Forums in the fall of 2023.

The topics for these nine forums included:

- 1. Inaugural Forum
- 2. Supporting U.S. Innovation in AI
- 3. Al and the Workforce
- 4. High Impact Uses of AI
- 5. Elections and Democracy
- 6. Privacy and Liability
- 7. Transparency, Explainability, Intellectual Property, and Copyright
- 8. Safeguarding Against AI Risks
- 9. National Security

The Insight Forums were designed to complement previous and ongoing committee hearings and promote an unvarnished discussion between AI stakeholders that are too often siloed from one another. As senators, we acted as moderators, aiming to foster an environment where experts could challenge each other's perspectives in a candid and productive manner. We invited all of our Senate colleagues as well as relevant Senate staff to attend.

To ensure these forums could effectively identify consensus areas, we recognized from the start that we would need a diverse range of experts capable of representing different perspectives on, and uses of, AI. In each forum, our aim was to include representation from:

- Across the AI ecosystem, encompassing developers, deployers, and users of AI from startups to established companies;
- Providers of key components of the AI supply chain, both in hardware and software; and
- Academia and civil society, from AI researchers and think tanks to labor unions and civil rights leaders.

In total, more than 150 experts participated in the forums. We extend our gratitude to each of them for their valuable time, insights, and continued engagement. A comprehensive list of attendees and links to their written statements are available in the appendix.

The AI Insight Forums propelled the AI Working Group to better understand the policy landscape of AI and helped inform a policy roadmap—pinpointing emerging areas of consensus within respective policy domains, as well as areas of disagreement, while also revealing where further work and research is needed.

The Road Ahead

To build on the many AI initiatives already undertaken and ongoing at the federal level, the following AI policy roadmap identifies areas of consensus that we believe merit bipartisan consideration in the Senate in the 118th Congress and beyond. To be certain, this is not an exhaustive menu of policy proposals.

As members of the AI Working Group, we are steadfast in our dedication to harnessing the full potential of AI while minimizing the risks of AI in the near and long term. We hope this roadmap will stimulate momentum for new and ongoing consideration of bipartisan AI legislation, ensure the United States remains at the forefront of innovation in this technology, and help all Americans benefit from the many opportunities created by AI.

A few final overarching thoughts from the AI Working Group:

Given the cross-jurisdictional nature of AI policy issues, we encourage committees to continue to collaborate closely and frequently on AI legislation as well as agree on shared clear definitions for all key terms.

Committees should reflect on the synergies between AI and other emerging technologies to avoid creating tech silos where the impact of legislation and funding could otherwise be collectively amplified.

We hope committees will continue to seek outside input from a variety of stakeholders and experts to inform the best path forward for this quickly advancing technology.

Finally, we encourage the executive branch to share with Congress, in a timely fashion and on an ongoing basis, updates on administration activities related to AI, including any AI-related Memorandums of Understanding with other countries and the results from any AI-related studies in order to better inform the legislative process.

Supporting U.S. Innovation in Al

The AI Working Group encourages the executive branch and the Senate Appropriations Committee to continue assessing how to handle ongoing needs for federal investments in AI during the regular order budget and appropriations process, with the goal of reaching as soon as possible the spending level proposed by the National Security Commission on Artificial Intelligence (NSCAI) in their final report: at least \$32 billion per year for (non-defense) AI innovation.

The AI Working Group also encourages the Senate Appropriations Committee to work with the relevant committees of jurisdiction to develop emergency appropriations language to fill the gap between current spending levels and the NSCAI-recommended level, including the following priorities:

- Funding for a cross-government AI research and development (R&D) effort, including relevant infrastructure that spans the Department of Energy (DOE), Department of Commerce (DOC), National Science Foundation (NSF), National Institute for Standards and Technology (NIST), National Institutes of Health (NIH), National Aeronautics and Space Administration (NASA), and all other relevant agencies and departments. This should include an all-of-government "AI-ready data" initiative, and direction for research priorities in responsible innovation, including but not limited to:
 - Fundamental and applied science, such as biotechnology, advanced computing, robotics, and materials science
 - Foundational trustworthy AI topics, such as transparency, explainability, privacy, interoperability, and security
- Funding the outstanding CHIPS and Science Act (P.L. 117-167) accounts not yet fully funded, particularly those related to AI, including but not limited to:
 - NSF Directorate for Technology, Innovation, and Partnerships
 - DOC Regional Technology and Innovation Hubs (Tech Hubs)
 - DOE National Labs through the Advanced Scientific Computing Research Program in the DOE Office of Science
 - DOE Microelectronics Programs
 - NSF Education and Workforce Programs, including the Advanced Technical Education (ATE) Program
- Funding, as needed, for the DOC, DOE, NSF, and Department of Defense (DOD) to support semiconductor R&D specific to the design and manufacturing of future generations of high-end AI chips, with the goals of ensuring increased American

leadership in cutting-edge AI through the co-design of AI software and hardware, and developing new techniques for semiconductor fabrication that can be implemented domestically.

- Authorizing the National AI Research Resource (NAIRR) by passing the CREATE AI Act (S. 2714) and funding it as part of the cross-government AI initiative, as well as expanding programs such as the NAIRR and the National AI Research Institutes to ensure all 50 states are able to participate in the AI research ecosystem.
- Funding a series of "AI Grand Challenge" programs, such as those described in Section 202 of the Future of AI Innovation Act (S. 4178) and the AI Grand Challenges Act (S. 4236), drawing inspiration from and leveraging the success of similar programs run by the Defense Advanced Research Projects Agency (DARPA), DOE, NSF, NIH, and others like the private sector XPRIZE, with a focus on technical innovation challenges in applications of AI that would fundamentally transform the process of science, engineering, or medicine, and in foundational topics in secure and efficient software and hardware design.
- Funding for AI efforts at NIST, including AI testing and evaluation infrastructure and the U.S. AI Safety Institute, and funding for NIST's construction account to address years of backlog in maintaining NIST's physical infrastructure.
- Funding for the Bureau of Industry and Security (BIS) to update its information technology (IT) infrastructure and procure modern data analytics software; ensure it has the necessary personnel and capabilities for prompt, effective action; and enhance interagency support for BIS's monitoring efforts to ensure compliance with export control regulations.
- Funding R&D activities, and developing appropriate policies, at the intersection of Al and robotics to advance national security, workplace safety, industrial efficiency, economic productivity, and competitiveness, through a coordinated interagency initiative.
- Supporting a NIST and DOE testbed to identify, test, and synthesize new materials to support advanced manufacturing through the use of AI, autonomous laboratories, and AI integration with other emerging technologies, such as quantum computing and robotics.
- Providing local election assistance funding to support AI readiness and cybersecurity through the Help America Vote Act (HAVA) Election Security grants.
- Providing funding and strategic direction to modernize the federal government and improve delivery of government services, including through activities such as

updating IT infrastructure to utilize modern data science and AI technologies and deploying new technologies to find inefficiencies in the U.S. code, federal rules, and procurement programs.

Supporting R&D and interagency coordination around the intersection of AI and critical infrastructure, including for smart cities and intelligent transportation system technologies.

The AI Working Group supports funding, commensurate with the requirements needed to address national security threats, risks, and opportunities, for AI activities related to defense in any emergency appropriations for AI. Priorities in this space include, but are not limited to:

- National Nuclear Security Administration (NNSA) testbeds and model evaluation tools.
- Assessment and mitigation of Chemical, Biological, Radiological, and Nuclear (CBRN) Al-enhanced threats by DOD, Department of Homeland Security (DHS), DOE, and other relevant agencies.
- Support for further advancements in Al-augmented chemical and biological synthesis, as well as safeguards to reduce the risk of dangerous synthetic materials and pathogens.
- Increased funding for DARPA's AI-related work.
- Development of secure and trustworthy algorithms for autonomy in DOD platforms.
- Ensuring the development and deployment of Combined Joint All-Domain Command and Control (CJADC2) and similar capabilities by DOD.
- Development of AI tools for service members and commanders to learn from and improve the operation of weapons platforms.
- Creation of pathways for data derived from sensors and other sources to be stored, transported, and used across programs, including Special Access Programs (SAPs), to reduce silos between existing data sets and make DOD data more adaptable to machine learning and other AI projects.
- Building up in-house supercomputing and AI capacity within DOD, including resources for both new computational infrastructure and staff with relevant

expertise in supercomputing and AI, along with appropriate training materials for preparing the next generation of talent in these areas.

- As appropriate, utilization of the unique authorities in AUKUS Pillar 2 to work collaboratively with our allies for co-development of integrated AI capabilities.
- Development of AI-integrated tools to more efficiently implement Federal Acquisition Regulations.
- Use of AI to optimize logistics across the DOD, such as improving workflows across the defense industrial base and applying predictive maintenance to extend the lifetime of weapons platforms.

Furthermore, the AI Working Group:

- Encourages the relevant committees to develop legislation to leverage publicprivate partnerships across the federal government to support AI advancements and minimize potential risks from AI.
- Recognizes the rapidly evolving state of AI development and supports further federal study of AI, including through work with Federally Funded Research and Development Centers (FFRDCs).
- Encourages the relevant committees to address the unique challenges faced by startups to compete in the AI marketplace, including by considering whether legislation is needed to support the dissemination of best practices to incentivize states and localities to invest in similar opportunities as those provided by the NAIRR.
- Supports a report from the Comptroller General of the United States to identify any significant federal statutes and regulations that affect the innovation of artificial intelligence systems, including the ability of companies of all sizes to compete in artificial intelligence.

The AI Working Group also encourages committees to:

- Work with the DOC and other relevant agencies to increase access to tools, such as mock data sets, for AI companies to utilize for testing.
- Encourage DOC and other relevant agencies such as the Small Business Administration (SBA) to conduct outreach to small businesses to ensure the tools related to AI that the agencies provide meet their needs.

- Identify ways the SBA and its partners, including the Small Business Development Centers, Small Business Investment Companies, and microlenders, can support all entrepreneurs and small businesses in utilizing AI as well as innovating and providing services and products related to the growth of AI.
- Clarify that business software and cloud computing services are allowable expenses under the SBA's 7(a) loan program to help small businesses more affordably incorporate technological solutions including AI (Small Business Technological Advancement Act (S. 2330)).

AI and the Workforce

During the Insight Forums there was wide agreement that workers across the spectrum, ranging from blue collar positions to C-suite executives, are concerned about the potential for AI to impact their jobs. The AI Working Group recognizes the apprehension surrounding the inherent uncertainties of this technology, and encourages a conscientious consideration of the impact AI will have on the workforce – including the potential for displacement of workers – to make certain that American workers are not left behind. Additionally, there are opportunities to collaborate with and prepare the American workforce to work alongside this new technology and mitigate potential negative impacts.

Therefore, the AI Working Group encourages:

- Efforts to ensure that stakeholders from innovators and employers to civil society, unions, and other workforce perspectives – are consulted as AI is developed and then deployed by end users.
- The committees of jurisdiction to explore ways to ensure that relevant internal and external stakeholder voices, including federal employees, impacted members of the public, and experts, are considered in the development and deployment of AI systems procured or used by federal agencies.
- Development of legislation related to training, retraining, and upskilling the private sector workforce to successfully participate in an AI-enabled economy. Such legislation might include incentives for businesses to develop strategies that integrate new technologies and reskilled employees into the workplace, and incentives for both blue- and white-collar employees to obtain retraining from community colleges and universities.

- Exploration of the implications and possible solutions (including private sector best practices) to the impact of AI on long-term future of work as increasingly capable general-purpose AI systems are developed that have the potential to displace human workers, and to develop an appropriate policy framework in response, including ways to combat disruptive workforce displacement.
- The relevant committees to consider legislation to improve the U.S. immigration system for high-skilled STEM workers in support of national security and to foster advances in AI across the whole of society.

The AI Working Group also recognizes:

- The promise of the federal government's adoption of AI to improve government service delivery and modernize internal governance as well as upskilling of existing federal employees to maximize the beneficial use of AI.
- Opportunities to recruit and retain talent in AI through programs like the U.S. Digital Service, the Presidential Innovation Fellows, the Presidential Management Fellows, and others authorized in the Intergovernmental Personnel Act and other relevant legislation, and encourages the relevant committees to consider ways to leverage these programs.

The AI Working Group is encouraged by the Workforce Data for Analyzing and Tracking Automation Act (S. 2138) to authorize the Bureau of Labor Statistics (BLS), with the assistance of the National Academies of Sciences, Engineering, and Medicine, to record the effect of automation on the workforce and measure those trends over time, including job displacement, the number of new jobs created, and the shifting indemand skills. The bill would also establish a workforce development advisory board composed of key stakeholders to advise the U.S. Department of Labor on which types of public and private sector initiatives can promote consistent workforce development improvements.

High Impact Uses of AI

The AI Working Group believes that existing laws, including related to consumer protection and civil rights, need to consistently and effectively apply to AI systems and their developers, deployers, and users. Some AI systems have been referred to as "black boxes" which may raise questions about whether companies with such systems are appropriately abiding by existing laws. Thus, in cases where U.S. law requires a clear understanding of how an automated system operates, the opaque nature of some AI systems may be unacceptable. We encourage the relevant committees to consider identifying any gaps in the application of existing law to AI systems that fall under their committees' jurisdiction and, as needed, develop legislative language to address such gaps. This language should ensure that regulators are able to access information directly relevant to enforcing existing law and, if necessary, place appropriate, caseby-case requirements on high-risk uses of AI, such as requirements around transparency, explainability, and testing and evaluation.

Al use cases should not directly or inadvertently infringe on constitutional rights, imperil public safety, or violate existing antidiscrimination laws. The Al Working Group acknowledges that some have concerns about the potential for disparate impact, including the potential for unintended harmful bias. Therefore, when any Senate committee is evaluating the impact of Al or considering legislation in the Al space, the Al Working Group encourages committees to explore how Al may affect some parts of our population differently, both positively and negatively.

The AI Working Group:

- Encourages committees to review forthcoming guidance from relevant agencies that relates to high impact AI use cases and to explore if and when an explainability requirement may be necessary.
- Supports the development of standards for use of AI in our critical infrastructure and encourages the relevant committees to develop legislation to advance this effort.
- Encourages the Energy Information Administration to include data center and supercomputing cluster energy use in their regular voluntary surveys.
- Supports Section 3 of S. 3050, directing a regulatory gap analysis in the financial sector, and encourages the relevant committees to develop legislation that ensures financial service providers are using accurate and representative data in

their AI models, and that financial regulators have the tools to enforce applicable law and/or regulation related to these issues.

- Encourages the relevant committees to investigate the opportunities and risks of the use of AI systems in the housing sector, focusing on transparency and accountability while recognizing the utility of existing laws and regulations.
- Believes the federal government must ensure appropriate testing and evaluation of AI systems in the federal procurement process that meets the relevant standards, and supports streamlining the federal procurement process for AI systems and other software that have met those standards.
- Recognizes the AI-related concerns of professional content creators and publishers, particularly given the importance of local news and that consolidation in the journalism industry has resulted in fewer local news options in small towns and rural areas. The relevant Senate committees may wish to examine the impacts of AI in this area and develop legislation to address areas of concern.

Furthermore, the AI Working Group encourages the relevant committees to:

- Develop legislation to address online child sexual abuse material (CSAM), including ensuring existing protections specifically cover AI-generated CSAM. The AI Working Group also supports consideration of legislation to address similar issues with non-consensual distribution of intimate images and other harmful deepfakes.
- Consider legislation to protect children from potential AI-powered harms online by ensuring companies take reasonable steps to consider such risks in product design and operation. Furthermore, the AI Working Group is concerned by data demonstrating the mental health impact of social media and expresses support for further study and action by the relevant agencies to understand and combat this issue.
- Explore mechanisms, including through the use of public-private partnerships, to deter the use of AI to perpetrate fraud and deception, particularly for vulnerable populations such as the elderly and veterans.
- Continue their work on developing a federal framework for testing and deployment of autonomous vehicles across all modes of transportation to remain at the forefront of this critical space. This effort is particularly critical as our strategic

competitors, like the Chinese Communist Party (CCP), continue to race ahead and attempt to shape the vision of this technology.

- Consider legislation to ban the use of AI for social scoring, protecting our fundamental freedom in contrast with the widespread use of such a system by the CCP.
- Review whether other potential uses for AI should be either extremely limited or banned.

Al is being deployed across the full spectrum of health care services, including for the development of new medicines, for the improvement of disease detection and diagnosis, and as assistance for providers to better serve their patients. The Al Working Group encourages the relevant committees to:

- Consider legislation that both supports further deployment of AI in health care and implements appropriate guardrails and safety measures to protect patients, as patients must be front and center in any legislative efforts on health care and AI. This includes consumer protection, preventing fraud and abuse, and promoting the usage of accurate and representative data.
- Support the NIH in the development and improvement of AI technologies. In particular, data governance should be a key area of focus across the NIH and other relevant agencies, with an emphasis on making health care and biomedical data available for machine learning and data science research, while carefully addressing the privacy issues raised by the use of AI in this area.
- Ensure that the Department of Health and Human Services (HHS), including the Food and Drug Administration (FDA) and the Office of the National Coordinator for Health Information Technology, has the proper tools to weigh the benefits and risks of AI-enabled products so that it can provide a predictable regulatory structure for product developers.
- Consider legislation that would provide transparency for providers and the public about the use of AI in medical products and clinical support services, including the data used to train the AI models.
- Consider policies to promote innovation of AI systems that meaningfully improve health outcomes and efficiencies in health care delivery. This should include examining the Centers for Medicare & Medicaid Services' reimbursement mechanisms as well as guardrails to ensure accountability, appropriate use, and broad application of AI across all populations.

Elections and Democracy

The AI Working Group encourages the relevant committees and AI developers and deployers to advance effective watermarking and digital content provenance as it relates to AI-generated or AI-augmented election content. The AI Working Group encourages AI deployers and content providers to implement robust protections in advance of the upcoming election to mitigate AI-generated content that is objectively false, while still protecting First Amendment rights.

The AI Working Group acknowledges the U.S. Election Assistance Commission (EAC) for its work on the AI Toolkit for Election Officials, and the Cybersecurity and Infrastructure Security Agency (CISA) for its work on the Cybersecurity Toolkit and Resources to Protect Elections, and encourages states to consider utilizing the tools EAC and CISA have developed.

Privacy and Liability

The AI Working Group acknowledges that the rapid evolution of technology and the varying degrees of autonomy in AI products present difficulties in assigning legal liability to AI companies and their users. Therefore, the AI Working Group encourages the relevant committees to consider whether there is a need for additional standards, or clarity around existing standards, to hold AI developers and deployers accountable if their products or actions cause harm to consumers, or to hold end users accountable if their actions cause harm, as well as how to enforce any such liability standards.

The AI Working Group encourages the relevant committees to explore policy mechanisms to reduce the prevalence of non-public personal information being stored in, or used by, AI systems, including providing appropriate incentives for research and development of privacy-enhancing technologies.

The AI Working Group supports a strong comprehensive federal data privacy law to protect personal information. The legislation should address issues related to data minimization, data security, consumer data rights, consent and disclosure, and data brokers.

Transparency, Explainability, Intellectual Property, and Copyright

The AI Working Group encourages the relevant committees to:

- Consider developing legislation to establish a coherent approach to public-facing transparency requirements for AI systems, while allowing use case specific requirements where necessary and beneficial, including best practices for when AI deployers should disclose that their products use AI, building on the ongoing federal effort in this space. If developed, the AI Working Group encourages the relevant committees to ensure these requirements align with any potential risk regime and do not inhibit innovation.
- Evaluate whether there is a need for best practices for the level of automation that is appropriate for a given type of task, considering the need to have a human in the loop at certain stages for some high impact tasks.
- Review to what degree federal agencies are required to provide transparency to their employees about the development and deployment of new technology like AI in the workplace.
- Consider federal policy issues related to the data sets used by AI developers to train their models, including data sets that might contain sensitive personal data or are protected by copyright, and evaluate whether there is a need for transparency requirements.
- Review forthcoming reports from the executive branch related to establishing provenance of digital content, for both synthetic and non-synthetic content.
- Consider developing legislation that incentivizes providers of software products using generative AI and hardware products such as cameras and microphones to provide content provenance information and to consider the need for legislation that requires or incentivizes online platforms to maintain access to that content provenance information. The AI Working Group also encourages online platforms to voluntarily display content provenance information, when available, and to determine how to best display this provenance information by default to end users.
- Consider whether there is a need for legislation that protects against the unauthorized use of one's name, image, likeness, and voice, consistent with First

Amendment principles, as it relates to AI. Legislation in this area should consider the impacts of novel synthetic content on professional content creators of digital media, victims of non-consensual distribution of intimate images, victims of fraud, and other individuals or entities that are negatively affected by the widespread availability of synthetic content.

- Review the results of existing and forthcoming reports from the U.S. Copyright Office and the U.S. Patent and Trademark Office on how AI impacts copyright and intellectual property law, and take action as deemed appropriate to ensure the U.S. continues to lead the world on this front.
- Consider legislation aimed at establishing a public awareness and education campaign to provide information regarding the benefits of, risks relating to, and prevalence of AI in the daily lives of individuals in the United States. The campaign, similar to digital literacy campaigns, should include guidance on how Americans can learn to use and recognize AI.

Safeguarding Against AI Risks

In light of the insights provided by experts at the forums on a variety of risks that different AI systems may present, the AI Working Group encourages companies to perform detailed testing and evaluation to understand the landscape of potential harms and not to release AI systems that cannot meet industry standards. Multiple potential risk regimes were proposed – from focusing on technical specifications such as the amount of computation or number of model parameters to classification by use case – and the AI Working Group encourages the relevant committees to consider a resilient risk regime that focuses on the capabilities of AI systems, protects proprietary information, and allows for continued AI innovation in the U.S. The risk regime should tie governance efforts to the latest available research on AI capabilities and allow for regular updates in response to changes in the AI landscape.

The AI Working Group also encourages the relevant committees to:

Support efforts related to the development of a capabilities-focused risk-based approach, particularly the development and standardization of risk testing and evaluation methodologies and mechanisms, including red-teaming, sandboxes and testbeds, commercial AI auditing standards, bug bounty programs, as well as physical and cyber security standards. The AI Working Group encourages committees to consider ways to support these types of efforts, including through the federal procurement system.

- Investigate the policy implications of different product release choices for Al systems, particularly to understand the differences between closed versus fully open-source models (including the full spectrum of product release choices between those two ends of the spectrum).
- Develop an analytical framework that specifies what circumstances would warrant a requirement of pre-deployment evaluation of AI models.
- Explore whether there is a need for an AI-focused Information Sharing and Analysis Center (ISAC) to serve as an interface between commercial AI entities and the federal government to support monitoring of AI risks.
- Consider a capabilities-based AI risk regime that takes into consideration short-, medium-, and long-term risks, with the recognition that model capabilities and testing and evaluation capabilities will change and grow over time. As our understanding of AI risks further develops, we may discover better risk-management regimes or mechanisms. Where testing and evaluation are insufficient to directly measure capabilities, the AI Working Group encourages the relevant committees to explore proxy metrics that may be used in the interim.
- Develop legislation aimed at advancing R&D efforts that address the risks posed by various AI system capabilities, including by equipping AI developers, deployers, and users with the knowledge and tools necessary to identify, assess, and effectively manage those risks.

National Security

The AI Working Group will collaborate with committees and relevant executive branch agencies to stay informed about the research areas and capabilities of U.S. adversaries.

The AI Working Group encourages the relevant committees to develop legislation bolstering the use of AI in U.S. cyber capabilities.

Managing talent in the realm of advanced technologies presents significant challenges for the DOD and the Intelligence Community (IC). In collaboration with the relevant committees, the AI Working Group:

- Encourages the DOD and IC to further develop career pathways and training programs for digital engineering, specifically in AI, as outlined in Section 230 of the FY2020 National Defense Authorization Act (NDAA).
- Supports the allocation of suitable resources and oversight to maintain a strong digital workforce within the armed services.
- Urges the relevant committees to maintain their efforts in overseeing the executive branch's efficient handling of security clearance applications, particularly emphasizing swift processing for AI talent, to prevent any backlogs or procedural delays.
- Encourages the relevant committees to develop legislation to improve lateral and senior placement opportunities and other mechanisms to improve and expand the AI talent pathway into the military.

The AI Working Group recognizes the DOD's transparency regarding its policy on fully autonomous lethal weapon systems. The AI Working Group encourages relevant committees to assess whether aspects of the DOD's policy should be codified or if other measures, such as notifications concerning the development and deployment of such weapon systems, are necessary.

The AI Working Group encourages the Office of the Director of National Intelligence, DOD, and DOE to work with commercial AI developers to prevent large language models, and other frontier AI models, from inadvertently leaking or reconstructing sensitive or classified information.

The AI Working Group acknowledges the ongoing work of the IC to monitor emerging technology and AI developed by adversaries, including artificial general intelligence (AGI), and encourages the relevant committees to consider legislation to bolster this effort and make sure this long-term monitoring continues.

The AI Working Group:

- Recognizes the significant level of uncertainty and unknowns associated with general purpose AI systems achieving AGI. At the same time, the AI Working Group recognizes that there is not widespread agreement on the definition of AGI or threshold by which it will officially be achieved. Therefore, we encourage the relevant committees to better define AGI in consultation with experts, characterize both the likelihood of AGI development and the magnitude of the risks that AGI development would pose, and develop an appropriate policy framework based on that analysis.
- Encourages the relevant committees to explore potential opportunities for leveraging advanced AI models to improve the management and risk mitigation of space debris. Acknowledging the substantial efforts by NASA and other interagency partners in addressing space debris, the AI Working Group recognizes the increasing threat space debris poses to space systems. Consequently, the AI Working Group encourages the committees to work with agencies involved in space affairs to discover new capabilities that can enhance these critical mitigation efforts.
- Encourages the relevant committees, in collaboration with the private sector, to continue to address, and mitigate where possible, the rising energy demand of AI systems to ensure the U.S. can remain competitive with the CCP and keep energy costs down.

The AI Working Group recognizes the importance of advancements in AI to other fields of scientific discovery such as biotechnology. AI has the potential to increase the risk posed by bioweapons and is directly relevant to federal efforts to defend against CBRN threats. Therefore, the AI Working Group encourages the relevant committees to consider the recommendations of the National Security Commission on Emerging Biotechnology and the NSCAI in this domain, including as they relate to preventing adversaries from procuring necessary capabilities in furtherance of an AI-enhanced bioweapon program.

The Secretary of Commerce, through BIS, holds broad and exclusive authority over export controls for critical technologies such as semiconductors, biotechnology, quantum computing, and more, covering both hardware and software. The AI Working Group encourages the relevant committees to ensure BIS proactively manages these technologies and to investigate whether there is a need for new authorities to address the unique and quickly burgeoning capabilities of AI, including the feasibility of options to implement on-chip security mechanisms for high-end AI chips.

Additionally, the AI Working Group encourages the relevant committees to:

Develop a framework for determining when, or if, export controls should be placed on powerful AI systems. Develop a framework for determining when an AI system, if acquired by an adversary, would be powerful enough that it would pose such a grave risk to national security that it should be considered classified, using approaches such as how DOE treats Restricted Data.

Furthermore, AI Working Group encourages the relevant committees to:

- Ensure the relevant federal agencies have the appropriate authorities to work with our allies and international partners to advance bilateral and multilateral agreements on AI.
- Develop legislation to set up or participate in international AI research institutes or other partnerships with like-minded international allies and partners, giving due consideration to the potential threats to research security and intellectual property.
- Develop legislation to expand the use of modern data analytics and supply chain platforms by the Department of Justice, DHS, and other relevant law enforcement agencies to combat the flow of illicit drugs, including fentanyl and other synthetic opioids.
- Work with the executive branch to support the free flow of information across borders, protect against the forced transfer of American technology, and promote open markets for digital goods exported by American creators and businesses through agreements that also allow countries to address concerns regarding security, privacy, surveillance, and competition. As Russia and China push their cyber agenda of censorship, repression, and surveillance, the AI Working Group encourages the executive branch to avoid creating a policy vacuum that China and Russia will fill, to ensure the digital economy remains open, fair, and competitive for all, including for the three million American workers whose jobs depend on digital trade.



Appendix

Insight Forum Participants

September 13, 2023

INAUGURAL FORUM

- 1. Alex Karp Co-Founder & CEO, Palantir
- 2. Arvind Krishna CEO, IBM
- 3. Aza Raskin Co-Founder, Center for Humane Technology
- 4. Bill Gates Former CEO, Microsoft
- 5. **Brad Smith** President, Microsoft
- 6. Charles Rivkin Chairman & CEO, Motion Picture Association
- 7. Clément Delangue CEO & Co-Founder, Hugging Face
- 8. Deborah Raji Researcher, U.C. Berkeley, and Fellow, Mozilla
- 9. Elizabeth Shuler President, AFL-CIO
- 10. Elon Musk CEO, X, Tesla
- 11. Eric Fanning President & CEO, Aerospace Industries Association
- 12. Eric Schmidt Chair, Special Competitive Studies Project
- 13. Jack Clark Co-Founder, Anthropic Al
- 14. Janet Murguía President & CEO, UnidosUS
- 15. Jensen Huang CEO and Founder, NVIDIA
- 16. Karyn Temple Senior Executive Vice President, Motion Picture Association
- 17. Kent Walker President of Global Affairs, Alphabet Inc., Google
- 18. Laura MacCleery Senior Director of Public Policy, UnidosUS
- 19. Mark Zuckerberg Co-Founder & CEO, Meta
- 20. Maya Wiley President & CEO, Leadership Conference on Civil & Human Rights
- 21. Meredith Stiehm President, Writers Guild
- 22. Nick Clegg Vice President of Global Affairs, Meta
- 23. Patrik Gayer Global Al Policy Advisor, Tesla
- 24. Randi Weingarten President, American Federation of Teachers
- 25. Rumman Chowdhury CEO, Humane Intelligence
- 26. Sam Altman CEO, OpenAl
- 27. Satya Nadella CEO & Chairman, Microsoft
- 28. Shyam Sankar Executive Vice President & CTO, Palantir
- 29. Sundar Pichai CEO, Alphabet Inc., Google
- 30. Tristan Harris Co-Founder & Executive Director, Center for Humane Technology
- 31. Ylli Bajraktari CEO, Special Competitive Studies Project

October 24, 2023

SUPPORTING U.S. INNOVATION IN AI

- 1. Aidan Gomez CEO, Cohere
- 2. <u>Alexandra Reeve Givens</u> President & CEO, Center for Democracy and Technology
- 3. <u>Alondra Nelson</u> Fellow, Institute for Advanced Study and Center for American Progress
- 4. <u>Amanda Ballantyne</u> Director, AFL-CIO Technology Institute
- 5. Austin Carson Founder & President, SeedAl
- 6. Derrick Johnson President & CEO, NAACP
- 7. Evan Smith Co-Founder & CEO, Altana Technologies
- 8. Jodi Forlizzi Herbert A. Simon Professor in Computer Science, Carnegie Mellon University
- 9. John Doerr Engineer & Venture Capitalist, Kleiner Perkins
- 10. <u>Kofi Nyarko</u> Professor, Department of Electrical and Computer Engineering, Morgan State University
- 11. Manish Bhatia Executive Vice President of Global Operations, Micron
- 12. Marc Andreessen Co-Founder & General Partner, Andreessen Horowitz
- 13. Max Tegmark President, Future of Life Institute
- 14. Patrick Collison Co-Founder & CEO, Stripe
- 15. Rafael Reif Former President, Massachusetts Institute of Technology
- 16. Sean McClain Founder & Former CEO, AbSci
- 17. Stella Biderman Executive Director, EleutherAl
- 18. Steve Case Chairman & CEO, Revolution
- 19. <u>Suresh Venkatasubramanian</u> Professor of Computer Science and Data Science, Brown University
- 20. Tyler Cowen Holbert L. Harris Chair of Economics, George Mason University
- 21. <u>Ylli Bajraktari</u> CEO, Special Competitive Studies Project

November 1, 2023

AI AND THE WORKFORCE

- 1. Allyson Knox Director of Education Policy and Programs, Microsoft
- 2. Anton Korinek Professor of Economics, University of Virginia
- 3. <u>Arnab Chakraborty</u> Senior Managing Director, Accenture
- 4. <u>Austin Keyser</u> International President for Government Affairs, International Brotherhood of Electrical Workers
- 5. Bonnie Castillo Executive Director, National Nurses United
- 6. Chris Hyams CEO, Indeed
- 7. Claude Cummings President, Communications Workers of America
- 8. Daron Acemoglu Professor of Economics, Massachusetts Institute of Technology
- 9. José-Marie Griffiths President, Dakota State University
- 10. Michael Fraccaro CPO, Mastercard
- 11. Michael R. Strain Director of Economic Policy Studies, American Enterprise Institute
- 12. Patrick Gaspard President and CEO, Center for American Progress
- 13. Paul Schwalb Executive Secretary-Treasurer, UNITE HERE
- 14. <u>Rachel Lyons</u> Legislative Director, United Food and Commercial Workers International Union
- 15. Robert D. Atkinson President, Information Technology and Innovation Foundation

HIGH IMPACT USES OF AI

- 1. Alvin Velazquez Associate General Counsel, Service Employees International Union
- 2. Arvind Narayanan Associate Professor of Computer Science, Princeton University
- 3. Cathy O'Neil CEO, ORCAA
- 4. Dave Girouard Founder & CEO, Upstart
- 5. Dominique Harrison Senior Fellow, Center for Technology Innovation, Brookings Institution
- 6. Hoan Ton-That Co-Founder & CEO, Clearview Al
- 7. Jason Oxman President & CEO, Information Technology Industry Council
- 8. Julia Stoyanovich Associate Professor, Department of Computer Science and Engineering, New York University
- 9. Lisa Rice President & CEO, National Fair Housing Alliance
- 10. Margaret Mitchell Chief Ethics Scientist, Hugging Face
- 11. Prem Natarajan Chief Scientist, Capital One
- 12. **<u>Reggie Townsend</u>** Vice President of Data Ethics, SAS
- 13. Seth Hain Vice President of R&D, Epic
- 14. Surya Mattu Co-Founder & Lead, Digital Witness Lab at Princeton University
- 15. Tulsee Doshi Head of Product, Responsible AI, Google
- 16. Yvette Badu-Nimako Vice President of Policy, Urban League

November 8, 2023

ELECTIONS AND DEMOCRACY

- 1. Alex Stamos Former Director, Stanford Internet Observatory
- 2. Amy Cohen Executive Director, National Association of State Election Directors
- 3. Andy Parsons Senior Director of the Content Authenticity Initiative, Adobe Inc.
- 4. Ari Cohn Free Speech Counsel, TechFreedom
- 5. Ben Ginsberg Volker Distinguished Visiting Fellow, The Hoover Institution
- <u>Damon Hewitt</u> President and Executive Director, Lawyers' Committee for Civil Rights Under Law
- 7. Dave Vorhaus Director for Global Election Integrity, Google
- 8. Deidre Henderson Lieutenant Governor, State of Utah
- 9. Jennifer Huddleston Technology Policy Research Fellow, Cato Institute
- 10. Jessica Brandt Former Policy Director for AI and Emerging Technology, Brookings Institution
- 11. Jocelyn Benson Secretary of State, State of Michigan
- 12. Kara Frederick Director of Tech Policy Center, The Heritage Foundation
- Lawrence Norden Senior Director of Elections & Government, Brennan Center for Justice at New York University
- 14. Matt Masterson Director of Information Integrity, Microsoft
- 15. Melanie Campbell President and CEO, National Coalition on Black Civic Participation
- 16. Michael Chertoff Co-Founder and Executive Chairman, Chertoff Group
- 17. Neil Potts Public Policy Director, Facebook
- 18. Yael Eisenstat Former Vice-President, Anti-Defamation League

PRIVACY AND LIABILITY

- 1. Arthur Evans Jr. CEO and Executive Vice President, American Psychological Association
- 2. Bernard Kim CEO, Match Group
- 3. Chris Lewis President and CEO, Public Knowledge
- 4. Daniel Castro Director and Vice President, Center for Data Innovation
- 5. Ganesh Sitaraman Assistant Professor, Vanderbilt Law School
- 6. Gary Shapiro CEO, Consumer Technology Association
- 7. Mackenzie Arnold Head of Strategy, Legal Priorities Project
- 8. Mark Surman Executive Director, Mozilla
- 9. Mutale Nkonde CEO, AI For the People
- 10. Rashad Robinson President, Color of Change
- 11. Samir Jain Vice President of Policy, Center for Democracy and Technology
- 12. Sean Domnick President, American Association for Justice
- 13. Stuart Appelbaum President, Retail Wholesale and Department Store Union
- 14. Stuart Ingis Chairman, Venable
- 15. Tracy Pizzo Frey President, Common Sense Media
- 16. Zachary Lipton Chief Scientific Officer, Abridge

November 29, 2023

TRANSPARENCY, EXPLAINABILITY, INTELLECTUAL PROPERTY, AND COPYRIGHT

- 1. Ali Farhadi CEO, Allen Institute for Al
- 2. Andrew Trask Leader, OpenMined
- 3. Ben Brooks Head of Public Policy, Stability AI
- Ben Sheffner Senior Vice President & Associate General Counsel, Motion Picture Association
- 5. <u>Curtis LeGeyt</u> President & CEO, National Association of Broadcasters
- 6. Cynthia Rudin Earl D. McLean, Jr. Professor of Computer Science, Duke University
- 7. Danielle Coffey President & CEO, News Media Alliance
- 8. Dennis Kooker President of Global Digital Business & US Sales, Sony Music Entertainment
- 9. Duncan Crabtree-Ireland National Executive Director and Chief Negotiator, SAG-AFTRA
- 10. Jon Schleuss President, NewsGuild
- 11. <u>Mike Capps</u> Founder & Board Chair, Howso
- 12. Mounir Ibrahim Vice President of Public Affairs and Impact, Truepic
- 13. Navrina Singh Founder & CEO, Credo Al
- 14. <u>Nicol Turner Lee</u> Senior Fellow for Governance Studies & Director of the Center for Technology Innovation, Brookings
- 15. Rick Beato Producer & Owner, Black Dog Sound Studios
- 16. Riley McCormack President, CEO & Director, DigiMarc
- 17. <u>Vanessa Holtgrewe</u> Assistant Department Director of Motion Picture and Television Production, IATSE
- 18. Zach Graves Executive Director, Foundation for American Innovation
- 19. Ziad Sultan Vice President of Personalization, Spotify

December 6, 2023

SAFEGUARDING AGAINST AI RISKS

- 1. Aleksander Madry Head of Preparedness, OpenAl
- 2. Alexander Titus Principal Scientist, USC Information Science Institute
- 3. Amanda Ballantyne Director, AFL-CIO Technology Institute
- 4. Andrew Ng Managing General Partner, Al Fund
- 5. Hodan Omaar Senior Policy Analyst, Information Technology and Innovation Foundation
- Huey-Meei Chang Senior China Science & Technology Specialist, Georgetown's Center for Security and Emerging Technology
- 7. Janet Haven Executive Director, Data & Society
- 8. Jared Kaplan Co-Founder, Anthropic
- 9. Malo Bourgon CEO, Machine Intelligence Research Institute
- 10. Martin Casado General Partner, Andreessen Horowitz
- 11. Okezue Bell President, Fidutam

- 12. <u>Renée Cummings</u> Assistant Professor of the Practice in Data Science, University of Virginia
- 13. Robert Playter CEO, Boston Dynamics
- 14. Rocco Casagrande Executive Chairman, Gryphon Scientific
- 15. Stuart Russell Professor, U.C. Berkeley
- 16. Vijay Balasubramaniyan CEO & Co-Founder, Pindrop
- 17. Yoshua Bengio Professor, University of Montreal

NATIONAL SECURITY

- 1. Alex Karp CEO, Palantir
- 2. <u>Alex Wang</u> CEO & Founder, Scale Al
- <u>Anna Puglisi</u> Senior Fellow, Georgetown University Center for Security and Emerging Technology
- 4. <u>Bill Chappell</u> Vice President and CTO, Strategic Missions and Technologies, Microsoft
- 5. Brandon Tseng President & Co-Founder, Shield Al
- 6. Brian Schimpf CEO, Anduril
- 7. Charlie McMillan Former Director, Los Alamos National Laboratory
- 8. Devaki Raj Co-Founder, CrowdAl
- 9. Eric Fanning President & CEO, Aerospace Industries Association
- 10. Eric Schmidt Chair, Special Competitive Studies Project
- 11. <u>Faiza Patel</u> Senior Director of the Liberty and National Security Program, Brennan Center for Justice
- 12. <u>Greg Allen</u> Director of Wadhwani Center for Al and Advanced Technologies, Center for Strategic and International Studies
- 13. <u>Horacio Rozanski</u> CEO, Booz Allen Hamilton
- 14. Jack Shanahan Lieutenant General (USAF, Ret.), CNAS Technology & National Security Program
- 15. John Antal Author, Colonel (ret.)
- 16. Matthew Biggs President, International Federation of Professional and Technical Engineers
- 17. Michele Flournoy CEO & Co-Founder, Center for a New American Security
- Patrick Toomey Deputy Director of the National Security Project, American Civil Liberties Union
- 19. Rob Portman Former Senator & Co-Founder of Al Caucus
- 20. Scott Philips CTO, Vannevar Labs
- 21. Teresa Carlson President and CCO, Flexport

Summaries of the Al Insight Forums

Inaugural Forum (1st Forum)

The first forum gathered leading voices across multiple sectors, including AI industry executives, researchers, and civil rights and labor leaders, to discuss the significant implications of AI on the United States and the world. We discussed the many ways AI will impact critical areas such as the workforce, national security, elections, and healthcare, setting the stage for the detailed conversations that followed in the subsequent forums. All of the attendees agreed that there was an important role for government to play in fostering AI innovation while establishing appropriate guardrails.

Supporting U.S. Innovation in AI (2nd Forum)

The second forum focused on the need to strengthen AI innovation. Participants noted the need for robust, sustained federal investment in AI research and development funding. All of the attendees agreed that the federal government should invest in AI research and development at least at the levels recommended by the National Security Commission on AI (\$8 billion in Fiscal Year (FY) 2024, \$16 billion in FY 2025, and \$32 billion in FY 2026 and subsequent fiscal years). In addition to federal investment, participants highlighted the need to ensure the benefits of AI innovation reach underserved communities and communities not traditionally associated with the tech industry. Suggestions included boosting digital infrastructure; encouraging immigration of high-skilled science, technology, engineering, and math (STEM) talent; engaging workers in the research, development, and design processes; continuing to collect additional data; and avoiding regulatory roadblocks that could inadvertently compromise market competition.

AI and the Workforce (3rd Forum)

The third forum considered both the applications of, and risks from, AI to the workforce. Participants recognized that while AI has the potential to affect every sector of the workforce – including both blue collar and white-collar jobs – there is uncertainty in predicting the speed and scale of adoption of AI across different industries and the extent of AI's impact on the workforce. Despite that uncertainty, many participants emphasized the need for employers to start training their employees to use this technology. Some participants noted that, to maximize the benefits of AI in the workforce, workers should be consulted when deploying this technology in the workplace. Some participants noted that AI can help workers become more efficient, requiring industries to prepare and train employees with skills to use the technology.

High Impact Uses of AI (4th Forum)

The fourth forum examined specific high impact areas where AI might be used, including financial services, health care, housing, immigration, education, and criminal justice, among others. A number of participants testified that the effects of AI in these areas are not hypothetical, but are happening now, emphasizing the need to ensure AI developers and deployers are following existing laws and to consider where there might be gaps. Some participants noted that training AI systems on biased input data could lead to harmful biased outputs and suggested that high impact AI systems should be tested before they are deployed to detect potential civil rights and public safety impacts of those systems. Participants agreed that the use of AI in high impact areas presents both opportunities and challenges and that policymakers should protect and support U.S. innovation. They also emphasized that transparency and engagement from diverse stakeholders must be prioritized when deploying AI in these high impact areas.

Elections and Democracy (5th Forum)

The fifth forum analyzed the impact of AI on elections and democracy. Participants agreed that AI could have a significant impact on our democratic institutions. Participants shared examples demonstrating how AI can be used to influence the electorate, including through deepfakes and chatbots, by amplifying disinformation and eroding trust. Participants also noted how AI could improve trust in government if used to improve government services, responsiveness, and accessibility. Participants proposed a number of solutions that could be employed to mitigate harms and maximize benefits, including watermarking AI-generated or AI-augmented content, voter education about content provenance, and the use of other AI applications to bolster the election administration process. Some participants indicated state and local elections with less media attention might be the biggest potential targets of AI disinformation campaigns, as well as the biggest benefactors from proper safeguards.

Privacy and Liability (6th Forum)

The sixth forum explored how to maximize the benefits of AI while protecting Americans' privacy and the issue of liability as it related to the deployment and use of AI systems. Participants shared examples of how AI and data are inextricably linked, from relying on vast amounts of data to train AI algorithms to the use of AI in social media and advertising. Some participants noted that a national standard for data privacy protections would provide legal certainty for AI developers and protection for consumers. Participants observed that the "black box" nature of some AI algorithms, and the layered developer-deployer structure of many AI products, along with the lack of legal clarity, might make it difficult to assign liability for any harms. There was also agreement that the intersection of AI, privacy, and our social world is an area that deserves more study.

Transparency, Explainability, Intellectual Property, and Copyright (7th Forum)

The seventh forum focused on four critical components in the development and deployment of AI: transparency, explainability, intellectual property (IP), and copyright. Many participants noted that transparency during the development, training, and deployment, and regulation of AI systems would enable effective oversight and helps to mitigate potential harms. The use of watermarking and content provenance technologies to distinguish content with and without AI manipulation were discussed at length. Participants also discussed the importance of explainability in AI systems and their view that users should be able to understand the outputs of why AI systems and how those outputs are reached in order to use those outputs reliably. Some participants noted that there is a role for the federal government to play in protecting American companies' and individuals' IP while supporting innovation. Participants shared stories about creators struggling to maintain their identities and brands in the age of AI as unauthorized digital replicas become more prevalent. Participants agreed that the United States will play a key role in charting an appropriate course on the application of copyright law to AI.

Safeguarding Against Al Risks (8th Forum)

The eighth forum examined the potential long-term risks of AI and how best to encourage development of AI systems that align with democratic values and prevent doomsday scenarios. Participants varied substantially in their level of concern about catastrophic and existential risks of AI systems, with some participants very optimistic about the future of AI and other participants quite concerned about the possibilities for AI systems to cause severe harm. Participants also agreed there is a need for additional research, including standard baselines for risk assessment, to better contextualize the potential risks of highly capable AI systems. Several participants raised the need to continue focusing on the existing and short-term harms of AI and highlighted how focusing on short-term issues will provide better standing and infrastructure to address long-term issues. Overall, the participants mostly agreed that more research and collaboration are necessary to manage risk and maximize opportunities.

National Security (9th Forum)

The ninth forum focused on the crucial area of national security. Participants agreed that it is critical for the U.S. to remain ahead of adversaries when it comes to AI. To maintain a competitive edge, participants agreed that it would require robust investments from the U.S. in AI research, development, and deployment. From gaining intelligence insights to supercharging cyber capabilities and maximizing the efficiency of drones and fighter jets, participants highlighted how the U.S. can foster innovation in AI within our defense industrial base. Participants raised awareness about countries like China that are heavily investing in commercial AI and aggressively pursuing advances in AI capacity and resources. In order to ensure that our adversaries don't write the rules of the road for AI, participants reinforced the need to ensure the DOD has sufficient access to AI capabilities and takes full advantage of its potential.

