HARVARD Kennedy School
ASH CENTER
for Democratic Governance and Innovation
Allen Lab for Democracy Renovation

GETTING-Plurality Research Network
Allen Lab for Democracy Renovation
Ash Center for Democratic Governance and Innovation
Harvard Kennedy School
124 Mount Auburn Street, Suite 200-North
Cambridge, MA 02138

GETTING-Plurality Research Network Response to the White House OSTP Request for Information on the Development of an Artificial Intelligence Action Plan

The GETTING-Plurality Research Network appreciates the opportunity to provide feedback on the development of an artificial intelligence action plan. We have compiled comments below from members of our research community including Sarah Hubbard, Shlomit Wagman, Allison Stanger, and others from the GETTING-Plurality Research Network.

This document is approved for public dissemination. The document contains no business-proprietary or confidential information. Document contents may be reused by the government in developing the AI Action Plan and associated documents without attribution.

We appreciate OSTP's commitment to American global leadership in AI, and for their efforts to prioritize policy actions in this space. The Trump Administration made important progress in the first term by pursuing a U.S. national AI strategy, particularly with the February 2019 Executive Order on Maintaining American Leadership in Artificial Intelligence which contained critical actions related to: Investing in AI Research and Development; Unleashing AI Resources; Setting AI Governance Standards; Building the AI Workforce; and International Engagement and Protecting our AI Advantage. We hope for the continuation of many of these important initiatives in the second term, with renewed focus on addressing the transformative potential of AI, while safeguarding American values and security interests.

Below, we offer a few suggestions for your consideration which we believe will continue to build on the Administration's first term efforts, while adapting to the moment of rapid technological advances in AI which we are facing today.

Invest in Public AI Infrastructure

Investing in robust public AI infrastructure is a national security imperative for the United States. As outlined in our work on The National Security Case for Public AI, publicly-owned AI tech

stack components (e.g. compute resources) would create a more resilient, innovative ecosystem while reducing dependence on a few private firms. It is critical for the U.S. to remain on the cutting edge of AI innovation in our global competition with China, so we can ensure that AI development is oriented towards democracy-, privacy-, and rights-protecting values. This investment will help ensure government independence from market actors with potentially conflicting interests, democratically accountable deployment, and will address other public goods traditionally underserved by corporate actors. We envision this infrastructure as a complement to private sector developments that could improve American democracy, national defense, and benefit the American people in their daily lives.

Ensure Technical Leadership and International Collaboration

As directed in the Administration's 2019 Executive Order, the National Institute of Standards and Technology (NIST) should continue to lead in the development of appropriate technical standards. The work of the U.S. AI Safety Institute, within NIST, over the past few years has been an incredibly effective hub for bringing together U.S. AI companies, academia, and government on advancing standards and guidance for accelerating trustworthy AI innovation. We recommend:

- Maintain NIST U.S. AI Safety Institute Efforts: This body has brought technical leadership and talent into the federal government, and created important relationships domestically and internationally with the network of other similar institutes established around the world.
- Build Technical Capacity in Government: Along with the continuity of this body within NIST, we believe it is critical to continue to bring multi-disciplinary experts on AI into the federal government, so America has the expertise to analyze and assess the risks (e.g. misuses, vulnerabilities) and powerful opportunities new AI models present.
- Promote a Free and Fair Market for Tech Contracting: The government's tech needs should continue to be served by multiple companies to minimize the potential for the abuse of power and privacy violations.

Manage National Security Threats Posed by AI

The rapid advances in AI present profound national security risks, particularly as adversarial actors exploit its capabilities to destabilize societies, fuel cybercrime, disrupt public order, and undermine democratic institutions. AI has dramatically lowered barriers to cyberattacks, deepfake-driven manipulation, misinformation campaigns, large-scale fraud, and social engineering, creating new challenges for governments and private sector stakeholders in mitigating these threats. Some of these threats include:

- AI as a Tool for Terror and Psychological Warfare: The weaponization of AI for terror and psychological operations presents a serious national security risk. AI-driven misinformation and deepfake campaigns can be used to fabricate false diplomatic crises, provoke international conflicts, or incite large-scale panic among civilian populations.

Moreover, AI-optimized psychological operations enable adversarial actors to exploit political and social divisions, radicalizing individuals through hyper-personalized content and inciting civil unrest.

- Large-Scale AI-Powered Cybercrime & Financial Fraud: AI has dramatically scaled and enhanced cybercrime, particularly in fraud, identity theft, and financial crime. Social engineering scams, once reliant on human deception, are now fully automated, hyper-personalized, and deployed at scale. The rise of FraudGPT and other malicious AI tools has further enabled cybercriminals to generate fake documents, manipulate biometric authentication systems, and circumvent KYC (Know Your Customer) and AML (Anti-Money Laundering) regulations.
- AI in the Development of Unconventional Weapons & Cyber Threats: AI is increasingly being used to identify and exploit security vulnerabilities in defense systems, corporate networks, and critical infrastructure. By automating cyber reconnaissance and penetration testing, AI can enable adversarial actors to execute highly adaptive, autonomous cyberattacks at speeds far beyond human capabilities. These AI-driven attacks could disable military communications, manipulate satellite systems, or disrupt power grids, posing direct threats to national security. Beyond cyber threats, AI lowers barriers for the development of nuclear and bioweapons, automated hacking tools, and AI-optimized malware, allowing hostile nations and terrorist groups to build unconventional weapons with minimal resources.
- Election Interference & the Manipulation of Democratic Processes: The ability of AI to manipulate political discourse and democratic institutions is a growing threat to global stability. AI-generated misinformation and deepfake technology can fabricate political scandals, alter public records, and misrepresent candidates, misleading voters and eroding trust in electoral processes. These AI-driven disinformation campaigns not only influence election outcomes but also weaken democratic resilience by sowing distrust in legitimate institutions. Without intervention, AI's ability to manufacture consensus and manipulate voting behavior will pose an existential challenge to free societies and national security.

In order to address some of these threats, there is an urgent need to mitigate risks associated with AI misuse while promoting innovation. Some of the recommendations for managing these risks include:

- International Governance and Standards: AI threats transcend national borders, and without global coordination, we risk a race to the bottom in safety and security standards. The U.S. should spearhead efforts to ensure that governments and private sector actors globally align on shared principles and enforceable safeguards. One of the most effective models for such coordination is the Financial Action Task Force (FATF), which sets mandatory global standards for financial integrity and compliance by both governments and private sector. A similar approach could be applied to AI governance, requiring: baseline global standards for safe AI development; integration of AI safety measures into

national policies across jurisdictions; independent expert evaluations and audits to assess adherence; consistent obligations for the private sector worldwide, preventing regulatory arbitrage; regular reporting and enforcement mechanisms to ensure compliance. Without such a framework, AI safety efforts will remain fragmented, leaving gaps that adversarial actors will exploit.

- Market Incentives for AI Security: While billions of dollars have been invested in AI development, AI security remains relatively underfunded. Policymakers should incentivize investment in AI security solutions and protocols to keep pace with technological advancements. This includes:
    - Financial and operational incentives for companies developing AI security and safety tools (e.g., AI-driven fraud detection, deepfake authentication, and cybersecurity tools).
    - Public-private partnerships to accelerate research and deployment of AI adversarial defense mechanisms.
    - Developers should be encouraged, and in some cases required, to integrate risk assessments and adversarial testing for high-risk AI applications, and adopt defensive AI mechanisms that detect and mitigate adversarial manipulation.
- Public Awareness: Public education is critical to building resilience against AI-driven threats, including misinformation, fraud, and cyber-enabled social engineering. Governments, industry, and academia should:
    - Raise awareness of AI risks, particularly in election interference, deepfakes and impersonation, and financial crime.
    - Promote digital competence and responsible AI use, ensuring the public understands how to identify and respond to AI-generated deception.
    - Encourage transparency in AI development and deployment, including better authentication and tracking of AI-generated content.
- Regulation: Consider whether a regulatory framework is necessary to enhance the above recommendations, recognizing that certain AI risks - such as national security threats, cybercrime, and threats to democratic values - may not be adequately addressed by the private sector on a voluntary basis. As noted, establishing a global framework and enforceable standards is highly recommended to ensure consistent implementation across jurisdictions, prevent regulatory gaps, and promote fair competition. This approach would help align stakeholders worldwide, ensuring AI safety measures are adopted broadly while supporting responsible innovation.

Implement Standards for AI Usage in Government Operations

As AI becomes an integral part of government operations, clear policies and guidelines must be in place to ensure secure, fair, and responsible use. AI systems used in government must prioritize data protection, transparency, explainability, and accountability, while ensuring human oversight in decision-making. In order to maintain public trust while leveraging AI, we recommend:

- Adopt Policies for Government Use: Prohibit the use of confidential, classified, or personal data in commercial AI models, unless appropriate data protection arrangements are in place (e.g., sensitive data is not used to train a commercial model), to prevent security and privacy risks. Mandate transparency and explainability, ensuring AI decisions are traceable and justifiable to the public. AI use must be auditable, with clear records of how AI-assisted decisions are made, enabling oversight and accountability. Ensure explainability of AI outcomes, allowing public officials to assess fairness and accuracy. Agencies should track and log AI-generated decisions and regularly address AI's impact on decision-making to adjust policies as necessary.
- Training for Government Employees: AI training for government officials is essential to enable the use of AI tools responsibly and securely. Proper training will equip civil servants to leverage AI-powered tools to improve decision-making, streamline operations, and enhance service delivery, while following data protection protocols, privacy and security laws. Officials should be familiar with best practices in AI deployment, risk mitigation, and ethical considerations, including privacy protection, cybersecurity, and bias detection. Additionally, learning from private sector AI adoption will help governments harness innovation effectively, ensuring public institutions remain adaptive, data-driven, and capable of leveraging AI's full potential while safeguarding public trust.

Prepare the American Workforce

AI will continue to play a prominent role in the U.S. economy, and as these technologies continue to improve, we must prepare the American workforce for the implications. A recent report from Pew Research shows that "workers are more worried than hopeful about future AI use in the workplace"[1] and a recent study from Microsoft and Carnegie Mellon demonstrated that the rise of generative AI in knowledge work is negatively impacting workers critical thinking skills and practices.[2] We expect that AI will have a significant destabilizing and transformative impact on workers, their families, and communities. We must figure out how to plan for these changes, to equip young people, and to harness innovation for individual and collective good.

- Engage with Civil Society: It is increasingly important to engage with civil society to understand and mitigate the impacts felt at home from the global race for AI dominance.
- Expectations for National Service: There is an urgent need for colleges and universities with high levels of graduates in technical fields to build an expectation for graduates of national service at some point in their careers. America needs talent in the public workforce with the technical capabilities to keep pace with AI (e.g. to evaluate models). In parallel, many American workers will be displaced by AI. A government works

[1] https://www.pewresearch.org/social-trends/2025/02/25/u-s-workers-are-more-worried-than-hopeful-about-future-ai-use-in-the-workplace/

[2] https://www.microsoft.com/en-us/research/wp-content/uploads/2025/01/lee_2025_ai_critical_thinking_survey.pdf

program at the state and local level with well designed objectives could harness their talents in service of their country.

- Renew Civic Education: As AI becomes more prevalent, it is crucial to reinforce that American democratic values and practices–not algorithms–should guide our nation's decisions. Understanding the role of virtue and education in American self-governance is a prerequisite for sustaining the republic. So that citizens are equipped to engage in cross-ideological debate over shared technological futures, it is necessary to invest in digital competence and civic mindedness.
- Revitalize Higher Education. American universities must recommit to academic freedom and the rule of law so that learning and scientific discovery can flourish. Our university system has been the engine of American technological leadership, producing research breakthroughs which drive private and public sector advancements. To continue this legacy, we must ensure our educational institutions foster free inquiry and prepare students to succeed in an AI-transformed economy.

Invest in Research & Development

While there is often a focus on risk, we should also seek to ensure that new opportunities are seized. In some cases, there will be new opportunities for research and development, where commercialization is not the best vehicle for supporting development and scaling of novel technologies. We recommend the development of national research and development in areas such as: personalized education and vocational training; advances in drug development, cancer research, and other sciences; entrepreneurial opportunities; and increased opportunities to engage in our democratic system. Strategic government investment can complement private sector innovation to benefit the American people, while strengthening American leadership and economic growth.

About the GETTING-Plurality Research Network

Governance of Emerging Technology and Tech Innovations for Next-Gen Governance (GETTING-Plurality) is a multi-disciplinary research network linking philosophers, social scientists, computer scientists, legal scholars, and technologists. We are building a unique collaborative that unites technology and policy initiatives at Harvard University with external impact partners across higher education and the tech industry. More information: https://ash.harvard.edu/programs/getting-plurality/

For any additional information on the comments above, please reach out to Sarah Hubbard at sarah_hubbard@hks.harvard.edu.