ALERT MEMORANDUM

White House Releases Action Plan Outlining America's Path to Global AI Leadership

August 5, 2025

Last month, the White House released a report titled "Winning the Race: America's AI Action Plan" (the "Action Plan"), which builds on an executive order released by the Trump Administration in January. The Action Plan outlines three pillars: (1) accelerating AI innovation; (2) building American AI infrastructure; and (3) leading in international AI diplomacy and security. The Action Plan also sets forth three policy priorities underpinning those pillars. These priorities are creating opportunity for American workers, keeping AI systems free from ideological bias, and preventing advanced technology from being misused or stolen by malicious actors. In connection with the Action Plan, President Trump also signed three executive orders focused on promoting the export of the American AI technology stack, accelerating federal permitting of data center infrastructure, and preventing "woke AI" in the federal government. Additionally, the Action Plan previews a forthcoming National AI R&D Strategic Plan but does not give a timeline for its release. Overall, the Action Plan contains several policy recommendations, but it remains unclear how many of these will ultimately be implemented.

If you have any questions concerning this memorandum, please reach out to your regular firm contact or the following authors:

SILICON VALLEY

Angela L. Dunning
+1 650 815 4131
adunning@cgsh.com

NEW YORK

Daniel Ilan
+1 212 225 2415
dilan@cgsh.com

LONDON

Gareth Kristensen
+44 20 7614 2381
gkristensen@cgsh.com

SAN FRANCISCO

Marcela Robledo
+1 415 796 4450
mrobledo@cgsh.com

Acceleration of AI Innovation

Removing rules that "unnecessarily hinder AI development or deployment." The Action Plan is largely focused on the first pillar, acceleration of AI innovation, and includes a wide range of related policy recommendations. In particular, the Trump Administration is focused on the removal of red tape and regulations, noting that "AI is far too important to smother in bureaucracy at this early stage, whether at the state or Federal level." The Action Plan contains several recommended policy actions to further this goal, including having the Office of Management and Budget ("OMB") work with federal agencies to identify, revise, or repeal rules, regulations, guidance documents, policy statements, and other federal documents that unnecessarily hinder AI development or deployment. OMB is also encouraged to work with federal agencies that have AI-related discretionary funding to ensure they "consider a state's AI regulatory climate when making funding decisions and limit funding if the state's AI regulatory regime may hinder the effectiveness of that funding or award," suggesting that states with AI-specific laws in place (including California, Utah, Colorado, and Texas) may be under increased scrutiny.

The Action Plan also recommends that the Office of Science and Technology Policy ("OSTP") put forward a Request for Information from businesses and the public regarding current federal regulations that hinder AI innovation and adoption. Additionally, the Action Plan recommends reviewing Federal Trade Commission actions commenced under the previous administration to ensure they do not advance theories of liability that unduly burden AI innovation.

Ensuring that frontier AI "protects free speech." Another priority of the Trump Administration is ensuring that frontier AI protects free speech. The Action Plan recommends that the Department of Commerce and the National Institute of Standards and Technology ("NIST") revise the NIST AI Risk Management Framework to eliminate references to misinformation; Diversity, Equity, and Inclusion; and climate change. It also indicates that the federal procurement guidelines will be updated to ensure that the government only contracts with developers of large language models (LLMs) who ensure their systems are "objective and free from top-down ideological bias." This standard may be challenging for developers to meet, given that LLMs are trained on (and thus learn from) human-generated content, which may contain inherent human biases (whether ideological or otherwise). An accompanying executive order directs OMB to issue guidance to federal agencies within 120 days, advancing the government's policy of procuring LLMs developed in accordance with the principles of truth-seeking and ideological neutrality (formally called the "Unbiased AI Principles.") Within 90 days of such guidance, agency heads are directed to adopt procedures to ensure that LLMs procured by their agency comply with the Unbiased AI Principles.

Open sourcing. Encouraging open-source and open-weight AI models is another priority in the Action Plan. Some AI models have been made freely available by developers for researchers, businesses, and the public to download and modify. According to the Action Plan, this will spur innovation because startups can use them without being dependent on a closed model provider. Additionally, commercial and government adoption of AI may benefit "because many businesses and governments have sensitive data that they cannot send to closed model vendors." The Action Plan does not, however, address potential risks that may be associated with relying on open source and open weight AI or the specific terms that would or should govern use of any particular model.

AI adoption. The Action Plan criticizes the slow adoption of AI, particularly in established and larger organizations, and notes that certain critical sectors, including healthcare, have been "especially slow." To address this issue, the Action Plan recommends a coordinated federal effort to promote a "try-first" culture for AI, including potential domain-specific efforts in the healthcare, energy, and agriculture sectors. As expected, AI adoption by the federal government to improve efficiency is also a key priority. This will include formalizing the Chief Artificial Intelligence Officer Council as the primary

venue for coordination on AI adoption across government agencies. Adoption of AI within the Department of Defense is also highlighted in the Action Plan.

AI-enabled science. Another focus of the Action Plan is AI-enabled science, which corresponds with other goals of building world-class scientific datasets and advancing the science of AI. One notable policy recommendation would require federally funded researchers to disclose non-proprietary, non-sensitive datasets used by AI models for research and experimentation. However, the Action Plan does not explain how determinations will be made regarding which datasets are proprietary or sensitive.

Copyright enforcement and fair use. The Action Plan and related executive orders do not address the question of whether AI developers should be liable for copyright infringement or benefit from the "fair use" defense when they use copyrighted content to train their models without authorization. Nor does the Action Plan reference any initiatives to evaluate potential changes to copyright law. Issues of copyright infringement liability, fair use, and ownership over outputs created using AI tools are being actively litigated in U.S. courts under the existing framework established by the U.S. Copyright Act and cases interpreting it.

Deep fakes and other challenges. Despite championing acceleration and criticizing the slow adoption of AI, the Action Plan also acknowledges certain drawbacks to the rapid expansion of AI, including the potential use of deepfakes. On this point, the Action Plan recommends that the Department of Justice's Office of Legal Policy file formal comments on deepfake-related additions to the Federal Rules of Evidence. The Action Plan also addresses certain challenges with AI systems as they exist today, particularly how the workings of such systems are "poorly understood," observing that the inability to explain why a model produced a certain output makes it difficult to predict an AI system's behavior. This makes it hard to deploy AI in sensitive sectors like defense and national security. AI interpretability, control, and robustness will be part of a forthcoming National AI R&D Strategic Plan. Establishment of better AI evaluation and assessment tools is also a priority.

Building American AI Infrastructure

The second pillar focuses on the need for modernized American infrastructure and a skilled workforce to support the country's ambitious AI goals. This includes streamlined approvals for data centers, semiconductor manufacturing, and energy infrastructure and a recommendation that federal lands be made available for the construction of data centers and power generating infrastructure. The Action Plan also discusses returning semiconductor manufacturing to the U.S, as well as building high security data centers for use by the military and intelligence communities. An accompanying executive order addresses accelerating permitting for data center infrastructure through several measures. Among those measures, the order directs the Secretary of Commerce to launch an initiative to provide financial support for various data center related projects. The Administrator of the Environmental Protection Agency is also directed to assist in expediting permitting on federal and non-federal lands by developing or modifying regulations promulgated under the Clean Air Act and other statutes.

A significant portion of the second pillar focuses on cybersecurity of AI tools and adversarial threats to AI infrastructure. The Action Plan recommends establishing an AI Information Sharing and Analysis Center led by the Department of Homeland Security ("DHS") to promote the sharing of AI-security threat information across critical infrastructure sectors. DHS would also issue and maintain guidance to private sector entities on remediating and responding to AI-specific vulnerabilities and threats. The government would share known AI vulnerabilities with the private sector, as appropriate, leveraging existing mechanisms for the sharing of information regarding cybersecurity vulnerabilities. The Action Plan also briefly discusses security by design for AI technologies and recommends that the Department of Defense continue

to refine its Responsible AI and Generative AI Frameworks, Roadmaps, and Toolkits.

In addition to cybersecurity, AI-related incident response is also a priority. The Action Plan recommends that NIST partner with the AI and cybersecurity industry to ensure AI is included in incident response standards and frameworks, and that the Cybersecurity and Infrastructure Security Agency modify its Cybersecurity Incident & Vulnerability Response Playbooks to includes considerations for AI systems. While it is not clear when to expect new NIST guidelines, companies should continue to adjust their incident response and business continuity plans for AI risk scenarios as part of their overall AI governance programs.

Leading in International AI Diplomacy and Security

In the third pillar, the Action Plan encourages exporting the full U.S. AI technology stack (including hardware, models, software, applications, and standards) "to all countries willing to join America's AI alliance," with the Departments of State and Commerce facilitating deals. An accompanying executive order directs the Secretary of Commerce, in consultation with the Secretary of State and the Director of the OSTP, within 90 days, to establish and implement the American AI Exports Program to support the development and deployment of U.S. full-stack AI export packages. The Secretary of Commerce will also issue a public call for proposals from industry-led consortia.

Export control is also a priority of the third pillar of the Action Plan. One recommended policy action includes having the Department of Commerce develop new export controls for semiconductor manufacturing sub-systems. Alignment with allies on global protection measures is also a priority.

The Action Plan also calls for additional evaluation of cybersecurity risks and investment in biosecurity, noting the potential for "novel national security risks in the near future." Here, the government recommends evaluating frontier AI systems for national security risks in partnership with AI developers. For increased biosecurity, the Action Plan recommends requiring all institutions receiving federal funding for scientific research to use nucleic acid synthesis tools and synthesis providers that have robust nucleic acid sequence screening and customer verification procedures. It also recommends convening government and industry stakeholders to develop a mechanism to facilitate data sharing between nucleic acid synthesis providers to screen for potentially fraudulent or malicious customers. These measures are intended to protect against biothreats by malicious actors.

Conclusion

While the Action Plan is generally aimed at federal preparedness, it is also designed to accelerate AI development and adoption of AI by the private sector. The Action Plan appears very positive for AI developers as the federal government aims to roll back rules, regulations, and guidance that, in its view, may hinder development and deployment. It also promotes building AI platforms on open-source and open-weight foundation models which will accelerate, and decrease the cost of, AI development and deployment.

Although these objectives are beneficial to developers, the Action Plan does not detail many specifics on how some goals will be advanced and does not address some of the risks posed by accelerated AI development. For example, promoting open-source and open-weight foundation models can increase the risk that bad actors will more easily access sophisticated models for bad intents (such as deep fakes or building weapons); and while emphasizing the importance of private sector defense of AI innovation against security risks, the Action Plan lacks specifics of how these security goals should be advanced in practice.

More generally, it remains to be seen whether implementation of the Action Plan and executive orders will be primarily focused on the goal of "winning the AI race" or will also include measures to address potential risks associated with unregulated AI

development and use, including in the context of agentic AI.

Takeaways

The Action Plan exemplifies the Trump Administration's focus on AI growth and development, and companies should take notice. In the absence of more concrete guidance and rules, companies should continue to do the following:

— Monitor for new government AI standards and frameworks;

— Prioritize strong AI governance programs as AI pilots are rolled out and ultimately integrated into day-to-day operations;

— Consider security-related risks and risks to confidential and proprietary information associated with the use of open-source AI models, and

— Ensure contracts with third-party vendors address AI-related security risks.

…

CLEARY GOTTLIEB