ALERT MEMORANDUM

White House Unveils Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence

November 15, 2023

On October 30, 2023, the Biden Administration issued a landmark Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (the "Order"), directing the establishment of new standards for artificial intelligence ("AI") safety and security and laying the foundation to ensure the protection of Americans' privacy and civil rights, support for American workers, promotion of responsible innovation, competition and collaboration, while advancing America's role as a world leader with respect to AI.

Issued nearly one year after publication of the Biden Administration's AI Bill of Rights, the Order tasks a number of federal departments and agencies with the responsibility of generating, implementing and/or overseeing standards and guidance with respect to AI-related risks. Deviating from the approach adopted under the G7 AI Code of Conduct (discussed here), which sets out voluntary guidance for the development and use of advanced AI systems by the private sector, the Order contains a limited set of requirements applicable to private enterprises and directs most of its mandates to federal agencies.

In addition to the Order's enhancement of current federal agency obligations to oversee and implement responsible uses of AI, the Order establishes a new White House AI Council, comprised of the heads of a number of federal agencies and executive offices, which will be responsible for coordinating the activities of federal agencies to ensure the effective formulation, development, communication, and timely implementation of AI-related policies, while ensuring appropriate industry engagement.

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

New York

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

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

Angela Dunning
+1 680 815 4131
adunning@cgsh.com

Brendan J. Cohen
+1 212 225 2443
bcohen@cgsh.com

The scope of the Order is sweeping, seeking to address all currently imaginable harms or misuses of AI, identify opportunities for potential growth or engagement, and devise a framework for the federal government to take action to regulate public and private sector use and development of AI systems. With staggered timelines for implementation, the Order's anticipated impacts and overall effectiveness will not be realized for some time. Entities engaging with AI systems—whether as developers or users of AI tools—should stay abreast of rulemaking activities as the resulting guidance is likely to build the architecture for best practices in AI development, deployment and implementation for years to come.

Guiding Policies and Principles

To protect Americans from the growing potential risks of AI systems, the Order sets forth eight guiding principles applicable to the AI-related activities of federal agencies to advance and govern the development and use of AI technologies. The Order places special focus on industries where infrastructure is provided as a service (IaaS), focusing on the susceptibility of AI-enabled IaaS to be used in malicious cyber-enabled activity, complementing the guidelines provided in prior Executive Order 13984 of January 19, 2021.

A. Ensuring the Safety and Security of AI Technology

In the most sweeping set of obligations set forth under the Order, federal agencies and departments, such as the Secretary of Commerce, Departments of Energy and Homeland Security, the Office of Management and Budget and the National Institute of Standards and Technology ("NIST") amongst others, are directed to develop standards for AI safety, security and reliability throughout the AI lifecycle. At a high level, the Order:

- Instructs federal agencies to promulgate guidelines for public, (and in more limited circumstances, private) enterprises, including obligations on NIST to establish standards for extensive red-team testing[i] of AI systems (particularly dual-use foundation models[ii]), which the Departments of Energy and Homeland Security are further instructed to apply to critical infrastructure to address chemical, biological, radiological, nuclear and cybersecurity risks;
- Imposes requirements applicable to AI developers that create foundation models that pose serious risks to national security, national economic security or national public health and safety, requiring notification to the federal government when training the model, and mandating sharing the results of all red-team safety testing;
- Provides for formulation of strong standards for biological synthesis screening to thwart the risks of using AI to engineer dangerous biological materials;
- Requires implementation of guidance and tools for content authentication and watermarking to clearly label AI-generated content to protect against AI-enabled fraud and deception; and
- Building upon the Administration's ongoing AI Cyber Challenges, requires establishment of an advanced cybersecurity program to develop AI tools to find and fix vulnerabilities in critical software.

B. Promoting Innovation and Competition

To secure America's leadership in the field of AI innovation, the Order:

- Sets forth a number of initiatives to promote AI research; foster a fair and competitive AI ecosystem; expand the ability of AI experts from around the world to study, stay and work in the United States and clarify intellectual property issues of authorship and inventorship related to AI.
- Directs federal agencies to launch a pilot of the National AI Research Resource, a tool that will provide the research community with key AI resources and data, and to

expand grants for AI research in areas such as healthcare and climate change.

With rising concern about the potential for market consolidation in this area, the Order also instructs the federal agencies that are developing AI-related policies and regulations to promote fair competition in the AI market. In particular, the Order calls on the Federal Trade Commission ("FTC") to consider whether to exercise its existing authority, including under the FTC Act, "to ensure fair competition in the AI marketplace and to ensure that consumers and workers are protected from harms that may be enabled by the use of AI." The Order also directs the Secretaries of State and Homeland Security to implement changes to the visa process to attract foreign AI talent. While the Order does not itself resolve the intellectual property issues involving AI, it sets the stage for future guidance and executive actions by (i) instructing the Director of the U.S. Patent and Trademark Office to publish guidance addressing inventorship and the use of AI in the inventive process, (ii) directing the U.S. Copyright Office to issue recommendations to the President on potential executive actions related to copyright and AI and (iii) directing the Departments of Homeland Security and Justice to develop a training, analysis and evaluation program to mitigate AI-related intellectual property risks.

C. Supporting Workers

Given the myriad ways in which AI promises to revolutionize the labor market, the Order sets forth measures to mitigate the risks of workplace surveillance, bias and job displacement, and to support workers' ability to bargain collectively and invest in accessible workforce training and development. In particular, the Order directs the Secretary of Labor to develop principles and guidance to prevent employers from undercompensating workers, evaluating job applications unfairly or impinging on workers' ability to organize. The Order also instructs the Chairman of the Council of Economic Advisers to submit to the President a report on the labor-market effects of AI. Finally, the Order asks the Secretary of Labor to identify options for strengthening federal support for workers who may be displaced by the adoption of AI and other technological advancements.

D. Advancing Equity and Civil Rights

To mitigate the potential harms from irresponsible use of AI, particularly discrimination, bias and injustice, the Order seeks to provide guidelines across agencies to address and limit harmful algorithmic decision-making, and calls for clear guidance regarding the use of algorithms for housing, federal benefits programs and federal contractors, including in hiring and benefits administration. For law enforcement, the Order calls for increased information-sharing across relevant agencies, and law enforcement agencies are further directed to develop best practices for (i) investigating and prosecuting civil rights violations related to AI and (ii) the use of AI in sentencing, parole and probation, pretrial release and detention, risk assessments, surveillance, crime forecasting and predictive policing and forensic analysis.

E. Protecting Consumers, Patients, Passengers and Students

While AI promises many benefits to consumers, such as making products potentially better, less expensive and more widely available, the Order addresses the risks that AI poses to patients, students and other individuals, including the possibility that its use may injure, mislead or otherwise be harmful. The Order:

- Encourages independent regulatory agencies to ensure that existing laws and principles are applied to AI and to consider using each agency's rulemaking authorities to enact new protections against fraud, discrimination, threats to privacy and financial stability and other AI-related harms;
- Directs the Department of Health and Human Services to establish a safety program to receive reports of, and act to remedy, harms or unsafe healthcare practices involving AI; and
- Instructs the Secretary of Education to develop policies that address the safe,

responsible and nondiscriminatory uses of AI in education and provide an "AI toolkit" for education leaders.

F. Protecting Privacy

To mitigate the privacy risks exacerbated by the use of AI systems, particularly in light of the growing dependence of such systems to exploit private and personally identifiable data for training purposes, the Order sets forth a number of evaluation, rulemaking and research initiatives to encourage adoption of privacy-enhancing technologies ("PETs")[iii] by federal agencies. Specifically, the Order requires varying agency heads to (i) reevaluate and strengthen privacy guidance with respect to the government's collection and use of commercially available information (in particular where such information includes personally identifiable information) to ensure it is lawful and secure, (ii) prioritize federal support for accelerating the development and use of PETs including to strengthen privacy-preserving research and opportunities, such as the use of cryptographic tools, related thereto and (iii) develop and renew guidelines for federal agencies to evaluate the effectiveness of PETs.

Absent from the Order are any transparency mandates, including obligations to notify individuals of, or to receive consent regarding, the use of their personally identifiable information in connection with the training or development of AI systems—obligations that have been at the forefront of Federal Trade Commission enforcement activities with respect to AI, and proliferated by state privacy legislation that has come into effect over the last few years—perhaps because the President seeks to leave that regulation to Congress or the states. Notably, in a Fact Sheet published alongside the Order, the President sends a clear directive to Congress to "pass bipartisan data privacy legislation to protect all Americans, especially kids."

G. Advancing Federal Government Use of AI

Recognizing the power of AI as a tool when used responsibly, the Order:

- Articulates the federal government's desire to use AI to build agencies' capacities to regulate, govern and disburse benefits, to reduce operation costs and increase the security of government systems;
- Calls for clear standards designed for agencies introducing AI, with the goal of protecting the rights of citizens, improving AI procurement and strengthening AI deployment;
- Directs relevant agencies to contract with private AI developers rapidly and efficiently to deploy AI-based solutions, particularly generative AI products and services; and
- Instructs relevant agencies to prepare for rapid hiring and training of AI professionals.

H. Strengthening American Leadership Abroad

Because of the global nature of AI, the Order emphasizes the Biden Administration's desire to continue working with other nations to support the safe, secure and reliable use of AI worldwide. To that end, the Order directs the State Department, in collaboration with the Commerce Department, to establish robust international frameworks for managing and implementing AI safely, including considerations of expanding bilateral, multilateral and multistakeholder engagements.

In addition to risk mitigation, the Order envisions an increased use of AI to promote rights-affirming development and help solve global challenges—specifically, sustainable development and mitigating danger to critical infrastructure—and imagines the United States and its international partners working with other organizations to accelerate the development of AI and implementation of related AI standards to ensure that the technology is safe, secure, trustworthy and interoperable.

…

CLEARY GOTTLIEB

[i] Under the Order, "red-teaming" refers to a structured testing effort to find flaws and vulnerabilities in an AI system, often in a controlled environment and in collaboration with developers of AI. AI red-teaming typically involves use of adversarial methods to identify flaws and vulnerabilities, such as harmful or discriminatory outputs from an AI system, unforeseen or undesirable system behaviors, limitations or potential risks associated with the misuse of the system.

[ii] The Order defines a "dual-use foundation model" generally to include any AI model that: (i) is trained on broad data, (ii) generally uses self-supervision, (iii) contains at least tens of billions of parameters, (iv) is applicable across a wide range of contexts and (v) exhibits, or could be easily modified to exhibit, high levels of performance at tasks that pose a serious risk to security, national economic security, national public health or safety or any combination thereof. Models meet this definition even if they are provided to end users with technical safeguards that attempt to prevent users from taking advantage of the relevant unsafe capabilities.

[iii] Under the Order, "privacy-enhancing technology" means "any software or hardware solution, technical process, technique, or other technological means of mitigating privacy risks arising from data processing, including by enhancing predictability, manageability, disassociability, storage, security and confidentiality. These technological means may include secure multiparty computation, homomorphic encryption, zero-knowledge proofs, federated learning, secure enclaves, differential privacy and synthetic-data-generation tools."