WILMERHALE

President Biden's Executive Order Sets Ambitious Agenda for AI Development and Use

NOVEMBER 6, 2023

Our initial thoughts on the Biden Executive Order first appeared on WilmerHale's Privacy and Cybersecurity Blog the day that the Executive Order was released.

On October 30, 2023, the Biden Administration issued its highly anticipated Executive Order on the Safe, Secure, Trustworthy Development and Use of Artificial Intelligence (Order). The Order provides a broad vision of the administration's legal, regulatory and policy approach to the development and implementation of artificial intelligence (AI) in the United States and attempts to set the tone for regulating the technology globally. Through the Order, the administration seeks to assert American leadership in an area where there is concern that the federal government's efforts are not keeping pace with the speed at which the technology is being adopted or regulated in other countries. The Order also makes clear the administration will require measures to ensure safe and responsible development and use of AI but that it will take an overall cautious approach to regulation in this area to ensure continued innovation and American competitiveness.

The Order provides a road map of some of the key issues that the administration has been focused on as it seeks to develop guardrails for the technology. Specifically, in a set of obligations imposed across the federal government, the Order directs action on new standards for AI safety and security, measures to protect Americans' privacy, consumer and the workforce, promotion of innovation and competition, advancement of American AI leadership abroad, and responsible and effective government use of AI.

The Order is ambitious—directing numerous federal agencies to take action on AI across a range of issues. Although most private entities will not be immediately affected by the Order, all businesses need to understand what the Order means about the administration's priorities as well as its future implications for industries and economic sectors.

We anticipate that this Order will have meaningful effects for our clients in the near and longer terms regardless of whether they are already an established AI player or are just now beginning to consider the potential for the technology in their day-to-day operations. We have lawyers with a broad range of expertise advising businesses of all sizes and across all industries on AI legal and regulatory strategy, compliance, risk and governance issues, and we are happy to help current and prospective clients understand and navigate the effects of the Order on their organizations.

Below are some of our key takeaways from the Order and considerations for organizations, followed by an overview of many of the actions required by the Order.

Key Takeaways

- The Order will increase pressure on Congress to pass legislation in the near term to address AI. Although it is unlikely that comprehensive AI legislation will be introduced anytime soon, we anticipate that we will very quickly start seeing more proposals aimed at specific issues or concerns highlighted by the Order. The Order also has the potential to refocus Congress on passing federal privacy legislation (either a "comprehensive" proposal or as one focused on children), given the privacy issues raised by AI and the relatively mature legislation that was being debated in Congress over the past several years.
- The Order should be of interest to organizations across a wide variety of industries, with heightened immediate importance to government contractors and large technology companies that are developing advanced AI systems. Virtually every federal agency is tasked with something under the Order, which means that companies need to understand how any agencies with regulatory authority over them are being tasked and what the relevant and likely outcomes of what any eventual agency action based on those tasks will be.
- Most of the Order is focused on future efforts by the federal government that are intended to shape standards, norms and legal requirements going forward. The Order requires numerous actions across the executive branch, including the development of guidance for federal government agencies' use of AI, standards for red-teaming models, and guidance for detecting AI-generated content and digital content authentication. Although these measures are only applicable to the public sector in the first instance, the ultimate effect on the private sector will be profound. It is critical that organizations pay close attention to how federal agencies approach the requirements of the Order and any standards, recommendations and reporting requirements as they are being developed, given the likelihood that many of the requirements will eventually flow down to the private sector as contracting requirements before being adopted more broadly in regulation or legislation or as de facto norms.

- Through the Order, the administration clearly adopts and endorses the National Institute of Standards and Technology (NIST) AI Risk Management Framework (RMF) as the standard for risk assessments and relevant safety and security guidelines. If they have not already, organizations should familiarize themselves with the AI RMF and consider using it to benchmark and guide their AI programs.
- The Order also highlights key areas where the administration (and others) have been raising concerns about potential risks of discrimination and other consumer protection concerns—including in education, healthcare, housing, transportation and employment. At the same time, the administration is focusing on ways to promote innovation and competition. AI is a groundbreaking yet disruptive technology, with many areas of potential concern. However, it is also an area where there are meaningful opportunities both for companies and for consumers. The Order attempts to identify and explain these risks, balance these considerations, and ensure orderly technological development that provides benefits without raising substantial new or expanded risks.
- The Order also focuses on critical concerns about privacy and cybersecurity, and it endorses the need for bipartisan national privacy legislation to protect all Americans (with a focus on children). It further provides support for the development of "privacy-enhancing technologies" as a means of realizing the benefits of AI without raising new privacy concerns. The Order also recognizes that there are meaningful cybersecurity concerns raised by AI technology, and it establishes an advanced cybersecurity program to develop AI tools to find and fix vulnerabilities in critical software.
- The Order calls for the heads of all agencies developing policies and regulations related to AI to use their authorities to promote competition in AI and related technologies. In particular, the Federal Trade Commission (FTC) is encouraged to consider whether to exercise its existing authorities 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. Given how vocal the FTC has been on AI, and the focus of the Order on privacy, consumer protection and competition, it is surprising that there was not more attention given to that particular agency in the Order. In response to the Order, FTC Chair Lina Khan posted on social media, "There is no AI exemption from existing laws, and the FTC will continue to promote fair competition, privacy, and honest business practices," indicating that the FTC—at least for now—expects to be able to use its existing regulatory tools to take action against AI activities that impact consumer protection concerns.
- The Order is notable for what it does not include. In particular, there is no suggestion of the need for a new federal regulator to oversee the technology or that there should be a licensing regime administered by an independent oversight body, as some in Congress have suggested. This suggests that the administration views a reliance on existing regulators as sufficient to establish guardrails for the technology, and that taking a more aggressive approach that reshapes how technology has traditionally been regulated in the

US—that is, sectorally, with the FTC as a "catchall" regulator—is unlikely, at least in the near term.

Overview of Biden's Executive Order

AI Safety and Security

Ensuring AI safety and security is a key priority for the administration and is a focus of the Voluntary Commitments for Ensuring Safe, Secure, and Trustworthy AI it secured with private companies. The Order builds on those commitments and attempts to better articulate the risks of AI and address those risks through standardizing safe AI practices and development. To that end, the Order directs various agencies to develop safety guidelines and evaluation tools for AI models. For example, the Department of Commerce is directed to establish guidelines and best practices for developing and deploying safe, secure and trustworthy AI systems by July 2024 to promote a consensus industry standard. The guidance is to address how to evaluate and audit AI capabilities, with a focus on the areas of cybersecurity and biosecurity, and develop standards for AI red-teaming tests, especially for dual-use foundation models.

The administration is also particularly concerned about AI's potential to pose cyber, critical infrastructure, and chemical, biological, radiological or nuclear threats. The Order requires the establishment of guidelines and mandates for owners of critical infrastructure to ensure the safety and security of critical infrastructure to prevent AI-related threats by June 2024, and it directs the Secretary of the Treasury to issue a public report on best practices to protect financial institutions from AI-specific cybersecurity risks by March 2024. The Order also requires the Secretary of Defense and the Secretary of Homeland Security to complete an operational pilot project for identifying and deploying AI capabilities to discover and remediate vulnerabilities in critical US government software, systems and networks by June 2024.

Consistent with the administration's concerns about national security and a global AI alignment strategy, the Order requires the US infrastructure as a service providers and foreign resellers of AI models to set certain user verification standards, keep records of users and ensure safe use of their models abroad. The Order also requires the Department of Commerce to issue reporting requirements for companies deploying dual-use foundation models relating to the models' training, red-teaming exercise and weights. Notably, the administration also appears to be considering the risks and benefits of having dual-use foundation models with model weights widely available and the potential for such open-source models to pose security risk to existing systems or allow uncontrolled development. To that end, the Secretary of Commerce is directed to study the potential risks and benefits related to dual-use foundation models for which the model weights are widely available and to submit a report to the President with policy and regulatory recommendations by July 2024.

The potential for disinformation and deep fakes has also been of serious concern to the administration and policymakers, and the Order requires the Secretary of Commerce to submit a report identifying standards, tools, methods and best practices for authenticating content, labeling (including watermarking) content, detecting synthetic content, preventing generative AI from producing child sexual abuse materials, testing software, auditing and maintaining synthetic content. This report will form the basis for guidance regarding digital content authentication and synthetic-content detection measures.

Competition and Innovation

The Order takes several steps to encourage innovation as well as to address some of the intellectual property (IP) concerns that have been brought to the fore over the past several months as generative AI has become more widely available. For example, the Order directs the Under Secretary of Commerce for Intellectual Property and the US Patent and Trademark Office Director to publish guidance addressing inventorship and the use of AI as well as other considerations at the intersection of AI and IP. There are also significant measures supporting AI-related research and development, including the establishment of training programs and grantmaking and other awards, as well as the introduction of measures to streamline and facilitate immigration into the United States for non-citizens specializing in AI.

The Order also aims to promote competition by requiring the head of each agency developing policies and regulations related to AI to use their authorities to promote competition in AI and related technologies. In particular, the FTC is encouraged to consider whether to exercise its existing authorities 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 will also provide resources to small businesses specializing in AI, including by prioritizing the allocation of Regional Innovation Cluster program funding for clusters that support small businesses seeking to advance the development of AI.

Workforce Issues

The potential for AI to fundamentally reshape labor and work has been of significant concern to the Biden Administration. Through the Order, the administration seeks to mitigate the risks associated with AI in the workplace (for example, increased workplace surveillance bias and job displacement), ensure that AI deployed in the workplace advances employees' well-being, and invest in AI-related workforce training and development. The Order requires a number of measures to advance the government's understanding of AI's implications for workers. For example, the Order requires that the Chairman of the Council of Economic Advisers prepare and submit a report to the President on AI's labor-market effects. The Secretary of Labor is also directed to submit to the President a report analyzing the abilities of agencies to support workers displaced by the adoption of AI and other technological advancements. The Order also calls for the Director of the National Science

Foundation (NSF) to prioritize available resources to support AI-related education and AI-related workforce development through existing programs.

Equity and Civil Rights

Issues of equity and civil rights have been a major focus of the administration and were front and center in the White House Blueprint for an AI Bill of Rights. The Order continues this focus by requiring multiple federal agencies to assess how the use of AI for their functions could result in discrimination or otherwise affect civil rights. For example, the Order requires the Secretary of Health and Human Services (HHS) to publish a plan addressing the use of automated or algorithmic systems in the implementation by states and localities of public benefits and services administered by the Secretary. The Order also requires the Secretary of Labor to publish guidance for federal contractors regarding nondiscrimination in hiring involving AI and other technology-based hiring systems by October 2024. There are also provisions designed to ensure fairness in the criminal justice system. Specifically, the Order requires the Attorney General, in consultation with the Secretary of Homeland Security and the Director of the Office of Science and Technology Policy, to submit a report addressing the use of AI in the criminal justice system that identifies areas where AI can enhance law enforcement efficiency and accuracy and recommending best practices for law enforcement agencies.

Healthcare and Education

The Order contemplates the uses and risks of AI in the healthcare, education and transportation sectors. Consistent with a broad recognition of how AI technologies—if used appropriately—can benefit society and consumers, the Order seeks to advance the responsible use of AI in healthcare and the development of affordable and lifesaving drugs through the establishment of an HHS AI task force that will issue a strategic plan on the responsible use and deployment of AI technologies in the health and human services sector. In addition, the Order requires the Secretary of HHS to create an AI safety program through which a common framework can be created for identifying and capturing errors from AI deployed in healthcare settings that could result in harm to patients and caregivers and to develop a strategy to regulate the use of AI-enabled tools in drug-development processes to identify appropriate regulation throughout each phase of drug development. And, the Order requires the Secretary of Education to develop resources and guidance to address AI in education, including the impact AI systems have on vulnerable and underserved communities.

Privacy

The Biden Administration has also been focused on potential privacy harms of AI, especially in the absence of federal comprehensive data privacy legislation. During his remarks about the Order, President Biden again emphasized the need for Congress to pass bipartisan legislation to limit the personal data collected by large technology companies, with a particular emphasis on legislation directed at kids and teenagers online. The Order reflects this focus on privacy and takes significant steps toward strengthening privacy protections. The Order requires the Director of the Office of

Management and Budget (OMB) to evaluate how agencies collect and process commercially available information (including personally identifiable information and information from data brokers and their vendors) in order to inform agencies about how to mitigate privacy and confidentiality risks. The Order further requires the Secretary of Commerce, acting through the Director of the NIST, to develop guidelines for agencies to evaluate the efficacy of differential-privacy-guarantee protections, including for AI (the Order uses "differential-privacy guarantee" to refer to the ability to share information about a group, while limiting the improper use of information about an individual entity). The Order also requires the Director of the NSF to fund the creation of a research coordination center dedicated to advancing privacy research and the development, deployment and scaling of privacy-enhancing technologies by April 2024.

Government Use of AI

The Order directs agencies to study and implement safe use of AI for government. The Order makes clear that federal agencies should consider incorporating AI in carrying out their executive functions after a careful review of any risks. For example, the Order requires the Director of the OMB to convene and chair an interagency council to coordinate the use of AI across federal agencies. The Order further requires the Director of the OMB and the interagency council to issue guidance to agencies to strengthen the effective and appropriate use of AI, advance AI innovation and manage risks from AI in the federal government as well as for each agency to appoint a Chief Artificial Intelligence Officer. The guidance will specify required minimum risk-management practices for government uses of AI that impact people's rights or safety, external testing requirements for AI, reasonable steps to watermark or label generative AI output, AI training principles, and public reporting requirements. The Order also requires the Director of the Office of Personnel Management to develop guidance on the use of generative AI for work by the federal workforce. The Order also directs agencies to review how to attract AI talent to work in the government, including by allowing noncitizens to be employed.

International Collaboration

The Order addresses international collaboration on AI engagement and the establishment of international AI standards. Around the globe, countries are exploring how AI can help their citizens. The Order acknowledges that without global alignment on basic standards for AI, there is a risk of international inconsistency in the development and use of these technologies. Therefore, the Order mandates that the Secretary of Homeland Security develop a plan for multilateral engagements to encourage the adoption of AI safety and security guidelines by critical infrastructure owners and operators. The Order also requires the Secretary of State to establish a plan for global engagement on promoting and developing AI standards to potentially include best practices regarding data capture, handling, and analysis, as well as AI risk management.

Contributors

Kirk J. Nahra
PARTNER

kirk.nahra@wilmerhale.com
+1 202 663 6128

Benjamin A. Powell
PARTNER

benjamin.powell@wilmerhale.com
+1 202 663 6770

Arianna Evers
SPECIAL COUNSEL

arianna.evers@wilmerhale.com
+1 202 663 6122

Roma Gujarathi
ASSOCIATE

roma.gujarathi@wilmerhale.com
+1 617 526 6280

Nancy Stephen
ASSOCIATE

nancy.stephen@wilmerhale.com
+1 202 663 6162

Jack You
ASSOCIATE

jack.you@wilmerhale.com
+1 202 663 6164