November 3, 2023

Skadden

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on the last page or call your regular Skadden contact.

This memorandum is provided by Skadden, Arps, Slate, Meagher & Flom LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This memorandum is considered advertising under applicable state laws.

One Manhattan West
New York, NY 10001
212.735.3000

Biden Administration Passes Sweeping Executive Order on Artificial Intelligence

On October 30, the U.S. government released its long-awaited, sweeping executive order (the AI EO or Order) on artificial intelligence (AI). The Order directs various U.S. government departments and agencies to evaluate AI technology and implement processes and procedures regarding the adoption and use of AI. The AI EO also imposes obligations on the private sector and builds out a coordinated government infrastructure on AI policy. The AI EO marks the Biden administration's most significant attempt to regulate the burgeoning technology to date.

Executive Summary

The AI EO directs federal, state, local and tribal agencies and bureaus, private companies, research institutions and regulatory bodies to consider providing guidance regarding the use, development and adoption of AI. The AI EO requires AI developers to provide reports to the federal government detailing testing and training protocols (including in connection with developing dual-use foundation models and large-scale computing clusters), both before and after powerful AI systems are released to the public. Companies looking to develop and launch AI products should therefore pay close attention to the obligations set forth in this AI EO, as well as monitor future guidelines and regulations as directives in the Order are implemented in the coming months and years. In addition, such guidance may impact various regulated sectors, such as the financial and life sciences industries. Companies in regulated sectors should monitor guidelines and evaluate how such guidelines may impact their businesses.

Scope of Executive Order

The AI EO centers around safeguarding against threats posed by AI, and ensuring AI systems are "safe, secure and trustworthy." The Order is organized by eight guiding principles and priorities, some of which are derived from the "Blueprint for an AI Bill of Rights"[1] previously released by the Biden administration in October 2022.

The EO's directives cover various sectors, such as the technology, financial and biotechnology industries. The Order's release was timed to coincide with the November 1 U.K. AI Safety Summit, at which global leaders, including Vice President Kamala Harris, discussed AI risks and opportunities on a global scale.

[1] Published by the White House Office of Science and Technology Policy, the "Blueprint for an AI Bill of Rights" (AI Bill of Rights) identified five principles to guide the design, use and deployment of automated systems to protect the American public in the age of artificial intelligence.

Biden Administration Passes Sweeping Executive Order on Artificial Intelligence

Key Points in Executive Order

'Ensuring the Safety and Security of AI Technology'

- **Standards and Testing:** The AI EO requires the secretary of commerce — acting through the National Institute of Standards and Technology (NIST), in coordination with the heads of other relevant departments and agencies — to establish guidelines and best practices for developing and deploying "safe, secure and trustworthy" systems. These guidelines include creating standards for extensive "red-team testing" of AI systems to ensure powerful systems meet certain safety standards. The threshold criteria for which models are subject to this requirement will be determined by the commerce secretary. Notably, the "default" included in the Order would likely pick up few, if any, of the AI models in use today. As detailed below, the AI EO, leveraging its powers under the Defense Production Act, will in turn require companies building these AI models to adhere to these testing standards and report any deviations from or failures to meet them. The AI EO also includes additional directives for the commerce secretary, acting through NIST, that focus on testing AI systems and so called "dual-use" foundation models, including:
  - Developing companion resources to existing NIST frameworks, such as the AI Risk Management Framework[2] and the Secure Software Development Framework, to incorporate secure development practices for generative AI and dual-use foundation models.
  - Coordinating or developing guidelines related to assessing and managing the safety, security and trustworthiness of dual-use foundation models.
  - Developing and ensuring the availability of testing environments, in coordination with the secretary of energy and director of the National Science Foundation, to support the development of safe, secure and trustworthy AI technologies, including the design, development and deployment of associated privacy-enhancing technologies (PETs).

The AI EO also imposes obligations on the secretary of energy — in coordination with the heads of other Sector Risk Management Agencies (SRMAs) or in consultation with private AI laboratories, academia or third-party evaluators — to develop and implement a plan for AI system evaluation tools and testbeds, noting that these tools should be designed to identify AI systems that could generate outputs that may represent nuclear, nonproliferation, biological, chemical, critical infrastructure and energy-security threats or hazards.

- **Obligations on Companies To Comply With Standards and Testing:** Importantly, the AI EO requires companies that are developing, or intending to develop, any dual-use foundation models to provide information to the federal government on a rolling basis, including regarding ongoing or planned activities relating to the training, development or production of the models and measures taken to protect against security threats. Critically, such companies are also required to conduct tests on these models and share the results of such tests with government officials, before any new capabilities are available to consumers. These tests, and the results, must adhere to the standards developed by NIST (or, if prior to the development of the NIST testing standards, results of any testing conducted to enhance safety objectives detailed in the AI EO).

These reporting obligations imposed on companies will have broad implications on how AI models are developed. According to the AI EO, the Biden administration expects these measures to ensure AI systems are safe, secure and trustworthy before they are made available to the public.

- **Cloud Computing Obligations:** The AI EO also imposes certain obligations regarding large-scale computing clusters, including:
  - Requiring companies, individuals or other organizations or entities to report any acquisition, development or possession of such large-scale computing clusters, including the existence and location of the clusters and the amount of total computing power available in each cluster.
  - Directing the commerce secretary (in consultation with other agencies) to define, and update on a regular basis, technical conditions for models and computing clusters that would trigger reporting obligations.
  - Requiring the commerce secretary to propose regulations requiring the maintenance of records of foreign transactions involving United States infrastructure as a service (IaaS) products.
  - Requiring U.S. IaaS providers to submit a report to the commerce secretary when a foreign person transacts with that provider (or their foreign resellers) to train a large AI model with potential capabilities (with a set of technical conditions to be determined by the commerce secretary) that could be used in malicious cyber-enabled activity.

[2] For more information, see our May 18, 2023, client alert "AI Risk: Evaluating and Managing It Using the NIST Framework."

- **Managing AI in Critical Infrastructure and in Cybersecurity:** The AI EO includes requirements directed at ensuring the protection of "critical infrastructure," including that:
  - The head of each agency with relevant regulatory authority over critical infrastructure and various other key stakeholders evaluate and provide to the Department of Homeland Security an annual assessment of potential risks related to the use of AI in critical infrastructure sectors.
  - The secretary of treasury issue a public report on best practices for financial institutions to manage AI-specific cybersecurity risks.
  - The secretary of homeland security — in coordination with various SRMAs and government departments and agencies — incorporate NIST frameworks (including the AI Risk Management Framework) and security guidance into relevant safety and security guidelines for use by critical infrastructure owners and operators.
  - U.S. government departments and agencies develop plans for, conduct and complete operational pilot projects to identify, develop, test, evaluate and deploy AI capabilities to discover and remediate vulnerabilities in critical U.S. software, systems and networks.

The AI EO also requires the establishment of an Artificial Intelligence Safety and Security Board as an advisory committee, including AI experts from the private sector, academia and government, to provide advice, information or recommendations for improving security, resilience and incident response related to AI usage in critical infrastructure.

Finally, the AI EO directs U.S. government agencies that fund life science projects to establish new standards for biological synthesis screening as a condition of federal funding. The Biden administration expects that such conditions would create powerful incentives to ensure appropriate screening and manage the risk that AI may be used to synthesize biological threats.

- **Reducing Risk Posed by AI-Generated Content:** The AI EO directs the Department of Commerce, in coordination with other agencies, to develop "science-backed standards and techniques" for authenticating and tracking the provenance of content, labeling AI-generated content (including using watermarking), detecting AI-generated content and preventing generative AI from producing abusive or nonconsensual material. It also directs U.S. government departments and agencies to develop tools to enable Americans to easily identify whether communications they receive from the government are authentic. The directive addresses concerns surrounding the ability of generative AI to create widespread fake or misleading content, and will likely impact how regulators, and even legislators, tackle these issues moving forward.
- **Promoting Safe Release and Preventing the Malicious Use of Federal Data for AI Training:** To improve public data access and manage security risks — and consistent with the objectives to expand public access to federal data assets in a machine-readable format while also taking into account security considerations — the AI EO directs the Chief Data Officer Council to develop initial guidelines for performing security reviews. These include reviews to identify and manage the potential security risks of releasing federal data that could pose security risks (including the development of chemical, biological, radiological or nuclear weapons or other offensive cyber capabilities). Companies that process or use federal data should monitor such guidelines to align their data-handling practices with these evolving security standards.
- **Directing the Development of a National Security Memorandum:** To develop a coordinated executive branch approach to managing AI's security risks, the assistant to the president for national security affairs and the assistant to the president and deputy chief of staff for policy are directed to oversee an interagency process with the purpose of developing and submitting a proposed National Security Memorandum on AI to the president, which shall address the governance of AI used as a component of a national security system or for military and intelligence purposes. Companies that consult in the military and intelligence space should pay close attention to how these guidelines, and the subsequent memorandum, take shape.

'Promoting Innovation and Competition'

The AI EO reinforces previous statements made by the Biden administration on the importance of maintaining a global competitive advantage on advancements in AI technology. In furtherance of this objective, the AI EO imposes a number of obligations, including requiring:

- The launch, maintenance and expansion of AI-related research programs and institutes.
- Regulators, such as the secretaries of energy and veterans affairs, to engage in activities designed to catalyze AI-related innovation in their respective fields.

The AI EO also includes the following initiatives directed at promoting innovation and competition:

- **Attracting Top AI Talent:** In order to attract the best AI talent to the United States, the AI EO directs the secretaries of state and homeland security to streamline the application and visa process for noncitizens working in AI, and it charges federal agencies with developing a comprehensive online guide explaining the options and opportunities AI experts have to work in the U.S.
- **Intellectual Property:** The AI EO addresses three topics relating to intellectual property and AI: use of AI in the inventive process for patents, copyrights and AI and mitigating AI-related IP risks, like AI theft.
  - First, the AI EO requires the under secretary of commerce for intellectual property and the director of the United States Patent and Trademark Office (USPTO) to publish guidance, with illustrative examples, addressing how the use of AI in the inventive process may affect inventorship of patents. Note that the Court of Appeals for the Federal Circuit held in *Thaler v. Vidal* that an AI system cannot be named as an inventor on a patent. The USPTO has conducted listening sessions on the topic, but neither the courts nor the USPTO have yet provided specific guidance regarding when human inventors can obtain a patent claiming an invention AI helped to conceive or reduce to practice.
  - Second, the AI EO calls on the United States Copyright Office to issue recommendations on potential executive actions relating to copyright and AI. The directive comes on the heels of various decisions, opinions and guidance from the Copyright Office over the past year with respect to the registrability of works containing AI-generated content — potentially signaling that further guidance in the space is needed in light of increased innovation in the space.
  - And third, the AI EO encourages Homeland Security, in coordination with the U.S. attorney general, to work alongside enforcement agencies such as the FBI and U.S. Customs and Border Protection to implement a policy of sharing information and coordination to mitigate AI-related IP risks, such as IP theft.

The AI EO also calls on the Federal Trade Commission (FTC) to consider, "as it deems appropriate," whether to exercise its existing authority, including its rulemaking authority, to ensure fair competition in the AI marketplace and ensure consumers and workers are protected from harms related to AI. The AI EO does not, however, delve into the specific areas in which the FTC should consider investigating.

'Supporting Workers'

The AI EO sets forth a number of directives related to the labor market. These directives build on prior executive branch guidance addressing AI's potential for discrimination and bias and directing agencies to examine how they could use AI to help their efforts to advance equity. The Equal Employment Opportunity Commission previously issued its own guidance on how employers can avoid violating the Americans with Disabilities Act and Title VII of the Civil Rights Act of 1964 when using AI in the workplace. The AI EO's directives include:

- Directing the chairman of the Council of Economic Advisers to submit a report on the labor market effects of AI. The AI EO also charges the secretary of labor with submitting a report analyzing the ability for government agencies to support workers displaced by AI in the workplace. The labor secretary's report will evaluate government programs already in place that could be utilized to help workers disrupted by AI and evaluate potential new legislative measures to develop additional support for workers.
- Charging the labor secretary, in consultation with unions and workers, with producing a list of best practices and principles for employers to mitigate harm to workers while still maximizing AI's benefits in the workplace. The best practices will cover, among other topics, job displacement, career opportunities, AI's evaluation of workers and applicants, labor standards, job quality, equity, health and safety, data collection and use, compensation and protected activities.
- Requiring that employees who have their work augmented or monitored by AI continue to be compensated for their hours worked as defined under the Fair Labor Standards Act.

'Protecting Privacy'

The AI EO requires agencies to issue guidance to mitigate specific risks related to discrimination resulting from the use of AI, building upon related requirements, such as restrictions against profiling, under certain existing sector-specific and jurisdictional-specific U.S. privacy regulations. For example, the AI EO directs the Department of Health and Human Services to issue guidance that addresses:

- Human oversight in the development, maintenance and use of AI in health care delivery and financing.
- The use of representative population data sets when developing new models and monitoring AI performance against discrimination.
- The incorporation of safety, privacy and security standards into the software lifecycle for protection of personally identifiable information.

- The development and availability of documentation to help users determine safe uses of AI in the health and human services sector.

The AI EO also encourages the Federal Communications Commission to consider building upon the requirements of the Telephone Consumer Privacy Act (TCPA), which restricts the sending of certain robotexts and robocalls without the consent of the recipient, through rulemaking designed to combat such unwanted calls and texts facilitated or exacerbated by AI.

Recognizing AI's potential to exacerbate privacy risks as a result of its ability to easily collect, use and generate information about individuals, the AI EO also tasks certain agencies with mitigating such risks in the public sector:

- The Office of Management and Budget (OMB) must evaluate how agencies use commercially available data, particularly that which contains personal information, as well as solicit feedback on whether privacy impact assessments (required by the E-Government Act for the processing of personal information by government agencies in certain circumstances) effectively mitigate privacy risks exacerbated by AI.
- The commerce secretary must create guidelines for agencies to evaluate the efficacy of differential-privacy-guarantee protections (defined as protections that allow information about a group to be shared while provably limiting the improper access, use or disclosure of personal information about particular individuals).
- The National Science Foundation must engage with agencies to identify opportunities to incorporate privacy-enhancing technologies into their operations.

'Advancing Civil Rights'

The AI EO also sets forth a number of directives targeted at advancing equity and civil rights, and avoiding discriminatory impacts of AI systems, aligning with the Biden administration's ongoing emphasis on addressing AI-related discrimination, as demonstrated in the AI Bill of Rights released in 2022. Specifically, the AI EO:

- Directs government agencies to impose training and technical assistance for investigating and prosecuting civil rights violations related to AI, establishing mechanisms to ensure fairness in the criminal justice system and through law enforcement agencies (including in connection with hiring).
- Imposes obligations to avoid discriminatory harms from the use of AI in connection with government benefits and programs, housing and the consumer financial markets, and federal records (such as criminal records, credit information, eviction records, etc.).

'Advancing Federal Government Use of AI'

The AI EO directs federal agencies to enhance their utilization of AI and mitigate AI-related risks, aiming to set an example for private sector practices.

- **Creation of Interagency Council:** Notably, the AI EO establishes an interagency council, chaired by the director of OMB and staffed with the heads of every major agency, to facilitate the development of AI in federal agencies.
- **Guidance for Federal Agencies:** The AI EO also tasks the OMB director with providing guidance to agencies to specify, among other topics, (1) the creation of their own internal "Artificial Intelligence Governance Boards" and designation of a chief artificial intelligence officer; (2) requirements to develop AI strategies and pursue high-impact AI use cases; and (3) recommendations for testing and safeguarding against discriminatory or deceptive outputs from generative AI.

  In addition, the AI EO underlines the significance of the Biden administration's AI Bill of Rights and the NIST AI Risk Management Framework by obligating agencies to follow risk management practices derived from these documents for AI uses impacting people's rights or safety.
- **Increasing AI Government Talent:** The AI EO emphasizes the urgency of bolstering AI talent in federal government, creating an AI and Technology Talent Task Force to expedite AI talent recruitment and encouraging agencies to enhance their hiring and training practices to effectively fulfill the AI EO's mandates.

Other Administration AI Activities

The AI EO follows a number of measures taken by the federal government attempting to establish guardrails around AI use and adoption, including the publication of the AI Bill of Rights, securing self-regulatory commitments from private companies,[3] providing guidance on outbound U.S. investments to foreign actors in certain sectors[4] and updating export controls on certain technologies.[5]

[3] In July 2023, the administration secured self-regulatory commitments from seven AI companies to enhance safety, security and trust in the development of certain AI models, including with respect to information sharing and public reporting. See our July 25, 2023, client alert "The White House Secures Voluntary Commitments From Seven Leading AI Companies To Promote Safety, Security and Trust in AI." In September 2023, eight more companies signed on to these commitments.

[4] In August 2023, the president released an executive order directing the Department of the Treasury to create a new regulatory program to prohibit or require notification of outbound U.S. investments to China in certain sensitive sector, including artificial intelligence. See our August 10, 2023, client alert "US Moves To Narrowly Limit Investment in China."

[5] In October 2023, the Department of Commerce's Bureau of Industry and Security released a package of rules updating export controls on advanced computing semiconductors and semiconductor manufacturing equipment used in AI development to China. These restrictions were aimed to close perceived loopholes in chip-related rules the U.S. announced in 2022. See our October 25, 2023, client alert "BIS Updates October 2022 Semiconductor Export Control Rules."

Conclusion

The AI EO represents another step in the Biden's administration's ongoing efforts to shape AI usage and adoption at a time when there has not been any meaningful AI legislation proposed by Congress to date nor any on the short-term horizon. The administration hopes that closely monitored, responsible adoption of AI by government agencies could provide a sandbox within which AI governance and adoption is tested and serve as a possible framework for future legislative efforts.

Although broad in scope, the AI EO does not go so far as to make the AI Bill of Rights binding on the federal government's use of AI systems, a request that was made in a September 2023 letter to the administration by a number of civil, technology, labor, consumer, transparency, accountability and human rights groups, and echoed in a letter from 16 members of the Senate and House to the administration on October 11, 2023.

The order also represents a significantly different approach to AI than the EU AI Act, initially proposed by the European Commission in April 2021, and now being discussed in a "trilogue" amongst the European Commission, the European Parliament and the European Council. While the EU AI Act applies broadly to the sale and use of AI systems in the EU, the AI EO seeks to strike a balance between fostering AI adoption and managing AI-related risks The EU AI Act, which adopts a risk categorization system (unacceptable, high, limited and minimal/none), is a more proscriptive approach imposing, among other requirements, a comprehensive set of risk management, data governance, monitoring and record-keeping practices, human oversight obligations and standards for accuracy. Given that foreign individuals or entities may also be captured under the different regulations, companies should carefully adopt a proactive approach to compliance, staying informed about updates and changes in AI-related regulations both in the U.S. and internationally.

Contacts

Ken D. Kumayama
Partner / Palo Alto
650.470.4553
ken.kumayama@skadden.com

Stuart D. Levi
Partner / New York
212.735.2750
stuart.levi@skadden.com

William Ridgway
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

David E. Schwartz
Partner / New York
212.735.2473
david.schwartz@skadden.com

David A. Simon
Partner / Washington, D.C.
202.371.7120
david.simon@skadden.com

Pramode Chiruvolu
Counsel / Palo Alto
650.470.4569
pramode.chiruvolu@skadden.com

Jordan Cannon
Associate / Washington, D.C.
202.371.7542
jordan.cannon@skadden.com

Guodong Fu
Associate / New York
212.735.3605
guodong.fu@skadden.com

MacKinzie M. Neal
Associate / New York
212.735.2856
mackinzie.neal@skadden.com

Connor A. Riser
Associate / New York
212.735.3762
connor.riser@skadden.com

Lisa V. Zivkovic
Associate / New York
212.735.2887
lisa.zivkovic@skadden.com

Priya R. Matadar
Law Clerk / New York
212.735.2542
priya.matadar@skadden.com