wiley

ALERT

New AI Executive Order Outlines Sweeping Approach to AI

October 31, 2023

On October 30, 2023, the White House released an Executive Order for Safe, Secure, and Trustworthy Artificial Intelligence (EO), which outlines a sweeping plan for encouraging the development and managing the risks of artificial intelligence (AI). The notably lengthy EO includes dozens of directives to numerous agencies that will be implemented in the next year. These wide-ranging directives will generally impact companies that are developing and deploying AI and will result in new requirements for government contractors, as well as new AI standards, guidance, and best practices for the private sector, among other things.

At a high level, the EO's directives relate to a set of eight "guiding principles and priorities," which include ensuring safety and security; promoting innovation and competition; advancing equity and civil rights; and protecting privacy and civil liberties. There are several key takeaways for companies developing and using AI tools:

- *The EO's Directives on Safety and Security Will Result in New Requirements and Influence Expectations for Companies Developing and Using AI*: The EO focuses heavily on safety and security risks for AI and launches several government efforts that will have both direct and indirect impacts on private sector use of AI technologies and systems. For example, the EO mandates reporting requirements for companies developing "dual-use foundation models" for use by the federal government and building large-scale computing clusters. More generally, the EO requires the National Institute of Standards and Technology (NIST) to lead an effort to develop and establish guidelines and best practices for AI safety and security.

Authors

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Kara M. Sacilotto
Partner
202.719.7107
ksacilotto@wiley.law

Lisa Rechden
Associate
202.719.4269
lrechden@wiley.law

Lauren N. Lerman
Associate
202.719.4664
llerman@wiley.law

Practice Areas

Artificial Intelligence (AI)
Government Contracts
Privacy, Cyber & Data Governance
Telecom, Media & Technology

- *Directives Around Transparency May Establish New Standards for Identifying and Labeling AI*: The EO identifies specific concerns around fake content generated by AI and instructs the U.S. Department of Commerce to issue guidance for the use of data content authentication tools and practices. The EO specifically identifies labeling synthetic content, such as using watermarking, among the tools and practices to be included in the guidance.
- *The EO Will Lead to Additional Guidance and Guardrails for Companies to Protect Against Unlawful Discrimination and Bias*: The EO instructs agencies to build on existing guidance to stakeholders to address unlawful discrimination and bias in using AI tools. Agencies have issued such guidance as applied to AI in several sectors—for example, in financial services—and the EO should prompt agencies to build this out more.

Below we provide (1) brief context for the EO; (2) a high-level overview of the EO's main principles, workstreams, and stakeholder impacts; and (3) some of the key next steps that will flow from the order. Overall, this EO marks a critical advancement in federal AI policy; its output will form the basis of AI best practices and potentially regulations moving forward, and it will have direct and indirect impacts on AI innovation, development, and deployment for years to come.

BACKGROUND: THE EO BUILDS UPON THE ADMINISTRATION'S FOUNDATIONAL EFFORTS TO PROMOTE TRUSTWORTHY AI

This EO follows prior Office of Science and Technology (OSTP) activity on AI, such as the release of the AI Bill of Rights and efforts to secure voluntary commitments from leading AI companies to use and promote safe, secure, and trustworthy AI. The EO's eight principles build on those outlined in the AI Bill of Rights, such as promoting safe and effective systems, preventing algorithmic discrimination, and protecting personal data.

The EO also states that it builds from NIST's landmark AI Risk Management Framework (AI RMF) and calls for new work product to be spun off from the AI RMF. For example, the EO directs NIST to develop a companion AI RMF resource for generative AI and for the U.S. Department of Homeland Security (DHS) to incorporate the AI RMF into its guidance on AI safety and security for Critical Infrastructure.

SUMMARY: EIGHT CORE PRINCIPLES UNDERLY THE EO AND WILL DRIVE ITS POLICY IMPACTS

AI Safety and Security. One of the Administration's primary AI policy goals is to ensure that AI is safe and secure, and that AI is utilized to promote national security and national interests. Section 4—which outlines this principle—includes some of the most imminent mandates for stakeholders.

- **Develop Guidelines, Standards, and Best Practices for AI Safety and Security:** NIST is tasked with establishing several pieces of guidance and best practices. For example, the EO instructs NIST to create a companion to both the AI RMF and Secure Software Development Framework that cover generative AI. Additionally, NIST will launch an initiative for AI auditing, which will include best practices and benchmarks for use of AI in cybersecurity and biosecurity. NIST will also create procedures and processes for "red-teaming tests" to be conducted on "dual-use foundational models," which the EO

defines as an AI model "that is trained on broad data; generally uses self-supervision; contains at least tens of billions of parameters; is applicable across a wide range of contexts; and that exhibits … high levels of performance at tasks that pose a serious risk to security, national economic security, national public health or safety …" The EO also mandates that the Secretary of Energy conduct similar efforts.

- **Ensure Safe and Reliable AI**: The EO relies on the Defense Production Act to require companies developing or planning on developing "dual-use foundation models" to be provided to the federal government, to provide reports and keep records on the ownership of the models, type of cybersecurity and privacy measures employed, and results from any "red-testing" conducted. The EO also requires companies developing or possessing large-scale computing clusters to report the existence and location of each cluster and technical conditions to be outlined by the Secretary of Commerce. Recordkeeping requirements and other limitations are also imposed on Infrastructure as a Service (IaaS) products that are tested or sold by foreign persons.
- **Manage AI in Critical Infrastructure and in Cybersecurity**: The EO requires the head of cyber agencies to conduct various assessments and reports on the best practices and methods for managing AI-related cybersecurity risks.
- **Reduce Risks at the Intersection of AI and CBRN Threats**: The Secretary of Homeland Security and other chief cybersecurity officials are tasked with identifying and reporting on the Chemical, Biological, Radiological and Nuclear risks enhanced by AI. These cybersecurity officials are also tasked with developing a framework to implement "comprehensive, scalable, and verifiable synthetic nucleic acid procurement screening mechanisms, including standards and recommended incentives."
- **Reduce the Risks Posed by Synthetic Content**: The Secretary of Commerce shall issue a report about and guidance for the use of existing standards and tools to provide digital authentication and detect synthetic media. Among the guidance, the EO specifically requires measures for (1) authenticating content and tracking its provenance; (2) labeling synthetic content, such as using watermarking; (3) detecting synthetic content; (4) preventing generative AI from producing child sexual abuse material; (5) testing software used for the above purposes; and (6) auditing and maintaining synthetic content. The EO also requires NIST to issue guidance to federal agencies, specifically on labeling and authenticating content that they produce or publish.
- **Solicit Input on Dual-Use Foundation Models with Widely Available Model Weights**: The EO requires the Secretary of Commerce to submit a report that outlines the risks, benefits, and mechanisms to regulate "dual-use foundation models" for which the model weights are widely available.
- **Promote Safe Release and Prevent the Malicious Use of Federal Data for AI Training**: The Chief Data Officer Council is instructed to develop initial guidelines for performing security reviews, including reviews to identify and manage the potential security risks of releasing federal data.
- **Direct the Development of a National Security Memorandum**: The Assistant to the President for National Security Affairs and the Assistant to the President and Deputy Chief of Staff for Policy will develop a National Security Memorandum on AI to provide guidance to the U.S. Department of Defense for AI assurance and risk-management practices for national security uses of AI and direct other actions to address risks of AI-use by adversarial foreign actors.

The broad guidance and reporting guidelines outlined throughout this section of the EO provide many potential obligations for industry stakeholders. As the EO directs many agencies to issue best practices for a variety of AI use cases, the implications of this order will have a direct impact on how AI may be developed and deployed in the private sector.

Promoting Innovation and Competition. The EO seeks to promote the growth and development of AI by creating a "fair, open, and competitive ecosystem and marketplace for AI and related technologies so that small developers and entrepreneurs can continue to drive innovation." In particular, the EO issues the following instructions.

- **Attract AI Talent to the United States**: The Secretary of State and Secretary of Homeland Security shall streamline the visa process for noncitizens who travel to the United States to study or research AI or other emerging technologies and consider rulemakings and Requests for Information to adjust various immigration policies to improve immigrant pathways to the United States for those with skills or expertise in AI and emerging technologies. Additionally, the Secretary of State, the Secretary of Commerce, and the Director of OSTP, are directed to publish informational resources to attract and retain AI experts.
- **Promote Innovation**: The Director of the National Science Foundation (NSF) is instructed to launch the National AI Research Resource (NAIRR), at least one NSF Regional Innovation Engine that prioritizes AI-related work, and a pilot program to train scientists to study and develop AI. Additionally, the Under Secretary of Commerce for Intellectual Property and Director of the United States Patent and Trademark Office must issue guidance for patenting inventions developed using AI, including generative AI, and copyrighting work created using AI. Along these lines, the Secretary of Homeland Security is to develop a training, analysis, and evaluation program to mitigate AI-related IP risks. The EO further mandates specific policies and reports to promote innovation in healthcare technologies, specifically veterans' health care, and clean energy technologies.
- **Promote Competition**: The Federal Trade Commission is tasked with exercising its authority to address potential harms created by AI and promote competition in the AI marketplace. The EO focuses on the semiconductor industry as critical to AI development, and instructs the Secretary of Commerce to utilize the Creating Helpful Incentives to Produce Semiconductors (CHIPS) Act of 2022 to provide more opportunities to startups and small businesses through increased funding and access to the National Semiconductor Technology Center membership. The EO directs the Small Business Administration to allocate funding and support to small-business development of AI and small-business adoption of AI.

Impact of AI on Workers. The EO is concerned about the potential impacts of AI on workers. In particular:

- **Labor Market Impacts:** The EO calls for a study to determine the most likely negative and positive impacts to the market and whether, for federal workers specifically, federal agencies can accommodate and re-distribute the workers to other agencies should their positions become obsolete due to AI.
- **Best Practices:** The EO encourages the development of industry-wide best practices to address the potential risks to workers from companies' use of AI tools.

Advancing Equity and Civil Rights. The EO highlights the need to ensure that AI is deployed fairly and avoids unlawful discrimination.

- **Civil Rights**: The EO warns of the potential for AI tools to introduce additional biases into government benefits programs, such as those for housing assistance, and encourages contractors and agencies to screen algorithms for any red flags. To this end, the EO recommends providing training and technical assistance to agencies in this area, and coordinating with the U.S. Department of Justice and federal civil rights offices when questions arise as to investigating and prosecuting potential civil rights violations involving AI tools.
- **Criminal Justice System**: The EO examines the possible AI applications in the various stages of the criminal justice system.

Consumers, Patients, and Students. The EO also focuses on how AI can benefit and create potential risks for consumers, patients, and students. Although the EO recognizes the benefit of utilizing AI systems, it emphasizes the need for users to be fully informed prior to agreeing to use the system. It also spells out sector-specific considerations including in communications, health care, and education. For example:

- **Communications:** The EO encourages the Federal Communications Commission (FCC) "to consider actions related to how AI will affect communications networks and consumers," including with respect to spectrum management, spectrum sharing, improving network security, and combatting illegal robocalls and robotexts. The FCC has already started two such inquiries—with respect to spectrum management and mitigating robocalls and robotexts—so the Communications Sector can certainly expect more in this regard from the FCC.
- **Healthcare**: The EO focuses on the potential for using AI efficiently and safely in healthcare, including developing life-saving drugs. The U.S. Department of Health and Human Services also will be standing up a safety program to address reports of potentially unsafe healthcare practices related to AI.

Privacy. The EO seeks to promote data privacy in federal agencies to "mitigate privacy risks potentially exacerbated by AI."

- **Identify and Potentially Regulate Agency Use of Commercially Available Information**: The Director of the Office of Management and Budget (OMB) is directed to identify commercially available information (CAI) procured by agencies through reporting processes, evaluate appropriate guidance for agency handling of CAI, and issue a Request for Information.
- **Promote Use of Privacy-Enhancing Technologies (PETs)**: The Secretary of Commerce, acting through NIST, is required to create guidelines surrounding certain privacy-enhancing technologies. Additionally, the EO instructs the Director of NSF to create a Research Coordination Network (RCN) dedicated to scaling PETs and work with agencies to incorporate PETs into their operations.

Ensuring Responsible and Effective Government Use of AI. The EO notes that AI has the potential to improve the way in which the government operates, from cutting processing times for benefits to strengthening the security of sensitive systems, but that risks must be mitigated, including those related to unreasonable bias

and safety.

- **Alternative Procurement Methods**: The EO contemplates the use of alternative procurement methods that can expedite the federal acquisition process, reflecting an overall desire to streamline agencies' access to commercial AI capabilities without needing to individually negotiate and procure each item.
- **AI Guidance:** Agencies will likely issue standards for the procurement and deployment of AI tools and systems which reflect the specific agency's needs and sensitivities.
- **Training:** As AI use begins to proliferate throughout the government, employees will need to be properly trained on its applications and risks. The EO anticipates an uptick in training and education opportunities for employees working in areas particularly impacted by these developments. The government also anticipates recruiting AI professionals as part of a "government-wide AI talent surge," including a potential willingness to ease restrictions on noncitizens' access to classified information and research laboratories.

Companies capable of developing and deploying AI, even those that do not typically view themselves as "government contractors," are likely to see a flurry of new opportunities across the government. The government appears motivated to utilize non-traditional procurement methods, where applicable. These opportunities will likely come with contractual strings attached, including implementation of risk management principles drawing from the Administration's AI Bill of Rights and AI RMF.

Strengthening American Leadership Abroad. The EO suggests that the United States has the opportunity to work with international allies and partners to lead the way on AI policy and to establish international standards for AI to promote the principles discussed in the EO.

- **Engage with International Allies and Partners**: The Secretary of State, Assistant to the President for National Security Affairs, Assistant to the President for Economic Policy, and the Director of OSTP are tasked with expanding engagement with international allies and partners to (1) provide updates on U.S. AI policy and (2) establish an international framework to address the risks and benefits of AI.
- **Develop Plan for Global Engagement**: The Secretary of State is responsible for establishing a plan for global engagement on AI policy which will be guided, in part, by the NIST AI RMF principles.
- **Promote Development of Safe, Responsible AI**: The secretaries of State and Commerce, acting through NIST, are directed to publish an AI in Global Development Playbook that incorporates the AI RMF's principles, guidelines, and best practices. Additionally, the Secretary of State is to establish a Global AI Research Agenda.
- **Coordinate on Critical Infrastructure Safety**: The Secretary of Homeland Security and Secretary of State are to develop a plan that encourages international adoption of AI safety and security guidelines for critical infrastructure.

LOOKING FORWARD

The EO outlines numerous deadlines over the next year for agencies to solicit input and execute the Administration's mandates. Some notable timelines for companies to monitor include:

- The Secretary of Commerce will issue guidance regarding tools and practices for digital content authentication and synthetic content detection measures within 180 days of the EO, by April 27, 2024.
- All of NIST's frameworks and best practices must be established 270 days from the issuance of the EO, which is July 26, 2024.
- The National Security Memorandum on AI must also be submitted to the President by July 26, 2024.
- July 26, 2024 also marks the date by which the Secretary of Commerce must establish a plan, and subsequent report, for global engagement on promoting and developing AI standards.

In addition to the numerous mandates for agencies, the EO also creates the White House Artificial Intelligence Council, which will be chaired by the Deputy Chief of Staff for Policy and consist of at least 28 members, representing most of the Executive Branch offices.

This substantive EO demonstrates the Administration's continued focus on AI and its efforts to create guardrails for its use. Many agency actions will be open for comment and other types of industry engagement. Stakeholders should consider weighing in on the development of best practices and guidance across agencies.

***

Wiley's Artificial Intelligence and Government Contracts practices counsel clients on AI compliance, risk management, and regulatory and policy approaches, and we engage with key government stakeholders, including NIST, in this quickly moving area. Please reach out to a member of our team with any questions.