Memorandum

President Biden Executive Order dated October 30, 2023, on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence. (November 16, 2023)

Overview

The 10/30/23 EO on AI has the potential to set far-reaching standards governing the use and development of AI across industries, but it does not directly regulate private industry, apart from certain large-scale models or computing clusters deemed to potentially impact national security (discussed below). The EO also requires federal agencies including the Departments of Commerce (principally through the National Institute of Standards and Technology (**"NIST"**), Energy, and Homeland Security, among others, to issue standards and guidance and to use their existing authorities, including regulatory authorities, to police the use of AI in ways that will impact business for years to come. In addition, it devotes federal resources toward AI-related education, training and research, including the further development of privacy enhancing technologies (**"PETs"**) such as differential privacy and synthetic data generation.

Even though the required agency guidelines will not directly apply to private industry in many cases, they are likely to still have significant impact through their incorporation into federal contracts. Similarly, standards set by the NIST like the NIST Cybersecurity Framework have had a substantial industry impact through voluntary adoption – which has set industry expectations – and it would not be surprising to see a similar effect here.

The EO follows on the heels of the administration's Blueprint for an AI Bill of Rights, issued in October 2022 (the **"Blueprint"**) and the administration's meetings with leading AI and technology companies earlier this year. Like the Blueprint, the EO sets forth a number of guiding principles to ensure a safe, reliable and unified approach to AI governance: ensuring safety and security, promoting responsible innovation, competition, and collaboration, supporting the rights of American workers, advancing equity and civil rights, protecting the interest of American citizens, protecting privacy and civil liberties, promoting government efficiency, and advancing American leadership abroad.

Safety and Security

The EO requires NIST to issue new guidelines and standards for the testing and development of AI that are likely to shape business processes going forward. It also imposes rules under the Defense Production Act on "dual-use foundation models" that have the potential to pose a serious risk to national security, national economic security, or national public health or safety.

Testing the Safety and Efficacy of AI: NIST, in collaboration with the Departments of Energy and Homeland Security, is tasked with creating guidelines, best practices, and standards to ensure the safe and secure development of AI technologies. These efforts include developing standards and guidelines around managing AI risks, incorporating secure practices for generative AI, and developing testing environments for AI safety. NIST is specifically instructed to issue a companion resource to the AI Risk Management Framework, NIST AI 100-1 for generative AI. The required guidelines will also support and develop standards for red-teaming

tests around the safety and efficacy of AI systems to promote trustworthy AI deployment. Additionally, the Secretary of Energy is instructed to develop tools and testbeds for assessing AI systems' capabilities, focusing on preventing security threats across various domains like nuclear, biological, and critical infrastructure.

Identification and Labeling of Synthetic Content: The EO calls for strengthening the integrity and traceability of digital content amidst the rise of AI-generated synthetic media. The Secretary of Commerce, with input from other agencies, is tasked to report on and then develop guidance for standards and techniques for authenticating and tracking digital content's provenance, labeling synthetic media, and detecting AI-generated content. This includes preventing the misuse of AI in creating harmful materials. Subsequently, the Office of Management and Budget (**"OMB"**), in consultation with various department heads, will issue directives for labeling and verifying government-produced digital content to bolster public trust. The Federal Acquisition Regulatory Council is instructed to consider revising acquisition regulations in line with these new guidelines, ensuring that government procurement aligns with the practices of digital content authentication and synthetic content management.

Defense Protection Act: The EO issues new requirements directly applicable to businesses developing or demonstrating an attempt to develop so-called "dual-use foundation models" that have the potential to impact national security, including national economic security and public health or that are in possession of so-called "large-scale computing clusters." In doing so, the EO relies on the Defense Production Act, as amended, 50 U.S.C. § 4501 *et seq.*, which provides the President with authority to influence industry in the interest of national defense. The Secretary of Commerce in consultation with the Secretaries of State, Defense and Energy and the Director of National Intelligence are required to define the set of technical conditions for the models and computing clusters that would make them subject to these requirements. Prior to that time, the terms are defined with reference to a degree of computing capacity that is unlikely to impact most businesses outside of some of the largest cloud computing vendors or AI-models. However, because the requirements will apply during the development and acquisition stage, businesses should be mindful of whether their activities could meet these thresholds.

Businesses developing "dual-use foundation models" are required to make reports regarding their planned activities related to development and production, including the cybersecurity protections taken to protect the integrity of the training process. They must also report on the ownership and protection of model weights and the results of relevant AI red-team testing. Companies acquiring large-scale computing clusters are required to report these acquisitions, the location of the clusters and amount of total computing power.

The EO will also add a "Know Your Customer" requirement applicable to certain Infrastructure as a Service (**"IaaS"**) Providers. The Secretary of Commerce is required to make regulatory proposals to ensure that IaaS Providers report when freeing entities use their services. Moreover, these regulations will demand verification of foreign persons' identities by resellers of U.S. IaaS Products and ensure compliance with cybersecurity best practices to mitigate the misuse of American IaaS Products by foreign malicious cyber actors.

The Secretary of Commerce is further mandated to engage with various sectors via a public consultation within 270 days to evaluate the implications of making dual-use AI foundation

models with accessible weights widely available, focusing on the potential security risks, such as the disabling of built-in safeguards, alongside the benefits to AI innovation. The input will guide a comprehensive report to the President, assessing the balance of risks and benefits, and shaping policy and regulatory recommendations for managing dual-use AI models whose weights are broadly distributed.

Equity and Civil Rights

While not establishing specific new rules, the EO instructs the Attorney General, in cooperation with other agencies, to use existing federal laws and authorities to address civil rights and discrimination related to the use of AI. The EO specifically calls for the Civil Rights Division to convene within 90 days to discuss the comprehensive use of agency authorities to address discrimination in the use of automated systems, including algorithmic discrimination. The Biden administration has paid particular attention to the risks around AI-influenced discrimination, so this should not come as a surprise. In April, for example, the Consumer Financial Protection Bureau (**"CFPB"**), Federal Trade Commission (**"FTC"**), Equal Employment Opportunity Commission (**"EEOC"**) and other federal agencies issued a Joint Statement on Enforcement Efforts Against Discrimination and Bias in Automated Systems. The EO reenforces the focus that agencies are likely to place around these issues, heightening the risk of enforcement. In addition, the EO gives specific instructions around the use of AI in areas like criminal justice and government benefits.

Privacy

Following on the Blueprint's concerns around the potential for AI to exacerbate privacy risks, the EO includes measures to enhance privacy protections. The Director of the OMB is tasked with multiple initiatives aimed at addressing privacy risks. These include evaluating and potentially revising the processes for how agencies handle commercially available information that contains personal data, which may be directly purchased or procured through third-party vendors. There is a specific call for the Director of OMB to issue a Request for Information (**"RFI"**) to review the effectiveness of privacy impact assessments under the E-Government Act of 2002 and consider potential enhancements in light of AI's capabilities. The Director is also instructed to take necessary steps informed by the RFI to update guidance and collaborate with other agencies and the Federal Privacy Council as required.

Notably, the EO would direct further federal resources toward the development of PETs. To further support the advancement and implementation of PETs, the Director of the National Science Foundation (**"NSF"**), in collaboration with the Secretary of Energy, is directed to establish a Research Coordination Network (**"RCN"**) to foster communication and collaboration among privacy researchers, especially in the development and scaling of PETs. The NSF Director will also identify opportunities for incorporating PETs into agency operations and prioritize research that propels the adoption of PETs across agencies. Moreover, the NSF will utilize insights from the US-UK PETs Prize Challenge to guide the research and adoption strategies for PETs.

Promoting Innovation

The EO order includes a number of initiatives designed to foster innovation of new AI-related technologies. These include efforts to attract talent through streamlined immigration procedures. Additionally, the EO includes a number of instructions related to intellectual property (**"IP"**) rights and ownership. The Under Secretary of Commerce for Intellectual Property and Director of the USPTO is instructed to provide guidance to patent examiners and applicants on issues of inventorship in the context of AI within 120 days. This guidance is expected to include examples illustrating the various roles AI may play in the inventive process and how inventorship should be determined in such cases. Further guidance will be issued within 270 days to address broader considerations at the intersection of AI and IP law, which could involve updated guidelines on patent eligibility concerning AI innovations.

Additionally, the USPTO Director is expected to consult with the Director of the United States Copyright Office and make recommendations to the President on executive actions relating to copyright issues raised by AI, subsequent to the publication of a study by the Copyright Office. To combat AI-related IP risks, the Secretary of Homeland Security, via the Director of the National Intellectual Property Rights Coordination Center and in consultation with the Attorney General, is to develop a training, analysis, and evaluation program. This program will include dedicated personnel for handling reports of AI-related IP theft, coordinating enforcement actions where appropriate, and sharing information with other agencies and stakeholders. Guidance and resources will be provided to the private sector to mitigate AI-related IP theft risks, and information will be shared to help AI developers and law enforcement identify and deal with IP law violations, as well as to develop mitigation strategies. This initiative is part of a broader update to the Intellectual Property Enforcement Coordinator Joint Strategic Plan to encompass AI-related issues.

Industry-Specific Impacts Including Health Care

The EO includes a number of initiatives focused on particular industries. For example, the Secretary of the Treasury is required to issue, within 150 days, a public report on best practices for financial institutions in managing AI-specific cybersecurity risks.

In particular, the EO focuses on risks in the health care industry, given the significant opportunities and also risks around the use of AI for diagnoses and treatment. The Secretary of Health and Human Services (**"HHS"**), in collaboration with other key departments, is directed to establish an AI task force within 90 days of the order. This task force is to create a strategic plan within a year, focusing on the deployment and use of AI in health care delivery, patient experience, and public health. The plan will address several critical areas, including the development and use of AI for predictive purposes, safety and performance monitoring, incorporating equity principles to prevent bias, ensuring privacy and security standards, and developing documentation for appropriate AI uses. Strategies will also be formulated to work with state and local agencies, advance positive AI use cases, and promote workplace efficiency. Furthermore, within 180 days, HHS is to develop AI performance evaluation policies and strategies to assess AI-enabled technologies in health care for quality maintenance, including pre-market assessment and post-market oversight. HHS will also consider actions to ensure understanding of and compliance with federal nondiscrimination laws in relation to AI. Within a year, an AI safety program is to be established, providing frameworks to identify and capture clinical errors from AI use and disseminating recommendations to avoid such harms. Finally, a strategy will be developed for regulating the use of AI in drug-development processes,

identifying needs for new regulations or authority, resources, and potential partnerships, and addressing risks related to AI.

Conclusion

The EO sets a number of deadlines for agencies to issue new guidance and regulations, and so additional significant developments in the coming months should be expected. Already, the OMB has issued draft guidance for federal agencies following the issuance of the EO. The OMB guidance directs each federal agency to designate a Chief AI Office (**"CAIO"**) and requires some agencies to develop a specific AI strategy. CAIOs are tasked with coordination around the agency's use of AI, promoting innovation and managing risk. Similarly, the EO anticipates a number of multilateral initiatives, tasking the Secretary of State and others with leading efforts to establish strong international frameworks around AI risks.

With that said, many issues addressed in the EO order may require legislative action—the fact sheet accompanying the EO notably calls on Congress to adopt federal privacy legislation, for example. While the EO will have direct impact on the federal government, in most cases it does not require specific industry actions. The Biden Administration has demonstrated a clear focus on guiding the development and secure use of AI technologies, however, and is likely to use the considerable resources of the federal government to push forward these initiatives through future agency regulation and enforcement.

Definitions.

For purposes of the 10/30/23 EO on AI:

(a) The term "agency" means each agency described in 44 U.S.C. 3502(1), except for the independent regulatory agencies described in 44 U.S.C. 3502(5).

(b) The term "artificial intelligence" or "AI" has the meaning set forth in 15 U.S.C. 9401(3): a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Artificial intelligence systems use machine- and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action.

(c) The term "AI model" means a component of an information system that implements AI technology and uses computational, statistical, or machine-learning techniques to produce outputs from a given set of inputs.

(d) The term "AI red-teaming" means 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. Artificial Intelligence red-teaming is most often performed by dedicated "red teams" that adopt 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.

(e) The term "AI system" means any data system, software, hardware, application, tool, or utility that operates in whole or in part using AI.

(f) The term "commercially available information" means any information or data about an individual or group of individuals, including an individual's or group of individuals' device or location, that is made available or obtainable and sold, leased, or licensed to the general public or to governmental or non-governmental entities.

(g) The term “crime forecasting” means the use of analytical techniques to attempt to predict future crimes or crime-related information. It can include machine-generated predictions that use algorithms to analyze large volumes of data, as well as other forecasts that are generated without machines and based on statistics, such as historical crime statistics.

(h) The term “critical and emerging technologies” means those technologies listed in the February 2022 Critical and Emerging Technologies List Update issued by the National Science and Technology Council (NSTC), as amended by subsequent updates to the list issued by the NSTC.

(i) The term “critical infrastructure” has the meaning set forth in section 1016(e) of the USA PATRIOT Act of 2001, 42 U.S.C. 5195c(e).

(j) The term “differential-privacy guarantee” means protections that allow information about a group to be shared while provably limiting the improper access, use, or disclosure of personal information about particular entities.

(k) The term “dual-use foundation model” means 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, 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 of those matters, such as by:

(i) substantially lowering the barrier of entry for non-experts to design, synthesize, acquire, or use chemical, biological, radiological, or nuclear (CBRN) weapons;

(ii) enabling powerful offensive cyber operations through automated vulnerability discovery and exploitation against a wide range of potential targets of cyber attacks; or

(iii) permitting the evasion of human control or oversight through means of deception or obfuscation.

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.

(l) The term “Federal law enforcement agency” has the meaning set forth in section 21(a) of Executive Order 14074 of May 25, 2022 (Advancing Effective, Accountable Policing and Criminal Justice Practices To Enhance Public Trust and Public Safety).

(m) The term “floating-point operation” means any mathematical operation or assignment involving floating-point numbers, which are a subset of the real numbers typically represented on computers by an integer of fixed precision scaled by an integer exponent of a fixed base.

(n) The term “foreign person” has the meaning set forth in section 5(c) of Executive Order 13984 of January 19, 2021 (Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities).

(o) The terms “foreign reseller” and “foreign reseller of United States Infrastructure as a Service Products” mean a foreign person who has established an Infrastructure as a Service Account to provide Infrastructure as a Service Products subsequently, in whole or in part, to a third party.

(p) The term “generative AI” means the class of AI models that emulate the structure and characteristics of input data in order to generate derived synthetic content. This can include images, videos, audio, text, and other digital content.

(q) The terms “Infrastructure as a Service Product,” “United States Infrastructure as a Service Product,” “United States Infrastructure as a Service Provider,” and “Infrastructure as a Service Account” each have the respective meanings given to those terms in section 5 of Executive Order 13984.

(r) The term “integer operation” means any mathematical operation or assignment involving only integers, or whole numbers expressed without a decimal point.

(s) The term “Intelligence Community” has the meaning given to that term in section 3.5(h) of Executive Order 12333 of December 4, 1981 (United States Intelligence Activities), as amended.

(t) The term “machine learning” means a set of techniques that can be used to train AI algorithms to improve performance at a task based on data.

(u) The term “model weight” means a numerical parameter within an AI model that helps determine the model’s outputs in response to inputs.

(v) The term “national security system” has the meaning set forth in 44 U.S.C. 3552(b)(6).

(w) The term “omics” means biomolecules, including nucleic acids, proteins, and metabolites, that make up a cell or cellular system.

(x) The term “Open RAN” means the Open Radio Access Network approach to telecommunications-network standardization adopted by the O-RAN Alliance, Third Generation Partnership Project, or any similar set of published open standards for multi-vendor network equipment interoperability.

(y) The term “personally identifiable information” has the meaning set forth in Office of Management and Budget (OMB) Circular No. A-130.

(z) The term “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. This is also sometimes referred to as “privacy-preserving technology.”

(aa) The term “privacy impact assessment” has the meaning set forth in OMB Circular No. A-130.

(bb) The term “Sector Risk Management Agency” has the meaning set forth in 6 U.S.C. 650(23).

(cc) The term “self-healing network” means a telecommunications network that automatically diagnoses and addresses network issues to permit self-restoration.

(dd) The term “synthetic biology” means a field of science that involves redesigning organisms, or the biomolecules of organisms, at the genetic level to give them new characteristics. Synthetic nucleic acids are a type of biomolecule redesigned through synthetic-biology methods.

(ee) The term “synthetic content” means information, such as images, videos, audio clips, and text, that has been significantly modified or generated by algorithms, including by AI.

(ff) The term “testbed” means a facility or mechanism equipped for conducting rigorous, transparent, and replicable testing of tools and technologies, including AI and PETs, to help evaluate the functionality, usability, and performance of those tools or technologies.

(gg) The term “watermarking” means the act of embedding information, which is typically difficult to remove, into outputs created by AI — including into outputs such as photos, videos, audio clips, or text — for the purposes of verifying the authenticity of the output or the identity or characteristics of its provenance, modifications, or conveyance.