November 9, 2023

Key Provisions and Impacts of Biden's Executive Order on AI Regulation and Development

By: Vejay Lalla , Stuart P. Meyer , Zohra Tejani , David L. Hayes , Adine Mitrani , Alberto Tohme

On October 30, 2023, the Biden administration issued a sweeping Executive Order on the Safe, Secure and Trustworthy Development and Use of Artificial Intelligence (the "Executive Order"), which ambitiously directs the development of new guidelines, reports and governance structures relating to the development and deployment of AI. Because the Executive Order is technically quite dense, an associated fact sheet provides a more accessible way to understand its key principles.

The Executive Order is a binding legal order that directs numerous government agencies to investigate and promulgate policies and initiatives to harness the power of AI for the benefit of both citizens and key governmental priorities. The order is also a continuation of several efforts by the Biden administration to establish the groundwork for AI regulation aimed at consumer protection, including privacy and security safeguards, together with the creation of a Blueprint for an AI Bill of Rights and related executive actions announced last year, the development of the AI Risk Management Framework, and, most recently, the hosting of an AI-focused week in Washington during September

2023 that brought together policymakers, industry leaders and experts to exchange ideas and collaborate on shaping AI regulation.

Here, we summarize notable provisions of the Executive Order and provide some perspective on how the Executive Order may impact our clients:

1. Development of Guidelines and Reporting Requirements.

a. <u>Safety Guidelines</u>: The Executive Order directs the National Institute for Standards and Technology ("NIST") in coordination with other relevant agencies to establish guidelines and best practices for developing and deploying safe, secure and trustworthy AI systems within 270 days of the Executive Order, including guidelines applicable to generative AI models and "dual-use foundation models." As detailed below, the Executive Order requires certain companies to submit ongoing reports to the federal government against the guidelines established by NIST, thus effectively thrusting NIST – a non-regulatory agency – into a regulatory role. While industry generally has been in favor, or at least accepting, of such a requirement, it did not take long before some contrary voices were heard. For example, by November 2, 2023, a number of investors, representatives of smaller AI industry players and academics sent a letter to President Biden expressing concern that the approach presented in the Executive Order favored established large players and instead urging "a balanced approach that fosters innovation and prevents market consolidation,"

including by encouragement and support of open-source AI models accessible to all.

b. <u>Reporting Requirements</u>: The Department of Commerce must almost immediately (within 90 days) mandate the following:

- Companies developing or demonstrating an intent to develop "dual-use foundation models" must provide information to the federal government on an ongoing basis relating to the development process, physical and cybersecurity measures taken to safeguard the model, model weight ownership, and results of "red-teaming" and safety testing based on guidance from NIST. "Dual-use foundation models" refer to the largest, most capable foundational models that are trained on broad datasets and contain at least tens of billions of parameters (e.g., OpenAI's GPT-4). And "red-teaming" is a method under which a group of individuals, namely hackers, conduct adversarial testing (e.g., by submitting various prompts to an AI model) to detect vulnerabilities and other errors in a technical system.
- Companies or persons possessing large-scale computing clusters must report to the federal government the location of these clusters and the amount of total computing power available in each cluster.

Note that these reporting requirements are based on a minimum threshold of computational power that will likely subject a greater number of entities to such requirements over time as AI models

become more powerful, including small and mid-sized companies.

Further, the Biden administration's reference to "dual-use foundation models" and the Defense Production Act indicates a national security-centered approach to AI regulation. The largest, most capable foundational models are referred to as "dual-use" foundation models in the Executive Order to signify systems having both civilian and military applications, even though such models have broad, multiuse capabilities. The Executive Order interestingly invokes the Defense Production Act in directing the Department of Commerce to require companies to regularly submit records and reports to the federal government; the Defense Production Act is typically used only when the government must address emergencies or prioritize resources for national defense or security. Notably, the Executive Order was followed almost immediately by a DoD publication of its 2023 Data, Analytics, and AI Adoption Strategy.

c. CBRN Threats: The Executive Order directs various government agencies to evaluate the potential of AI models to be used for chemical, biological, radiological and nuclear ("CBRN") threats and to provide corresponding regulation, oversight and safety recommendations.

d. Authentication of Synthetic Content: The Executive Order directs the Department of Commerce to identify existing standards and practices relating to the authentication, labeling, testing and detection of synthetic content and develop guidance regarding the use of such

techniques, including watermarking, to protect the American public. The FTC has also weighed in on synthetic content, warning of enforcement for use of such content in a deceptive or misleading manner.

e. <u>Infrastructure-as-a-Service (IaaS) Providers</u>: The Executive Order directs the Department of Commerce to impose certain reporting requirements on U.S. IaaS providers ("IaaS providers"). IaaS providers must report any transaction with a foreign person that involves the training of large AI models which may be used for malicious cyber activities. Additionally, IaaS providers must obtain reports from foreign resellers of their products which detail: (i) the identity of any foreign persons that are party to a transaction with a foreign reseller and (ii) any transaction between a foreign reseller and a foreign person that involves the training of large AI models which may be used for malicious cyber activities. Those reports must be disclosed to the Department of Commerce.

2. Promoting Innovation and Competition.

a. <u>Promoting Innovation:</u> The Executive Order aims to promote innovation in AI in various ways:

- Directing the Departments of State and Homeland Security to attract and retain AI talent in the United States by streamlining visa processing and implementing other measures to support AI professionals.
- Directing the National Science Foundation to strengthen public-private

industry partnerships.

- Directing the U.S. Patent and Trademark Office to publish guidance for patent examiners and patent applicants on AI inventorship and patentable subject matter, and, in consultation with the U.S. Copyright Office, issue recommendations to the president on potential executive actions relating to copyright and AI, including the scope of protection for works produced using AI and the treatment of copyrighted works in AI training. For patent practitioners and filers, this guidance will be helpful in understanding the patentability and enforcement landscape with respect to AI tools and systems. From a copyright standpoint, the Copyright Office has already issued guidance on the lack of copyright protection for certain AI outputs that are generated by AI systems, and courts have recently affirmed a requirement of human authorship based on the 1976 Copyright Act and case law precedent. Reading between the lines, a larger governmental concern regarding intellectual property appears to be aimed at avoiding theft of key intellectual property developments from U.S. businesses by foreign companies or countries and ensuring the U.S. maintains a leading role and competitiveness in this new landscape.

b. Promoting Competition: The Executive Order aims to promote competition in AI by providing financial resources to small businesses in AI. Given these purported financial commitments and that the regulatory goals of the Executive Order were developed in consultation with the most prominent tech companies operating

in the space, however, it appears that at least mid-sized businesses may have slipped outside the Executive Order's zone of focus, even if the smallest players are provided some financial help.

3. Supporting American Workers.

The Executive Order directs the Department of Labor in consultation with other agencies and outside entities to develop and publish a set of principles and best practices for employers to maximize the benefits and mitigate the risks of AI in the labor market.

4. Advancing Equity and Civil Rights.

The Executive Order directs the U.S. Attorney General in coordination with the appropriate government agencies to advance equity and civil rights by:

- Analyzing and providing guidance on the potential use of AI in areas such as the criminal justice system, federal programs, benefits administration and the broader economy to address discrimination and biases.
- Issuing guidance on preventing AI-related biases in hiring, housing markets, consumer financial markets and providing assistance for people with disabilities to ensure equal treatment and access to technology.
- Protecting consumers, patients, passengers and students by using AI to address fraud, discrimination and privacy threats and promote safe, responsible AI deployment in the healthcare, public health, human services, transportation and education sectors.

These directives are consistent with previous guidance issued by the federal government, including: (i) a joint statement from the Equal Employment Opportunity Commission, Department of Justice, Consumer Financial Protection Bureau and Federal Trade Commission in April 2023 that resolved to enforce existing applicable laws and regulations to mitigate the potentially adverse impact of AI systems on civil rights, fair competition, consumer protection and equal employment opportunities and (ii) the White House's Blueprint for an AI Bill of Rights, which outlined five non-binding principles that should guide the development and deployment of AI systems such as protecting individuals from the effects of algorithmic discrimination and safeguarding individual privacy rights.

5. Advancing Federal Government Use of AI.

The Executive Order sets forth the federal government's policy to promote effective and responsible AI usage, innovation, and risk management across federal agencies. The Executive Order and the subsequent Office of Management and Budget ("OMB") draft memo (the "Draft OMB Memo") published on November 3, 2023, indicate the types of requirements expected for federal agencies and the companies that provide AI-based solutions to them. Some highlights include:

- The Draft OMB Memo establishes a set of minimum risk management practices that all federal agencies (except for those in the intelligence community) would be required to implement relating

to "safety impacting AI" and "rights impacting AI." "Safety impacting AI" refers to AI that has the potential to meaningfully impact the safety of human life or well-being, the environment, critical infrastructure or strategic assets or resources, while "rights impacting AI" refers to AI whose output serves as a basis for an action that has a legal or material effect on civil rights, equal opportunities (e.g., equitable access to education, housing or credit) or access to critical resources or services (e.g., healthcare, financial or social services).

- AI vendors can expect documentation requirements to show compliance with the agency's AI risk-related requirements. The level of documentation, verification and process will likely vary based on the agency's AI maturity, type of AI (e.g., dual-use foundation model) and use case. The Executive Order and the Draft OMB Memo emphasize leveraging existing compliance frameworks.

- The Executive Order also highlights the need to strengthen public confidence in the integrity of official U.S. government digital content and directs the consideration of a Federal Acquisition Regulation for guidance on the authentication of synthetic content.

- The Executive Order aims to mitigate the privacy risks posed by AI used by federal agencies by directing OMB to evaluate agency standards and procedures associated with the handling of commercially available information that contains personally identifiable information of Americans.

- In addition to contractual requirements for managing risk, content integrity and privacy, the Draft OMB Memo signals future contractual and regulatory requirements for federal procurement of AI solutions that address alignment with national values and laws, transparency, performance improvement, promotion of competition, interoperability, data value maximization, and responsible procurement of generative AI.

The Executive Order and the Draft OMB Memo do not only address responsible use of AI by federal agencies. Several initiatives would facilitate and promote the federal government's use of AI, including:

- For the adoption of generative AI in the federal government, the Executive Order discourages federal agencies from imposing general bans and instead directs agencies to evaluate and limit usage of such generative AI solutions based on case-by-case risk assessments.
- To facilitate the procurement of AI solutions by federal agencies, the Executive Order directs increased allocation of funding for AI projects via the Technology Modernization Fund, mandates public disclosure of agency AI usage and plans, and directs the prioritization of critical and emerging technologies, starting with generative AI, for the FedRAMP authorization process.

The public may comment on the Draft OMB Memo until December 5, 2023.

6. Ensuring International Cooperation in AI Development and Regulation.

The Executive Order emphasizes the value of a multijurisdictional approach to AI development and regulation in noting that the U.S. will focus on working with international allies, partners and multi-stakeholder entities to establish a robust global framework regarding AI development and regulation and to promote the adoption of voluntary commitments backed by common regulatory principles. To this end, the Executive Order directs the Departments of Commerce and State to establish global technical standards for AI development and use, emphasizing cooperation, coordination and information sharing with key international allies, partners and standards development organizations.

This collaborative approach is consistent with the aims of the EU AI Act and other global initiatives such as the Bletchley Declaration, pursuant to which numerous countries resolved on November 1, 2023, to commit resources to support an internationally inclusive network for scientific research and other collaborations related to the development of "frontier AI systems" which include highly capable general-purpose foundational models as well as more narrowly focused AI systems that pose safety risks due to potential intentional misuse, particularly in areas like cybersecurity, biotechnology and disinformation.

7. Implementation of the Executive Order.

The Executive Order calls for the expansion of the White House Artificial Intelligence Council to drive the implementation of the initiatives outlined in

the Executive Order. The purpose of the White House Artificial Intelligence Council is to coordinate the activities across federal agencies, ensuring effective formulation, development, communication and industry engagement related to AI policies, including those set forth in the Executive Order.

It is important to note that the Biden administration may encounter some of the following challenges in implementing the initiatives outlined in the Executive Order:

- The Executive Order imposes short deadlines and assigns multiple initiatives to various government agencies which will inevitably require government agencies to prioritize certain initiatives over others due to limited financial and personnel resources.
- The Executive Order explicitly states that its implementation is subject to the availability of appropriations; thus, without adequate financial resources, many of its initiatives may not be executed.
- The Executive Order may face legal challenges in addition to the informal criticism that has already arisen, including claims that its initiatives exceed the scope of powers granted to the president under the Constitution or that it otherwise is inconsistent with well-settled legal principles.

Key Takeaways:

- **Prepare for new guidelines and consider whether your company may be subject to reporting requirements**. Companies operating in the AI space should familiarize themselves with the

forthcoming safety guidelines and best practices set forth by NIST and other government agencies. If your company is developing or intending to develop large-scale AI models, especially those that may be considered as "dual-use foundation models" as defined in the Executive Order, understand that you may be subject to ongoing testing and reporting requirements and consider proactively directing resources accordingly. Please reach out to a member of your Fenwick team if you are unsure whether you may be subject to the reporting requirements.

- **Leverage opportunities for innovation, competition and workforce development.** Consider taking advantage of the incentives and support outlined in the Executive Order, such as streamlined visa processing for AI professionals, strengthened public-private partnerships and funding for small businesses in AI.

- **Enhance your IP and regulatory strategy.** Consider developing a comprehensive internal document detailing your AI use cases and develop policies and mitigation strategies for such use cases from an intellectual property, regulatory and privacy standpoint. To the extent AI is a key driver of a product or suite of products, consider implementing a more formal AI governance program and AI-specific policies that can be provided both to enterprise customers and consumers as applicable.

- **Companies providing AI services to federal agencies should anticipate potential contractual requirements.**

For companies providing or planning to offer commercial AI products to federal agencies, the AI Executive Order and the draft OMB Memo signal possible contractual requirements. Consider proactively (i) analyzing whether your AI offering could have use cases that impact rights or safety and (ii) documenting practices that align to the NIST AI Risk Management Framework and the Blueprint for an AI Bill of Rights.

- **It is unclear whether the initiatives outlined in the Executive Order will be implemented as planned.** The implementation of the initiatives set forth in the Executive Order may face delays due to budgetary constraints or legal challenges. We will keep you apprised of any developments related to the Executive Order; please contract a member of your Fenwick team with any questions or for clarifications.