The President's AI Executive Order: Why should every business know and care about it?

By Natalia Aranovich, Esq. @aranovichlawfirm.com

Disclaimer: This document has undergone revisions with the assistance of an AI-based language model, which provided grammar suggestions.

Introduction

On October 30, 2023 President Biden issued an Executive Order (EO) aimed at establishing a Safe, Secure and Trustworthy Artificial Intelligence. The EO is grounded in principles and priorities built on the Administration's previously released Blueprint for an AI Bill of Rights[1] and the National Institute of Standards and Technology (NIST) AI Risk Management Framework[2]. While the AI EO does not immediately implement new policies or regulations, it signals potential future adjustments concerning AI and mobilizes government agencies to lay the groundwork for a secure AI infrastructure.

The EO represents an initial stride towards the regulation of AI not just within governmental bodies but also across the private sector. It stipulates specific timelines for government agencies to conduct due diligence and generate reports, paving the way for businesses to adopt corresponding guidelines. The document comprises thirteen sections of directives and sets deadlines for more than twenty federal agencies, outlined as follows:

Section 1: Purpose.

Section 2: Policy and Principles.

Section 3: Definitions.

Section 4: Ensuring the Safety and Security of AI Technology.

Section 5: Promoting Innovation and Competition.

Section 6: Supporting Workers.

Section 7: Advancing Equity and Civil Rights.

Section 8: Protecting Consumers, Patients, Passengers, and Students. Section 9: Protecting Privacy.

Section 10: Advancing Federal Government Use of AI.

Section 11: Strengthening American Leadership Abroad.

Section 12: Implementation.

Section 13: General Provisions.

As previously mentioned, the EO is a "call to action" to government agencies to engage in study, research and keep the government apprised of AI's potential risks in various domains such as cybersecurity, employment, healthcare and labeling AI material created by the government. It addresses discrimination and bias in AI usage. Additionally, the EO directs the Small Business Administration (SBA) to facilitate capital access for AI small enterprises for immigration reforms to attract AI talent to the United States.

---

[1] https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf

[2] https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf

The EO extends its reach to the private sector as well, mandating developers of "dual foundation models" to report their training and testing methodologies to the government. It is imperative that businesses stay informed and prepare for the upcoming implementation phase of the EO. This paper aims to alert businesses to the anticipated AI guidelines and what they entail.
In the following sections, we will delineate the key points that businesses should be cognizant of with respect to each section of the EO.

Section 3: Important Definitions for AI businesses in the EO

Section 3 of the Executive Order provides essential definitions that businesses involved with AI should understand. “AI Red-Teaming” and “Dual-Use Foundation Model” are of particular importance, as these terms are specifically directed at the private sector. Below are some key definitions from the EO that are crucial for those in the AI industry to be aware of:

- 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.
- 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.
- 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.
- The term “AI system” means any data system, software, hardware, application, tool, or utility that operates in whole or in part using AI.
- 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.

- 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.
- 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.

Section 4: New Standards for AI Safety and Security - Establishes reporting requirements for AI businesses and Developers through guidance issued by the Department of Commerce.

Ensuring the safety and security of AI technologies is a critical section for AI businesses because it outlines the reporting requirements that they must be adhered to. These requirements, to be followed by businesses, are to be submitted to the Secretary of Commerce. Moreover, the section stipulates that developers of advanced AI systems employing Dual-Use Foundation Models are obligated to disclose safety test results to the government. This necessitates thorough red-team testing prior to any public release, representing a pivotal move to reinforce AI safety and security protocols.

The specific reporting obligations that businesses need to submit to the Department of Commerce remain undefined in the EO and they are yet to be crafted. However, businesses should start to anticipate those guidelines on how to prepare and present these reports, including the details that must be included. This guidance is expected to be issued within a timeframe of 90 to 270 days following the EO’s enactment.

Highlighted below are pertinent segments of the EO to which businesses and AI developers should pay close attention:

- Section 4.1. Establishes that in 270 days of the date of the EO the Secretary of Commerce, acting through the Director of the National Institute Standards and Technology (NIST) in coordination with the Secretary of Energy, the Secretary of the Homeland Security, and the head of other relevant agencies must establish appropriate guidelines (except for AI used as a component of a national security system), including appropriate procedures and processes, to enable developers of AI, especially of dual-use foundation models, to conduct AI red-teaming tests to enable deployment of safe, secure, and trustworthy systems. Here even though the private sector must wait for the Government to establish the appropriate guidelines, businesses that work with “dual -use foundation model” must be prepared to present reports and red teaming tests to make sure the use of AI is safe, secure and trustworthy .
- Section 4.2 (i). Establishes that in 90 days of the date of the EO the Secretary of Commerce shall require Companies developing or demonstrating an intent to develop “dual -use foundation models” to provide the Federal Government, on ongoing basis, with information, reports or records regarding: (i) Companies developing or demonstrating an intent to develop potential dual-use foundation models to provide the Federal Government, on an ongoing basis, with information, reports, or records regarding the following: (A) any ongoing or planned activities related to training, developing, or producing dual-use foundation models, including the

physical and cybersecurity protections taken to assure the integrity of that training process against sophisticated threats; (B) the ownership and possession of the model weights of any dual-use foundation models, and the physical and cybersecurity measures taken to protect those model weights; and (C) the results of any developed dual-use foundation model's performance in relevant AI red-team testing based on guidance developed by NIST pursuant to subsection 4.1(a)(ii) of this section, and a description of any associated measures the company has taken to meet safety objectives, such as mitigations to improve performance on these red-team tests and strengthen overall model security. Prior to the development of guidance on red-team testing standards by NIST pursuant to subsection 4.1(a)(ii) of this section, this description shall include the results of any red-team testing that the company has conducted relating to lowering the barrier to entry for the development, acquisition, and use of biological weapons by non-state actors; the discovery of software vulnerabilities and development of associated exploits; the use of software or tools to influence real or virtual events; the possibility for self-replication or propagation; and associated measures to meet safety objectives.

- Section 4.2. (iii) establishes that Companies, individuals, or other organizations or entities that acquire, develop, or possess a potential large-scale computing cluster to report any such acquisition, development, or possession, including the existence and location of these clusters and the amount of total computing power available in each cluster. This report requirement will be defined by the Secretary of Commerce, in consultation with the Secretary of State, the Secretary of Defense, the Secretary of Energy, and the Director of National Intelligence. Thus, companies who work with large computing clusters must be prepared to make such reports to the government.
- Section 4.2(c) requires US IaaS providers to report when a foreign person uses their services to train an AI model. This report requirement will be established by the Department of Commerce in 90 days of the EO. The term Iaas providers was defined in the EO 13984. Iaas Provider is the short for "Infrastructure as a Service Product" and means any product or service offered to a consumer, including complimentary or "trial" offerings, that provides processing, storage, networks, or other fundamental computing resources, and with which the consumer is able to deploy and run software that is not predefined, including operating systems and applications. The consumer typically does not manage or control most of the underlying hardware but has control over the operating systems, storage, and any deployed applications. The term is inclusive of "managed" products or services, in which the provider is responsible for some aspects of system configuration or maintenance, and "unmanaged" products or services, in which the provider is only responsible for ensuring that the product is available to the consumer. The term is also inclusive of "virtualized" products and services, in which the computing resources of a physical machine are split between virtualized computers accessible over the Internet (e.g., "virtual private servers"), and "dedicated" products or services in which the total computing resources of a physical machine are provided to a single person (e.g., "bare-metal" servers).

- Section 4.3. (ii) establishes that in 150 days from the EO the Secretary of Treasury shall issue a public report on best practices for financial institutions to manage AI- specific cybersecurity risks. Financial Institutions must keep an eye on those best practices and make sure that they are using AI in a way that is safe and secure.

Section 5: Promoting Innovation and Competition (Immigration, Intellectual Property, availability of resources to startups and small businesses and employment issues raised by AI).

Section 5 addresses actions that, while mandated for government agencies, will have implications for AI businesses. Those actions include:

- attract AI talent to the US calling for a small immigration reform to facilitate the attraction of foreign nationals with special skills in AI and other critical emerging technologies seeking to work, study, or conduct research in the United States;
- calls for the USPTO to promote innovation and clarify issues related to AI and inventorship of patentable subject matter;
- regarding Copyrights, the EO calls for in 270 the United States Copyright Office to publish its forthcoming AI study that will address copyright issues raised by AI and consult with the Director of the United States Copyright Office and issue recommendations to the President on Potential executive actions relating to copyright and AI;
- in 180 days from the date of the order the USPTO shall create a program to assist developers of AI in combating AI -related risks, and develop in conjunction with the Secretary of Homeland Security and Attorney- General a training, analysis and evaluation program to mitigate AI- related IP risks. Here is addressed one of the main concerns regarding the training of AI models using IP rights of third parties and it will be interesting to see how the USPTO will address these issues. In my article published in Chapter 6 of the book written by Beverly Macy called “From PCs to AI - Pioneering Digital Ownership and Beyond” Beverly and I discussed that a great technology that could be used to avoid IP risks is through the use of blockchain and NFTs. If the IP owner registers his/her/its IP rights in the blockchain and issues a NFT he/she/it will be able to know what part of the work was used to train an AI model and if the work was used in violation of their IP rights; and
- discusses the Small Business Administration's role in supporting small businesses in adopting AI and developing programs for small AI businesses to have access to capital and specific government funding. The Government wants to make sure that small businesses have access to capital and grow in America.

It's crucial for businesses to stay informed about these measures, as they may indirectly shape industry standards and expectations.

Section 6. Supporting workers

Section 6 outlines the procedures that government agencies must undertake, which are poised to influence business operations, particularly in the context of adopting AI tools in place of human employees. The stipulations set forth in this section are as follows:

- the Secretary of Labor shall in 180 days of the date of the order develop and publish principles and best practices for employers that could be used to mitigate AI's potential harms to employees' well being to maximize its potential benefits. Those principles and best practices shall include specific steps for employers to take with regard to AI, and shall cover: (A) job-displacement risks and career opportunities related to AI, including effects on job skills and evaluation of applicants and workers; (B) labor standards and job quality, including issues related to the equity, protected-activity, compensation, health, and safety implications of AI in the workplace; and (C) implications for workers of employers' AI-related collection and use of data about them, including transparency, engagement, management, and activity protected under worker-protection laws.

Section 7. Advancing Equity and Civil Rights (algorithmic discrimination)

Section 7 of the EO emphasizes that AI technologies reflect the principles and biases of their creators, which necessitates careful oversight. Although Section 7 primarily details actions to be taken by government agencies, it is noteworthy for businesses to consider the government's concern regarding algorithmic discrimination in AI applications.

This section explicitly addresses the implications of AI in the real estate sector, with a focus on tenant screening systems. It underscores the potential for discriminatory practices if these systems are not designed and used with consideration for fairness and inclusivity.

Therefore, while the immediate directives of this section are for government agencies, the broader implications are clear: businesses involved in developing or utilizing AI, particularly in sensitive areas like real estate, must be vigilant about the ethical construction and deployment of these technologies to prevent bias and discrimination.

Section 8. Protecting Consumers, Patients, Passengers and Students

This section addresses the use of AI in the healthcare industry, transportation and in education. The Government is concerned that the data analisis made by AI is accurate.

Section 09. Protecting Americans' Privacy

The order acknowledges AI's potential privacy risks and calls for bipartisan data privacy legislation. It emphasizes the development of privacy-preserving techniques, safeguarding personal data while fostering AI innovation.

Section 9 of this Executive Order focuses on the protection of privacy in relation to the use of artificial intelligence (AI).

The Section is divided into two parts. Part (a) aims to mitigate potential privacy risks exacerbated by AI. It tasks the Director of the Office of Management and Budget (OMB) with several responsibilities, including evaluating and identifying commercially available information (CAI) that contains personally identifiable information, consulting with other agencies to assess privacy and confidentiality risks, issuing a Request for Information (RFI) for possible revisions to privacy provisions of the E-Government Act of 2002, and advancing near-term actions and long-term strategy identified through the RFI process. Parts (b) and (c)

outline steps to advance research, development, and implementation related to Privacy Enhancing Technologies (PETs). Within a year, the Secretary of Commerce, via the Director of the National Institute of Standards and Technology (NIST), shall create guidelines for agencies to assess the efficacy of differential-privacy-guarantee protections for AI. Furthermore, the Director of the National Science Foundation (NSF) shall create a Research Coordination Network (RCN) for advancing privacy and PETs research, engage with agencies to identify potential opportunities to incorporate PETs into their operations, and use the results of the United States-United Kingdom PETs Prize Challenge to inform PETs research and adaptation.

Section 10. Advancing Federal Government use of AI (labeling requirements for the AI content generated by Government)

In Section 10, the EO acknowledges the government's intention to utilize artificial intelligence, contingent upon the establishment of appropriate security measures. The order calls for the development of specific guidance to the Federal workforce's use of generative AI. It also states that the government should take prudent measures to watermark any generative AI-generated content to clearly indicate its origin.

Furthermore, the EO advises against the imposition of prohibitions on the use of generative AI within government agencies. It highlights that as generative AI technologies become increasingly prevalent and integrated into online platforms, agencies should avoid enacting policies that broadly prevent their use but must use it in a safe manner.

This guidance reflects a nuanced approach, promoting the responsible adoption of AI while acknowledging its growing role in digital communications and content creation. It is a clear indication that the government recognizes the potential of generative AI and seeks to balance innovation with necessary safeguards

CONCLUSION

In conclusion, the EO is an extensive document spanning 63 pages, detailing the multifaceted use of AI across various governmental sectors including immigration, workforce, intellectual property, healthcare, and more. While the EO itself is not directly legally binding for business, it serves as a precursor to the comprehensive regulation of AI across all industries that we shall see in the near future. In anticipation of these developments, businesses must proactively prepare to adhere to the EO's directives within the next year. It is imperative for companies to establish internal policies and guidelines that govern the use of AI by their employees to ensure compliance and readiness for the upcoming regulatory environment.