White House Issues Sweeping Executive Order on AI: Key Takeaways

DECEMBER 20, 2023

Key Takeaways

- President Biden's recent Executive Order on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence:
  - Establishes a federal government-wide effort to mitigate risks of improper AI development and use.
  - Calls on several federal agencies to prepare reports and generate guidance on the use of AI.
  - Sets forth a number of privacy and cybersecurity considerations to attempt to mitigate AI's potential threats to personal data.
  - Provides authority to the Secretary of Commerce to mandate reporting on AI models with potential national security implications.
  - Requires that guidelines for "red-teaming" tests be established to ensure that AI systems are safe, secure, and trustworthy.

Introduction

President Biden issued an Executive Order on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (AI) on October 30, 2023 (Order). The Order states that it seeks to create a broad framework for the "responsible use of AI" by establishing policies that ensure proper use of AI while mitigating harms that may affect national security and Americans, including "fraud, discrimination, bias, and disinformation."[1] The Order builds upon the foundation established in the Blueprint for an AI Bill of Rights and the AI Risk Management Framework.[2] The enhanced approach establishes a federal government-wide effort to mitigate risks of improper AI development and use. The effort calls on federal agencies and executive departments to tailor their implementation of "responsible AI use" based on eight guiding principles set forth in the Order:

- AI must be safe and secure.
- AI policies and development must protect Americans' privacy.
- AI must be dedicated to advancing equity and civil rights.
- AI policies and development must protect the interests of American consumers, patients and students.
- AI developments must support American workers.
- AI must promote responsible innovation and competition.
- The federal government should lead the way to global societal, economic, and technical progress and ensure that American is acting as a leader to support safe, secure and trustworthy deployment of AI around the world.
- AI policies must manage risks of the federal government's use of AI.

The Order authorizes federal agencies to regulate AI development by private companies, directs them to review and test federal agencies' internal development and use of AI and highlights national security implications that must be taken into consideration. A White House AI Council (Council) established by

the Order will oversee the Order's implementation and coordinate activities across federal agencies.[3] Federal agencies are required to implement actions established by the Order between 30 and 365 days of the Order's release.

In addition to applying directly to federal agencies, the Order also outlines requirements that affect private companies using "dual-use foundation models" and that meet certain other criteria outlined in the Order.[4]

The Order aims to regulate AI use in critical fields, such as cybersecurity, healthcare, financial services, education, housing law and transportation.

Financial Institutions

An overarching theme of the Order is the trustworthiness of AI. The Order calls on several agencies whose regulations affect financial institutions to prepare reports or generate guidance on the use of AI. For example, the Order calls on the Secretary of the Department of the Treasury to issue a "public report on best practices for financial institutions to manage AI-specific cybersecurity risks" within 150 days of the Order's release.[5] Actions taken by agencies pursuant to the order will affect financial institutions.

Financial Services

The sweeping effects of the Order will impact financial services firms, some of which use natural language processing to analyze and synthesize large volumes of data in their day-to-day operations. The data is used to create internal workflow efficiencies, tailor marketing strategies, and aid product development. In addition, many investment advisers and asset managers are considering or deploying various uses of generative AI in the investment, analysis and research processes and in preparing investor communications.

Although the Securities and Exchange Commission (SEC) is not called to a particular action by the Order, the agency is "encouraged to…consider using [its] full range of authorities" to either propose and implement regulations that will address fraud, discrimination, threats to privacy and other risks that may arise from the implementation of AI by financial services institutions or clarify existing regulations and guidance application to AI. The SEC is likely to view the Order as encouraging its already assertive rulemaking and examinations agenda relating to predictive data analytics and generative AI.

In addition to regulating AI use by financial services institutions, the SEC will also need to evaluate its internal development and use of AI, in accordance with the Order.

Civil Rights and Consumer Protection in Financial Products

AI is already used in many facets of the consumer financial industry. Lenders have come to rely on AI in connection with advertising, underwriting, credit decisions, pricing, risk mitigation, fraud detection, product development, regulatory compliance and general operational efficiency. The Order endeavors to regulate such uses of AI so that it is leveraged in a fair and transparent manner and does not violate the civil rights of Americans or perpetuate unintended bias or discrimination.

The Order seeks to start a conversation around the comprehensive use of automated systems, including AI, for the prevention, identification, investigation and prosecution of discrimination (including algorithmic discrimination) and other civil rights violations in the context of lending, housing and other consumer financial products .[6] Regulators will have to evaluate these concerns not only in the context of the AI algorithms but also in the data sets that are used to train them.

In addition to lending and the consumer financial markets generally, the Order is also focused on ensuring that the use of AI does not lead to discrimination in housing, whether in the context of access to housing, unfair rent setting, use of data for background checks or even how potential housing opportunities are marketed to consumers. Private companies are encouraged to ensure their AI tools are in compliance with all applicable laws, by, among other things, evaluating underwriting models for bias or disparities affecting protected groups and evaluating automated collateral-valuation and appraisal processes in ways that minimize bias.

Privacy and Cybersecurity

The protection of personal data is one of the guiding principles and priorities of the Order and, noting that "[w]ithout safeguards, AI can put Americans' privacy further at risk,"[7] the Order sets forth a number of privacy and cybersecurity considerations to attempt to mitigate AI's potential threats to it.

For example, the Order requires the Director of the Office of Management and Budget to: (1) evaluate and take steps to identify commercially available information procured by agencies, including such information that contains personal information and/or information procured from data brokers and vendors; (2) evaluate agency standards and procedures associated with the collection, processing, maintenance, use, sharing, dissemination and disposition to inform potential guidance to agencies on ways to mitigate privacy and confidentiality risks from agencies' activities related to relating to such information; and (3) issue a request for information to inform potential revisions to guidance to agencies on implementing the privacy provisions of the E-Government Act of 2002 seeking feedback regarding how privacy impact assessments may be more effective at mitigating privacy risks, including those that are further exacerbated by AI.

The Order further instructs the Secretary of Commerce, acting through the Director of the National Institute of Standards and Technology (NIST), to create guidelines for agencies to evaluate the efficacy of differential-privacy-guarantee protections, including for AI. These guidelines must describe the significant factors that bear on differential-privacy safeguards and common risks to realizing differential privacy in practice. Further, the Order requires the Director of the National Science Foundation, in collaboration with the Secretary of Energy, to fund, coordinate and implement privacy research.

In addition, the Order urges Congress to pass comprehensive federal data privacy and cybersecurity law. Privacy and cybersecurity practitioners have been waiting for such legislation for years and, given recent partisan gridlock, this is unlikely to happen in the coming years. Further, the Order recommends that the Federal Trade Commission (FTC) use its rulemaking authority "to ensure fair competition in the AI marketplace and to ensure that consumers and workers are protected from harms that may be enabled by the use of AI." Moreover, the Order encourages the private sector to examine and take measures related to its development and use of AI that dovetail with the policy positions in the Order.

Cybersecurity considerations underlie almost every section of the Order, and the White House requires the implementation of certain standards by various agencies regarding the sharing of personal data. For example, the Secretary of Commerce must issue certain reporting requirements by late January 2024 regarding reporting requirements for companies that power dual-use foundation models. These reporting requirements include: (1) the physical and cybersecurity protections taken to assure the integrity of that training process against sophisticated threats; (2) the ownership and possession of the model weights of any dual-use foundation models; and (3) the physical and cybersecurity measures taken to protect those model weights. These reporting requirements must also include the results of any developed dual-use foundation model's performance in relevant AI red-team testing based on guidance developed by NIST.

In addition, within this same timeframe, the Secretary of Commerce must also propose regulations for foreign nationals who train certain AI models with potential capabilities that could be used in malicious cyber-enabled activity prior to their access to United States infrastructure as a service.

In addition, the Order requires the Secretary of Homeland Security to execute a number of tasks, which include: (1) issuing a public report on best practices for financial institutions to manage AI-specific

cybersecurity risks by late February 2024; and (2) incorporating as appropriate the AI Risk Management Framework, NIST AI 100-1, as well as other appropriate security guidance, into relevant safety and security guidelines for use by critical infrastructure owners and operators by late March 2024.

AI and National Security Objectives

The Order serves as another way for the Biden Administration to achieve its national security goals with respect to AI, and national security considerations are among the most prominent in the Order. As detailed in the Biden Administration's National Security Strategy last year (which we discussed here), the U.S. Government is committed to U.S. advancement in the technology sector so the United States may remain competitive and enhance its security, which includes building trustworthy artificial intelligence. To this end, the Order consistently seeks AI risk mitigation as a primary objective in the context of national security and critical infrastructure. To remain apprised of national security risks arising from AI, and as discussed above, the Order provides authority to the Secretary of Commerce to mandate reporting on AI models with potential national security implications.[8]

Commerce, in consultation with other agencies, must adopt certain standards and tools to protect against AI systems that could pose threats to critical infrastructure, nuclear capabilities, nonproliferation and other key national security areas. The protection of critical infrastructure is an ongoing national security objective, and the Secretary of Commerce is tasked with developing tools, like AI testbeds, to assess potential risks arising from AI. Based on the Order, relevant agencies with authority over critical infrastructure, as well as other stakeholders, will provide to the Department of Homeland Security an annual[9] assessment of cross-sector risks and vulnerabilities related to the use of AI in critical infrastructure sectors.

The Order also directs certain officials to oversee an interagency process regarding AI and national security risks. Specifically, the Order authorizes the Assistant to the President for National Security Affairs and the Assistant to the President and Deputy Chief of Staff for Policy to oversee an interagency process to develop and submit a "National Security Memorandum on AI" to the President. The purpose of the memorandum is to address, among other things, AI as a component of national security as well as potential national security risks and benefits arising from AI. Moreover, the memorandum will seek to direct continued action and address how AI systems may be used by adversaries and other foreign actors in ways that could undermine the intelligence community or the United States and its allies more broadly. The memorandum will likely serve as a first step toward a broader initiative to tackle AI in the national security context.

Red-Teaming Testing Regulation

With the goal of promoting the safe and secure implementation of AI, the Order calls on the Director of NIST to establish guidelines and industry standards for AI systems within 270 days of the date of the Order. In particular, the Order requires that NIST establish guidelines for "red-teaming" tests to ensure that AI systems are safe, secure and trustworthy. AI red-teaming is "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."[10] The AI red-teaming testing guidelines are intended to focus especially on dual-use foundation models and will be required to address (i) safety, security and trustworthiness assessments of dual-use foundation models and (ii) the development of testing environments to "support the development, of safe, secure, and trustworthy AI."[11]

The Order also calls on the Secretary of Commerce to ensure the protection of critical infrastructure and national security. As noted above, the Secretary of Commerce can mandate reporting on AI models, which includes reporting on "results of any developed dual-use foundation model's performance in relevant AI red-team testing."[12] Testing results shared with the Secretary of Commerce are required to address testing conducted related to (i) "lowering the barrier to entry for the development, acquisition, and use of biological weapons by non-state actors;" (ii) "the discovery of software vulnerabilities and development of associated exploits;" (iii) the use of software or tools to influence real or virtual events;" (iv) the possibility for self-replication or propagation;" and (v) "associated measures to meet safety objectives."[13]

The red-teaming testing requirements are expressly intended to ensure that AI developers identify vulnerabilities within AI models, giving developers the opportunity to mitigate national security and privacy concerns. In addition, these requirements could be intended to establish red-teaming as a broader industry practice.

Conclusion

Although the Order itself does not contain new regulations or mandates on AI, the directives to federal agencies contained in the Order demonstrate the seriousness with which the Biden Administration is taking this generational shift in technology and business practices. Further emphasizing this point, on December 14, 2023, the Financial Stability and Oversight Council's (FSOC) annual report highlighted potential vulnerabilities in the U.S. financial system that may result from AI use, noting that "existing requirements and guidance may apply to AI."[14] In SEC Chair Gary Gensler's comments to the FSOC, he stated that although AI will "create great efficiencies across the economy," current regulatory guidance is insufficient.[15] Gensler further noted that future guidance and regulation will require a cross-agency approach.[16] In addition to U.S. regulation, the European Parliament and Council released the Artificial Intelligence Act, which will create a comprehensive AI framework in the European Union.[17]

The result will surely be a flurry of additional regulations, rulemaking and hearings over the coming year as regulators and lawmakers look to exercise leadership and influence in this developing arena. Industry participants will have to carefully monitor developments and regulations in their respective regulatory areas as they are announced and consider how to adopt best practices to ensure they maintain compliance with federal laws and guidance.

Footnotes

1. Exec. Order No. 14110, 88 Fed. Reg. 75191 (Oct. 30, 2023) (hereinafter "Order")

2. *See generally* WHITE HOUSE OFF. OF SCI. AND TECH. POL'Y, BLUEPRINT FOR AN AI BILL OF RIGHTS (2022); *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* (https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf)

3. The Council will be chaired by the White House Deputy Chief of Staff for Policy and include representatives from each agency.

4. "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." See Order, *supra* note 1.

5. *Id.*

6. *Id.*

7. *FACT SHEET: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence*, White House, https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/ (Oct. 30, 2023).

8. The executive has found its authority to do this under the Defense Production Act, as amended. 50 U. S.C. 4501 *et seq*.

9. The first risk assessment must be provided within 90 days of the Order.

10. Order, supra note 1.

11. *Id.*

12. *Id*.

13 *Id.*

14. Press Release, U.S. Dep't of the Treasury, Financial Stability Oversight Council Releases 2023 Annual Report (Dec. 14, 2023) (https://home.treasury.gov/news/press-releases/jy1991).

15. Gary Gensler, Chairman, Sec. Exch. Comm'n, Remarks before the Financial Oversight Council 2023 Annual Report (Dec. 14, 2023).

16. *Id.*

17. Press Release, Council of the Eur. Union, Artificial intelligence act: Council and Parliament strike a deal on the first rules for AI in the world (Dec. 9, 2023) (https://www.consilium.europa.eu/en/press/press-releases/2023/12/09/artificial-intelligence-act-council-and-parliament-strike-a-deal-on-the-first-worldwide-rules-for-ai/).

Related Professionals

PARTNER

Linda Ann Bartosch

Philadelphia

+1 215 994 2132

PARTNER

Mark D. Perlow

San Francisco

+1 415 262 4530

PARTNER

Brenda R. Sharton

Boston

+1 617 728 7113

PARTNER

Timothy Spangler

Los Angeles

+1 949 442 6044

Silicon Valley

+1 650 813 4803

ASSOCIATE

Keith R. Harden

New York

+1 646 731 6145

ASSOCIATE

Katherine Hurley

Boston

+1 617 728 7126

Related Services

Financial Services and Investment Management
Fintech
Privacy & Cybersecurity
Global Finance

Dechert LLP

Subscribe to Dechert Updates