Westlaw Today
powered by Reuters

Biden's AI executive order has national security, government contractor implications

By Tina Reynolds, Esq., Charles Capito, Esq., Brandon Van Grack, Esq., and Lyle Hedgecock, Esq., Morrison Foerster LLP*

NOVEMBER 29, 2023

The Biden administration issued a widely anticipated executive order on artificial intelligence ("AI") Oct. 30. The Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (the "EO")[1] addresses a multitude of issues reflecting an emerging national policy on AI. This article focuses on those aspects of the EO most directly related to national security and federal procurement.

National security considerations

Generative and other emerging AI applications have myriad implications for U.S. national and global security.

The EO requires that developers of the most powerful AI systems conduct and report the results of safety testing, and share other critical information with the federal government.

The EO seeks to address a few of these.

First, the EO requires that developers of the most powerful AI systems, so-called "dualuse foundational models," conduct and report the results of safety testing, and share other critical information with the federal government. These foundational models implicate national security, economic security, and public health and safety. Companies will also be required to report planned activities in training dual-use AI, developing or producing such systems, and to outline the precautions they are taking during the development process.

The administration invokes the Defense Production Act as the authority for compelling disclosure of this information, much of which will be proprietary. Although several leading AI companies already share such information voluntarily, this provision seeks greater disclosure regarding companies' deployment of AI and the testing and risk assessments underpinning AI models.

This disclosure requirement is related to one of the EO's many agency directives. Specifically, the EO directs the National Institute of Standards and Technology ("NIST") to develop standards to verify that AI systems are safe, secure, and trustworthy, in the form of companion guidance to already-existing NIST publications, such as the AI Risk Management Framework (NIST AI 100-1).[2]

Second, the EO calls for regulations to require U.S. Infrastructure as a Service ("IaaS") providers to report transactions with foreign persons to train large AI models with potential capabilities that could be used in malicious cyber activity. The forthcoming regulations will also require IaaS providers to prohibit foreign resellers from providing services unless they provide details about the end users, end uses, and the underlying applications.

This requirement addresses similar concerns that the Department of Commerce flagged in its October 17, 2023 advanced semiconductor rules concerning cloud-based access to advanced computing and AI training models.

The forthcoming regulations will require IaaS providers to prohibit foreign resellers from providing services unless they provide details about the end users, end uses, and the underlying applications.

Finally, the EO recognizes the potential for misuse of AI in a manner that might allow non-experts to design, synthesize, acquire, or use chemical, biological, radiological, or nuclear ("CBRN") weapons. As such, the EO directs the Department of Homeland Security, in consultation with the Department of Energy and the Office of Science and Technology Policy, private AI laboratories, and academia, to evaluate CBRN threats from AI models and develop means to mitigate these risks.

Various government agencies are also directed to consider what government data might present security risks with respect to CBRN

weapons and to ensure that such data is restricted from public access and not used to train AI systems.

Federal procurement considerations

The EO also includes numerous developments and takeaways for government contractors, as the administration, as it often does, leverages its purchasing power to effect policy goals.

First, the EO provides guidance for the procurement of AI products and services by federal agencies. The EO directs the Office of Management and Budget ("OMB") to specify minimum risk-management practices for governmental use of AI. These requirements include:

(1) establishing a Chief Artificial Intelligence Officer ("CAIO") charged with AI implementation in the agency;

(2) defining the CAIO's roles and responsibilities;

(3) requiring certain agencies to create an AI governance board;

(4) implementing minimum risk management practices;

(5) identifying AI uses that impact individual rights or safety;

(6) recommending ways to reduce barriers to AI use;

(7) requiring certain agencies to develop AI strategies and pursue advantageous use of AI;

(8) external AI testing for generative AI, safeguards preventing discriminatory use or other misuse of AI, watermarking, minimum risk management practices, independent assessment of vendor effectiveness and risk mitigation claims, documentation and oversight of AI, maximizing value of contracted AI services, and incentivizing continuous improvement of AI;

(9) training agency employees on AI; and

(10) public reporting on compliance with these requirements.

Additionally, OMB is tasked with requiring that agencies make sure that any contracts for AI services address: privacy, civil rights, and civil liberty concerns; ownership and security of data; and means to prevent misuse, unauthorized use, or corruption of AI systems.

Second, Section 4.5(d) of the EO directs the Federal Acquisition Regulatory Council to consider amending the Federal Acquisition Regulation ("FAR") to reduce risks posed by "synthetic content" and to require identification of synthetic content produced by AI systems used by the federal government or on its behalf.

The aim is to promote trust in the integrity and authenticity of U.S. government digital content by establishing transparency regarding the provenance of generated content and preventing generation of inappropriate or inaccurate content.

Third, in line with this goal, the EO directs the Secretary of Commerce (in consultation with other agencies) to develop standards, tools, methods, and practices for use by federal government agencies and contractors: (1) to authenticate and track the provenance of AIgenerated material; (2) to label AI content using methods such as "watermarking"; (3) to detect synthetic content; (4) to prevent AI from producing certain abusive, explicit materials, such as nonconsensual, AI-generated representations of real people (i.e., "deepfakes"); to (5) test and (6) audit software for these purposes.

Pending release of this guidance, agencies seeking to obtain AI products or services are required to implement "minimum risk-management practices" defined in Section 10.1(b)(iv). These practices are derived from the White House Office of Science and Technology Policy's Blueprint for an AI Bill of Rights[3] and the NIST AI Risk Management Framework,[4] and they include: (1) public consultation; (2) review of data quality; (3) assessing and mitigating discriminatory impacts from AI; (4) providing notice when an agency employs AI; (5) continuously monitoring and evaluating AI in use; and (6) granting separate, "human" consideration and remedies for adverse decisions made by AI systems.

The EO encourages acceleration of grants to explore transportation-related opportunities and challenges of AI, including regarding software-defined AI enhancements impacting autonomous mobility ecosystems.

Section 7.2 also requires agencies to "use their respective civil rights and civil liberties offices and authorities ... to prevent and address unlawful discrimination and other harms that result from uses of AI in Federal Government programs and benefits administration."

Finally, beyond the directives and proposed regulatory requirements, the EO suggests business opportunities for potential recipients of federal grant and contract funding. It directs the General Services Administration to facilitate government-wide acquisition solutions for AI services and products, thereby creating future consolidated contracting opportunities to provide AI tools to the federal government.

Specifically, the EO encourages acceleration of grants awarded through the National Institutes of Health Artificial Intelligence/ Machine Learning Consortium to Advance Health Equity and Researcher Diversity program and through the Advanced Research Projects Agency-Infrastructure (ARPA-I) to explore transportation-related opportunities and challenges of AI, including regarding software-defined AI enhancements impacting autonomous mobility ecosystems.

The EO also proposes a pilot project to "identify, develop, test, evaluate, and deploy AI capabilities, such as large-language models, to aid in the discovery and remediation of vulnerabilities in critical United States Government software, systems, and networks." It also seeks to promote competition and innovation in the semiconductor industry, by working in concert with the Creating Helpful Incentives to Produce Semiconductors ("CHIPS") Act of 2022 to use AI in the industry and provide other assistance,

particularly for small businesses, and to share data for CHIPS research and development programs.

Next steps and final thoughts

The EO requires implementation in the form of agency-issued guidance and potentially legislation to effectuate some of its more ambitious aspects. Given the EO's tight deadlines, in the coming months we expect to see new agency-level AI policies, as well as requests for information and requests for comments on proposed rules.

IaaS providers and developers of "dual-use" AI should anticipate a roll out of reporting requirements and requests for information. Similarly, government contractors should expect that reporting regarding their AI models may become part of the proposal evaluation and embedded as contract requirements, particularly as it relates to safety of AI products, routine testing for bias, and data security and privacy protections. Contractors should also anticipate requirements for AI transparency and provenance to become a feature in government AI procurement.

Although many of the policy details are still under development, the EO represents the Biden administration's first robust attempt to shape development of the AI industry.

Notes

[1] https://bit.ly/49rDjN2

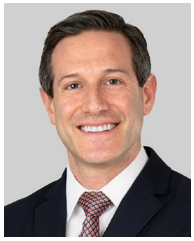
[2] https://bit.ly/3uiaylQ

[3] https://bit.ly/48jLdre

[4] https://bit.ly/3uiaylQ

About the authors






(L-R) **Tina Reynolds**, a partner and co-chair of **Morrison Foerster LLP**'s government contracts and public procurement practice, represents clients in the information technology, defense, biotechnology and pharmaceutical industries with general contract counseling and compliance concerning intellectual property and cybersecurity matters. She can be reached at treynolds@mofo.com. **Charles Capito**, a partner in the firm's national security and government contracts and public procurement practices, counsels clients on the Committee on Foreign Investment in the United States, as well as on compliance and litigation issues. He can be reached at ccapito@mofo.com. **Brandon Van Grack**, a partner and co-chair of the firm's national security and global risk and crisis management groups, focuses on investigations, criminal defense and compliance matters involving sanctions and export controls, foreign investment, and cyber incidents. He can be reached at bvangrack@mofo.com. **Lyle Hedgecock** is an associate in the firm's government contracts and public procurement practice. He previously served as a director for the National Oceanic and Atmospheric Administration Satellite Operations Center. He can be reached at lhedgecock@mofo.com. The authors are based in Washington, D.C. This article was originally published Nov. 3, 2023, on the firm's website. Republished with permission.

This article was published on Westlaw Today on November 29, 2023.