WINSTON & STRAWN LLP

BLOG

"Safe, Secure and Trustworthy Artificial Intelligence:" What the Biden Administration's Latest Executive Order Could Mean for Government Contractors

OCTOBER 31, 2023

On October 30, 2023, President Biden signed an Executive Order regarding "Safe, Secure, and Trustworthy Artificial Intelligence." The administration's goal is to provide a legal and regulatory framework for the largely unregulated world of artificial intelligence (AI) so that the U.S. can reap the benefits of AI while avoiding the pitfalls. This wide-reaching order directs government agencies to promulgate rules, form task forces, and provide guidance on the risks of AI to national security, biological research, data privacy, civil rights, consumer protections, and the ability of workers to bargain collectively. While this order will have a broad impact across the entire economy, government contractors will be particularly impacted in the coming months and years as they are forced to adapt to emerging rules and regulations governing how they can use AI and what forms of AI the government will approve for use on government contracts. This order signals a shift in how federal agencies will operate in the future, and those changes will require contractors to adapt, whether or not they actively use AI in their operations.

REPORTING REQUIREMENTS

Pursuant to this order, President Biden is invoking the Defense Production Act of 1950 (DPA) to require technology developers to reveal information about new AI applications to the federal government. The DPA gives the President authority to provide financial incentives and assistance to ensure that contractors can produce supplies and materials as needed for national defense.[1] President Biden has invoked the DPA on multiple occasions to bolster the clean energy supply chain, encourage DOD investment in defense suppliers, and ensure the U.S. is on the cutting edge with respect to electronic and energy capacity, all in pursuit of strengthening the country's national defense.

Using his authority under the DPA, President Biden is requiring "developers of the most powerful AI systems" to share information with the federal government, such as safety test results and "other critical information" prior to the applications becoming public. It is unclear exactly which companies will be included in this requirement and what data will need to be shared. An administration official told *The Wall Street Journal* that companies would be required to "tell the Commerce Department how they are working to protect their technology from malicious use," and White House aides suggested that these requirements would only apply "to big tech companies' next-generation AI systems, and not current versions."[2]

STANDARDS AND TESTS TO ENSURE AI SYSTEMS ARE SAFE AND SECURE

In addition to requiring companies to report certain information regarding new AI technology to the government, this order seeks to establish uniform testing standards to ensure that AI technology is safe and secure prior to public release. President Biden has tasked the National Institute of Standards and Technology (NIST) with setting standards for "extensive red-team testing[3] to ensure safety before public release" of AI applications. NIST, which is responsible for issuing recommendations for government cybersecurity standards, does not have the power to directly regulate companies or individuals, so the Department of Homeland Security (DHS) will be responsible for applying the NIST testing standards and establishing the AI Safety and Security Board. Along with DHS, the Department of Energy will be responsible for addressing the threat of AI systems to "critical infrastructure, as well as chemical, biological, radiological, nuclear, and cybersecurity risks."[4]

In January, NIST released the Artificial Intelligence Risk Management Framework, which is designed to provide guidance for organizations using, designing, and deploying AI technologies. This framework may be an early example of the testing standards NIST will release pursuant to this Executive Order. Given the Administration's push towards safe AI, NIST may be tasked with developing AI security standards that all government contractors will be required to follow. Contractors should pay close attention to this framework as it develops to help them anticipate future AI opportunities and compliance obligations.

In addition, the Federal Trade Commission (FTC) currently is developing a new rule that would regulate how companies must handle personal data. The FTC is concerned that "companies use algorithms and automated systems [such as AI] to analyze the information they collect" and "many companies do not sufficiently or consistently invest in securing the data they collect from hackers and data thieves."[5] It is unclear exactly what the rule would require, but it appears that it would apply to all companies operating in the U.S., including government contractors.

Between broad data security legislation regarding AI, the FTC's future rule, and existing FAR regulations that implement cyber defense requirements such as NIST SP 800-171, contractors will have to navigate through a maze of new data security regulations.

DATA PROTECTION

Perhaps the largest threat posed by the rise of AI is the threat to data security. AI systems are "socio-technical" systems, "meaning they are influenced by societal dynamics and human behavior. AI risks can emerge from the complex interplay of these technical and societal factors, affecting people's lives in situations ranging from their experiences with online chatbots to the results of job and loan applications."[6]

In this order, President Biden calls for Congressional action to pass bipartisan data privacy legislation to protect against the data privacy risks posed by AI. Specifically, he seeks to prioritize the development of privacy-preserving techniques, strengthen privacy-preserving research and technology, and evaluate how agencies collect and use commercially available data. Importantly, the President also calls for legislation to strengthen privacy guidance for federal agencies and develop guidelines for agencies to evaluate the effectiveness of the privacy-preserving techniques. What is certain is that as the data security requirements for federal agencies change, the requirements for government contractors will change as well.

OPPORTUNITIES FOR CONTRACTORS USING AND DEVELOPING AI

While the main function of the order is to propose a new framework to evaluate and regulate AI technologies, President Biden has indicated there will be significant government investment in the development of safe and secure AI. In an effort to ensure that the U.S. remains the world leader in AI technology, the order proposes to expand grants for AI research in vital areas, such as healthcare and climate change, and directs further agency guidance for the purpose of using the procurement power to quickly modernize federal AI infrastructure. Recipients of such funding, who may not be accustomed to working with federal agencies, are likely to be subject to Uniform Grant Regulations[7] applicable to federal grant recipients and subrecipients, as well as agency supplements thereto.

This order demonstrates that the Administration is spearheading a government-wide effort to understand, evaluate, and engage with AI, while guarding against its potential negative repercussions. The government's continued involvement in the development, evaluation, regulation, and use of AI will present opportunities for contractors

developing and investing in AI, as well as guardrails for those using AI to perform their contracts. There will be significant regulatory activity in the years to come, and companies that do business with the government will need to understand what AI technologies and standards will be approved for use by and for the government to remain competitive and compliant as these rapidly changing technologies and standards evolve.

RECOMMENDATIONS

- Monitor the release of new guidance and regulations regarding AI and data protection, including the NIST testing standards, FTC rule on data security, and Congressional action.
- Contractors that use AI technology in their operations should review NIST's Artificial Intelligence Risk Management Framework and begin to implement the recommended security controls.
- Companies (whether government contractors or not) that develop AI technology should determine if they fall under President Biden's invocation of the Defense Production Act, requiring the disclosure of security data about new AI products.
- Look for opportunities to incorporate safe and secure AI systems into contracting operations, which may in turn earn a bidder preference on future procurement bids.

Please contact the authors or your Winston & Strawn relationship attorney if you have any questions or need further information.

---

[1] 50 U.S.C. §§ 4531, 4533; FEMA, Defense Production Act, https://www.fema.gov/disaster/defense-production-act, FEMA.gov, Apr. 19, 2023.

[2] John D. McKinnon et al., *Biden to Use Emergency Powers to Mitigate AI Risks*, The Wall Street Journal (Oct. 30, 2023), https://www.wsj.com/politics/policy/biden-to-use-emergency-powers-to-mitigate-ai-risks-cf7735d5.

[3] Red-team testing is a procedure used to test a system's cybersecurity strength by having a team of expert hackers ("red team") attempt to penetrate the system's cyber defenses. *See* https://www.crowdstrike.com/cybersecurity-101/red-teaming/.

[4] *Fact Sheet: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence*, The White House (Oct. 30, 2023), 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/.

[5] *Fact Sheet on the FTC's Commercial Surveillance and Data Security Rulemaking.* Federal Trade Commission, https://www.ftc.gov/system/files/ftc_gov/pdf/Commercial%20Surveillance%20and%20Data%20Security%20Rulemaking%20Fact%20Sheet_1.pdf.

[6] *NIST Risk Management Framework Aims to Improve Trustworthiness of Artificial Intelligence*, National Institute of Standards and Technology (Jan. 26, 2023), https://www.nist.gov/news-events/news/2023/01/nist-risk-management-framework-aims-improve-trustworthiness-artificial.

[7] 2 C.F.R. Part 200.

7 Min Read

Authors

Lawrence "Larry" Block

Lawrence S. Sher

Elizabeth Leavy

William T. Kirkwood

Michael Hill

Related Topics

National Institute of Standards and Technology | Artificial Intelligence (AI) | U.S. Department of Homeland Security | U.S. Department of Energy | FTC

Related Capabilities

Government Investigations, Enforcement & Compliance | Government Contracts | Artificial Intelligence (AI)

Related Professionals

Lawrence “Larry” Block

Lawrence S. Sher

Elizabeth Leavy

William T. Kirkwood

Michael Hill

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.

© 2024 Winston & Strawn LLP.