WILSON SONSINI

AI in the Biden Administration's Crosshairs—Summarizing the Sweeping New Executive Order and Ten Top Takeaways

CONTRIBUTORS

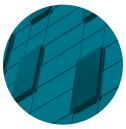

Joshua F. Gruenspecht


Maneesha Mithal


Scott A. McKinney


Jess Cheng


Seth Cowell


Nikhil Goyal

ALERTS

November 2, 2023

On October 30, 2023, President Biden announced a sweeping new Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (EO). The EO signals an "all-hands-on-deck" approach, with roles for agencies across the federal government, proposed requirements and/or guidance that will apply both to companies that offer artificial intelligence (AI)-related services and those that consume such services, and still-unfolding implications for the legal operation of such businesses.

Highlights of the EO for providers and consumers of AI products and services follow, with our 10 top takeaways for private sector investors and companies immediately after:

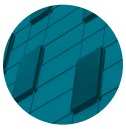
Highlights

- **Government Reporting Requirements for Private Companies Using High-Powered AI Algorithms and Computing Clusters:** Certain entities that develop or demonstrate an intent to develop dual-use foundation models[1] will become subject to new reporting requirements to the Department of Commerce (DoC). These entities develop models that have certain technical parameters and exhibit a high level of performance at tasks of potential national security significance (which under the EO may include tasks as diverse as learning to deceive humans in order to evade their control). Under rules to be established within 90 days of the issuance of the EO, such entities will be required to:
  - provide reports and records to the federal government concerning ongoing or planned training, development or production of such models;
  - provide information related to the ownership and possession of such models; and
  - share the results of red-team safety tests carried out pursuant to National Institute of Standards of Technology (NIST) guidance.

  In addition, the EO requires entities that acquire, develop, or possess large-scale computing clusters to report such activity to the government. The specifics of the technical triggers that will define which dual-use foundation models and computing clusters will be subject to reporting will be determined by the DoC, though preliminary parameters are provided in the EO.
- **New Federal AI Security Standards and Testing Tools:** Under the EO, NIST is required to more generally establish guidelines and best practices for developing and deploying safe, secure, and trustworthy AI systems of all stripes.[2] These include pre-release AI red-teaming tests not just for the dual-use foundation models obligated to use them under the DoC rules, but also for generative AI and other types of AI systems. NIST also is required to work with other federal agencies to establish AI testing tools and testbeds for use in red-teaming activities. The EO calls for various other non-binding security standards for AI companies in various specific fields as

Kara D. Millard

Rosalind J. Schonwald



Graham Hendrick

well—e.g., standards developed by DoC, NIST, and healthcare-focused agencies intended for adoption by providers of synthetic nucleic acid sequences.

- **Reporting Requirements for Foreign Use of Major Infrastructure Providers Supporting AI Activity:** DoC is separately charged with implementing reporting requirements for major U.S. cloud service providers, with more specifics to be established in proposed regulations due within 90-180 days. Such infrastructure services providers will be obligated to:
  - report any rental by a foreign person of U.S. cloud server space to train large AI models with potential capabilities that could be used in malicious cyber-enabled activity;
  - prohibit foreign resellers from reselling such services unless they also agree to similar reports prior to contracting with foreign buyers for cloud server space; and
  - require their foreign resellers to verify the identities of customers, maintain certain records concerning those customers and their activities, and secure those records appropriately.

- **Longer-Term Guidance and Potential Restrictions on U.S. Government (USG) and Critical Infrastructure End-Use of AI Tools:** The EO also mandates specific national security-related actions by government agencies and private sector operators of "critical infrastructure" (e.g., defense systems, utilities, telecommunications, major financial services) that use AI:
  - **USG Software Improvements.** The Department of Homeland Security (DHS) and Department of Defense must create an "operational pilot project" to identify, develop, test, evaluate, and deploy AI capabilities, such as large-language models, to discover and remediate software vulnerabilities in critical USG systems and networks.
  - **Protecting Critical Infrastructure.** DHS and various other agencies are tasked with assessing and mitigating AI systems' threats to U.S. critical infrastructure (e.g., power grids, water supplies, transportation, and communication networks), and other risks including chemical, biological, radiological, nuclear, and cybersecurity risks. The EO asks DHS to incorporate NIST's AI Risk Management Framework and other appropriate security guidance into relevant safety and security guidelines, which the EO seems to contemplate would be a precursor for "the Federal Government to mandate such guidelines…through regulatory or other appropriate action."

- **AI Opportunities/Challenges for Government Contractors:** The EO also suggests the USG should leverage and/or support the development of AI tools through government procurement and grants:
  - **Increasing the Availability of AI Products to Agencies.** The EO tasks General Services Administration to take steps, within 90 days, to develop and issue a framework that prioritizes generative AI offerings that have the primary purpose of providing large language model-based chat interfaces, code-generation and debugging tools, and associated application programming interfaces, as well as prompt-based image generators in the Federal Risk and Authorization Management Program (FedRAMP) authorization process. The EO also directs agency authorizing officials to prioritize granting "authorities to operate" to generative AI and other critical and emerging technologies.
  - **Funding Innovation.** The EO directs DoC to promote competition in the semiconductor space by ensuring that the resources, mentoring and funding available under the CHIPS Act (administered by DoC) is awarded to start-ups and small businesses, in order to support participation in the semiconductor and microelectronics industry across all parts of the AI ecosystem and promote the development of such companies.

- **Protecting Consumers and Competition:** The EO "encourages" the Federal Trade Commission to consider rulemaking 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. It also encourages independent regulatory agencies to consider using their full range of authorities to protect American consumers from fraud, discrimination, and threats to privacy, including by considering rulemaking and clarification of the application of existing regulations to AI. The EO focuses on transparency and explainability. And it requires the DoC to issue guidance regarding tools and best practices for authenticating digital content (e.g., through watermarking), detecting AI-generated synthetic content, and preventing child sexual abuse material, among other things.
- **Maintaining Privacy:** The EO explicitly makes consumer privacy in AI a priority for the administration. For example, the EO directs the Office of Management and Budget to identify personal information that the government purchases and establish guidelines to reduce privacy risks associated with government usage of data purchased from data brokers. It also prioritizes federal support for accelerating the development and use of privacy-preserving techniques in the AI context. And it explicitly calls for Congress to pass bipartisan privacy legislation.
- **Intellectual Property:** The EO includes requirements that the U.S. Secretary of Commerce for Intellectual Property and the USPTO Director provide guidance regarding patent and copyright protection available (or not available) to AI-related works, including those created with some contribution from generative-AI technologies. As those rules develop, we will provide additional

advice regarding strategy, internal policies, and contractual processes for best protecting AI-generated IP and technology.

- **Commercial Contracting Considerations in Light of the EO**: Since the EO makes it all but certain that numerous new and revised U.S. AI rules and regulations will be enacted across regulatory agencies in the next six to twelve months, companies using or selling AI-related technology should consider including flexible mechanisms such as flow-down terms and termination rights in their contracts, so that AI-related agreements can be adapted or exited if they are not compatible with upcoming rules and regulations, including regulations regarding sales to foreign customers. Companies should also consider building in flexibility to third-party developer contracts related to AI development and AI supplier contracts, particularly with respect to content authentication and labeling.
- **AI and the Financial Sector:** The order requires the Secretary of the Treasury to issue a public report on best practices for financial institutions to manage AI-specific cybersecurity risks. As a point of comparison, the Federal Reserve Board's recently published Cybersecurity and Financial System Resilience Report to Congress cautioned that AI, among other machine learning tools, could be used by bad actors to automate cyberattacks. The Federal Reserve's report also identified the use of generative AI by bad actors as an emerging threat, due to its ability to generate content that can be used in enhancing social engineering attacks, including email- and text message-based phishing attacks.

Ten Top Takeaways for AI Builders, AI Investors, and AI Users

1. **This is the beginning of the beginning for AI regulation**. As the highlights above illustrate, nearly all of the EO is either intended to be implemented through yet-to-be-written rules or framed in terms of recommendations, guidance, principles, toolkits, or best practices. Until the agencies responsible for these various tasks have a chance to implement their respective pieces of the order over the next year, even the initial impact of the EO will not be fully apparent.
2. **The Biden administration views AI as a national security concern without a recent parallel among emerging technologies**. During the President's press conference prior to signing the EO, he emphasized his conviction that the appearance of AI marks an inflection point in history. Parts of the EO use the Defense Production Act (DPA), which gives the President the power to "allocate materials, services, and facilities" for national defense purposes, as justification for various requirements for private sector entities to share information with the government. The use of the DPA, a federal power previously reserved for emergencies such as war or a pandemic, demonstrates the magnitude of this critical juncture, and highlights the urgency felt by the federal government in ensuring that AI technologies are developed in a safe and secure manner.
3. **The authority implicitly claimed by the EO is very broad but only the largest players are subject to prescriptive rules—for now**. The EO defines "AI system" as any data system, software, hardware, application, tool, or utility that operates in whole or in part using AI—potentially a startlingly diverse set of products and software tools. Many provisions ask government agencies like NIST to address the activities of *all* such systems with guidance. In addition, the EO is silent on the proper geographic scope of many of its components, leaving clarity to be provided by future regulations and opening the door to potential extraterritorial impacts. However, the actual reporting requirements currently only appear to be intended to apply to the major U.S. AI players.
4. **With that said, there may be future implications for biotechnology start-ups, fintech companies, cybersecurity services providers, and many other entities that are only tangential users of AI**. Repeatedly throughout the text, the EO suggests that agencies should "establish a framework" or "conduct a study" but implies that activity will then serve as a prelude to authoring regulation. For private sector companies that provide services or software to telecommunications operators or utilities; procure federal research funding for work on pathogens, omics, or synthetic biology; or simply create tools that may be used to impersonate humans, the EO will provide "guidance" for now. However, the strong implication is that requirements for "AI systems" across those various sectors may soon follow.
5. **The long-term impact of the EO depends on its bipartisan acceptance, and thus U.S. AI regulation may not have the staying power of rules in other jurisdictions.** Given the limitations of executive authority, agency proclamations—especially those issued only in the form of guidance—have an inherent shelf life. It is unclear whether the EO will remain in effect to the extent there is a change in administration. This is all in contrast to, e.g., the EU AI Act, which has a set of far-reaching consequences, which carry fines of up to 40 million Euros or seven percent of annual revenue, whichever is higher, for violations.
6. **The private sector will push back.** Industry-affiliated associations such as NetChoice have already been pushing back on some of the EO's provisions. The invocation of the DPA to obtain information from AI model creators is an aggressive use of authority that has been traditionally exercised in national emergencies. Companies should expect pushback both during the

regulatory notice and comment period and, in the longer term, via litigation. Court decisions may further alter the EO's impact.

7. **Opportunities may soon abound for AI providers ready to do business with the federal government**. Despite the intense focus on the safe and secure use of AI, certain sections of the EO also emphasize that AI presents an opportunity like few others for innovation within the government. As USG agencies are tasked in various ways with encouraging AI research and incorporating AI into their own activities—from cybersecurity preparedness to defense procurement—private sector AI companies in search of funding may wish to revisit the federal government as a potential source of contracts or grants.
8. **Regardless of the EO, the federal government is going to continue to pay ever more attention to AI systems and their users**. AI is in the spotlight, and companies can expect increased federal intervention into the development and use of AI technologies. Agencies are using existing authority to target companies developing and using AI, with regulators as diverse as the FTC, BIS, and CFIUS having already stepped up enforcement actions or investigations of companies with AI-related technologies.
9. **Geopolitical competition: speaking loudly without saying a word.** Although the nation itself is never directly referenced in the EO, AI innovation in China clearly is motivating many of the EO's provisions. AI has increasingly been seen in the national security context as a threat when held by malicious foreign actors and governments, and increasing concerns about the strength of foreign AI research has underpinned multiple recent actions by the Biden administration.[3] For example, the section requiring reporting of foreign access to U.S. cloud services—with the implication that such access may be prohibited in some future cases—appears to pair with recent rules suggesting that U.S. companies and investors should not support China's development of in-country advanced AI technology.[4]
10. **Companies in other emerging technology sectors should take heed—additional cutting-edge technologies may be next.** At several junctures the EO asks agencies to study or provide recommendations with respect to AI "and other critical and emerging technologies." The extensive 2022 White House list of critical and emerging technologies referenced by that phrase encompasses technologies ranging from additive manufacturing to genome engineering to quantum computing to satellites. The use of the DPA to regulate critical AI companies, if upheld, could embolden the Biden administration to create similar rules for other technologies of interest using that same authority.

In sum: keep watching this space. Affected companies should carefully monitor the implementation of this executive order and any follow-on actions by agencies under the EO.

Wilson Sonsini Goodrich & Rosati routinely helps companies navigate complex privacy, data, and national security issues in developing policy sectors. For more information or advice concerning your compliance efforts related to AI, please contact Joshua Gruenspecht, Maneesha Mithal, Scott McKinney, Jess Cheng, Barath Chari, Manja Sachet, Seth Cowell, Nikhil Goyal, Kara Millard, Rosalind Schonwald, or any member of the firm's national security practice, privacy and cybersecurity practice, or artificial intelligence and machine learning working group.

---

[1] More specifically defined as "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 [. . .]"

[2] In January 2023, NIST released an Artificial Intelligence Risk Management Framework intended to provide a resource to organizations designing, developing, deploying, or using AI systems to manage risks and promote trustworthy and responsible development and use of AI systems. See our previous alert for more details.

[3] As one example, in an effort to slow China's development of advanced AI technologies, the DoC recently issued an array of semiconductor and supercomputer-related export controls. See recent client alerts here and here for a discussion of these export controls. As another, see our recent client alert on proposed outbound investment rules to restrict U.S. support for AI innovation in China here.

[4] *Id.*