Morgan Lewis

LAWFLASH

BIDEN ISSUES SWEEPING EXECUTIVE ORDER PRESENTING OPPORTUNITY AND RISK FOR AI

November 01, 2023

AUTHORS

Dion M. Bregman, Nicholas M. Gess, Giovanna M. Cinelli, W. Barron A. Avery, Eric S. Bord

President Joseph Biden issued an executive order on October 30 designed to protect against the risks of artificial intelligence (AI) while encouraging the global growth and expansion of AI development and use.

Although the executive order (EO), titled Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, EO 14110, 88 Fed. Reg. 75191-75226 (Nov. 1, 2023), is largely not self-effectuating and thus does not have a practical impact at this time, it provides a robust roadmap of the Biden administration's anticipated policy, regulatory, legal, and practical changes that will affect a broad range of industries—not only those that develop AI, but also those that use AI. Of particular import is the focus on technology and healthcare, privacy, immigration, and accessibility—all areas of significant ongoing attention from the Biden administration.

The EO requires, at least, the following:

1. Developers of powerful AI systems must disclose their safety test results and other information to the US government.
2. NIST must publish requirements for testing prior to public release ("red teaming") and various implementation functions are assigned to other federal agencies, including the Department of Homeland Security (DHS) and the Department of Energy. The DHS will also establish an AI Safety and Security Board. This is akin to what is likely already occurring with respect to other rapidly developing technologies, such as chemical, biological, radiological, nuclear, and cybersecurity.
3. Federal funding for key AI life sciences projects will be predicated on compliance, creating internal development pressures to comply.
4. Establish standards for "watermarking" AI-generated content by government agencies to ensure public confidence in government communications and encourage private sector adoption of "watermarking" standards for non-government products. This, along with asking the Consumer Financial Protection Bureau (CFPB) to develop rules protecting tenants against the use of "unfair" AI in the leasing process, may go a long way toward protecting vulnerable populations. However, tools such as "watermarking" are only as effective as the public is educated about them and the EO also does not apply to the majority of sources of misinformation, such as propaganda news outlets and foreign provocateurs.
5. An AI cybersecurity program will be established to reward private development of AI tools and to find and repair vulnerabilities in critical software.

6. Direction to entities within the Executive Office of the President, including the National Security Council (NSC) and chief of staff to develop standards for the use of AI by the US military and intelligence community to ensure that AI is used safely, ethically, and effectively by those entities.
7. Grant priority resources to programs that accelerate the development and use of privacy-preserving techniques, research, and technology, evaluate how government agencies collect and use commercially available information, and set guidelines for federal agencies to evaluate the effectiveness of these techniques.
8. Grant certain civil rights protections, including guidance to landlords, federal benefits programs, and federal contractors on the use of AI algorithms to prevent their use for discriminatory purposes; require the US Department of Justice (DOJ) to work on best practices for the investigation and prosecution of algorithmic civil rights violations and work to ensure "fairness" in the criminal justice system as AI is used for sentencing, forensic, and investigative tools. These protections can be mandated for the federal, but not the state criminal justice systems, and their adoption by states is constrained by constitutional, policy, and resource considerations.
9. Advance efforts to promote the use of AI in the development of healthcare and new drugs while establishing a safety program to prevent the harms and unsafe practices that AI may create. In a similar vein, the EO will promote educational programs that can use AI to provide personalized individual tutoring in schools.
10. Addressing a key concern in the workforce (for example, the displacement of workers by AI), the EO directs the production of a report on labor-market impacts and the development of best practices to mitigate the harms and provide benefits of AI for workers.
11. The use of existing authorities to update immigration rules and policies to reduce barriers to the issuance of visas and permanent residence to highly skilled foreign nationals so that the United States can attract and retain talent in AI and other critical emerging technologies.

The EO may provide significant support to developers and customers of AI, reduce barriers to the employment of highly skilled foreign national talent in the United States, and pave the way for additional government funding (whether through grants or government contracts), but under strict constraints of federal procurement and criminal sanctions, which carry heavy potential penalties for both businesses and individuals.

If implemented, industry, academia, individuals, researchers, and global allies can expect to see additional administrative bureaucracy through US government working groups, advisory committees, and outreach, but also an attempt to bring to bear all the US government's regulatory authority to manage, if not control, the use and application of AI.

The EO relies on agency rulemaking under the Administrative Procedures Act (APA) for implementation and assertively presses Congress to enact a comprehensive privacy law, while leaving in place a patchwork of potentially conflicting state laws. This is in contrast to broader and more prescriptive actions taken by the European Union.

However, pragmatically speaking, several areas of the EO highlight the Biden administration's continued focus on consolidation of regulatory authority, consistency where needed, and broad multilateral engagement. It invokes both the Defense Production Act of 1950 (DPA), 50 USC §§ 4501, et seq., and the International Emergency Economic Powers Act, 17 USC §§ 1701, et seq., as its underlying authority—two statutes that maximize the president's flexibility when it comes to announcing policy and directing agencies to implement that policy through regulatory constructs.

The DPA was used extensively during the COVID-19 pandemic and allows the president to regulate and compel the means and manner of industrial production in furtherance of national defense and security. While first conceived during the Cold War, the law remains relevant and was most recently the lynchpin of vaccine and other production during the initial stages of the pandemic. It remains a key tool of administrations in the technology industry, where the DPA has been invoked to declare critical materials and issue rated orders to support national security requirements.

Similarly, the president's invocation of the International Emergency Economic Powers Act (IEEPA), 50 USC §§ 1701, et seq., emphasizes the importance the administration places on its ability to declare a national emergency and take immediate and potentially unilateral actions. Under this provision, even with the existence of the Export Control Reform Act of 2018 (ECRA), we anticipate additional export controls on AI writ large—whether on the software, hardware, technology, equipment, or materials side.

However, the EO is necessarily heavily dependent on agency rulemaking and implementation. Rulemaking may be constrained by the US Supreme Court's recent resurrection of the Major Questions Doctrine and action the Court may take with respect to Chevron deference in the current term. Congress also wields influence through its ability to legislate, limit funding, develop funding constraints, or condition funding upon completion of other actions.

Moreover, because AI risks are transnational and not readily stopped at a physical border, enforcement of many of the proposed efforts remains uncertain. Absent multilateral consensus, partners, and allies, as well as other countries, may determine alternative paths for addressing AI governance. Deviations or diversions from a common focus will likely limit the effectiveness and reliability of any proposed US efforts.

While that may not discourage the US from proceeding down a particular path, it will create challenges for companies, researchers, academics, and others who will need to balance varying objectives by jurisdiction. Increased regulation may also result in AI companies choosing to develop their capabilities in less regulated countries. An upcoming meeting of the G-7 nations could serve as an indicator for how this EO is perceived among key allies.

Although the EO creates broad sweeping policies, its focus can be distilled to at least the following areas:

- Monitoring and oversight—as reflected in the "red teaming" concept
- Common definitions—as noted in Section 3 where terms for which agreement may not currently exist are nonetheless defined for purposes of the EO
- Management and use of other authorities—such as export controls and government contracts
- Reporting—as noted in the testing and vulnerabilities policies

At the same time, the EO also embeds what appears to be primary responsibility in the US Department of Commerce, an agency already overburdened with export controls, supply chain, CHIPS Act, tariffs, Information and Communications Technology and Services Supply Chain regulation, and foreign direct investment (inbound and outbound through the Bureau of Economic Analysis (BEA) processes).

While the EO tasks other agencies—such as the Departments of Energy, Defense, and Health and Human Services and the Office of Science and Technology Policy—with responsibilities, the Department of Commerce seems to be the coordinating and lead agency across a number of areas, in part perhaps because Commerce includes the National Institute of Standards and Technology (NIST), National Telecommunications and Information Administration (NITA), and the US Patent and Trademark Office (USPTO). How this coordination will ultimately play out remains an open question.

Federal contractors can expect a review and study of new regulatory requirements. Government contractors that use AI or provide AI to the government can expect to feel the effects of the EO through new contract terms and potential regulatory clauses. By requiring agencies to take certain steps regarding the AI that they use, the administration is implicitly requiring agencies to pass those restrictions along to their contractors, as necessary. In that vein, the EO directs myriad changes that will impact agencies' administration of government contracts. Contractors may be affected by proscriptions ranging from privacy and security standards to red-teaming and watermarking requirements.

As noted above, the EO also includes an express requirement that agencies provide clear guidance to federal contractors to keep AI algorithms from being used to exacerbate discrimination. In addition to those regulatory requirements, the EO's requirements may create new contract opportunities as agencies work to find tools that will help them advance fraud detection and authentication efforts and meet other EO mandates.

Industries, academics, researchers, and global partners can expect some export controls related to AI development, design, and application. The EO highlights the diligence requirements when working with third parties and the need for companies and others to remain vigilant regarding how third parties use certain AI-specific technologies and products. While a "know your customer" approach exists across a number of regulatory constructs, it has been particularly challenging within the export controls regulations, as those have expanded and imposed additional obligations on industry to assess how they manage exchanges with unrelated parties.

AI overall is not expressly controlled as a separate category by either the Department of Commerce or State, although many aspects of AI (as defined in Section 3 of the EO) are embedded within both the Export Administration Regulations and the International Traffic in Arms Regulations.

Both Commerce and State would need to update the control lists under each regime to clarify the covered AI and then establish policies for how exports of those controlled items are managed. As the EO notes, the president directed Commerce and State to engage in these types of reviews, and we expect regulations in this area.

ANTICIPATED AI PRIVACY LEGISLATION THAT MAY NOT MATERIALIZE

The EO recognizes the constraints on the president's authority and calls on Congress to enact comprehensive national privacy legislation addressing AI. Legislative proposals to expand or enhance existing authorities have existed for several years and none have proceeded beyond the proposal stage despite widespread support. In large measure, difficulties in finding common ground on definitions, scope of application, and the extent to which preemption applies, have resulted in stalemates on most legislative proposals.

In addition, because there is no agreement on the extent to which federal law would preempt state law privacy provisions, regulate private industry, or integrate with privacy regimes in other jurisdictions, most notably the European Union as well as the United Kingdom and the European Economic Area, additional obstacles create challenges to legislative progress.

TAKEAWAYS

- The EO's breadth and depth represent a powerful statement by the president but is constrained by the rulemaking system and requirements that undertakings be authorized by congressional appropriation. It is therefore, practically speaking, a policy roadmap, but nothing has yet changed from a regulatory requirements perspective.
- Congress remains a key player and can affect how the agencies implement the EO. How Congress reacts remains to be seen, certainly in the runup to a 2024 election for president, one-third of the US Senate, and

the entire US House of Representatives.

- Not surprisingly, this EO is focused on the federal government. However, given the reach of the DPA and the federal government's status as a funder and consumer of AI, standards set by the federal government will likely be adopted by state and local governments as well as other industries, and compliance may assist in the backing of the federal government overseas. That, of course, is largely limited to allies and may leave the United States at an economic disadvantage elsewhere.
- The EO presents significant opportunities and incentives for AI developers and users but poses risks, including criminal prosecution of businesses and individuals. Caution will be the watchword and it is important to note that President Biden has pledged not to interfere with decision-making by the US Department of Justice. The attorney general has not yet spoken on this, and prosecution standards remain to be seen.
- Careful consultation and thorough review with both AI experts and legal counsel with intellectual property, criminal, DPA, IEEPA, commerce, and government contracting, will be essential.
- The EO recognizes the need to modify elements of the US immigration system so the that United States can compete effectively with other countries to attract and retain highly skilled global talent. Major changes will require legislative action, but the EO proposes regulatory and policy changes that will be rolled out in the coming months.
- Lawyers and in-house legal departments will need to stay up to date on new regulations and guidance related to AI. The order directs various agencies to issue regulations, guidance, and reports on topics like non-discrimination, privacy, cybersecurity, and IP for AI systems. Lawyers, especially those working in related areas like civil rights, employment, privacy, cybersecurity, and IP, will need to monitor these developments and understand how they impact their practice areas.
- AI compliance will likely have a key seat at the table for both corporate leadership and the counsel that support them. As agencies issue new regulations and guidance per the order, companies will need legal help understanding their new compliance obligations. Law firms with relevant expertise could see increased demand for advisory services on topics such as AI safety, preventing algorithmic discrimination, protecting privacy, and securing data used for AI.
- IP lawyers and in-house legal departments will need to advise clients on AI inventorship and patent eligibility. The order calls for the USPTO to issue guidance on patenting AI inventions. IP lawyers will need to stay up to date on the evolving guidelines and case law around inventorship and patent eligibility for AI systems. They will need to counsel clients on open questions such as whether an AI system can be named as an inventor.
- Corporate leadership and their counsel will need to develop expertise in AI as it features more prominently in litigation. As AI becomes more widespread, it is likely to appear more regularly as a supporting tool to enhance the litigation process and to ensure that foot faults do not occur through the possible misuse of AI in the process. Lawyers will increasingly need AI literacy and expertise to effectively argue cases involving algorithmic decision-making and weigh in on issues such as liability for AI systems. Developing expertise in AI safety, privacy, and security will become more important.

The EO imposes numerous agency deadlines for actions, including rulemaking. Morgan Lewis will monitor those deadlines and provide updates as the details of this whole-of-government approach become apparent.

CONTACTS

If you have any questions or would like more information on the issues discussed in this LawFlash, please contact any of the following:

Authors

Dion M. Bregman (Silicon Valley)
Nicholas M. Gess (Washington, DC)
Giovanna M. Cinelli (Washington, DC)

W. Barron A. Avery (Washington, DC)
Eric S. Bord (Washington, DC)

Washington, DC

W. Barron A. Avery
Eric S. Bord
Giovanna M. Cinelli
Ronald W. Del Sesto, Jr.
Ron N. Dreben
Nicholas M. Gess
Meaghan H. Kent
Kenneth J. Nunnenkamp
Dr. Axel Spies
Katelyn M. Hilferty
Eli Rymland-Kelly
Christian Kozlowski

Silicon Valley

Dion M. Bregman
Andrew J. Gray IV
Manita Rawat
David V. Sanker, Ph.D.

Los Angeles

Neeraj Arora
Yardena R. Zwang-Weissman

Philadelphia

Ezra D. Church
John C. Goodchild, III
Kristin M. Hadgis
Scott A. Milner
Gregory T. Parks

Miami

Kimberley E. Lunetta

Boston

Laurie A. Cerveny
Doneld G. Shelkey

Chicago

Elizabeth B. Herrington

Houston

Casey Weaver