The Texas Lawbook

Free Speech, Due Process and Trial by Jury

Navigating Artificial Intelligence in the Lone Star State: Biden's Executive Order on AI

DECEMBER 13, 2023 | BY MICHELLE REED & AMANDA HURD

On Oct. 30, President Joe Biden announced a sweeping new executive order titled "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence" that will impact businesses across Texas. The EO takes a multifaceted approach, creating roles for agencies across the federal government, as well as proposing requirements and providing guidance for businesses that offer or consume artificial intelligence services.

The order issues directives to over 20 federal agencies, instructing them to advance key policy objectives, including ensuring safety and security with the advancement of AI, encouraging responsible innovation and competition, protecting consumer interests, safeguarding privacy and civil liberties and promoting global cooperation on AI governance. The deadlines for implementation span between 30 and 365 days.

The EO stands as one of the first federal statements regarding AI in the United States, following behind international regulations on AI. In April 2021, the EU AI Act, was proposed and includes a set of far-reaching consequences that carry fines of up to 40 million euros or seven percent of annual revenue, whichever is higher, for violations.

The proposed act also includes a complex oversight and enforcement regime that is modeled on EU product-safety legislation. If passed it would impose a detailed set of technical and organizational requirements on providers and users of AI systems. Providers of "high-risk" AI systems, such as applications related to transport, education, employment and welfare, will face obligations relating to data governance, training, testing and validation, conducting conformity assessments, building risk management systems and post-market monitoring. The EU IA Act would also prohibit some uses of AI systems altogether and impose transparency obligations on others. On Oct. 27, the Group of Seven leaders issued international principles and a code of conduct for businesses developing advanced AI systems. Some G7 leaders have additionally begun to increase regulation of AI technologies as well.

In contrast, the EO does not create new legislative obligations. Rather, it introduces a number of directives to government agencies, including instructing the Department of Commerce to develop rules requiring disclosures from businesses that develop or provide infrastructure for AI models under certain circumstances. The EO defines an "AI system" as any data system, software, hardware, application, tool or utility that operates in whole or in part using AI, encompassing a strikingly wide array of products and software tools. The EO directs government agencies like the National Institute of Standards and Technology to provide guidance that addresses the activities of all such systems but remains silent on the proper scope of many of its components.

Some believe the U.S. government will face significant challenges and limitations in the implementation of tis initiative, but certain agencies maintain that they have the authority to regulate AI through existing frameworks. The FTC has already and will continue to use its enforcement authority to challenge unfair or deceptive practices related to emerging AI products. Further, the White House Office of Management of Budget issued a draft memorandum to executive agency heads stating that each agency must designate a chief AI officer within 60 days. The designated CAIO will be tasked with "advancing responsible AI innovation" and "managing risks from the use of AI."

For Texas businesses, there are some direct considerations for providers and consumers of AI products and services.

New Reporting Requirements, Standards and Restrictions

Under the EO, the NIST is set to establish new federal AI standards and testing tools to establish best practices for developing and deploying safe, secure and trustworthy AI systems. This includes pre-release AI red-teaming tests (a multilayered, full-scope cyberattack simulation designed to test the effectiveness of an organization's security controls) for the generative AI and other types of AI systems in addition to the dual-use foundation models that are already obligated to institute such measures under the DOC rules. NIST will work with other federal agencies to establish AI testing tools and testbeds for use in red-teaming activities. The EO additionally calls for various nonbinding security standards for AI businesses in certain fields such as healthcare agencies that provide synthetic nucleic acid sequences.

There are new government reporting requirements for private businesses using high-powered AI algorithms and computing clusters. Certain entities that develop or intend to develop dual-use foundation models will be subject to new reporting requirements to the DOC. These entities develop models that exhibit a high level of performance for tasks that may potentially involve matters of national security. Under the new rules, which are to be established within 90 days of the issuance of the EO, these 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 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.

There are also new reporting requirements for foreign use of major infrastructure providers that support AI activity. The DOC is now charged with implementing reporting requirements for major U.S. cloud service providers, and more specifics are to be established in proposed regulations that are due within 90 to 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 that potentially have the capability to be used in malicious cyber-enabled activity;
- prohibit foreign resellers from reselling these services unless they also agree to submit 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.

Seeking to address the use of U.S. Infrastructure as a Service products by foreign malicious cyber actors, the EO also requires the DOC to prescribe reporting requirements for IaaS providers to ensure that foreign resellers of such products verify the identity of any foreign person that obtains an IaaS account. The EO also provides for longer-term guidance and potential restrictions on U.S. government and critical infrastructure end-use of AI tools. It mandates specific national security-related actions by government agencies and private sector operators of "critical infrastructure," such as defense systems, utilities, telecommunications and major financial services that use AI.

The department of Homeland Security and Department of Defense must create an "operational pilot project" to identify, develop, test, evaluate and deploy AI capabilities like large-language models in order to discover and remediate software vulnerabilities in critical U.S. government systems. The DHS and various other agencies are being tasked with assessing and mitigating the threat different AI systems may pose to critical infrastructure, including power grids, water supplies, transportation and communication networks. They are also addressing chemical, biological, radiological, nuclear and cybersecurity risks. The EO directs DHS to incorporate the NIST's AI Risk Management Framework into relevant safety and security guidelines as a precursor to "the Federal Government ... mandat[ing] such guidelines ... through regulatory or other appropriate action."

In the financial sector, the EO requires the secretary of the Treasury to issue a public report on best practices for financial institutions to manage AI-specific cybersecurity risks. The Federal Reserve Board recently published their Cybersecurity and Financial System Resilience Report to Congress and 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.

In addition to its agency-specific directives, the EO creates a White House AI Council to more broadly coordinate the federal government's AI activities. The council will be chaired by the White House deputy chief of staff for policy and will be comprised of representatives from each agency. Agencies' implementation of the directives outlined in the EO will occur alongside continued legislative efforts to continue to pave the path forward on AI legislation.

Leveraging and Supporting the Development of AI Tools

The EO suggests the federal government should leverage and/or support the development of AI tools through government procurement and grants. In order to increase the availability of AI products to different agencies, the EO tasks the General Services Administration to take steps within 90 days to develop and issue a framework that prioritizes generative AI offerings that focus on providing large language model-based chat interfaces, code-generation and debugging tools, and associated application programming interfaces. The EO additionally directs agency officials to prioritize granting "authorities to operate" to generative AI and other critical and emerging technologies.

The EO also directs the DOC to promote competition in the semiconductor space by ensuring that the resources, mentoring and funding available under the Creating Helpful Incentives to Produce Semiconductors (CHIPS) Act of 2022, which is administered by DOC, be 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, thereby promoting the development of these businesses. It further seeks to promote competition by providing small developers access to technical assistance and encouraging the FTC to exercise its authority in ensuring fair competition.

Lastly, the EO requires the U.S. Secretary of Commerce for Intellectual Property and the U.S. Patent and Trademark Office director to provide guidance regarding patent and copyright protections that are both available and unavailable with respect to AI-related works, including those created with some contribution from generative-AI technologies. As those rules continue to develop, businesses will likely need to seek advice regarding strategy, internal policies, and contractual processes for best protecting AI-generated IP and technology.

Consumer Protection

The EO seeks to enforce existing consumer protection laws and to promote enacting appropriate safeguards against fraud, unintended bias, privacy infringements and other harms, including by advancing the responsible use of AI in healthcare, especially with regard to drug-development processes. The EO also encourages independent regulatory agencies to consider using their full range of authorities to protect American consumers from fraud, discrimination and threats to privacy by considering exercising their rulemaking authorities and clarifying how existing AI regulations should apply. The EO further requires the DOC to issue guidance regarding tools and best practices for authenticating digital content, detecting AI-generated synthetic content and preventing child sexual abuse material, among other things.

Agencies have additionally been tasked with identifying personal information that different entities purchase and establishing guidelines to reduce the privacy risks associated with the usage of data purchased from data brokers. The EO seeks to ensure that that the collection, use, and retention of data is lawful, secure, and promotes privacy, including by directing federal agencies to use privacy-enhancing technologies where beneficial. In the EO, President Biden explicitly called for Congress to pass bipartisan data privacy legislation and reaffirmed federal support for accelerating the development and use of privacy-enhancing technologies in the AI context.

Conclusion

AI will have a profound effect on the burdens Texas businesses face as AI continues to advance into new spaces. President Biden's EO is just a start to future guidance and regulation through priority-setting, principles and best practices, frameworks across the federal AI landscape. In the 118th Congress, at least 40 bills have been introduced that either focused on AI or contained AI-focused provisions. There have also been numerous congressional roundtables and hearings to help inform lawmakers of potential legislative and regulatory needs around the use of AI. Congress is considering whether the current federal government mechanisms are sufficient for AI oversight and policymaking, the role of the federal government in supporting AI research and development, the potential impact of AI technologies on the workforce, and disclosure of AI use, testing and validation of AI systems. As Congress continues to debate these issues, the EO sets up a structure of collaboration and monitoring between U.S. government entities, as well as a mechanism for the U.S. to play a strong role in the global governance of AI. The EO answers many critical questions on the way in which the U.S. will internally govern AI and its expectations of U.S.-based businesses abroad. The U.S. has also signed the Bletchley Declaration, the outcome of the AI Safety Summit in the U.K., along with 27 other countries. The Declaration reaffirmed the importance of addressing AI risks at both national and international levels. Over the next several months, Texas businesses will have to adjust to U.S. agencies' new regulations, as well as their effects on national, regional and multilateral efforts to regulate emerging AI technologies.

Michelle Reed is a partner in the Dallas office of Akin and co-heads the firm's cybersecurity, privacy and data protection practice.