Most AI National Security Regs Likely To Remain in Place Under the Next Administration

– Rapid advances in artificial intelligence (AI), alongside the growing accessibility of AI platforms and tools, present unique national security risks and opportunities.

– U.S. regulators are implementing AI-related prohibitions, restrictions and reporting requirements across the AI supply chain with a focus on defense and cyber uses of AI, and a particular eye on China.

– While current restrictions and prohibitions regarding AI technology remain narrowly focused on defense and cyber-related capabilities, new requirements focused on monitoring and informing the U.S. government of the state of AI capabilities may lead to future scrutiny of AI, domestically and abroad.

– We do not expect the Trump administration to implement major changes to these regulatory initiatives.

With the rapid commercialization of artificial intelligence (AI) technology, the Biden administration has been grappling with its implications, including its potential impact on national security. Several departments have issued regulations to protect national interests against potential AI threats.

While President Trump said during the election campaign that he would roll back some of the restrictions that have been imposed on AI, we think it is unlikely that the provisions focused on national security — some of which target China, in particular — are likely to be significantly modified under the new administration.

Here is a summary of the major AI-related regulatory initiatives to date and what we believe is likely to remain largely in place.

The Current State of US National Security AI Regulations

Over the past two years, the Biden administration pursued several initiatives to regulate the development of AI in the interest of U.S. national security. President Biden's October 2023 Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (AI Order) laid out both a broad approach and many policy details. With respect to national security, the AI Order directed the U.S. government to establish policies "for addressing AI systems' most pressing security risks — including with respect to biotechnology, cybersecurity, critical infrastructure, and other national security dangers — while navigating AI's opacity and complexity."

Several new regulatory initiatives address that concern, although some rules have yet not been finalized and could be changed or delayed by the new administration:

Investments in Chinese AI companies: On October 28, 2024, the Treasury Department released a final rule restricting U.S. investments in Chinese companies engaged in developing AI systems, quantum technologies, and semiconductors and related computers, equipment and materials. The rule, which takes effect January 2, 2025, imposes additional diligence responsibilities as well as recordkeeping and notification requirements. It also adds restrictions on U.S. persons and their controlled foreign entities engaging in transactions with foreign persons in "countries of concern" (currently limited to China) that perform certain specified activities related to AI, semiconductors and microelectronics, or quantum information technologies.

While the rule attempts to focus on AI technologies that "pose a particularly acute national security threat to the United States," the scope of coverage (*e.g.*, for AI systems for "cybersecurity applications" or "the control of robotic systems") is potentially broad.

AI-related export controls: Building on export controls implemented in the fall of 2022 and 2023, in September 2024 the Commerce Department's Bureau of Industry and Security (BIS) issued an interim final rule tightening export controls on semiconductors and related items, including so-called "neural network" semiconductors that may be used for machine learning of AI systems. This is the latest in a series of efforts by BIS to restrict the export to China of the types of hardware, software and technology powering advanced AI systems.

Transfers of U.S. person data: In February 2024, President Biden signed Executive Order 14117, which directs the Department of Justice (DOJ) to restrict the transfer of bulk U.S. individual or U.S. government-related personal data to countries of concern (*i.e.*, China, Russia, Iran, North Korea, Cuba and Venezuela). Executive Order 14117 is inspired by AI-related concerns. It notes that U.S. adversaries can use AI "to analyze and manipulate bulk sensitive personal data to engage in espionage, influence, kinetic, or cyber operations" and that bulk data sets can "fuel the creation and refinement of AI and other advanced technologies."

On October 29, 2024, the DOJ published a proposed rule to implement these restrictions. We believe it is unlikely this rule will be finalized before the change in administrations.

AI model reporting requirements: On September 11, 2024, BIS proposed a new rule that would require AI companies to report to the U.S. government on their development of dual-use AI foundation models, and related cybersecurity and safety measures. This rule, which would be issued pursuant to the Defense Production Act of 1950 (DPA), would impose periodic reporting requirements on AI companies similar to the initial disclosures that BIS has already required from several AI companies

"Defense-related export and technology controls will remain an area of bipartisan focus, and we would expect continued development of U.S. export controls to address AI-related concerns."

under the AI Order. BIS has the authority under the DPA to conduct industry surveys, and the proposed rule would amend BIS's existing industry survey regulations by mandating ongoing periodic reporting related to relevant AI models and clusters. This rule has not yet been finalized.

Cloud services reporting requirements: In January 2024, BIS issued a proposed rule that would require U.S. cloud services providers to submit reports to BIS when foreign customers use U.S. cloud computing services to train large AI models for potential use in malicious cyber-enabled activity. The proposed rule, which imposes several national security-oriented obligations on U.S. cloud services providers, faced significant pushback from industry. Commerce has indicated that it expects to publish a final rule in December 2024, but this timing is subject to change.

National Security AI Regulations in a Trump Administration

During the presidential campaign, President Trump stated that he would "cancel" the AI Order on "day one." While a new Trump Administration may well carry through with this pledge, we do not expect significant softening of the national security-oriented regulatory initiatives outlined above.

– Congress generally supported, on a bipartisan basis, the Biden administration's initiative to create

restrictions on outbound investments in Chinese companies developing technologies of U.S. national security concern. It is possible that a new administration may impose further restrictions in this area.

– Defense-related export and technology controls will remain an area of bipartisan focus, and we would expect continued development of U.S. export controls to address AI-related concerns.

– While the incoming administration reportedly is considering a massive overhaul of the DOJ, the department's draft rule restricting transfers of data about U.S. persons to China does not seem to be a likely candidate for significant change.

– The draft BIS rules requiring reporting by U.S. AI companies and cloud services providers are perhaps the rules most likely to be changed or delayed, because of their ties to the AI Order (in the case of reporting by U.S. AI companies) and because of significant U.S. industry pushback (in the case of reporting by U.S. cloud services providers).

We also do not foresee changes in other AI-related national security regulations that rest on different legal grounds. For example, we expect continued close scrutiny by the Committee on Foreign Investment in the United States (CFIUS) of foreign investments in domestic AI capabilities and technology. We also expect BIS to implement AI-related U.S. supply

chain restrictions under the Information and Communications Technology and Services regulations — a regulatory program that was initially developed under the Trump Administration.

A Trump administration may also seek to accelerate national security-related AI innovation in the U.S. President Trump's advisers have reportedly worked on a new AI executive order that would seek to remove "unnecessary and burdensome regulations" that impede AI development in the interest of national security. President Biden's October 24, 2024 national security memorandum on "advancing the United States' leadership in Artificial Intelligence" adopted some relatively modest measures in this direction — for example, by prioritizing the recruitment of non-U.S. "AI talent" under U.S. immigration laws. We would not be surprised if the new administration doubles down on these efforts.

———

Authors

Brian J. Egan / Washington, D.C.

Michael E. Leiter / Washington, D.C.

David A. Simon / Washington, D.C.

Tatiana O. Sullivan / Washington, D.C.

Nicholas Kimbrell / Washington, D.C.

———