Department of Commerce
International Trade Administration

American AI Exports Program

[Docket No. 251023-0165]

AUTHORS

Jack Burnham
Research Analyst, FDD's China Program

Craig Singleton
Senior Director and Senior Fellow, FDD's China Program

Leah Siskind
Director of Impact and AI Research Fellow

Washington, DC
November 18, 2025

FDD
FOUNDATION FOR DEFENSE OF DEMOCRACIES

www.fdd.org

Introduction

The Commerce Department's efforts to streamline and promote American artificial intelligence (AI) exports offer a strong opportunity for the United States to cement its lead over China and build the next generation of technologies intended to ensure peace and prosperity.

The United States has an unparalleled AI ecosystem, combining cutting-edge semiconductors, hyperscaler expertise, vast cloud-computing options, and strong software tools with deep capital markets, an open regulatory environment, and developed and dedicated AI expertise. These advantages drive unprecedented commercial opportunities and are also well-suited to enhancing America's enduring assets: its vast array of like-minded allies and partners and its military prowess.

Together, American firms and Washington offer an advantage that no country can currently hope to match, not even China. Accordingly, Beijing has attempted to beg, borrow, and steal from American firms both domestically and overseas to access U.S. AI technologies.

Lacking its own domestic supply of chips, expertise, or a technical edge, China has attempted to leverage a range of legal and illegal means to circumvent U.S. AI export controls. Beijing conducts industrial espionage, smuggles components through neighboring countries, and relies on foreign investments to alleviate American pressure on its domestic AI sector. Largely locked out of America's AI ecosystem, China is reliant on its network of foreign investments in AI, particularly within the Gulf region, to fuel the modernization of the People's Liberation Army. These efforts are backstopped by Beijing's domestic legal architecture, which compels Chinese firms operating abroad to cooperate on matters of state security while allowing the Chinese Communist Party significant sway over corporate decision-making.

To prevent further erosion of America's national security and enhance its AI advantage, the Commerce Department must ensure that American AI exports prioritize close U.S. allies and partners whose foreign policy goals and economic security regulations align with those of the United States and that participating American firms commit to strong physical and cybersecurity measures.

Prioritize Countries and Projects Contributing to Current U.S. AI Priorities

The Commerce Department should prioritize exports to frontline democracies whose expertise and technical edge align with the needs of the United States and its warfighters. Confronting a series of authoritarian powers whose military capabilities have expanded rapidly over the past decade, the United States should tap partners' innovations to improve its military lethality and significantly bolster its warfighting potential. By heavily investing in the development of battle-tested products, allied AI firms can and are providing a valuable service to the American defense industrial base by serving as an effective pipeline for funneling innovation while saving Washington from duplicative spending on research and development.

U.S. allies and partners can positively contribute to the Department of Defense's AI strategy, from improving intelligence, surveillance, and reconnaissance during counterinsurgency and conventional operations to deploying AI-enhanced unmanned aerial systems. Israel has developed certain components of a truly secure, combat-proven AI. These should be integrated into the American tech stack from the start, rather than bolted on later. Israel represents the ideal "trusted partner" model outlined by the Commerce Department, with collaboration between

Israel and American AI companies forming a strategic counterweight to the Iran-China-Russia-North Korea "Axis of Aggressors." The Trump administration has already laid the groundwork for this partnership through an MOU on AI and energy collaboration signed in July 2025. Additional regional alliances founded on knowledge sharing and mutual security will create a ring of AI expertise around Iran.

Additionally, furthering AI partnerships with Ukrainian firms offers a significant benefit to the United States in the form of battle-tested AI systems, which have proven capable of executing both tactical and strategic-level strikes against Russia. As shown by Ukraine's strike against Russia's strategic bomber fleet in June 2025 and by Kyiv's ability to rapidly identify targets using cheap, mass-produced drones, Ukrainian firms offer a wealth of expertise for American forces — lessons that the United States Army is already beginning to integrate into its European command.

The Commerce program should also bolster economic ties with key allies in the Indo-Pacific, particularly Japan and South Korea. With the Trump administration signing technology cooperation agreements with both Seoul and Tokyo, this program should focus on integrating shared AI tools for reconnaissance, surveillance, and monitoring into both countries' alliances with the United States, enhancing their domestic investment partnerships, and building out an open global market for American AI. This approach will also prevent greater Chinese penetration into the global AI market by allowing Washington to capitalize on its current lead.

Prioritize Countries That Demonstrate Commitment to U.S. Economic Security Interests

The program should offer priority to interested countries that have a strong track record of adhering to U.S. economic security practices. The Commerce Department should review the capacity of interested countries to monitor foreign adversarial investments into their AI development streams, such as research, manufacturing, and technology transfers alongside their harmonization with U.S. export controls.

This review should also extend beyond the immediate technology stack to encompass broader security concerns. Focusing upstream, the program should account for recipients' research funding regulations, screening guidelines for international student visas, and capacity for maintaining strict on-campus security measures to prevent unauthorized access to ongoing AI-related research programs. This should be coupled with Commerce's consideration of each country's overarching cybersecurity strategy, particularly in projects related to critical infrastructure, health care, and military-adjacent industries, which have all been repeatedly targeted by Chinese cyber intrusions.

Implement Stringent Cyber-Physical Security Standards for Participating Firms

The export promotion program should also require stringent foreign ownership disclosure requirements, including potentially barring participation by American firms whose ownership structure may be compromised by foreign adversaries. These requirements should apply to any firm owned 10 percent or more by an entity or individual under the control or direction of a foreign adversary, while firms engaged in higher-risk sectors, such as healthcare or defense, should be held to a 5 percent threshold. Rather than seeking to discriminate against foreign investors with holdings in American AI firms, these types of reporting requirements are common across other regulated critical infrastructure sectors to safeguard American intellectual property

and prevent espionage or sabotage. These safeguards are also essential due to China's use of unusual corporate structures, such as "golden shares," and Beijing's National Intelligence Law and Cybersecurity Laws to exert influence and conduct surveillance over Chinese firms operating abroad.

The program should also require exporters to adhere to high cyber and physical security standards, which should apply both to data centers and to their adjacent infrastructure. This adjacent infrastructure includes systems used by third-party contractors, critical communications, and relevant edge devices, all of which Beijing has targeted with malicious cyber operations. Moreover, these standards, which should be set by the National Institute of Standards and Technology, should be subject to periodic reviews and revisions in response to the threat landscape.

Conclusion

As China continues to advance its own AI sector with the aim of displacing the United States as a preeminent global power, Washington must expand its efforts to maintain its scientific and technological edge over Beijing. The Department of Commerce's proposal to allow private firms to ramp up AI exports, while critical to establishing America's lead over China, should be guided by a commitment to close U.S. allies and partners and tempered by stringent security criteria.

Thank you for considering our comments, and we look forward to seeing how our input is incorporated into the department's ongoing policy work.