The Honorable John Thune
Senate Majority Leader
511 Dirksen Senate Office Building
Washington, DC 20515

The Honorable Chuck Schumer
Senate Minority Leader
322 Hart Senate Office Building
Washington, D.C. 20510

Sen. Tim Scott
Chairman
Senate Committee on Banking
534 Dirksen Senate Office Building
Washington, D.C. 20510

Sen. Elizabeth Warren
Ranking Member
Senate Committee on Banking
534 Dirksen Senate Office Building
Washington, D.C. 20510

February 20, 2026

Dear Leader Thune, Leader Schumer, Sen. Scott, Sen. Warren, and Members of the U.S. Senate:

We write to urge you to prioritize passage of the Remote Access Security Act, legislation introduced by Sens. Dave McCormick and Ron Wyden to close a loophole in U.S. export control law that enables foreign bad actors to access advanced AI chips via cloud computing. This critical legislation, which passed the House of Representatives with overwhelming bipartisan support this year, is urgently needed to ensure the Bureau of Industry and Security can fully enforce export controls and prevent destabilizing dual-use technologies from falling into the wrong hands.

Current U.S. export control policy restricts the physical shipment of certain advanced AI chips to China. Yet the law that governs this policy, the Export Control Reform Act of 2018, does not explicitly authorize the Bureau of Industry and Security to regulate remote access to these same chips via cloud computing.

Chinese entities are systematically exploiting this gap at a massive scale. In December 2025, Barron's reported that Tencent, a Chinese company prohibited from purchasing Nvidia's most powerful Blackwell chips, had secured access to 15,000 Blackwell processors through a Japanese cloud provider, Datasection.[1] Because Tencent does not own the chips, this arrangement does not violate current export restrictions. Chinese AI developers can therefore train advanced models using American hardware. These models are deployed for military modernization, mass surveillance, and intelligence operations.[2] They also directly compete with U.S. AI companies for global market share.

[1] https://www.barrons.com/articles/china-tencent-nvidia-blackwell-chips-cloud-9d5e5998?gaa_at
[2] https://www.aspi.org.au/report/the-partys-ai-how-chinas-new-ai-systems-are-reshaping-human-rights/

Tencent is far from the only example. The Financial Times documented that iFlytek – a Chinese AI company sanctioned by the U.S. for human rights violations – accessed banned Nvidia chips through cloud service providers.[3] For Chinese companies boxed out by export restrictions, cloud rental has become a viable strategy.

Top Chinese executives willingly admit that Chinese chip firms cannot domestically produce sufficient compute to meet demand. Tencent's Vice President of its Cloud Computing Unit publicly stated that the most severe problem the company has faced in developing AI "is the [limited] resources of [graphics] cards and computing resources."[4]

Under China's policy of military-civil fusion, commercial AI capabilities developed using American chips are rapidly adapted for military applications.[5] Advanced AI chips accessed through cloud services can support the development of autonomous weapons systems, intelligence surveillance platforms, battlefield decision-making tools, and cyber capabilities that could undermine U.S. national security interests.

Chinese AI labs such as DeepSeek have already demonstrated their capacity to develop frontier AI models that a senior U.S. official warned "willingly provided and likely will continue to provide support to China's military and intelligence operations."[6] A recent analysis by Georgetown's Center for Security and Emerging Technology reviewed thousands of AI-related contracts from the People's Liberation Army (PLA) and found that close to three-quarters of suppliers are "nontraditional vendors" – civilian companies with no state ownership ties – rather than traditional defense contractors.[7] Allowing unrestricted cloud access to our most powerful AI hardware only accelerates Chinese military development.

The Remote Access Security Act addresses this vulnerability by explicitly authorizing the Bureau of Industry and Security to regulate remote access to export-controlled items through cloud computing services. The legislation does not create new export restrictions or impose new controls. It extends existing export control authority to remote access scenarios, giving BIS the ability to ensure that adversaries cannot circumvent physical export controls by accessing the same technology through cloud providers.

The Remote Access Security Act is a measured, necessary update to U.S. export controls that reflects the technological reality of modern computing. Physical possession of advanced chips is no longer required to leverage their capabilities. Our export controls must account for this reality.

---

[3] https://www.ft.com/content/9706c917-6440-4fa9-b588-b18fbc1503b9
[4] https://www.semafor.com/article/12/09/2025/trump-says-nvidia-can-sell-h200-ai-chips-to-china
[5] https://thehill.com/opinion/technology/5630281-nvidia-china-military-chips/
[6] https://www.reuters.com/world/china/deepseek-aids-chinas-military-evaded-export-controls-us-official-says-2025-06-23/
[7] https://cset.georgetown.edu/wp-content/uploads/CSET-Pulling-Back-the-Curtain-on-Chinas-Military-Civil-Fusion.pdf

We strongly urge the Senate to consider and pass the Remote Access Security Act, providing the Bureau of Industry and Security with the clear statutory authority it needs to close this critical loophole and protect America's technological edge from exploitation.

Sincerely,

Brad Carson, *Americans for Responsible Innovation*

Chris McGuire, *Council on Foreign Relations*

Brendan Steinhauser, *The Alliance for Secure AI*

Peter Wildeford, *The AI Policy Network*