United States Senate

WASHINGTON, DC 20510

November 12, 2026

The Honorable Howard W. Lutnick
United States Secretary of Commerce
U.S. Department of Commerce
1401 Constitution Avenue NW
Washington, D.C. 20230

Secretary Lutnick:

We write to urge you to take immediate steps to close loopholes in the export regime for advanced AI chips.

We are deeply concerned by reports that the recently departed CEO of the nation's top semiconductor company, NVIDIA, was caught in a honeypot scheme with a Chinese spy and executive at Megaspeed, a Singaporean firm known to help Chinese companies circumvent export controls.[1] Despite the intelligence community raising concerns that Mr. Huang had been compromised, the Department has taken no action to tighten export controls on Megaspeed and other high-risk companies in Southeast Asia[2]. These concerns are only exacerbated by reports that Under Secretary Kessler discussed ongoing investigations into Megaspeed with NVIDIA's General Counsel.[3] This scenario raises numerous alarms about how you and the Trump Administration are safeguarding highly sensitive technologies.

Our concerns about insufficient export controls on these technologies are magnified by numerous rogue artificial intelligence incidents, including autonomous hacking incidents, unauthorized agent access to the internet, and attacks on real-world targets. Whistleblowers from the nation's leading AI companies have warned that technology is accelerating without sufficient guardrails, further compounding our concerns.

Collectively, these incidents show the urgent need for the Trump administration to act and protect the safety and security of Americans. Responsible U.S. domestic AI policy must promote our competitive edge in artificial intelligence through reasonable innovation and regulation. It should not enable our strategic adversaries to embrace risky behaviors with these technologies or to acquire them through nefarious means.

China's frontier artificial intelligence capabilities are rapidly approaching those of the United States, with some experts estimating China's frontier to be just six to nine months behind the United States.[4] Gaining a competitive advantage is a significant motivating factor behind its development of artificial intelligence. China also seeks to leverage the technology to enhance its national security, including by bolstering military capabilities, surveilling adversaries, and tightening its control over information. This is well demonstrated by Anthropic's recent report *Detecting and countering misuse of AI: September 2026*, in which Anthropic's Threat Intelligence team details incidents in which China-based entities and Chinese

---

[1] https://www.nytimes.com/2026/11/08/technology/nvidia-investigation-jensen-huang.html
[2] https://www.nytimes.com/2026/11/09/business/economy/nvidia-megaspeed-investigation-huang.html
[3] *Ibid.*
[4] https://www.cnbc.com/2026/07/07/chinese-ai-models-costs-us-openai-anthropic.html

government affiliates used artificial intelligence for cyber operations, surveillance, scams and fraud, conventional weapons, and distillation.[5] If China develops superior artificial intelligence capabilities, it would only increase the threat to the United States and its interests around the globe.

Fortunately, the United States and its allies remain ahead in the key technologies necessary to develop and operate the most advanced frontier models: advanced chips and the equipment necessary to manufacture them. To maintain its competitive edge while promoting responsible domestic AI policy, the United States must ensure Chinese AI labs cannot easily procure the compute required to develop, test, and train advanced artificial intelligence models. To overcome this severe disadvantage, China has developed illicit or subversive means to access advanced chips through remote access, smuggling, and U.S. based subsidiaries of Chinese companies.

As you know, Chinese companies are restricted from purchasing advanced chips, yet they can easily *rent* access to them through U.S. subsidiaries, overseas shell companies, and other companies like Megaspeed.[6] The Carnegie Endowment for International Peace has documented at least eleven state-linked Chinese entities seeking access to chips through cloud services. While Congress is considering legislation to address the Department's authorities over remote access to chips, we appreciate that you are reportedly making efforts to close this loophole.[7] However, the details of the policy changes will be critical. We urge you to condition licenses for the export of advanced AI chips on an agreement that recipients will not provide Chinese companies with remote access unless granted a separate and additional license to do so. These policies should not be geographically limited in scope. If they are, China will simply rent access to chips elsewhere, creating a whack-a-mole scenario.

Furthermore, we are concerned by the access afforded to Chinese companies with subsidiaries located in the United States and urge you to restrict the sale of export-controlled chips to these subsidiaries. This risk is most recently exemplified by the Inspur Group and its U.S. subsidiary, Aivres. The Inspur Group has long been listed on the Department of Commerce's Entity List, restricting its capacity to do business with the United States due to security concerns.[8] However, Aivres exported at least $5.6 billion of advanced technology from the United States to Southeast Asia over a two year period, including more than $3 billion of computers containing the advanced Blackwell chips.[9] This technology was then deployed in data centers and technology firms in Southeast Asia, where it serves Chinese tech firms like Alibaba and ByteDance.[10] Unfortunately, this is just one subsidiary. To maintain our competitive edge in artificial intelligence, we must close this loophole expeditiously.

Finally, we urge you to restrict the sale of export-controlled chips to non-trusted companies in countries with a high risk of smuggling, including those in Southeast Asia. Some estimate that smugglers have diverted or resold several hundred thousand chips to China, providing up to 40 percent of its training capacity.[11] However, smuggling operations will likely adapt to geographic restrictions. To preempt this

---

[5] https://www.anthropic.com/threat-intelligence-report-september-2026
[6] https://www.ft.com/content/9706c917-6440-4fa9-b588-b18fbc1503b9?syn-25a6b1a6=1
[7] https://www.theinformation.com/articles/commerce-department-finalizing-long-awaited-ai-remote-access-rule
[8] https://www.nytimes.com/2026/09/06/technology/ai-chips-china-blacklist.html
[9] Ibid.
[10] Ibid.

risk, we urge you to impose a license requirement on exports of large quantities of chips to non-trusted companies in a broader set of countries.

During your confirmation hearing, you called for stronger export controls, saying, "If they are going to compete with us, let them compete, but stop using our tools to compete with us."[12] Today, the stakes are clear, and our adversaries are not playing by the rules. We must close these loopholes if the United States is to maintain its competitive edge in artificial intelligence.

Thank you for your prompt attention to this matter.

Sincerely,

Lisa Blunt Rochester
United States Senator

John Curtis
United States Senator

[11] https://www.cnas.org/press/press-release/new-paper-warns-ai-chip-smuggling-to-china-may-undermine-u-s-national-security-interests

[12] c-span.org/program/senate-committee/commerce-secretary-nominee-howard-lutnick-testifies-atconfirmation-hearing/655039