

JOHN MOOLENAAR, MICHIGAN
CHAIRMAN
ROB WITTMAN, VIRGINIA
ANDY BARR, KENTUCKY
DAN NEWHOUSE, WASHINGTON
DARIN LAHOOD, ILLINOIS
NEAL DUNN, FLORIDA
DUSTY JOHNSON, SOUTH DAKOTA
ASHLEY HINSON, IOWA
CARLOS GIMENEZ, FLORIDA
GUS BILIRAKIS, FLORIDA
YOUNG KIM, CALIFORNIA
NATHANIEL MORAN, TEXAS
ZACH NUNN, IOWA



Congress of the United States
House of Representatives
SELECT COMMITTEE ON CHINA

RO KHANNA, CALIFORNIA
RANKING MEMBER
RAJA KRISHNA MOORTHY, ILLINOIS
KATHY CASTOR, FLORIDA
ANDRÉ CARSON, INDIANA
SETH MOULTON, MASSACHUSETTS
HALEY STEVENS, MICHIGAN
RITCHIE TORRES, NEW YORK
SHONTEL BROWN, OHIO
GREG STANTON, ARIZONA
JILL TOKUDA, HAWAII

January 28, 2026

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

Dear Secretary Lutnick,

As Chairman of the United States House Select Committee on Strategic Competition between the United States and the Chinese Communist Party (Committee), I write regarding NVIDIA Corporation's (NVIDIA) engagement with Hangzhou DeepSeek Artificial Intelligence Basic Technology Research Co., Ltd. (DeepSeek), a People's Republic of China (PRC)-based artificial intelligence (AI) company, and the implications for U.S. national security and the future of American AI dominance. While NVIDIA asserts its relationship with DeepSeek is "to promote the [AI] ecosystem flywheel and improve NVIDIA's products," documents produced to the Committee reveal NVIDIA provided extensive technical support that enabled DeepSeek—now integrated into People's Liberation Army (PLA) systems and a demonstrated cyber security risk—to achieve frontier AI capabilities. These findings demonstrate why rigorous enforcement of the Department's H200 export rule, which requires certification that chips will not serve military purposes, is essential—even if such enforcement effectively prevents H200 exports to the PRC altogether.

NVIDIA's experience with DeepSeek illustrates why the PRC Military-Civil Fusion strategy makes it impossible to distinguish between commercial and military entities. When NVIDIA collaborated with DeepSeek, the company appeared to be exactly what it claimed: a civilian AI research lab. DeepSeek was not on any U.S. blacklist. It operated openly as a commercial entity. Nothing in the public record flagged it as a military contractor. NVIDIA treated DeepSeek accordingly—as a legitimate commercial partner deserving of standard technical support.

Only later did DeepSeek's true nature become clear. As the Committee detailed in its April 2025 report, DeepSeek is not a typical commercial AI system: it routes Americans' data back to the PRC through infrastructure tied to a U.S.-designated Chinese military company, manipulates outputs to comply with Chinese Communist Party (CCP) propaganda and censorship mandates,

steals intellectual property from frontier U.S. AI firms, and runs on advanced NVIDIA chips restricted from export to China.¹

A Jamestown Foundation report released in October 2025 cited PRC military procurement records that confirm DeepSeek is a CCP-aligned AI company whose AI systems are now being integrated directly into military capabilities. PLA entities have reportedly begun deploying DeepSeek models inside PLA institutions, including military hospitals and defense mobilization planning units.² Procurement documents and state media further indicate DeepSeek-enabled tools are being adopted and tested for broader integration across the PRC's command-and-control and intelligence workflows as part of the CCP's push toward "intelligentized warfare."³ In parallel, PRC public security and policing organs are reportedly embedding DeepSeek into surveillance and data fusion systems to strengthen state monitoring, predictive policing, and internal repression.⁴

Beyond enabling PRC military and security capabilities, DeepSeek's free, open-weight models have been shown to be the source of serious cyber security risks. In November 2025, cyber security firm CrowdStrike released a report outlining its internal testing of DeepSeek's R1 671B model directly, i.e., downloading the model weights to a CrowdStrike computer and running it locally. The CrowdStrike Counter Adversary Operations group found that R1 was comparable to Western LLMs in coding, validating DeepSeek's capability. However, their tests also discovered that "when DeepSeek-R1 receives prompts containing topics the CCP likely considers politically sensitive, the likelihood of it producing code with severe security vulnerabilities increases by up to 50%."⁵ In other words, when a DeepSeek user's prompt identified themselves as associated with one of the "CCP five poisons," specifically Uyghurs and the Falun Gong, the code R1 produced was substantially and consistently more vulnerable. While CrowdStrike could not ascertain the reason R1 wrote vulnerable code for a specific set of users, it demonstrates that a PRC-controlled AI alters its output based on the user's identification as an enemy of the CCP.

The Committee requested documents from NVIDIA to understand its relationship with DeepSeek. The records reveal the extent of NVIDIA's support and how it allowed DeepSeek to dramatically improve R1:

¹ DeepSeek Unmasked: Exposing the CCP's Latest Tool for Spying, Stealing, and Subverting U.S. Export Control Restrictions, House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party (Apr. 16, 2025), <https://chinaselectcommittee.house.gov/media/reports/deepseek-unmasked-exposing-the-ccp-s-latest-tool-for-spying-stealing-and-subverting-us-export-control-restrictions>.

² Jack Burnham, China's Military Reportedly Deploys DeepSeek AI for Non-Combat Duties, Foundation for Defense of Democracies (Mar. 27, 2025), https://www.fdd.org/analysis/policy_briefs/2025/03/27/chinas-military-reportedly-deploys-deepseek-ai-for-non-combat-duties/.

³ Sunny Cheung & Kai-shing Lau, DeepSeek Use in PRC Military and Public Security Systems, The Jamestown Foundation (Oct. 27, 2025), <https://jamestown.org/deepseek-use-in-prc-military-and-public-security-systems/>.

⁴ Id.

⁵ Stefan Stein, CrowdStrike Researchers Identify Hidden Vulnerabilities in AI-Coded Software, CrowdStrike, (Nov. 20, 2025), <https://www.crowdstrike.com/en-us/blog/crowdstrike-researchers-identify-hidden-vulnerabilities-ai-coded-software>

- (1) **NVIDIA enabled DeepSeek to achieve “frontier” AI performance on export-controlled chips.** According to NVIDIA records, NVIDIA technology development personnel helped DeepSeek achieve major training efficiency gains through an “optimized co-design of algorithms, frameworks, and hardware,” with internal reporting boasting that “DeepSeek-V3 requires only 2.788M H800 GPU hours for its full training”— less than what U.S. developers typically require for frontier-scale models. In effect, NVIDIA’s technical support allowed DeepSeek to extract near-frontier performance from “deprecated” H800 chips, undermining the export-control bottlenecks that U.S. policy was designed to impose.
- (2) **NVIDIA moved to operationalize and distribute DeepSeek through its enterprise ecosystem.** NVIDIA even proposed “offering DeepSeek as an NVIDIA NIM,”⁶ packaging DeepSeek as an NVIDIA-supported, enterprise-ready product designed for rapid deployment on NVIDIA infrastructure. NVIDIA’s own materials also describe using the “open-source DeepSeek-R1 model” for “automatically generating GPU attention kernels without explicit programming,” further embedding PRC-origin models into NVIDIA’s development pipeline and making DeepSeek easier to run, scale, and adopt worldwide.

NVIDIA provided this extensive support while treating DeepSeek as a civilian customer. Even now, despite mounting evidence of DeepSeek’s integration with the PRC military and security services, NVIDIA CEO Jensen Huang has said “we don’t have to worry” about American chip technology being used by China’s military.⁷ Mr. Huang’s comments reflect a blindness to one of the most effective aspects of the CCP’s military modernization campaign: the PRC’s Military-Civil Fusion strategy erases the line between civilian and military development, while Chinese law compels all entities to cooperate with state intelligence. The H200 rule requires exporters to certify chips will not serve military end users—the very determination NVIDIA was unable to make. If even the world’s most valuable company cannot rule out the military use of its products when sold to PRC entities, rigorous licensing restrictions and enforcement are essential to prevent such assurances from becoming superficial formalities.

I recommend the following actions.

Clarification of H200 End User Restrictions

- The Commerce Department’s recent release of the H200 rule rightly implements national security guardrails on chips sales to the PRC. In particular, it prohibits licensees from transferring or allowing remote access to those chips by prohibited end users such as the military or security services. As illustrated above, chips sales to ostensibly non-military end users in China will inevitably result in a violation of the military end use restrictions. The Commerce Department should issue clarifying guidance on the implementation of

⁶ NVIDIA’s “enterprise-ready model package”—a supported, preconfigured container that makes an AI model easy to deploy and run on NVIDIA GPUs.

⁷ GPS0713-NVIDIA-US-China-AI, CNN (July 13, 2025), <https://www.cnn.com/2025/07/13/world/video/gps0713-nvidia-us-china-ai>.

The Honorable Howard W. Lutnick

January 28, 2026

Page 4 of 4

the end use restrictions to include measures that would effectively and reliably prevent prohibited end users from gaining the type of access the PLA gained from DeepSeek.

OICTS Restriction on PRC-Origin AI Models

- CrowdStrike’s findings show that the use of DeepSeek may implement vulnerable code that can be exploited in the future by a PRC cyber actor. If DeepSeek and other free PRC AI models become standard tools for U.S. software developers, they have the potential to create a systemic cyber security risk across American industries. The Office of Information and Communications Technology and Services (OICTS) should immediately propose sectoral rulemaking to address the risks posed by using AI models developed by PRC entities such as DeepSeek, Alibaba, and Tencent in the United States.

I remain committed to advancing the Administration’s strategy for ensuring America “retain[s] dominance in this global race.”⁸ Accordingly, I request a briefing no later than February 13, 2026, on the above recommendations and how the Department of Commerce will enforce the security guardrails in the H200 rule. I look forward to working with you to ensure America wins the AI race.

Sincerely,



John Moolenaar
Chairman

⁸ The White House, Winning the Race: America’s AI Action Plan (July 2025), <https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf>.