August 1, 2025

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

Dear Secretary Lutnick,

We write to you regarding concerning security vulnerabilities and the potential compromising of American personal and enterprise data through the use of DeepSeek Artificial Intelligence (AI) reasoning models. Recent reporting states that U.S. officials believe that DeepSeek "has willingly provided and will likely continue to provide support to China's military and intelligence operations."[1] The article further states that U.S. officials allege that DeepSeek is sharing user information and statistics with Beijing's surveillance apparatus.[2]

These allegations are deeply troubling. DeepSeek's R1's model release in late January demonstrated the aptitude of People's Republic of China (PRC) national AI talent and the progress their home-grown models have made relative to leading U.S. products. The Trump Administration has rightly emphasized winning the AI competition against the PRC, and the development of AI use case applications for businesses and consumers is an important facet of that competition. Ensuring that such applications are secure and not prone to leaking secure information and malign exploitation is paramount.

R1 offers open-source access to its model weights, meaning that software engineers are able to modify portions of its code in order to further refine outputs to meet specific purposes or complete specialized tasks. Concerningly, R1 has been found to produce potentially harmful content at higher rates than peer American models.[3] It is probable that R1 did not undergo comprehensive red-teaming and safety tests to prevent the generation of harmful content prior to release. For example, a Wall Street Journal reporter was able to get R1 to write text for a social media campaign intended to encourage self-harm amongst teenage girls, as well as to provide instructions for carrying out a bioweapon attack.[4]

Shortly after R1's release, Wiz Research found a publicly accessible database belonging to DeepSeek, which allowed full control over database operations including the ability to access internal data. Concerningly, Wiz researches found over a million lines of log streams containing sensitive information like chat history and secret keys.[5]

Given their restricted access to the most advanced compute resources, the PRC has seemingly adopted a strategy of embedding open-source AI models into applications and services as a way to compete with the U.S. for global AI leadership. At an April 2025 Politburo meeting, PRC President Xi Jinping directed

---

[1] Feng, Coco. "Exclusive: DeepSeek Aids China's Military in AI Push, U.S. Firm Says." Yahoo Finance, 23 June 2025, https://ca.finance.yahoo.com/news/exclusive-deepseek-aids-chinas-military-090153898.html.
[2] *Ibid.*
[3] Schechner , Sam. "DeepSeek Offers Bioweapon, Self-Harm Information." *The Wall Street Journal,* 8 Feb. 2025. https://www.wsj.com/tech/ai/china-deepseek-ai-dangerous-information-e8eb31a8
[4] *Ibid.*
[5] Wiz. (2025, January 29). Wiz research uncovers exposed DeepSeek database leak. *Wiz.io*. https://www.wiz.io/blog/wiz-research-uncovers-exposed-deepseek-database-leak

China's AI industry to be, "strongly oriented toward applications."[6] Further, Huawei founder Ren Zhengfei told *People's Daily* –a Communist Party of China (CCP) newspaper—that, "there will be thousands of open-source software [programs] to meet the needs of the entire society."[7]

The U.S. government has previously recognized the threats posed by the wide-spread adoption of certain PRC technologies. For example, Congress funded a multi-billion program to remove Huawei telecommunications hardware from American networks after it was determined that such hardware could contain backdoors for PRC espionage.

In order to prevent a similar situation, we ask that you identify and evaluate any potential backdoors or vulnerabilities posed by Chinese open-source models like DeepSeek's R1. Particularly, please identify:

1. Any threats which may arise from data collected by such applications being fed back to PRC located servers;
2. Any information regarding verifiable or likely cases of DeepSeek and other Chinese open-source models feeding American personal or enterprise data to the Chinese People's Liberation Army (PLA) or to companies known to be part of the PRC's military-industrial complex or surveillance apparatus.
3. How you plan to use resources like the Center for AI Standards and Innovation (CAISI), to work with relevant agencies with expertise in cyber security, data protection, and national security to investigate how U.S. businesses and persons could be harmed by AI applications built atop R1 and other Chinese open-source models.
4. Any findings related to how Chinese open-source models may have improperly accessed export-controlled semiconductors or violated use terms of U.S. models to advance their capabilities.
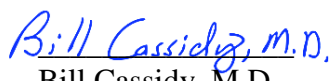
We also request that you provide a briefing to members of Congress and relevant Congressional Committees on your findings and any threats posed by Chinese open-source models as soon as practical.

Thank you for your attention to this request and your efforts to protect American citizens and businesses from potential threats.
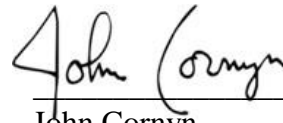
Sincerely,
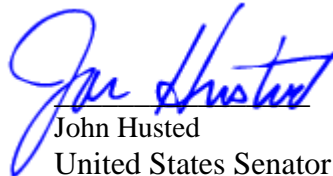

Ted Budd
United States Senator
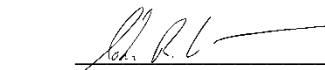
Bill Cassidy, M.D.
United States Senator

John Cornyn
United States Senator

Marsha Blackburn
United States Senator

John Husted
United States Senator

John Curtis
United States Senator

Todd Young
United States Senator

---

[6] Rosen, Miriam. "China's Use of AI in its Military Modernization." *RAND Corporation*, July 2024, https://www.rand.org/pubs/perspectives/PEA4012-1.html.