United States Senate
WASHINGTON, DC 20510

February 10, 2025

Ms. Leslie A. Beavers
Acting Chief Information Officer
Department of Defense
6000 Defense Pentagon
Washington, D.C. 20301-6000

Dear Ms. Beavers,

We write to express our concern that Department of Defense (DoD) employees accessed the Chinese artificial intelligence application DeepSeek on their work devices and, as a result, Chinese servers.[1]

We understand that the National Security Council (NSC) is currently reviewing the national security implications of DeepSeek and expect this will be an ongoing conversation between Congress, the NSC, and relevant agencies.[2] However, in the immediate term, we request that the Department provide information regarding potential impacts to the Defense Information Systems Network (DISN) and the Department of Defense Information Network (DODIN) of the recent incident.

The office of the *Director of National Intelligence's 2024 Annual Threat Assessment* states that "China remains the most active and persistent cyber threat to the U.S. Government, private-sector and critical infrastructure networks".[3] This is evidenced by the recent Salt Typhoon Hack, a breach of at least eight U.S. telecommunications providers, among many other reports of cyberattacks originating from China.

It is also our understanding, based on the *DoD's Use of Mobile Applications 2023*[4] report, that misuse of mobile applications on DoD personnel devices may not be simply a series of isolated incidents. While our immediate concern is to understand the impact of DoD employees' access to DeepSeek on national security, we are also interested in understanding the DoD's policy regarding mobile device applications to the end of ensuring we are diminishing cybersecurity risks associated with certain platforms.

---

[1] Katrina Manson & Jordan Robertson, Pentagon Staff Used DeepSeek's Chatbot for Days Before Block, *Bloomberg* (January 30, 2025), https://www.bloomberg.com/news/articles/2025-01-30/pentagon-workers-used-deepseek-s-chatbot-for-days-before-block?embedded-checkout=true

[2] Andrea Shalal et al, White House evaluates effect of China AI app DeepSeek on national security, *Reuters* (January 28, 2025), https://www.reuters.com/technology/artificial-intelligence/white-house-evaluates-china-ai-app-deepseeks-affect-national-security-official-2025-01-28/.

[3] Office of the Director of National Intelligence, Annual Threat Assessment of the U.S. Intelligence Community (2024), https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf

[4] Department of Defense Office of Inspector General, Management Advisory: The DoD's Use of Mobile Applications (2023), https://www.dodig.mil/reports.html/Article/3294159/management-advisory-the-dods-use-of-mobile-applications-report-no-dodig-2023-041/

Therefore, we request answers to the following questions by no later than March 4, 2025.

- How many Department employees connected their work computers and/or mobile devices to Chinese servers via the DeepSeek Application?
- Has the DeepSeek app now been deleted from all DoD devices? If not, what steps will you take to ensure the DeepSeek app is removed from all DoD devices?
- What steps have been made to limit access on DoD devices to only those applications with a justified and approved need?
- What is the Defense Information Systems Agency's (DISA's) initial assessment about whether Chinese servers were able to access and exfiltrate sensitive information due to Department personnel use of DeepSeek?
- How has the use of the DeepSeek app by Department personnel impacted the operational and cybersecurity risks to the DISN as well as the DODIN?
- What guidance or training has DISA shared with Department employees regarding accessing Chinese AI app DeepSeek or any other Chinese-affiliated app?
- We understand that the Navy issued guidance against using open-source AI systems for official work. What guidance (if any) are the other services and/or the Department issuing to employees?
- What is DISA's process for assessing which networks, websites and or applications have a connection to the People's Republic of China and what are DISA's standard operating procedures when made aware of such a connection?
- What action (if any) has been taken regarding the DoD employees who connected their work computers and/or mobile devices to Chinese servers via the DeepSeek Application?
- Have all of the recommendations from Management Advisory: The DoD's Use of Mobile Applications (Report No. DODIG-2023-041) been implemented? If not, why not?

Thank you for your consideration and we look forward to hearing from you and working with the Department of Defense to keep our networks safe from persistent cyber threats.

CC:

Lt. Gen. Paul T. Stanton, Director of the Defense Information Systems Agency

Sincerely,

Ted Budd
United States Senator

Eric S. Schmitt
United States Senator

Tommy Tuberville
United States Senator

Mark Kelly
United Staes Senator