United States Senate
COMMITTEE ON FOREIGN RELATIONS
WASHINGTON, DC 20510–6225

July 29, 2025

The Honorable Pete Hegseth
Secretary of Defense
U.S. Department of Defense
1400 Defense Pentagon
Washington, DC 20301-1400

Dear Secretary Hegseth:

I am writing with deep concern about recent reporting that Microsoft allowed software engineers located in the People's Republic of China (PRC) to access and maintain critical Department of Defense (DOD) systems, including those of other U.S. federal agencies, posing a grave national security risk to the United States.[1] While I am encouraged that Microsoft has announced that it will end this arrangement, this incident raises serious questions about whether the DOD is fully implementing U.S. laws that require guardrails around the procurement of information technology (IT) systems.[2]

In 2018, I authored Section 1655 of the Fiscal Year 2019 National Defense Authorization Act (NDAA), which requires contracting entities with the DOD to disclose instances in which they have been asked to share their source code with any country that poses a cybersecurity threat to the United States, including the PRC.[3] This requirement followed revelations in 2018 that HP Enterprise had allowed a Russian defense agency to review the company's cybersecurity software, which at the time the Pentagon was using to defend its own networks.[4] While I was pleased to see the DOD issue a notice of proposed rulemaking in November 2024 in order to implement this law, it unfortunately took the Department ***six years*** to take this initial step.[5] Meanwhile, PRC engineers were engaged in providing support to the DOD that could have exposed the Department to serious vulnerabilities.

PRC-nexus cyber actors have become increasingly sophisticated and better resourced in recent years and therefore pose a higher risk to U.S. national security. In November 2016, the PRC enacted its Cybersecurity Law, which grants the Chinese Communist Party even more powers to demand access

[1] Renee Dudley, "A Little-Known Microsoft Program Could Expose the Defense Department to Chinese Hackers," *ProPublica*, July 15, 2025; Renee Dudley, "Microsoft Used China-Based Support for Multiple U.S. Agencies, Potentially Exposing Sensitive Data," *ProPublica*, July 25, 2025.
[2] Stephen Nellis, "Microsoft to Stop Using Engineers in China for Tech Support of U.S. Military, Hegseth Orders Review," *Reuters*, July 18, 2025.
[3] John S. McCain National Defense Authorization Act for Fiscal Year 2019, (P.L. 115-232), Aug. 13, 2018.
[4] "HP Enterprise Let Russia Scrutinize Cyber Defense System Used by Pentagon," *Reuters*, Oct. 2, 2017.
[5] "Defense Federal Acquisition Regulation Supplement: Disclosure of Information Regarding Foreign Obligations," *Federal Register,* November 15, 2024.

from PRC-based entities to sensitive data, including cybersecurity vulnerabilities.[6] These facts alone make Microsoft's contract with individuals in the PRC highly concerning.

I respectfully request a response to the following questions **no later than August 15, 2025**:

- What is the anticipated timeline for the final rule to implement Section 1655 and why did it take six years for the DOD to issue the proposed rulemaking?
- Did the DOD's contract with Microsoft include a clause, consistent with subsection (c) of Section 1655, requiring the contracting entity to disclose to the DOD when the entity has an obligation to share sensitive information with a foreign government? If so, did Microsoft disclose to the DOD that it is obligated to allow the PRC government to review the code of its product, should the PRC government request it under its Cybersecurity Law?
- How does the DOD intend to mitigate similar risks in the future, including via the implementation of Section 1655?
- What is the scope of the review you announced on July 18, 2025? Please provide the results of that review and any additional steps the DOD will take as a result.

As cybersecurity risks stemming from the PRC compound, the United States government should not be proactively opening the door to its critically sensitive IT systems due to a lack of U.S. government oversight.

Thank you for your attention to this matter, and I look forward to receiving your response.

Sincerely,

Jeanne Shaheen
Ranking Member

[6] Rogier Creemers et al., "Cybersecurity Law of the People's Republic of China," *Stanford University*, June 29, 2018.