United States Senate
WASHINGTON, DC 20510

Mr. John Sherman
Office of the Department of Defense
Chief Information Officer
6000 Defense Pentagon
Washington, D.C. 20301-6000

May 29, 2024

Mr. Sherman,

We write with serious concern that the Department of Defense (DoD) is doubling down on a failed strategy of increasing its dependence on Microsoft at a time when Congress and the administration are reviewing concerning cybersecurity lapses that led to a massive hack of senior U.S. officials' communications.

On May 15, 2024, Axios published a draft DoD memo, which would require DoD components using Microsoft's 365 cloud-based productivity software to upgrade to the most expensive software license, known as E5. The memo states that the upgrade is necessary to enhance security, compliance, and analytical capabilities that Microsoft reserves to customers that pay for premium E5 licenses.

Although we welcome the Department's decision to invest in greater cybersecurity, we are deeply concerned that DoD is choosing not to pursue a multi-vendor approach that would result in greater competition, lower long-term costs, and better outcomes related to cybersecurity. Cybersecurity should be a core attribute of software, not a premium feature that companies upsell to deep-pocketed government and corporate customers. The Department of Defense is one of the largest purchasers of cybersecurity services. Through its buying power, DoD's strategies and standards have the power to shape corporate strategies that result in more resilient cybersecurity services. When the DoD demands sophisticated cybersecurity products, there are not only positive effects across the U.S. government, but also beneficial consequences across the public and private sector. The Department of Defense's pursuit of an anti-competitive strategy results in wasted taxpayer dollars and promotes a stagnant environment for innovation that has negative spill-over effects far beyond the federal government.

The risks associated with the government's dependence on Microsoft were evident when a hacking group associated with the Chinese government known as Storm-0558 successfully compromised 22 enterprise organizations and over 500 individuals globally due to what the Cyber Safety Review Board (CSRB) described as "a cascade of failures" by Microsoft. According to press reports, in May 2023, Storm-0558 successfully exploited vulnerabilities across email systems used by the U.S. State Department, U.S. Department of Commerce, and the U.S. House of Representatives. Those same press reports reveal that hackers accessed thousands of sensitive emails by high-level officials, including the Secretary of Commerce and high-ranking officials at the Department of State among others.

Moreover, DoD's further push towards software monoculture exposes our national security apparatus to avoidable risks. DoD should embrace an alternate approach, expanding its use of open source software and software from other vendors, that reduces risk-concentration to limit the blast area when our adversaries discover an exploitable security flaw in Microsoft's, or another company's software. The CSRB report released in April 2024 only reinforces this point.

To inform our work ahead of the Senate Armed Services Committee mark-up of the FY 2025 National Defense Authorization Act, we request responses to the following:

1. The Department of Defense has had 180 days since the enactment of the FY 2024 NDAA to comply with the cybersecurity reporting requirement contained in Section 1553. As Chief Information Officer of the Department, when do you plan to release the required report and provide a briefing to members of Congress and their staff?
2. Please walk us through the DoD's technical justification process which led to mandating deployment of all Microsoft E5 security solutions to meet 91 of the target level Zero Trust requirements. Additionally, given this mandate, the DoD will be depending on one company for the majority of its productivity, collaboration, security, cloud, and OS needs. What consideration was given to the fact our near peer adversaries seemingly need to breach just one company to potentially compromise DoD assets and data?
3. The only vendor mentioned in the draft memo is Microsoft. Do you plan to provide guidance for interoperability with other cybersecurity vendors? If not, why?
4. What is your plan for ensuring a multi-vendor approach that encourages innovation and competition?
5. DoD' 2018 Cyber Strategy directed the Department to increase the use of secure open source software. Please describe DoD's efforts to meet this directive.
6. In each of the last three fiscal years, how much financial support has DoD provided to support the maintenance of and cybersecurity-related improvements to open source software projects used by DoD?
7. In the aftermath of the Storm-0558 hack, Microsoft pledged to provide free enhanced security logs to its customers, rather than restricting those logs to organizations paying for E5 licenses. Has Microsoft made good on its promise to provide enhanced security logs free of charge to DoD?
8. Your draft memo requires DoD components to begin initiating implementation of E5 by June 3, 2024. What is the rationale for the timeline requested in the draft memo?

As our national security becomes more intertwined with technology, it is imperative Congress and the DoD work together to ensure robust cybersecurity practices. We appreciate your attentiveness to these concerns, as well as your prompt response to these questions.

Sincerely,

Eric S. Schmitt
United States Senator

Ron Wyden
United States Senator