C.A. DUTCH RUPPERSBERGER
2ND DISTRICT, MARYLAND

REPLY TO:

2206 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
(202) 225-3061
FAX: (202) 225-3094

375 WEST PADONIA ROAD, SUITE 200
TIMONIUM, MD 21093
(410) 628-2701
FAX: (410) 628-2708

www.dutch.house.gov

Congress of the United States
House of Representatives
Washington, DC 20515

COMMITTEE ON APPROPRIATIONS

SUBCOMMITTEES:
Commerce, Justice, Science and Related Agencies
Defense
Homeland Security

Facebook.com /RepDutchRuppersberger
Instagram.com/DutchRuppersberger
Twitter.com /Call_Me_Dutch

February 23, 2023

The Honorable Lloyd J. Austin, III
Secretary of Defense
1000 Defense Pentagon
Washington, DC 20301-1000

Dear Secretary Austin,

As the home to the National Security Agency, Fort Meade, U.S. Cyber Command, the Defense Information Systems Agency (DISA), the 175th Cyberspace Operations Group, and Aberdeen Proving Ground, the State of Maryland prides itself on being the Cyber Capital of the world. Since 2003, I have proudly represented Maryland's second congressional district in the United States Congress and have long been a staunch advocate for bolstering our nation's cybersecurity, both here in Maryland and across the Department of Defense (DoD). Over the course of my more than twenty years in public service, I have seen first-hand the critical importance of utilizing the best, most advanced defenses in our cyber domain in the digital information age and as great power competition continues to grow.

I strongly support the Biden Administration's actions over the past two years to improve the country's cybersecurity defenses, including through the President's Executive Order on "Improving the Nation's Cybersecurity" issued in May 2021, and its memo on "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles " in January 2022. I was also pleased to see the release of the "DoD Zero Trust Strategy" last November, which "...spells out how it plans to move beyond traditional network security methods to achieve reduced network attack surfaces, enable risk management and effective data-sharing in partnership environments, and contain and remediate adversary activities over the next five years" (DoD Press Release, Nov. 28, 2022).

Given the many components needed for a comprehensive cybersecurity solution that meets DoD's Zero Trust Strategy, such as Endpoint Detection and Response, Identity and Access Management, Vulnerability Management, and Security Information and Event Management, it is critical that DoD pursue a fair and open competition that ensures procurements for cybersecurity solutions are based on technical merits and are not limited to a single one-size-fits-all enterprise solution.

I am concerned the Department may default to the "path of least resistance" in the name of achieving Zero Trust Strategy at the cost of competition from a diverse set of cybersecurity vendors and ultimately putting mission at risk with inferior solutions. Procurement vehicles that only allow for large technology companies with significant market power (50 percent or more in a relevant market) to bundle operating systems, applications, and cybersecurity into large enterprise-wide agreements limit competition and fail to appropriately value the cybersecurity merits of the proposed solutions.

Having a single vendor across multiple software segments also presents a far more attractive and vulnerable target for cyber-attacks by sovereign and private bad actors. Foreclosing smaller, “best of breed” vendors also discourages the innovation and new entry necessary to stay ahead of expanding cyber-attack capabilities.

In addition to stifling competition, large, bundled procurements often lock agencies into long-term licenses on bundled products that increase costs over time—which are not apparent at the outset. Agencies then face increasingly high switching costs that act as barriers to entry and effectively foreclose smaller or single-product vendors—regardless of their potential functional superiority and/or lower cost.

Finally, the vendor responsible for developing and/or running hardware and software programs should not be the same vendor responsible for testing security, conducting security audits, or reporting on security. Much like the proverbial “fox guarding the henhouse,” that would appear to create an inherent conflict of interest and misaligned incentives for the vendor.

As part of this engagement, please provide answers to the following questions:

1. How would a single vendor across multiple software segments and for multiple cybersecurity requirements present increased vulnerabilities for cyber-attacks by sovereign and private bad actors?

2. If DoD relies on the same vendor that develops and/or operates hardware and software to also test the system for security, conduct security audits, or report on security, how is the Department mitigating/working around the inherent conflict of interest and misaligned incentives that such a structure creates?

3. What is DoD’s strategy to ensure that no single vendor has a broad enough enterprise license agreement that it locks out “best of breed” cybersecurity solutions and thereby increases cyber risk?

4. Does DoD plan to issue a new department-wide acquisition strategy to meet Zero Trust requirements that includes a fair and open competition for multiple cybersecurity vendors?

5. Are there concerns that entering an enterprise agreement for cybersecurity solutions with a large technology company with significant market power discourage innovation and new entry necessary to stay ahead of expanding cyber-attack capabilities? Why or why not?

6. Recognizing that there are many components to a comprehensive cybersecurity solution, such as Endpoint Detection and Response, Vulnerability Management, Identity and Access Management, and Security Information and Event Management, what is your strategy to ensure that the Department incorporates the best of each component to ensure reduced cyber risk?

I am well versed in the challenges of Federal agencies to modernize their Information Technology systems and managing in real-time the cybersecurity threats from China, Russia, and Iran facing the government. Given the critical importance and on-going attacks from our adversaries, I request an in-person briefing on this matter.

Thank you for your attention to this issue and I look forward to a constructive dialogue in the months ahead.

Sincerely,

C.A. Dutch Ruppersberger

C.A. Dutch Ruppersberger
Member of Congress