



CHIEF INFORMATION OFFICER

## DEPARTMENT OF DEFENSE

6000 DEFENSE PENTAGON  
WASHINGTON, D.C. 20301-6000

MAY 30 2023

The Honorable C.A. Dutch Ruppertsberger  
U.S. House of Representatives  
2206 Rayburn House Office Building  
Washington, DC 20515

Dear Representative Ruppertsberger:

Thank you for your letter dated February 23, 2023, regarding the pursuit of a fair and open competition that ensures procurements for cybersecurity solutions are based on technical merits. I am responding on behalf of Secretary Austin as his senior advisor for cybersecurity solutions, Zero Trust (ZT), and for all matters pertaining to the Department of Defense (DoD or Department) cybersecurity posture.

The Department is looking for industry to accelerate the adoption of ZT Target Level in advance of the FY 2027 deadline established by the DoD ZT Strategy. The Office of Secretary of Defense (OSD) Cost Assessment and Program Evaluation (CAPE) directed a detailed analysis led by DoD CIO and United States Cyber Command (USCYBERCOM) with support from the Defense Information Systems Agency (DISA), National Security Agency (NSA), and the Military Services to inform the long-term way forward. In other areas such as DISA's Thunderdome project and Enterprise Identity, Credentialing and Access Management (ICAM), we are pursuing interoperable best-of-breed capabilities with the specific intent of ensuring they support the DoD's complex and hybrid cyber terrain.

The following are answers to the specific questions:

**Question 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?**

DoD Components will determine the acquisition strategy approach that best meets their unique environments. Single vendor solutions provide multiple advantages and disadvantages that need to be weighted against multi-vendor solutions to define the best-of-breed solutions. The objective is to define which solutions best achieve ZT Target Levels. In some cases, it is possible that single vendor solutions might not address the full range of requirements based on the threat environment and therefore require a multi-vendor approach.

**Question 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?**

The Department has a robust process for independent evaluation of vendor procedures prior to granting provisional authorization. Also, accreditation requirements will be layered upon each application within commercial cloud offerings to provide cybersecurity protections based upon specific controls and criticality of the data and applications. We depend upon data from vendor tools to provide dashboarding for defensive cyber operators and cyber security service providers. All tool choices must also balance costs, performance, and terrain coverage so the CAPE analysis mentioned earlier will help drive the Department's long-term plan.

**Question 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?**

We share this concern and we're working towards a long-term balanced strategy. As an example, one vendor's license bundling model may be attractive from a cost perspective but may include an array of cyber and non-cyber capabilities. While this bundled licensing could play a part for some endpoints and for some cloud hosting terrain, it is not applicable to all endpoints, all commercial cloud terrain, or many of the other facets of DoD's IT infrastructure.

For endpoint security, we are focusing on data and functional requirements rather than requiring specific tools for use across the DoD enterprise. While costs are not the sole driver, the Department must determine the best value it can receive from both the large and small cybersecurity vendors. Our current cyber defenses include layers provided by multiple vendors. We do not expect that to change but are continuously evaluating the mix of tooling at each point within our infrastructure and believe this will require continuous tuning to defend against emerging threats and incorporate improving capabilities.

**Question 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?**

The Department is committed to fair and open competition for the procurement of cybersecurity solutions. Examples of this commitment are the recently awarded competitive Joint Warfight Cloud Capabilities (JWCC) Contract or the Department's increased use of competitive Other Transaction Authority (OTA) contracting processes (e.g., Thunderdome) for cyber requirements.

There is no anticipation or need for a new department-wide acquisition strategy. The Components are developing approaches for acquisition of ZT capabilities and solutions as part of their ZT Implementation Plans (I-Plans) due in January 2024. Components are responsible for conducting any market research and requirements definition to determine if they need to revise their current acquisition strategies. These ZT requirements will not preclude Components from meeting fair and open competition requirements as prescribed in the Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation Supplement (DFARS).

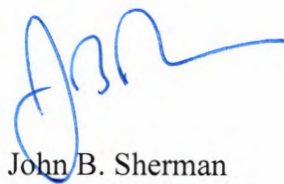
Additionally, the Department is currently assessing DoD-wide acquisition guidance and policy for implementing the DoD ZT Strategy. This includes assessing the need for inclusion of ZT related acquisition language into existing policy or development of additional guidance.

**Question 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?**

Enterprise licensing agreements are generally the best way to achieve DoD buying power but need to be carefully crafted to reflect the fluid nature of cyber requirements. Absent these agreements, each component only receives cost breaks based upon their specific order quantities. Contract vehicles like the Navy enterprise software initiative (ESI) and the Defense Office Solutions (DEOS) contracts balance commitments and costs to achieve best value. On a macro-level, we are leveraging industry innovation driven across the commercial market. That innovation is not typically dependent upon being selected for use in the DoD. As an example, we are implementing automated security validation tooling that originated in the commercial sector and are evaluating other commercial tools that could possibly replace legacy government created solutions.

Thank you for your interest in the Department’s cybersecurity posture and a fair and open competition process for the Zero Trust Strategy implementation. DoD’s goal remains to ensure all vendors are given an opportunity to compete fairly and openly regardless of size. We look forward to the in-person brief to address any further questions or concerns.

Sincerely,

A handwritten signature in blue ink, appearing to read "John B. Sherman", is positioned above the printed name.

John B. Sherman