CompTIA.

September 14, 2021

The Honorable Adam Smith
Chairman
House Armed Services Committee
2216 Rayburn House Office Building
Washington, DC 20515

The Honorable Mike Rogers
Ranking Member
House Armed Services Committee
2216 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Smith and Ranking Member Rogers:

On behalf of the Computing Technology Industry Association (CompTIA), we appreciate your efforts to advance the Fiscal Year 2022 National Defense Authorization Act through the House of Representatives. We would respectfully request the minor attached additions to Section 1502 (Enterprise Procurement of Commercial Cyber Threat Information Products) within a manager's amendment when the legislation is considered on the House floor.

As you may know, CompTIA is a leading voice and advocate for the $5 trillion global information technology ecosystem; and the estimated 75 million industry and tech professionals who design, implement, manage, and safeguard the technology that powers the world's economy. Through education, training, certifications, advocacy, philanthropy, and market research, CompTIA is the hub for advancing the tech industry and its workforce.

Our suggested language would (1) require the inclusion of the use of artificial intelligence-based endpoint security that prevents cyber-attacks and does not require constant internet connectivity to function. to include the use of artificial intelligence-based endpoint security that prevents cyber-attacks and does not require constant internet connectivity to function and (2) include enhancing the security of the Department's software supply chain within the provision's coordination mandate as it relates to commercial cyber threat information product.

The Department of Defense should leverage innovative technologies and invest in its cybersecurity capabilities and workforce to help prevent, respond to, and recover from cyberattacks. Artificial Intelligence (AI)-driven cybersecurity tools use AI to improve cyber threat prevention, protection, and remediation by quickly reviewing large volumes of cyber incident data, including information drawn from previous malware attacks, while leveraging machine learning (ML) and automation to identify potential threats. The Department should prioritize consideration of unified endpoint security tools leveraging AI and ML to enable best-in-class prevention, response, and recovery from cyberattacks.

Additionally, as the U.S. is expected to face a shortage of 1.8 million skilled cybersecurity workers by 2022, educating and empowering the next generation of cybersecurity professionals is imperative to our future national and economic security. Government must continue to invest in cyber skills and knowledge for government employees but also seek creative and economical ways to fill gaps.

We are hopeful that you would either consider these minor changes to Section 1502 within a manager's amendment. We strongly believe that these adjustments would strengthen Section 1502 and better equip the Department of Defense with the tools they need to effectively counter ongoing cyber threats.

Sincerely,

David Logsdon
Staff Director, CompTIA Federal Cybersecurity Committee