



June 14, 2022

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

Ranking Member Mike Rogers  
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 are writing to express our support for the committee's work thus far on the Fiscal Year 2023 National Defense Authorization Act. CompTIA is a leading voice and advocate for the \$5 trillion global information technology ecosystem and the estimated 75 million industry and technology professionals who design, implement, manage, and safeguard the technology that powers the world's economy. CompTIA's Public Sector Cybersecurity Committee connects leading cybersecurity and information technology companies with key cybersecurity decision makers and stakeholders across the federal government. It works closely with federal departments and agencies, the White House, and Congress, to advocate for sustained federal investment in cybersecurity and modern commercial capabilities across government and privately-owned critical infrastructure.

We respectfully request the minor attached additions to the mark approved last week by the Cyber, Innovative Technologies, and Information Systems Subcommittee – within a section entitled “Sec. 2\_\_\_\_[Log 75005]. Study on Costs Associated with Underperforming Software and Information Technology.” Our suggested language would: (1) ensure that the personnel survey reflect on cybersecurity issues within the independent study's broader focus on software and information technology challenges, and (2) ensure that the recommendations developed to address the most important software and information technology challenges identified, including those related to cybersecurity, examine how the Departmentwide adoption of mature artificial intelligence-based endpoint security could help address those challenges.

Representatives Jay Obernolte (R-CA) and Jimmy Panetta (D-CA) recently introduced the [Artificial Intelligence for National Security Act \(H.R. 7811\)](#). This bipartisan legislation offers an important expansion on Section 1521 of last year's NDAA (P.L. 117-81), “Enterprise-wide procurement of cyber data products and services” by requiring the inclusion of artificial intelligence-based endpoint security that prevent cyberattacks and does not require constant internet connectivity to function, among the cyber data products to be procured by the new program management office established under that provision.

In tandem with efforts to move the *Artificial Intelligence for National Security Act* forward, our suggested language would further promote the adoption of mature artificial intelligence-driven cybersecurity tools that are urgently needed at the Department of Defense, as highlighted at the Subcommittee on Cyber's May 3, 2022 [hearing](#) to receive testimony on artificial intelligence applications to operations in

cyberspace. Especially in today's evolving cyber threat environment, these advanced technologies are critical to the department's ability to improve cyber threat prevention, protection, and remediation by quickly reviewing large volumes of cyber incident data and leveraging machine learning to identify potential threats on the horizon.

At CompTIA, we appreciate the committee's focus on advancing innovative solutions that prioritize cyber threat response – especially at the nexus of cybersecurity and emerging technologies. We are hopeful that you will consider these minor adjustments to this section within a manager's amendment ahead of the forthcoming full committee markup next week. We strongly believe that these additions would enhance the already strong cybersecurity provisions within this year's NDAA, and better prepare the Defense Department with the sophisticated technologies required to effectively counter against the cyber threats – both now and in the future.

Sincerely,

A handwritten signature in black ink, appearing to read 'D. Logsdon', with a horizontal line extending to the right.

David Logsdon  
Staff Director, CompTIA Public Sector Cybersecurity Committee