CompTIA

September 30, 2021

The Honorable Jack Reed
Chairman
Senate Armed Services Committee
228 Russell Senate Office Building
Washington, DC 20510

The Honorable James Inhofe
Ranking Member
Senate Armed Services Committee
228 Russell Senate Office Building
Washington, DC 20510

Dear Chairman Reed and Ranking Member Inhofe:

On behalf of the Computing Technology Industry Association (CompTIA), we appreciate your efforts to advance S. 2792, the Fiscal Year 2022 National Defense Authorization Act (NDAA), through the Senate. As the legislation moves to the Senate floor, we would respectfully request that you include:

- Section 1502 (Enterprise-Wide Procurement of Commercial Cyber Threat Information Products) from the House-passed version of the NDAA (H.R. 4350), with the below minor changes if there is an opportunity within the manager's amendment.
- Section 802 (Special Emergency Reimbursement Authority) from the House-passed version of the NDAA, with the below minor changes if there is an opportunity within the manager's amendment.

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.

Section 1502 of H.R. 4350

Section 1502 would direct Joint Forces Headquarters-Department of Defense Information Networks (JFHQ-DODIN) to establish a program management office for the purposes of procuring and managing the Department of Defense's enterprise-wide licensing and use of commercial cyber threat information products.

S. 2792 already contains notable references in Section 1612 ("Comparative Analysis of Cybersecurity Capabilities") to the Committee's interest in the artificial intelligence (AI) and machine-learning (ML) capabilities associated with cybersecurity tools used across the

Department, as well as how adoption of commercial off-the-shelf (COTS) solutions for the continuous monitoring and management of the Department's internet-facing systems and assets ("Application of commercial off-the-shelf solutions to address intelligence and operations gaps" item of special interest) has contributed to JFHQ-DODIN's abilities to conduct defensive cyber operations, to secure the DODIN, and could similarly benefit U.S. Cyber Command.

The modification we are proposing to Section 1502 of H.R. 4350 would bridge the House's focus on establishing consistency across the enterprise-wide procurement of commercial cyber threat information products with S. 2792's emphasis on the value of COTS AI/ML-enabled cybersecurity tools to enhance the Department's cybersecurity capabilities.

We support the goals of Sec. 1502, but recommend the following two minor additions –

Our suggested language would:

(1) Require the inclusion of artificial intelligence-based endpoint security use that prevents cyberattacks 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 products.

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. 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 ML and automation to identify potential threats. The Department should prioritize consideration of unified endpoint security tools that leverage AI and ML to enable best-in-class prevention, response, and recovery from cyberattacks.

Section 802 of H.R. 4350

Section 802 takes the lessons learned during COVID—and builds upon the authorities established in section 3610 of the CARES Act (P. L. 116-136)— to create a permanent authority that would allow the Department of Defense to retain its contractor workforce in the event of a future pandemic.

Section 3610 of the CARES Act authorized federal agencies to reimburse certain company expenses for keeping skilled and trusted personnel in a ready state when they are unable, through no fault of their own, to perform work due to government-imposed closures or similar restrictions. The authority could be used at the discretion of the contracting officer as appropriate to the mission, and as directed by the implementation guidance – without requiring any additional appropriations.

This authority has been a critical lifeline for government programs and the contractor industry during the COVID-19 emergency. It has been used across government, including by DoD, DHS, NASA, the Department of Energy, and the Intelligence Community. As noted in a recent Government Accountability Office (GAO) report, 80% of the contractors they spoke to indicated that "paid leave reimbursement had a great or moderate effect on their ability to retain employees, in particular those with specialized skills or clearances."

We support the goals of section 802 of H.R. 4350, but recommend the following minor changes:

Our suggested language would:

(1) Extend the scope of the special emergency authority to cover all federal agencies, not just the Department of Defense; and

(2) Allow the authorities to be used for a broader set of potential future emergencies, including an emergency or major disaster as defined in section 102 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5122), which prevents the employees of a contractor of the Department of Defense or the employees of a subcontractor (at any tier) of such a contractor from performing work under a covered contract, as determined by the Secretary.

We are hopeful that you would consider including Sections 1502 and 802 of the House's version of the NDAA and incorporate our suggested changes within a manager's amendment. We strongly believe that these adjustments would better equip the Department of Defense with the tools they need to effectively counter ongoing cyber threats and ensure that government-wide operations are better prepared to mitigate unforeseen emergency disruptions to the government-wide industrial base.

Sincerely,

David Logsdon
Staff Director, CompTIA Federal Cybersecurity Committee