CompTIA.

May 21, 2021

The Honorable Jack Reed
Chairman
Committee on Armed Services
United States Senate
Washington, DC 20510

The Honorable James Inhofe
Ranking Member
Committee on Armed Services
United States Senate
Washington, DC 20510

The Honorable Adam Smith
Chairman
Committee on Armed Services
United States House of Representatives
Washington, DC 20515

The Honorable Mike Rogers
Ranking Member
Committee on Armed Services
United States House of Representatives
Washington, DC 20515

Dear Chairmen Reed and Smith and Ranking Members Inhofe and Rogers:

On behalf of the Computing Technology Industry Association (CompTIA), the largest information technology association with over 2,500 members, we respectfully submit our consensus positions on the cybersecurity issues outlined in this letter.

Our country faces unprecedented times dealing with the twin pillars of COVID-19 and persistent threats from State and non-State actors. Our national industrial base is under a heavy strain and we believe that decisions made on the FY2022 NDAA will have a lasting impact on its well-being. We look forward to working closely with your staff on any, or all, of these issues.

Targeted funding for IT modernization and infrastructure, with a focus on cyberattack prevention and resilience

State, Local, Tribal, and Territorial IT Stimulus & Government Modernization Grants

- Authorize grants to States, localities, and tribes to support investment in IT maintenance and modernization projects to bolster the cybersecurity prevention, response and recovery capabilities of State, local, and tribal governments.

Establish a National Cybersecurity Assistance Fund

- Establish a National Cybersecurity Assistance Fund, as proposed by the Cyberspace Solarium Commission, for projects and programs aimed at systemically increasing the resilience of public and private entities, thereby increasing the overall resilience of the U.S.

Enforcing minimum cybersecurity requirements, and facilitating information sharing & reporting in the new cyber environment

Establish a National Cyber Labelling and Certification Authority

- Create a National Cybersecurity Certification and Labeling Authority to coordinate with the private sector, a voluntary, cybersecurity certification and labeling program, based on industry-led standards for information and communication technologies.

Amend the Sarbanes-Oxley Act to Include Cybersecurity Reporting Requirements

- Harmonize and clarify cybersecurity oversight and reporting requirements for publicly traded companies by amending the Sarbanes-Oxley Act to explicitly account for cybersecurity prevention and mitigation, including requiring Pen Testing.

Pass a National Cyber Incident Reporting Law

- DHS and DOJ to establish requirements for critical infrastructure entities to report cyber incidents to the federal government, as the federal government presently lacks a mandate to systemically collect cyber incident information reliably and at the scale necessary to inform situational awareness. Collaboration between the public and private sector will be required to identify the types of critical infrastructure entities to which such reporting requirements should apply.

Thank you very much for your consideration of our perspectives. We look forward to working with both chambers as the process moves forward. If you should have any questions regarding the recommendations outlined in this letter, please feel free to contact me at dlogsdon@comptia.org

Sincerely,

David Logsdon
Staff Director, CompTIA Federal Cybersecurity Committee