TECHNET
THE VOICE OF THE INNOVATION ECONOMY

1420 New York Avenue NW, Suite 825
Washington, D.C. 20005
www.technet.org | @TechNetUpdate

September 18, 2023

The Honorable Jack Reed
Chairman
Senate Committee on Armed Services
228 Russell Senate Office Building
Washington, D.C. 20510

The Honorable Roger Wicker
Ranking Member
Senate Committee on Armed Services
228 Russell Senate Office Building
Washington, D.C. 20510

The Honorable Mike Rogers
Chairman
House Committee on Armed Services
2216 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Adam Smith
Ranking Member
House Committee on Armed Services
2216 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Reed, Chairman Rogers, Ranking Member Wicker, and Ranking Member Smith:

As you work to reconcile the House- and Senate-passed *National Defense Authorization Act* (NDAA) for fiscal year 2024, TechNet renews our commitment to advancing this critical legislation in a manner that furthers the tech industry's long-standing partnership with the military in advancing U.S. national security objectives. We look forward to serving as a resource to you and the conferees to support our men and women in uniform and further America's interests abroad.

TechNet is the national, bipartisan network of technology CEOs and senior executives that promotes the growth of the innovation economy by advocating a targeted policy agenda at the federal and 50-state level. TechNet's diverse membership includes dynamic American businesses ranging from startups to the most iconic companies on the planet and represents over 4.5 million employees and countless customers in the fields of information technology, artificial intelligence, e-commerce, the sharing and gig economies, advanced energy, transportation, cybersecurity, venture capital, and finance.

As you know, meeting our national security objectives depends on a number of factors, including maintaining our economic strength and securing our position as the global leader in technology. Earlier this year, the Australian Strategic Policy Institute published a report that shows China has taken the lead over the U.S. in 37 of 44 technologies examined, across the sectors of defense, space, robotics, energy, environment, biotechnology, artificial intelligence, advanced materials, and quantum technology. In the long term, China's leading research position means that it has set itself up to excel not just in current technological development in almost all sectors, but in future technologies that don't yet exist.

As we look to the future, TechNet urges you to support provisions that will invest in U.S. research and development (R&D) capabilities and strengthen our leadership in emerging

technologies like artificial intelligence and quantum computing, bolster our cybersecurity defenses, secure critical supply chains, and enhance the STEM talent pipeline through updated education, workforce development, and high-skilled immigration policies. At the same time, we urge Congress to enhance our global competitiveness without pursuing heavy-handed or burdensome policies that would stifle innovation and disrupt global commerce.

Specifically, we offer the following recommendations as you craft the final bill:

Invest in R&D and Strengthen U.S. Leadership in Emerging Technologies

Artificial intelligence (AI) is transformational technology that has the potential to revolutionize how we live and work and help us solve the greatest challenges of our time. However, AI innovation must be developed and implemented responsibly. We appreciate that Congress is pursing responsible AI policymaking in the NDAA. TechNet supports the inclusion of Section 222 and Section 230 of the Senate-passed NDAA, which cover "Update to Plans and Strategies for Artificial Intelligence" and "Review of Artificial Intelligence Investment," respectively. The Department of Defense ("DOD" or "the Department") has a legacy of being a leading investor in emerging technologies and finding novel deployments of modern innovations for national security and civilian use. We appreciate the Department's intentional review of how to best use AI to improve defense applications and to build upon existing investments in these systems.

TechNet also supports the inclusion of Section 218 of the Senate-passed NDAA related to competition for technology that detects and watermarks the use of generative AI. This provision would establish a competition to best research how to detect synthetic content produced by generative AI and would involve participants from federally-funded research and development centers (FFRDCs), the private sector, the defense industrial base, academia, government agencies, and other participants that the Secretary of Defense deems appropriate. Many entities are researching how to best identify and disclose AI-produced content, and we appreciate this effort to help Americans best understand the context of the information they receive. We believe this research is crucial to building trust in AI technologies and giving Americans confidence when engaging with modern media.

Bolster U.S. Cybersecurity Capabilities and Secure Critical Supply Chains

Our foreign adversaries, including China and Russia, are well-resourced and highly motivated to steal our data and trade secrets and disrupt critical infrastructure using the most sophisticated cyber weapons. To meet today's urgent cybersecurity needs in a silent digital war, policymakers and industry leaders must focus on educating and training a highly-skilled workforce, modernizing government IT, and building long-lasting public-private partnerships to share the latest in threat information with the private sector in real-time. In addition, our increasingly interconnected digital world requires a comprehensive cybersecurity strategy that increases the security and resilience of all networks and protects against cyberattacks through the voluntary coordination of industry and government.

TechNet urges Congress to build upon its previous investments in cybersecurity resiliency as it completes consideration of the FY24 NDAA to ensure that our nation's critical infrastructure is safeguarded from cyberattacks. Specifically, we support Section 1707 of Senate-passed NDAA, which would establish a pilot program that would enable the National Security Agency Cybersecurity Collaboration Center to work with semiconductor

manufacturers in the United States to improve the semiconductor manufacturing supply chain. Additionally, we appreciate the goals of Section 216 of the Senate-passed NDAA, which acknowledges DOD's continued need to enhance the security and availability of microelectronics through evidence-based assurance processes and techniques that leverage existing data-generation and analysis practices of leading commercial semiconductor producers. We believe that it is important to build on the progress of existing pilot programs and to transition the critical work to a program of record with enhanced and permanent institutional support.

We also support Section 1399 of the Senate-passed NDAA, which would promote digitalization and cybersecurity in the Western Hemisphere. This important effort led by the Secretary of State, in coordination with the heads of other relevant agencies, would promote digitalization and cybersecurity in the Western Hemisphere through collaborative efforts with democratic partners, including the promotion of digital connectivity, facilitation of e-commerce, and the development of robust cybersecurity partnerships that share best practices to mitigate cyber threats to critical infrastructure and strengthen resilience against cyberattacks and cybercrime. Additionally, we support Section 6306 of the Senate-passed NDAA, which would establish a Digital Connectivity and Cybersecurity Partnership with our allies by expanding and increasing secure internet access and digital infrastructure, adopt policies that foster and encourage open, interoperable, reliable, and secure internet, the free flow of data, multi-stakeholder models of internet governance, and pro-competitive and secure information and communications technology policies and regulations. These efforts would establish best practices and common standards for national approaches to cybersecurity.

Enhance Global Competitiveness

Our ability to win the global competition for innovation and technology leadership depends on doubling down on our dynamic strengths and potential as a country. Congress made this objective clear by passing the *CHIPS and Science Act*, which funded the *CHIPS for America Act* originally authorized by the FY22 NDAA, to invest in our leadership in science, R&D, and manufacturing and reclaim our global competitiveness, especially with respect to China. Specifically, the *CHIPS and Science Act* made historic investments in America's production capacity for semiconductors, and billions of dollars have already been pledged to enhance our chip manufacturing capabilities. But chip production will not be swift without more talent and timely regulatory processes, namely environmental reviews. We were pleased that the Senate-passed NDAA included the *Building Chips In America Act of 2023*, which will ensure environmental reviews for semiconductor projects are completed in a timely manner through streamlined approval processes, including those already under construction.

Just as we prioritize domestic investments necessary to enhancing our global competitiveness, we must also think critically about how U.S. investments are made abroad. However, we are deeply concerned by the Senate's inclusion of a measure offered by Senators John Cornyn (R-TX) and Bob Casey (D-PA) that would establish a notification method regarding investments made by firms in countries of concern like China. The measure would establish a novel mechanism that would cover large portions of U.S. economic activity across the world. We are concerned by many of the technologies and business practices captured by the definitions used in the measure and strongly believe that improvements to this provision are necessary. With these concerns in mind, and in light of President Biden's Executive Order on "Addressing United States Investments in Certain

National Security Technologies and Products in Countries of Concern," we urge you not to include this measure in the final FY24 NDAA.

Develop a Competitive STEM Talent Pipeline and Workforce

A significant challenge facing the United States is that we do not have nearly enough cybersecurity experts to serve as the first line of defense. As of 2022, there were 755,743 unfilled cybersecurity positions, compared to a total cybersecurity workforce of 1,112,410. Cybersecurity job roles are projected to grow by 31 percent over the next decade, the fastest among tech occupations. Additionally, the Semiconductor Industry Association estimates that by 2030, America's chips sector will face a shortage of 67,000 technicians, computer, scientists and engineers. In the long term, Congress must invest in our STEM talent pipeline in order to address the long-term skills gap needed to support critical sectors to our national security through legislation that will provide grants and financial assistance to graduate students and postdoctoral researchers studying cybersecurity, such as the *Energy Cybersecurity University Leadership Act*, which passed the House earlier this year. There are also bipartisan solutions to meet immediate workforce needs, such as proposals to exempt Ph.D. and Master's Degree holders in STEM fields from green card caps.

TechNet urges Congress to include at least two provisions in the final FY24 NDAA to address this challenge. First, section 1081 of Senate-passed NDAA would create a comprehensive strategy to establish appropriate and effective talent development and management policies that allow the DOD to develop an adaptable, qualified workforce with respect to computer programming skill needs, including technical and nontechnical skills related to AI and software coding. Second, Section 1726 of the Senate-passed NDAA would support the development of foundational expertise in critical cyber operational skills at institutions of higher learning for current and future members of the Armed Forces and civilian employees of the Department. These efforts include the expansion of cyber educational programs, hands-on cyber opportunities, and direct financial assistance to civilian and military students at the Department to increase access to courses and hands-on opportunities.

The annual bipartisan passage of the NDAA is critical to the American economy and our national security, and we hope Congress will work together to ensure that this year is no different. In an increasingly complex world that relies more and more on emerging technologies, passage of the NDAA has never been more important to helping the United States address emerging threats while meeting global challenges with strength and resolve. We appreciate your attention to our views on this critical legislation and stand ready to serve as a resource as you complete your deliberations.

Sincerely,

Linda Moore

Linda Moore
President and CEO