October 20, 2022

The Honorable Adam Smith
Chairman
House Armed Services Committee
United States House of Representatives

The Honorable Jack Reed
Chairman
Senate Armed Services Committee
United States Senate

The Honorable Mike Rogers
Ranking Member
House Armed Services Committee
United States House of Representatives

The Honorable James Inhofe
Ranking Member
Senate Armed Services Committee
United States Senate

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

The Alliance for Digital Innovation (ADI) is a nonpartisan alliance of the nation's most cutting-edge technology firms. Our members represent key critical technologies at all levels of the federal government's technology stack, including cloud infrastructure, digital identity, human resources software, quantum computing, digital services, and a range of sophisticated cybersecurity tools and services critical to the United States' national security. Our mission is to break down barriers for government to bring the technological advancements in commercial innovation to the public sector to build a modern, 21st century digital government.

As the House and Senate work toward enacting the Fiscal Year 2023 National Defense Authorization Act (NDAA), ADI would like to highlight some key priorities for consideration.

Continued Migration to Modern Cloud Environments

As in years past, the House and Senate Armed Services Committees continue to provide the Department of Defense (DOD) with authorization to invest in modern, cloud-based infrastructure and applications. Many of these efforts stem from the need to identify and replace underperforming or "legacy" information technology solutions that hamper mission effectiveness. Given this dynamic, ADI supports the inclusion of Section 236 in the House-passed version of the bill that requires the DOD to produce a study on costs associated with underperforming software and information technology. The results of this study will assist the military departments and the other information technology leaders across the

DOD to better identify systems, processes, and workloads that should be moved to more modern, cloud-based environments.

Additionally, the House and Senate Armed Services Committees – through language included in their respective reports – encourage the consideration of multiple, interoperable cloud services across IaaS, PaaS, and SaaS that allow for portable applications and programs. Encouraging and incentivizing the ability to use the best application or service for a particular use case and will ensure the individuals and units depending on these systems will never wonder what could have been. The House report also included language assessing the ways in which restrictive software licensing may negatively impact how such software can be accessed or deployed across the Department's cloud environments. ADI supports the committees' efforts to ensure the Department considers tools that can enable the use of and provide for interoperability and portability across cloud environments.

Cybersecurity and Compliance

Enabling access to more modern, commercial technology often provides military departments and service branches with more secure operating environments. Legacy systems and older technology solutions are often unsupportable as they approach end-of-life, creating the possibility for less secure environments. Further, the threat environment that service members face continues to evolve as DOD incorporates technology to support the execution of its mission. ADI supports many of the enhancements to cybersecurity made by the House and Senate committees throughout the legislation. Additionally, ADI supports many of the amendments that improve the cybersecurity of the Department of Defense and the wider public sector ecosystem as well as the committees' ongoing efforts to increase funding authorizations aimed at better protecting the DoD Information Network (DODIN) and enabling access to modern commercial technology.

ADI supports the efforts of the committees to streamline and harmonize the compliance landscape across the federal government. Specifically, ADI supports language in the Senate NDAA report that requires the Comptroller General of the Department of Defense to complete the review of the Cybersecurity Maturity Model Certification (CMMC) reciprocity with the Federal Risk and Authorization Management Program (FedRAMP). This provision has the potential to save millions of taxpayer dollars by avoiding duplication and allowing DOD access to secure cloud technology already deployed across civilian agencies. ADI also supports language in the House NDAA report that commends the efforts by some military departments to implement Continuous Authorization to Operate (cATO) initiatives, especially as this concept will encourage faster innovation and rollouts of security features.

As both chambers consider proposed amendments to the bill and report, ADI recommends the inclusion of the Federal Risk and Authorization Management Program (FedRAMP) Authorization Act of 2022 as well as the Federal Information Security and Modernization Act of 2022 (FISMA). We believe the FedRAMP program has provided a strong security foundation for the federal government, and it could continue to thrive with formal Congressional authorization and additional authorized funding for its operations. FISMA improves government security and promotes adoption of modern, cloud-based

commercial security solutions that are the foundation of zero trust environments. In general, these pieces of legislation will provide support to programs and offices that support security and drive compliance across the federal government.

Finally, while ADI supports both Committees' focus on strengthening supply chain security, including software supply chain security. we do not support certain provisions related to Software Bill of Materials (SBOM)[1]. ADI and other trade associations have urged Congress "to remove the SBOM language from the NDAA and give industry and agencies more time to develop solutions that will better secure the country's cybersecurity supply chain,"[2] such as ongoing efforts associated with implementation of Executive Order 14028.

Acquisition Reform

Access to commercially available technology remains critical to protecting and empowering our warfighters. From commercially available information to train artificial intelligence models to commercial technology such as quantum computing, nontraditional defense contractors are critical to meeting the missions across the DOD. ADI supports the provisions in both the House and Senate reports that promote the use of commercial terms and conditions, including as part of the requirements generation and request for proposal processes, in efforts to do business with nontraditional defense contractors.

Further, ADI encourages the Committees to consider including language that passed out of the Homeland Security and Government Affairs Committee called the Advancing Government Innovation with Leading-Edge (AGILE) Procurement Act[3]. The provisions of the AGILE Procurement Act align with other sections of the current legislation and would help promote more rapid acquisition of essential modern technology. It would also provide pathways for small businesses to provide innovative solutions to the government, and it would work to educate the next generation of procurement professionals by providing, among other things, education on best practices associated with market research so these innovative companies and solutions can be found and brought into the federal marketplace.

Workforce

Both the House passed and Senate versions of the NDAA contain provisions that authorize targeted and sustained efforts to improve key aspects of the workforce. ADI supports provisions in the bill text and report language that authorize building the acquisition workforce as well as provisions that invest in the development and training of the cybersecurity workforce. Specifically, In the House passed version of the bill, ADI supports efforts to help educate contracting officers on best practices for software

[1] This includes language in Sec. 6722 of the House passed version of the NDAA – "DHS Software Supply Chain Risk Management" – that requires DHS to issue contracting guidance requiring submission of an SBOM as part of a bid proposal.
[2] https://alliance4digitalinnovation.org/wp-content/uploads/2022/09/Multi-association-letter-on-SBOM-final-9.14.2022.pdf
[3] https://www.congress.gov/117/bills/s4623/BILLS-117s4623is.pdf

procurement. In the Senate bill, ADI supports reviews of investments in training, educating, and retaining the cybersecurity workforce.

Data, AI, and Digital Solutions

Both the House and Senate versions of the NDAA contain provisions that encourage, authorize, and lay the groundwork for investments in technology such as data analysis, machine learning, artificial intelligence, quantum computing, sensor technology, and other areas of technological development. ADI is supportive of these efforts and applauds the provisions that authorize research and partnerships with commercial companies to pursue these cutting-edge technologies. As the Committees continue to invest in research and development at the Department of Defense, ADI encourages Members to continue supporting public/private partnerships and to include commercial innovation as the bedrock for future development. Enabling the warfighters and enterprise mission owners to partner with commercial companies and then use the buying power of the government to invest in the fruits of the shared research and development will allow the United States to maintain its technological edge throughout this century and beyond.

Sincerely,

The Alliance for Digital Innovation

Cc:

Chairman Gary Peters and Ranking Member Rob Portman of the U.S. Senate Homeland Security and Government Affairs Committee

Chairman Bennie Thompson and Ranking Member John Katko of the U.S. House Committee on Homeland Security

Chairwoman Carolyn Maloney and Ranking Member James Comer of the U.S. House Committee on Oversight and Reform