June 15, 2021

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

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

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

On behalf of the following member organizations of the Acquisition Reform Working Group (ARWG) — the Computing Technology Industry Association (CompTIA), Information Technology Industry Council (ITI), National Defense Industrial Association (NDIA), and the U.S. Chamber of Commerce—thank you for your leadership and work to produce the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2022.

Together, our organizations represent thousands of small, mid-sized, and large companies and hundreds of thousands of employees that provide goods, services, and personnel to the Department of Defense (DoD) and have extensive experience partnering with the federal government to meet many of our country's most critical needs and objectives.

We are writing to share our suggestions and proposals for the defense authorization legislation for FY 2022. We respectfully request your and your committees' consideration of them.

—

Collaborate with industry and implement a strategic approach to reviewing and implementing domestic content preferences.

ARWG encourages defense authorizers to take a strategic approach to applying Buy America requirements and other domestic content preferences, with the goal of promoting resilient and secure supply chains, and securing critical national security sectors, such as semiconductors. In doing so, we encourage policymakers to also consider the importance of working with allies, ensuring that we do not unintentionally create supply chains with single domestic points of failure, retaining the statutory commercial information technology (IT) exception, and protecting U.S. competitiveness in global defense, aerospace, and commercial information technology and communication markets. Domestic content

preferences must also help maintain U.S. access to cutting edge technologies developed overseas and promote the resiliency of supply chains by preserving (when appropriate) alternate sources of supply. We also urge Congress to focus on investing in and creating a vibrant and globally competitive domestic industrial base in key sectors *before* requiring domestic preference requirements.

As contemplated by the Executive Order on Ensuring the Future is Made in America by All of America's Workers, any expansion of Buy America requirements should include definitions that reflect input from appropriate stakeholders and a transition period to ensure compliance and avoid unnecessary disruptions and cost increases. Additionally, we urge the government to ensure that the waiver process for Buy America requirements does not become a barrier to efficient project delivery by a transparent and accountable process that results in timely decisions.

Ensure implementation of new cybersecurity requirements accounts for existing contract requirements and promotes robust two-way information sharing between the government and industry.

While industry is broadly supportive of ensuring government and contractor data is adequately protected, ARWG encourages Congress to ensure that when implementing the mandates in the Executive Order (EO) on Improving the Nation's Cybersecurity, new cyber-incident reporting requirements take into account current requirements in both the Federal Acquisition Regulation (FAR) and the Defense Federal Acquisition Regulation Supplement (DFARS). Reporting cyber incidents and breaches is a vital part of information sharing between government and industry. However, requirements to do so may also place significant burdens on contractors to report incidents in short timeframes when they are already likely surging resources to respond to ongoing attacks and address vulnerabilities in real time, and may not have complete information on the same timelines as reporting is directed. When considering new information-sharing regimes around cyber incidents, we encourage Congress to require the Department to develop a robust two-way information-sharing capability to ensure that those performing work on behalf of the government have access to up-to-date information about known threats and vulnerabilities.

Require a Defense Science Board review and recommendations on federal cybersecurity risk, FedRAMP, and the laws and regulations impacting the cybersecurity framework for the U.S. government.

Increased system complexity with no system consistency across agency environments, which makes the maintenance of proper compliance with security updates and patching a monumental task, is a key challenge in the public sector's information technology infrastructure. Adding to the complexity is rapidly changing and advancing technology, inconsistent funding, emerging threats, shifting federal strategies, and constant changes in legal and regulatory requirements. Each of these complexities and conflicting strategies presents obstacles to IT modernization efforts and has entrenched both the private and public sector in a compliance-over-outcome approach to security.

ARWG asks that the Committee direct the Comptroller General to submit a report to the Armed Services Committees by December 2022 on the laws and regulations impacting the U.S. government cybersecurity framework. Specifically, we request that the report describe: how these laws and regulations differ among agencies; how agencies manage risk within their networks; how agency acceptance of FedRAMP Joint Authorization Board (JAB) certifications, as well as the application of agency Authorities to Operate (ATO's) across government and by other agencies; how the accreditation program at the Defense Information Systems Agency (DISA) corresponds to FedRAMP and other cybersecurity requirements; and

what are the proposals for centralizing the U.S. government cybersecurity posture to better coordinate agency systems and processes.

Require the Defense Information Systems Agency (DISA) to expedite security certifications for cloud service providers.

The Department's pursuit of cloud and cognitive computing promises to significantly alter warfighting and defense business operations. To better enable this transition, the Defense Information Systems Agency (DISA) has been tasked with migrating applications and services out of DoD owned and operated data centers to commercial cloud services while maintaining the security of and control over all DoD data, in accordance with DoD policies. DISA is responsible for granting provisional authorization (PA) to host DoD information and systems to non-DoD owned and operated cloud service providers (CSPs) so they can provide cloud and cognitive computing services to DoD and service Department customers. For DoD to have access to the most innovative technologies, DISA must ensure that the process it uses is transparent, structured, and enables the Department to leverage the commercial sector, CSPs, and the technology industry to the greatest extent possible. DISA should also work with the service departments to onboard CSPs as quickly as prudent to meet the needs of the service missions.

ARWG is concerned about delays in issuing PAs and ATOs to CSPs, especially those who have achieved FedRAMP certification since a multi-CSP environment enables greater competition and cost savings. ARWG recommends that the Armed Services Committees include report language directing DISA to provide the resources necessary to expedite the issuing of PAs and ATOs to CSPs and to provide a report every 6 months to the congressional defense appropriations subcommittees and authorization committees, beginning 30 days after the enactment of the NDAA. This report should include information detailing the process for accrediting CSPs, the number of CSPs that have applied for accreditation, where the CSPs are in the PA process, as well as details on the progress in achieving expedited timelines for these accreditations and certifications.

Require the Department of Defense to leverage innovative technologies and invest in its cybersecurity capabilities and workforce to help prevent, respond to, and recover from cyberattacks.

President Biden's Executive Order on Improving the Nation's Cybersecurity, to enhance software supply chain security (Section 4), identifies automated tools—including those that check for known and potential vulnerabilities and remediate them—as among the security-enhancing practices of the software supply chain that the Secretary of Commerce, acting through the Director of NIST, should consider when issuing guidance to enhance software supply chain security. Artificial Intelligence (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 machine learning (ML) and automation to identify potential threats. ARWG recommends the inclusion of a provision in the FY 2022 NDAA or accompanying committee reports that ensures the Department prioritizes consideration of unified endpoint security tools leveraging AI and ML to enable best-in-class prevention, response, and recovery from cyberattacks. Additionally, as the U.S. is expected to face a shortage of 1.8 million skilled cybersecurity workers by 2022, educating and empowering the next generation of cybersecurity professionals is imperative to our future national and economic security. Government must continue to invest in cyber skills and knowledge for government employees but also seek creative and economical ways to fill gaps.

Promote competition, cost savings, and Department of Defense-wide cybersecurity through acquisition policies that support supplier diversity.

ARWG encourages policymakers to promote competition, cost savings, and DoD-wide cybersecurity through acquisition policies that support supplier diversity. While category management strategies and enterprise agreements can create significant efficiencies in the federal acquisition process, they also risk limiting the government's access to the full range of available innovative solutions, which are called out directly by the recent cybersecurity EO. Consequently, the government cannot unleash the full potential for future cost savings associated with further order-level competition. To promote competition, increase cost savings, and potentially reduce risks associated with limited suppliers, ARWG encourages defense authorizers to direct the Department's category management program offices to prefer multiple-award, solution-based categories and contracts over single-award, vendor-specific categories and contracts. The DoD should closely monitor contract awards and take the necessary steps to diversify the industrial base in areas necessary to perform mission-critical needs.

Encourage Department of Defense use of qualified bidder lists (QBLs) and qualified manufacturer lists (QMLs).

Qualified Bidder Lists (QBLs) and Qualified Manufacturer Lists (QMLs) can be useful tools to mitigate information and communications technology (ICT) supply chain risks through the exclusive inclusion of vendors with high levels of maturity and capability. ARWG recommends that DoD IT acquisition personnel leverage QBLs and QMLs, where possible, for high-priority acquisitions. DoD personnel should also look to guidance released by the DHS ICT Supply Chain Risk Management Task Force to determine when and how to construct QBLs and QMLs and establish a clear process for regularly updating these lists. Transparent criteria for how companies are included on the list, why a vendor may have been excluded from a list, and recommendations for how a company can fix any issues preventing their inclusion on the list should be provided. It is also recommended that the Department be required to make these lists broadly available across the government and to the public.

Require the Department of Defense to establish consistent, standardized requirements for safeguarding sensitive information, including adopting a phased implementation model for new mandates.

ARWG supports reasonable flexibility in and sufficiently phased implementation of cybersecurity mandates, including those discussed by the EO, to ensure that industry can effectively, fairly, and comprehensively protect public and private owners' sensitive information to advance national security and secure proprietary and personal information. To enable companies to properly safeguard covered information, it is important that they be provided the guidance, consistency, and clarity to scope implementation correctly. Unambiguous and comprehensive guidance about what information constitutes controlled unclassified information (CUI) is crucial, and it is essential for a standardized system of CUI marking to be widely and uniformly implemented in a timely fashion. Requiring sufficient input from appropriate stakeholders and a transition period to ensure compliance for any new cybersecurity and supply chain risk management mandates is essential to the continued health of the defense industrial base. Industry and federal agencies are currently undergoing a dramatic increase in cybersecurity compliance and SCRM prohibitions, including: Cybersecurity Maturity Model Certification, self-assessment requirements, Section 889 of the FY 2019 NDAA, and Section 1656 of the FY 2018 NDAA (covered telecommunications provisions), among other requirements.

Improve the Department of Defense supply chain risk management posture by allowing vendors to proactively attest to their capabilities.

Though the CMMC is intended to ensure the cybersecurity of the Department's supply chain, the specific CMMC requirements do not address product integrity or a contractor's overall SCRM maturity. To fill in the gaps, we recommend that vendors have the opportunity to demonstrate the actions they take to protect their networks and supply chains through enhanced cybersecurity program certifications and product security mechanisms. Only some examples of program attestation could be a signed U.S. Treasury Committee on Foreign Investments in the United States (CFIUS) National Security Agreement, Customs Trade Partnership Against Terrorism (CTPAT) certification, or demonstrated implementation of NIST SP 800-161, Supply Chain Risk Management for Federal Information Systems, or other global, industry-led standards. Enhanced product security practices, such as Software Bills of Material (SBOMs) and sophisticated cryptographic code-signing should be encouraged as a means for vendors to demonstrate a commitment to following SCRM best practices. The Department's acquisition personnel should be encouraged to accept these attestation mechanisms offered by potential vendors when evaluating bids and, in recognition of the considerable compliance investments government contractors have made to prove their cybersecurity capabilities, allow for reciprocity between schemes.

Improve transparency and accountability with the defense Operation & Maintenance accounts to address supply chain vulnerabilities and materiel readiness objectives.

Given that Operation & Maintenance (O&M) represents approximately 40 percent of the national defense budget function, Congress and the American public should expect greater transparency in the O&M budget. Not only does the current budget display limit oversight, but it also poses challenges for the resiliency of the supply chain. The fiscal transparency suppliers enjoy for acquisition programs in development and production (funded by RDT&E and procurement) does not exist within the sustainment ecosystem. As a result, sudden demand changes can significantly disrupt the supply chain, particularly for smaller to mid-size suppliers, up to the point of insolvency. Therefore, ARWG urges Congress to require additional, unclassified O&M budget display to identify the material readiness objectives for each major weapon system (as already required by 10 USC 118), as well as the funds obligated, budgeted, and programmed for the purpose of achieving the material readiness objectives. The budget display should also include a narrative discussing DoD's performance against their objectives and any related supply chain risks. This information can be provided without limiting the operational flexibility the military requires. Such a budget display would create a consistent, repeatable framework for assessing supply chain vulnerabilities at an actionable level. It would also foster meaningful oversight and debate regarding the trades between requirements and available resources, as Congress already conducts for the modernization accounts. Finally, it would share actionable insights into future years' sustainment priorities to allow the industrial base to plan for and invest in the capacity and capability necessary to support the attainment of the materiel readiness objectives of each weapon system.

Maintain existing procurement frameworks for architect and engineering services.

As the government seeks to improve procurement processes, there is often a bias toward consistency in policies and procedures. It is important to understand and continue policies that protect the warfighter, facilities performance and sustainability, the environment, the public, and lifetime ownership and operations costs. This is paramount in the selection of architect and engineering (A&E) services providers, whose performance is critical to achieving effective and efficient physical infrastructure (intended to last and perform well for decades) and whose cost of services are relatively insignificant (approximately 1

percent of life-cycle costs). For these reasons, the need to select A&E service providers based on their qualifications remains. Care should be taken to clearly exclude A&E services from general procurement changes and avoid weakening Public Law 92-582 or existing implementing regulations.

Require DoD acquisition programs to prioritize the use of commercial items to the maximum extent practicable.

ARWG requests that the FY 2022 NDAA direct the Department's acquisition planning for new DoD Acquisition Programs to prioritize the use of commercial or commercially available off-the-shelf (COTS) technologies items to the maximum extent possible, reinforcing the statutory preference for commercial items. In addition, 10 USC 2306a and the Defense Federal Acquisition Regulation Supplement make it clear that a contracting officer may presume that a prior commercial item determination shall serve as a determination for subsequent procurements (unless the contracting officer follows the process to overturn the prior determination). However, a July 2019 revision to the Department of Defense Guidebook for Acquiring Commercial Items Part A: Commercial Item Determination, inserted the statement "[Commercial Item Determinations] for subcomponents and spare parts of items determined to be commercial must be considered independently." This declaration is not supported by the Commercial Item Handbook (Version 2.0), the FAR definition of a "commercial item" (Federal Acquisition Regulation 2.10—Definitions), or the statutory definition of a "commercial item" (41 USC 103) and is causing significant additional work for both government and industry.

ARWG notes that contracting officers are working diligently to comply with the Guidebook's direction to complete and document a commercial item determination (CID) on parts and subcomponents of items that have already been determined to be commercial. This is of little value to the government, and appears to run counter to the intent of Congress behind the preference for acquisition of commercial items in section 10 USC 2377. Section 2377(b)(5) directs the head of agency to ensure that the agency's procurement officials "revise the agency's procurement policies, practices, and procedures not required by law to reduce any impediments in those policies, practices, and procedures to the acquisition of commercial items." ARWG recommends Congress reinforce the intent and requirements of the law pertaining to commercial items determinations in order to alleviate this unnecessary burden.

Require DoD information and communications technology acquisition programs to prioritize the use of commercial technologies to the maximum extent practicable.

To effectively modernize government systems and increase mission capabilities, the DoD and government must prioritize the use of commercial or commercially available off-the-shelf (COTS) technologies to the greatest extent possible. This includes leveraging commercial cloud solutions and purchasing cloud technology as a commercial item whenever possible. Commercial ICT allows the government to leverage industry's most innovative solutions, including much more rapid technical and security updates. In contrast, many government systems are based on customized technology. Maintaining and upgrading these systems requires significant development work, often through costly service contracts. The latest security upgrades and patches may not be readily compatible with overly customized government systems, leaving these systems open to cyberattacks. ARWG requests that the FY 2022 NDAA direct the Department's acquisition planning for new ICT Acquisition Programs, whenever possible, to include documented, actionable processes to retire customized existing systems in favor of COTS solutions.

Enhanced reporting of commercial item determinations.

ARWG notes that in a July 2018 Report (GAO #18-530), the U.S. Government Accountability Office concluded that improved information sharing could help DoD determine whether products and services are commercial and reasonably priced. It is critical that this type of information be shared by DoD with the commercial supply base as well. However, commercial item determinations are not consistently made available to the contractor asserting commerciality. Much time could be saved by not requiring redundant commercial item reviews by prime contractors and subcontractors. Improved information sharing would also enable contractors to provide additional supporting information prior to the government making a premature non-commercial determination.

ARWG is aware that the FY 2021 NDAA revised 10 USC 2380 to require a memorandum of a commercial item determination (CID) to be issued no later than 30 days after contract award. However, the provision does not state to whom the memorandum is to be issued. To be effective, the memorandum must be issued prior to a contract award and shared with the prospective contractor. Therefore, ARWG recommends 10 USC 2380 be clarified to ensure that the memorandum documenting the CID be provided to Defense Contract Management Agency (DCMA) for inclusion in the database, and to the contractor asserting commerciality in advance of contract award. Sufficient detail, including supplier name, part number, basis for approval or disapproval, date, and name of agency making the determination, should be included in the memorandum.

Require transparent and comprehensive market research procedures, particularly when used in support of limiting full and open competition.

The Department should require contracting officers, when performing market research, to publish market research opportunities on the government point of entry (GPE). This should include a requirement to conduct market research for commercial items. To ensure DoD contracting officers are meeting required standards for market research—including discovering and taking full advantage of available innovative capabilities—ARWG recommends that the DoD be directed to conduct an assessment of Department of Defense-wide market research reports prepared in support of justifications for limiting competition on a brand name or sole source basis. We recommend the Department use the results of this assessment to make further policy improvements to market research requirements.

Support modernization decisions by requiring price evaluations to consider the total cost of solutions.

We are concerned that government customers may avoid migrating away from legacy offerings in favor of modern, secure solutions based on transition costs. Additionally, they may have existing maintenance agreements and integrated support teams in place to support legacy solutions. This adds to the perception that moving to a new, innovative solution (which may require recompeting maintenance agreements) is cost-prohibitive—even if doing so will improve mission performance and reduce long-term costs. ARWG urges the committees to include language in the FY 2022 NDAA that ensures the Department requires officials to ensure, when conducting an evaluation of a proposal that intends to leverage goods or services pursuant to a separate agreement, that the cost or price of such goods or services under the separate agreement, including the costs associated with integration of the product into existing architectures and the necessary process and retraining costs associated, are included in the evaluation of the proposal.

Encourage agencies to better coordinate contract requirements through integrated project teams including technical, security, and acquisition professionals.

With technology and program requirements increasing in complexity, acquisition professionals must work closely with technical and security professionals to ensure requirements and contracts are developed in accordance with modern best practices. ARWG urges the establishment of required models for program management offices and integrated project teams that include representatives from technical and acquisition specialties, as well as representatives from the office of the Chief Information Officer (CIO). This will ensure cybersecurity requirements are prioritized in the development of new IT systems and appropriately documented in the early stages of the acquisition process.

Advance the organic industrial base through automation and innovative technologies.

The DoD industrial facilities that manufacture, maintain, repair, and overhaul military weapons and equipment—often referred to as the organic industrial base (OIB)—play a vital role in maintaining defense readiness. Unfortunately, many OIB facilities operate using inefficient processes and with aging infrastructure. A recent GAO report (GAO 19-242) found that "The condition of facilities at a majority of the [DOD] depots is poor and the age of equipment is generally past its useful life, but the services do not consistently track the effect that these conditions have on depot performance. Twelve of the 21 depots GAO reviewed—more than half—had 'poor' average facility condition ratings…. In addition, the average age of depot equipment exceeded its expected useful life at 15 of the 21 depots."

ARWG urges Congress to continue oversight of the Department's implementation of the 13 recommendations made by the GAO in this report and to support additional investments in OIB infrastructure necessary to enable DoD depots, shipyards, and arsenals to integrate innovative technologies such as automation, virtualization, predictive analytics, and intelligent workflow into their operations. Such investments are needed to improve OIB operations, maintenance, and repair capabilities, and to enable the OIB to work effectively with industry in supporting modern, digitally-enabled platforms.

Streamline undefinitized contractual actions.

ARWG recommends that Congress require the Department to streamline contract financing payments under undefinitized contractual actions (UCAs). Specifically, we recommend that a new provision amend 10 USC 2307 to raise the cap on the customary progress payment rate under UCAs from 80 percent to 90 percent. The provision should also amend 10 USC 2326 to eliminate the obligation limit (i.e. 75 percent of the not-to-exceed (NTE) contract price) on certain UCAs. Taken together, these changes would provide needed flexibility for the government and contractor to structure appropriate contract financing payments on UCAs where the contractor has submitted a qualifying proposal.

Maintain due process protections for contractors.

A broad, diverse, and capable pool of contractors willing and able to do business with the Department, as well as the entirety of the federal government, is important to ensuring the warfighter and government retain access to the best available products, services, capabilities, and expertise, and that taxpayer dollars are well used. Accordingly, the committees are urged to uphold and encourage the use of the existing processes to adjudicate the suspension, debarment, and/or exclusion of contractors when necessary. It is requested that the FY 2022 NDAA refrain from enacting or codifying policies that impose penalties,

requirements, and processes on contractors without appropriate due process or beyond the existing procedure. Doing so could lead to greater inconsistencies in the acquisition process across government agencies and would likely make it harder, more inconsistent, and risky for new, small businesses to do business with the government.

Streamline contractor audit system criteria.

ARWG supports recommendation #72 of Volume 3 Report of the Advisory Panel on Streamlining and Codifying Acquisition Regulations (809 Panel), to implement a streamlined internal control audit framework. FAR 16.301-3 (Limitations) recognizes the critical role of accounting systems by requiring contractors to maintain an adequate accounting system for contracts awarded on the basis of costs. As set forth in DFARS 252.242-7006, contractor accounting systems are audited using eighteen system criteria. These criteria are often not objective and add significant complexity and cost to audits without adding value to audit quality. By contrast, industry often relies on more efficient and effective internal-control frameworks. For example, one consists of seven system criteria for auditing the reliability of accounting systems that capture all but one of the elements contained in the list of 18 government-unique system criteria. ARWG urges Congress to require DoD to implement the 809 Panel's recommendation #72, which is a more effective way to conduct audits of contractor accounting systems. Recommendation #72 protects government interests in streamlining accounting system criteria, will make the criteria more objective, reduces disputes related to business system deficiencies, and shortens the time required to determine adequacy of contractor business systems.

Make special emergency reimbursement authority permanent.

We recommend including a provision providing special emergency reimbursement authority to the Secretary of Defense under certain circumstances, subject to the availability of appropriations. This special emergency reimbursement authority is modeled after the authority provided by section 3610 of Public Law 116-136, the "Coronavirus Aid, Relief, and Economic Security (CARES) Act." Similar to the section 3610 authority, this provision would authorize the Secretary to reimburse a contractor for the costs of paid leave provided by the contractor to employees or subcontractors to keep those employees or subcontractors in a ready state. The reimbursement for paid leave would only cover those employees or subcontractors who cannot perform work on an approved site due to facility closures or other restrictions, and who cannot telework because their job duties cannot be performed remotely. Unlike the 3610 authority, this provision does not specifically relate to the response to the coronavirus pandemic. The authority provided in this provision would be available for use by the Secretary in responding to a wide range of emergency circumstances as described in 41 USC 1903. These circumstances include: supporting contingency operations; recovering from or defending against a cyber, nuclear, biological, chemical, or radiological attack against the United States; or responding to a national emergency or major disaster. In contrast to the 3610 authority, this authority would not have a set expiration date but would be available for use for the duration of the emergency circumstance.

Continue support for the implementation of the 21st Century Integrated Digital Experience Act (IDEA) at the Department of Defense.

The Department must continue to be appropriately supported in the implementation of the 21st Century Integrated Digital Experience Act (IDEA) and be held accountable for the requirements of that law. The implementation of the 21st Century IDEA, which requires all government-produced digital products to be consistent, modern, and mobile-responsive is important to ensuring modern digital service delivery to

citizens, which will become even more important as the United States moves to a post-pandemic era. The Act has a set of criteria for new and redesigned websites and digital services including accessibility for individuals with disabilities (as required by section 508 of the Rehabilitation Act of 1973), consistency in appearance, provision of services through industry standard secure connections, the presence of a search function, an option for a self-service customized experience, and full functionality on mobile devices. ARWG urges the Armed Services Committees to adequately support and provide appropriate oversight to ensure effective implementation of the Act, including mechanisms to assess the extent of existing public facing websites that comply with the requirements of the law.

Eliminate certified cost and pricing data reporting requirements for non-commercial modifications to commercial items.

ARWG is concerned that the requirement to submit certified cost or pricing data on "noncommercial modifications" of a commercial item that are expected to cost more than the threshold identified in the Truthful Cost or Pricing Data Act, or 5 percent of the total contract price, may constitute a barrier to entry for companies that are only making minor modifications to commercial items to address federal requirements. Submitting certified cost or pricing data may be especially problematic for companies that generally sell only commercial items to the government, as many are not required to and do not maintain government-approved cost accounting systems. We encourage Congress to require the Department to broadly interpret terms such as ''of a type'' and ''minor modifications,'' which will increase the pool of commercial companies that are eligible to sell to the government. This type of broad interpretation is consistent with Congressional intent for commercial items under the Federal Acquisition Streamlining Act and will ensure the Department maintains timely access to critical best-in-class commercial technologies.

Review and adopt best practices for price realism in procurement.

ARWG requests that Congress require the Department to review and report on its use of price realism evaluations during contract awards, including the success of price realism analyses in reducing future contract administration challenges related to contract price modifications and/or terminations due to nonperformance. ARWG believes price realism analyses offer an important tool for contracting officers to evaluate the extent to which a bidder is underbidding a contract and/or does not fully understand technical requirements. By excluding these bidders from the competitive range, the Department can potentially reduce downstream price increases or costly terminations if the contractor cannot ultimately perform for the price proposed. We recommend Congress require the DoD to adopt department-wide standards and criteria for conducting price realism analyses, and provide workforce training on best practices for using this evaluation technique. We recommend that Congress require the Department to prioritize reviewing price realism analyses and best practices for services contracts, which are frequently subject to price adjustments based on insufficient proposed labor rates and/or an inability to recruit and retain qualified contractor staff at those rates.

Extend and make permanent the Small Business Innovation Research (SBIR) program.

The Small Business Innovation Research (SBIR) Program is a longstanding channel for disruptive innovation which supports the DoD moving from research to delivery. The SBIR program was established under the Small Business Innovation Development Act of 1982 (P.L. 97-219) to strengthen the role of innovative small business concerns in federally funded research and development (R&D). Since that time, the SBIR program has been reauthorized and extended multiple times, the most recent of which expires September 30, 2022. ARWG supports the 809 Panel recommendation #21b of their Volume 1 Report to amend 15

USC 638 to make SBIR permanent. From 1982 through FY 2019, the program has provided over 179,000 awards totaling over $54.3 billion. At a time when businesses are leaving the defense sector, providing this permanent authority would help solidify the commitment to small businesses in the SBIR pipeline. Additionally, a permanent program would support a standardized Phase III contracting approach, providing a contract vehicle for follow-on work from Phase I & II aligned with the pilot program authorized in Section 1710 of the FY 2018 NDAA.

—

Thank you very much for your consideration of our perspectives. If we can provide further detail, or should you have any questions about these proposals and recommendations, please do not hesitate to contact us.

Sincerely,

Computing Technology Industry Association (CompTIA)

Information Technology Industry Council (ITI)

National Defense Industrial Association (NDIA)

U.S. Chamber of Commerce