September 08, 2021

The Honorable Kathleen Hicks
Deputy Secretary of Defense
United States Department of Defense
1010 Defense Pentagon
Washington, DC 20301-1010

CC:
Gregory Kausner, PTDO Under Secretary of Defense, Acquisition and Sustainment
John Sherman, Acting Chief Information Officer
Jesse Salazar, Deputy Assistant Secretary, Industrial Policy
LTG David Bassett, Director, Defense Contract Management Agency
John Garstka, Acting Chief Information Security Officer, Acquisition and Sustainment

Dear Deputy Secretary Hicks,

The undersigned industry associations write in support of the Department of Defense's (DoD's) efforts to secure IT networks and systems throughout the defense industrial base (DIB) critical infrastructure sector. We represent the Department's aerospace, defense, and technology industry partners that provide products and/or services for mission critical activities. Our collective membership comprises prime contractors, subcontractors, and suppliers of all sizes from small businesses to multi-national enterprises.

We recognize the national security and programmatic implications of the cybersecurity regulations defined by the Federal Acquisition Regulation (FAR) and the accompanying Defense Federal Acquisition Regulation Supplement (DFARS). These regulations include provisions relating to the safeguarding of DoD controlled unclassified information (CUI), the assessment score management in the Supplier Performance Risk System (SPRS), and the integration of practices by the Cybersecurity Maturity Model Certification (CMMC) program. Currently, our collective members are facing critical decision points that will impact their budgets, strategic planning, and resource allocation without the benefit of knowing the status of DoD cybersecurity policy implementation. Further, the continued proliferation of federal cybersecurity requirements at the agency level compounds this uncertainty as it remains unclear how DoD requirements will align with those required by other federal agencies. This causes operational impacts that result in procurement inefficiencies and contractual modifications that are passed on to the Government.

We appreciate the opportunity to share industry feedback with you. We believe it is important for the Department to remain publicly committed to the CMMC program to underscore the program's importance for national and supporting global cyber ecosystems. This public commitment should be communicated promptly and is particularly important in the context of

the Department's continued internal review, updates to SPRS tracking and reporting, and the pending publication of the Government Accountability Office's (GAO's) report on CMMC. Without a statement of support for cybersecurity assurance, we are concerned that some companies may continue to delay implementation of important security practices pending an understanding of the final requirements. We would like to offer the following observations and recommendations to better support the evaluation of potential modifications to the program, the assessment practices, or the operational procedures.

Foremost, we view transparency as the foundation upon which the success of the program rests. We believe DoD and industry will achieve the best risk management outcomes when they engage in bi-directional information sharing and act transparently in their decision-making. While we understand that the transition to new senior leadership often leads to a review or assessment of existing programs, it has also highlighted the increased need for frequent and transparent bilateral communications between DoD and industry regarding cybersecurity regulation, assessment products, and programs.

The lack of clarity during the review process has increased uncertainty throughout the DIB and among commercial vendors seeking to provide covered commercial items. Changes to CMMC, for example, would conceivably impact the timeline, scope, and manner of implementation for program requirements. Considering this uncertainty, contractors, subcontractors, and suppliers may defer substantial investments pending communication and greater certainty about the program's requirements. Simultaneously, companies will find it easier to develop innovative services, technologies, and processes to fit their needs if they clearly understand requirements, practices, and operational efficiencies. The initial public announcement of CMMC and the interim DFARS rule motivated many companies to work diligently to improve their cybersecurity practices. We believe that increased communications and reinitiating collaboration in the areas detailed below will build on the initial success to further improve our nation's security posture across the dynamic threat landscape.

First, we see an increasingly urgent need to standardize and improve the marking practices for the Department's CUI requiring protection and dissemination instructions. Currently, DoD agencies must only list what the Department has described in the National Archives and Records Administration (NARA) CUI registry as CUI requiring protection. Recently, however, DIB members have been encountering DoD agencies that require the protection of all the 100+ federal agency specific categories in the NARA CUI Registry without an attempt to identify the particular categories that relate to contract performance. For the CUI program to work, it is imperative that all DoD agencies involved in all acquisition contracts clearly, accurately, and correctly identify, define, and describe the CUI requiring protection. This is particularly true whenever the Department decides[1] to leave the identification and definition of CUI up to the

[1] DFARS Clause 252.204-7012 provides that CUI is "(1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or (2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract,"

contractor. In these cases, the Department must still provide detailed guidance regarding the type of information to be protected and should continue to collaborate with contractors and subcontractors that generate DoD CUI. Without this critical information being defined to industry, there is a great risk that industry will not correctly identify or protect what the DoD would ultimately want to be protected. It does not serve anyone's interests to leave the boundaries of CUI in permanent doubt.

Second, we are concerned that the Department may be reviewing outdated/static information. We see a risk that officials will begin to implement changes to the CMMC program without the benefit of sufficient, current industry perspectives and inputs. DoD officials indicated that an updated DFARS rule for CMMC would not be ready until the end of calendar year 2021 – more than one year since public comments to the interim rule were submitted. It is unclear how those comments from 2020 on DFARS 252.204-7012, -7020, and -7021 have been or will be adjudicated. If there will be significant changes to CMMC, we encourage DoD to share those changes via a proposed rule rather than an immediate final rule. We also encourage DoD to conduct virtual public hearings if the Department contemplates material changes to the present structure and methods. Such steps would demonstrate to industry that DoD is receptive to new perspectives and aware that input in the fast-moving IT industry may have changed since late 2020. It would also alleviate some of the uncertainty that the ecosystem is facing while the Department completes the adjudication of received comments.

Third, we commend the administration for its transition toward a more holistic approach to federal and IT service provider information risk management. A continued federal commitment to established, consensus-based nonfederal industry standards will provide the foundation for developing a coherent strategy. The administration can pursue this strategy with critical operational urgency by enabling reciprocity between analogous domestic and international cybersecurity mandates, frameworks, and standards. The current piecemealed landscape of security controls needs to be streamlined and complemented by transferable requirements. Framework reciprocity partnered with standardized performance metrics will enable the government to adopt an outcomes-focused approach to information risk management. To that end, the Department should work with the interagency to clarify how reciprocity will work between its agency-specific guides and other agency initiatives like the Federal Risk and Authorization Management Program (FedRAMP). For DoD, the need for harmonization and reciprocity is most relevant in the context of CMMC and the Cloud Computing Security Requirements Guide (SRG). Similarly, the harmonization with existing auditing standards, such as AICPA's SOC2, and recognition of commercially viable methods of validating cloud security, will expedite the scaling of domestic and global assessments and audits increasing overall efficiency, particularly for small businesses.

To further ensure a whole of government approach, new security requirements should be harmonized with the relevant FAR and DFARS clauses to the maximum extent practicable. The ongoing proliferation of new security requirements furthers the need for harmonization. In May, the President signed Executive Order 14028 on Improving the Nation's Cybersecurity (Cyber EO). In August, the Department of Homeland Security (DHS) announced an RFI for a

vendor cybersecurity assurance program similar to CMMC. Simultaneously, members of Congress continue to sponsor individual legislative proposals and are marking up the draft of the National Defense Authorization Act for Fiscal Year 2022. Governmental mandates like these call for centralization with considerations for conditions under liability protection and criteria over negligence instead of retaliation for intrusions. An accord across agencies, services, and at program levels will strengthen our nation's defenses and avoid divergence of national security, critical infrastructure, and civilian security. Ultimately, the harmonization of existing and future cybersecurity directives will move the administration closer towards its goal of coherent information and cybersecurity risk management.

To better support the evaluation of potential modifications to the CMMC program, the assessment practices, or the operational procedures, we respectfully suggest the following to the Department:

1) **Regularly engage with industry:** The task of securing DIB networks is too critical and too dependent on public-private collaboration to be successfully carried out without industry engagement and input. We believe that scheduled, routine and bi-directional interactions between the Department and the DIB would improve the Department's program as well as industry's implementation of the requirements. We suggest the creation of a government-industry advisory board to host monthly meetings with representatives from the full range of stakeholders in the Department, including senior leadership from OUSD (A&S), OUSD (I&S), and the Office of the Chief Information Officer. The undersigned industry associations are willing to represent contractors, subcontractors, and suppliers of all business sizes.

2) **Standardize and improve the marking practices for DoD CUI requiring protection:** The best risk management outcomes will be achieved when the Department and contractors work collaboratively towards a mutual goal. To that end, industry depends on the Department to identify, define, and describe the CUI requiring protection. This is especially true whenever the Department assigns the identification responsibilities to contractors. If the guidance is clear, accurate, and consistent, contractors can apply it to the data they generate for or at the direction of DoD and take necessary steps to ensure the protection of the data. This would also reduce the Department's workload of responding to clarification requests from contractors. Without this critical information being defined to industry, there is a great risk of goal misalignment which could waste scarce resources at best and leave open vulnerabilities in sensitive systems at worst.

3) **Harmonize CMMC and related contractual clauses with existing and future cybersecurity directives:** We urge the Department to harmonize CMMC requirements with other federal cybersecurity directives to support the adoption of a holistic risk management strategy. To that end, we encourage DoD to issue authoritative guidance on reciprocity with existing certifications and to harmonize not-yet implemented security requirements as appropriate. We are most concerned about existing authorizations issued by FedRAMP and the DoD SRG Impact Level Assessments. These programs implement many of the same security controls from NIST SP 800-171 and will leverage the new NIST SP 800-53 Rev.5 controls as

appropriate for their respective implementation. Another area of particular concern are the requirements pursuant to the Cyber EO. We see the greatest overlap with those requirements that relate to the implementation of zero-trust architecture, verification, and operational requirements for "critical software," National Security Systems, and the adoption of data encryption and multi-factor authentication. DoD should articulate courses of action that can move from the presently applicable set of methods and controls to outcomes and update training materials to ensure consistency in control definition and implementation across certification schemes. Yet another area of overlap that should be considered is the threat hunting program assessment pursuant to Sec.1739 of the National Defense Authorization Act for Fiscal Year 2021. To avoid duplicative or inconsistent requirements, the Department should embrace a whole-of-government approach to cybersecurity risk management, harmonize existing and future requirements, and grant reciprocity where applicable.

4) **Clarify Inter-Governmental Authorities for Implementing CMMC and Related Cybersecurity Requirements:** We are concerned by the ongoing ambiguity regarding where the authority lies for key elements of CMMC. According to the interim rule the Department published in late 2020 (DFARS Case 2019-D041, *Assessing Contractor Implementation of Cybersecurity Requirements*), the DoD CIO can grant exceptions as to whether a procurement or program needs CMMC certification. The Cyber EO appears to vest related authorities, as they pertain to National Security Systems, with the Director of the National Security Agency (NSA). We believe that additional clarity is needed regarding the respective roles of the Under Secretary for A&S, the DoD CIO, and the Director of NSA. The respective budgets for these offices should be updated to account for the redistribution of responsibilities and to ensure sufficient funding and human resources are available for mission success.

5) **Provide additional implementation guidance and support for small businesses:** Small businesses are an integral part of the DIB. It is essential that small businesses, like other participants in the DIB, improve their cybersecurity and sustain defenses against evolving cyber threats. The delay in implementation requirements and a protracted program review have caused great confusion across industry and have negatively impacted small businesses who do not know how to budget for an assessment against an undefined program scope. In the case of DFARS and CMMC, compliance costs are a specific concern of small businesses due to their size and scale to remain competitive in the marketplace. For many small businesses, both engaging directly with DoD and working as sub-contractors, recouping CMMC costs will depend on the successful contract award. This uncertainty creates a disincentive for small businesses to participate in firm fixed price contracts. At the same time, information security is important regardless of business size and all government contractors should be held to the same rigorous standards. To alleviate some of the burden on small businesses, the Department should provide them with additional implementation support and guidance. For example, solutions could include 1) specific assistance and incentives to offset the cost of implementation, such as a Cybersecurity as a Service program, 2) recommendations to the services and prime contractors to leverage existing

certified technologies to limit the exposure of CUI to the small business contractor, or 3) reducing the burden of the assessments for small businesses operating at Levels 1 and 2.

6) **Evaluate and clarify remaining policy and process questions around the implementation of DFARS:** Specifically, industry is seeking clarity on the certification requirements in DFARS 252.204-7012, -7020, and -7021 as they relate to the CMMC program and forthcoming procurements. Members of the DIB remain unclear about system scope for CMMC compliance and DoD CUI. We would like to remind the Department of the enormous significance that scoping guidance has to many enterprises, particularly those that operate in complex environments. Without detailed guidance, companies may not know what systems and business processes will be subject to DFARS 252.204-7012 and the CMMC program. The absence of scoping guidance also impairs the ability of the Accreditation Body to perform its presently assigned functions. We suggest that OUSD (A&S) prioritize the publication of this system scoping guidance. The technical scoping guidance will drive large technology investments across the DIB, and the sooner that can be provided, the better. This technical document should also be sufficiently comprehensive in its examples and guidance[2] to ensure companies are successful in implementing DFARS and CMMC standards and practices commensurate with risk and operating environments from small businesses to global enterprises.

These are some of the most significant priorities around the implementation of DFARS and CMMC that still need to be resolved. We believe that any broadening on the scope of federal and DoD regulation should be subject to public consultation in advance, inclusive of notice-and-comment rulemaking. With urgency and criticality, if DoD is considering major changes to CMMC, we strongly recommend that these be aired with industry before any final decisions are made since it is industry that bears the responsibility to meet the Department's security requirements.

Thank you for your consideration of our suggestions. Our collective industry trade associations are eager to continue working with the Department to improve cybersecurity throughout the DIB. We look forward to increased communication and collaboration as the Department continues to implement its cybersecurity policies and programs.

Sincerely,

Information Technology Industry Council
National Defense Industrial Association
Professional Services Council

[2] For example, the technical guidance should delineate for which systems federal information processing standards (FIPS) and Common Criteria certifications are required. While the vagaries of the standard as written provide much needed flexibility, they also increase the chance that companies will interpret the processes and controls in a way deemed unacceptable to their assessor.