March 26, 2020

The Honorable Ellen M. Lord
Under Secretary of Defense for Acquisition and Sustainment
United States Department of Defense
3010 Defense Pentagon Room 3E1010
Washington, DC 20301

Ms. Katie Arrington
Chief Information Security Officer
Office of the Under Secretary for Acquisition and Sustainment
United States Department of Defense
3010 Defense Pentagon
Washington, DC 20301

Dear Secretary Lord and Ms. Arrington:

As strong proponents of a secure and hardened defense industrial base (DIB), we write to outline our recommendations for improving the implementation, administration and enforcement of the Cybersecurity Maturity Model Certification (CMMC). We represent the producers and operators of some of the most sophisticated and widely used information technologies and have considerable first-hand knowledge of the challenging and evolving nature of the most persistent cyber threats. As cyber threats continue to evolve, it is essential that the federal government ensure their front-line cyber defenses stay current and are equipped with the tools and techniques to protect sensitive systems and information of the government and industrial partners. We respectfully request your consideration of our perspectives regarding how to further evolve the CMMC to best accomplish its objectives.

We strongly support efforts to improve DIB cybersecurity and appreciate the Department's openness in meeting with and accepting input from industry about the CMMC during the Autumn of 2019. We pledge to continue this partnership, as it is imperative that industry stakeholders and government continue to work together to ensure that the CMMC meets its overall objectives. We are concerned that current plans for implementing CMMC lack sufficient clarity and predictability in key areas, and as a result may unnecessarily generate confusion, delay and associated costs. These challenges could lead to the DIB being even less secure, if left

unaddressed. Accordingly, we urge DoD to thoroughly consider the following suggestions and questions as the CMMC evolves during its implementation.

Enhance Clarity about CMMC's Scope, Applicability, and Implementation Timeline

We support DoD's decision to phase-in the CMMC by initially limiting its requirements to 10 RFPs and 10 RFIs in Fiscal Year 2020 and ramping up over five years before requiring all new contracts to include CMMC compliance as a provision for Fiscal Year 2026. That said, we are concerned that standing up a completely new third-party auditing process that will enable enterprise scale audits in 2020 is very ambitious and believe that more clarity about the CMMC's scope and applicability is needed, if the timeline is to be met.

Flow-Down Requirements. The current CMMC approach asserts that certification requirements for DIB subcontractors will flow down from contractors in relation specifically to the contracts and components on which they are working. Additional clarity is needed regarding these flow-down requirements. It is conceivable – potentially even likely – that a subcontractor may be required to attain one level of certification for one contract or component, only to find out that a higher level is required on another contract. DoD should ensure that procurement officials, prime contractors and system integrators have sufficient knowledge of the model's requirements to understand what needs to flow down to subcontractors, and at what specific CMMC level.

Consistency in Procurement Requirements. The flow-down risk is exacerbated if no centralized approach to determining certification requirements is established; in other words, if each acquisition authority or prime contractor is allowed to establish certification requirements on its own, multiple authorities may set different level requirements for substantially similar services. This approach could require contractors and subcontractors to undergo certification multiple times at different levels, based on changing contract requirements – a scenario that is costly and inefficient. A more efficacious approach might be for DoD to evaluate, based on previous contracting histories, the anticipated certification requirements for contractors and subcontractors and provide upfront notification of these determinations or at least of illustrative examples, especially where there are multiple sets of cybersecurity requirements to consider. Such information will help the DIB make informed cybersecurity investment decisions.

Scope of coverage. The CMMC Model and accompanying materials provide only limited information about the intended scope of certification requirements, leaving several important questions unanswered. For example, it is unclear whether certification would be required in cases in which a subcontractor handles no CUI or is a non-US company; for instance, computer chips are usually sourced offshore and acquired as commercial-off-the-shelf hardware products. It also remains unclear whether the certification requirements will apply to non-procurement contracts such as cooperative agreements and grants.

Certification and Recertification.

The Department should clarify whether contractors covered by this year's RFIs and RFPs will need to recertify in three years, even though the CMMC model will not be fully implemented until 2026. In addition, DoD should also provide information about how companies that are not currently part of the DIB will be prioritized for certification, to ensure there is no interruption in bringing their innovations to the defense market.

Certification in Complex Environments. CMMC v1.0 provided some technical details on how to operate solutions in a complex environment but more guidance is needed about how to define organizational and logical system boundaries in order to determine the appropriate level of CMMC certification. One example to consider is how to scope the CMMC level for a corporate entity that does not store or process DoD data, but may provide centralized support to employees of a federal subsidiary (H.R., payroll, *etc.*). Another example which highlights this concern is CMMC levels 4 and 5 require a Security Operations Center (SOC) for incident response. The clarifying example discusses a SOC that spots trends across company networks. Does that SOC need to be dedicated only to the specific business unit handling CUI? Or is the SOC intended to span the whole corporate enterprise, including the non-federal or even non-US subsidiary business units across that enterprise? In either example, what is the implication of logical and/or organizational integration of a SOC for the CMMC level required of the business unit and the enterprise?

Streamlining Federal Cybersecurity Requirements

DoD should align the CMMC with the DoD Cloud Computing Security Requirements Guide (SRG), DFARS 252.204-7012 and FEDRAMP. With regard to cloud services, DoD should look to leverage FedRAMP and the SRG for CMMC designations at the product level *(i.e.* for servers, hardware, IaaS, PaaS and SaaS). While CMMC covers a broader range of products and services, those companies that have FedRAMP and SRG authorizations already surpass the vast majority if not all of the CMMC's control requirements, certainly at CMMC Levels 1-3, since FedRAMP requires continuous monitoring and improvement. If DoD believes that there are shortcomings in the FedRAMP or SRG requirements, it should work to address those with other Federal Government stakeholders. Allowing for reciprocity with other cybersecurity requirements will reduce the cost and administrative burden of compliance and allow DoD to achieve its cybersecurity goals on a quicker timeline. This applies to not only the providers of FedRAMP and SRG services but also to contractors and subcontractors who leverage FedRAMP services in their own environments. We recommend that DoD and the CMMC Accreditation Board document this reciprocity, develop a reference architecture and certification process compliant with DFARS 252.204-7012 to ensure that the FedRAMP services do not need to be re-accredited each time they are used by a contractor or sub-contractor and encourage subcontractors to leverage those reference models as best practices to streamline and improve their cybersecurity posture. When and where possible, we also recommend that anticipated and emerging cybersecurity requirements, such as for

IOT and new cryptographic standards, be accounted for appropriately, by defining objectives rather than by referencing particular standards that are evolving asynchronously with the CMMC standards.

Ensure No New Risks are Created

We also seek further clarity from the DoD on how CMMC assessment priorities will be set and how assessment results, which will contain very sensitive information, will be handled and stored. For example, if a CMMC assessor finds cybersecurity vulnerabilities in an existing DoD supplier, how is that finding communicated and what are the consequences? If the assessor finds a vulnerability, how is that information to be shared with other assessors and other members of the DIB in order to close the vulnerability as quickly as possible? Where a new best practice is identified, how is that information to be shared? For all of these examples, how is information shared in a way that protects the unique intellectual property and business practices of the contractor?

Further, we believe that some of the controls in CMMC apply best to traditional models, but not as well to modern large scale infrastructure. Rigid conformance to those controls may actually introduce new risks to the controls in place for high security and high availability or operational technology systems and environments (life/safety systems, military weapon systems, SCADA systems, etc.). We encourage DoD to work with providers of these systems, including Cloud Service Providers and System Integrators of large scale mission systems that operate at hyperscale, to develop and apply appropriate methods for verifying and certifying alternate controls and their implementation.

We recognize that there is a real tradeoff between speed of implementation and addressing these issues, given the risks to the DIB. At the current implementation speed, unless there is a continued commitment to improving CMMC in the areas noted, we are concerned it may limit competition and reduce the government's access to new technologies, while also recreating many of the previously experienced FedRAMP accreditation issues that resulted in years-long delays for both government and industry.

We stand ready to assist DoD in optimizing the CMMC's effectiveness. Considering and incorporating IT industry feedback will help ensure that DoD implements a structurally sound and holistic initiative from the beginning. Doing so will also help to meet our shared goal of improving DIB cybersecurity in a manner that is aligned with other federal government initiatives and requirements to address supply chain security.

We thank you in advance for your consideration.

Sincerely,

Alliance for Digital Innovation

BSA: The Software Alliance
Cybersecurity Coalition
Information Technology Industry Council (ITI)
Internet Association
The Computing Technology Industry Association (CompTIA)