NDIA
AT THE HEART OF THE MISSION

2101 Wilson Boulevard, Suite 700, Arlington, VA 22201-3060 • (703) 522-1820 • (703) 522-1885 Fax • NDIA.org

# AN ALTERNATIVE APPROACH TO INCREASING CYBERSECURITY THROUGHOUT THE DEFENSE INDUSTRIAL BASE

## INTRODUCTION

The National Defense Industrial Association (NDIA) fully supports the overarching policy objectives behind Section 1648 of the National Defense Authorization Act for Fiscal Year 2020 (Pub. L. 116-92) and the vision of creating a unified cybersecurity standard for DoD acquisitions. We strongly support the national priority to protect controlled unclassified information (CUI) stored and processed throughout the defense industrial base (DIB). We also support the Department of Defense's (DoD) objectives as expressed by Mr. Jesse Salazar, Deputy Assistant Secretary of Defense for Industrial Policy. In his recent testimony to the Senate Armed Services Committee, Mr. Salazar identified three objectives of the Cybersecurity Maturity Model Certification (CMMC) program: 1) to incorporate a unified set of cybersecurity requirements; 2) to provide the Department with assurance that industry meets the cybersecurity requirements; and 3) to provide supporting resources to help industry. The CMMC program, however, needs work to accomplish these objectives.

NDIA has worked hard with our member companies, other trade associations, and the Department of Defense to assist in the development of an interim rule to implement CMMC. We offer this paper as a collection of additional suggestions on how best to re-evaluate the CMMC program, with a focus on more up-front planning and requirements definition in addition to greater collaboration among DoD, industry providers, and enabling organizations. We are confident that, with proper planning and execution, DoD can overcome many of the CMMC challenges preventing the wide-scale adoption of greater cybersecurity throughout the DIB.

## THE PROBLEM

CMMC imposed a compliance regime without first establishing clear technical requirements or an executable path for industry implementation. This regime resulted from nine factors:

- CMMC benefited greatly from early champions within DoD. Recently, however, the program has suffered from a lack of leadership, communication, and transparency. While we understand that DoD is currently adjudicating comments to the interim rule and finalizing an internal review of the program, the lack of certainty of potential changes to the program is unsettling to those companies already taking steps towards CMMC compliance. DoD should provide clear, consistent communication to the DIB as soon as possible about any forthcoming changes to the program.
- CMMC, as conceptualized, does not fully leverage the capabilities of the cloud delivery model. CMMC should take steps to more carefully consider the role of Cloud Service Providers (CSPs) and the cloud-first environment that many businesses employ.
- The CMMC framework is designed for an "on-premises" network infrastructure that is rarely deployed today and is decreasing in use for legacy systems. The role that CSPs play in the CMMC ecosystem remains unclear, and the relationship between CMMC and FEDRAMP-authorized systems remains uncertain.
- CMMC did not properly sequence requirements development. Before developing acquisition rules, CMMC should have first assessed the impact of existing technical requirements and their ability to be executable and verified. The current design of all-

or-nothing compliance does not adequately consider the complexities of today's business environment.

- The cost of compliance with CMMC has been underappreciated and the degree to which those expenses will be allowable costs is uncertain. The actual costs that companies face to both attain CMMC compliance and receive CMMC certification are well above program office estimates, while allowability remains in question.
- CMMC did not create a clear, executable plan for implementation, particularly for small businesses. CMMC should have understood that asking DIB small businesses to understand and implement potentially vague requirements was not a viable path to success. CMMC should have first established an implementation plan with clearer requirements, a proposed solution, and supplemental resources for all businesses to achieve compliance.
- CMMC relies on the accurate identification, marking, and dissemination of controlled unclassified information. CUI continues to remain ill-defined without adequate government-wide guidance. The issue of CUI is further exacerbated by the lack of a clear demonstration of how CUI compares to federal contractor information (FCI), controlled technical information (CTI), and controlled defense information (CDI).
- CMMC does not properly delineate the unique differences between information technologies (IT) and operational technologies (OT). Though both types are networked, differences between IT and OT cannot be overstated. Issues such as latency can have a serious negative impact, especially in the manufacturing sector. CMMC needs to better account programmatically for these differences.
- Turbulence has hindered the trust in, and the effectiveness of, the CMMC Accreditation Body (CMMC-AB). The turbulent history and continued uncertainty surrounding the CMMC-AB—to include multiple resignations, charges of conflicts of interest, changes in leadership, and shifts in mission—have proven detrimental to trust in the organization and have increased the risk of a failed deployment of certifiers.

## OUR SUGGESTIONS

CMMC's mission should read: To provide the DIB with a flexible, affordable, and effective approach for assured cybersecurity at scale. We believe a simple barometer of CMMC success could be assessed in the response to one question: How would a one-person startup company that seeks to do business with DoD affordably achieve compliance in order to contract with the U.S. government?

As the steps below indicate, CMMC will need to perform significantly more requirements definition and implementation planning. We recommend the following steps be taken to make CMMC successful:

**Fully Leverage Cloud Capabilities and Advantages Where Practical.** CMMC should take advantage of the inherent capabilities of the cloud where it makes sense. This process can include collaborating with CSPs to deploy preconfigured and CMMC-compliant cloud environments for small businesses to easily adopt. DoD could also provide a government-furnished environment for small businesses, new entrants, and so on. Importantly, this step would include accounting for the unique attributes and requirements of IT versus OT. It would also enable DoD to coordinate the adoption of evolving cybersecurity methods consistent with the President's Executive Order on Improving the Nation's Cybersecurity.

**Establish Adequate Definitions of Critical Terms.** There continues to be confusion over the definition of key terms related to the CMMC program, including federal contracting information, controlled unclassified information, controlled defense information, and controlled technical information. Inconsistent use of these classifications of data and contract materials exacerbates the ability of companies to configure processes to ensure compliance with CMMC. Clear definitions, marking and dissemination guidance, and examples of each classification should be prioritized and published as quickly as possible.

**Provide Clear Guidance on the Pathway to Adoption of CMMC.** The current DFARS requirements implementing NIST SP 800-171 can jump-start CMMC adoption—but only if companies are given the tools and the financial assistance to successfully implement the NIST standards. Providing clear guidance on when individual programs, contracts, or companies are expected to be CMMC compliant and at what level will also help tremendously in ensuring that the DIB is ready to respond to DoD's forthcoming requirements.

**Reinvigorate the Maturity Model.** The current all-or-nothing compliance system moves the CMMC program away from a model based on maturity of implementing cyber controls and instead imposes a checklist regime that requires full compliance with the set-forth requirements. Even at CMMC Maturity Level 1, there are requirements, like 1.077, which—when taken literally not to allow any non-approved devices access to information systems—would likely cause all organizations seeking certification to fail. Instead of taking steps towards the maturity of implementing controls as the CMMC levels increase, the controls require full compliance at each level to receive certification. This rigid method of compliance will likely prove difficult to implement when reaching the assessment and certification stages of implementation, and so it should be further examined. There is also some question of whether such an approach will be effective in mitigating the adaptive nature of the cyberthreat.

**Establish Guidance Materials.** Current guidance materials have been helpful but fall short of providing clear examples of effective implementation while also demonstrating a rubric with which the assessor will determine compliance. Every company is currently approaching the adoption of the CMMC program from a different starting place and with a different existing network architecture. The vagueness of NIST SP 800-171 standards as well as the delta between NIST and CMMC requirements provide flexibility, but they leave companies having to interpret exactly how to implement the controls in a way that will satisfy an assessor. Reference materials that provide clear examples of compliant methods for CMMC implementation will help to drive up compliance while driving down compliance costs. CMMC could offer complete technical documentation, including pre-developed System Security Plans (SSPs) based on each blueprint, along with recommended implementation approaches for the remaining subsystems and non-technical requirements. Complete technical documentation will also offer DIB members the ability to replicate the implementation on their different system if they choose not to use a specific blueprint.

We also recommend leveraging the existing expertise within government and academia to create CMMC-related Toolkits, Job Aids, Training Modules, and Certificates to enhance the adoption of CMMC requirements. This method would be like the approach used to aid Facility Security Officers (FSOs) and the Department's industrial security program.

**Expand the Universe of Assessors to Include the Government.** We recommend that CMMC consider reassessing its second CMMC objective "to provide the Department assurance, via external assessment, that all contractors and subcontractors…meet mandatory cybersecurity requirements." Under an alternative proposed approach, external assessment would not be the only option for DoD assurance. The DCMA DIBCAC group has already demonstrated the ability to successfully perform CMMC assessments and could provide needed capacity.

**Provide Clear Guidance for Cost Allowability.** The cost of compliance with the CMMC program is a current hurdle to adoption and, in the future, will prove to be a high barrier to entry for new entrants. The ability to document and pass along compliance costs is a must to ensure that current DIB companies remain healthy and that DoD remains an attractive customer to new entrants.

**Provide Clear Public Expectations for the CMMC-AB.** The role of the CMMC Accreditation Body is essential to the success of the CMMC program. However, to this point, the CMMC-AB has been marred with resignations, conflicts of interest, and murky expectations. DoD should publish clear expectations of the CMMC-AB and exert more oversight of the AB to ensure that assessments and compliance can be effectively implemented and monitored.

**Prepare for What Comes Next.** Implementing this approach better positions the Department and the DIB to work collectively to address growing near-term (e.g., ransomware, phishing, DDOS, and others risks) and evolving threats as well as to better prepare for future challenges. The President's recent Executive Order on Improving the Nation's Cybersecurity directs a public-private partnership to "adapt to the continuously changing threat environment." We understand that changes to CMMC and other cyber requirements will be needed over time. Using a collaborative, public, and hands-on approach will help to ensure broad adoption and to raise the cyber foundation of our entire defense and manufacturing industrial bases.

## CONCLUSION

Despite CMMC's early implementation challenges, cybersecurity remains a national priority. We must protect CUI stored and processed throughout the DIB. We fully support that priority and recommend that CMMC embrace the mission to provide the DIB with a flexible, affordable, and effective implementation for assured cybersecurity at scale. That mission can only be achieved by taking steps to implement the solutions suggested herein. With those solutions in place, the CMMC program can assure compliance while continuously developing improvements and preparing for evolving cybersecurity threats. We are ready, willing, and able to assist a collaborative approach to accomplishing this national priority.