IPC®

BUILD ELECTRONICS BETTER

STRENGTHENING NATIONAL SECURITY AND SUPPLY CHAIN RESILIENCY BY IMPROVING DOD CYBERSECURITY CERTIFICATION

An IPC Report — June 2021

TABLE OF CONTENTS

FOREWORD

Cyberattacks on the U.S. industrial base continue to grow in number, scope, and sophistication. U.S. electronics manufacturers are especially attractive to attackers given the unique importance of electronics in nearly all defense applications and weaponry. In response, the industry has taken proactive steps to protect controlled unclassified information (CUI) and other sensitive information related to the design, production, and performance of defense electronics.

The most notable example of the industry's proactive posture is the development of the IPC-1791 "Trusted Supplier" standard and the corresponding Qualified Manufacturers List (QML) for those that design and fabricate printed circuit boards and printed circuit assemblies. The standard, which was developed in collaboration with the U.S. Defense Department's Executive Agent for Printed Circuit Boards and Interconnect Technology, builds on previously existing standards to cover both cyber and physical security. More and more companies are getting validated to the standard, establishing a more robust community of trusted suppliers of electronics to the Department of Defense (DoD).

IPC-1791 anticipated the Cybersecurity Maturity Model Certification (CMMC). Those companies that are validated to IPC-1791, in fact, are better prepared to achieve the requisite certification under CMMC. However, the CMMC places significant new obligations on electronics manufacturers, who tend to operate on razor-thin margins in a highly competitive global marketplace. Defense-related work is usually a small percentage of overall revenue for these businesses, raising concerns for many companies about whether the higher-than-expected costs of CMMC compliance can be justified.

This report, drawing on IPC industry survey results, amplifies concerns that the CMMC may weaken U.S. industrial base resiliency even as it seeks to bolster security for those that remain in it. The report's author, defense cyber policy expert Leslie Weinstein of HITRUST, lends her analysis of the survey results and offers opportunities for DoD to better support the industry through CMMC compliance and certification.

IPC will continue to be an advocate for the industry on this important issue and encourages companies to take all necessary steps to understand the CMMC and seek certification as necessary.

John W. Mitchell
President and CEO
IPC

EXECUTIVE SUMMARY

This report finds:

- The costs and burdens anticipated to be necessary to achieve Cybersecurity Maturity Model Certification (CMMC) compliance will drive many suppliers out of the U.S. Department of Defense (DoD) supply chain, which will negatively impact national security.
  - Nearly one-quarter (24 percent) of IPC survey respondents indicate that the costs and burdens of CMMC compliance will likely force them out of the DoD supply chain.
  - A third (33 percent) of respondents feel the CMMC will weaken at least part of the electronics industrial base, while 18 percent are unsure, highlighting the uncertainty around CMMC.
  - Roughly 41 percent of respondents believe that applying the CMMC clause to their suppliers will create problems within the supply chain.
- DoD underestimates the cost impact of the Defense Federal Acquisition Regulation Supplement (DFARS) interim rule, which is premised on a false understanding that the cost burden on the U.S. defense industrial base (DIB) is manageable and sustainable.
  - Approximately 68 percent of respondents foresee the need to hire a consultant or bring in outside help to prepare for CMMC assessment.
  - Nearly one-third (32 percent) report it will take one to two years to prepare to undergo a CMMC assessment.
- Most companies seem unaware of the potentially heavy costs associated with CMMC compliance, and the DoD has provided too few resources to ensure the DIB can achieve CMMC compliance.
  - Less than half (49 percent) of survey respondents feel they are “very” or “extremely” familiar with CMMC compliance.
  - Some 52 percent of respondents report that DoD has not provided industry with sufficient guidance to support CMMC preparedness efforts.
- The DoD should leverage existing standards to help reduce the costs and burdens of CMMC compliance.
  - While the CMMC’s stated objective is to improve supply chain visibility and monitoring, it does so at the expense of other key aspects of supply chain health. The CMMC runs the risk of creating barriers to entry which will complicate supplier onboarding and reduce supply chain diversity and resiliency.

INTRODUCTION

Last year, the U.S. Department of Defense (DoD) issued an interim rule establishing a new framework for strengthening the cybersecurity posture of the U.S. defense industrial base (DIB). Referred to as the Cybersecurity Maturity Model Certification (CMMC), the framework sets out new requirements, as well as an assessment and certification process, that is designed to better safeguard sensitive federal contract information (FCI) and controlled unclassified information (CUI). When it is fully implemented, the CMMC will place new obligations on all U.S. electronics manufacturers that directly or indirectly serve the U.S. defense market.

The CMMC is a laudable and necessary DoD initiative, but it is not without risk to the resiliency of the DIB. In creating the CMMC, DoD has failed to appreciate the true costs associated with certification. The costs, in fact, are considerable, especially for electronics manufacturers which operate in a highly competitive, thin-margin business. Given that DoD-related sales are a small percentage of overall sales for most electronics manufacturers, many may exit the defense market, concluding that CMMC costs cannot be justified.

To better understand the potential impact of the CMMC on U.S. electronics manufacturers, IPC fielded an industry survey between February 25 and March 5, 2021. The survey garnered 108 responses from contract manufacturers, printed circuit board fabricators, original equipment manufacturers and suppliers that self-reported they are planning to undergo a CMMC assessment in the next five years.

The results of the survey confirm the likelihood that the CMMC will push many companies out of the defense market unless DoD takes steps to support the industry's assessment and compliance. Even more worrisome, the risk to industrial base resiliency may be greater than currently realized as most companies are not fully aware of the heavy costs associated with CMMC compliance.

This report concludes that the DoD should reduce the costs and burdens of the CMMC on the DIB by leveraging existing industry standards and certifications. There are several widely adopted security standards and certification processes that have been implemented by thousands of companies around the world. Recognizing additional certifications currently available in the market will not only save DIB companies money and reduce the number of redundant audits by leveraging their existing certifications, but it will also create a pool of DIB companies who are able to bid on solicitations containing the CMMC Defense Federal Acquisition Regulation Supplement (DFARS) clause.

CMMC DFARS INTERIM RULE OVERVIEW

On September 29, 2020, the DoD published an emergency interim rule in the Federal Register to amend the DFARS to implement a DoD Assessment Methodology and the CMMC framework to assess contractor implementation of cybersecurity requirements and enhance the protection of unclassified information within the DoD supply chain. The CMMC requires a third-party verification of contractor implementation of cybersecurity requirements and has a five-year implementation timeline. The DoD assessment and scoring methodology measures contractor implementation of existing cybersecurity requirements. The existing cybersecurity requirements, found in the DFARS clause 252.204-7012, requires contractors who handle CUI to implement NIST SP 800-171 in their environments which handle CUI. However, findings from a DoD Inspector General report (DODIG-2019-105, "Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems") indicated that DoD contractors did not consistently implement mandated system security requirements for safeguarding CUI, and it recommended that DoD take steps to assess a contractor's ability to protect this information. The DFARS interim rule was issued in direct response to this finding and is meant to provide DoD visibility into the cybersecurity posture of its supply chain.

In addition to the DoD Assessment Methodology, the DFARS interim rule introduced three new DFARS Clauses:

- 7019 Clause: Requires contractors who handle CUI to implement NIST SP 800-171 for environments which handle CUI; conduct a self-assessment (Basic Assessment) using NIST SP 800-171A1A[1] and the DoD Assessment Methodology scoring rubric; and submit their score into the Supplier Performance Risk System (SPRS) to be considered for award with a contract containing both the -7012 and -7019 Clauses. The -7019 Clause has a three-year implementation timeline, with 100% of new RFPs to contain the clause by October 1, 2023. The score on record must not be more than three years old.
- 7020 Clause: Paired with the -7012 and -7019 Clauses, it requires a contractor to provide the Government with access to its facilities, systems, and personnel when it is necessary for DoD to conduct or renew a higher-level assessment, known as Medium and High Assessments.
  - Medium Assessment: Required for certain DoD awardees. The contractor provides DoD access to its facilities and personnel, if necessary, and prepares for/participates in the assessment conducted by the DoD. The DoD assessor will review the system security plan description of how each requirement is met and will identify any descriptions that may not properly address the security requirements. DoD will post the results in SPRS.

[1]Ross, Dempsey, and Pillitteri, U.S. National Institute of Standards and Technology (NIST), "Assessing Security Requirements for Controlled Unclassified Information," NIST Special Publication 800-171A, June 2018.

  - High Assessment: Required for certain DoD awardees. The contractor provides the DoD access to its facilities, systems, and personnel and prepares for/participates in the assessment conducted by DoD. The DoD assessors will review the system security plan description of how each requirement is met and the contractor will demonstrate the implementation to the DoD assessors. DoD will post the results in SPRS.

- 7020 Clause: The CMMC clause. It is prescribed for use in solicitations and contracts, including solicitations and contracts using FAR Part 12 procedures for the acquisition of commercial items, excluding acquisitions exclusively for COTS items. CMMC will apply to all DoD solicitations and contracts, including those for the acquisition of commercial items (except those exclusively COTS items) valued at greater than the micro-purchase threshold, starting on or after October 1, 2025. CMMC certification requirements are required to be flowed down to subcontractors at all tiers, based on the sensitivity of the unclassified information flowed down to each subcontractor.

This white paper provides an analysis of an IPC industry survey and compares the findings with the DFARS Interim Rule's analysis of the impact of the CMMC to industry, highlighting major discrepancies that have the potential to detrimentally impact the DIB and ultimately undermine national security.

THE CMMC MAY CAUSE FURTHER EROSION OF THE DIB AND UNDERMINE NATIONAL SECURITY

The 2018 National Security Strategy "highlights the importance of a vibrant manufacturing sector to comprehensive national power, while warning of the dangers inherent in the weakening of America's manufacturing base: A healthy defense industrial base is a critical element of U.S. power and the National Security Innovation Base."[2] According to Dun & Bradstreet, the four characteristics of a healthy supply chain are supplier diversity, supply chain visibility, effective supplier onboarding, and supply chain monitoring.[3] While the CMMC's stated objective is to improve supply chain visibility and monitoring, the CMMC does so at the expense of other key aspects of supply chain health. The CMMC creates barriers to entry which complicate supplier onboarding and decrease supplier diversity, therefore reducing supply chain resiliency. Since 2010, critical manufacturing and DIB manufacturing industries have seen fluctuations in federal obligations spending, creating variability in vendor counts, and deteriorating DoD's supply chain (Figure 1). The effects of sequestration and the budget caps accelerated the downward trend in vendor counts, resulting in an estimated 20% decline in the number of prime vendors.[4]

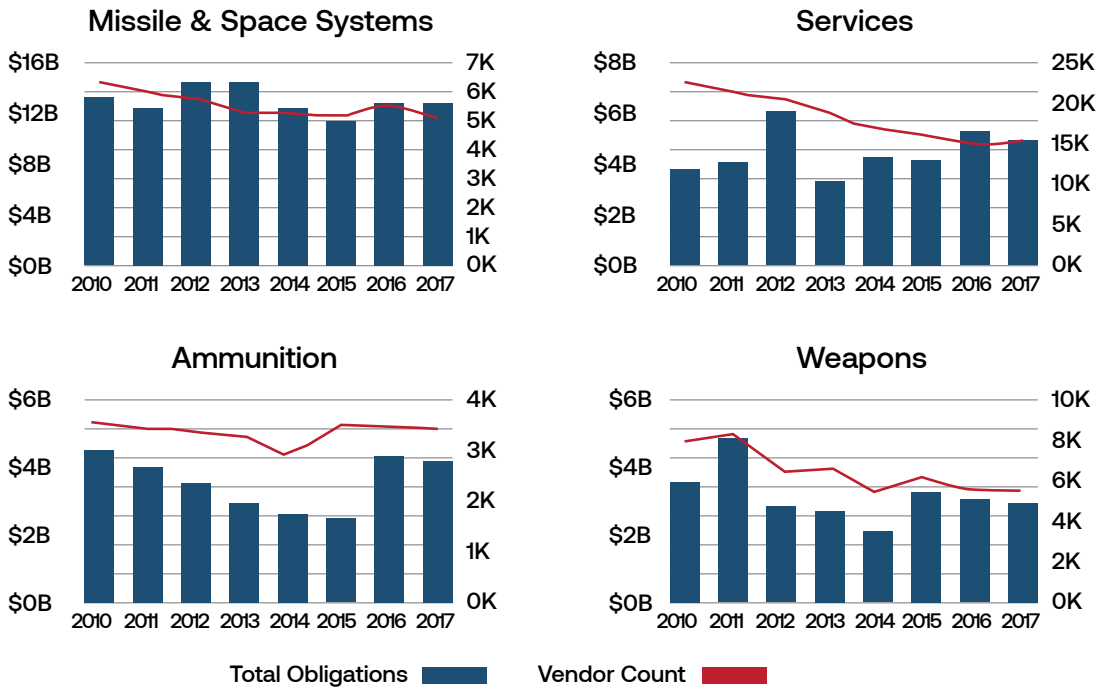
---

[2] U.S. Dept. of Defense, Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States, Report to President Donald J. Trump by the Interagency Task Force in Fulfillment of Executive Order 13806, September 2018, page 24. Hereafter cited as the "Defense Industrial Base Report."

[3] Brian Alster, Dun & Bradstreet Supply Chains Need Health Checks, Too, July 12, 2018

[4] US. Department of Defense, Defense Industrial Base Report, p. 26.

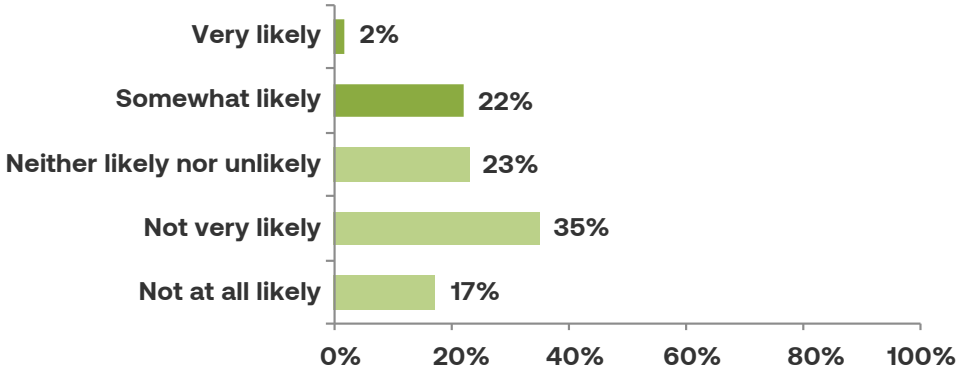
Figure 1: Falling Vendor Counts in Key Manufacturing and Defense Industrial Base Areas



Source: U.S. Department of Defense, Defense Industrial Base Report, p. 26.

Nearly one-quarter of the IPC CMMC survey respondents indicated that the costs and burdens of CMMC compliance are likely to force them out of the DoD supply chain (see Figure 2). Most of the survey respondents report that 50% or less of their annual company revenue comes from the DoD. For many small businesses, the costs and burdens of CMMC compliance may outweigh the benefits gained by supplying to the DoD. Respondents of the survey also indicated that the DoD has not done enough to prepare the DIB for the CMMC, noting a lack of sufficient guidance on the requirements. This lack of guidance on the requirements has created difficulties for the DIB in evaluating external resources, such as consultants, which 68% of respondents believe will be needed to prepare for the CMMC.

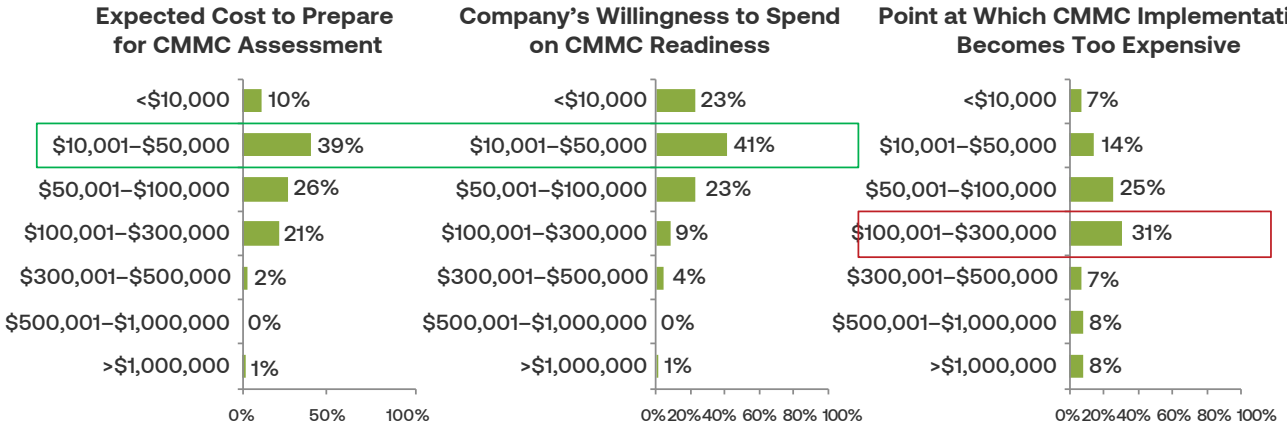
Figure 2: Likelihood of Being Forced Out of the U.S. Defense Market



Source: IPC Industry Survey, 2021

Most suppliers expect and are willing to spend upwards of $50,000 on CMMC readiness. At the same time, more than half of suppliers report implementation costs exceeding $100,000 would make CMMC readiness too expensive. In DoD's cost analysis submitted as supporting documentation with the DFARS interim rule, DoD estimated the cost of a CMMC Maturity Level 3 (ML3) certification to be more than $118,000 in the first year. Therefore, DoD's own cost analysis of CMMC ML3 compliance is in the range of being too expensive for 77% of IPC CMMC survey respondents. Figure 3 also highlights the apparent lack of awareness the DIB has of DoD's estimated cost of CMMC compliance.

Figure 3: Industry Willingness to Spend on CMMC Readiness



Source: IPC Industry Survey, 2021

The CMMC-Accreditation Body (CMMC-AB), the sole entity recognized by the DoD to issue CMMC certifications, created the concept of a "registered practitioner" (RP) and a "registered provider organization" (RPO). According to the CMMC-AB's website (cmmcab.org), "The RPOs and RPs in the CMMC ecosystem provide advice, consulting, and recommendations to their clients." RPs and RPOs are the "implementers" and consultants, but do not conduct Certified CMMC Assessments. These RPs "have attended CMMC-AB sponsored training classes, completed a test, signed the Code of Professional Conduct, and passed a criminal background check" prior to being listed on the CMMC-AB Marketplace. RPOs must "receive authorization from the CMMC-AB as a result of registering, sign the RPO agreement with the CMMC-AB, pass an Organizational Background Check via data provided to the CMMC-AB by Dun & Bradstreet and have a DUNS number, and at least one RP must be associated with the RPO at all times" to be listed on the Marketplace. The CMMC-AB's website further states that attaining the RPO badge simply means that a company has a "basic understanding of [the CMMC's] requirements" and does not connote expertise. The RP badge costs individual consultants $500 annually to maintain, and the RPO badge costs companies $5,000 annually to maintain.

While the preponderance of the IPC survey respondents claimed that DoD had not done enough to guide the DIB to qualified CMMC practitioners, a few respondents believed that the CMMC-AB RP badge helped them identify qualified consultants. Fortunately, only a small minority of respondents believed that the RP badge implies expertise.

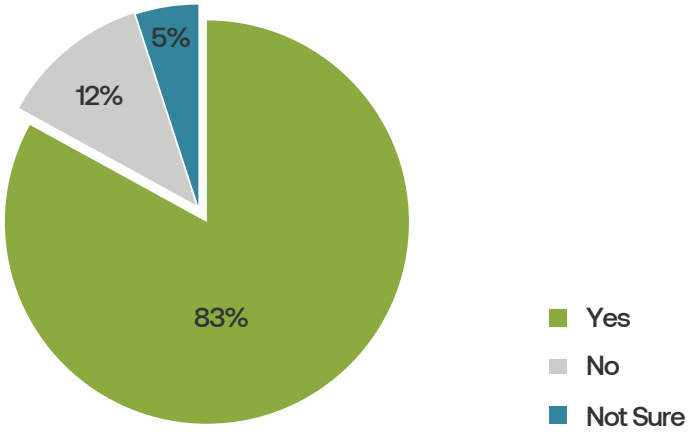
To steer industry to qualified professionals who can help with implementing the CMMC, the DoD and the CMMC-AB could leverage the DoD Cyber Workforce Framework (DCWF) to communicate to industry the knowledge, skills, and attributes of qualified internal cyber workers or external consultants. The DCWF describes the work performed by the full spectrum of the cyber workforce as defined in DoD Directive (DoDD) 8140.01. The DCWF leverages the original National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NCWF) and the DoD Joint Cyberspace Training and Certification Standards (JCT&CS).[5] The DCWF has a hierarchical structure with seven broad categories (e.g., "securely provision" and "oversee and govern"), 33 specialty areas (e.g., "systems administration" and "data administration"), and 54 work roles (e.g., "system administrator" and "technical support specialist"). Each work role contains a definition as well as a representative list of tasks and knowledge, skills and abilities (KSAs) describing what is needed to execute key functions. There is also a Certified Information Systems Auditor (CISA) certification issued by the Information Systems Audit and Control Association (ISACA), which could be leveraged to connote IT auditing expertise and experience.

THE COST OF THE CMMC DFARS RULE IS VASTLY UNDERESTIMATED

In the DFARS interim rule, the DoD claims that only 30% of the DIB would be expected to attain a CMMC ML3, while the majority (60%) will only need a CMMC ML1. This rule implies that only 30% of the DIB handles or needs to handle CUI, as CMMC ML3 or higher is required to handle CUI. But according to the IPC survey results, 83% of respondents handle CUI and ITAR (International Traffic in Arms Regulations) data (see Figure 4). While the IPC survey respondents may not accurately represent the actual distribution of companies in the DIB who handle CUI, the survey results indicate that DoD's assumption that a minority of the DIB handle CUI may be uninformed.

[5] U.S. Dept. of Defense Chief Information Officer, "The DoD Cyber Workforce Framework." (DCWF), https://dodcio.defense.gov/Cyber-Workforce/DCWF.aspx.

Figure 4: Does Your Company Handle Control Unclassified Information or ITAR Data?



Source: IPC Industry Survey, 2021.

The DoD estimates a CMMC ML1 will cost $2,999 for small entities, for both the contractor support and the C3PAO assessment. The DoD estimates a CMMC ML3 will cost small entities $26,214 in nonrecurring engineering costs, $41,666 in annual recurring costs, and $51,096 for contractor support and the C3PAO assessment. Thus, the cost of a CMMC ML3 in the first year is more than $118,000. The cost difference between the CMMC ML1 and CMMC ML3 is more than $115,000 per small entity.

The DoD believes there are 163,391 small companies in the DIB. The DoD estimates the total cost to small entities in the first 10 years of the CMMC to be $3 billion, based on the assumption that 30 percent of the DIB will need a CMMC ML3 (see Table 1).

Table 1: DoD Cost Impact of CMMC ML3 for First 10 Years

Level 3	Quantity Unique Small Entities					
Year	Initial	Recert	Recert	Recert	Total	Total Cost
1	335	0	0	0	335	$39,856,827
2	1,661	0	0	0	1,661	$211,576,581
3	5,543	0	0	0	5,543	$742,647,086
4	10,624	335	0	0	10,959	$1,595,233,775
5	10,623	1,661	0	0	12,284	$2,105,527,148
6	10,623	5,543	0	0	16,166	$2,746,498,185
7	9,590	10,624	335	0	20,549	$3,342,948,078
8	0	10,623	1,661	0	12,284	$2,669,250,684
9	0	10,623	5,543	0	16,166	$2,867,603,803
10	0	9,590	10,624	335	20,549	$3,091,555,818

Source: U.S. Department of Defense, "Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019–D041)," Federal Register 85, no. 189 (September 29, 2020), pp. 61505-61522. https://www.govinfo.gov/content/pkg/FR-2020-09-29/pdf/2020-21123.pdf

If, however, one assumes that the distribution of the IPC survey results is representative of the CMMC ML3 distribution, the cost of the CMMC ML3 certification to small entities skyrockets from $3.3 billion in the 7th year of implementation (the most expensive year out of the first 10) to $9.3 billion. If the actual percentage of DIB companies needing a CMMC ML3 is between the DoD's estimate and the IPC survey results, at 60 percent, the cost in year seven is more than $6.6 billion to small businesses (see Table 2).

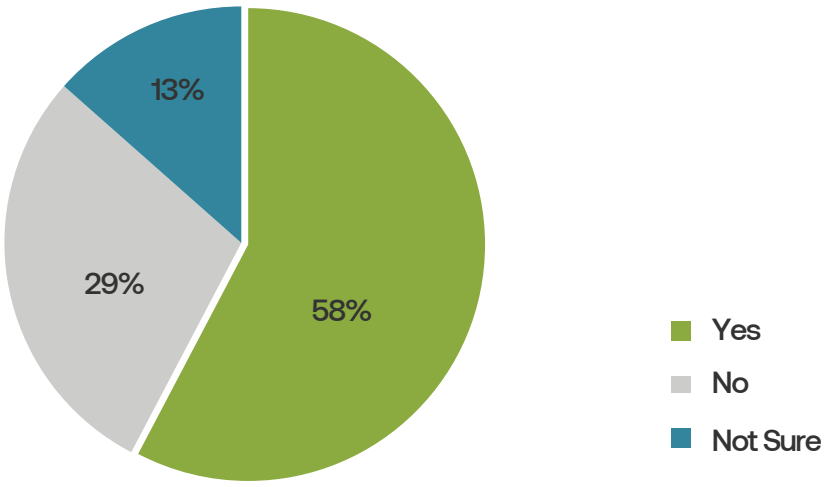
Table 2: Annual Costs of CMMC ML3, Three Scenarios

Year	Total Small Entities	Total Cost 30% ML3	Total Cost 60% ML3	Total Cost 84% ML3
1	335	$39,856,827	$79,713,654	$111,599,116
2	1,661	$211,576,581	$423,153,162	$592,414,427
3	5,543	$742,647,086	$1,485,294,172	$2,079,411,841
4	10,959	$1,595,233,775	$3,190,467,550	$4,466,654,570
5	12,284	$2,105,527,148	$4,211,054,296	$5,895,476,014
6	16,166	$2,746,498,185	$5,492,996,370	$7,690,194,918
7	20,549	$3,342,948,078	$6,685,896,156	$9,360,254,618
8	12,284	$2,669,250,684	$5,338,501,368	$7,473,901,915
9	16,166	$2,867,603,803	$5,735,207,606	$8,029,290,648
10	20,549	$3,091,555,818	$6,183,111,636	$8,656,356,290

Source: Author's analysis based on the DFARS CMMC interim rule and the IPC industry survey.

In addition to needing a CMMC ML3 at some point in the next five years, companies that handle CUI will also be required to conduct a NIST SP 800-171 self-assessment and submit their scores to SPRS as part of the DFARS-7019 Clause. While the self-assessment and reporting of the score is meant to be triggered by companies bidding on new contracts with the -7019 DFARS Clause, large prime contractors have been preemptively asking suppliers to conduct a self-assessment and to report their score into SPRS. At least 58% of the IPC survey respondents have already been asked by a prime contractor to conduct a NIST 800-171 self-assessment and to report the score to SPRS, before any solicitations with the -7019 Clause have been released (Figure 5). The respondents to the IPC survey overwhelmingly handle CUI and therefore the self-assessment requirements would apply to them at some point over the next three years. It is worrisome that more than half of the respondents have already been asked to conduct a self-assessment by a prime contractor, even though there is no legal or contractual requirement to conduct the assessment. According to DoD's cost impact analysis, "the need for a Basic Assessment will begin to impact entities as they compete on solicitations that include the new solicitation provision and contract clause, and the clause at DFARS 252.204-7012, if the entity has covered contractor information systems that are required to be in compliance with NIST SP 800-171."

Figure 5: Has Your Company Already Been Asked to Conduct a Self-Assessment?



Source: IPC Industry Survey, 2021

The NIST SP 800-171 self-assessment and reporting is estimated by DoD to take less than an hour and cost less than $100 per assessment. According to a NIST Cybersecurity Self-Assessment Handbok, "conducting security control assessments can be challenging and resource-intensive. Successful assessments require cooperation throughout the company. Establishing expectations before, during, and after an assessment is important to achieve an acceptable outcome. Thorough preparation is an important aspect of conducting effective security control assessments." The handbook also explains that, "It is expected that the business owner, chief operating officer, IT manager, security manager, and plant manager(s) will work together to assess the security of the system(s) that process, store, or transmit CUI."[6] Based on NIST's advice for preparing for and conducting a NIST 800-171 self-assessment, it would take much longer than an hour and cost more than $100 to conduct one properly. NIST does not provide an estimated number of personnel hours needed to properly conduct a NIST 800-171 self-assessment, but with 110 controls and more than 200 assessment objectives, it can be estimated that at least 30 minutes is needed to assess each control; properly acknowledging some controls will take far longer; and others much less. At 30 minutes per control, the NIST 800-171 self-assessment would take 55 hours to complete. Using a journeyman-level-2 rate of pay of $99/hour, a basic self-assessment would cost $5,445, which is $5,300 more than DoD's estimate of $73.30.

[6] U.S. National institute of Standards and Technology (NIST), "NIST MEP Cybersecurity Self- Assessment Handbook for Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements," https://nvlpubs.nist.gov/nistpubs/hb/2017/nist.hb.162.pdf

In their impact analysis, DoD claims the annualized cost of the self-assessments is $971,083, based on a cost of $74.31 per self-assessment for 40,824 entities (and one assessment every three years). The self-assessment requirement, however, is going to impact far more than 40,824 companies because every company that handles CUI must conduct the self-assessment. According to the DFARS interim rule, at least 30% of the DIB will need a CMMC ML3, which implies that they handle CUI. The DoD estimates there are 220,000 companies in the DIB, which means that there are closer to 66,000 companies that will need to conduct a NIST 800-171 self-assessment. Currently, more than half (58%) of the IPC survey respondents are being required by prime contractors to conduct the self-assessment. If 58% of the rest of the DIB is being asked by a prime contractor for a self-assessment, the number of impacted companies jumps to 127,600 companies. If the price of the self-assessment is closer to $5,445 and the number of impacted companies is 30% of the DIB, as the DoD estimates in the interim rule, the actual annualized cost of the Basic self-assessment jumps from $971,803 to $119,790,000, which is 123 times more expensive than the DoD's total estimated cost impact to both the government and the DIB. If 58% of the DIB are required to conduct Basic self-assessments, the annualized cost jumps to $231,594,000, which is more than 200 times more expensive than DoD's total cost impact to the DIB and the government.

CONCLUSIONS AND RECOMMENDATIONS

President Biden's Executive Order on Improving the Nation's Cybersecurity instructs the Executive Branch to modernize FedRAMP (a cloud security framework), including identifying and mapping relevant compliance frameworks and allowing those frameworks to be used as a substitute for the relevant portion of the authorization process. Likewise, the DoD can proactively modernize the CMMC along with the FedRAMP process by recognizing existing compliance frameworks.

The DoD and the CMMC-AB should establish qualification criteria for consultants so that the DIB is better suited to vet potential consultants for CMMC preparation. The DoD should help educate the DIB that the qualification criteria expressed as KSAs and a list of other attributes associated with qualifications (certifications, experience, and education) which demonstrate those KSAs. In the same way that DoDM 8570 establishes a list of baseline certification requirements for the DoD cybersecurity workforce, DoD should establish and publish baseline qualification standards for CMMC consultants and CMMC assessors that map to the DCWF.

To reduce the costs and burdens of the CMMC on the DIB, the DoD should consider leveraging existing industry standards and certifications. There are several widely adopted security standards and certification processes that have been implemented by thousands of companies around the world. The DoD should evaluate the level of risk mitigation and assurances provided by these existing certifications to determine if they provide equivalent or better protection for FCI and CUI. Recognizing additional

certifications currently available in the market will not only save DIB companies money and reduce the number of redundant audits by leveraging their existing certifications, but it will also create a pool of DIB companies who are able to bid on solicitations containing the CMMC DFARS clause. The CMMC-AB currently has no approved C3PAOs who may conduct CMMC assessments, but by recognizing other industry certifications, DoD will gain instant capacity for recognized assessments and a cadre of qualified and experienced assessors.

The U.S. electronics manufacturing industry is highly competitive with thin margins. DoD continues to assert that the CMMC costs will be recouped through general and administrative overhead costs in DoD contracts. This method of reimbursement favors late adopters and those that skimp on compliance expenses, which drives the industry to implement the bare minimum to pass the CMMC assessment. DoD should provide details into the method by which CMMC overhead costs are calculated and reimbursed. Overhead costs vary greatly from company to company, with no transparency to the DoD nor to the rest of the industry. The U.S. electronics manufacturing industry cannot remain in the DIB if they are forced to subsume additional overhead costs to remain competitive against peers who calculate their general and administrative CMMC costs differently.

About the Author

Leslie Weinstein is an Army Reserve Major with more than 15 years of experience consulting and working for the Department of Defense. In addition to her experience on active duty at the Defense Intelligence Agency and with offensive cyber operations at Army Cyber Command, Leslie has consulted for the Office of the Undersecretary of Defense for Acquisition and Sustainment (OUSD (A&S)), the DoD CIO, and the Air Force. As a consultant, Leslie focused on cyber policy and strategy and contributed to several initiatives impacting the entire DoD cyber workforce, including the DoD Cyber Workforce Framework and the Cyber Excepted Service. Leslie is currently serving as the Solutions Director for HITRUST.

Leslie has a Bachelor of Science degree in Management of Information Systems from the University of Alabama in Huntsville; a Master of Science in Strategic Intelligence from the National Intelligence University; and a Master of Business Administration from Cornell University.

IPC®
BUILD ELECTRONICS BETTER
3000 Lakeside Drive, Suite 105 N
Bannockburn, IL 60015 USA
+1 847-615-7100 **tel**
+1 847-615-7105 **fax**
www.**ipc**.org

IPC is the global association that helps OEMs, EMS, PCB manufacturers, cable and wiring harness manufacturers and electronics industry suppliers build electronics better. IPC members strengthen their bottom line and build more reliable, high quality products through proven standards, certification, education and training, thought leadership, advocacy, innovative solutions and industry intelligence.