Technical Support
INTERNATIONAL
Professional IT Services

WHAT YOU ARE MISSING ABOUT THE CMMC:

A Guide to the Technical CMMC Program Management Controls & Components of the CMMC

By **JOHN BERMINGHAM, CISSP**
Director of Cybersecurity & Compliance

Introduction to the CMMC

The Department of Defense (DoD) has migrated to a new cybersecurity model designed to assess and enhance the cybersecurity posture of the Defense Industrial Base (DIB) and its supply chain. The DoD's Cybersecurity Maturity Model Certification (CMMC) will also serve as the verification mechanism to ensure these appropriate levels of cybersecurity practices and processes are in place throughout the DIB contractor space.

In order to help clarify and guide your organization through the entire CMMC process, this white paper will begin with an overview of CMMC, then transition to provide practical implementation advice intended to help DIB contractors view and ultimately achieve their CMMC compliance requirements from a ground-level perspective.

To clarify the scope of CMMC requirements, including their respective domains, we have included the following charts taken from the Cybersecurity Maturity Model Certification, Version 1.0, dated January 30, 2020.

The first figure below illustrates the 17 CMMC Domains of the model. Each Domain consists of a series of Capabilities, Practices and Processes that DoD requires contractors to recognize and develop to help secure CUI whereas Figure 2 depicts the five Practice and Process Levels of the model.

Practice levels range from Basic Cyber Hygiene (Level 1), to that of Advanced/Progressive at (Level 5). Similarly, Process levels range from Performed (Level 1), to Optimized at (Level 5). The premise being that contractors implement practices and processes consistent with the sensitivity of information (CUI) they have access to.

Fig. 1. *The 17 CMMC Domains of the Model*

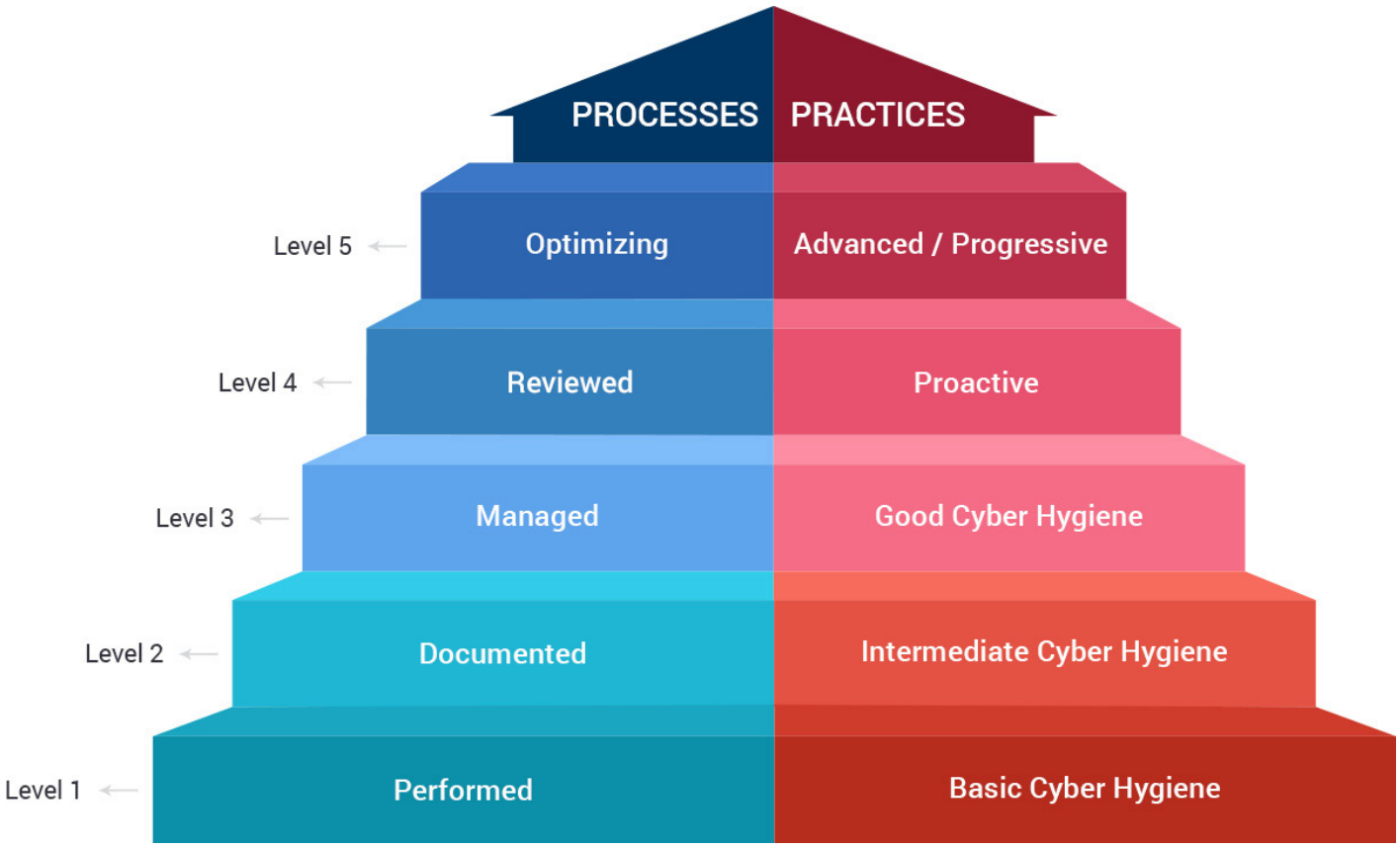


Fig. 2. *the Five Practice and Process Levels of the Model*

For an organization to achieve a certification level, they will need to be audited by a CMMC Third-Party Assessment Organization (C3PAO). These organizations are trained and authorized to conduct audits by the CMMC Accreditation Body (CAB).

Upon completing an audit, the C3PAO will make their recommendation to the CAB as to what CMMC level a company should be certified to. The CAB subsequently makes the certification available to the DoD so that contracting officers can confirm the certification level.

As of this publishing, the provisional program is underway using a group of CAB selected provisional C3PAOs, to help shepherd a series of pathfinder solicitations through this process. This will be followed with the rollout of the CMMC in an orderly manner until all DIB contractors and subcontractors are covered by the target date of January 2026. To get to this point, several technical exercises including penetration testing or unannounced red teaming may be required for the higher CMMC maturity levels, however, this will not affect most companies.

With this overview of CMMC out of the way, we can now explore some of the practical implementation and sustainment components of the CMMC, including a few meaningful insights that can help clarify how these may apply to your organization. To do so, we will use the CMMC Maturity Level-3 as a baseline example for the remainder of the discussion.

The Technical Components

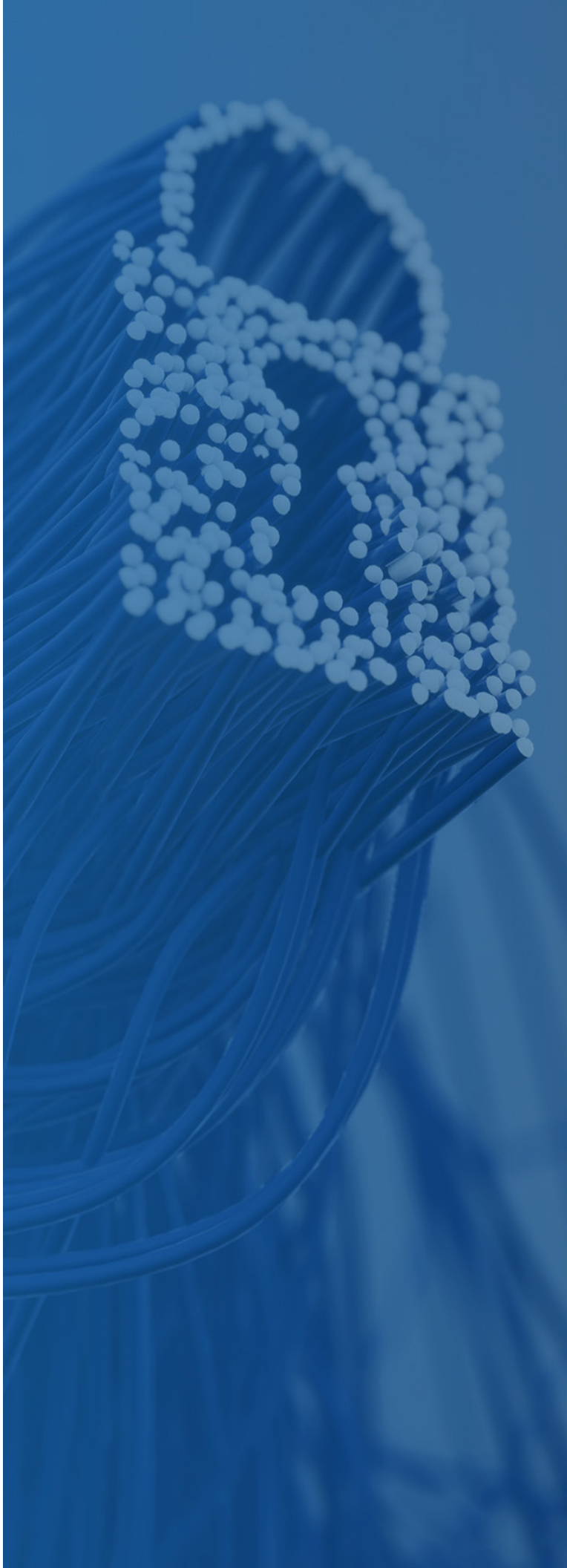
When one steps back and examines the CMMC, it becomes apparent that it has two main components; a technical component and a cybersecurity program component, both of which are essential toward addressing the CMMC requirements.

Historically, most small to midsize DIB contractors have focused primarily on technical controls (now referred to as practices in CMMC) necessary to meet FAR and DFARS requirements. Among these include:

- Access management.
- Having firewalls in place.
- Monitoring incoming and outgoing traffic.
- Monitoring internal traffic.
- Managing ports and protocol.
- Using Multi-Factor Authentication (MFA).
- Auditing system and user behavior.

It was assumed that if sufficient technical controls coupled with a few administrative ones like approving access to facilities and system accounts were in place, the environment would be considered protected and the DoD's requirements satisfied. In general, this was the case before NIST 800-171 and CMMC arrived on scene in 2017 and 2019 respectively.

Since then, the CMMC has introduced an additional 20 controls at Maturity Level-3, which are beyond the 110 required in NIST 800-171. Satisfying these additional technical controls can prove to be a heavy lift for many organizations and would require a degree of expertise not commonly found within the typical DiB contractor environment.



Cybersecurity Program Component

While both NIST 800-171 and CMMC require a significant amount of documentation such as policy letters and evidence to prove that controls are implemented, CMMC requires much more than its predecessor. So much so, that it has evolved to the level of a genuine cybersecurity program. These revisions can be viewed as subcomponents or pillars of a CMMC-focused cybersecurity program, as implicitly designed in within CMMC Level-3.

These subcomponents include:

- Practices that are implemented, documented and managed.
- Process that are developed, documented and managed.
- Developing an implementation plan for each domain.
- Developing Domain level policies for all practices in each domain.
- Program components must be institutionalized, socialized and repeatable.
- Program components must be managed, reviewed for changes and updated.

So, with introducing Maturity levels, the DoD has clearly signaled that it wants DIB contractors to not only put controls in place, but provide resources to manage and ensure they are sustained in an ongoing manner, much like the DoD does with its own networks and environments. Fortunately for DoD, it has an abundance of resources to meet the rigors and complexity of CMMC-like requirements whereas a large, less fortunate segment of the 300 plus DIB contractors who are now straddled with the pain of complying with the CMMC's stringent requirements. Some contractors view the additional 20 controls levied with CMMC as

additional expenses in the form of hardware, applications, appliances and upgrades. This is a fair assumption, but these variables could change, pending the results of the required gap assessment. In many cases, an assessment will identify a series of compensating controls that might reduce the need or cost to implement more costly single controls. Regardless of your current organization's CMMC posture, the rigor and "long-poles" under DoD's CMMC tent can be daunting for many DIB contractors without the expertise and resources of larger enterprises.

Another problem area I have identified is that oftentimes, companies overlook the technical expertise required to select, install and configure the right solution to meet a particular control. Here again and in extremely rare circumstances, the right engineer can often find a solution that will meet several controls, resulting in savings. Other elements that are sometimes overlooked involve cost avoidance and total cost of ownership. A lower skilled, less experienced IT asset can sometimes make costly errors in trying to engineer and implement solutions or services. This oftentimes negatively impacts production systems and operations causing shutdowns which ultimately leads to non-compliance. Additionally, total cost of ownership can sometimes be an unknown, but should be calculated to the extent possible across the enterprise. Many- if not the majority- of these costs can potentially be reduced by shared services such as those provided by MSSPs.

However, the CMMC's bigger surprise is manifested in the programmatic component of the CMMC requirements. Cybersecurity program management introduces a functional area and expertise requirement that is foreign to most small to mid-sized DIB contractors, which presents a very long pole to implement and sustain. Having listed the relevant subcomponents, now is a good point to dive further into that point of the discussion.

As previously mentioned, the CMMC requires that an implementation plan be developed and sustained for each of the 17 domains. We can use this as a programmatic example to examine in further detail. It specifies that several elements must be included in the plan in order to meet the CMMC maturity level-3 requirements. One element is how the plan will be resourced which entails identifying who is responsible for what, what methods and tools will be used, what level of training and certification is required of the individuals/positions involved, how the

plan is funded, and a number of other similar programmatic requirements. One quickly realizes the potential rigor and complexity involved with this component alongside the required resources to complete them. Such a comprehensive, congruent and technical program requires skill sets and experience outside of those found in many contractor firms, let along DIB SMBs. These elements cannot normally be developed, implemented or sustained by say, a system administrator or IT managers. Cybersecurity program development and sustainment most often requires an advanced resource with a cross-section of skills and knowledge that comes with at least ten years of experience within the regulatory compliance space. These areas include:

- Management skills.
- Collaboration and communication skills.
- Information Security Management and Classification.
- Cybersecurity.
- System security and configuration requirements.
- An understanding and experience with DoD audit language helps.

The time and effort necessary to build a mature program and remediate findings identified during a gap assessment can be lengthy and grueling, especially if an organization is lacking internal CMMC audit expertise. Even with an experienced support resource available, one can anticipate long hours and lots of communication with various elements of the firm to ensure facts, consistency as well as congruence are maintained and aligned. It will require at a minimum, one-two individuals dedicated full-time for several months to make reasonable progress. My observation and involvement with assisting government agencies and DIB contractors with NIST 800-53, NIST 800-171, and now CMMC requirements, is that it takes on average 12-18 months to fully prepare for a successful audit after a comprehensive gap assessment is conducted.

Another common pitfall in the development phase often includes competing interests, personalities, and all too often, incorrectly interpreting the language of the CMMC requirements. Although having experience with other types of audits can help and at some level overlap may overlap with the CMMC, it is highly encouraged to seek assistance if passing an audit determines what contracts are available to the DIB contractor- including the option years which CCMC can be applied to at the discretion of DoD. After all, CMMC audits are pass or fail, with very little consideration given for time to remediate findings.

The intent and expectation of the DoD is that the contractor will be fully prepared to pass an audit the first time. Beyond this, a contractor that fails an audit will need to schedule a second audit which could conflict with the timelines of contract deadlines. How soon a second audit can be scheduled will depend on a variety of factors including the number of audits already in the pipeline, with the second audit moving to last in line.

With so many moving parts and the potential impact of not passing an audit at risk, companies should consider the services of a vCISO to ensure a successful, first time outcome. These are seasoned professionals who can help develop and sustain a professional, mature security program and are readily available and prepared to undergo the rigors of an audit with confidence. As with any successful project, the first steps of attaining and sustaining CMMC compliance starts with the development of a strategy to build the security program, then formalizing it with relevant security documentation and processes, followed by implementation and enforcement, and lastly, managing the processes to make the process repeatable to ensure the program and practices are institutionalized. Partnering with a vCISO during this process not only helps reduce the risk of failing an audit but also losing out on DoD contract opportunities and revenue that are essentially critical to the DIB contractor.

Gauging Your Current CMMC Compliance Posture

So, for the organization that has kept up with cybersecurity best practices but not with every aspect of the CMMC requirements, one might ask, is there a degree of flexibility for any unaddressed gaps with these compliance requirements? For the sake of clarification, let's assume, they've had a third-party gap assessment, identified gaps, had internal IT staff address the areas that they can, and dusted off the HR or any other company polices they have and updated them- will that sufficiently prepare for a CMMC Maturity Level-3 audit? Unfortunately, the answer is no. While it has likely made your environment more secure, it will not meet the rigors of CMMC requirements.

In the instance where an organization has already passed the CMMC Maturity Level-3 certification, what would be next? First, relax and get some rest, you deserve it! Second, recognize that is important to maintain the security and compliance posture that you achieved. The long-term sustainment of your compliance program is a requirement under the CMMC, and that CMMC certification is valid for three years, after which, a new CMMC audit is required to renew the certification. Varying too far off path between audits can make it challenging and costly to regain audit-readiness. It is important to have a dedicated resource who can continuously manage program-sustainment, ensure continued implementation and enforcement in accordance with the program, as well as keep the contractor's leadership current on the security and compliance posture of the company. There are many moving parts involved with long term programmatic success that include but are not limited to ensuring that the technical controls and configurations are within compliance and the coordination between management and the MSP/MSSPs is consistent, documented and clear. These tasks are typically performed by a CISO, or more often is the case will small and midsize businesses, a vCISO.

Additional CMMC Challenges to Recognize & Selecting a Strategic Partner

During my engagements with companies that are new to the CMMC requirements, I have learned to initiate an early discussion focused on envisioning a new paradigm, asking them to momentarily dismiss any old paradigms they may have surrounding compliance.

This generally helps to open minds and presents a blank canvas with which we can discuss CMMC. Once the complexity, newness and rigor required for CMMC ML-3 certification and sustainment are recognized, it can be overwhelming for many small and midsize companies, which leaves them with four possible courses of actions.

- Use the old paradigm and hope for the best.
- Hire a CISO and more experienced IT security support.
- Utilize the shared services and expertise of an MSSP.
- Employ a hybrid approach using a combination of the above options.

While internal resources are a known and valuable commodity, it is important that the appropriate due diligence is taken if a decision is taken to leverage outsourced, external support. Specifically, regarding the CMMC, there are several meaningful questions that should be answered by MSSPs or vCISOs prior to selection.

- Do they have audit experience with the FAR, DFARS, NIST and CMMC?
- Do they have experience in developing cybersecurity programs?
- Do they have technical experience implementing NIST/CMMC controls?
- Do they have the capability to monitor & audit my network resources?
- What technical certification do they have: CISSP, Network +, CEH etc.?
- Can they develop a complete road map to compliance with CMMC?
- Are thy CMMC compliant?
- Will they be onsite during the audits to answer questions on your behalf?

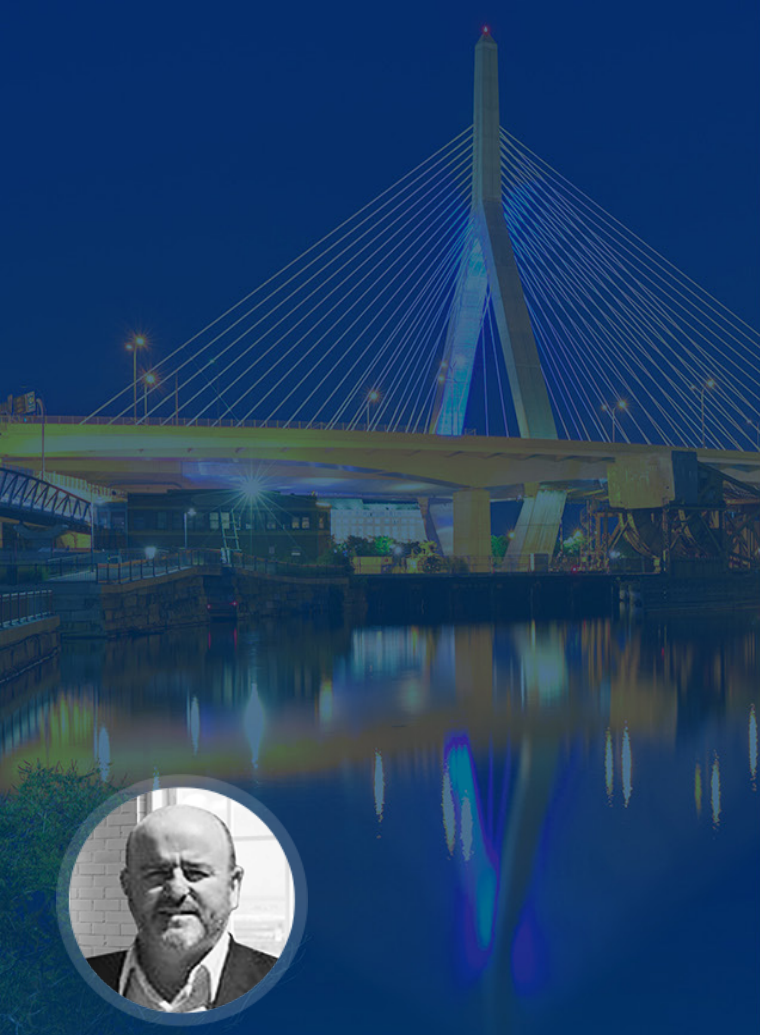
Overall, the DoD wants contractors to have comprehensive programs that manage and drive the controls and processes used to remove or reduce risks by using DIB contractor defined practices to address the CMMC defined capabilities designed to protect CUI.

Concluding Thoughts & Your Next Steps

There is no question that accomplishing your CMMC compliance requirements can be both a daunting and extensive undertaking that can challenge any SMB's capabilities. The purpose of this white paper is to clarify the scope of the CMMC, so these challenges can be adequately addressed and help ensure your ability to attain and maintain CMMC certification.

Although the technical and programmatic aspects of the CMMC consist of the majority of the requirements, it's of equal importance to approach your compliance strategy with an open mind, abandoning the paradigms of the past. Today's cybersecurity landscape consists of hostile and capable threat actors. DIB contractors must quickly adapt to combat these evolving threats.

Whether your motivations stem from a desire to be a better steward of CUI or to maintain your ability to secure DoD contracts, it's of the utmost importance to recognize the potential impact non-compliance may have on your organization and most importantly, the strength of our nation's defenses.



JOHN BERMINGHAM, CISSP

Director of Compliance & Cybersecurity

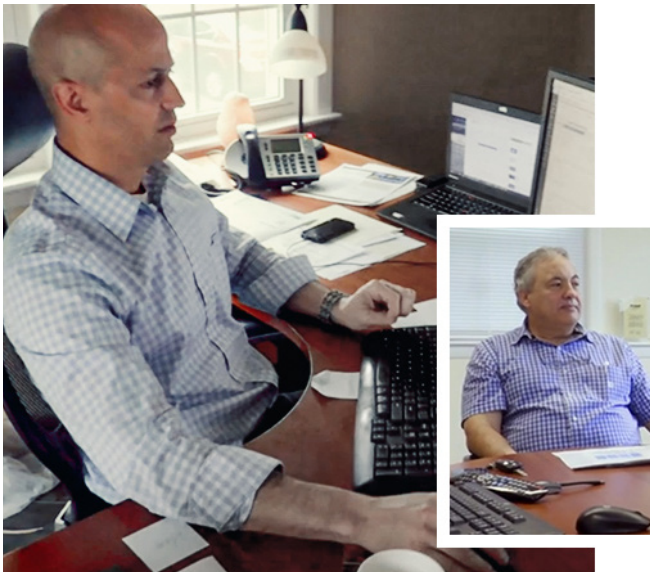
John Bermingham joined the team in 2020 as TSI's resident cybersecurity and compliance expert. Throughout his twenty-five years in the IT and cybersecurity industry as a US Airman and later on as a contractor, John has worked with a wide variety of government agencies and companies to include ACS Defense Inc., Lockheed Martin Corp., Northrop Grumman Corp., and several Federally Funded Research and Development Centers (FFRDCs).

John looks forward to sharing his rich experience and expertise with TSI's clients to help address their compliance requirements, improve their security postures and ensure they have the tools and resources to address today's volatile cybersecurity landscape. John is also registered by the CMMC Accreditation Board as a CMMC Registered Practitioner: https://www.cmmcab.org/registered-practitioners

Outside of work, John enjoys attending church with his family, going on long walks, and taking trips. He also likes to read non-fiction, playing racquetball or ping pong, and keeping up with international soccer.

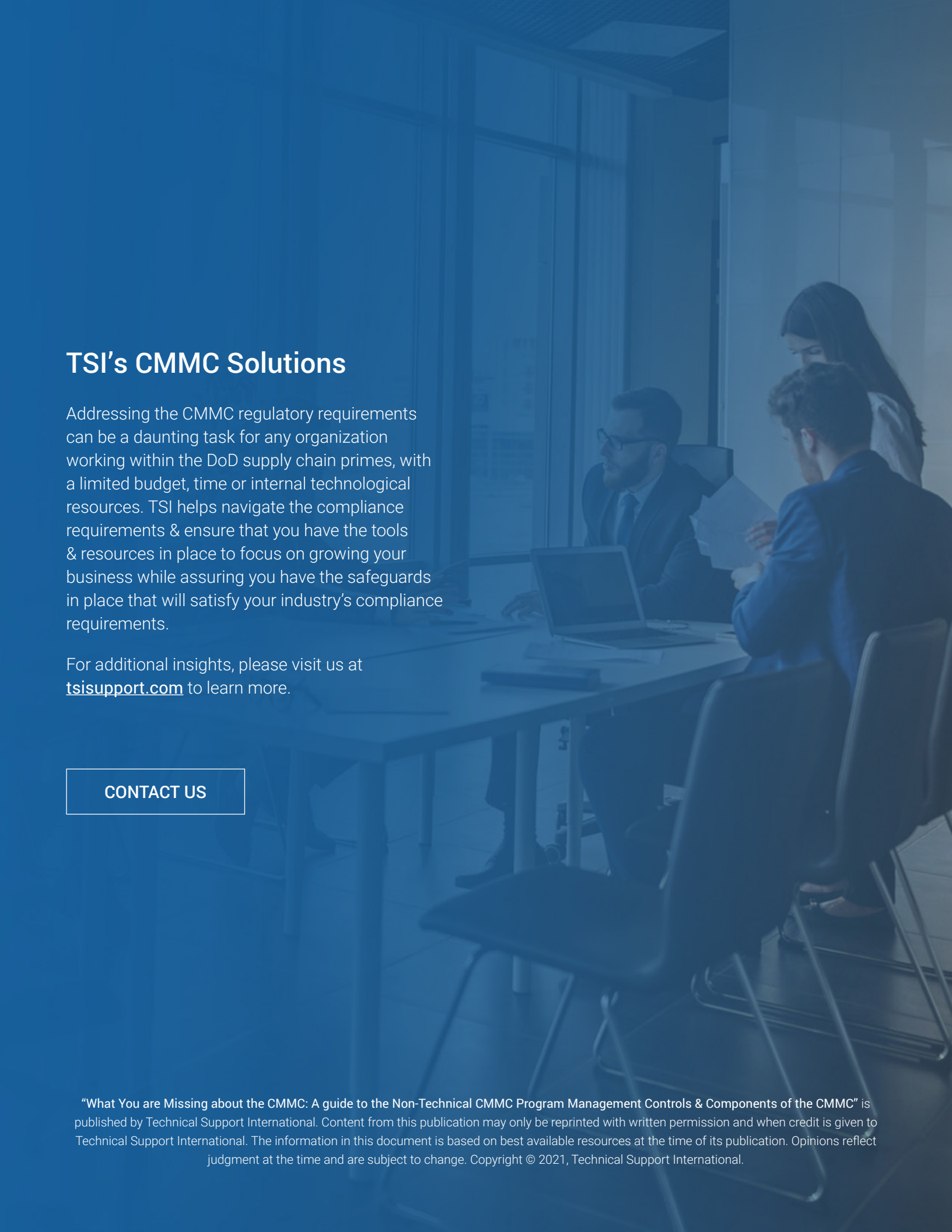
About TSI

Since 1989, Technical Support International (TSI) has been a leading Managed Services (MSP) and Managed Security Services Provider (MSSP), proudly serving the IT support needs of SMBs and DIB contractors.



Addressing the CMMC regulatory requirements can be a daunting task for any organization but TSI helps navigate these compliance requirements to ensure that you have the tools and resources to focus on growing your business alongside the assurance that the appropriate safeguards in place that will satisfy your industry's compliance requirements.

To learn more, please visit our site or feel free to reach out to us directly at sales@tsisupport.com



TSI's CMMC Solutions

Addressing the CMMC regulatory requirements can be a daunting task for any organization working within the DoD supply chain primes, with a limited budget, time or internal technological resources. TSI helps navigate the compliance requirements & ensure that you have the tools & resources in place to focus on growing your business while assuring you have the safeguards in place that will satisfy your industry's compliance requirements.

For additional insights, please visit us at tsisupport.com to learn more.

CONTACT US