PREPARING FOR A CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)

BDO

Organizations planning to conduct business with The U.S. Department of Defense (DoD) will be required to achieve a Cybersecurity Maturity Model Certification (CMMC) prior to receiving contract awards, or else risk forfeiture of those opportunities. Is your organization prepared to become certified?

This insight will not only provide a point-in-time summary overview of the CMMC model framework and certification process, with a projected overall timeline and approach for roll-out of the program, but also provides examples of potential impacts and challenges organizations seeking certification may face with actions to consider taking now to prepare for successfully achieving a CMMC certification.

INTRODUCTION

The much-anticipated CMMC model framework (version 1.0) was released by DoD on January 30, 2020, providing a foundational set of standards from which all organizations wishing to conduct business with DoD must achieve a CMMC certification. It should be noted that all organizations–whether prime contractors or subcontractors – will be required to comply, and each organization will also be responsible for flowing down CMMC requirements to their subcontractors (i.e., down the supply chain), who are providing services in support of prime DoD contracts.

DoD plans to begin including CMMC requirements within select Requests for Information (RFIs) and corresponding Requests for Proposals (RFPs) as soon as June and September of 2020, respectively. Considering the existing Defense Industrial Base (DIB) consists of approximately 300,000 organizations providing services to DoD, the impacts of these requirements will be far-reaching and felt by all stakeholders of these organizations – both internal and external – as they scramble to position themselves for achieving CMMC certifications once requirements go into effect.

BACKGROUND

The CMMC model framework was developed with the intention of building upon – rather than replacing – existing guidance and standards for safeguarding information systems and data, such as DFARS 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting" and NIST SP 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations."

The framework incorporates a risk-based approach to cybersecurity compliance by introducing the concept of maturity, where organizations seeking certification can become certified under a specific maturity level ranging from one (basic) to five (advanced). The maturity level an organization certifies under will be reflective of their cybersecurity capabilities in terms of being able to protect data they're handling in performance of DoD contracts – specifically Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) – and will be commensurate with the level of cybersecurity risk associated with the scope of work under a particular contract award.

Generally speaking, the framework consists of various cybersecurity practices and maturity processes, primarily based on existing cybersecurity standards and guidance, which are organized across 17 domains, with each practice and process mapping to one of five maturity levels. The following table provides a summarized breakout of practices and processes by CMMC maturity level (see Table 1).

TABLE 1

CMMC MODEL FRAMEWORK (VERSION 1.02) - SUMMARY BREAKDOWN BY MATURITY LEVEL

CMMC Maturity Level					
	1	**2**	**3**	**4**	**5**
Objective	Safeguarding of FCI	Transitioning towards protection of CUI	Protection of CUI	Protect CUI against APTs[1] w/ partial adoption of advanced cybersecurity practices	Protect CUI against APTs[1] w/ full adoption of advanced cybersecurity practices
Practices					
Description of Practice Capabilities	Basic (minimum) cybersecurity hygiene	Intermediate (improving cybersecurity hygiene	Good cybersecurity hygiene	Proactive; enhanced detection and response capabilities	Advanced; layered cyber controls and overall sophistication
Number of Practices (by Maturity Level)	17	55	58	26	15
Cumulative Practices[2] (for Certification)	**17**	**72**	**130**	**156**	**171**
Processes					
Description of Process Maturity	Ad-hoc; processes performed but not documented	Repeatable; performed / supported by documentation	Managed; plan established and effectively executed	Reviewed; continuous monitoring / measurement	Optimized; continuous improvement
Number of Processes (by Maturity Level)	0	2	1	1	1
Cumulative Processes[2] (for Certification)	**0**	**2**	**3**	**4**	**5**

1 APT = Advanced Persistent Threat; for definition see National Institute of Standards and Technology's website: https://csrc.nist.gov/glossary/term/advanced-persistent-threat

2 Cumulative totals represent overall required number of practices and processes necessary for achieving certification for a certain maturity level (including all lower maturity levels up to a target certification level); for detailed listing of CMMC practices and processes see website: https://www.acq.osd.mil/cmmc

Perhaps most importantly, it should be noted that the CMMC certification process will include a verification step involving an accredited and independent Certified 3rd Party Assessment Organization (C3PAO), which must be engaged by organizations seeking certifications after determining the appropriate level of certification they must achieve. The independent verification requirement may be one of the more significant wrinkles of the program that organizations serving DoD must be aware of, when considering they were permitted to self-assess their cybersecurity capabilities against NIST SP 800-171 security requirements under the prior regime.

Organizations seeking certification should anticipate C3PAOs performing independent testing procedures during their engagements, which may vary in effort and complexity depending upon desired CMMC maturity level and must be prepared to provide adequate documented evidence to support verifications. Certification will not be possible without involvement of a C3PAO, and self-assessments will not be considered where CMMC requirements are included in solicitations.

WHAT'S NEXT FOR THE CMMC PROGRAM?

While release of the CMMC model framework provides a solid foundation for the overall program, additional activities are underway to continue the roll-out. Separate but related to the framework's release, the CMMC Accreditation Body (CMMC-AB) was formed in January 2020, and in March 2020 signed a Memorandum of Understanding (MOU) with DoD clarifying their responsibilities around oversight of the program's implementation and ongoing program management activities. With the overall goal of including CMMC requirements for all DoD contract awards by the year 2025, DoD and CMMC-AB will continue to coordinate efforts towards rolling out the program by conducting the following activities throughout 2020:

- Establishment of C3PAO accreditation qualification requirements and deployment of CMMC Marketplace portal (within CMMC-AB website) for individuals and organizations wishing to participate
- Training and accreditation for individuals and organizations wishing to participate in the CMMC program to provide certification services, to receive accreditation status
- Inclusion of CMMC requirements within RFI solicitations for a subset of DoD contract awards
- Inclusion of CMMC requirements within RFP solicitations for a subset of DoD contract awards

DoD and CMMC-AB are committed to ensuring that a group of accredited C3PAOs will be ready and available by the time CMMC requirements begin showing up in DoD solicitations. DoD further stated that organizations wishing to pursue future business opportunities with DoD will have the option of proactively engaging available C3PAOs to become certified when they are ready.

In other words, organizations may want to consider becoming certified sooner to avoid risk of preclusion from bidding of future opportunities, as the CMMC requirement will be used as a discriminator in the down-select process for future DoD awards – organizations already meeting CMMC certification prerequisites in advance of DoD solicitations will most likely have an advantage over other bidders that do not. It should be also noted that CMMC certifications will be accepted across all DoD agencies, and will remain active for three years from the certification date.

POTENTIAL IMPACTS AND CHALLENGES

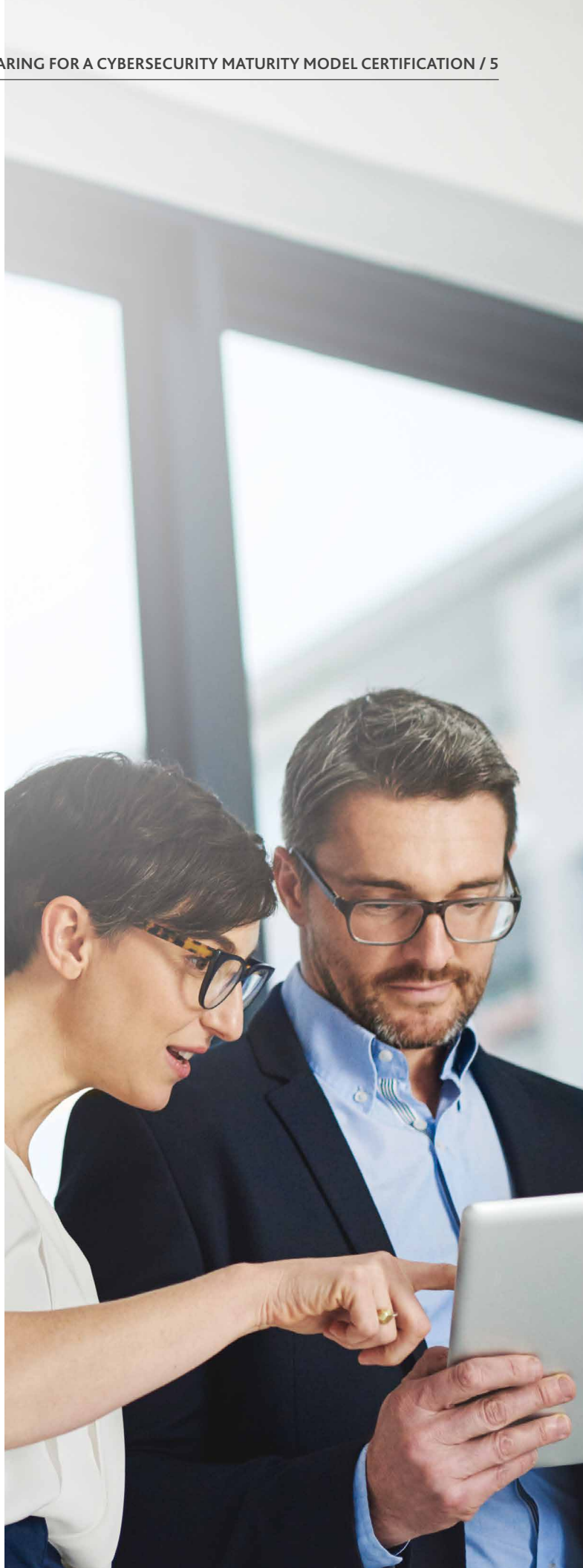
The CMMC model framework is building upon existing guidance and standards, such as DFARS 252.204-7012 and NIST SP 800-171. For those organizations who are already compliant with existing guidance and standards, and have invested time and effort necessary towards planning, designing, implementing, and documenting adequate cybersecurity controls and processes, there may be only minor impacts encountered during the CMMC certification process.

However, for organizations that have not put forth similar efforts and/or are unprepared – perhaps due to lack of awareness, resources, or a myriad of reasons – there could be numerous challenges awaiting them as they go through the process of becoming certified. Some common areas where pitfalls may exist are provided below, and – if challenges are encountered within these areas – there could be adverse downstream impacts on an organization's ability to adequately implement cybersecurity controls and processes, as well as meet overall CMMC certification goals:

CMMC Common Challenges

- Identification and Marking of FCI and CUI Data
- Determination of Scope and Applicability (of CMMC requirements)
- Supply Chain Management (SCM)
- Cybersecurity Control and Process Documentation
- Cybersecurity Training and Awareness
- Cybersecurity Governance and Oversight

Organizations need to be able to identify where they lack visibility and/or have deficiencies within their cybersecurity program, in order to proactively address those challenges in advance of seeking CMMC certification. Unfortunately, however, many organizations simply don't have visibility into what and where those deficiencies lie, because they haven't invested the necessary time and effort to assess their existing cybersecurity capabilities.



HOW ORGANIZATIONS CAN PREPARE

Organizations must be prepared to embrace cybersecurity within all aspects of their business operations, moving away from the traditional view of treating cybersecurity as a compliance-driven, "check-the-box" effort that only needs to be addressed periodically just to pass regulatory scrutiny. As technology continues to evolve, new threats will arise, new vulnerabilities will be exposed, and cybersecurity practices – consisting of any combination of people, processes, and technology – must evolve accordingly to manage cybersecurity-related risks.

Organizations that follow continuous, risk-based approaches towards implementing cybersecurity practices across their enterprises should be better positioned to achieve CMMC certifications at higher maturity levels. Taking those points into consideration, organizations seeking certification should consider taking preparatory actions in advance of pursuing a certification, including but not limited to:

Establishing a Cybersecurity Program

By taking a programmatic approach towards implementing cybersecurity controls and processes, organizations will increase the likelihood of achieving their cybersecurity goals and objectives, which may include but not be limited to a CMMC certification. The following diagram provides an example of a programmatic approach an organization may take towards achieving a CMMC certification (see Figure 1). Note that the diagram reflects an overall continuous approach which involves planning, readiness assessment, remediation, certification, and ongoing management and monitoring of cybersecurity controls and processes.

Formalizing Cybersecurity Practices

During the certification process, as mentioned above, organizations must be prepared to provide documented evidence. Cybersecurity practices should primarily be based on documented policies, procedures, and plans to help ensure effectiveness and consistency. In addition, all cybersecurity practices should be designed and operated in a manner that allows for appropriate testing procedures to be applied as requested by C3PAOs. Examples of documented evidence includes formal policies, procedures, and plans from which cybersecurity practices will be based. Most importantly, however, organizations must understand that their cybersecurity practices must be verifiable. In other words – from an auditor's perspective – cybersecurity practices should be designed and implemented in a way that allows for appropriate testing procedures to be applied in order to verify the operating effectiveness of certain cybersecurity controls and processes, in accordance with the practices and processes contained within the CMMC model framework.

Proactively Engaging C3PAOs and other Third Parties

Organizations wishing to conduct business with DoD in the future should avoid waiting to prepare for achieving a CMMC until these requirements show up on RFI or RFP solicitations for specific DoD business opportunities they are interested in pursuing, as there may not be enough time for them to engage a C3PAO and achieve a CMMC certification before time of contract award. In those cases, the potential contractor risks preclusion from bidding on or accepting contract awards. To avoid these scenarios, organizations should consider proactively achieving a certification at a maturity level that seems most appropriate, based on the types of services they provide to the DoD or prime contractors (as subcontractors) in support of DoD contract work, carefully considering if and how they will process, store, access, or transmit FCI and CUI in performance of those contracts.

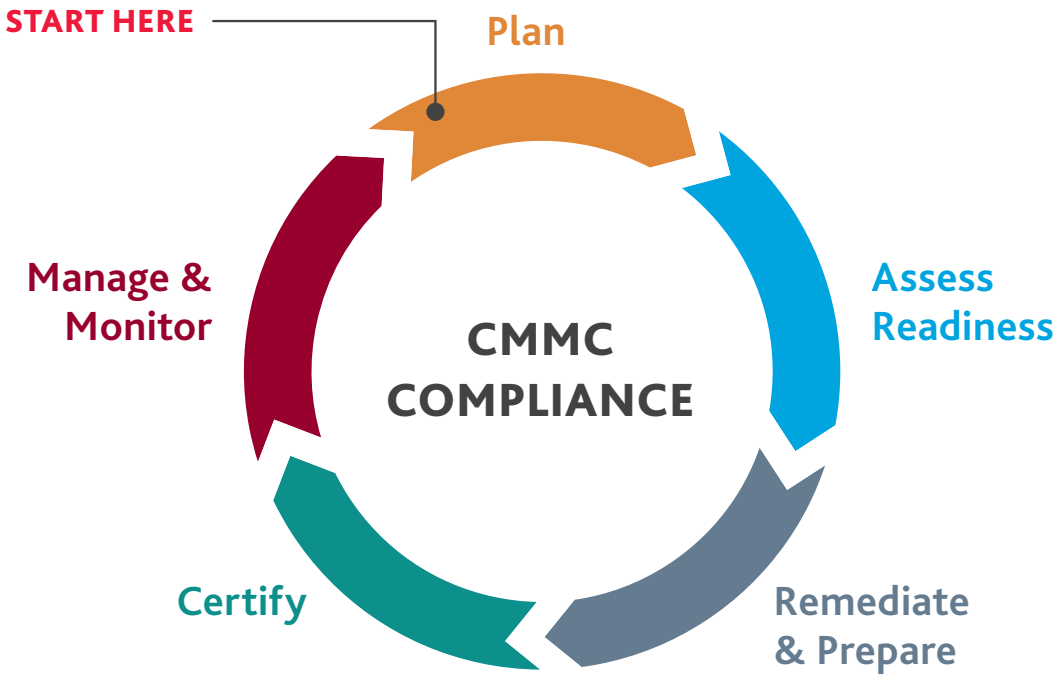
Monitoring Regulatory Developments

All organizations considering a CMMC certification should regularly monitor CMMC program developments and updates, and may do so by visiting the DoD Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD[A&S]) CMMC website (www.acq.osd.mil/cmmc) or the CMMC-AB website (www.cmmcab.org), where they will be able to subscribe to receive alerts and updates. Moving forward, those organizations should also remember to regularly monitor standards and guidance from which the CMMC model framework is based, as these are managed independently of DoD and CMMC-AB, and often undergo further revisions and updates. Those organizations must understand that after they've achieved a certification, while they may hold an active CMMC certification for a period of time, the standards and guidance under which they've been certified may no longer be current and they may still need to comply with other regulatory requirements following more current standards and guidance.

FIGURE 1

ILLUSTRATION OF A CMMC COMPLIANCE PROGRAM

This is an example of a program an organization could follow to achieve a CMMC.



HOW BDO CAN HELP

Organizations should consider engaging BDO to support their CMMC readiness preparation efforts. Using the diagram provided in Figure 1, for example, trusted third party service providers and/or C3PAOs can add value by supporting in several ways throughout the lifecycle of your program – based on your specific needs. The following are examples of types of services or engagements where BDO may be able to assist:

- Readiness Gap Assessments
- Remediation Planning and Support Services
- Implementation and Audit Support Services

It should be noted that as of the time of this article, there are no accredited C3PAOs available, as the CMMC-AB is still in the process of defining accreditation requirements and developing a training program.

Organizations may, however, find value in contacting a Registered Provider Organization (RPO) like BDO, to begin planning and preparing for future assessment engagements. RPOs could offer extremely valuable insight if conducting a readiness assessment for an organization seeking certification.

CONTACT

Craig Christie
Regional IS Assurance and Third Party Attestation Partner
Atlantic Region
215-241-8969 / cchristie@bdo.com

Michael Wright
Managing Director, Third Party Attestation - Government Contracts
410-423-4575 / mwright@bdo.com