Cybersecurity Maturity Model Certification (CMMC)

The Road to Compliance

Tuesday, February 02, 2021

PREPARED FOR:

Cyber Security and Information Systems IAC (CSIAC) User Community

PREPARED BY:

CSIAC Cyber Security & Information Systems Information Analysis Center

Operated by Quanterion Solutions Incorporated

266 Genesee Street
Utica, NY 13502

https://www.quanterion.com
qinfo@quanterion.com

CSIAC is sponsored by the Defense Technical Information Center (DTIC) under Contract #FA8075-17-D-0001. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the DTIC.

Table of Contents

This document is only intended to provide a summary overview of the upcoming changes. Here are some additional resources for further reference:

> The Office of the Under Secretary of Defense for Acquisition and Sustainment's (OUSD(A&S)) CMMC website publishes guidance, releases updates and answers to Frequently Asked Questions (FAQ). https://www.acq.osd.mil/cmmc/
>
> The CMMC Accreditation Board (AB) offers additional insights into the preparation and assessment process. https://www.cmmcab.org/

Organizations seeking certification but requiring some additional support may wish to consult one or more of CMMC-accredited services such as a Registered Provider Organization (RPO), or Licensed Instructors.

The CMMC AB will identify credentialed providers for training and preparation, similar to the C3PAOs. The approval process is still being refined and implemented, but those accepted into the program are anticipated to be approved in the coming months. These and other resources can be explored further using the links above.

Introduction

In response to the repeated attacks on the industrial supply chain, the Department of Defense (DoD) has taken proactive measures to ensure that critical DoD suppliers are adequately protecting Controlled Unclassified Information (CUI) resident on supplier/contractor information systems. Such requirements initially date back to 2013, at which time the Defense Federal Acquisition Regulation Supplement (DFARS) final rule (78 FR 69273)[1] was released. Over time, the requirements have been updated to better suit the Defense Industrial Base (DIB) as well as to address shortcomings of previous frameworks. One example includes the 2015 release of DFARS clause 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting," which has since been updated as recently as 2019. After acknowledging that these requirements were insufficient, DoD announced the planned migration to the Cybersecurity Maturity Model Certification (CMMC), which introduces a more stringent and independently validated approach to assessing the security of DIB suppliers and contractors. The most recent development, however, is a phased implementation timeline under which CMMC will be implemented. At the time of this report's release, CMMC's implementation is on the horizon, but has not officially been put in place. There are, however, requirements to be met by all DoD contractors.

Compliance Roadmap

As cyberspace grows increasingly contested, DoD has acknowledged that the supply chain is a prime target for Advanced Persistent Threats (APTs), offering a unique asymmetric opportunity to steal the nation's secrets and proprietary technology. Efforts to counter such attacks have evolved over time, initially involving a subset of requirements from the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 (since updated to Rev. 5), "Security and Privacy Controls for Information Systems and Organizations." The 2015 DFARS interim rule (80 FR 81472) later directed the DoD's transition from NIST SP 800-53 to NIST 800-171 (recently updated to Rev.2), "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations." The cybersecurity implementations prescribed in NIST SP 800-171 were primarily considered to be sufficient, but one of the critical shortfalls involved the framework's self-inspection and oversight for DIB contractors. The omission of a means for DoD to verify a contractor's implementation of the NIST SP 800-171 security controls ultimately led to a situation where many had not met these requirements, as reported in contractor surveys and a DoD Inspector General Report.[2]

The introduction of CMMC specifically attempts to address these shortcomings, building upon the NIST SP 800-171 framework and additionally providing the DoD with a means to verify a contractor's implementation of the security requirements. The final details of the CMMC Model (version 1.02) were published in March of 2020, though many had begun preparations for a Summer/Fall 2020 requirement based on earlier announcements and draft publications. However, there are certain requirements and considerations that led to an alternate phased roll out, as announced in DFARS's Fall 2020 interim rule

[1] 78 FR 69273: https://www.govinfo.gov/app/details/FR-2013-11-18/2013-27313

[2] Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019–D041)

(DFARS Case 2019-D041). There are a few different components to break down from the DFARS interim rule and the cited DFARS clauses:

DFARS clause 252.204-7019: “Notice of NIST SP 800-171 DoD Assessment Requirements”

- Consistent with NIST SP 800-171, all DIB contractors are required to complete a Basic (i.e., self) Assessment against the CUI security requirements. One key update from the interim rule involves the requirement to populate the results of the Basic Assessment in the Supplier Performance Risk System (SPRS).
    - While the elimination of self-assessments is a CMMC priority, they remain for the time being, albeit with renewed assessment guidance provided by NIST.3
    - Additional information regarding the SPRS is provided on the CMMC website.4
    - The interim rule, and thus the requirement to populate the Basic Assessment results into SPRS, took effect on November 30, 2020.
- Only Basic Assessments are required at this time. Medium and High Assessments, to be performed by the Government, will be phased in during the transition but performed on far fewer organizations due to resource limitations. The selection of contracts requiring higher-level assessments will be based on the sensitivity of the information involved in that activity.

DFARS clause 252.204-7020: “NIST SP 800-171 DoD Assessment Requirements”

- This clause further defines the activities performed in completing the Basic, Medium and High Assessments, and further requires DIB contractors to provide DoD access to its facilities, systems and personnel for the completion of the higher-level assessments.
- The NIST SP 800-171 Basic, Medium, and High Assessments will eventually be replaced by the CMMC Assessments, which will be performed by Certified 3rd Party Assessment Organizations (C3PAOs). CMMC’s roll out also involves the establishment of an Accreditation Board (CMMC-AB), a non-profit entity that will authorize C3PAOs as well as Provider Organizations and training professionals to assist DIB contractors.

DFARS clause 252.204-7021: “Cybersecurity Maturity Model Certification Requirements”

- Solicitations and contracts released on or after October 1, 2025 will require the inclusion of this DFARS clause, which requires that contractors possess a current CMMC Certificate (valid for three years) at the specified maturity level at the time of award and for the duration of the effort. Through September 30, 2025, the inclusion of the CMMC requirement in solicitations or contracts requires the approval of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)).

[3] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 DoD Assessment Methodology: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041). https://www.acq.osd.mil/cmmc/docs/Assessing-Contractor-Implementation-of-Cybersecurity-Requirements-one-pager_rd5.pdf

[4] The Use of the Supplier Performance Risk System (SPRS) in Implementing DFARS Case 2019-D041, Assessing Contractor Implementation of Cybersecurity Requirements. https://www.acq.osd.mil/cmmc/docs/FINAL-Supplier-Performance-Risk-System_Rd4.pdf

- (OUSD(A&S)) states that they are working to identify pilot programs under which they will employ the CMMC requirement during the FY21-FY25 phased rollout, providing target metrics for the number of programs to complete the pilot each fiscal year.[5]

The interim rule helps to provide clarification on the details of the phased roll out including applicable dates and milestones. At a minimum, contractors need to immediately complete a Basic Assessment against NIST SP 800-171 security requirements and upload the results to SPRS as soon as possible to remain eligible for DoD contract awards. Contractors should additionally begin working towards demonstrating compliance to the appropriate CMMC maturity level, especially with the anticipation of pilot programs including this requirement as early as FY21.

The following attempts to highlight the fundamental components of the CMMC framework, including its expansion on the requirements identified under NIST SP 800-171. Those that have not yet completed their Basic Assessment are encouraged to consult the references identified in the preceding paragraphs. Given the quantity of impacted organizations, numerous firms are attempting to capitalize on this business opportunity, mostly providing factual information but some spreading false claims regarding their ability to certify organizations. At the time of this document's release, no such organization has been formally approved by the CMMC-AB to perform these assessments. DIB contractors are encouraged to consult the official documents detailing the CMMC roll out and supporting websites to stay current on the latest developments.[6]

Model Overview

At first glance, the CMMC terminology can be confusing given the different technical requirements, required processes and maturity scoring. In simple terms, achieving a higher maturity level requires an organization to both (a) implement/perform additional security practices (i.e., technical and procedural security controls), while also (b) demonstrating the regularity, consistency and quality of the employed processes. This breakdown of the CMMC model is illustrated in Figure 1.

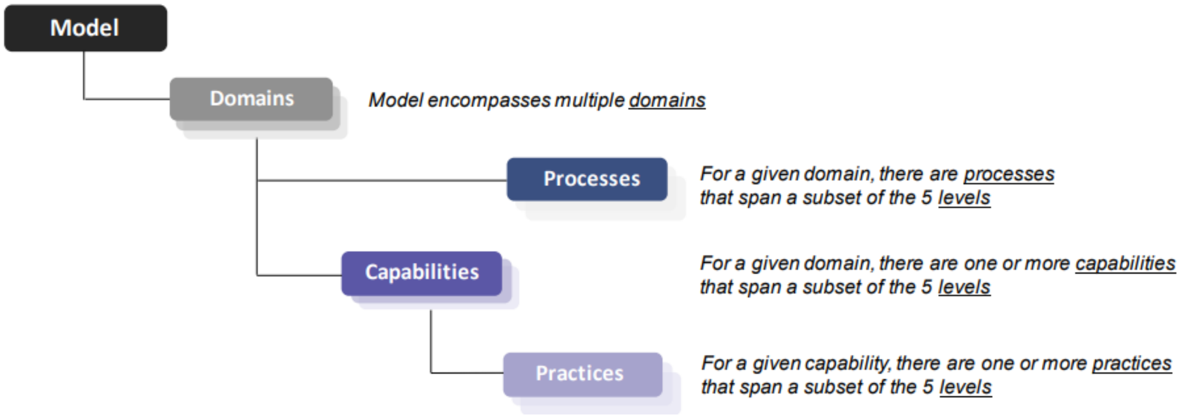
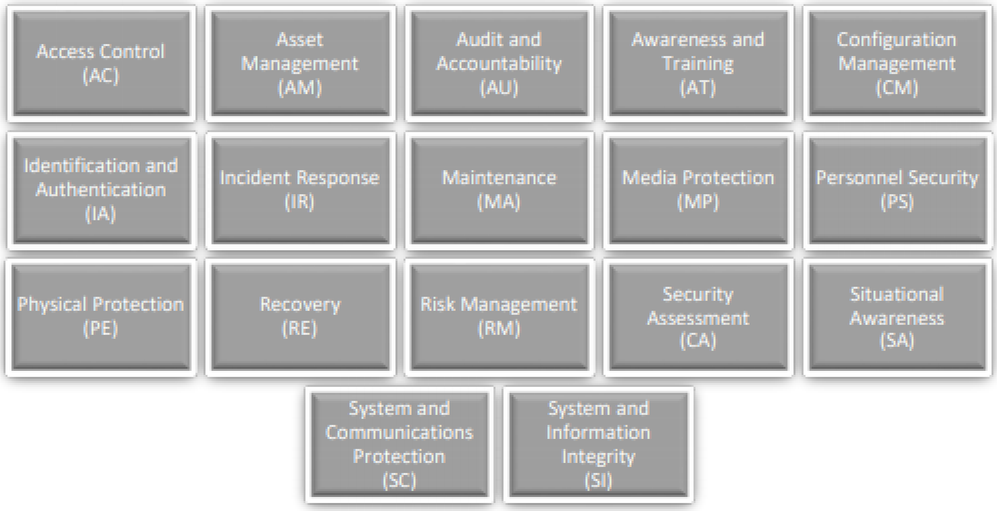

Model
Domains
Model encompasses multiple domains
Processes
For a given domain, there are processes that span a subset of the 5 levels
Capabilities
For a given domain, there are one or more capabilities that span a subset of the 5 levels
Practices
For a given capability, there are one or more practices that span a subset of the 5 levels

Figure 1: CMMC Model Description (Reference CMMC v1.02 p. 3)

[5] (OUSD(A&S)) CMMC Frequently Asked Questions (FAQ): https://www.acq.osd.mil/cmmc/faq.html
[6] OUSD(A&S) CMMC Website: https://www.acq.osd.mil/cmmc/index.html;
CMMC Accreditation Board: https://www.cmmcab.org/

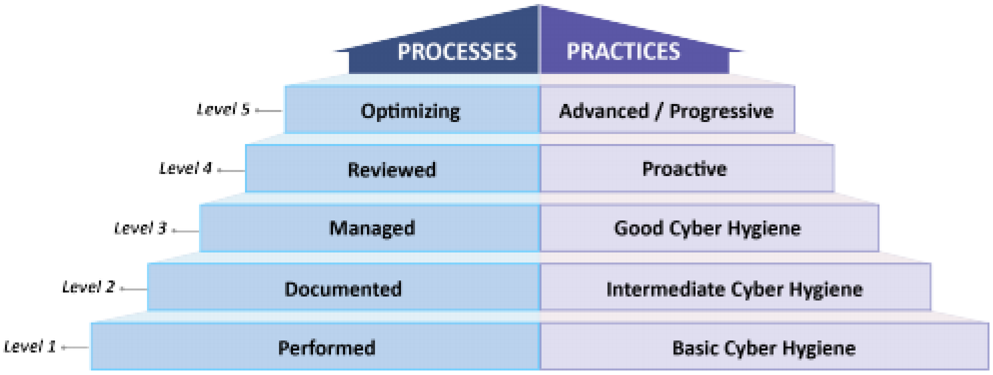
Following this hierarchical breakdown, the Model's "Domains" include a collection of cybersecurity objectives (e.g., Access Control, Configuration Management, etc.). Those familiar with the National Institute of Standards and Technology (NIST) Special Publication 800-171[7] requirements will easily recognize the CCMC model's 17 domains, which reflect a modest revision to the 14 control families identified in the NIST document.



Access Control (AC)
Asset Management (AM)
Audit and Accountability (AU)
Awareness and Training (AT)
Configuration Management (CM)
Identification and Authentication (IA)
Incident Response (IR)
Maintenance (MA)
Media Protection (MP)
Personnel Security (PS)
Physical Protection (PE)
Recovery (RE)
Risk Management (RM)
Security Assessment (CA)
Situational Awareness (SA)
System and Communications Protection (SC)
System and Information Integrity (SI)

Figure 2: CMMC Model Domains (Reference CMMC v1.02 p. 7)

Each of the 17 domains consists of processes and practices. The processes are mapped across the five maturity levels to reflect the extent to which security activities are institutionalized within the organization. The process descriptions, progressing from maturity levels 1 – 5, reflect an increasingly mature program, in the sense that the established processes are repeatable, consistently employed, effectively managed and able to resolve identified shortfalls. This process mapping is relatively straightforward and presented below in Figure 3.

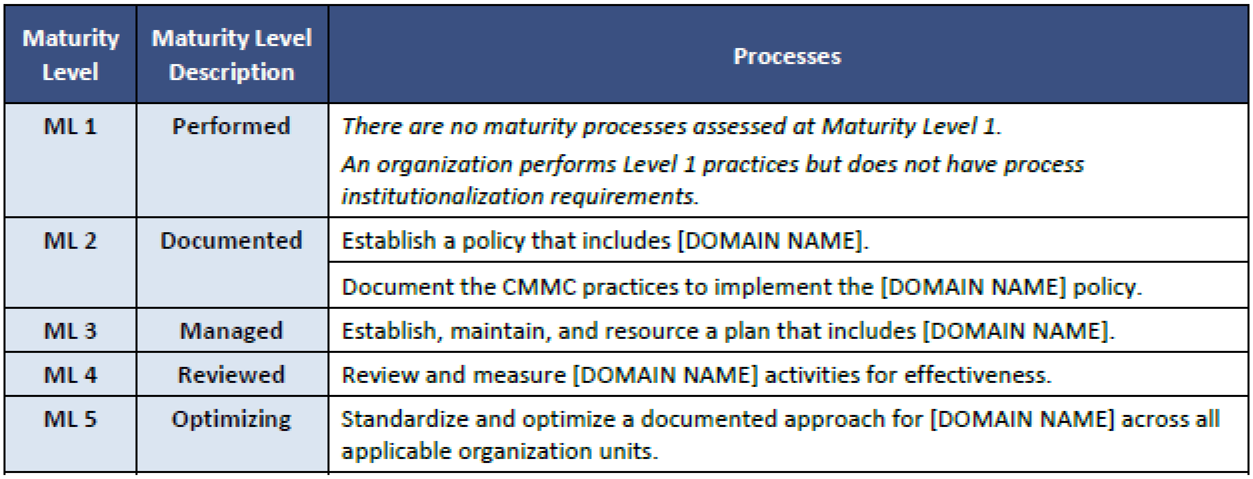


	PROCESSES	PRACTICES
Level 5	Optimizing	Advanced / Progressive
Level 4	Reviewed	Proactive
Level 3	Managed	Good Cyber Hygiene
Level 2	Documented	Intermediate Cyber Hygiene
Level 1	Performed	Basic Cyber Hygiene

Figure 3: CMMC Processes and Practices (Reference CMMC v1.02 Doc Fig 2)

[7] NIST SP 800-171 Rev. 2, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations", February 2020

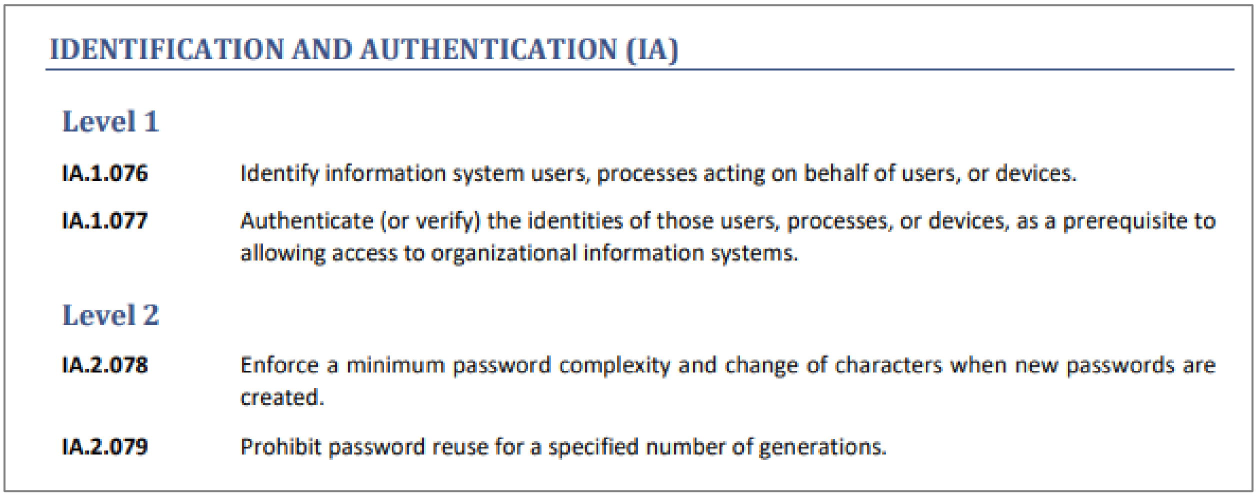
Higher maturity levels include activities that facilitate a more robust process, such as documenting, managing, reviewing, and optimizing processes. For instance, an organization may have policies in place that document their list of approved software (Level 2), but if they additionally review logs to determine what software is running on local machines, that would demonstrate Level 4 process maturity. Figure 4, below, displays the CMMC processes and their various levels. Figure 4 provides some additional insight into the process maturity level assessments



Maturity Level	Maturity Level Description	Processes
ML 1	Performed	*There are no maturity processes assessed at Maturity Level 1.* *An organization performs Level 1 practices but does not have process institutionalization requirements.*
ML 2	Documented	Establish a policy that includes [DOMAIN NAME].
		Document the CMMC practices to implement the [DOMAIN NAME] policy.
ML 3	Managed	Establish, maintain, and resource a plan that includes [DOMAIN NAME].
ML 4	Reviewed	Review and measure [DOMAIN NAME] activities for effectiveness.
ML 5	Optimizing	Standardize and optimize a documented approach for [DOMAIN NAME] across all applicable organization units.

Figure 4: CMMC Maturity Level Descriptions (Reference CMMC v1.02 Doc Table 2)

“Practices”, the second CMMC component, include the prescribed security measures (i.e., activities) that are employed to adequately protect Federal Contract Information (FCI) and CUI. The Practice descriptions identified in Figure 33 merely represent the aggregate summary of the many practices that are actually required for each maturity level. As organizations progress up the CMMC maturity levels, the number of the practices increases from 17 (for Level 1) all the way up to 171 (for Level 5). The CMMC Model documentation clearly outlines the practices required for specific maturity levels, as is illustrated in Figure 2.



IDENTIFICATION AND AUTHENTICATION (IA)

Level 1

IA.1.076	Identify information system users, processes acting on behalf of users, or devices.
IA.1.077	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

Level 2

IA.2.078	Enforce a minimum password complexity and change of characters when new passwords are created.
IA.2.079	Prohibit password reuse for a specified number of generations.

Figure 2: CMMC Model Practices for the IA Domain (Reference CMMC V1.02 p. 15)

The CMMC assessment model's level-based approach requires an organization to meet both the process and practice requirements to satisfy each maturity level. Thus, both factors have an equally important role in an organization's preparations for a CMMC assessment.

Tailored Implementation

While CMMC is intended to address all DIB contractors to secure the DoD supply chain, the developers also acknowledge that different organizations will have different requirements based on their provided products/services. The maturity levels present this flexibility such that the provider of facility maintenance services is not subject to the same cybersecurity practices as a weapons system manufacturer. This additionally helps to prevent (or at least mitigate) the possibility that doing business with DoD becomes prohibitively costly to an organization, based on these new requirements. This is reflected in the specified focus of each maturity level, which are defined below:

- Level 1 - Safeguard Federal Contract Information (FCI)
- Level 2 - Serve as transition step in cybersecurity maturity progression to protect CUI
- Level 3 - Protect Controlled Unclassified Information (CUI)
- Level 4-5 - Protect CUI and reduce risk of Advanced Persistent Threats (APTs)

This type of tailored approach is fairly consistent across the various government and industry-related compliance frameworks, in attempt to apply requirements that are commensurate with the associated threats, data sensitivity and a number of related factors. That being said, there is some uncertainty for organizations attempting to implement a CMMC compliance strategy based on the uncertainty of CMMC maturity level requirements for future solicitations.

What's New

Although much of the foundation for the CMMC includes the recommendations and guidelines introduced under the legacy CUI and cybersecurity documentation, CMMC introduces new elements in the requirements and certification process. Many of these refinements are intended to improve upon those initial frameworks with a more detailed and independently-verified assessment of an organization's security program.

The majority of the CMMC domains come from the Federal Information Processing Standards (FIPS) Publication 200 [12] and the NIST SP 800-171 [4], but CMMC also introduces 3 additional domains, which include Asset Management (AM), Recovery (RE), and Situational Awareness (SA). These three new domains complement the 14 security requirement families from NIST SP 800-171, forming the previously mentioned 17 CMMC domains. These changes bring greater awareness to an organization's assets, security threats and preparations to recover from a potential cyber incident.

CMMC's five maturity levels also allow for greater flexibility in only having to meet the specific security requirements that are necessary for an organization's contracted services. The maturity levels provide greater granularity than previous CUI compliance documents, with tiered implementation requirements for the necessary security practices and processes. For example, CMMC Level 3 has a total of 130 practices, which include all of the requirements that are in the NIST SP 800-171, while Levels 1 and 2 have 17 and 72 practices, respectively. Levels 4 and 5 similarly introduce additional security requirements, such as those intended to enhance situational awareness and improve the ability to protect against and/or respond to Advanced Persistent Threats (APT). This flexibility in only having to meet the necessary requirements for an organization's business profile improves upon blanket security requirements that apply to all DoD contractors.

Another CMMC refinement, is the need for independent third-party assessment of an organization's practices and processes. Previous models, such as NIST SP 800-171, allowed contractors to self-certify their compliance status without outsider involvement. While no one would argue that organizations would falsify any assessment findings, there is certainly a higher level of scrutiny when an assessment is performed by an outside party. The CMMC Accreditation Board (AB) is currently in the process of releasing instructions for organizations that wish to become a Certified 3rd Party Assessment Organization (C3PAO), as well as other contributing roles (e.g., Registered Provider Organization (RPO), Licensed Training Providers, etc.). Self-assessments have not been completely eliminated, as they are still encouraged to be performed as a preparation activity that precedes the C3PAO assessment.

One potential area of uncertainty involves an acquisition program's selection of the required maturity level for specific DoD contracts. While there are likely examples where the subject tasking clearly aligns with a CMMC maturity level, there are also likely to be situations where there is some uncertainty. The question that arises is whether maturity levels may be artificially inflated to protect against all possible outcomes, in which case contractors could grow concerned about eliminating themselves from competition by not setting out to achieve the highest (or higher) maturity level. In these initial stages, the first contractual requirements have been requesting offerors' planned approach to achieving CMMC compliance. One other aspect that is not fully clear is whether certification requires an organization to be compliant with each and every security practice required for a specific maturity level (i.e., is any aspect of a POA&M considered acceptable).

Road to Compliance

Organizations that are new to such cybersecurity compliance frameworks should start this endeavor by identifying the internal stakeholders that should be involved in the process. This typically includes the designers/operators of an organization's Information Technology (IT) backbone, including network engineers and system administrators, but also members of the management team to ensure the compliance strategy is both supported at the executive level and consistent with the established business goals. Organizations which have previously performed similar cybersecurity requirements may use the CMMC's implementation as an opportunity to revisit this task, ensuring that they have the right mix of personnel contributing to this activity.

Once the key stakeholders have been identified, an organization should identify the CMMC maturity level that is best suited to their current and future government contracts/subcontracts. This will determine the necessary practices and processes which the organization will need to satisfy. The discussion in this document and the supporting CMMC Model description provide detail to help understand the certification requirements for different types of DoD contracts.

Organizations should next inventory the current controls they have in place, eventually performing a comparison against the practices and processes dictated by the selected maturity. For example, do they periodically perform and test backups, do they routinely conduct risk assessments, are they using multi-factor authentication? These types of questions often cannot be answered by a single individual, thus reinforcing the need for a team of participants scattered within the organization. Furthermore, those new to the process may be surprised to discover that not all requirements involve technical security implementations. More specifically, CMMC's practices and processes include a somewhat substantial amount of documentation, ranging from implementation details and process descriptions to planned responses to particular events/scenarios (e.g., incident response). After comparing the organization's current security implementations (to include plans and policies) to the CMMC maturity level requirements, the organization should identify and prioritize corrective actions to address the unanswered CMMC practices and processes.

Organizations that have previously completed the NIST SP 800-171 CUI certification process admittedly have a head start for the CMMC model. As mentioned previously, up through CMMC maturity level 3, the required practices are nearly identical to those found in the NIST 800-171, while lower maturity levels have even fewer requirements. Identifying the gaps in the preferred maturity level's required practices against any previous NIST P 800-171 implementations, and additionally consulting a prior Plan of Action & Milestones (POA&M), should help with the formulation of a CMMC compliance strategy. Clearly, organizations that can leverage any previously completed implementations, even if they require updates/revisions, can limit the cost and timeline for achieving CMMC compliance.

References

[1] https://www.natlawreview.com/article/counting-down-to-2020-and-department-defense-s-cybersecurity-maturity-model

[2] https://blog.rapid7.com/2020/04/15/preparing-for-the-cybersecurity-maturity-model-certification-cmmc-part-1-practice-and-process/

[3] https://breakingdefense.com/2020/02/cmmc-1-0-vs-nist-800-171-eight-essential-differences/

[4] https://www.acq.osd.mil/cmmc/

[5] https://www.csoonline.com/article/3535797/the-cybersecurity-maturity-model-certification-explained-what-defense-contractors-need-to-know.html

[6] https://www.pwc.com/us/en/services/consulting/cybersecurity/cmmc-aerospace-defense.html

[7] https://insights.sei.cmu.edu/sei_blog/2020/03/an-introduction-to-the-cybersecurity-maturity-model-certification-cmmc.html