OSIbeyond

DoD Contractor’s Guide to CMMC 2.0 Compliance

February, 2024

Contents

DoD Contractor’s Guide to CMMC 2.0 Compliance

Introduction

The cyber threat landscape is evolving at a rapid pace and guarding critical infrastructure and sensitive information against both nation-states and non-state actors has become a top priority for the government. Recent attacks including the SolarWinds supply chain compromise, HAFNIUM exchange vulnerabilities and Log4j exploits have only increased the focus on this issue.

Although there have been many attempts in the past to enforce the adoption of robust cybersecurity measures in the defense industry, they've largely failed to deliver the desired results, leaving vital assets exposed and vulnerable.

Now, the Cybersecurity Maturity Model Certification (CMMC) is here to change that, and all contractors working for the Department of Defense (DoD) must familiarize themselves with it and their obligations if they want to continue offering their products and services.

The road to CMMC compliance may seem long and difficult, but this guide makes it much less daunting by explaining each and all steps contractors need to take to prepare for it, achieve it, and maintain it.

What Is CMMC 2.0?

The Cybersecurity Maturity Model Certification v2.0 is a new assessment requirement for DoD contractors and subcontractors. It replaces the previous CMMC 1.0 model and brings together cybersecurity requirements necessary to protect Federal Contract information (FCI) and Controlled Unclassified Information (CUI).

There are several major differences between CMMC 2.0 and CMMC 1.0:

- First, CMMC practices not directly taken from NIST SP 800-171 have been eliminated at Level 2, including the 20 additional practices added to the 110 practices from NIST 800-171. The CMMC process maturity requirements (997/998/999) have also been removed.
- Second, only some contractors will be assessed by third-party entities (the so-called CMMC 3rd Party Assessor Organizations, or C3PAOs for short). CMMC 1.0 required all organizations to undergo a third-party assessment. CMMC 2.0 limits this to a subset of organizations holding CUI Data and requiring CMMC 2.0 Level 2 or 3. Organizations holding only FCI data at CMMC 2.0 Level 1, or CUI of lesser sensitivity at Level 2, may now be permitted to conduct an annual self-assessment. However, DoD estimates indicate self-assessments at Level 2 will be rare (~5% of total), therefore all Level 2 contractors should prepare for a third-party assessment.
- Third, the five certification levels outlined in CMMC 1.0 have been reduced to only 3. Level 1, for organizations in possession of FCI, Level 2, for organizations in possession of CUI and Level 3, for organizations possessing prioritized CUI. Most likely, prioritized CUI will be restricted to CTI related to critical weapons systems and space or aerospace applications.
- Fourth, some open POAM items, with a limited remediation window, are now permitted.

CMMC 2.0 assessment guidelines and model documentation were posted to the DoD CIO site in December 2021, followed by the 32 CFR CMMC 2.0 rule being made available for public comment in December 2023.

Eventually, all DoD contractors and subcontractors that handle FCI or CUI will be required to meet CMMC 2.0 requirements, documented either by third party assessment or self-assessment & attestation. Only contractors that provide commercial-off-the-shelf products and don't handle any CUI won't be required to achieve one of the three levels of compliance.

CMMC Timeline

The most important CMMC dates include:

- **January 2020** - The introduction of CMMC Version 1.0.
- **April 2021** - The first C3PAO's begin to be assessed against CMMC Level 2 (previously CMMC 1.0 Level 3) by the Defense Industrial Base Cybersecurity Assessment Center (DIBCAC). C3PAO's must pass their own Level 2 assessment before being able to conduct assessments themselves.
- **November 2021** – The DoD review of the CMMC program is concluded, CMMC v1.0 is effectively terminated and replaced by CMMC 2.0.
- **December 2021** – CMMC v2.0 model documentation and assessment guides released.
- **January 2022 – December 2023** – Rulemaking underway while DIB contractors prepare for CMMC 2.0 requirements.
- **December 2023** – 32 CFR CMMC 2.0 DFARS rule released for public comment, along with supporting documentation including CMMC 2.0 assessment and scoping guidelines.
- **January 2024 – December 2024** – DoD review and analysis of comments on 32 CFR CMMC 2.0 rule and release of 48 CFR CMMC 2.0 rule for public comment.
- **January-March 2025 (Estimated)** – The CMMC 2.0 rule takes effect requiring self-assessment and attestation for all new contracts. Self-attestation will be replaced by third party (C3PAO) assessment requirements as the assessment ecosystem ramps up.
- **July-September 2025 (Estimated)** - Third party (certification) assessment requirements introduced at Level 2.
- **July-September 2026 (Estimated)** – Third party certification requirements are introduced for the exercise of options to extend existing contracts.
- **July-September 2027 (Estimated)** – Rollout concludes with CMMC 2.0 requirements now included in all DoD solicitations and contracts.

What Are the CMMC 2.0 Certification Levels?

To reflect the fact that not all contractors handle information of the same sensitivity, the CMMC 2.0 framework defines three cybersecurity levels. These levels begin as a subset of NIST SP 800-171 (Level 1) and progress to a full implementation of NIST SP 800-171 plus additional components from NIST 800-172 (Level 3)

In other words, the higher CMMC 2.0 level a contractor must comply with, the more sophisticated and better documented its cybersecurity program needs to be. ntory must be main

CMMC 2.0 Level 1

CMMC 2.0 level 1 is about meeting the basic requirements to protect FCI, such as ensuring access to systems is restricted to authorized users and maintaining an accurate inventory of authorized users, applications, and devices. FCI is defined as information, not intended for public release, that is provided by or generated for the government under a contract to develop or deliver a product or service to the government.

All organizations that have an active contract with the DoD should be able to achieve Level 1 compliance without any significant investment in new technology; however, improvements in documentation and processes are often required. Under CMMC 2.0, all Level 1 compliance will be managed via a self-assessment and attestation process. No third-party certification will occur at this level.

CMMC 2.0 Level 2

Level 2 is all about demonstrating good cyber hygiene and having the controls necessary to protect CUI. Contractors who would like to achieve Level 2 compliance should be prepared to continuously review all activities based on their cybersecurity polices. CMMC 2.0 Level 2 will be obtained by a third-party independent assessment for formal certification, or through a self-assessment process conducted by the contractor. Per DoD estimates, 95% of Level 2 assessments will be conducted by a third party.

This level encompasses all requirements specified in NIST SP 800-171 Rev 2. These requirements cover everything from logging and monitoring to incident response to configuration management. Note that while the CMMC 1.0 controls that directly specified requirements for policies, procedures and plans have been removed from CMMC 2.0, in reality it will be nearly impossible to pass a CMMC 2.0 third party assessment without a robust suite of documentation for an assessor to review. NIST SP 800-171, and therefore CMMC 2.0, assumes that an organization has developed the policies specified in NIST SP 800-171 Appendix E (800-53 NFO Controls). These policies include most, but not all of those that were required in CMMC 1.0 and are necessary to support NIST 800-171 / CMMC 2.0 Level 2 compliance.

The release of CMMC 2.0 provided additional scoping guidance, particularly for manufacturers and other organizations with Operational/Industrial Technologies (OT), test equipment and Internet-Of-Things (IOT) devices. These devices must be documented in an organization's SSP, inventory and systems diagrams, but are not required to be assessed per other CMMC 2.0 practices. However, following risk-based management principles, these assets should be protected using administrative functions and technology to the extent that this is possible. This new guidance is extremely beneficial for organizations with OT/IOT systems that are unable to meet CMMC 2.0 requirements and cannot be replaced without an unsustainable financial outlay.

CMMC 2.0 Level 3

CMMC 2.0 Level 3 focuses on addressing the changing tactics, techniques, and procedures used by Advanced Persistent Threats (APT) adversaries. This level includes the entirety of NIST SP 800-171 plus 24 controls from NIST SP 800-172 as an additional supplement. Contractors previously selected for a Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) High assessment are likely Level 3 candidates. Level 3 assessments will be conducted by DoD DIBCAC directly and not by a C3PAO.

How to Determine Which Level Applies to You?

The CMMC 2.0 framework is divided into three levels so that DoD contractors are not expected to comply with requirements that are not necessary to protect the type of information they handle. A contractor at the very bottom of the supply chain will possibly be required to be compliant only to Level 1, while a contractor with access to sensitive space or weaponry data will be required to be compliant/ certified to Level 2 or Level 3. However, the nature of the DoD subcontracting flow has led to the widespread overuse of contract provisions mandating compliance with NIST 800-171 (i.e., CMMC 2.0 Level 2) for organizations that do not and are unlikely to ever hold CUI. These organizations are in a difficult position and must either push back on these requirements during contract negotiations or commit to a CMMC 2.0 Level 2 security posture.

To determine which CMMC 2.0 level a contractor should be working toward, it's important to inventory all systems with the goal of determining the locations, if any, of FCI and CUI. Contractors that don't have the capacity to complete this first step in-house should partner with a managed services provider (MSP) offering CMMC 2.0 readiness assessments.

Once a readiness assessment has been performed to reveal how FCI and CUI is stored, and access to information is controlled, determining which systems must comply with which CMMC 2.0 level shouldn't be a problem. FCI and therefore CMMC 2.0 Level 1 will generally apply to most systems at most contractors. The scope of an environment containing CUI and meeting CMMC 2.0 Level 2 requirements should be more limited to minimize ongoing compliance overhead. Only contractors that are CMMC 2.0 compliant will be allowed to store FCI or CUI in their environment.

CMMC 2.0 does not apply to Commercial Off-the-shelf (COTS) products or services. These are commercial items sold in substantial quantities in the commercial marketplace which are offered to the government, under a contract or subcontract at any tier, without modification, in the same form in which it is sold in the commercial marketplace.

What Is the Difference Between FCI and CUI?

Since the CMMC 2.0 framework revolves around the protection of FCI and CUI, it's important that we clarify the difference between these potentially confusing terms. Here's how the National Archives and Records Administration defines each term:

Federal Contract Information (FCI)	Controlled Unclassified Information (CUI)
"Information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public Web sites) or simple transactional information, such as necessary to process payments."	"Information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended."

As the definitions explain, the terms FCI and CUI are both used to describe information created or collected by or for the government, and also information received by the government. FCI data is of a lower sensitivity. It includes contract documents, performance metrics and pricing or sensitive vendor information that may not be publicly disclosed. CUI often includes building schematics, measurements and specifications for parts and other information that could be valuable to an adversary.

The DoD is obligated to label CUI as such when provided to a contractor, however in practice this does not always occur. The migration from legacy compliance terms such as FOUO and training of DoD contract officers is ongoing. Contractors should make their best effort to review the data in their possession and ensure it is appropriately protected if deemed to be CUI.

There are two subsets of CUI:

- **CUI Basic:** Laws, Regulations, or Government-wide policies that DO NOT require specific protections. Agencies handle CUI Basic according to the uniform set of controls set forth in this part and the CUI Registry.
- **CUI Specified:** Laws, Regulations, or Government-wide policies that require specific protections. The CUI Registry indicates which laws, regulations, and Government-wide policies include such specific requirements.

Controlled Technical Information (CTI) is a special type of CUI. It consists of technical information with military or space application that is subject to controls on access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Examples of CTI include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identification, data sets, studies and analysis, and related information, and computer software executable code and source code. CTI is a CUI category that has been specifically singled out by the DoD in the CMMC 2.0 framework. It is information that may need additional protection above and beyond CMMC 2.0 Level 2, meaning contractors with this information are possible candidates for CMMC 2.0 Level 3. Contracts containing CTI will likely be prioritized for third-party assessments at Level 2, and self-attestation will not be available.

In summary, it can be said that all CUI is also FCI, but not all FCI is CUI. At the same time, both FCI and CUI are distinctly different from information that is marked for public release because that doesn't carry any minimum-security requirements.

What Is the Difference Between NIST SP 800-171 and CMMC 2.0?

NIST 800-171 Rev2 contains the minimum-security requirements that the federal government has deemed necessary to protect CUI data, regardless of the size of the entity that holds the data. For a contractor holding CUI, CMMC 2.0 is the assessment and verification mechanism that will ensure that contractors have implemented 800-171 in its entirety.

Third-Party Certification

Under existing DFARS 252.204-7012 requirements, contractors don't have to pass any official certification process to prove that they have the ability to protect CUI. While some behaved responsibly and took cybersecurity seriously, many merely developed a plan for how compliance would eventually be achieved in the future.

This is changing with CMMC 2.0, which requires most contractors holding CUI to be certified by CMMC 3rd Party Assessment Organizations. These organizations will be licensed by the CMMC Accreditation Body (Cyber AB), which was established in January 2020 to train, test, and license up to 10,000 C3PAOs.

Mandatory Certification

NIST SP 800-171 compliance was presented by the DoD as a competitive advantage in the tender process, but today's cybersecurity landscape demands a different approach, one that doesn't depend on contractors voluntarily strengthening their defenses to protect sensitive information from malicious third parties and unintended public disclosure.

To work with the DoD in the future, all contractors will eventually be required to either attest to their CMMC 2.0 compliance status or obtain a CMMC 2.0 certification from a C3PAO or the DoD.

What do contractors Need to Know About Cybersecurity FAR and DFARS?

CMMC 2.0 builds upon existing regulations, extending them to meet the cybersecurity challenges government contractors face in this day and age. These regulations are included in the Federal Acquisition Regulations (FAR) and the Defense Federal Acquisition Regulation Supplement (DFARS), which implements and supplements the FAR.

Both FAR and DFARS clauses are referenced in DoD contracts and are often flowed down to subcontractors as well. A DoD contractors' commitment to a specific cybersecurity standard begins with the contractual commitments outlined in these clauses. Any compliance work undertaken prior to a thorough review of existing contracts is time wasted.

FAR 52.204-21 governs requirements for managing Federal Contract Information (FCI). These are 15 relatively straightforward controls that all contractors must meet in order to handle FCI. They will be assessed as part of any CMMC 2.0 certification, beginning with Level 1.

In October of 2016, the DoD issued the DFARS 252.204-7012 clause, requiring contractors to implement NIST 800-171 standards to protect information systems containing CUI. 7012 requires contractors to maintain a System Security Plan (SSP) and Plan of Actions & Milestones (POAM) and also includes requirements for reporting security incidents that impact CUI. The contractors' level of compliance with 800-171 is not reportable to DoD under DFARS 7012. Today, the 7012 clause is commonly found in both DoD contracts and subcontracts.

CMMC 2.0 will be required in contracts by adding a reference to DFARS 252.204-7021. There is no allowance for certification of a contractor after a contract has been awarded. Certification, if required, should be obtained before or during the bid process. Importantly, CMMC 2.0, via DFARS 7021 will be included in contracts alongside 800-171 and DFARS 7012, assuming the contract requires CMMC 2.0 Level 2 or above. CMMC 2.0 does not replace the previous DFARS 7012 requirements. This is critical as DFARS 7012 contains requirements in paragraphs c-g of the regulation itself that are not included in CMMC 2.0. Additionally, NIST 800-171 Appendix E contains 61 Non-Federal Organization (NFO) controls that also are assumed to be implemented per DFARS 7012 and are not included in CMMC 2.0.

In November of 2020, DoD elected to strengthen the existing DFARS 7012 requirements as an interim step due to the extended ramp up of the CMMC program. The so-called "interim rule", implemented via DFARS 252.204-7019 and 7020, requires contractors to perform a self-assessment against NIST 800-171 and provide a score to the DoD prior to contract award. DFARS 7019/7020 are not retroactive, however their implementation has been far more rapid than CMMC and requirements for self-assessment completion are now commonplace, especially from prime contractors seeking to verify the security posture of their subcontractors and supply chain. This self-assessment methodology will remain under CMMC 2.0, with the scoring system and other attributes re-purposed in the CMMC 2.0 assessment process.

CMMC Accreditation Body and Ecosystem

The CMMC Accreditation Body (Cyber AB) is an independent nonprofit organization operating under an agreement with the DoD. The Cyber AB is not part of the DoD or the US government by design. The Cyber AB was designed to be run by an independent board of directors, to ensure the CMMC business model is mindful of any potential impact to small and midsized businesses that are relied upon by the DoD.

The Initial governance architecture and business model were designed through committees with representatives from across industries and academia. The Cyber AB continues to engage the industry through working groups for feedback and was designed to be a listening organization that welcomes feedback from industry advisory councils.

The Cyber AB has a strong relationship with DoD, which oversees the CMMC 2.0 framework. While the Cyber AB manages the CMMC 2.0 ecosystem, the DoD controls the CMMC 2.0 model and sets minimum thresholds for acceptable CMMC 2.0 assessments. The DoD can also impose at its option additional cybersecurity requirements outside of the CMMC ecosystem. The DoD requires the implementation of CMMC 2.0 requirements by contractors through DFARS and other contractual requirements.

The CMMC ecosystem is managed by Cyber AB, which defines the ecosystem structure, entities, training, exam requirements, etc. It also creates additional refinements as necessary to ensure a strong CMMC ecosystem and provides feedback to DoD about the CMMC 2.0 model and documentation, to further refine and enhance the model. The Cyber AB's role is to help contractors, consultants, and assessors better understand what is acceptable under CMMC 2.0 and ensure that the assessments are fair and meet requirements. The Cyber AB does not perform assessments, or consulting.

The CMMC ecosystem consists of a marketplace that includes Service Provider Organizations and Individuals Performing Services. Services Provider Organizations consist of Registered Practitioner Organizations (RPOs), and CMMC 3rd Party Assessment Organizations (C3PAOs). RPOs are consulting companies that help contractors prepare for assessments but are not permitted to provide formal third-party assessments, whereas C3PAOs can provide assessments or consulting services to contractors. However, an organization providing assessment readiness consulting services to a contractor cannot conduct a CMMC 2.0 assessment on that same organization. Individuals Performing Services consist of Registered Practitioners (RPs) who are consultants that help contractors prepare for assessments, Certified Professionals (CCPs) who are consultants that can participate on assessment teams, and Certified Assessors (CAs) who are consultants that lead formal assessments.

Contractors can visit the Cyber AB service provider marketplace to find an RPO or C3PAO, who will then determine which type of individual service performers need to engage with the contractor. Contractors can also prepare for an assessment by themselves without engaging with an RPO or C3PAO.

How to Prepare for a CMMC 2.0 Assessment?

Prior to the arrival of CMMC 2.0, defense contractors were required to self-certify that they follow cybersecurity requirements, however there was no reporting back to DoD on the contractor's cybersecurity posture. CMMC 2.0 adds additional reporting and requirements to the status quo and requires a subset of contractors to pass a CMMC 2.0 assessment performed by a C3PAO or the DoD itself.

Because it can take a lot of time and work to prepare for a CMMC 2.0 assessment, the CMMC Accreditation Body (Cyber-AB) advises contractors to start preparing for it at least six months in advance, depending on their current cybersecurity readiness and resources. In OSIbeyond's experience, most organizations require 12-18 months to advance from a typical small business cybersecurity posture to one that is assessment ready.

Step 1: Start with a Readiness Assessment and Gap Analysis

Because CMMC 2.0 is comprised of existing standards and common business practices, it's possible that many DoD contractors have already done some of the work required to achieve one of the lower CMMC 2.0 levels.

The goal of a readiness assessment is to first provide a detailed inventory of information technology systems including types of data stored, how that data flows to other systems, where it is stored, and how users access systems during day-to-day work. This inventory allows for an accurate diagram and environment scope to be prepared, clearly showing which systems must be compliant with 800-171 versus those that do not need to be as stringently protected.

Step 2: Resolve Major Scope Issues

With the information collected in Step 1, it is possible to immediately determine if any major migrations or changes are necessary in the contractor's environment. Examples may include CUI or export-controlled data that is currently stored in a non-compliant cloud platform, or a non-compliant managed security services provider (MSSP) that is responsible for security functions. The contractor should resolve these issues before moving forward with a detailed gap assessment against all requirements.

Step 3: Assess environment against CMMC 2.0 requirements.

Once issues identified in Step 2 have been resolved, the organization may move forward with a comprehensive gap analysis. At CMMC 2.0 Level 2, this must include the 320 assessment objectives in NIST SP 800-171 and should also include a review of DFARS 7012 c-g requirements, export control (ITAR) considerations and any other compliance commitments that may be placed on the contractor. A gap analysis plays an essential role in helping DoD contractors prepare for CMMC 2.0 requirements because it identifies risks, reveals the cost of remedial steps, and helps develop an efficient plan for implementation.

Once all cybersecurity gaps have been identified, they must be resolved according to a remediation plan, which is an actionable plan that lists all activities necessary to resolve security issues in the order they should be performed.

The remediation plan should describe how the cybersecurity gaps were uncovered and quantify the risk they represent. A timeline should be provided to help ensure the remediation doesn't take too long, and estimated remediation costs should be included to avoid budget overruns. For CMMC 2.0, most of these gaps will be related to written policies and procedures that must be developed. The effort required to implement these for an organization is significant.

Step 4: Ongoing Monitoring and Reporting

The DoD expects contractors to monitor their systems on an ongoing basis and report any incidents they detect. Ongoing access reviews, auditing and monitoring of controls should also be expected. Newly implemented policies and procedures must now be reviewed on a recurring basis and updated as necessary. For large contractors with a wealth of resources and plenty of cybersecurity experience with specialized cybersecurity monitoring tools, this last step won't be too much of a challenge. Smaller contractors, on the other hand, may find it to be the most difficult step of the three.

Such contractors are often unable to do everything in-house without losing focus on their core business and maintaining the quality of service that has helped them secure a government contract in the first place. Fortunately, they can outsource cybersecurity monitoring—and many other activities associated with CMMC 2.0 assessments for that matter—to a Managed Security Service Provider (MSSP).

A partnership with an experienced MSSP allows DoD contractors to get the expertise they require without stretching themselves too thin, and it typically results in substantial time and cost savings compared with the in-house approach, making it the best way to prepare for a CMMC 2.0 assessment.

What Does a third party CMMC 2.0 Assessment Involve?

Third-party CMMC 2.0 assessments are performed by CMMC Third-Party Assessment Organizations (C3PAO), which are companies accredited by the CMMC Accreditation Body (Cyber AB). CMMC 2.0 assessments are evidence-based and take place on-site. The result of a successful CMMC 2.0 assessment is a CMMC 2.0 certification, which represents that the contractor has demonstratively achieved a certain level of cybersecurity.

Here's what a CMMC 2.0 assessment will involve in practice:

- **Review of the current security program:** First, the C3PAO will get in touch with the person who is responsible for the organization's cybersecurity. This can be a dedicated CISO, but it can also be the network administrator, or other designated personnel. The C3PAO will go over the current security program to better understand the environment that it's dealing with. Specifically, the C3PAO will want to know what FCI/CUI data is stored and transmitted by the organization and how. This will include a full review of the system security plan (SSP) and supporting documentation to verify that the contractor is ready for assessment. Second, only some contractors will be assessed by third-party entities (the so-called CMMC 3rd Party Assessor Organizations, or C3PAOs for short). CMMC 1.0 required all organizations to undergo a third-party assessment. CMMC 2.0 limits this to a subset of organizations holding CUI Data and requiring CMMC 2.0 Level 2 or 3. Organizations holding only FCI data at CMMC 2.0 Level 1, or CUI of lesser sensitivity at Level 2, may now be permitted to conduct an annual self-assessment. However, DoD estimates indicate self-assessments at Level 2 will be rare (~5% of total), therefore all Level 2 contractors should prepare for a third-party assessment.
- **Assessment of vendor ecosystem** The C3PAO will also perform verification that any cloud service providers (CSP), managed services providers (MSP) and Managed Security services providers (MSSP) have a valid CMMC 2.0 certification or FedRAMP Authorization as needed. They will also require shared responsibility matrices from these providers to define which requirements are being met with the service provider's help.
- **Verification of the implementation of controls:** Next, the C3PAO will perform an in-depth analysis of individual controls to verify their implementation. An assessor may ask the person who is responsible for the organization's cybersecurity to explain a certain process or demonstrate how a specific control works. Depending on the CMMC 2.0 level, the assessor may need to see an informal walkthrough of the process for level 1 but may require written documentation in the form of a policy, procedure, or configuration data at level 2 or 3. This verification can involve any staff member or job function mentioned in a policy or procedure including HR, Operations, and individual end users. All staff must be able to demonstrate familiarity with policies, procedures and training material that includes them.
- **Issuing of an official assessment report:** Finally, the C3PAO will submit an official report to the CMMC Accreditation Body (Cyber AB), after doing its own internal QA, detailing how well the assessed organization performed and whether it meets the requirements of the target CMMC 2.0 Level. The C3PAO will keep details about specific findings confidential, so the organization doesn't have to worry about suffering damage to its reputation. The Cyber AB will then conduct its own QA to validate the C3PAO's assessment and then determine whether certification can be issued directly to the contractor.

It's important to keep in mind that passing one CMMC 2.0 assessment doesn't mean that the certified contractor can stop worrying about CMMC and its requirements. According to the DoD, CMMC is intended to be an evolving certification and compliance process that will very likely introduce new controls to the various levels in response to emerging threats. Because CMMC 2.0 certification will be valid for three years, contractors must prepare for regular reassessments by working toward ensuring ongoing compliance.

External Service Provider Considerations

Most smaller contractors leverage some combination of Internal IT staff and/or outsourced IT resources from Managed Services Providers (MSP) and/or Managed Security Services Providers (MSSP). These outsourced providers may be responsible for user account management, device setup, security functions & more.

The CMMC 2.0 rule as published includes requirements mandating that these service providers be third party certified to the same CMMC 2.0 level as the contractor, even if they do not directly hold CUI data, through a loosely defined requirement for the handling of "security protection data". This creates significant risk for many contractors. Unless an MSP has a significant percentage of DIB business, building a compliant information system and going through the certification process will not make business sense and is therefore unlikely to happen.

A contractor must effectively bet the future of their own contracts and business on their MSP obtaining CMMC 2.0 certification in a timely manner. Any contractor leveraging an MSP or MSSP should already be in discussions with them around CMMC 2.0 compliance and provision of a shared responsibility matrix and other supporting documentation for an assessment. A lack of certainty around CMMC 2.0 plans with an existing MSP should result in a contractor transitioning to a CMMC 2.0 focused provider as soon as possible.

Cloud Service Provider Considerations

Cloud Service Providers are entities that store or process data for a company, including Office 365, Box, Dropbox, etc. As expected, and in a continuation of existing requirements, Cloud Service Providers (CSP) are required to hold FedRAMP Moderate authorization and be in the FedRAMP marketplace or provide evidence of equivalency to that standard. OSIbeyond believes that the use of the equivalency option will be rare, as it would involve a CSP that meets the FedRAMP moderate standard but has elected not to become authorized and be added to the FedRAMP marketplace. Equivalency also requires C3PAO approval of CSP provided evidence, which is inherently unvalidated. C3PAOs may be reluctant to accept evidence of this type.

How to Ensure Ongoing Compliance?

The road to CMMC 2.0 compliance doesn't end with a successfully obtained certification. To maintain the ability to protect sensitive information and pass future assessments, DoD contractors must take certain steps to keep their cyber defenses effective against the latest threats coming from cybercriminals and state-sponsored actors alike. A functional CMMC 2.0 program will include numerous requirements for audits, reviews or checks of security controls on an ongoing basis.

Designate a Compliance Position

The first step any organization must take to ensure ongoing CMMC 2.0 compliance is to designate a compliance officer if this has not already been done. The job of a compliance officer is to maintain compliance with outside regulations and internal policies by monitoring the controls put in place to mitigate compliance risk and proactively suggesting ways in which they can be improved.

The role of a compliance officer is suitable for someone who has an in-depth knowledge of the organization and understands the regulatory landscape in which it operates. In smaller organizations, it's not unheard of for the compliance officer to also have the title of Chief Information Security Officer (CISO) or Chief Information Officer (CIO), while larger organizations tend to separate the roles to prevent the overlap of responsibilities.

Maintain Policies and Procedures

Policies and procedures can be seen as two sides of the same coin. The goal of policies is to guide decisions and actions by providing a deliberate system of principles. Procedures, on the other hand, are established ways of doing something.

All DoD contractors that want to achieve compliance with CMMC 2.0 Level 2 and above must document their policies and procedures to the extent necessary to support NIST 800-171 requirements for identification, inventory, and monitoring.

More importantly, they must regularly audit them and update them, as necessary, to maintain their relevancy and effectiveness. Significant changes to the environment will require re-assessment, potentially increasing assessment frequency for organizations that change the scope of their CUI environment.

Maintain Technical Capabilities

Cybercriminals are constantly evolving their tactics, exploring increasingly sophisticated strategies for circumventing the cybersecurity defenses of organizations handling sensitive government information. For DoD contractors to ensure ongoing CMMC 2.0 compliance, they must prevent their tools from becoming obsolete and ineffective.

This is possible only when cybersecurity is given a sufficiently high priority to maintain technical capabilities on an ongoing basis. For many contractors, this means partnering with a managed security services provider that understands what it takes to protect sensitive government information against release.

Conclusion

The Cybersecurity Maturity Model Certification v.20 aims to address the growing number of cybersecurity threats faced by the DoD and its contractors. It unifies the implementation of cybersecurity defenses by requiring all DoD contractors to become compliant with one of three levels of the CMMC 2.0 model.

By October 2027, CMMC 2.0 certification or compliance will be a prerequisite to be awarded defense contracts. As such, it's in the best interest of all DoD contractors to learn what it takes to obtain it and start taking the steps necessary to protect CUI and FCI.

If you have any questions about CMMC 2.0 and the steps it takes to achieve compliance with it, contact us at OSIbeyond and let us help you improve the maturity of your cybersecurity defenses.

OSIbeyond®

About

Whether your organization is a DoD contractor seeking to obtain CMMC certification or another industry standard such as ISO 27001, PCI DSS, HIPAA etc., cybersecurity compliance is a critical component of your business. Even if your organization does not have to adhere to any specific compliance requirements, cybersecurity should still be a top priority for your business.

Cyber threats continue to evolve and become more malicious every day. Organizations that don't take these threats as seriously as they would with any other external forces will risk the demise of their business.

OSIbeyond offers comprehensive cyber security solutions to help your organization stay ahead of cyber threats. Our compliance services are focused on helping your organization meet compliance standards, while our managed security services help maintain compliance on an ongoing basis. The combination of both services offers an end to end cyber security solution for organizations.

AB
THE CYBER AB
CMMC CERTIFICATION
REGISTERED PRACTITIONER

www.osibeyond.com