PL
PREVENTING RAMPANT CYBERATTACKS WITH CHR Solutions
MINIMIZING SATELLITE OUTAGES WITH AI
PREPARING FOR AI & QUANTUM THREATS FROM dispersive
SAVING LIVES WITH SATCOM + 5G WITH ORACLE
DT MIGRATION ASSURANCE
PREVENTING GENAI SOCIAL ATTACKS
THE ABCs OF CMMC CERTIFICATION
FRAUD-FREE IOT
AI SECURITY & SAFETY
DATA PRIVACY & SECURITY
SECURITY & ASSURANCE

www.pipelinepub.com
Volume 21, Issue 1

The ABCs of CMMC: Clarifying CMMC Certification

By: Scott Singer - CEO, CyberNINES

Navigating the requirements for Cybersecurity Maturity Model Certification (CMMC), not to mention the various players involved, can seem overwhelming to organizations relying on Department of Defense (DoD) contracts as a mainstay of their business, especially considering the risk of losing that business if not compliant. This article provides an overview of CMMC, the partners and providers you will work with as you become compliant, and important considerations when engaging these providers.

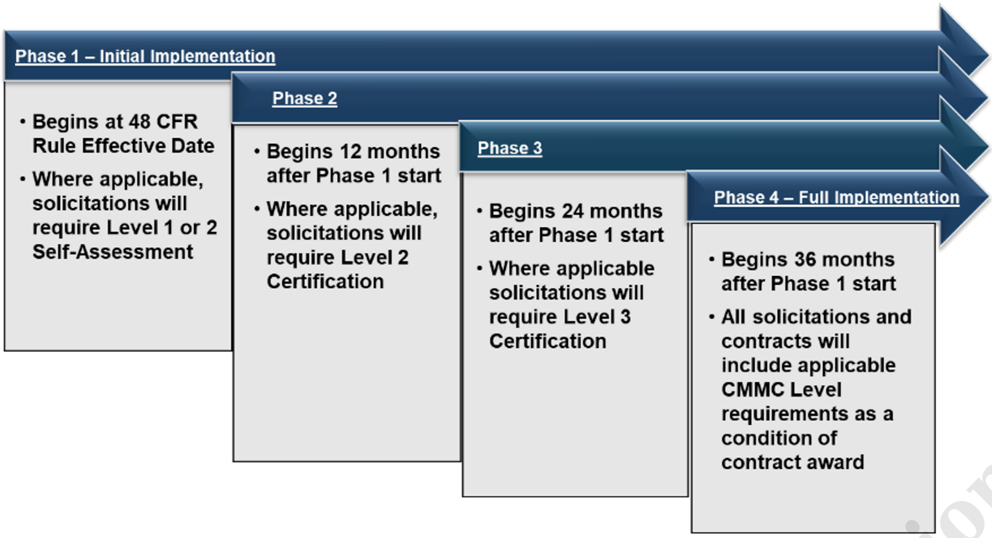
The CMMC Program and The Cyber AB

A good place to start is with the Cybersecurity Maturity Model Certification (CMMC) itself. The DoD created its CMMC program to protect its data, because much DoD project work is done by non-government contractors. CMMC is not a new idea. NIST SP 800-171 was released back in 2017 with the associated DoD acquisition regulation, DFARS 252.204-7012. Since that time Defense Contractors have been required to maintain a program of compliance and make progress towards meeting all 110 controls. The Cybersecurity Maturity Model Certification (CMMC) program was created when the government found that contractors were not making significant progress. CMMC requires contractors to have a third-party assessment similar to ISO 9001 and AS 9100.

CMMC incorporates two rules:

32 CFR Part 170 describes the program and authorizes organizations to do assessments; it became a final rule October 11, 2024, and is expected to take effect December 16, 2024.

48 CFR Subpart 204.75 creates the Defense Federal Acquisition Regulation Supplement (DFARS) that will show up in contracts as DFARS 252.204-7021; the effective date is expected to be mid-year 2025.



Phase 1 – Initial Implementation

- Begins at 48 CFR Rule Effective Date
- Where applicable, solicitations will require Level 1 or 2 Self-Assessment

Phase 2

- Begins 12 months after Phase 1 start
- Where applicable, solicitations will require Level 2 Certification

Phase 3

- Begins 24 months after Phase 1 start
- Where applicable solicitations will require Level 3 Certification

Phase 4 – Full Implementation

- Begins 36 months after Phase 1 start
- All solicitations and contracts will include applicable CMMC Level requirements as a condition of contract award

Click to enlarge

CMMC will be rolled out in phases. Ultimately it will be expected to be in all contracts, which could be required as early as 2027.

If your organization is, or aspires to be, a contractor or subcontractor on DoD projects, you will need CMMC to be eligible for any new DoD contracts after the 48 CFR rule goes into effect. While you pursue certification and until you achieve it, you are considered an Organization Seeking Certification (OSC). The level of certification required will depend on the type of government data you will be working with.

CMMC Level 1 is required when Federal Contract Information (FCI) is provided or generated as part of a product or service contract. Look for CMMC Level 1 is required when Federal Contract Information (FCI) is provided or generated as part of a product or service contract. Look for FAR 52.204-21 Basic Safeguarding of Covered Contractor Information Systems in your contracts to see if it applies. Examples include contracts, financial information, performance reports, and process documentation. At this level, the OSC is self-assessed.

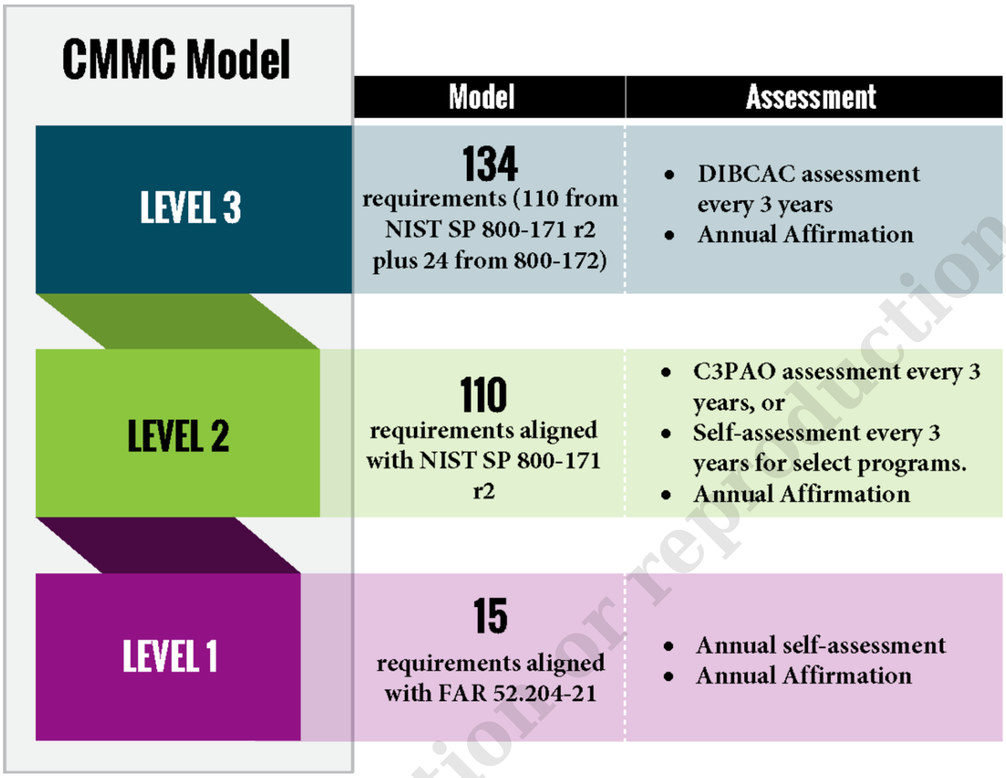
CMMC Level 2 is required for Controlled Unclassified Information (CUI), which could harm national security if leaked. Examples include technical drawings and inspection reports with military or space application. This level requires assessment by a third party.

CMMC Level 3 will be required for some prime contractors and will involve assessment by the DoD Industrial Base Cybersecurity Assessment Center (DIBCAC)after first passing a Level 2 Assessment from a C3PAO. Most DoD contractors will need to have a CMMC Level 2 Assessment performed by a third party. This can be a complex process. Fortunately, there are organizations and individuals with the expertise to help you through it.

Foremost is The Cyber Accreditation Body (The Cyber AB), the official accreditation body of the Cybersecurity Maturity Model Certification (CMMC) Ecosystem and the sole authorized non-governmental partner of the U.S. Department of Defense in implementing and overseeing the CMMC conformance regime. They authorize the assessment and consulting organizations that will help you on your journey, as well as the individuals who work for them. The Cyber AB Marketplace can help you find authorized providers of the services you need.

Assessment Services: C3PAOs

One service all OSCs will require is that of a CMMC Third Party Assessment Organization (C3PAO). C3PAOs are the only organizations authorized by The Cyber AB to perform CMMC Level 2 Assessments. You will need to engage one once you are ready to be certified.



CMMC Model

	Model	Assessment
LEVEL 3	134 requirements (110 from NIST SP 800-171 r2 plus 24 from 800-172)	• DIBCAC assessment every 3 years • Annual Affirmation
LEVEL 2	110 requirements aligned with NIST SP 800-171 r2	• C3PAO assessment every 3 years, or • Self-assessment every 3 years for select programs. • Annual Affirmation
LEVEL 1	15 requirements aligned with FAR 52.204-21	• Annual self-assessment • Annual Affirmation

Click to enlarge

The requirements to become a C3PAO include passing the same DoD cybersecurity assessment required of defense contractors, plus a review of Foreign Ownership and Control (FOCI), organizational background check, proof of insurance, and eventual certification in ISO 17020, Conformity Assessment. The individuals working for C3PAOs must also be certified by The Cyber AB.

Certified CMMC Assessors (CCAs) can perform CMMC Level 2 Assessments and their certification process inlcudes background checks, training, and practical experience.

Certified CMMC Professionals (CCPs) can perform CMMC Level 1 Assessments and can also assist on Level 2 assessments by assessing the Level 1 practices on those assessments, which helps them gain the experience toward becoming a CCA.

When looking for a C3PAO, you should verify they are legitimate. They should be listed in The Cyber AB Marketplace and should display The Cyber AB accreditation logo on their website. Then find out about their experience. Ask them how many Joint Surveillance Voluntary Assessments (JSVAs) they have conducted. JSVAs are CMMC Assessments conducted jointly with DIBCAC which will eventually translate to CMMC Level 2 per the 32 CFR rule after it goes into effect in December. Ask them what environment they used to pass their DIBCAC Assessment. Ask for references from other companies in your industry to ensure they understand your needs. Review the credentials of their CCAs and CCPs.

Consulting Services: C3PAOs and RPOs

Most OSCs will require consulting services to prepare for CMMC assessment. A consultant can determine if your organization is ready for assessment or help discover and remediate any gaps. For these services, you can engage either a C3PAO or a Registered Practitioner Organization (RPO).

C3PAOs frequently provide precertification consulting. Their CMMC expertise makes them valuable in this capacity; however, a C3PAO cannot legally provide both consulting and assessment services to the same OSC. If you choose one C3PAO to help you prepare for an assessment, you will need to choose another to perform the assessment.

Alternatively, you could choose an RPO for consulting. RPOs are registered with The Cyber AB and are knowledgeable about CMMC but have not gone through the rigorous process to be authorized as a C3PAO. They cannot perform assessments, but they can provide preassessment consulting, remediation services, and other CMMC-related guidance. The requirements to become an RPO include ownership by a U.S. person (citizen or lawful resident noncitizen), organizational background check, and commitment to comply with The Cyber AB Code of Professional Conduct. The individuals working for them, Registered Practitioners (RPs) and Registered Practitioner Advanced (RPAs), provide these consulting services.

When looking for an RPO, as with a C3PAO, make sure they are listed in The Cyber AB Marketplace. Look for experience with NIST SP 800-171 and other regulatory frameworks. If you are aware of gaps in your own organization, you might want to partner with an RPO that has a strong background in those areas.

External Service Providers: MSPs and MSSPs

CMMC also has requirements for External Service Providers (ESPs), a category of business partners that has been defined in the new draft CMMC 32 CFR Part 170 rule. An ESP is a third party organization that provides services to a business. Two key types of ESPs relevant to CMMC are Managed Service Providers (MSPs) and Managed Security Service Providers (MSSPs). An MSP manages a specific aspect of a customer's business such as website hosting and administration, routine and emergency maintenance and support, and billing or payroll functions. An MSSP is more specialized, providing cybersecurity services including constant systems monitoring, firewall and VPN management, threat prevention and incident response, gap analyses and vulnerability assessments, and regulatory compliance support.

MSPs and MSSPs are often confused with C3PAOs and RPOs. Although individual MSPs and MSSPs can be authorized C3PAOs or RPOs, they are not necessarily so. Regardless, MSPs and MSSPs can be helpful in supporting your CMMC journey — as long as you choose your providers carefully. There are clear benefits to engaging MSPs and MSSPs; it can be far more cost-effective to have a third party handle functions that are necessary to your organization but not your core focus, allowing your own staff to concentrate on the product or service that you provide for your customers. However, working with these providers also presents some challenges.

MSPs and MSSPs may need Federal Risk and Authorization Management Program (FedRAMP) authorization if acting as a Cloud Service Provider (CSP). Not all MSPs and MSSPs are aware of these requirements, so be careful to find a provider whose security priorities match your own. For MSSPs in particular, you should engage an organization with NIST SP 800-171 expertise; they will understand the level of compliance you need and help you maintain it, and they can help you prepare for an assessment, especially if the MSSP is an authorized C3PAO or RPO.

When considering an MSP or MSSP, ask them for their Shared Responsibility Matrix (SRM). If they don’t know what that is then the best course should be to find one that has an SRM and is aware of the requirements to support a company needing to meet CMMC L2. They will need to support you both before and during the actual assessment. Ask for references or case studies from clients similar to your organization who have achieved CMMC compliance. Their Shared Responsibility Matrix should map to NIST SP 800-171 requirements at the Assessment Objective level. Aside from CMMC considerations, you will want a provider who understands your business and is a good fit for your organization.

For more information on CyberNINES and how they can help your organization with CMMC Compliance: Get CMMC Compliant with CyberNINES | Expert Guidance Available