S|3 SPECIALIZED SECURITY SERVICES

THE PATH TO CMMC READINESS

PREPARING YOUR BUSINESS FOR DOD CYBERSECURITY STANDARDS

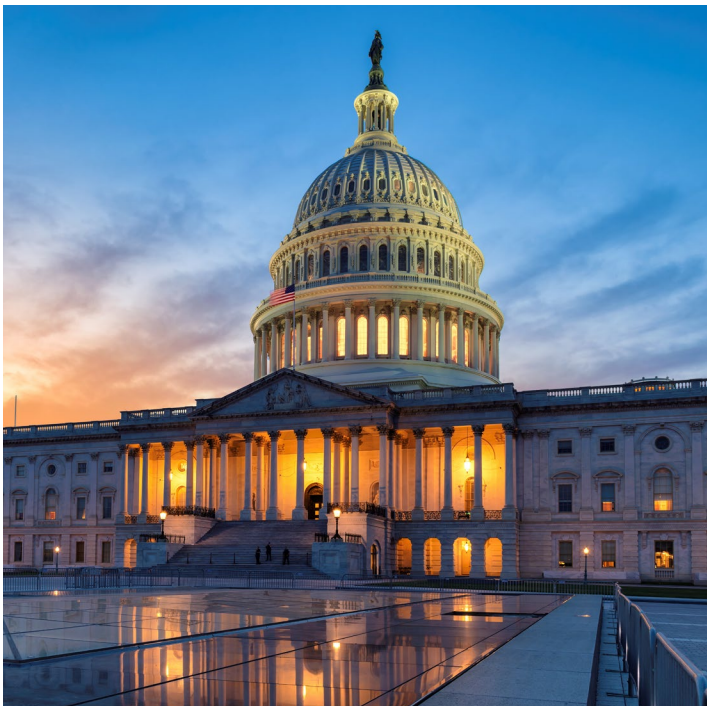
After many months of delay, the CMMC final rule was finally effective December 16, 2024.

While some companies may (correctly) presume that the impact of CMMC falls heaviest on prime DoD contractors and other core participants in the DoD mission, CMMC is farther reaching than many might expect. DoD estimates that over 150,000 small entities will be impacted by the program. In fact, roughly 220,000 companies overall will be subject to new CMMC rules.

So, what is the prevailing wisdom regarding how to best address CMMC? As always, preparation is key. If you're not yet looking at what CMMC could mean for your company, you need to start doing so. Immediately.

In this whitepaper, we will evaluate:

1. The Key Components of the Rule
   - » Phased Roll-Out
   - » Affirmation
   - » External Service Providers (ESPs)
   - » Plans of Actions and Milestones (POAMs)
2. Scoping
3. Technology and Business Risk
4. Industry Best Practices for Compliance



KEY COMPONENTS OF THE RULE

Let's start with what is in the CMMC final rule.

The original goal of the DoD in implementing CMMC was to hold contractors and subcontractors accountable for the cybersecurity requirements that were initially outlined in the Defense Federal Acquisition Regulation Supplement (DFARS) in 2017 (CFR 252.204-7012). All contractors must have implemented the requirements of NIST SP-800-171 or have Plans of Action and Milestones in place to achieve compliance. Signing a DoD contract with the 'DFARS 7012 clause' indicated a company was self-attesting to its compliance with the clause.

CMMC was born in 2019 based on the perception that such self-attestation was insufficient to protect DoD information. DoD required third-party certification to determine compliance, and contracts would specify the minimum certification contractors had to comply with to bid on a contract. CMMC included five maturity levels and 181 controls.

When CMMC 2.0 rolled out in November of 2021, the CMMC Maturity levels decreased from 5 to 3.

- **Level 1** is geared towards protecting Federal Contract Information (FCI), and the seventeen controls that comprise CMMC Level 1 were derived from controls in NIST-SP 800-171 (which adopted them from FAR 52.204-21). The rule allows for Level 1 entities to self-assess.
- **Level 2** is based on the remaining ninety-three controls from NIST SP 800-171 and is required to protect the confidentiality of Controlled Unclassified Information (CUI). Level 2 assessments must be performed by a certified third-party assessment organization (an authorized C3PAO).
- **Level 3** includes additional controls from NIST SP 800-172. Twenty-four enhanced controls from NIST SP 800-172 are required for Level 3. Level 3 assessments will be performed by the Defense Contract Management Agency (DCMA) Defense Industrial Base Cybersecurity Assessment Center (DIBCAC).

PHASED ROLLOUT

After the revision of DFARS 252.204-7021 (under separate rulemaking), the phased rollout of CMMC has started.

- **Phase 1**: – December 16, 2024: Level 1 and Level 2 self-assessments will be required in all new contracts as part of contract awards.
- **Phase 2**: – December 16, 2025: Will go into effect one year later and will include Level 2 Certification Assessments as a condition of the contract award.
- **Phase 3**: – December 16, 2026: Will begin one year after Phase 2 for Level 3 Certification Assessments.

One year following Phase 3 (December 16, 2027), the CMMC rollout will be complete with all CMMC requirements incorporated into new solicitations.

AFFIRMATION

One of the most consequential components of the CMMC final rule is the requirement for affirmation. The final rule requires that organizations affirm continuing compliance with the appropriate CMMC level. Organizations must have a senior official responsible for ensuring compliance with CMMC program requirements. This senior official will attest that the organization has implemented and will maintain implementation of all applicable CMMC security requirements for all in-scope systems. It's important to note that this affirmation requirement introduces a risk exposure for False Claims Act (FCA) violations. The FCA is a whistleblower law that could impose fines for a company's failure to comply with CMMC. If a company affirmed that they met all the CMMC requirements and a whistleblower alleged that they had not implemented all the controls, the government could initiate an FCA suit. If it is found that a company has violated the FCA, the law allows the government to recover significant damages plus civil penalties the whistleblower would share. Thus, it's imperative that the affirmation for CMMC be valid and accurate.

SUBCONTRACTORS AND EXTERNAL SERVICE PROVIDERS

Another significant component of DFARS and the CMMC is the flow down of requirements for subcontractors, a contractor's supply chain, and third parties that provide cloud services or other managed services.

The CMMC final rule requires that a contractor that uses an external service provider (ESP) that is not a cloud service provider (CSP) must document the services the ESP provides in their system security plan (SSP) and that those services used to meet CMMC requirements are assessed against the applicable controls as part of the contractor's assessment. As part of the DFARS clause, CSPs used in performing a DoD contract must be FedRAMP certified to the moderate baseline or equivalent. But the 'or equivalent' part of this clause has been historically vague. The DoD released a memo regarding establishing such equivalency. Its length and complexity testify to how critical the DoD considers external service providers to be when securing CUI appropriately.

PLANS OF ACTION AND MILESTONES

Another important aspect of the final rule is the use of Plans of Actions and Milestones (POAMs). POAMs are time-bound remediation efforts that contractors may have in place to correct a deficiency. It is worth noting that just implementing mitigating controls is not sufficient – POAMs should result in a fully implemented control, not just a reduction in risk. The final rule also specifies that POAMs are not allowable for any Level 1 control. While some Level 2 and Level 3 controls may have POAMs, they are limited in number and relate to low impact controls. Furthermore, a contractor must have at least 80% of the remaining controls implemented and POAMs should be no longer than 180 days in duration.

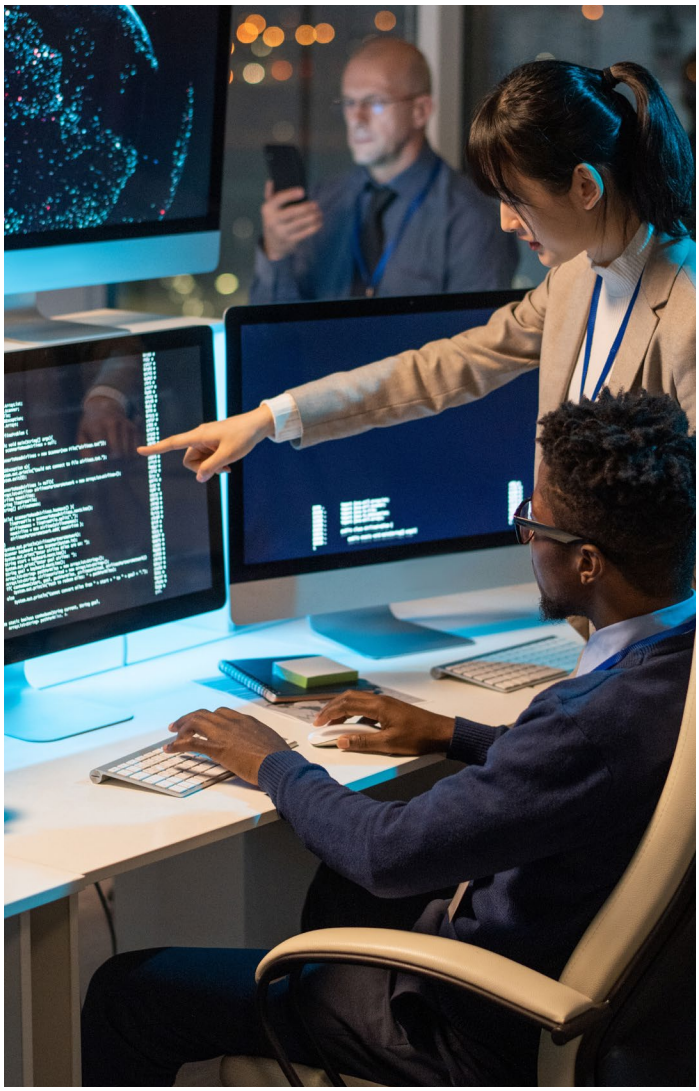
SCOPING

How does a company mitigate its CMMC risk? One way is to narrow the scope of CMMC. Scoping of the CMMC environment can limit the systems to which the CMMC controls must be applied. Especially in an organization with both commercial and DoD businesses, narrowing the scope of your CMMC environment to an enclave or isolated network can reduce the impact of your CMMC compliance efforts.

To narrow the scope of your CMMC environment, you must first determine where CUI is being stored, processed and transmitted. Doing this requires answers to the following questions:

- What are the data flows?
- Which systems interconnect?
- What functionality does the system provide?
- Since network segmentation can have both physical and logical components, what security systems need to be in place to secure the CUI environment?

The CMMC Assessment Scope documentation is a great tool that contractors should use to identify the assets and the asset categorization that will be in scope for their assessment. Determining which assets are CUI Assets, Security Protection Assets, Contractor Risk Managed Assets, Specialized Assets, or Out of Scope Assets is an important exercise in preparing for an assessment. S3 Security also recommends you ensure that documentation and implementation conform to the architectural design of the segmented environment and review those security controls at a defined frequency.



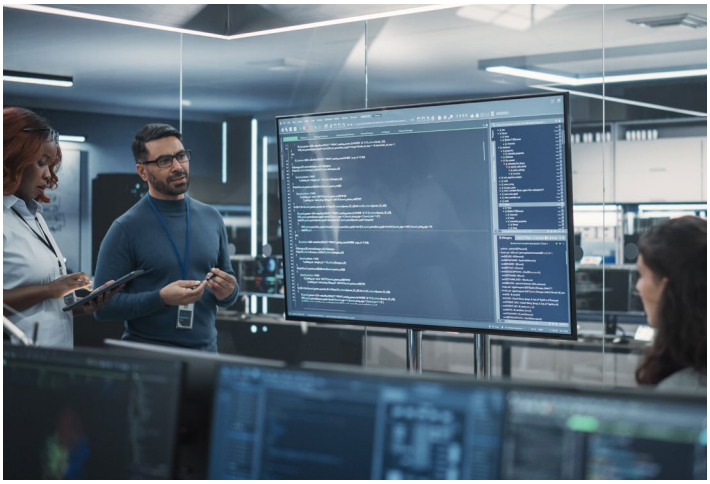
TECHNOLOGY AND BUSINESS RISK

Other risks that should be evaluated as part of your CMMC journey are technical debt and infrastructure upgrades. While logging and monitoring, network upgrades, access controls and vulnerability management programs are all part of a mature cybersecurity program, smaller organizations may need to invest in new technologies to meet the requirements of CMMC.

A gap assessment against the CMMC controls can help identify where a company will get the biggest bang for its investment in any additional technology required. Registered Practitioner Organizations (RPO) are specifically trained to perform readiness assessments and should be a resource for any organization planning for assessment or certification.

On the business side, it is critical to achieve executive buy-in and sponsorship for the efforts required to become CMMC compliant. Achieving compliance may divert both monetary and human resources from other projects. CMMC can cause change and present all the challenges that come with it. You may get pushback from business stakeholders who need help understanding the need for additional security controls. Therefore, a commitment from leaders to devote the time and energy to implementing the controls and communicating the reasons for the effort is crucial.

Other business considerations relate to companies entering DoD contracting for the first time or who are part of the supply chain that now requires compliance. Different rules and regulations for defense contractors require companies to assess their appetite for additional scrutiny of their cybersecurity programs from the government or prime contractors. While CMMC and DFARS exceptions for Commercial Off the Shelf (COTS) products may apply to a company's product, expanding a line of business in the defense space can open new markets, create a new customer base, and increase revenue. For some, the offsets associated with increased cybersecurity requirements are worth the extra effort.



BEST PRACTICES

How does an organization navigate through the morass of acronyms and decide if CMMC compliance is or should be part of its cybersecurity strategy?

- Perform a gap assessment to get a sense of where you stand based on your evaluation of the controls.

- Engage a third party – specifically an RPO. An RPO will have trained experts on staff to determine where your gaps are and how best to remediate them. Engagements with RPOs can be for a gap assessment or extend to having that RPO perform some or all configurations and documentation as an implementation partner.

- Have open and honest conversations with your business advisors and internal leadership. Do you have the right staff, budgets, documentation, business partnerships, legal counsel and customer experience to support your CMMC endeavors? If the answer is yes, do not hesitate to start your CMMC compliance journey as soon as possible.

ENSURING CMMC COMPLIANCE WITH STRATEGIC GUIDANCE AND SUPPORT

As the Department of Defense (DoD) tightens the reins on cybersecurity through the Cybersecurity Maturity Model Certification (CMMC) program, the urgency for DoD contractors and their supply chains to safeguard sensitive data has never been more critical to their success. The newly unveiled CMMC rules mark a significant shift in how defense information security is managed and enforced, impacting a broad spectrum of companies.

Your readiness for CMMC compliance is not just a regulatory mandate but a strategic advantage in the defense sector. Set your company apart and prepare for the evolving demands of DoD contracts by establishing immediate understanding and implementation of the requirements of CMMC.

S3 Security is a both a CMMC RPO and an authorized C3PAO. We stand ready as your ally in this critical journey. With extensive expertise in navigating the intricate details of the CMMC framework – from phased rollout to the specific requirements of each CMMC level – we are prepared to guide you through every step of the compliance process. Our approach is designed to simplify the complexities of CMMC, ensuring that your business not only meets but exceeds the DoD's expectations for data security and defense readiness. We understand the challenges of adapting to new regulations, especially for small entities and subcontractors now facing the extensive reach of CMMC. Our team specializes in crafting tailored solutions that address the unique aspects of your business, from scoping and technological upgrades to full-scale compliance strategies.

By partnering with S3 Security, you gain access to a wealth of knowledge and resources to mitigate risks, enhance your cybersecurity posture and achieve compliance with confidence. We are committed to helping you navigate the CMMC landscape with comprehensive planning, actionable insights and continuous support.

Preparation for CMMC is critical. **Contact us today** to start your CMMC compliance journey and secure your position as a trusted DoD contractor. Doing so will allow you to embrace the challenge of CMMC with the peace of mind that comes from having a seasoned advisor by your side who can ensure your success in the ever-evolving world of defense contracting and cybersecurity.

Sources:

1. *CMMC Final Rule*
2. *FedRAMP Equivalency memo*
3. *CMMC Scoping Guide*
4. *FAR 52.204-21*
5. *NIST 800-171r2*
6. *NIST 800-172*