SYSTEMS
engineering

WHAT TO KNOW ABOUT CMMC:
Cybersecurity Maturity Model Certification

The increasing theft of intellectual property and sensitive information is at an all-time high and a growing threat to our national security. The 2021 ransomware attacks on the largest gasoline pipeline and meat producer in the U.S. are clear evidence of these increasingly frequent and complex cyberattacks. In the interest of protecting American ingenuity and safeguarding national security information against these cyberattacks, the U.S. Department of Defense (DoD) developed the Cybersecurity Maturity Model Certification (CMMC) program to strengthen security within its Defense Industrial Base (DIB). Here's what to know about CMMC and the IT security hygiene your organization may need to address.

TABLE OF CONTENTS

What is the Cybersecurity Maturity Model Certification?

In November 2020, the DoD published its initial vision of the CMMC program (CMMC 1.0) derived from multiple cybersecurity standards, frameworks, and references. Shortly after, in March 2021, the DoD initiated an internal review, informed by public comment, to refine the policy and program implementation. On November 4, 2021, the U.S. DoD announced the completion of their internal assessment and released the strategic direction for the CMMC program, dubbed CMMC 2.0. The refined program structure and requirements are designed to verify the ability of Defense Industrial Base (DIB) contractors to implement security requirements specified in NIST SP 800-171 Revision 2, and to "protect Controlled Unclassified Information in Nonfederal Systems and Organizations."

The CMMC 2.0 framework is organized into a three-tier model that requires companies entrusted with national security information to achieve a progressively advanced CMMC level, depending on where the Controlled Unclassified Information (CUI) or Federal Contract Information (FCI) to be protected is processed, stored, or transmitted. This protection also applies to information shared and exchanged with subcontractors in a multi-tier supply chain. The flow down of CMMC requirements to subcontractors is necessary to respond to threats that reach even the lowest supply chain tiers.

Both CUI and FCI include information created, collected, or received, by or for the Government, that is not intended for public release. Specifically, CUI must also be safeguarded at every stage of existence (in use, storage, and transmission) until it is destroyed, disseminated, or decontrolled.

Level 1 **FOUNDATIONAL**	Annual Self-Assessment	17 Security Controls and Processes
Level 2 **ADVANCED**	Annual Self-Assessment or Triennial Third-Party Assessment	110 Security Controls and Processes
Level 3 **EXPERT** (under development)	Triennial Assessment by DoD	110+ Security Controls and Processes

Once CMMC is fully implemented, certain DoD contractors that handle sensitive unclassified Department information will be required to achieve a particular CMMC level as a condition of contract award. Depending on the level (Foundational, Advanced, or Expert), an authorized and accredited CMMC 3rd Party Assessment Organization (C3PAO) will conduct a verification of the DIB company's cybersecurity posture and implementation of the required processes and practices. Upon completing the assessment, an independent CMMC Accreditation Body (AB) will award the DIB company the appropriate CMMC level certification. The contractor's CMMC level is then stored in the Supplier Performance Risk System (SPRS). The DoD will use the SPRS to verify a contractor's certification level before awarding a contract, where required. The assessments are valid for three years and must be renewed every three years to remain current.

▲ BACK TO TOP

CMMC IS COMING IN 2023
START PREPARING NOW!

Why did the DoD create CMMC?

To best understand the current CMMC Framework and Assessment methodology, it is helpful to know the origins of this rule. **Protection of unclassified information through minimum cybersecurity standards within the DoD supply chain has been in effect on DoD contracts since 2013.** The regulations relied on the DIB contractors to self-attest that they will or have implemented the security requirements of the FAR 52.204-21 and DFARS 252.204-7012 clauses upon submission of a contract offer. These regulations fell short in the DoD's ability to assess and verify a contractor's compliance with the protection of government information before the contract was awarded.

The FAR clause mandates protection of any Federal Contract Information not intended for public release, provided by or generated for the Government.

The DFARS clause requires a DIB contractor to protect Controlled Unclassified Information in Nonfederal Systems and Organizations by implementing the up to 110 security controls under NIST SP 800-171 Revision 2 DoD Assessment Methodology.

▲ BACK TO TOP

Why is the CMMC framework important?

Suspicion of non-compliance from the contractors to implement the basic safeguarding and security requirements was realized when DIB contractors reported 248 security incidents to the DoD Cyber Crime Center between 2015 – 2018. These numbers got the attention of the Secretary of Defense, who subsequently requested an audit by the DoD Inspector General (IG) to determine whether contractors were protecting CUI on their networks and systems. The 2019 IG report findings indicated that DoD contractors did NOT consistently implement the mandated requirements. The report emphasized that "malicious actors can exploit the vulnerabilities of contractors' networks and systems and exfiltrate information related to some of the Nation's most valuable advanced defense technologies." The IG report recommended that the DoD take steps to allow for verification of a contractor's ability to protect CUI, which resulted in the CMMC Framework and Assessment Methodology.

▲ BACK TO TOP

Who needs to comply with CMMC?

The CMMC requirement applies to **any company or group within the DIB sector that receives, handles, or processes FCI or CUI from the DoD.** A DIB contractor that does not handle information deemed critical to national security (level 1 and a subset of level 2) will be required to perform an annual self-assessment and a senior company official will need to submit an attestation form confirming compliance. These acknowledgments of compliance will likely need to be submitted to the SPRS as well.

Contractors that manage information critical to national security (a subset of level 2) must align with the 110 security practices of NIST SP 800-171 Revision 2, and undergo third-party assessments from accredited C3PAOs. For the most critical defense programs requiring Level 3 certification, contractors will be accountable to a subset of the NIST SP 800-172 requirements, which are a supplement to NIST SP 800-171 Revision 2 and currently under development. The DoD intends for Level 3 cybersecurity requirements to be assessed by government officials, rather than accredited C3PAOs. The assessment requirements are also currently under development.

▲ BACK TO TOP

When will CMMC changes be enforced?

The original timeline for implementation of CMMC 1.0 was based on a five-year phased rollout strategy. Now that the DoD has developed CMMC 2.0, the Department intends to suspend any CMMC piloting efforts until the forthcoming rulemaking process is complete and in effect.

While rulemaking efforts are underway and ongoing, it would be prudent for contractors to move towards improving their security posture NOW to avoid the potential scramble for compliance when the forthcoming rules go into effect.

Additionally, the DoD is exploring opportunities to provide incentives for contractors who voluntarily obtain the proper CMMC level ahead of full implementation of the CMMC 2.0 requirement.

▲ BACK TO TOP

How to prepare for a CMMC assessment?

The CMMC framework and assessment is relatively new and, for many DoD contractors and sub-contractors, it can feel like a daunting process. The good news is that Systems Engineering has been working within the NIST 800-171 Revision 2 framework and other compliance regimes for years. We fully understand the cybersecurity processes and practices necessary to become and remain CMMC compliant.

We're ready to help your organization prepare for this new assessment and certification. It all begins with a CMMC Gap Analysis to compare your organization's policies, procedures, and technologies to the controls required to achieve the appropriate CMMC Level. The analysis is performed using a combination of interviews with your staff, a review of any existing policies, and when appropriate, a review of the technical controls you have in place. This analysis will identify any gaps you may have, along with recommendations and solutions to close those gaps. The analysis output will also provide information on controls you are currently meeting for a complete picture of your current security posture.

Having confidence in your security controls will be essential as you move forward with your CMMC C3PAO or self-assessment. For more information on scheduling a CMMC gap analysis with Systems Engineering, please select the link below.

▲ BACK TO TOP

REQUEST A CMMC
GAP ANALYSIS

If you have any questions on the CMMC readiness process, customers please reach out to your account manager, call us at 888.624.6737, or email us at info@systemsengineering.com.