WHAT IS POA&M?

With the implementation of CMMC 2.0, the DoD will allow companies to receive contract awards with a limited-time Plan of Actions and Milestones **(POA&M)** in place to complete CMMC requirements. A baseline number of requirements must be achieved prior to contract award, with the remaining subset to be addressed in a POA&M within a clearly defined timeline. Critical and highly weighted controls are not eligible for a POA&M.

The allowance of POA&Ms means a DIB company that is not currently meeting all requirements of NIST SP 800-171 will be allowed extra time to implement. However, the POA&M must be completed and closed within 180 days of the initial assessment or the conditional certification will expire.

Once CMMC 2.0 goes live in 2025, the required CMMC level for contractors and sub-contractors will be specified in the solicitation and in Requests for Information (RFIs), if utilized. Depending on the nature of the contract award, you may be required to demonstrate either level 1 or level 2 CMMC compliance right away.

WE CAN HELP

TotalCare IT can help your organization prepare for CMMC by walking you through an alignment to the NIST standards.

We will create a roadmap for you that clearly outlines where your organization is currently meeting NIST SP 800-171 controls and where you need improvement.

Then, as part of our ongoing compliance management service, we help you implement all the controls in your organization. We can also help you create POA&Ms if needed and walk your organization through self-assessments.

Implementing security controls does not happen overnight. If your DIB organization hasn't started preparing for the rollout of CMMC in 2025, what are you waiting for? Give us a call today to get started!

TotalCare IT
(208) 881-9713
www.TotalCareIT.net/cmmc

TotalCare IT
We Keep People Working

WHAT THE HECK IS CMMC COMPLIANCE?

CMMC 101 for Defense Industrial Base Companies and their Subcontractors

TotalCare IT
We Keep People Working

WHAT IS CMMC?

The upcoming Cybersecurity Maturity Model Certification (CMMC) from the Department of Defense (DoD) makes the adoption of NIST SP 800-171 mandatory for the Defense Industrial Base **(DIB)**. This includes both prime contractors and subcontractors.

NIST SP 800-171 is a publication that lists specific security controls for *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*. It puts forth a minimum standard of cybersecurity protections for businesses working with the Federal Government to ensure Federal Contract Information **(FCI)** and Controlled Unclassified Information **(CUI)** are secure.

CMMC is designed to give the DoD a way to enforce the protection of national security information and American ingenuity.

CMMC only applies to DIB organizations. DIB organizations enable research and development of military weapons systems, subsystems, and components or parts. DIB companies perform under contract to the Department of Defense.

CMMC 2.0 is the newest version of the program and has 3 levels of maturity, with each level increasing in robustness of cybersecurity controls, processes and procedures.

CMMC Level 1 is 'foundational' cyber protection and requires the implementation of 17 controls from NIST SP 800-171. In addition, an annual self-assessment is required. This level is mainly for a DIB company that does not process, store, or transmit CUI on its unclassified network, but does process, store or handle FCI.

Level 2 is referred to as 'Advanced' and includes all 110 controls from NIST SP 800-171. Compliance is measured with a yearly self-assessment for level 2, or, for contracts with information critical to national security, a triennial third-party assessment by a Certified Third-Party Assessor Organization (C3PAO). For scoring, controls will be weighted at 1, 3, or 5 points depending on risk. Each control not met is points docked. The highest possible score is 110 and the lowest could be in the negatives.

Level 3 builds on the previous two levels by requiring full implementation of all 110 controls from NIST SP 800-171 plus controls from NIST SP 800-172 (*Enhanced Security Requirements for Protecting Controlled Unclassified Information*). This 'Expert' level advances to a triennial assessment led by government officials.

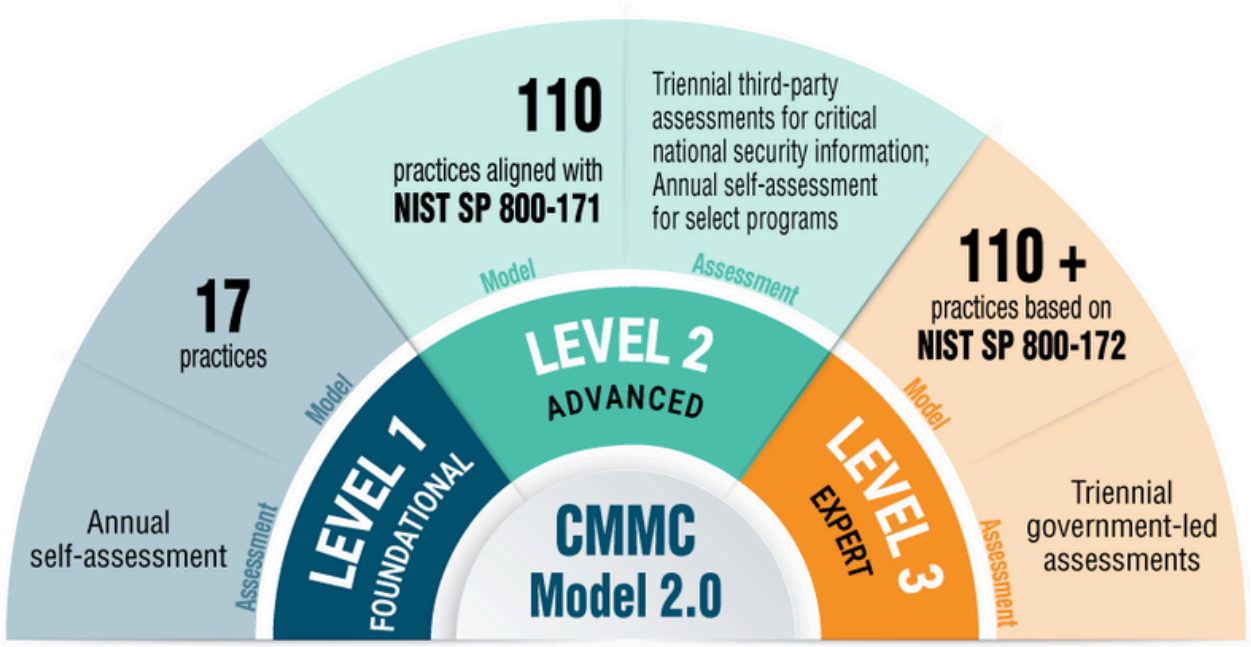

Image from ControlCase