



Cybersecurity Maturity Model Certification (CMMC)

What it means for your business and how to tackle it, step-by-step.

What is CMMC?

The Cybersecurity Maturity Model Certification (CMMC) was introduced by the US Department of Defense (DoD) on January 31, 2020. The CMMC is a new unified standard that aims to implement cybersecurity for over 300,000 companies in the defense industrial base (DIB) supply chain.

Prior to the introduction of CMMC, defense contractors were responsible for implementing, monitoring, and certifying the security of their own IT systems and any sensitive information transmitted by or stored on these systems. With the rollout of CMMC, contractors must now work with third-party auditors to assess and verify their compliance with CMMC practices.

The CMMC model contains five levels of cybersecurity maturity (basic to advanced/progressive) with each level consisting of a different set of processes and practices.



Key Facts:

- Failure to meet the required CMMC maturity level negates your chances at landing government contracts.
- Right now, around 300,000 vendors must comply with CMMC to continue business. The DoD estimates that only 10% of them meet the standard, as released, on January 31, 2020.
- The DoD plans to release around 20 RFPs this year that will require CMMC when the contract is awarded.
- By FY26, all new DOD contracts will contain CMMC requirements. All DoD contractors should already be at Level 1 as that parallels some existing requirements. Level 3 is going to be the level that most contractors need to achieve to be relevant.
- Things have changed some: under the new requirements, you must demonstrate that you are certified prior to the final award. Previous standards allowed you to identify the areas of needed improvement and put them on a Plan of Action and Milestones (POAM) to address later.