



Cybersecurity Maturity Model Certification (CMMC) - Frequently Asked Questions

Who will need CMMC?

All companies conducting business with the Department of Defense, this includes DoD contractors and subcontractors

Can I Self Certify?

No.

DCAP already helped me to meet NIST SP 800-171, what does this mean for me?

If you have implemented all 110 controls of NIST 800-171 you are well on your way to being ready for a Level 3 CMMC certification. As a client of DCAP you were likely handling controlled unclassified information (CUI) and will then at a minimum need to be certified to Level 3. There are 20 additional controls that CMMC v1.0 has included for Level 3 certification that you will need to implement. Once you are ready and all of the controls have been implemented, you will then need to be certified by an approved assessor. (Please note that there are not yet any approved assessors as they are just beginning to go through the training processes required by the CMMC Accreditation Body)

Who will perform the CMMC Assessment?

Assessments and Certification will typically be performed by an accredited 3rd party assessment organization (C3PAO's). However, per the CMMC website, some of the higher-level assessments may be performed by the Defense Contract Management Agency (DCMA) or the Defense Counterintelligence and Security Agency (DCSA).

When can I request certification?

The CMMC accreditation body is currently working to establish and train certifiers. Once the certification organizations are identified by the CMMC accreditation body, you will coordinate directly with the certifier to request and schedule your CMMC assessment based on the specific level of certification your company will be required to achieve.

Who will be able to see my assessment results?

Your certification level will be public and visible to the DoD, but any specific findings will not be released publicly.

What happens if an organization is compromised after being certified to CMMC?

The organization will not lose their certification. However, depending on the circumstances surrounding the compromise and the direction of the government program manager, an organization may be required to be recertified to CMMC.



Cybersecurity Maturity Model Certification (CMMC) - Frequently Asked Questions

How will an organization know what the CMMC level is required for a contract?

The required CMMC level will be contained in sections L & M of the Request for Proposal (RFP).

What is the cost of certification?

The full cost of CMMC certification is unknown but will likely align with the level requested. Certification cost will be considered an allowable, reimbursable cost and should not be prohibitive. For contracts that require specified levels of CMMC, you may be disqualified from participating if your organization is not certified at the time in which the contract is awarded. Per the DoD, the goal is for CMMC to be cost-effective and affordable for small businesses to implement at the lower CMMC levels.