Cybersecurity Maturity Model Certification (CMMC) Common Questions and Answers

Question: What is CMMC?

Answer: CMMC is a new standard that will take the place of National Institute of Standards and Technology (NIST) 800-171 on Department of Defense (DoD) contracts. CMMC is not entirely derived from NIST 800-171; rather, it builds upon it along with many other regulations to create five levels of certification that will better reflect the type of cybersecurity that a contractor will need to attain for a particular DoD contract.

Question: Why was CMMC created?

Answer: DoD is planning to migrate to the new CMMC framework in order to assess and enhance the cybersecurity posture of the Defense Industrial Base (DIB). The CMMC is intended to serve as a verification mechanism to ensure appropriate levels of cybersecurity practices and processes are in place to ensure basic cyber hygiene as well as protect Controlled Unclassified Information (CUI) that resides on the Department's industry partners' networks.

Question: Is the CMMC framework available to the public?

Answer: Yes, it's available for download at https://www.acq.osd.mil/cmmc/.

Question: Is CMMC and NIST 800-171 different?

Answer: Yes, many of the same controls that are in NIST 800-171 will be included in CMMC along with controls from other standards such as International Organization for Standardization (ISO), Federal Risk and Authorization Management Program (FedRAMP), and various NIST frameworks. CMMC also requires a 3rd party audit in order to gain certification, whereas NIST 800-171 is a "self-certification".

Question: Can you self-certify with CMMC?

Answer: No, an audit was preformed by the DoD and they assessed 10 contractors with DoD contracts worth at least $1 million and found the security controls they had implemented to protect DoD CUI were not consistently implemented. Each DoD contractor was found deficient in as many as 8 of the 10 basic security controls.

Question: How does NIST 800-171 tie into CMMC?

Answer: Existing DoD contracts that contain the 252.204-7012 Defense Federal Acquisition Regulation Supplement (DFARS) clause will still require your organization to provide documentation proving compliance with 800-171. We don't know if Contracting Officers will be asked to modify active contracts to swap CMMC and 800-171. This may end up being a per-contract decision. CMMC is different than NIST 800-171, but the controls can be mapped from 800-171 to the levels of certification within CMMC.

Cybersecurity Maturity Model Certification (CMMC) Common Questions and Answers

Question: What if we do not handle CUI? Will we still need to be certified?

Answer: Yes, all companies doing business with DoD will need to obtain CMMC. Even if you are a subcontractor.

Question: Which level of CMMC will I need to be certified in?

Answer: We're not sure yet. This will depend entirely upon what level of certification your contract requires and the sensitivity of the information you handle. We can say this: ALL companies handling CUI can expect to certify at a CMMC Level 3 certification (which will include all 110 controls from NIST 800-171). Levels 1 and 2 will be required of companies that handle Federal Contract Information (FCI) while Levels 4 and 5 will be required among a small subset of contracts handling extremely sensitive information. The safe bet at this point is to shoot for a Level 3.

Question: What are steps I can take now to prepare for CMMC certification?

Answer: Number One, get NIST 800-171 documentation out of the way. This will get you through many of the CMMC Level 3 requirements and keep you compliant with the current DFARS clause.

Number two, identify the remaining CMMC requirements you expect to be subject to (future RFPs or your prime will determine what level you need to meet). Be ready to address any gaps you find and implement solutions to remediate them since CMMC requires 100% implementation. Hire a reputable cybersecurity firm like First Team Cyber to help with pre-audit support.

Number three, identify an authorized 3rd party to audit your assessment and give you a certification for the level you need. There are currently no companies that are accredited to give an official CMMC audit and certification, but the CMMC Accreditation Body (AB) has indicated a small number will be available soon.

Question: How often do we need to re-certify?

Answer: Most CMMC levels will require recertification once every 3 years.

Question: How much will this whole process cost me?

Answer: We can't say for sure. That depends entirely on the market. Ms. Katie Arrington and her team have made it clear that they are trying to keep the cost down and are encouraging industry to automate as much of this process as possible. First Team Cyber is taking that approach and applying it to our business model. Our services are cost-effective and practical. Our Consultants can get you your NIST 800-171 documentation ready, and when the time comes, we'll migrate you to the new CMMC standard at no additional cost.