FIRST TEAM CYBER

Federal Contractors Guide to Passing CMMC Audits

When is it coming?

CMMC was signed into law January 2020 and will go into full effect by fall 2020. Third-party assessment Organizations (3PAOs) maybe trained as early as April-May 2020 timeframe. The CMMC will appear in Requests for Information (RFI's) by June 2020 and Requests for Proposal (RFP's) as early as August-September 2020.

What is the impact of noncompliance?

You lose your ability to compete for or retain government contracts. As a part of the new DoD acquisition process, companies need to comply with DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, which requires DoD Contractors to implement National Institute of Standards and Technology (NIST) Special Publication (SP) 800 series, "Protecting Controlled Unclassified Information (CUI) in Nonfederal Systems and Organizations".

Why is the government doing this?

Cybersecurity is now the leading source of risk for the US. In addition to government entities, supply chain partners are being attacked. This means the government needs to secure everyone they work with to keep national data, IP and infrastructure safe.

What does it mean for my business?

All companies doing business with DoD will be required to obtain CMMC--even subcontractors.

Do I need a third-party auditor?

Yes—federal contractors CANNOT self-certify. The DoD will no longer take your word that appropriate cyber security protocols are in place. Instead, the government mandates that formal audits by qualified C3PAOs will be required for CMMC certification and, by extension, to do business with the government.

Can I approach CMMC as a basic checklist exercise?

No. Most of the 171 plus security requirements deal with business processes unique to the contractor being audited. A cookie cutter approach will likely fail under scrutiny by government auditors.

What kind of expertise is required to pass?

Since the government is taking cybersecurity seriously, deep expertise is needed. Recently, for example, an audit performed by the DoD assessed ten contractors with DoD contracts worth at least $1 million. The government found that their implemented security controls to protect

DoD CUI were not consistently implemented. Each DoD contractor was found deficient in as many as eight of the ten basic security controls.

How do NIST standards play a role?

Many of the same controls that are in NIST 800-171 will be included in CMMC but there are key deviations. CMMC compliance will also rely on 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".

Existing DoD contracts that contain the 252.204-7012 DFARS clause will still require your organization to provide documentation proving compliance with NIST. 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.

What should I be doing now and in the next months to prepare?

Federal contractors should:

- ❑ Get NIST 800-171 documentation out of the way. This could help you meet CMMC Level 3 requirements and keep you compliant with the current DFARS clause.
- ❑ Identify your maturity level and the remaining CMMC requirements that may apply to you. Be ready to address any gaps you find and implement solutions to remediate them since CMMC requires 100% implementation.
- ❑ Hire a reputable cybersecurity firm to help with pre-audit support to get you ready for an impending audit.
- ❑ 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.

About First Team Cyber

First Team Cyber can protect your business, ensuring you're not shut out from government contracts due to a failed audit. Founded by Navy veterans with 60 combined years of experience as auditors and auditees, we have sweated hundreds of audits. And we've chosen cyber security as our mission because we know what our country faces. First Team Cyber isn't something to do, it's an extension of our patriotic obligations.

First Team Cyber offers a free initial consultation to help you prepare and pass your CMMC audit. Contact our team today and take the first step so that together, we can ensure you're not just compliant, but also successful and secure.

Contact us at info@firstteamcyber.com or 877-684-TEAM (8326).

FIRST TEAM
CYBER