CMMC Consulting Services for DoD Contractors

ARTICLE 05.08.20   DEAN DORTON

Prepare for Certification with Our CMMC Readiness Assessment

In an effort to focus on security and resiliency, the Department of Defense (DoD) is working with various industries to enhance the protection of the following types of unclassified information within the supply chain:

https://deandorton.com/wp-content/uploads/2020/05/Security-lock-300×168.jpg

Federal Contract Information (FCI)

https://deandorton.com/wp-content/uploads/2020/05/Digital-fingerprint-300×169.jpg

Controlled Unclassified Information (CUI)

FCI is information provided by or generated for the Government under contract not intended for public release. CUI is information that requires safeguarding of dissemination controls pursuant to and consistent with laws, regulations, and government-wide policies.

DoD Approach

Contractors working with FCI or CUI will be required to be certified based on one or more of the five CMMC maturity levels. The levels are as follows:

https://deandorton.com/wp-content/uploads/2020/05/CMMC-blog-post-graphics-2-2.png

At a minimum contractors will need to be Level 1 certified. If a contract requires a higher level of certification, the contractor is required to meet that level and all lower levels. The levels build on one another. The level requirement will be specified in Requests for Information (RFI) and Requests for Proposals (RFP) coming from the DoD later this year.

CMMC Timeline

A CMMC timeline has been established with important milestones scheduled in mid to late 2020. These milestones were established prior to the COVID-19 pandemic and may be revised. For now, the guidance we have is:

https://deandorton.com/wp-content/uploads/2020/05/CMMC-blog-post-graphics-22-1-e1588955821671.png

Get Prepared with Our CMMC Consulting Services

Every DoD contract is different. However, the one thing all new contract RFPs and RFIs now have in common is that CMMC compliance is mandatory. Companies that are not compliant will automatically be disqualified. To make the most of your time, efforts, and resources, count on our CMMC consultants to help efficiently guide you through evolving CMMC regulations. Here's a step-by-step approach to the CMMC readiness process to start:

- **Know the CMMC level your organization needs to comply with:** It's an obvious first step, but a vital one. Any certification above Level 1 will require a more significant time and cost investment. While it's beneficial to be prepared with certification before an RFP arrives, it's not practical (or cost effective) to guess which level will be required for an upcoming contract. One option would be to reach out to your organization's DoD contract representative for some idea about what to expect from a CMMC Level standpoint.

- **Prep for an internal readiness assessment:** Start by reviewing the CMMC documentation provided for the various levels to ensure you have the appropriate information. Consider whether your organization has an established system security plan (SSP) that meets NIST 800-171 standards. Having this in place will help you assess risks, and to be in a ready cyber security posture to expedite the certification process.

  Next, **identify your scope**. To help make certification smoother and more efficient, consider isolating the relevant departments of your organization into its own network. Exclude unrelated departments like sales and marketing where FCI and CUI **will not** be stored, processed, or transmitted.

- **Review or establish key policies, processes, and plans:** Establishing documentation is key in CMMC certification, and shows your commitment to cyber security.

Indicate the high-level guidelines your organization will adhere to **(policies)** that communicate vision and the values upheld in day-to-day operations. Show how individuals will perform specific activities **(process)** that satisfy policies. And describe how you will implement, schedule, and maintain **(plan)** those processes.

Identify **key people** responsible for implementing your SSP, as well as the **tools** that will enable them to securely communicate and share information, collect data, and store the sensitive information.

- **Perform an internal pre-assessment:** This vital step in the process will help identify and collect evidence regarding important gaps in your organization's CMMC readiness. Communicate with key personnel about your state of compliance as it stands for the CMMC level you seek certification. From there, you can take the missing controls and policies to develop your **plan of action and milestones** (POAM) to establish what actions need to be implemented, and the period of time expected to complete.

- **Remediation:** Simply put, it's time to address and remedy the gaps where your internal assessment showed vulnerabilities. Build additional time into your POAM if the results indicate extensive network development is necessary.

- **Step and repeat:** Before attempting certification, ensure that your organization has implemented all recommended practices revealed in your internal assessment.

- **Hire a Certified Third-party CMMC Assessor Organization (C3PAO):** While internal exploration is key in preparing for the appropriate CMMC level your organization needs to achieve, self assessments are not acceptable for certification. Choose a C3PAO with experience in your industry and fits within your budget.

If you have any questions regarding how to prepare for CMMC requirements feel free to contact Kevin W. Cornwell at 502.566.1011 or kcornwell@ddaftech.com or Amy Justice at 859.425.7793 or ajustice@ddaftech.com.