ARTICLE

EXOSTAR®
We build trust.

Top Five Concerns about Securing the DoD Supply Chain:

NIST 800-171, CMMC, and What the DIB Really Wants to Know.

The release of version 1.0 of the Cybersecurity Maturity Model Certification (CMMC) adds to the complexity of cybersecurity requirements facing members of the defense industrial base (DIB). Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012 already mandates compliance with the 110 security controls found in NIST Special Publication 800-171 for any company in the U.S. Department of Defense supply chain that handles or stores Controlled Unclassified Information, or CUI.

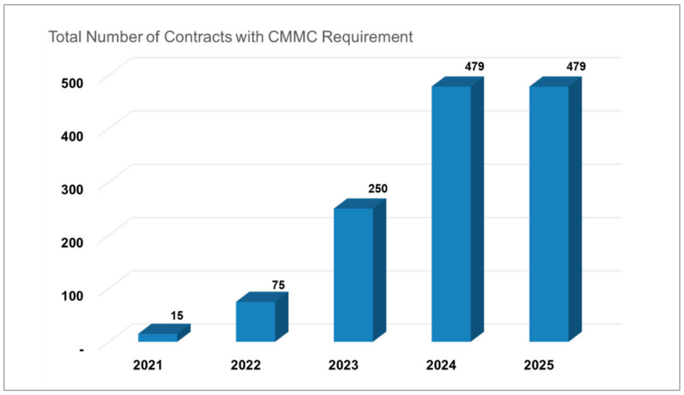
Are DIB organizations required to comply with both NIST 800-171 and CMMC?

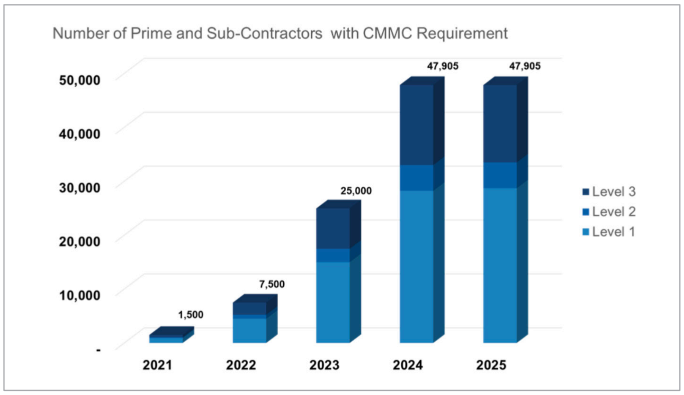
To help bring clarity to a confusing situation for DoD prime contractors and lower-tier suppliers, Exostar led a webinar, “CMMC is here, but 800-171 isn’t going away – know what to do?” The event featured insight and expertise from Darren King, Director and Senior Information Security Officer at the Defense Contract Management Agency (DCMA), and J.C. Dodson, Global Chief Information Security Officer for BAE Systems.

The live program offered a question-and-answer session on the aspects of NIST 800-171 and CMMC that mattered most to the audience – whether questioners represented a large enterprise with mature cybersecurity protocols, or a small-to-medium business with few IT resources inexperienced with CUI. Discussion focused on five key topics.

1. CMMC Timing

Many questions boiled down to a variant of, “*When will CMMC affect us?*” CMMC’s rollout begins in 2020, with the requirement first appearing in ten Requests for Information (RFIs), and then in ten Requests for Proposals (RFPs) for DoD programs of varying size, scope, and sensitivity. Approximately 1,500 members of the DoD supply chain are anticipated to be affected initially. The DoD expects the transition from NIST 800-171 to CMMC to continue until 2026, when CMMC will be incorporated into all DoD RFIs, RFPs, and programs. At that time, certification will impact all members of the DIB as a requirement.



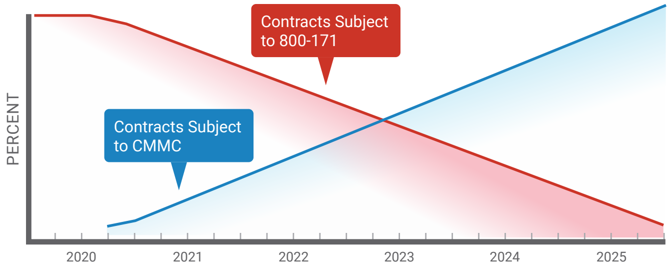


CMMC will not be inserted retroactively into ongoing programs. Only new DoD programs and those up for renewal will be subject to it. For individual companies, the precise timing over the next five-plus years to obtain CMMC certification depends on the lifecycles of the contracts they currently support, and the new opportunities on which they bid or participate.

2. Addressing the Coexistence of NIST 800-171 and CMMC

A related set of concerns focused on the interplay of NIST 800-171 and CMMC: “*Where do we start? Do we still need to comply with NIST 800-171, or should we jump right to CMMC?*” Given the transition schedule to CMMC, NIST 800-171 will remain relevant for the foreseeable future, particularly as CMMC slowly ramps up over the next two or three years before accelerating.

Organizations that store or handle CUI absolutely must maintain NIST 800-171 compliance, as dictated by DFARS clause 252.204-



7012. Although the clause allows self-attestation for prime contractors and their subcontractors, these businesses should expect increased scrutiny in the form of audits conducted by DCMA. Inconsistencies between self-assessments and audits could put companies in jeopardy of adverse contract impacts or penalties under the False Claims Act.

The overlap between NIST 800-171 controls and CMMC practices places a premium on all members of the DIB – regardless of whether they touch CUI – to understand and implement some or all of NIST 800-171 as quickly as possible. One hundred percent of CMMC's Level 1 practices, 90 percent of Level 2 practices, and 85 percent of Level 3 practices come from NIST 800-171 controls. Of important note, Plans of Actions and Milestones (POA&Ms) that may have been accepted as part of NIST 800-171 compliance likely will not be allowed to successfully achieve CMMC certifications. So, a top priority for all contractors subject to 800-171 compliance that expect to bid on future work requiring CMMC certifications should be prioritizing implementation (and thus elimination) of their POA&Ms.

3. Subcontractor Compliance Flowdown

DoD prime contractors wanted to know, "*Are we still responsible for ensuring that our subcontractors and suppliers can receive and protect CUI?*" Primes possess several motivations for maintaining subcontractor and supplier oversight in this regard, in both the short and long term.

The current version of DFARS 252.204-7012 includes a flowdown provision that places the onus on primes to ensure that their entire, multi-tier supply chains comply with NIST 800-171 if they are to receive CUI. This provision will remain valid for all current DoD programs until contract completion or renewal.

Meantime, the DoD plans updates to DFARS to account for the introduction of CMMC. DoD programs that incorporate CMMC make it mandatory for all participants on a bid team to possess certain levels of certification, with the minimum being a CMMC Level 1 certification for any first-tier subcontractor. Yes, CMMC supplements flowdown provisions and potentially shifts the onus by requiring all companies in the DoD supply chain to obtain their own certifications. However, prime contractors still must maintain visibility into the CUI capabilities and certifications of all of their subcontractors and suppliers. They need this so they can confidently bid on contracts at all five CMMC levels, particularly those at Level 3 and above when CUI is a factor, as well as to best protect their own sensitive data and intellectual property from compromise.

4. Who Pays

Both large and small companies expressed interest in financial obligations associated with obtaining a CMMC certification, essentially saying, "*Security isn't free, and neither is certification. Who pays?*" The DoD has consistently stated it does not want to place undue fiscal burden on the DIB, particularly on smaller businesses that may only seek a Level 1 certification. For this level, the DoD selected cybersecurity practices that represent basic protections that most organizations already should have in place, and are currently required by the FAR.

Yet the DoD also recognizes that stepping up to CMMC presents ongoing resource challenges for all members of the DIB. For this reason, security will be an allowable cost that contractors can claim for programs that require CMMC certification, based on contract type and required CMMC levels. In addition, prime contractors may offer assistance to their subcontractors to help them successfully achieve the necessary levels of certification.

5. Finding Help

Eager for guidance, many participants asked "*Where can we get help?*" The DoD continues to publish documents intended to clarify the practices and processes defined by version 1 of the CMMC standard. But many companies lack the cybersecurity expertise or personnel to leverage these resources and go it alone.

While cybersecurity consulting services represent one option for help, these services can often prove costly and time-consuming, while creating an ongoing dependency. Risk management products may offer a more viable alternative. An effective risk management product includes an intuitive, easy-to-use interface and comprehensive explanations. It provides guidance that progresses users, step-wise, through the process of gathering the necessary information and performing the appropriate activities to document NIST 800-171 effortsin support of being audited, and preparing for the forthcoming CMMC certification process.

To learn more about the coexistence of NIST 800-171 and CMMC and their impacts on all members of the DIB, watch our on-demand CMMC Meets NIST webinar and visit us online. We're here to help.