For those of you who already are Department of Defense contractors or for those who would like to be, there is a looming set of requirements called the Cybersecurity Maturity Model Certification (CMMC) that will most likely cause you some near-term angst.

CMMC came about as a result of a DoD IG finding that DoD contractors lacked consistency in the way they were addressing cybersecutity threats and incidents. DoD’s cybersecurity regulations under the Defense Federal Acquisition Regulation Supplement (DFARS) were substantially revised in 2016, and those revisions are reflected in DFARS clauses 252.204-7008 and 252.204-7012.. These clauses require actions such as damage assessment, mandatory reporting, and media preservation requirements and require an internal assessment be made of your organization’s current cybersecurity environment. The part of the equation that is blank at this time is how the certification process will eventually play out and who the certification organizations will be. I anticipate that we will see something like what we now see with ISO certifications with several certification organizations coming into existence.

Regardless of that process, you should now be taking action to assess your current cybersecurity posture and to identify near and short term actions required to best position your organization to meet threats. NIST has developed the NIST MEP Cybersecurity Self-Assessment Handbook For Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements which is a guide that describes the requirements and can lead you through the self-assessment process. Under the current requirements. All DoD contractors (unless strictly dealing with Commercial-off the Shelf items) will be required to perform a self-assessment of your current cybersecurity posture and to identify weaknesses and their attendant mitigation steps. This will become the basis for your CMMC plan which will submitted as part of your proposals either at the base contract level (Blanket Procurement Agreement or Department-wide acquisition contract) or at a task order level for those DoD acquisitions using non-DoD contracts (think Polaris, OASIS+, SEWP and the like). This is Level 1 certification. Eventually, those organizations that work with critical national security information will require a Level 2 certification with an assessment performed by an outside agency. Some number of organizations will also be able to self-assess at Level 2. The details of what constitutes “critical national security information” and thus requiring Level 2 certification are still somewhat murky. The highest-level certification will be Level 3 and will theoretically be conducted by the Government itself but I would expect some of the larger Fed contractors will develop practice areas to give them ins for exclusive contracts to provide these assessments.

Your homework from all of this is to take a hard look at NIST SP 800-171 and the current DoD Chief Information Officer’s CMMC documentation website. I’ve provided links to both in these in this episode’s transcript. Now would be a good time to consider the requirements and start your organization down the path of compliance through the self-assessment process. Remember tat no certifying organizations currently exist and any outside agency can only assist with your CMMC program setup and initial self-assessment.

And now a word from our sponsor. If you are a small to medium business struggling to get a handle on your capture and proposal efforts, our sponsor, WordSmart Business Services, may have a solution for you. WordSmart provides an affordable enterprise-level solution for business development and capture management. Reach out to David Nealey at WordSmart and ask about their Proposal Essentials Plus suite. Use code Foxtrot Papa Papa, that’s FPP, and see what they can do for your organization. Call David at 720-725-0009.

That’s it for this episode, Thanks for listening and as always provide any feedback to me at [ken.blair@fedprops.com](mailto:ken.blair@fedprops.com).

Links mentioned in this episode.

[NIST SP 180-171](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf)

[DoD CIO CMMC Documentation](https://dodcio.defense.gov/CMMC/Documentation/)