designDATA CENTRE LAW & CONSULTING

DEPARTMENT OF DEFENSE ISSUES CMMC INTERIM RULE

NOVEMBER 2020

Prepared by: Jonathan Roy
DesignData

Prepared By: David Warner, Esq
Partner, Centre Law & Consulting

02

SNAPSHOT

Who does this apply to?

- Currently applicable to only DOD contractors and subcontractors
- Other agencies expected to adopt standards
- “Covered systems” – computer systems that store, process, generate, transmit or access defense information

Impact on Government Contracts

- Before November 30, 2020 contractor must perform a self-assessment using the NIST controls and guidance found at: **https://nvipubs.nist.gov/nistpubs/hb/2017/NIST.HB.162.pdf**
- Self-assessment must be reported in the SPRS online at: **https://www.sprs.csd.disa.mil/**

Gaining a Competitive Advantage

- Beginning November 30, 2020, contractor must have a current security assessment in SPRS to be eligible for contract award·
- DFARS clause must be flowed-down to subcontractors
- CMMC third-party certification process phased-in over next five years

DEPARTMENT OF DEFENSE ISSUES CMMC INTERIM RULE

– ACTION REQUIRED BY ALL CONTRACTORS BY NOVEMBER 30TH

The Department of Defense (DoD) clearly has a new priority: Protect our warfighters and defense industrial base from cyber threats. While this has been a stated goal for a while now, the DoD is putting some teeth to this priority for, arguably, the first time. What has for a long time been a self-assessment-based honor system for contractors to ensure basic cyber hygiene, the government is now finally going to start asking for transparency and, soon, evidence. Not only must contractors live up to their cyber security responsibilities (which many have been doing, but others have been giving varying degrees of lip service), but now the reporting and accountability begins

WHAT HAPPENED?

On September 29th 2020, the DoD issues an interim rule to implementing its new Cybersecurity Maturity Model Certification (CMMC). The new rule issues a new mandate: The DoD Assessment Methodology, which serves as an interim certification process before the full CMMC third party certification becomes available.

The most impactful portion of this new DoD Assessment Methodology requires some new action by all defense contractors with DFARS 252.204-7012 clause: They MUST submit a self-assessment of NIST SP 800-171 (a framework that CMMC is largely based on) by November 30th, 2020.

WHY THIS INTERIM RULE?

For years, while the DoD has talked a big game about requiring its contractors (and all sub-contractors under them) to meet certain cybersecurity standards, but it has done surprisingly little to enforce them. The written requirements and specific controls have been published, but the DoD largely only required contractors to do self-assessments without the need to report on results or plans of action.

This interim rule is the first (and long-overdue) step towards accountability. While it is still only a self-assessment, contractors are required to submit their results and will be given a numerical score based on their answers. That score can be measured and compared to other contractors, and can start to be a differentiator that contract officers will pay attention to during contract review.

Additionally, this interim rule is a good lead-in to the upcoming CMMC certification, which will require third-party certification, that requires an outside auditor licensed by the CMMC Accreditation Body to issue your certification. While these new requirements may seem steep, the DoD is expecting contractors to incorporate the costs of getting these certification into their contract rates.

WHY IS THIS IMPORTANT TO ME?

If you have the DFARS 252.204-7012 clause in your government contract, you have a new urgent to-do item: Submit your self-assessment of NIST SP 800-171 by November 30th, 2020. Failing to submit this information or having a low score could well impact your ability to win or maintain contracts with the DoD.

While this rule may seem sudden, the NIST SP 800-171 controls they are asking about are not, and contractors should already have these in place: Not just for meeting the requirements, but because these controls help impose the good cyber hygiene that all organizations should be adhering to.

WHAT NOW?

If you have the DFARS 252.204-7012 clause in your government contract, go to the Supplier Performance Risk System (https://www.sprs.csd.disa.mil/) and complete the self-assessment by November 30th, 2020.

Even if you don't have this clause, you should still be looking at these controls (and more importantly, the CMMC framework that is the next evolution of these controls that will soon become the new standard) and start thinking about not only implementing these controls, but how you can best show the evidence needed for when CMMC certification level requirements start showing up in contracts.

WHAT DO I NEED TO KNOW?

Here is a recap of the important differences between this interim rule and the upcoming Cybersecurity Maturity Model Certification (CMMC):

- The interim rule represents a self-assessment, CMMC will require a 3rd party auditor to certify you.
- The interim rule is based on the NIST SP 800-171, while the new CMMC standard has its own controls (although if you previously complied with NIST SP 800-171, you'll have a relatively easy time with CMMC).
- The interim rule only applies if you have the DFARS 252.204-7012 clause in your contract, the CMMC will apply to EVERY DoD contractor and subcontractor that handles Controlled Unclassified Information (CUI). The government contracts themselves are considered CUI, so this will de-facto apply to all primes and all subs, even those aren't technology-oriented

CMMC requirements are coming, but the rollout is slow: We can expect to see the first DoD contracts requiring CMMC to come out in 2021, and they'll only require Level 1 to start. We can expect a full roll-out by 2025, and while CMMC levels will go up to 5, we expect only a handful of prime contractors will need to go for that level: Most contractors will want to target Level 3. Note that as of the time of this writing, the CMMC Accreditation Body only has provisional assessors picked and no Certified 3rd Party Assessment Organizations (C3PAO's) have been approved. Anyone claiming to be able to give you a CMMC certification today is misleading you

WHAT OTHER RESOURCES ARE AVAILABLE?

The full text of the interim rule can be found on govinfo.gov, or at this direct link:

- https://www.govinfo.gov/content/pkg/FR-2020-09-29/pdf/2020-21123.pdf

F**or the self-assessment required of this interim rule, you can view the full description of the different controls and guidance on interpreting them here:**

- https://nvlpubs.nist.gov/nistpubs/hb/2017/NIST.HB.162.pdf

For more information on the upcoming CMMC certification, including the status of assessment organizations, assessors, methodologies, and controls, you can reach out to designDATA's Security and Compliance team at **security@designdata.com.**

For more information regarding contract coverage, flow down requirements, and implications for contract award and performance, you can reach out to Centre Law & Consulting, LLC at **dwarner@centrelawgroup.com**