SheppardMullin

DoD's Long Awaited Rule on CMMC – Plus a New Cybersecurity Assessment Methodology for Contractors to Start Right Now

By: Townsend Bourne and Nikole Snyder

At long last, DoD has provided its interim rule to be published in the Federal Register setting forth requirements for its Cybersecurity Maturity Model Certification ("CMMC") program, as well as new requirements for a "NIST SP 800-171 DoD Assessment Methodology" that will take effect immediately.

Results of the NIST SP 800-171 DoD Assessments and CMMC certifications will be reported and maintained in the Supplier Performance Risk System ("SPRS") (information available here). Contracting Officers will be required to check SPRS and verify information on the contractor's assessment or CMMC status prior to contract award or prior to exercising an option period or extending a contract period of performance.

- NIST SP 800-171 DoD Assessment Methodology – For contractors already required to comply with NIST SP 800-171 per DFARS 252.204-7012, the Department of Defense ("DoD") is now going to hold those contractors accountable, instituting an assessment and reporting system to verify compliance before new contracts can be awarded. While the new requirement is for information to be provided prior to contract award, DoD encourages affected contractors to begin their self-assessments immediately.

    - The Assessment Methodology will include three assessment levels: (1) Basic, (2) Medium, and (3) High. The Basic Assessment will be a self-assessment completed by the contractor prior to contract award, while the Medium and High Assessments are available options for DoD to complete after award.
        - DoD estimates it will conduct 200 Medium Assessments and 110 High Assessments each year.
        - Information regarding DoD assessments is available here.

    - There is a specific scoring methodology to be followed for the Assessment. A contractor that has fully implemented all 110 NIST SP 800-171 controls will have a score of "110."
        - It goes without saying that contractors will need to be careful here. An inaccurate report could subject a company to exposure under the False Claims Act.

    - Assessments will be valid for three years unless there are issues requiring a reassessment sooner.
    - The newly-announced Assessment Methodology appears to be an immediate solution to provide DoD some peace of mind on contractor data security until the CMMC program can be fully implemented.

- Cybersecurity Maturity Model Certification (CMMC) Framework – The description of CMMC in the interim rule is largely consistent with information DoD previously has shared (see our blog articles here and here) CMMC will not apply to procurements solely for Commercially Available Off-the-Shelf ("COTS") items or procurements at or below the micro-purchase threshold.

    - The interim rule solidifies the timing associated with implementation of CMMC, clarifying that CMMC requirements may be included in solicitation and contracts through September 30, 2025 only where approved by the Office of the Under Secretary of Defense for Acquisition and Sustainment ("OUSD (A&S)"). On or after October 1, 2025, CMMC will apply to all DoD solicitations and contracts (excluding solely COTS procurements and procurements at or below the micro-purchase threshold).

    - A contractor may seek CMMC certification for the entirety of its enterprise network, or for a particular section of its network.

    - CMMC certification must be in place prior to contract award (rather than at the time of proposal submission or after award).

    - CMMC certifications will be valid for three years.

    - The interim rule specifies at a high level the procedure to be followed should a contractor dispute its CMMC third party assessment organization ("C3PAO") assessment, which includes submitting a dispute adjudication request to the CMMC-Accreditation Body ("CMMC-AB").

The rollout plan for CMMC with respect to small entities is set forth in the following table in the interim rule:

Year	Level 1	Level 2	Level 3	Level 4	Level 5	Total
1	665	110	335	0	0	1,110
2	3,323	555	1,661	2	2	5,543
3	11,086	1,848	5,543	4	4	18,485
4	21,248	3,542	10,624	6	6	35,426
5	21,245	3,541	10,623	7	7	35,423
6	21,245	3,541	10,623	7	7	35,423
7	19,180	3,197	9,590	7	7	31,981
1-7	97,992	16,334	48,999	33	33	163,391

The interim rule introduces three new DFARS clauses:

- DFARS 252.204-7019, Notice of NIST SP 800-171 DoD Assessment Requirements – This clause provides the requirement for an assessment to be completed prior to contract award where the offeror is required to implement NIST SP 800-171 (relating to protection of Controlled Unclassified Information ("CUI")).

    - It includes a requirement for an offeror to verify that its Assessment scores are timely and posted in SPRS.

- An offeror may complete and submit information on its Basic Assessment via webptsmh@navy.mil if not already posted in SPRS. Specific information to be provided, including a description of the System Security Plan, dates by which the offeror expects to implement incomplete controls, and the offeror's summary level score (up to 110), is included in the clause. Scores are to be posted within 30 days.

- The clause is required in all solicitations except for solely COTS procurements.

- DFARS 252.204-7020, NIST SP 800-171 DoD Assessment Requirements – This clause includes the DoD Assessment requirements for contractors.

  - It specifies that a Basic Assessment conducted by the contractor "[r]esults in a confidence level of 'Low' in the resulting score, because it is a self-generated score."

  - Where DoD elects to conduct a Medium or High Assessment, the contractor must provide DoD with access to its facilities, systems, and personnel. The contractor will have an opportunity to rebut DoD's assessment scores, and will have 14 business days to provide additional information.

  - Authorized contractor representatives will be able to access SPRS and view the contractor's scores in accordance with DoD guidance here.

  - The clause is required in all solicitations and contracts except for solely COTS procurements.

  - The clause is to be flowed down to subcontractors (except in solely COTS item subcontracts), and the prime contractor is responsible for verifying that its subcontractors have a reported Assessment at SPRS prior to subcontract award.

- DFARS 252.204-7021, Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirement – This clause describes requirements for DoD's new CMMC program.

  - The clause is required in all solicitations and contracts except for solely COTS procurements where the requirement document or statement of work requires a specific CMMC level. Prior to October 1, 2025, OUSD (A&S) must approve use of the clause.

  - The clause is to be flowed down to subcontractors (except in solely COTS item subcontracts), and the prime contractor is responsible for verifying that its subcontractors have a reported CMMC certificate at SPRS prior to subcontract award.

DoD specifically is seeking comment on how the interim rule will affect small businesses and on the requirement for CMMC certification at the time of contract award. Comments on the interim rule are due 60 days from posting in the Federal Register.

Questions? Contact:

Townsend Bourne
202.747.2184
tbourne@sheppardmullin.com

Nikole Snyder
202.747.3218
nsnyder@sheppardmullin.com