wiley

NEWSLETTER

Interim Rule on CMMC and NIST 800-171 Assessments Creates New Cybersecurity Compliance Requirements for Contractors

October 2020

Cybersecurity has been an increasingly important compliance area for government contractors for more than a decade. Over the past year, the U.S. Department of Defense (DOD) has been laying the foundation for a new Cybersecurity Maturity Model Certification (CMMC). This new model expands on the current model under Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012, which requires contractors to meet data security requirements prescribed in National Institute of Standards and Technology (NIST) SP 800-171. DOD has repeatedly criticized industry's inadequate compliance with these requirements and cited that dissatisfaction as a key driver behind this change to CMMC.

With the release of a new interim rule, that paradigm shift is now imminent, and all government contractors should take a close look at the state of their compliance with cybersecurity requirements. Indeed, the stakes are high – contractors that are not compliant with the requirements of the interim rule risk being found ineligible for new DOD contracts and even new option periods under existing contracts.

As we detailed in an earlier client alert, DOD released an interim rule on September 29, 2020 that created two distinct cyber compliance regimes for DOD contractors. As expected, the interim rule initiated the CMMC certification regime, which will be phased in over five years. In addition, the interim rule altered the current DFARS 252.204-7012 regime by requiring contractors to undergo an assessment process to ensure compliance with NIST SP 800-171. The interim rule will become effective November 30, 2020, and DOD is accepting comments until that time.

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Gary S. Ward
Partner
202.719.7571
gsward@wiley.law

Practice Areas

Government Contracts

Privacy, Cyber & Data Governance

White Collar Defense & Government Investigations

This article includes a brief summary of these new requirements and highlights several significant questions raised by the interim rule.

The Interim Rule Established the CMMC Regime

As expected, DOD will begin to include CMMC requirements in new DOD contracts by including a new clause, DFARS 252.204-7021, "Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirement." For now, DOD will include this clause in only a limited number of contracts approved by the Office of the Under Secretary of Defense for Acquisition & Sustainment. DOD has not articulated any criteria for deciding which contracts will be among the first to require a CMMC Level. By October 1, 2025, this clause will be applicable to all contracts, except for those below the micro-purchase threshold and for those exclusively for commercially available off-the-shelf (COTS) items.

The new clause does not alter any of the substantive requirements embedded in the CMMC model that DOD and the CMMC Accreditation Body have been developing over the last year. DOD and the CMMC Accreditation Body publicized the model through a series of public drafts and final publications. The model creates a third-party certification regime for contractors to achieve certifications ranging from Levels 1-5, demonstrating implementation of cybersecurity practices and process maturity. The security controls in CMMC are primarily derived from existing requirements in NIST SP 800-171 (which many defense contractors were already required to meet under DFARS 252.204-7012), but CMMC also draws from other security standards. Contractors will be required to possess the appropriate CMMC Level to be eligible to compete for DOD contracts. DOD expects to roll out CMMC requirements incrementally to the entire Defense Industrial Base. During FY21, DOD expects that 1,500 contractors will become certified, with all contractors becoming certified over the course of the next five years. Private sector Assessors, known as Certified Third Party Assessment Organizations (C3PAOs) and individual Assessors employed by the C3PAOs, will be trained and certified by the CMMC Accreditation Body. The C3PAOs and Assessors will be responsible for certifying DOD contractors to a specific CMMC Level.

The Interim Rule Requires NIST 800-171 Assessments

Although CMMC has received more attention – likely due to the anticipation surrounding CMMC – the interim rule announced a more immediate NIST SP 800-171 Assessment requirement. Under that requirement, contractors will be required to undergo an assessment process to ensure compliance with NIST SP 800-171, ranging from a Basic Assessment to a Medium or High Assessment. Basic Assessments must be completed by the contractor and submitted to DOD, while Medium or High Assessments are performed by DOD. Under a Basic Assessment, a contractor must score its implementation of NIST SP 800-171 controls on a 110-point scale using DOD's NIST SP 800-171 Assessment Methodology. Although the rule does not require offerors to achieve a minimum score as a condition of award, covered contractors will not be eligible for contract award unless they submit the Basic Assessment, which must identify the contractor's current score and the date by which the entity expects to achieve a perfect 110 score. Beginning on November 30, 2020, DOD will begin including two new DFARS clauses in DOD contracts, which will require that contractors perform Assessments and submit scores as a condition of award.

The Interim Rule Raises Implementation Questions

These new requirements have created several uncertainties that contractors will have to work through. DOD officials have stated that contractor and industry comment is welcome.

Practical Issues for NIST SP 800-171 Assessments

- **"Relevant" Information Systems:** The interim rule provides a vague standard for determining which (or how many) information systems must be subjected to the Assessments. The interim rule states that each covered contractor information system "relevant" to an offer or contract must have an Assessment. This leaves room for contracting officers to take different views on which systems are covered and potentially whether a contractor is eligible for award. To guard against this risk, contractors should consider inventorying the information systems that could potentially be subject to the Assessment requirement, and independently evaluating whether to perform Assessments on those systems (as well as how those systems would fare under the Assessments).
- **Competitive Value of Scores:** The interim rule requires offerors to submit their Basic Assessment scores but does not specify a minimum score. This leaves open the possibility that some contracting officers may use scores as competitive evaluation factors. Indeed, Defense Contract Management Agency (DCMA) representatives have acknowledged that contracting officers might do this. In the absence of uniform guidance, contractors will need to scrutinize individual solicitations to understand the impact of their Basic Assessment scores. This may also increase a contractor's incentive to implement the NIST SP 800-171 security controls and close out any open Plans of Actions & Milestones (POA&Ms).
- **Basic Assessments:** Contractors should give significant attention to how they conduct their Basic Assessments and be prepared to justify their results. Under the interim rule, System Security Plans (SSPs) and POA&Ms do not need to be provided to DOD as part of the Basic Assessment (only the compliance score and date of full compliance need to be provided). That said, contractors should expect for Basic Assessments to receive significant scrutiny from DOD. Indeed, the Medium and High Assessments are essentially tools for DOD to verify the accuracy of a Basic Assessment. Contractors with notably low scores or who have suffered a cyber incident are the most likely targets for this additional scrutiny.
- **Scope of Assessments:** As the interim rule acknowledges, many contractors may have the DFARS 252.204-7012 clause in contracts, but do not need to implement NIST 800-171 because they do not process CDI. These contractors are likely exempt from completing a NIST 800-171 Assessment, which makes sense – there is no need for an Assessment of something that is not required. However, the interim rule does not provide a clear mechanism to notify a contracting officer or assert that the contractor is exempt from the Assessments. This gap increases the risk of miscommunication or uncertainty at the time of award because a contracting officer may not understand why an offeror has not submitted an Assessment. In the absence of further guidance, contractors should scrutinize

individual solicitations to understand how to communicate their position in the midst of a competition. Contractors may also consider pressing contracting officers to provide clear guidance about whether they expect the contract to receive or generate CDI under the contemplated contract.

Practical Issues Under the CMMC Regime

- **Timing of CMMC Requirements:** In the near term, it is uncertain whether there will be adequate resources and infrastructure to certify contractors to the requisite CMMC Level, even under the phased roll-out approach adopted by DOD. The CMMC Accreditation Body (CMMC AB) was formally established just months ago, and the first cohort of Assessors have only recently completed their initial training with many more hundreds of Assessors required to meet the expected demand. This new process will likely create a number of disputes and inconsistencies as the CMMC standard is applied to different and unique circumstances, likely creating second-tier review or appeals of CMMC determinations and further demands on the limited time and resources of CMMC Assessors and the CMMC AB. As a result, some contractors may want to consider the timing of their CMMC efforts, in light of uncertainties about short-term implementation requirements.
- **CMMC Levels:** As CMMC is expanded over the next several years, anticipating what CMMC Level may be required under a specific contract will be challenging due to the paucity of formal guidance. The lack of clarity on this key issue makes long-term infrastructure investments fraught decisions. For contractors who believe they may be required to meet CMMC Level 3 because they currently process CDI, it may be prudent to ensure that all NIST SP 800-171 security controls are fully implemented, and they may consider performing an external audit under the direction of counsel to assess compliance. Contractors should also inquire about which upcoming contract opportunities are expected to include CMMC requirements.
- **Reciprocity:** Although it’s not addressed in the interim rule, DOD officials have indicated that CMMC Assessors will provide reciprocity between various security standards with overlapping requirements. For example, contractors who have achieved ISO 27001 certification may have certain controls deemed to be already satisfied for the purpose of the CMMC certification. Likewise, contractors who have achieved certain high scores under the NIST SP 800-171 Assessments may have those scores credited during a CMMC certification. But DOD has yet to finalize and publish this guidance, which will be critical to helping contractors focus on the areas necessary to achieve compliance. Contractors should be on the lookout for FAQs and guidance to be issued on DOD’s website on this and other areas of interest.

Managing Suppliers for Both CMMC and NIST 800-171 Assessments

- **Flow-Down and Verification:** Prime contractors are required under the interim rule to ensure that subcontractors have a Basic Assessment or the CMMC Level appropriate for the information being flowed down to them. However, they will not have access to the government database to verify these requirements are in place. As a result, contractors will need to develop policies and processes to ensure that any subcontractors meet these requirements.

Wiley is deeply engaged in the emerging CMMC and NIST 800-171 accreditation requirements and has advised government contractors across a wide range of cybersecurity compliance and incident response challenges.