wiley

ALERT

Not Just CMMC: New DOD Rule Creates Two Cybersecurity Assessment Frameworks

September 29, 2020

WHAT: After clearing the interagency review conducted by the Office of Management and Budget (OMB), the U.S. Department of Defense (DOD) has released a long-awaited interim rule to implement not one, but two new frameworks for verifying contractor compliance with cybersecurity requirements: (1) NIST SP 800-171 DOD Assessment Methodology and (2) the Cybersecurity Maturity Model Certification (CMMC).

WHEN: The interim rule was released today, September 29, 2020 and is scheduled to become effective on November 30, 2020.

WHAT DOES IT MEAN FOR INDUSTRY: This interim rule combines two items: (1) a new assessment framework, which will have an immediate impact on contractors, and (2) additional information about the long-anticipated CMMC framework, which DOD will roll out over the next five years.

The immediate impact comes from the NIST SP 800-171 DOD Assessment Methodology. Under this framework, contractors will be required to complete a self-assessment of their compliance with NIST SP 800-171 before they can receive DOD contracts. This framework also gives DOD new tools for verifying a contractor's compliance.

For CMMC, the interim rule introduces the long-anticipated DFARS clause that sheds some light on how DOD contractors are expected to flow down the requirements to subcontractors. But the interim rule also highlights DOD's desire to continue developing the CMMC requirements outside the DFARS rulemaking process.

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Jon W. Burd
Partner
202.719.7172
jburd@wiley.law

Tracye Winfrey Howard
Partner
202.719.7452
twhoward@wiley.law

Kara M. Sacilotto
Partner
202.719.7107
ksacilotto@wiley.law

Gary S. Ward
Partner
202.719.7571
gsward@wiley.law

Practice Areas

Cybersecurity

Government Contracts

Privacy, Cyber & Data Governance

White Collar Defense & Government Investigations

Continue reading for our take on the key questions, including what is happening and when; what types of contracts are covered; the differences between SP 800-171 Assessments and CMMC Certifications; what stages of the procurement lifecycle these rules apply to; how contractors are expected to flow down these requirements; and DOD's initial insight into potential dispute processes.

What is happening and when?

Today through November 29, 2020:

- **DOD will accept comments on the interim rule:** DOD determined that "urgent and compelling circumstances" make it impracticable to solicit comments first and elected to proceed with an interim rule that will become effective in 60 days. DOD will, however, consider any comments in preparing the final rule.

November 30, 2020 through September 30, 2025:

- **SP 800-171 Assessment requirements will apply broadly:** DOD will require all contractors to undergo an assessment process to ensure compliance with NIST SP 800-171, starting on November 30, 2020. Throughout this alert, we refer to these as **SP 800-171 Assessments** because they focus on a contractor's compliance with NIST SP 800-171.
  - The interim rule defines three levels of assessment. To be eligible for award, a contractor must complete the first level (a Basic Assessment); the other two levels (Medium and High) are assessments that DOD may conduct itself during the course of performance. Each assessment results in a summary level score, which represents the number of security requirements from NIST SP 800-171 that the contractor has implemented. Because NIST SP 800-171 includes 110 security requirements, the maximum score is 110. The interim rule does not prescribe a minimum score to be eligible for award, although a contractor must identify a date by which it expects to achieve a score of 110 in order to complete the Basic Assessment.
  - Contracting officers will implement these requirements by including two new DFARS clauses in DOD contracts:
    - DFARS 252.204-7019, *Notice of NIST SP 800-171 DOD Assessment Requirements*
    - DFARS 252.204-7020*, NIST SP 800-171, DOD Assessment Requirements*
  - **NOTE:** The procedures in the interim rule state that it takes 30 days to post the scores from a SP 800-171 Assessment to DOD's system of record (Supplier Performance Risk System or SPRS), so contractors should plan ahead to make sure their scores are posted by the time these requirements become effective to avoid any potential award delays.
- **CMMC requirements will apply to some DOD contracts**: DOD will also begin to roll out CMMC requirements on November 30, 2020. The interim rule does not identify any criteria for determining which solicitations or contracts will include CMMC requirements. Instead, it requires contracting officers to impose the CMMC requirements "if the requirement document or statement of work requires a contractor to have a specific CMMC level." To ensure some coordination between requiring activities,

the interim rule requires approval from the Office of the Undersecretary of Defense for Acquisition and Sustainment before including any CMMC requirements in a solicitation during this phase of the rollout.

- Contracting officers will implement these requirements by including a third new clause introduced in the interim rule:
  - DFARS 252.204-7021, *Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirement*.
- The 7021 Clause is brief. It requires contractors to maintain a current certification, it requires contractors to flow down the clause, and it refers to the CMMC website. This suggests that DOD will continue to develop the CMMC program outside the DFARS rulemaking process.

October 1, 2025 and on:

- **CMMC requirements will apply to virtually all DOD contracts**: By October 1, 2025, the interim rule will include CMMC requirements in virtually all DOD contracts.
- **SP 800-171 Assessment requirements will continue:** Nothing in the interim rule suggests that DOD plans to end the separate SP 800-171 Assessment requirements when the CMMC rollout is complete.

What types of contracts are covered?

- All of the new clauses apply to all contracts with only two exceptions: (1) contracts at or below the micro-purchase threshold and (2) contracts exclusively for commercially available off-the-shelf (COTS) items. The clauses implementing the SP 800-171 Assessments, however, require a current assessment only "if the Offeror is required to implement NIST SP 800-171," which is typically prescribed through DFARS 252.204-7012.

What is the difference between the SP 800-171 Assessments and CMMC Certifications?

- The table below identifies the key differences between the three types of SP 800-171 Assessments and the five levels in the CMMC framework.

Requirement / Level

Who is the assessor?

When is it required?

What is assessed?

SP 800-171 Assessment

Basic

Contractor (Self-Assessment)

Before award (DOD contracts subject to NIST SP 800-171)

- Review system security plan to assess compliance with NIST SP 800-171

Medium

DOD entity (e.g., DCMA)

DOD reserves right to conduct during performance

- Basic Assessment
- "Thorough document review"
- "Discussions with the contractor"

High

- Medium Assessment
- "Verification, examination, and demonstration" of the contractor's system security plan to validate implementation

CMMC

Level 1

C3PAOs (overseen by the CMMC-AB)

Before award (when no CUI used)

- 15 basic safeguarding requirements (FAR 52.204-21)

Level 2

Not required

- 65 security requirements from NIST SP 800-171
- 7 CMMC practices
- 2 CMMC processes

Level 3

Before award (when CUI used, specific level depends on sensitivity of the information)

- All 110 security requirements from NIST SP 800-171
- 20 CMMC practices
- 3 CMMC processes

Level 4

- All 110 security requirements from NIST SP 800-171
- 46 CMMC practices
- 4 CMMC processes

Level 5

- All 110 security requirements from NIST SP 800-171
- 61 CMMC practices
- 5 CMMC processes

At what stage in the procurement lifecycle will DOD apply these requirements?

- Contractors can complete a SP 800-171 Assessment and obtain a CMMC Certification at any time. Contracting officers will verify that a contractor has done so at three key points in the procurement lifecycle:

    - **Award**: The interim rule prohibits contracting officers from awarding a contract to a contractor that has not completed at least a Basic SP 800-171 Assessment and obtained a CMMC Certification at the level specified in the solicitation. DOD initially previewed CMMC requirements as something that contracting officers would include in Sections L and M of future solicitations. This would have meant that offerors would need to address these requirements in their proposals, and agencies would evaluate them as part of the source selection process. The interim rule departs from this approach. Instead, it suggests contracting officers will simply look up each offeror's record in SPRS. This may prove to be more complicated in execution, at least for the SP 800-171 Assessments, because contracting officers will need to identify the full list of "each covered contractor information system that is relevant to an offer." This could lead to some of the same issues that some agencies have encountered when trying to figure out which CAGE Code to look up when verifying an offeror's facility security clearance.
    - **Options/Extensions**: The interim rule requires DOD contracting officers to verify that the contractor has a current SP 800-171 Assessment and current CMMC Certification at the appropriate level before exercising any option periods.
    - **Throughout Performance**: The interim rule requires contractors to maintain current SP 800-171 Assessments and CMMC Certifications throughout the life of the contract.

If I have an existing DOD contract, will I have to meet these requirements?

- DOD has not fully addressed its plans for implementing these requirements in existing contracts. The interim will likely create some confusion for contracting officers when they evaluate exercising options in contracts that do not include both of the new clauses.
- For **SP 800-171 Assessments**, the interim rule requires contracting officers to verify that the contractor has a current assessment before exercising an option or extending a contract "with a contractor that is required to implement the NIST SP 800-171 in accordance with the clause at 252.204-7012." Because the interim rule ties this evaluation to the existing 7012 Clause, it will affect contractors with existing contracts. Indeed, in the background section, DOD noted that the interim rule "enables DOD to strategically assess a contractor's implementation of NIST SP 800-171 on existing contracts that include DFARS clause 252.204-7012."
- For **CMMC**, the interim rule ties this evaluation back to the applicable contract, by requiring contracting officers to verify that "the contractor has a CMMC certificate at the level required by the contract." Still, contractors should not be surprised to see DOD change its approach and negotiate the CMMC requirements through a contract modification in the future.

How are prime contractors required to administer these requirements for subcontractors?

- The flow down requirements are prescribed in the new DFARS clauses. Both clauses require prime contractors to flow down these requirements "in all subcontracts and other contractual instruments" as long as neither of the two exceptions listed above apply (micro-purchase threshold or COTS items).
- Under the **7020 Clause** for SP 800-171 Assessments, the higher tier contractor is responsible for confirming that the subcontractor has completed at least a current Basic Assessment "for all covered contractor information systems relevant to its offer that are not part of an information technology service or system operated on behalf of the Government." The interim rule does not elaborate on how to determine which information systems are "relevant" to an offer. And if the subcontractor does not have a current Basic Assessment, the prime "shall not award a subcontract or other contractual instrument."
- Under the **7021 Clause** for CMMC requirements, the higher tier contractor is responsible for confirming that the subcontractor has a current CMMC certificate "at the CMMC level that is appropriate for the information that is being flowed down to the subcontractor." The background section of the interim rule provides only limited guidance for determining what level is "appropriate for the information": if a company processes, stores, or transmits Controlled Unclassified Information (CUI), it must achieve at least a level 3 certification; if not, it must obtain a level 1 certification.
- Because contractors will not have access to other companies' records in SPRS, they will need to request some other form of documentation from their subcontractors to confirm compliance.

How long do the certifications remain current?

- All assessments and certifications discussed in the interim rule are considered current for three years, although an agency may require a more recent SP 800-171 Assessment by articulating a shorter

duration in the solicitation. The interim rule does not authorize contracting officers to shorten the duration for a CMMC Certification.

What happens if I disagree with an assessment?

- The interim rule offers only limited insight into how DOD plans to address situations where a contractor disagrees with an assessor's findings. For **SP 800-171 Assessments**, the interim rule prescribes a "rebuttal" process. Under this process, the contractor has 14 business days to provide information to demonstrate that it met any security requirements not observed by the assessment team or to rebut any findings.
- For **CMMC Certifications**, the interim rule discusses disputes only in the background. It explains that "[i] f a contractor disputes the outcome of a C3PAO assessment, the contractor may submit a dispute adjudication request to the CMMC-AB along with supporting information related to claimed errors, malfeasance, or ethical lapses." It also explains that contractors "may request an additional assessment by the CMMC-AB staff." This is consistent with statements made by DOD that a dispute or appeal process is under development, which will, among other things, ensure uniformity between various assessors.

What does this interim rule mean for companies that do not have any contracts with DOD?

- The rule itself is limited to contracts with DOD, but DOD's efforts in this area have been driving approaches to cybersecurity elsewhere. For example, in its recent solicitation for the STARS III governmentwide acquisition contract, the General Services Administration (GSA) required offers to outline their plans for obtaining a CMMC Certification. CMMC also features prominently in the Cyberspace Solarium Commission Report and is likely to inspire additional obligations in the future.