Updates
October 02, 2020
DoD’s Cybersecurity Rule Will Expand Assessments of Defense Industry to Safeguard Unclassified Information, Raising New Implementation Issues

The U.S. Department of Defense (DoD) has issued a long-awaited interim rule to safeguard unclassified information in the possession of defense contractors by making periodic assessments of a company's cybersecurity compliance a condition of eligibility for a contract award.

DoD's interim rule was published in the Federal Register on September 29, 2020, and will take effect November 30, 2020, subject to becoming final later after receipt of comments. DoD's decision to implement the rule before it becomes final—citing the need for urgency—unfortunately limits the opportunity for DoD to receive input.

DoD's rule provides a regulatory framework for its Cybersecurity Maturity Model Certification (CMMC) program, which will be introduced into new contracts over the next five years. The rule also provides for a separate track of assessments that will apply to contractors that possess government information that requires safeguarding using controls set forth in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171.

The interim rule has significant compliance and cost implications for the Defense Industrial Base (DIB). This update provides an overview of DoD's interim rule and several key open issues.

DoD's Revised Contract Clauses

According to the interim rule, defense contractors "must begin viewing cybersecurity as a part of doing business" in order to protect themselves and to "protect national security."

The interim rule sets forth a two-pronged approach to implementing cybersecurity requirements.

- First, the interim rule puts previously announced details related to CMMC into a regulatory and contractual framework to be rolled out over the next five years.
- Second, it adopts a new, parallel track of assessments to verify that contractors are complying with NIST SP 800-171 and government assessors will assume a role in that process.

The interim rule proposes three new standard contract clauses under Part 252 of the DFARS and amends other DFARS subparts as part of a broad overhaul of existing cybersecurity requirements.

CMMC and Third-Party Verification

Released in January 2020, CMMC is a risk-based model designed to measure a contractor's protection of information that supplements the requirements in NIST SP 800-171 with additional practices and processes that vary according to the CMMC level.

The interim rule outlines DoD's plan to insert CMMC requirements into new contracts as follows.

- Between now and October 2025, DoD's Office of the Undersecretary of Defense for Acquisition and Sustainment will determine which contracts will include CMMC as a requirement. DoD anticipates that nearly 130,000 entities will pursue CMMC certification during this five-year period.
- Once fully implemented, CMMC will be required for all DoD solicitations and contracts above the micro-purchase threshold, except for commercial off-the-shelf contracts.
- As of October 1, 2025, to be eligible for a contract subject to CMMC, a contractor must be certified at one of five CMMC levels as of the time of award, based on an assessment performed by a Third-Party Assessment Organization (C3PAO) overseen by the CMMC Accreditation Body (CMMC-AB). Contractors must maintain a certificate for the duration of the contract.
- A contractor can achieve a CMMC level for its entire enterprise network or particular segments or enclaves, depending on where the information is located.
- A new clause, DFARS 252.204-7021, must be flowed down in subcontracts, except for commercial off-the-shelf item subcontracts. Primes must "ensure" that, prior to awarding a subcontract, the subcontractor has a current CMMC certificate at the "appropriate" CMMC level based on the information to be made available.
- DoD's interim rule anticipates assessment-related disputes but offers few details. Contractors may bring challenges before the CMMC-AB "related to claimed errors, malfeasance, or ethical lapses" by a C3PAO and then seek further review before the CMMC-AB. The standards that will be applied to resolve disputes remain unclear.

According to the rule, more than 163,000 small entities will need CMMC certification. The rule states that the average annual costs for small businesses to obtain CMMC certification will range from $1,000 for CMMC Level 1 to more than $60,000 for Level 3. Obtaining CMMC Level 5 certification is projected to cost more than $480,000 annually.

NIST SP 800-171 Assessments

The interim rule adopts important changes applicable to companies whose contracts include the existing cybersecurity clause at DFARS 252.204-7012. That clause requires contractors that store, process, or transmit Covered Defense Information (CDI) to maintain "adequate security" on their information systems by, at a minimum, adopting controls set forth in NIST SP 800-171. The clause also requires contractors to report cyber incidents.

Noting that to date, contractors have been permitted to stop short of implementing all of the 110 security requirements in NIST SP 800-171, the rule calls for "correcting" implementation gaps "immediately."

Under the rule, companies subject to NIST SP 800-171 will undergo one of three types of assessments using a "NIST SP 800-171 DoD Assessment Methodology."

- Basic Assessments will be self-assessments performed by contractors that indicate how many NIST SP 800-171 requirements the contractor has yet to implement. For example, a company that implemented all 110 NIST SP 800-171 controls will have a score of 110.

- To be considered for award of a DoD contract, a company that has a "covered" contractor information system under DFARS 252.204-7012 must have, at a minimum, a Basic Assessment that is current, i.e., not more than three years old.
- The requirement to have a Basic Assessment will be phased in over a three-year period, incorporated into new solicitations and contract clauses in new contracts and orders.
- Medium and High Assessments may be performed by the government at its discretion after contract award based on the "criticality" of the program or the nature of the information at issue. DoD expects that Medium and High Assessments will be conducted on a "finite number" of awardees each year.
- The results of a NIST SP 800-171 assessment will be documented in DoD's Supplier Performance Risk System (SPRS). Prior to contract award, contracting officers will verify in SPRS that offerors have a current NIST SP 800-171 DoD assessment on record.
- The DoD assessments will be valid for three years and then must be renewed.

According to DoD, its methodology will enable assessments at the "entity level," avoiding duplicative or repetitive assessments on a contract-by-contract basis. Also, according to the rule, CMMC assessments "shall not duplicate" efforts from any comparable DoD assessment, except in rare circumstances. The manner in which CMMC will coexist with these assessments remains unclear.

Next Steps and Implementation Issues

DoD's interim rule represents a significant step with vast consequences for defense contractors. Significant implementation challenges, however, remain.

- DoD's decision to forego traditional notice-and-comment rulemaking, citing urgent and compelling circumstances, is unfortunate because it limits industry feedback on a major program. Nevertheless, the final rule can change based on comments received by November 30, 2020, and this introduces a degree of uncertainty.
- The rule encourages companies subject to NIST SP 800-171's requirements "to immediately conduct and submit" a self-assessment to facilitate later review by DoD. Companies subject to DFARS 252.204-7012 that process CDI should consider performing such an assessment if they have not already done so.
- DoD's two-track approach to assessments—with some performed by third parties and others performed by the government and contractors—raises questions about the roles to be played by third parties (i.e., the CMMC-AB and C3PAOs) and the government and the relationships between the various participating oversight entities.
- A prime contractor's flow-down obligations to subcontractors will present challenges. There will be interpretive questions such as what it means for a prime contractor to "ensure" that a subcontractor has a CMMC certificate that is "appropriate" for the information that is to be flowed down to the subcontractor and who will decide the meaning of "appropriate."
- The rule provides DoD with discretion to use a Medium or High Assessment after a contract is awarded, depending on the nature of the program or the sensitivity of the information, but this also creates uncertainty for companies trying to prepare their systems for assessment.
- Questions remain regarding the applicable standards and the information that needs to be protected (e.g., the definition of Controlled Unclassified Information (COI)), as well as the cost impact for small businesses.
- Issues remain unanswered about dispute resolution procedures under CMMC, including the extent to which DoD will be involved in resolving disagreements and the implications of CMMC's "Go/No Go"

requirements for bid protests challenging procurements.

Companies should continue to monitor developments in this area as they prepare for CMMC and the interim rule's effective date.

Authors

Explore more in

Government Contracts

Related insights

Update

HHS Proposal To Strengthen HIPAA Security Rule

Update

California Court of Appeal Casts Doubt on Legality of Municipality’s Voter ID Law