Cooley

DoD's New Cybersecurity Rules Take Effect November 30

November 16, 2020

The Department of Defense's interim rule implementing new cybersecurity requirements for government defense contractors is set to take effect on November 30, 2020. Published on September 29, 2020, the rule establishes a framework for assessing defense contractor implementation of cybersecurity requirements and enhancing the protection of *unclassified* information within the DoD supply chain. (Protection of classified information is regulated by a parallel regulatory framework.) Specifically, the interim rule implements not only DoD's much-anticipated Cybersecurity Maturity Model Certification regime for defense contractors, but also imposes a new mandate that contractors conduct and report the outcome of self-assessments of their compliance with the National Institute of Standards and Technology Special Publication 800-171 as required under the existing DFARS clause 252.204-7012.

DFARS 252.204-7021

In our February 2020 alert on the issue, we described the CMMC regime and DoD's plan to implement the regime in phases. Pursuant to that phase-in plan, for an initial period of five years (until September 2025), the new DFARS clause at 252.204-7021 (Cybersecurity Maturity Model Certification Requirements) will be incorporated into solicitations and contracts (except for those exclusively for commercial-off-the-shelf (COTS) items) if the contract statement of work requires CMMC compliance as a particular level, and such inclusion must be approved by the Office of Under Secretary of Defense for Acquisition and Sustainment. When DFARS 252.204-7021 is included in a contract, the contractor must be certified by an independent, accredited, third-party assessor (C3PAO) as compliant with the required CMMC level by the time of award. Following contract award, contractors must maintain the required CMMC level throughout contract performance, ensure that their subcontractors are compliant with their CMMC obligations and flow-down the DFARS clause as appropriate to lower-tier subcontractors.

After the initial five-year implementation period (beginning in October 2025), the CMMC regime will apply to *all* non-COTS solicitations and contracts above the micro-purchase threshold, and *all* defense contractors must have at least a CMMC Level 1 certification.

NIST SP 800-171 self-assessment

In addition to incorporating the CMMC regime into the DFARS, the interim rule introduces a new mandate that contractors conduct and upload the results of a basic self-assessment regarding compliance with the NIST SP 800-171 security requirements pursuant to the existing DoD cybersecurity clause at DFARS 252.204-7012 (a Basic Assessment). Pursuant to this mandate, contracting officers must:

1. Verify that any contractor that is required to implement NIST SP 800-171 upload its Basic Assessment to the Supplier Performance Risk System prior to contract award or the exercise of a contract option period, and
2. Incorporate the DFARS 252.204-7019 (Notice of NIST SP 800-171 DoD Assessment Requirements) and 252.204-7020 (NIST SP 800-171 DoD Assessment Requirements) in all solicitations and contracts, except those solely pertaining to COTS items.

In addition to these requirements, DoD may elect to conduct its own assessments of contractor facilities and systems if the criticality of the program or sensitivity of the information the contractor will handle so warrants. Finally, defense contractors must ensure that (i) they have appropriately flowed-down the relevant DFARS clauses in their subcontracts and (ii) all of their subcontractors to whom the requirements apply have a current Basic Assessment uploaded in SPRS.

Practical measures

Defense contractors should be actively preparing to comply with the CMMC regime and the NIST SP 800-171 self-assessment requirements as the November 30, 2020 effective date approaches. While DoD is receiving comments on the interim rule until that date, contractors should act on the assumption that the interim rule will be implemented in final form without modification and immediately undertake the measures to ensure compliance, including:

1. Conduct or update previous self-assessments regarding NIST SP 800-171 compliance, for use in uploading the Basic Assessment, and preparing for CMMC certification
2. Identify all system security plans and plans of action and milestones that may be relevant to both assessments
3. Ensure contracts, legal and IT personnel are familiar with the new rules and ready to assist
4. Be on the lookout for CMMC certification requirements in RFIs and RFPs

For assistance or questions, contact Cooley's government contracts team listed here.

Key Contacts

Christopher Kimball Washington, DC	ckimball@cooley.com +1 202 842 7892