Key Takeaways from the Department of Defense's Interim Rule on Assessing Contractor Implementation of Cybersecurity Requirements, Effective November 30, 2020

Litigation Alert
12.11.2020

The Department of Defense's (DoD) highly anticipated interim rule entitled "Assessing Contractor Implementation of Cybersecurity Requirements" (Rule) became effective on November 30, 2020, potentially impacting over 300,000 defense contractors and subcontractors.[1] With an eye toward enhancing the protection of sensitive unclassified information within the DoD supply chain and alleviating the rising costs to the U.S. economy resulting from malicious cyber activity,[2] this Rule first aims to enhance defense contractor compliance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 (800-171). While the Defense Federal Acquisition Regulation Supplement (DFARS) has required defense contractor compliance with 800-171 since 2016, compliance was inconsistent as DoD only verified compliance by contractor attestation. Significantly, on November 30, 2020, this Rule amended the DFARS to require DoD verification of 800-171 compliance prior to contract award. Further, and perhaps most notably, this Rule implements the Cybersecurity Maturity Model Certification (CMMC) framework to provide increased DoD assurance that Defense Industrial Base (DIB) contractors can adequately protect sensitive unclassified information.

Background

Controlled Unclassified Information (CUI) consists of "information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. However, CUI does not include classified information..."[3] Before November 4, 2010, each executive agency "employ[ed] ad hoc, agency-specific policies, procedures, and markings" to CUI leading to inefficient interagency document sharing and unnecessarily restrictive dissemination policies.[4] Executive Order (EO) 13556 established a government wide CUI Program seeking to standardize CUI safeguards, marking, and dissemination practices across the executive agencies. Specifically, EO 13556 notes that the order "shall be implemented in a manner consistent with...applicable Government-wide standards and guidelines issued by [NIST], and applicable policies established by the Office of Management and Budget."[5]

Therefore, in June 2015, NIST published 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations[,]" to "provide federal agencies with recommended security requirements for protecting the *confidentiality* of CUI...when CUI is resident in a nonfederal system and organization..." [6] Federal contractors often process, store, and transmit CUI when providing financial services or cloud services and when processing security clearances and healthcare data, etc.

SP 800-171 is essentially a codification of "security requirements for protecting the confidentiality of CUI when the information is resident in nonfederal systems and organizations..."[7] Stemming from the Federal Information Security Management Act of 2002 (FISMA), an 800-171 assessment contains 110 security controls across 14 separate categories. This assessment uses a scoring methodology, which reflects the net effect of 800-171 security requirements a contractor has not yet implemented. Further, there are three assessment levels (Basic, Medium, and High) reflecting the assessment's depth. Basic assessments are conducted by the contractor. Medium and High assessments are conducted by the Defense Contract Management Agency's (DCMA) Defense Industrial Base Cybersecurity Assessment Center (DIBCAC).[8]

In light of EO 13556, DoD amended the DFARS by adding section 252.204-7012 entitled "Safeguarding Covered Defense Information and Cyber Incident Reporting" in 2016.[9] Importantly, DFARS 252.204-7012 required defense contractors to: (1) flow down DFARS 252.204-7012 to all subcontracts involving covered defense information (CDI); (2) provide adequate security

for all covered contractor information systems which process, store, or transmit CDI; and (3) implement 800-171 security requirements for all covered contractor information systems.[10]

On September 21, 2017, DoD issued a memorandum regarding the implementation of DFARS 252.204-7012. [11] This memorandum required defense contractors to implement 800-171 no later than December 31, 2017. While DFARS 252.204-7008 notes that by submitting an offer, the offeror attests that it will implement 800-171 security requirements; before November 30, 2020, the DFARS did not provide for DoD verification or enforcement of such implementation. Therefore – notwithstanding this September 21, 2017 memorandum – defense contractors implemented 800-171 sporadically. This Rule seeks to remedy sporadic 800-171 implementation by including both verification and enforcement mechanisms.

To further enhance the DIB's cybersecurity posture, the Office of the Under Secretary of Defense for Acquisition & Sustainment (OUSD (A&S)) created the CMMC, which DoD released on January 31, 2020.[12] CMMC is a "verification mechanism to ensure appropriate levels of cybersecurity practices and process are in place to ensure basic cyber hygiene as well as protect CUI that resides on the DoD's industry partners' networks."[13] DoD plans to implement a phased CMMC rollout, ultimately migrating to the new CMMC framework over a five-year period. During this five-year period, inclusion of a CMMC solicitation requirement must be approved by OUSD (A&S). After September 30, 2025, DoD will require DFARS 252.204-7021, entitled "Cybersecurity Maturity Model Certification Requirements," in all DoD contracts above the micro-purchase threshold, excluding commercially available off-the-shelf items (COTS). DoD will also require prime defense contractors to flow down DFARS 252.204-7021 to all subcontracts.

General Mechanics of the Rule

NIST SP 800-171. DFARS 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting," must be included in all solicitations and contracts, including solicitations and contracts using Federal Acquisition Regulation (FAR) Part 12 procedures for the acquisition of commercial items, excepting solicitations and contracts solely for the acquisition of COTS items.[14] Further, DFARS 252.204-7012 must be flowed down to "subcontracts…for which performance will involve [CDI]." [15] This clause has required defense contractors to provide adequate security for covered contractor information systems since 2016, and adequate security – at a minimum – requires conducting a basic 800-171 self-assessment.[16]

This Rule amends the DFARS to include provisions 252.204-7019, "Notice of NIST SP 800–171 DoD Assessment Requirements," and 252.204-7020, "NIST SP 800–171 DoD Assessment Requirements."[17] Both provisions are now required in all defense contracts and subcontracts above the micro-purchase threshold excepting "acquisitions solely for commercially available off-the-shelf (COTS) items." If a defense contractor is required to conduct a basic 800-171 self-assessment,[18] DFARS 252.204-7019 requires this assessment to be current (within the last three years) and compels offerors to post the results of the self-assessment in the Supplier Performance Risk System (SPRS). The SPRS provides DoD visibility of completed 800-171 assessments and DoD contracting officers will leverage this visibility to verify 800-171 compliance prior to considering offerors for award.[19] DFARS 252.204-7020 requires defense contractors to provide the government with access to its facilities, systems, and personnel when it is necessary for DoD to conduct or renew a medium- or high-level 800-171 assessment. The Rule also mandates that the requirements of the clause flow down to all applicable subcontracts and that applicable subcontractors conduct and upload an 800-171 self-assessment to SPRS as well. Lastly, the Rule indicates that that the basic assessment requirement will be phased in over a three-year period.

Cybersecurity Maturity Model Certification. This Rule also amends the DFARS to add provision 204.75, "Cybersecurity Maturity Model Certification," and clause 252.204-7021, "Cybersecurity Maturity Model Certification Requirements."[20] CMMC will measure DIB contractors' institutionalization of cybersecurity processes and the implementation of cybersecurity practices. In short, CMMC will measure DIB contractors' cybersecurity maturity level. There are five maturity levels within this framework and each level is cumulative of the preceding level(s).[21]

- CMMC Level 1 consists of the 15 basic safeguarding requirements outlined in FAR 52.204-21.

- CMMC Level 2 consists of 65 security requirements from NIST SP 800–171 implemented via DFARS clause 252.204–7012, seven CMMC practices, and two CMMC processes. This level is intended as an optional intermediary step for contractors as part of their progression to Level 3. DoD does not anticipate releasing new contracts that requires contractors to achieve CMMC Level 2.
- CMMC Level 3 consists of all 110 security requirements from NIST SP 800–171, 20 CMMC practices, and three CMMC processes.
- CMMC Level 4 consists of all 110 security requirements from NIST SP 800–171, 46 CMMC practices, and four CMMC processes.
- CMMC Level 5 consists of all 110 security requirements from NIST SP 800–171, 61 CMMC practices, and five CMMC processes.

Solicitations containing DFARS 252.204-7021 will also note the required CMMC level offerors must achieve. Defense contractors must be certified at the requisite CMMC level at the time of award and maintain this certification for the duration of the contract. Contractors must also ensure subcontractors are certified at the appropriate CMMC level prior to subcontract award. Further, contractors can seek to achieve a certain CMMC level for their entire enterprise network or specific business segments depending on where protected information is processed, stored, or transmitted.

Contrary to the basic 800-171 assessment, self-attestation is not sufficient at any CMMC level. In order to achieve a specific CMMC level, defense contractors will undergo a CMMC assessment conducted by a CMMC Third Party Assessment Organization (C3PAO). After assessment, contractors will have a period to resolve issues identified during the assessment or any disputes with the assessment itself. The CMMC Accreditation Body (AB) will then review the C3PAO assessment and issue the appropriate three-year certification. Similar to the basic 800-171 self-assessment, this certification will be uploaded in SPRS for DoD visibility and verification. After the five-year phased CMMC rollout ending on September 30, 2025, DoD contracting officers will not make award or exercise an option if the contractor does not have a current (within three years) certification at the required CMMC level.

DoD expects to limit the number of solicitations specifying a CMMC requirement to 15 prime contracts in Fiscal Year (FY21), which will serve as the CMMC pilot program. OUSD (A&S) is also working with Military Services and DoD agencies to identify candidate pilot programs that will contain the CMMC requirement during the FY21-FY25 phased rollout. DoD will require defense contractors that do not process, store, or transmit CUI to obtain a CMMC Level 1 certification. Defense contractors that do process, store, or transmit CUI will be required to obtain a CMMC Level 3 or higher certification, depending on the CUI's sensitivity.

Evolving Issues. There are several points in the Rule that need clarification. Namely, industry has voiced concern regarding the distinction between controlled unclassified information and covered defense information, which may have compliance implications. The Rule does not indicate how DoD will use the 800-171 self-assessments during source selection. Additionally, the Rule does not indicate how unsuccessful defense contractors will learn that they were not awarded a contract due to improper 800-171 scoring when the contract is below the simplified acquisition threshold (SAT).[22] The Rule lacks details regarding the dispute process for 800-171 medium and high-level assessments and, similarly, CMMC assessments. Further, the Rule does not provide guidance on how prime contractors are to determine the appropriate CMMC level for their subcontractors to achieve prior to subcontract award. Understandably, a new rule's implementation comes with many industry questions and concerns. The points of clarification raised here are just a few of many.

Takeaways

Going forward, defense contractors and subcontractors with systems that process, store, or transmit CUI should be aware of DFARS 252.204-7008, 7012, 7019, and 7020. These clauses require basic 800-171 self-assessments, which DoD contracting

officers will verify in SPRS prior to contract award, when applicable. While CMMC will be phased in over five years with full implementation planned for October 1, 2025, defense contractors and subcontractors should also be aware of DFARS 252.204-7021, their current cyber hygiene, and the emergent requirement to institutionalize cybersecurity processes and practices. This awareness, implementation, and institutionalization will allow contractors to prepare for forthcoming third-party assessments, which will be required for all defense contractors. Prime contractors must also prepare to obtain 800-171 representations directly from subcontractors to which these rules apply, as SPRS visibility is limited to DoD personnel and a contractor's authorized representative.

For more information, please contact:

Jason N. Workmaster, jworkmaster@milchev.com, 202-626-5893

Elizabeth J. Cappiello, ecappiello@milchev.com, 202-626-5975

Joshuah R. Turner*

**Former Miller & Chevalier attorney*

---

[1] 85 Fed. Reg. 61505 (Sept. 29, 2020) .

[2] *See* February 2018 Council of Economic Advisers Report at 1 (noting costs between $57 billion and $109 billion in 2016 alone).

[3] 32 C.F.R. § 2002.4.

[4] *See* Executive Order 13556 (Nov. 4, 2010).

[5] *Id.*

[6] *See* NIST SP 800-171 Rev. 2 at 2.

[7] NIST SP 800-171 Rev. 2 at iii.

[8] *See* July 1, 2020 DoD Memorandum (Supplier Performance Risk System for [NIST] 800-171 Department of Defense Assessment).

[9] *See* DFARS 252.204-7012.

[10] Covered contractor information systems are unclassified information systems that are owned, or operated by or for a contractor that processes, stores or transmits CDI. *Id.*

[11] *See* September 21, 2017 DoD Memorandum (Implementation of DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting).

[12] *See* DoD January 31, 2020 Press Release; *see also* CMMC Version 1.0 Document.

[13] *See* OUSD (A&S) CMMC FAQ 5.

[14] *See* DFARS 204.7304.

[15] *See* DFARS 252.204-7012.

[16] *Id.*

[17] *See supra*, note 1.

[18] *See supra*, note 1 (noting that a basic assessment is required for each covered contractor information system); *see also supra*, note 15 (defining covered contractor information system).

[19] The Rule explains that 800-171 scores are protected in accordance with DoD Instruction 5000.79 and may only be accessed by DoD personnel and authorized representatives of the contractor.

[20] *See supra*, note 1.

[21] OUSD A&S released Assessment Guides for CMMC Levels 1 and 3, giving DIB contractors a clearer picture of what to expect and how to prepare.

[22] Mandatory debriefings are not required for contracts below the SAT. *See* FAR Part 13.