DOD's Cybersecurity Maturity Model Certification Program Takes a Step Forward

A breakdown of DOD's recently published interim rule to transition the Pentagon's current cybersecurity regime to the new CMMC program.

BY JACK HORAN

As discussed here in this column in the July 2020 issue of *Contract Management*,[1] the Department of Defense (DOD) has embarked on creating the Cybersecurity Maturity Model Certification (CMMC) program, "a unified cybersecurity standard for DOD acquisitions to reduce exfiltration of Controlled Unclassified Information (CUI) from the Defense Industrial Base (DIB)."[2]

On September 29, 2020, DOD published a much-anticipated interim rule to transition from the current cybersecurity regime under *Defense Federal Acquisition Regulation Supplement* (*DFARS*) 252.204-7012, "Safeguarding Covered Defense Information & Cyber Incident Reporting," to the CMMC program.[3]

DOD's Current Cybersecurity Requirements

Under DFARS 252.204-7012, DOD contractors and subcontractors must provide adequate security for "covered defense information" (CDI) – which is defined as follows:

> Unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies, and is –
>
> (1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DOD in support of the performance of the contract; or
>
> (2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.[4]

At a minimum, a contractor must provide the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations," in effect at the time the solicitation is issued or as authorized by the contracting officer. For an IT service or system operated on behalf of DOD, a contractor must also implement any additional security requirements specified by DOD in the contract.

In addition, a contractor must also "apply other information systems security measures" when the contractor "reasonably determines that additional information systems security measures may be required to provide adequate security in a dynamic environment or to accommodate special circumstances (e.g., medical devices) and any individual, isolated, or temporary deficiencies based on an assessed risk or vulnerability." These measures may be addressed in a system security plan. The clause specifies cyber incident responses and cyber incident reporting obligations of the contractor and requires the contractor to permit DOD access to equipment and information.[5]

In summary, under DFARS 252.204-7012, a contractor must –

- Provide the level of security required for the CDI available under the contract (starting with the minimum NIST SP 800-171 requirements),

- Create a security plan (if necessary), and
- Satisfy the government that the proposed security is adequate to protect the CDI required for the contract.

However, as DOD has noted, the "existing regulation [DFARS 252.204-7012]...is based on trust" and currently does not require any DOD or third-party verification that the contractor meets the *DFARS* requirements.

The Cybersecurity Maturity Model Certification Program

In March 2019, DOD began creating the Cybersecurity Maturity Model Certification (CMMC) program, which, as previously mentioned, is intended to be a unified DOD cybersecurity standard to reduce exfiltration of CUI from the DIB. The CMMC builds upon DFARS 252.204-7012 "by adding a verification component with respect to cybersecurity requirements." The CMMC reviews and combines "various cybersecurity standards and best practices and map[s] these controls and processes across several maturity levels that range from basic cyber hygiene to advanced." Most importantly, the CMMC will require contractors and subcontractors to receive a certification by third-party certifiers based on the level and maturity of cybersecurity practices implemented by the contractor.

The government program or project office will assess the level of maturity required for each DOD contract based on the type of contract and access to CDI the contractor will have. For example, contracts requiring access only to "federal contract information" (FCI)[6] will require only a Level 1 or Level 2 certification. Contracts that require access to or generation of CUI will likely require a Level 3 or Level 4 certification. Contracts that will likely be subject to what DOD refers to as "advanced persistent threats" (APTs) – i.e., cyberattacks from an "adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception)" – will require Level 5 certification. Based on the project office's recommendation, the contracting officer will list the maturity level required for a contractor to be eligible for award of the contract in the solicitation for the contract. Only contractors that have been certified to the identified maturity level can be awarded the contract.

The five maturity levels – ranging from Level 1 (the most basic) to Level 5 (the most secure) – are defined by increasingly numerous, complex, and sophisticated security "practices," and increasingly mature cybersecurity "processes." A *practice* is "a specific technical activity or activities that are required and performed to achieve a specific level of cybersecurity maturity for a given capability within a given domain," a *process* is a "specific procedural activity that is required and performed to achieve a capability level," and *processes* "[d]etail [the] maturity of an institution." Practices "measure the technical activities required to achieve compliance with a given capability requirement, and processes...measure the maturity of a company's" internal procedures.

Once the government awards the contract, the prime contractor, in consultation with the contracting officer, will undertake a similar process to identify the maturity level for each subcontract. Only subcontractors with that listed maturity level will be eligible for award of the subcontract. All new prime contracts and subcontracts in the DOD supply chain will be identified with a maturity level except for contracts and subcontracts for commercial of the shelf (COTS)[7] items.

DOD has made clear that without an appropriate certification, suppliers (other than COTS suppliers) *will not be eligible* to supply DOD once the CMMC program is implemented.

The Interim Rule

The recently issued interim rule begins the implementation of the CMMC program but also implements a separate assessment requirement – "NIST SP 800-171 DOD Assessment Methodology" – as a bridge between DFARS 252.204-7012 and the CMMC program. DOD promises that the two processes "will not duplicate efforts from each assessment, or any other DOD assessment, except for rare circumstances when a reassessment may be necessary, such as, but not limited to, when cybersecurity risks, threats, or awareness have changed, requiring a reassessment to ensure current compliance."

The interim rule amends DFARS Subpart 204.73, "Safeguarding Covered Defense Information and Cyber Incident Reporting," to implement the NIST SP 800-171 DOD Assessment Methodology and to phase in the CMMC program. The interim rule

creates the following new solicitation provisions and contract clauses:

- *DFARS 252.204-7019, "Notice of NIST SP 800-171 DOD Assessment Requirements"* – Advises offerors required to implement the NIST SP 800-171 standards under DFARS 252,204-7012 "of the requirement to have a current (not older than three years) NIST SP 800-171 DOD Assessment on record in order to be considered for award." The provision "requires offerors to ensure the results of any applicable current assessments are posted in the [Supplier Performance Risk System (SPRS) at https://www.sprs.csd.disa.mil/] and provides offerors with additional information on conducting and submitting an assessment when a current one is not posted in the SPRS."
- *DFARS 252.204-7020, NIST SP 800-171 DOD Assessment Requirements* – Requires a contractor to provide the government with access to its facilities, systems, and personnel when it is necessary for DOD to conduct or renew a higher-level assessment. The clause also requires the contractor to ensure that applicable subcontractors also have the results of a current assessment posted in the SPRS prior to awarding a subcontract or other contractual instruments. The clause provides additional information on how a subcontractor can conduct and submit an assessment when one is not posted in the SPRS, and requires the contractor to include the requirements of the clause in all applicable subcontracts.
- *DFARS 252.204-7021, Cybersecurity Maturity Model Certification Requirements* – Requires the contractor to have the CMMC certification at the level required in the solicitation by the time of contract award and to maintain the required CMMC level for the duration of the contract. A contractor can achieve a specific CMMC level for its entire enterprise network or particular segment(s) or enclave(s), depending on where the information to be protected is processed, stored, or transmitted.

Once the interim rule is effective, the NIST SP 800-171 DOD Assessment Methodology requirement will be applicable to all DOD contracts, including commercial item contracts, except for "acquisitions solely for [COTS] items." The interim rule also permits application of the CMMC program from the effective date of November 30, 2020, through October 1, 2025, and requires inclusion of CMMC requirements in all DOD solicitations and contracts, except for those exclusively for COTS items, after October 1, 2025. The applicable requirements must be "flowed down" to all subcontractors, including commercial item subcontracts, except for those exclusively for COTS items.

To implement the new requirements, contracting officers must include the clauses at DFARS 252.204-7019 and 252.204-7020 "in solicitations and contracts including solicitations

using FAR Part 12 procedures for the acquisition of commercial items, except for solicitations solely for the acquisition of COTS items." Contracting officers must include DFARS 252.204-7021 until September 30, 2025, "if the requirement document or statement of work requires a contractor to have a specific CMMC level" and after October 1, 2025, "in all solicitations and contracts or task orders or delivery orders, including those using FAR Part 12 procedures for the acquisition of commercial items, except for solicitations and contracts or orders solely for the acquisition of COTS items." To ensure an orderly, phased rollout of the CMMC program, "inclusion of a CMMC requirement in a solicitation [prior to October 1, 2025,] must be approved by the Office of the Under Secretary of Defense for Acquisition and Sustainment."

DFARS Subpart 204.73 directs contracting officers to verify in the SPRS that an offeror has a current NIST SP 800-171 DOD Assessment on record, prior to contract award, if the offeror is required to implement NIST SP 800-171 pursuant to DFARS 252.204-7012. When DFARS 252.204-7021 applies, contracting officers must verify in SPRS that the contractor's CMMC certification is current and meets the required level prior to making the award. Similarly, a contractor cannot award a subcontract unless the subcontractor has satisfied the applicable NIST SP 800-171 DOD Assessment Methodology requirements and the appropriate CMMC level requirements, if applicable.

The NIST SP 800-171 DOD Assessment Methodology

The Defense Contract Management Agency (DCMA) developed the NIST SP 800-171 DOD Assessment Methodology as DOD's "initial strategic DOD/corporate-wide assessment of contractor implementation of the mandatory cybersecurity requirements established in the contracting regulations." The Assessment Methodology provides for the assessment of a contractor's implementation of NIST SP 800-171 security requirements, as required by DFARS 252.204-7012. The resulting NIST SP 800-171 DOD Assessment reflects "the net effect of NIST SP 800-171 security requirements not yet implemented by a contractor."[8]

The NIST SP 800-171 DOD Assessment uses a standard scoring methodology, "and three assessment levels (Basic, Medium, and High), which reflect the depth of the assessment performed and the associated level of confidence in the score resulting from the assessment." The contractor or subcontractor completes a Basic Assessment, while the government completes Medium and High Assessments. The Assessments are completed for each covered contractor information system as required by DFARS 252.204-7012. The contractor (for Basic Assessments) or DOD (for Medium or High Assessments) must document the results in the SPRS to "provide DOD Components with visibility into the scores of Assessments already

At a minimum, a contractor must provide the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations," in effect at the time the solicitation is issued or as authorized by the contracting officer.

completed" and to "verify that an offeror has a current (i.e., not more than three years old, unless a lesser time is specified in the solicitation) Assessment, at any level, on record prior to contract award."

How Will Contractors and Subcontractors Know Whether the NIST SP 800-171 DOD Assessment or CMMC Applies?

When the interim rule becomes effective on November 30, 2020, all solicitations (except those solely for COTS items) will contain the new *DFARS* clauses implementing the NIST SP 800-171 DOD Assessment Methodology requirement.[9] The solicitations and contracts subject to the CMMC requirements will also contain DFARS 252.204-7021 and a statement of the certification level required for eligibility for award. DOD contractors should carefully review the solicitation to determine whether the contract will be subject to only the NIST SP 800-171 DOD Assessment Methodology requirement, or will also be subject to the CMMC requirements. Similarly, contractors, upon review of the solicitation and the items supplied by potential subcontractors, will have to work with the contracting officer to determine whether the CMMC requirements apply to the subcontract, and if so, what level of certification will be required.

What Should You Do Now?

DOD is committed to implementing the CMMC program, and to have it fully implemented by 2025. The publication of the interim rule is an important step in meeting that goal. Assuming the effective date of the interim rule does not change, beginning on November 30, 2020, DOD can include the requirement in solicitations. Even when CMMC requirements are not included, all DOD contract and subcontracts (except those solely for COTS items) will be subject to the new NIST SP 800-171 DOD Assessment Methodology requirements beginning on November 30, 2020.

Many contractors and subcontractors have been required to assess their compliance with NIST SP 800-171 under DFARS 252.204-7012. Contractors and subcontractors subject to such self-assessments should ensure that these assessments are compliant with the NIST SP 800-171 DOD Assessment Methodology so that the Assessment can be entered into the SPRS.

Contractors should also continue to prepare for the implementation of the CMMC program. As recommended in this column in the July 2020 issue, DOD contractors and subcontractors should organize a team of appropriate personnel from management, business development, information technology, compliance, and contract management to determine, at a minimum, the following:

- The current maturity level of its cybersecurity systems;
- The company's business goals in the DOD market, and the maturity level it will have to attain to meet those goals;
- The available resources to implement practices and processes required to reach the desired maturity level;
- The responsibility within the various components of the organization for creating, implementing, and ensuring compliance with the practices and processes necessary for certification under the CMMC program; and
- A schedule for making the required

changes to ensure the organization will not miss DOD contracting and subcontracting opportunities.

Level 1 certification will be the minimum required for all DOD contractors and subcontractors other than those providing COTS items. Contractors expecting to handle CUI will likely need at least a Level 3 certification, and for those contractors desiring access to the entire DOD market, a Level 5 certification will be required. **CM**

Jack Horan, JD

- Partner, Faegre Drinker Biddle & Reath LLP.
- General counsel, NCMA.

All information provided in this article is for general informational purposes only and does not, and is not intended to, constitute legal advice. For advice with respect to any legal matter, readers should consult with an attorney.

ENDNOTES

1 *See* Jack Horan, "The Current State of DOD's Cybersecurity Maturity Model Certification Program," *Contract Management* Magazine (July 2020): 8–17.
2 Unless otherwise noted, quotations in this article related to CMMC are from "Cybersecurity Maturity Model Certification (CMMC)," Version 1.2 (March 16, 2020) (CMMC v1.02), *available at* https://www.acq.osd.mil/cmmc/index.html.
3 Unless otherwise noted, all quotations in this article related to the interim rule are taken from 85 Fed. Reg. 61,505 (September 29, 2020).
4 DFARS 252.204-7012(a).
5 Contractors offering or using cloud computing services in the performance of a DOD contract must also satisfy the security requirements of DFARS 252.239-7010, "Cloud Computing Services."
6 *Federal contract information* is defined as "information, not intended for public release, that is provided by or generated for the government under a contract to develop or deliver a product or service to the government, but not including information provided by the government to the public (such as on public Web sites) or simple transactional information, such as necessary to process payments." (*Federal Acquisition Regulation* (*FAR*) 52.204-21).
7 As defined at FAR 2.101.
8 Editor's Note: Information on the NIST SP 800-171 DOD Assessment Methodology is available at https://www.acq.osd.mil/dpap/pdi/cyber/strategically_assessing_contractor_implementation_of_NIST_SP_800-171.html.
9 I.e., DFARS 252.204-7019 and 7020.

DOD is committed to implementing the CMMC program, and...[t]he publication of the interim rule is an important step in meeting that goal.