Department of Defense Addresses Cybersecurity

By J. William Eshelman / Nov 19, 2020

On Sept. 29, 2020, the Department of Defense (DOD) issued three new provisions to the Defense Federal Regulation Acquisition Supplement relating to information security. These new provisions implement DOD's Interim Rule of the same date entitled Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041). The new provisions (which become effective Nov. 30, 2020) are:

- DFARS 252.204-7019, Notice of NIST SP 800-171 DoD Assessment Requirements;
- DFARS 252.204-7020, NIST SP 800-171 DoD Assessment Requirements; and
- DFARS 252.204.7021, Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirement.

Overview

These new provisions implement two significant new programs addressing cybersecurity that require federal contractor compliance:

- The Cybersecurity Maturity Model Certification (CMMC) and
- The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 Assessment Methodology.

Both programs impose new assessment and certification requirements on both prime contractors and subcontractors throughout the supply chain. The only exception to their universal application appears to be concerning commercial-off-the-shelf (COTS) items, but even that exception is somewhat doubtful. The doubt arises from the preamble to the Interim Rule, which recites that these new provisions will not apply to micro-purchases. Yet, the implementing DFARS sections, [DFARS 204.7304(d)-(e)] include no COTS exception to plenary applicability.

Implementation of these sweeping requirements is without a standard period for public comment because DOD has determined that there is an urgent and compelling need to protect sensitive information. That determination was made under 41 U.S.C. § 1707(d) and FAR 1.501-3(b).

Although DOD specifies that it plans to use a "phased approach" to the incorporation of the CMMC requirements into solicitations and contracts over the next five years (beginning Nov. 30, 2020, with an anticipated "complete implementation" date of Oct. 1, 2020) the possibility of amending existing contract vehicles to fully include these requirements before Oct. 1, 2020, is not excluded. Thus, it is important for federal contractors to remain alert, and to prepare for that possibility as well as the new compliance requirements as they phase in.

Baseline Security Requirements Remain in Effect

Note should be taken that the baseline security requirements of DFARS 252.204-7012 remain in effect. The new DFARS are supplemental, not exclusive, to that existing requirement. Preexisting concern for contractor compliance with the security controls set forth in NIST SP 800-171 resulted in DOD 2019 instruction to Defense Contract Management Agency (DCMA) to create a program for assessing contractor compliance with the 110 security controls contained in NIST SP 800-171 where contracts were subject to DFARS 252.204-7012. [That DFARS applies to contractors with information systems that store, process, or transmit controlled unclassified information (CUI).] DOD apparently was concerned that the DFARS 252.204-7012 information security regime relies primarily on contractor-initiated plans and self-assessments amounting primarily to a "documentation exercise" lacking mandatory government oversight or explicit timing requirements.

The NIST SP 800-171 Assessment Methodology

The new DFARS 252.204-7019 and -7020 becoming effective on Nov. 30, 2020, will implement DCMA's NIST SP 800-171 Assessment Methodology. The DCASMA Program requires that contracting officers incorporate the NIST SP 800-171 Assessment Methodology into all solicitations and contracts exceeding the micro-purchase threshold (other than COTS items).

The Assessment Methodology employs two parts, each based on the development of a weighted score and a confidence level score. The scoring system is weighted to measure the extent a given offeror or contractor has implemented NIST SP 800-171's security controls. Confidence-level scores are based on the particular assessment involved. There are three levels of confidence, basic, medium, and high. The Basic Assessment level relies on a contractor's self-generated assessment materials. Thus, it provides the lowest level of confidence.

The Medium Assessment level adds a government review of a contractor's Basic Assessment at face value and adds discussion of any government concerns with the contractor.

Finally, the High Assessment level includes all of the components included in the Basic and Medium Assessments, but also adds validation and verification of each element. This produces a "High" confidence in the effectiveness of the contractor's implementation.

Contractors may dispute a government confidence assessment using an ill-defined procedure outlined in DFARS 252.407-7020(e)(2).

The Supplier Performance Risk System

The most likely concern to contractors will be that the assessment information will be stored in the publicly available Supplier Performance Risk System (SPRS). The SPRS will provide the summary-level scores for a given type of assessment, as well as a description of the contractor security system plan's architecture, the date of assessment, and (if applicable) the date by which the contractor will achieve a full score. Before the award of a contract or an extension to an existing contract, DFARS 204.7303(b) requires verification (in the SPRS) that the contractor or offeror has a "current assessment (i.e., not more than 3 years old unless a lesser time is specified in the solicitation) for each covered contractor information system that is relevant to the offer, contract, task order, or delivery order." DFARS 252.407-7020 is a mandatory flow down for all except COTS items. Of particular interest may be the recent "tweaking" of the definition for Commercial Items under the FAR.

CMMC Security Policies and Controls

Adding another level of complexity, the new DFARS 252.204.7021 follows DOD's final CMMC security policies and controls, which are divided into five "Maturity Levels." Maturity Level 1 aligns with the 15 controls reflected in FAR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems.

Maturity Level 2 is intermediary Maturity and intended to assist contractors to move from Maturity Level 1 to Maturity Level 3. Maturity Level 3 is mandatory for contractor information systems that will store, transmit, or process CUI. Maturity Level 3 requires contractors to have implemented all 110 security controls contained in NIST SP 800-171 as well as 23 additional CMMC-required practices and processes. Maturity Levels 4 and 5 implement yet more sophisticated cybersecurity requirements, which are primarily intended to combat advanced persistent threats (APTs).

Contractors subject to the CMMC under DFARS 252.204.7021 mandatorily must undergo formal assessments "conducted by accredited CMMC Third Party Assessment Organizations…" If a contractor completes the assessment successfully, it will be issued a certification by a CMMC Accreditation Body (AB) that will attest that the company has implemented required cybersecurity controls. Like the NIST SP 800-171 Assessment Methodology, companies must hold an active CMMC certification for the required CMMC Maturity Level before award or government exercise of an option period -- if the solicitation or contract incorporates DFARS 252.204-7020. These also are mandatory flowdowns. Moreover, and before the award of a subcontract, prime contractors (or a higher-tier subcontractor) must verify that the subcontractor holds a current CMMC certification for the appropriate Maturity Level.

Conclusion

Undoubtedly there will be "fits and starts" in the application of the new DFARS provisions. Heavy contributors (among others) to those challenges will be important questions concerning exactly how contracting officers will factor SPRS summary scores (under the NIST SP 800-171) Assessment Methodology into procurement decisions and contract actions.

In addition, the matter of how contractors should treat compliance costs is unresolved. This can be a particularly nettlesome point, given the False Claims Act implications that the government almost reflexively attaches to disagreements involving cost treatment.

Finally, there is the matter of COTS itself; and the Oct. 19, 2019 changes to the definition of "Commercial Item" and the operation with these new DFARS remain to be digested in practice.

The views and opinions expressed in the article represent the view of the author and not necessarily the official view of Clark Hill PLC. Nothing in this article constitutes professional legal advice nor is intended to be a substitute for professional legal advice.