THE GOVERNMENT CONTRACTOR®

THOMSON REUTERS

Information and Analysis on Legal Aspects of Procurement

Vol. 62, No. 38 **October 14, 2020**

FOCUS

¶ 287

FEATURE COMMENT: *They're Here*: New Cybersecurity Rules And Requirements Arrive To Haunt Defense Contractors

Undoubtedly a great film for its day, the 1982 classic *Poltergeist* might not have aged as well as the filmmakers had hoped. But the vivid imagery, jump scares and creepy marketing the PG-rated "family" movie employed remain burned into the minds of many. For those unfamiliar with the Spielberg classic, a "poltergeist" is largely understood as a ghost or other supernatural being responsible for physical disturbances such as loud noises and thrown-around objects. As seasoned Government contractors know all too well, the same could be said of cybersecurity regulations. Don't believe us? Just ask your information technology and information security professionals about the coffee mug shards scattered in the corner or the stapler embedded into the computer monitor. Constantly evolving cybersecurity regulations, arriving seemingly out of nowhere, are a fact of contractor life and are as sure to strike as that creepy clown doll in the rocking chair. As if on cue, more have arrived. Was that a crash we heard?

"Run to the light, Carol Anne. Run as fast as you can!"—In an effort to "enhance the protection of unclassified information within the [Department of Defense] supply chain," and meet its fiscal year 2020 National Defense Authorization Act mandate for the creation of "unified cybersecurity ... regulations ... to be imposed on the defense industrial base for the purpose of assessing the cybersecurity of individual contractors," DOD issued an interim rule refining the cybersecurity requirements demanded of all defense contractors on Sept. 29, 2020. See Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041), 85 Fed. Reg. 61505 (Sept. 29, 2020); National Defense Authorization Act for Fiscal Year 2020, P.L. 116-92, § 1648. Built on the foundation of existing FAR and DFARS cybersecurity requirements, the interim rule is intended to provide a cybersecurity "assessment methodology and framework" for contractors and subcontractors. Effective Nov. 30, 2020, the interim rule creates a mechanism pursuant to which DOD will begin assessing the current status of contractor implementation of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171. In this respect, the interim rule requires contractors and subcontractors to take steps to fully implement existing cybersecurity requirements, plus additional processes and practices, to protect Federal Contract Information (as defined in FAR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems) and Controlled Unclassified Information (CUI) in preparation for verification under the Cybersecurity Maturity Model Certification (CMMC) Framework.

The two-pronged approach adopted by the interim rule is not intended to be duplicative. DOD expects the CMMC framework to be predicated on a contractor's existing NIST SP 800-171-compliant architecture and commensurate with the existing obligations resident in DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting. For DOD contractors not in possession of Covered Defense Information (CDI) or CUI (and therefore existing outside of the ambit of -7012), the CMMC framework will require a complete overhaul of IT architecture sometime before Sept. 30, 2025 in order to keep DOD as a customer. The requirements may come well before this five-year mark if DOD's Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)) determines a particular solicitation or statement of work requires a specific CMMC level.

Key dates stemming from the interim rule include:

Nov. 30, 2020: Comment period closes for the interim rule

Nov. 30, 2020: interim rule becomes effective

Nov. 30, 2020–Sept. 30, 2025: CMMC requirements to be included in solicitations upon approval of DOD's OUSD(A&S)

Oct. 1, 2025: CMMC will apply to ***all*** DOD contracts except those for commercially available off-the-shelf (COTS) items

See generally, 85 Fed. Reg. 61505.

Notable changes and creations introduced in the interim rule include:

Amends DFARS 204.7302, Policy

Revises DFARS 204.7303, Procedures

Amends DFARS 204.7304, Solicitation provisions and contract clauses

Adds DFARS subpt. 204.75, Cybersecurity Maturity Model Certification

Creates DFARS 252.204-7019, Notice of NIST SP 800-171 DOD Assessment Requirements (NOV 2020)

Creates DFARS 252.204-7020, NIST SP 800-171, DOD Assessment Requirements (NOV 2020)

Creates DFARS 252.204-7021, Contractor Compliance with CMMC Level Requirements (NOV 2020)

Id.

After years of stalling, DOD is ready for a "jump scare" of its own. With the interim rule effective in approximately six weeks, the cybersecurity assessments it contemplates are expected to be completed sooner rather than later. The long-looming specter of CMMC is now larger than ever and should begin drawing the attention and consternation of contractors for years to come. DOD is in fact demanding that the defense industrial base (DIB) "run to the light…run as fast as you can" to meet its cybersecurity expectations. For those of you who like to read while you run, we have distilled below the practical implications of the interim rule along with some advice on how best to battle the poltergeists in your own companies.

DOD Assessment Requirements: *"You can't choose between life and death when we're dealing with what is in between"*—Like much of 1980s suburbia, the Freelings' home in *Poltergeist* possessed an extra-dimensional portal in their children's closet. In order to rescue her kidnapped daughter from the "other side," JoBeth Williams' Diane Freeling ties a rope around her waist, wades into the closet, retrieves young Carol Anne, then promptly falls through the ceiling covered in ectoplasmic residue (as one does). After years of wading through an amalgam of regulations and NIST requirements, contractors now have their own new dimension to navigate: the interim rule's NIST SP 800-171 DOD Assessment Methodology. So let's make sure that knot is tight.

As evidenced by its title, the NIST SP 800-171 DOD Assessment Methodology provides guidance and the processes necessary for contractors to certify their compliance with the 110 NIST SP 800-171 security requirements imposed by DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, in order to properly protect CUI. This assessment, however, is where some of the interim rule's efforts crash through the ceiling in a puddle of goo.

The interim rule clarifies the application of the NIST SP 800-171 requirements by amending DFARS 204.7302(a) to include specific direction that contractors,

> required to implement NIST SP 800-171, in accordance with the clause at 252.204-7012, Safeguarding Covered Defense Information and Cyber incident Reporting, are required at time of award to have at least a Basic NIST SP 800-171 DoD Assessment that is current (i.e., not more than 3 years old unless a lesser time is specified in the solicitation).

85 Fed. Reg. 61519; DFARS 204.7302(a)(2).

While we'll explain the DOD Assessment just below, the challenge most contractors will face with this new language is the omnipresence of DFARS 252.204-7012 in many contracts where it simply does not belong. The interim rule presupposes (wrongly) that -7012 is incorporated correctly by DOD acquiring activities and completely ignores and does nothing to remedy DOD inspector general findings that "DoD Component contracting offices and requiring activities *did not* establish processes to … notify contractors of the specific CUI category related to the contract requirements; determine whether contractors access, maintain, or develop CUI to meet contractual requirements; [and] mark documents that contained CUI and notify contractors when CUI was exchanged between DoD agencies and the contractor." *Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems* (DODIG-2019-105) (emphasis added) available at *www.dodig.mil/reports.html/Article/1916036/audit-of-protection-of-dod-*

controlled-unclassified-information-on-contractor-ow /; 61 GC ¶ 233.

The DOD IG went on to find that "DoD Component contracting offices and requiring activities did not always know which contracts required contractors to maintain CUI because the DoD did not implement processes and procedures to track which contractors maintain CUI." Id. Accordingly, if the NIST SP 800-171 DOD Assessment Methodology required by the interim rule is truly interrelated with DFARS 252.204-7012, contractors and subcontractors will need to be fully cognizant of that clause's presence and its effect. To the extent a contractor or subcontractor does not believe CDI or CUI is required to be held in order to perform the contract, it will need to be very clear of that upfront and seek the exclusion of DFARS 252.204-7012 from the contract if it does not apply. That has not been a common conversation since the clause has been introduced.

Factor that may now aid in that conversation in the near and long-term are the new clauses created when CDI, and therefore DFARS 252.204-7012, may be present in contract performance. The interim rule creates two new clauses that contractors may begin seeing with regularity after November 2020:

DFARS 252.204-7019, Notice of NIST SP 800-171 DOD Assessment Requirements (NOV 2020)

Pursuant to DFARS 204.7304(d), the clause at DFARS 252.204-7019 requires that for any offeror to be considered for award, that offeror must—within the last three years—perform and hold a NIST SP 800-171 DOD Assessment for each covered contractor information system that is relevant to the offer, contract, task order or delivery order. 85 Fed. Reg. 61520, DFARS 252.204-7019(b). The clause, which is required to be incorporated in all solicitations except those for the acquisition of COTS items, goes on to require that each offeror verify that the summary level scores associated with the assessments are posted in the Supplier Performance Risk System (SPRS). 85 Fed. Reg. 61520, 61521, DFARS 252.204-7019(c)(1)). Or, if the offeror has no summary level scores posted in SPRS, the clause permits the submission of a "Basic Assessment" (described in more detail below) to *webptsmh@navy.mil* for posting to SPRS in the format identified in paragraph (d) of the clause, which addresses the format and content required for a submission, the different levels of assessments (Basic (contractor-reported) or Medium/High (DOD-reported)) available, and the process by which the assessments may be reviewed/seen. 85 Fed. Reg. 61521.

DFARS 252.204-7020, NIST SP 800-171, DOD Assessment Requirements (NOV 2020)

Like -7019, DFARS 252.204-7020, NIST SP 800-171, DOD Assessment Requirements, is also to be included in all non-COTS acquisitions and is directed at covered contractor information systems. Unlike -7019, the DFARS clause at 252.204-7020 swings the closet door wide open and invites Government "access to [Contractor] facilities, systems, and personnel necessary for the Government to conduct a Medium or High NIST SP 800-171 DoD Assessment." 85 Fed. Reg. 61521, DFARS 252.204-7020(c). After conducting that Medium and High Assessment, the Government will provide the summary level scores to the contractor and will provide the opportunity for a 14-day rebuttal period and adjudication of assessment summary level scores prior to posting the summary level scores in the SPRS. Id., DFARS 252.204-7020(e)(1), (e)(2). The clause is intended to be included in all subcontracts and dictates that a contractor not award a subcontract or other contractual instrument unless the subcontractor has, similarly, completed at least a Basic NIST SP 800-171 DOD Assessment for all covered contractor information systems relevant to its offer within the last three years or otherwise submit a Basic Assessment for posting in SPRS. 85 Fed. Reg. 61522, DFARS 252.204-7020(g).

For contractors already tied in to the requirements of NIST SP 800-171, the jump into the extra-dimensional closet of the DOD Assessment requirements will be likely a quick, ectoplasm-free journey. That said, a math-heavy examination applying the NIST SP 800-171 DOD Assessment Methodology will still be required.

NIST SP 800-171 DOD Assessment Methodology: *"You left the bodies and you only moved the headstones!! YOU ONLY MOVED THE HEADSTONES!!! WHY?! WHY?!"*—The crux of the Freelings' story in *Poltergeist* (spoilers) is that their house was built on a graveyard after the developer chose not to relocate the deceased. Violent hauntings, reasonably, ensued. Similarly, DOD, wanting to avoid a "Cuesta Verde"-type situation (and resulting hauntings), wants to better understand the manner in which contractors expect to protect their data. The DOD Assessment Methodology referenced in the interim rule is addressed at length through a separate document available through the Defense

Pricing and Contracting website, under the heading for "Cyber" and the tab "Strategically Assessing Contractor Implementation of NIST SP 800-171." It may be the work of a malevolent spirit, but note that the link referenced in the interim rule is already obsolete and will not land you at the correct location: NIST SP 800-171 DOD Assessment Methodology, Version 1.2.1, June 24, 2020 (NIST Methodology). Once it's located, however, you will find over 20 pages explaining how to use the NIST Methodology.

The purpose of the NIST Methodology is simple and straight forward: to allow for DOD to conduct a strategic assessment of a contractor's (or a prime's assessment of a subcontractor's) implementation of NIST SP 800-171, as required by DFARS 252.204-7012. It is to be "used for assessment purposes only and does not, and is not intended to, add any substantive requirements to either NIST SP 800-171 or DFARS clause 252.204-7012." NIST Methodology at 3.

At the outset, it is worth noting that the methodology is premised on contractors being able to "mark or otherwise identify, *in accordance with direction contained within the specific contract*, DoD CUI that is collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of performance of the contract." NIST Methodology at 2 (emphasis added). We raise this point because, as noted above, much of what is expected of contractors is premised on DOD being able to (1) identify CUI and (2) direct the contractor as to how to manage what the Government deems to be CUI.

The NIST Methodology consists of three levels of assessment, each of which provides the assessor with a respective "confidence level":

- **Basic**: A contractor self-assessment based on a review of the system security plan(s) (SSP) associated with the covered contractor information system(s), and conducted in accordance with (i) NIST SP 800-171A, "Assessing Security Requirements for Controlled Unclassified Information," and (ii) Section 5 and Annex A of the NIST Methodology. This results in a "Low" confidence level due to it being self-reported.
- **Medium**: A review of the contractor's *SSP description* of how each NIST SP 800-171 requirement is met conducted by trained DOD personnel, anticipated as Program Management Office cybersecurity personnel, as part of a separately scheduled visit (e.g., for a Critical Design Review). The assessor is expected to examine the SSP descriptions to identify any descriptions that may not properly address the security requirements. This will result in a "Medium" confidence level and be recorded by the DOD assessor in SPRS.
- **High**: Presently able to be performed as an on-site (preferred) or virtual assessment (due to the COVID-19 pandemic), the assessment is conducted by trained DOD personnel using NIST SP 800-171A. It requires a "thorough on-site or virtual verification/examination/demonstration" of the Contractor's SSP and its implementation of the NIST SP 800-171 security requirements. Actions contemplated at this level of review may include evidence and/or demonstration of compliance (e.g., recent scanning results, system inventories, configuration baselines, demonstration of multifactor authentication) and will result in a confidence level of "High."

NIST Methodology at 3–5.

A notable element of the "High Assessment" is that its first step is the contractor's "Basic" self-assessment. That assessment is then submitted to and evaluated by DOD. The High Assessment then performs a "thorough document review and discussion with the contractor regarding the results to obtain additional information or clarification as needed, combined with government validation that the security requirements have been implemented" as described in the SSP. Perhaps most notable in the High Assessment is that it expressly notes that "**Network access by the assessor(s) is not required.**" NIST Methodology at 5 (emphasis added).

Scoring in the NIST Methodology is akin to darts, or maybe cricket. It's intended to serve as an "objective assessment" of NIST SP 800-171 implementation status and does not provide credit for partial implementation in most instances (but there are a few exceptions). In practice, contractors should start their assessment as if all 110 NIST SP 800-171 requirements have been met (and thereby the contractor has achieved 110 points), from which the score is reduced by any requirement not yet implemented. Further complicating the scoring methodology is the fact that not all requirements are weighted equally. For example, while implementing Requirement 3.1.1: *Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems)* will give you one

(1) point, **not** having it implemented will cost you five (5) points. All told, there are forty-three (43) "five point" requirements, fourteen (14) "three point" requirements, two (2) "three point" ***or*** "five point" (depending) requirements (related to the scope of multi-factor authentication (3.5.3) and FIPS validated encryption (3.13.11) implementation), and fifty-one (51) "one point" requirements.

The critical requirement to the NIST Methodology is the presence of the SSP (3.12.4). Without the SSP, a contractor cannot be scored. In addition, a contractor gets no credit for anything that is not fully implemented—meaning that contractors will lose critical points for requirements if they have an open Plan of Action and Milestones addressing weaknesses and gaps in meeting the NIST 800-171 requirements. While a contractor can achieve a maximum score of 110, a contractor with only an SSP could be scored at -207. Beyond this basic understanding, there is, of course, a lot of nuance when it comes to the scoring of the NIST Methodology that will require significant examination while performing any assessment. As reflected in the new clauses at 252.204-7019 and -7020, the NIST Methodology includes directions and instructions addressing how the assessment results will be posted on SPRS by either the contractor (for a Basic Assessment through the Procurement Integrated Enterprise Environment) or the Government (for a Medium or High Assessment), and how those assessments can be viewed and held by DOD personnel and authorized representatives of the contractor.

When applying the NIST Methodology, it is crucial that contractors don't just "move the headstones," they need to dig. The Basic Assessment is straight forward, but the challenge will come with the Medium and High Assessments. At these levels, Government assessors (equipped with nascent training and varied backgrounds) will be performing their assessments against a backdrop of insufficient DOD CUI guidance. When this happens, it will surely be the contractor who will feel the pain, so preparation and a keen understanding of what is expected by your contract's data-handling requirements is critical. After all, no one wants body-filled coffins erupting from your systems amidst the rainstorm of a Government assessment.

CMMC Requirements: *"I don't like the tree, Dad"*—Looming outside the window of young Robbie Freeling in *Poltergeist* was a knotty oak that took a menacing tone at night. With branches knocking and scratching at his window for days, the tree ultimately came to life, crashed through the glass, grabbed the boy, then swallowed him whole. You guessed it—*time to discuss the CMMC*.

We will forgo a rehash of the CMMC other than to remind readers that it is a unified standard for implementing cybersecurity across the DIB consisting of five, tiered certification levels, assessed by accredited CMMC Third Party Assessment Organizations (C3PAOs), and is intended to reflect the maturity and reliability of a contractor's cybersecurity infrastructure to safeguard Federal Contract Information, CUI or CDI resident on contractors' information systems. After years of rattling around, the interim rule now introduces the certification to the DFARS in a new subpart 204.75 and promises to swallow cybersecurity whole within its phased roll-out over the next five years.

Building upon the foundation of the NIST SP 800-171 DOD Assessment Methodology, the CMMC Framework set forth in the interim rule intends to add "a comprehensive and scalable certification element to verify the implementation of processes and practices associated with the achievement of a cybersecurity maturity level." 85 Fed. Reg. 61505. Over the course of its five-year roll-out, all DIB contractors are expected to achieve a CMMC certificate by an independent CMMC accreditation body at the appropriate CMMC level specified in the solicitation on which they are bidding. 86 Fed. Reg. 61506. Notably, the interim rule makes clear that while proposals may be submitted before the contractor receives a particular level, it must have achieved that required level by the time of award and then must maintain that level for the life of the contract, task order or delivery order, if such certificate is required by the applicable statement of work or requirement document. Id. See also DFARS 204.7501(b). The certificate, however, may not be more than three years old. Thus, for longer-running contracts, contractors will need to plan accordingly to ensure that any initial certification does not lapse.

While there is no doubt that CMMC will be crashing into our collective bedrooms, expect the manner in which it will appear to be very … very slow. Until Sept. 30, 2025, the new DFARS clause 252.204-7021, Contractor Compliance with CMMC Level Requirements, will only appear in contracts for non-COTS items if (i) the applicable requirement document or statement of work requires a contractor have a specific CMMC level, ***and*** (ii) its inclusion has been approved by the

OUSD(A&S). 85 Fed. Reg. 61520, DFARS 204.7503(a). It is only on or after Oct. 1, 2025, that all contractors should expect to see the new DFARS clause 252.204-7021, Contractor Compliance with CMMC Level Requirements, in non-COTS solicitations and contracts, task orders or delivery orders (DFARS 204.7503(b)). Id., DFARS 252.204-7021(c). When CMMC is in play, the contracting officer may neither award to an offeror that does not possess the requisite CMMC level, nor may she exercise an option or extend any period of performance unless the contractor has a CMMC certificate at the level required by the contract.

How, exactly, one survives a boy-eating tree is a mystery. Another mystery is how, precisely, CMMC functions in live contractual instruments. While the standard is established and is readily available for review and application (*www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf*) the application and assessment may be akin to getting pulled through a window. The cadre of necessary C3PAO assessors is still being established, and the tireless efforts of the organization charged with developing the education and training needed for those C3PAOs—the all-volunteer CMMC accreditation body—got derailed over the summer by leadership changes and allegations of conflicts of interest. None of that, however, should hinder defense contractors from pressing ahead and preparing to meet the CMMC requirements with which they expect they will have to comply. For most contractors and contractors currently holding CUI or CDI, expect to target, at the very least, Level 3. If a contractor is only just now hearing about this despite a significant history of defense contracts, target a Level 1 or 2. The tree is crashing through the window, you need to move or get swallowed.

DOD Cybersecurity 3.0: ***"There is no death. It is only a transition to a different sphere of consciousness"***—While the interim rule has been a long-time coming, its contents are not unexpected. The requirement that contractors protect and safeguard DOD data has been resident in contracts, in one form or another, since 2013. The interim rule further concretizes those obligations by (1) demanding that cybersecurity assessments be taken seriously; (2) harkening for the rise of CMMC; and (3) laying most the cost of those efforts—in terms of time, dollars and uncertainty—on the contractor. So while questions may persist—for example, as to CUI identification and marking—it is incumbent upon contractors to get to the bottom of the issue as soon as possible lest they bear the brunt of additional obligations and associated risks of noncompliance. For experienced defense contractors, this should not be a herculean endeavor at this point in the script. Working together, your compliance, legal and IT/IS teams should be able to navigate you to a serene conclusion and a report that: "This house is clean."

✦

This Feature Comment was written for The Government Contractor by **Alexander Major** ***and*** **Franklin Turner,** ***Partners and Co-Leaders of the Government Contracts & Global Trade Practice Group at McCarter & English, LLP.***