THE GOVERNMENT CONTRACTOR®

THOMSON REUTERS®

Information and Analysis on Legal Aspects of Procurement

Vol. 63, No. 45 December 8, 2021

Focus

¶ 359

FEATURE COMMENT: Get Back: DOD Retreats While Revealing Plans For CMMC 2.0

Over the Thanksgiving holiday, Disney+ released "*The Beatles: Get Back*," a three-part, seven-plus hour documentary intimately showcasing the Fab Four's creation of songs for what would ultimately become their final albums as a band (including such classics as "Abbey Road" and "Let It Be"). At the deft hand of director Peter Jackson, more than 60 hours of archival film footage has been digitally restored into a high-definition miracle that, save for the absence of face masks, looks like it was shot last year (not a half-century ago). The documentary shines a futuristic backlight not only on the creativity and musical genius of George, John, Paul and Ringo—but it also examines how the band gradually imploded on itself as the then-young superstars grappled with the realities of life, immense fame and one-of-a-kind artistry. The series (which we *strongly* recommend) provides unique insight into why and how productive and inspired ideas sometimes cannot overcome the reality of the world in which they are created. Enter the Cybersecurity Maturity Model Certification (CMMC) saga.

While we will in no way attempt to belittle the Beatles' legacy with a direct comparison between a one-of-a-kind band and regulatory requirements governing federal procurements, we can't help but note how the Department of Defense appears to be looking backward for the future of cybersecurity in its release of CMMC 2.0. While this may come as a welcome relief for many contractors who have been (or who should have been) dancing to this tune for years, there is a new backbeat—a remix, if you will—provided by the Department of Justice's Civil Cyber Fraud Initiative that could herald the end of contractor cybersecurity complacency. Discussed below are the significant hits surrounding CMMC and some educated suggestions as to how best to "listen" to the new tracks DOD is preparing to release.

The Long and Winding Road—CMMC 1.0— On Nov. 4, 2021 (following a period of purportedly extensive review), DOD unveiled its new vision of CMMC (CMMC 2.0). The revised standards, described in general terms on the website of the Office of the Under Secretary of Defense for Acquisition & Sustainment (OUSDAS) are a significant change from the initial set of standards that evolved over the past three and a half years. See *www.acq.osd.mil/cmmc/index.html*. However, before we can be led to that door, let's look at the wild and windy night that brought us here.

Reportedly working with DOD stakeholders, University Affiliated Research Centers, Federally Funded Research and Development Centers, and industry, CMMC 1.0 was initially envisioned by DOD as a set of requirements to be stapled to contracts where covered defense information (CDI) is present. The purpose of CMMC 1.0 was to calibrate the cybersecurity competency of federal contractors as graded against a tiered, five-level cybersecurity maturity model ranging from basic hygiene to state-of-the-art. The actual level required was intended to reflect the given acquisition's specific needs for security controls and institutionalized cybersecurity processes. The hope was to create a baseline against which contractors would be judged capable of being adaptive enough to keep up with pending information security threats.

Beginning with its tumultuous rollout, CMMC 1.0 evolved with intentions to include a broad spectrum of compliance elements, including alignment with the requirements of Defense Federal Acquisition Regulation Supplement 252.204-7012; real-time scoring of a contractor's cybersecurity compliance; redefined definitions of CDI and Controlled Unclassified Information (CUI); and a more granular timeline for CMMC implementation. DOD had identified the focus (in since-removed public notifications) as providing "increased assurance to DOD that a [Defense Industrial Base (DIB)] contractor can adequately protect CUI at a level commensurate with the risk, accounting for information flow down to its subcontractors in a multitier supply chain."

As of Jan. 30, 2020, when CMMC 1.0 was formally revealed, see *www.defense.gov/News/News-Stories/Article/Article/2071434/dod-to-require-cybersecurity-certification-in-some-contract-bids/*, DOD had created a robust matrix of requirements amalgamating practices from:

- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 Rev.1, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations;
- NIST SP 800-53 Rev. 4, Security and Privacy Controls for Information Systems and Organizations;
- FAR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems;
- (DRAFT) NIST SP 800-171B (now NIST SP 800-172), Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations: Enhanced Security Requirements for Critical Programs and High-Value Assets;
- NIST Framework for Improving Critical Infrastructure Cybersecurity v.1.1;
- Center for Internet Security Controls v.7.1;
- Software Engineering Institute—Computer Emergency Response Team Resilience Management Model v. 1.2; and
- Other standards promulgated by the United Kingdom, Australia, or crafted exclusively by the creators of CMMC.

Unique to CMMC from the compliance and assessment standpoint was the concept of "maturity," which was intended to measure progression. Version 1.0 defined a "maturity model" as a "set of characteristics, attributes, indicators, or patterns that represent capability and progression in a particular discipline. The content of such a model typically exemplifies best practices and may incorporate standards or other codes of practice of that discipline." The result of such a model would have been to provide contractors with a "benchmark against which an organization can evaluate the current level of capability of its processes, practices, and methods and set goals and priorities for improvement." See CMMC 1.0, at 2.1.

To demonstrate that maturity, CMMC 1.0 included five levels designed to evaluate the contractor's processes and practices, from performing basic cyber hygiene (Level 1) to optimizing advanced/progressive practices (Level 5) and the necessary steps in between. The crux of CMMC 1.0 for most of the DIB lay in Level 3, which required managed and good cyber hygiene processes and practices, largely through the application of the safeguarding/confidentiality requirements in NIST 800-171, plus a few more additives to account for data availability and integrity.

Most notable—and perhaps most problematic—with CMMC 1.0 was that it required the use of an accreditation body, the "CMMC-AB," to select and train those who would assess and grade contractors' cybersecurity levels. Plagued with problems from its beginning, the CMMC-AB was burdened with the overarching (and herculean) tasks of (i) creating the process and materials by which the DIB would be assessed, and (ii) teaching a newly developing cottage industry just how to perform those assessments. Despite some significant efforts, the CMMC-AB was only getting its feet under it when DOD was revealed on March 30, 2021, that CMMC 1.0 was undergoing an "internal assessment."

Unbeknownst at the time, that review was later understood to be focused on examining the concerns raised by industry while also seeking the means to clarify the standards and reduce its cost impact on the DIB. Accordingly, after that review, DOD told CMMC, "see you 'round the clubs," and CMMC 1.0 was put to rest with the new, less-onerous CMMC 2.0.

Across the Universe—How CMMC 2.0 Is Expected to Apply—While the news of DOD's break up with CMMC 1.0 came as a surprise, the issuance of the 2.0 requirements stole the show. Although certain to please the DIB, the newly unveiled CMMC 2.0 appears to be little more than an "acoustic cover" of DFARS 252.204-7012. Much of the language and intent of CMMC 2.0 is similar to the NIST SP 800-171 self-assessments contractors have been required to perform for years; only now those requirements are layered into a new three-tiered structure. The release of CMMC 2.0 also trumpeted an intent to ensure that any additional guidance or directions would follow the formal regulatory rulemaking process to better ensure industry feedback. Accordingly, specific details have been scant and will likely remain that way as the process unfolds. What details are known include the following:

- *Level 1*: Annual self-assessment of 17 practices in line with FAR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems. While this level appears to focus on securing contractor information systems, there are also indications that the rulemaking process may include a requirement for company leadership to affirm compliance. A scoping document for Level 1 self-assessment document was recently released by DOD. See *www.acq.osd.mil/cmmc/docs/Scope_Level1_V2.0_FINAL_20211203.pdf.*
- *Level 2*: Likely to include triennial third-party assessment of "critical national security information" and annual self-assessment for "select programs" of the 110 security requirements found in NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. This will be the applicable level to any contractor wishing to handle CUI, but significant details are still required. The manner in which holders of "critical national security information" or the "selected programs" are to be identified and the perhaps heightened assessment requirements all need to be fleshed out. Similarly, it remains unclear how the NIST 800-171 assessment requirements may apply to a contractor not designated as possessing "critical national security information" or working on a "select program." A scoping document for Level 2 self-assessment document was recently released by DOD. See *www.acq.osd.mil/cmmc/docs/Scope_Level2_V2.0_FINAL_20211203.pdf.*
- *Level 3*: Triennial Government-led assessment of 110 plus requirements in NIST SP 800-172, Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171. Noteworthy is that these assessments are expected to be performed by Government officials, not a third-party assessor. This standard contains the more robust selection of controls intended to thwart the advanced persistent threat posed by sophisticated actors (i.e., nation-states). Notably, however, the focus of NIST SP 800-172 remains on protecting the confidentiality of CUI, "i.e., not directly addressing integrity and availability." Accordingly, issues surrounding ransomware and deemed denial of service attacks are likely to remain prevalent unless additional extra-NIST measures are taken by contractors.

Aside from the changes to the levels and third-party assessment requirements, CMMC 2.0 also removed a host of CMMC-specific practices, many of which were uniquely directed at incident response procedures and CUI access and control. These largely addressed data integrity and availability areas, so their absence reinforces the dominance of the confidentiality requirements found in NIST SP 800-171/172. CMMC 2.0 also provides for added flexibility by not only permitting the inclusion of certain Plans of Action and Milestones (POA&Ms) to address ameliorative measures for unfulfilled requirements within 180 days of contract award (which CMMC 1.0 excluded) but also providing the possibility of a "a limited waiver process to exclude CMMC requirements from acquisitions for select mission-critical requirements." Such waivers are expected to be for a limited time, for limited mission-critical instances justified by the acquiring agency, and require senior leadership approval. Finally, CMMC 2.0 takes the odd tack of eliminating "all maturity processes." This announcement begs the question of just how many "M"s CMMC 2.0 will actually demand and whether or how DOD will address "maturity" in the rulemaking process.

Also unique to CMMC 2.0 is DOD's intent to leverage NIST's expertise before demanding the inclusion of new or unique requirements into DOD controls. NIST will likely serve as an assessor of such a requirement and—if it agrees—that requirement would be included in the next iteration of the appropriate NIST publication as applied through the CMMC 2.0 framework. Effectively, it appears as though CMMC 2.0 will serve as a launching point directing contractors to a perhaps dynamic new NIST Special Publication.

Unlike the previous iteration of CMMC, DOD promises that the formal rulemaking process will be at the center of CMMC 2.0. Not only does this signify a more predictable mechanism of creating the new requirements, but it also portends a significant timeline before contractors should expect to see CMMC 2.0 ready for action or consumption. The online OUSDAS CMMC Frequently Asked Questions forecasts a process and timeline that "can take 9-24 months," but likely complicating that effort will be two separate requirements for the FAR and DFARS, along with newly "empowered" roles being played by the Department of Homeland Security and its Cybersecurity and Infrastructure Security Agency. See *www.acq.osd.mil/cmmc/faq.html*. Suffice it to say, with DOD promising "CMMC 2.0 will become a contract requirement once rulemaking is completed," contractors should not expect to see CMMC 2.0 invade contracts any time soon.

Let It Be?—What's Happening with the CMMC-AB?—A significant change resident in CMMC 2.0 is the removal of mandatory assessments across all tiers and the inclusion of the "Government-led" assessments at CMMC 2.0 Level 3. However, this does not mean that the CMMC-AB is going away, but it remains unclear as to what its future looks like. On its website, the CMMC-AB expressly supports the new direction as a "meaningful and compelling improvement to the implementation of CMMC." See *cmmcab.org/news/cmmc-accreditation-body-endorses-pentagons-proposed-implementation-changes-in-cmmc-20/*. Moreover, the CMMC-AB recognized that there are going to be (even more) challenges ahead, as the CMMC-AB must now (again) adjust its curricula for training providers and account for changes resident in the federal rulemaking process. This remains a very fluid area and the CMMC-AB is expected to provide additional information on its future and role in the near term.

Maxwell's Silver Hammer—Cyber Enforcement—Although CMMC 2.0 appears largely to revert back to a direct reliance on a contractor's self-assessed compliance with NIST SP 800-171 and/or NIST SP 800-172, contractors should note that this simpler beat gives enforcers a lot more room to dance. This means that, once CMMC 2.0 gets released, it's fair to assume that agency inspectors general and the Defense Contract Management Agency, with its mandate to examine contractor compliance with cybersecurity requirements as part of its Contractor Purchasing System Reviews, will have a far clearer focus on assessing cybersecurity. To be sure, DOD has recognized in its CMMC 2.0 follow-on meetings that a contractor failing to meet its POA&M obligations may be subject to the typical contractual failure remedies, hinting at breach and maybe even False Claims Act liability.

Adding even more percussion to that compliance enforcement tune is DOJ's Civil Cyber-Fraud Initiative announced on Oct. 6, 2021. In her speech on the subject, Deputy Attorney General Lisa O. Monaco expressly announced DOJ's intent to "utilize the False Claims Act … to pursue cybersecurity related fraud by government contractors and grant recipients." Like the news of a Beatles song hitting number one in the '60s, such news should have come as no surprise. Nonetheless, DOJ indicated this initiative is intended to "hold accountable entities or individuals that put U.S. information or systems at risk by knowingly providing deficient cybersecurity products or services, knowingly misrepresenting their cybersecurity practices or protocols, or knowingly violating obligations to monitor and report cybersecurity incidents and breaches." The announcement posted on the DOJ website concluded with a link where potential whistleblowers could report tips and complaints about cyber-related fraud on the Civil Division's Fraud Section website. See *www.justice.gov/civil/report-fraud*.

In relative harmony with the DOJ announcement, the Acting U.S. Attorney in California filed its statement of interest in connection with defendants' motion for summary judgment in *U.S. ex rel. Markus v. Aerojet Rocketdyne Holdings* (E.D. Cal. 2:15-CV-02245 WBS AC). The motion arrived notwithstanding that, in 2018, DOJ declined to intervene in an FCA matter brought by a former Aerojet Rocketdyne senior director of cyber security, compliance, and controls. The allegations accused the company of fraudulently obtaining billions of dollars of DOD and NASA contracts while failing to meet or maintain its contractually mandated cybersecurity and breach reporting requirements, in violation of the FCA.

Although DOJ's statement of interest is silent as to its relation with the Cyber-Fraud Initiative, its message couldn't be clearer. DOJ forcefully rebuked the contractor's arguments that its purported noncompliance with cybersecurity requirements was immaterial to the Government's decision to pay. DOJ argued that the Government's understanding or knowing that cybersecurity issues plague both industry and the defendant was not enough to make the contractor's alleged cybersecurity shortcomings immaterial to payment decisions: "the government did not just contract for rocket engines, but also contracted with [Aerojet Rocketdyne] to store the government's technical data on a computer system that met certain cybersecurity requirements."

I've Got a Feeling—How Contractors Should Proceed—A segment of the "*Get Back*" documentary showcases how Paul McCartney, and later with John Lennon, arrives at the lyrics for the single "Get Back." In an awe-inspiring display of lyrical artistry, the words and phrases are chosen then melodically woven into the fabric of the music until a hit is born. The same creation is happening for federal defense contractors in the cybersecurity sense. The music is there, resident in DFARS 252.204-7012, and NIST SP 800-171 (and, for some, NIST SP 800-172), and now contractors, to the extent they haven't done so already, need to find the right words to fit the tune. While there is no substitute for the raw talent of Lennon-McCartney, there are vital resources contractors can use now to prepare for the fully formed hit that will be CMMC 2.0:

- Review DOD's NIST SP 800-171 DOD Assessment Methodology.

  Required to be reviewed and applied for the requirements found at DFARS 252.204-7012 and -7020, DOD Assessment Methodology is critical to understanding the priorities a company should first address when approaching compliance. The Methodology contains a weighted list of requirements identifying "security requirements that, if not implemented, could lead to significant exploitation of the network, or exfiltration." This ranking is beneficial in directing time and resources to meet cybersecurity requirements. As noted above, while CMMC 2.0 is expected to allow for some waivers, there are expected to be certain non-waivable Basic and Derived Security Requirements that contractors will need to meet. The Methodology points them out by giving each a weighted value of five points (meaning, in performing an assessment for input into the Supplier Performance Risk System, each incomplete requirement results in a five-point deduction from the 110 total points permitted). Presently there are 23 Basic Security Requirements and 19 Derived Security Requirements valued at this level. No need to do the assessment just yet. This step is intended as a starting point to address a contractor's most imminent needs.

- Review Appendix E, Tailoring Criteria of NIST SP 800-171.

  At the tail end of NIST SP 800-171, Appendix E stands as an often-overlooked resource for compliance professionals. It, however, should be everyone's first stop in that it shows up in the "Cautionary Note" found on page vi. The appendix highlights, in pertinent part, those NIST SP 800-53 security controls or control enhancements that are "expected to be routinely satisfied by nonfederal organizations without specification." These include the presence of policy and procedures for all fourteen of the security requirement families (i.e., access control, incident response, risk assessment, etc.), security training records, continuous monitoring and security assessment measures, the configuration management plan, and a whole litany of other elements the NIST expects are already "included as part of an organization's comprehensive security program." Ensuring that such efforts are included in a contractor's cybersecurity effort will better prepare it to adapt to what CMMC 2.0 may bring.

- Review and apply NIST 800-171A, Assessing Security Requirements for Controlled Unclassified Information.

  NIST 800-171A (and its in-draft corollary 172B for more sensitive data) is the ideal resource to get contractors ready for CMMC 2.0. After identifying and understanding the immediate needs using the Assessment Methodology then rounding that effort out with the "routinely satisfied" materials the NIST already assumes are being performed, the next step is to march through this straightforward assessment tool. The tool, for those unfamiliar, contains not only the security requirements but a breakdown of each assessment objective and the potential methods and objects that contractors can use to perform the assessment. Walking through this readily available resource, in the predetermined order of need identified above, will help contractors meet their DFARS 252.204-7012, -7019 and -7020 requirements. It will also facilitate the rapid adoption of CMMC 2.0 when finally released.

Although taste is subjective, many critics agree that the Beatles' final album, "*Let It Be,*" was not their best. Amidst animosity, breakups, egos and uncertainty, as the "*Get Back*" documentary reveals, it's a surprise that it was released at all, let alone a month after the band formally broke up. Some might say the same about where CMMC 2.0 appears to be heading and the tumultuous process that got it here. For nearly two years, contractors have been promised to be assessed by a third party against a harrowing standard intended to protect sensitive Government data against the advanced persistent threat. By contrast, CMMC 2.0 appears to let contractors get back to where they once belonged—into the self-assessed realm of NIST 800-171.

✦

This Feature Comment was written for The Government Contractor by* Alex Major and Franklin Turner.** ***Mr. Turner and Mr. Major are Partners in the Washington, D.C. office of McCarter & English, LLP, where they serve as Co-Leaders of the Government Contracts and Global Trade Practice Group. The authors routinely teach courses on a variety of Government contracts issues and can be reached at amajor@mccarter.com and fturner@mccarter.com.