DOD Cybersecurity Rule Will Burden And Benefit Contractors

By **Roger Abbott, Adam Bartolanzo and Kathryn Carlson** (November 13, 2024)

Roger Abbott

Adam Bartolanzo

Kathryn Carlson

The U.S. Department of Defense recently published a final rule formally implementing the Cybersecurity Maturity Model Certification program.[1] The final rule culminates five years of work to standardize the safeguards that government contractors must implement to protect federal contract information and controlled unclassified information while also bolstering compliance with these requirements.

Notably, the CMMC program does not alter existing requirements to comply with the cybersecurity safeguarding controls specified in Federal Acquisition Regulation 52.204-21 and Defense Federal Acquisition Regulation Supplement 252.204-7012.

Rather, it implements a three-tiered assessment framework that requires all domestic and foreign DOD contractors, including small business and commercial contractors, across the defense industrial base, or DIB, either to self-assess or receive external assessments of their compliance with DOD cybersecurity requirements at an appropriate level as a condition for receiving a DOD contract or subcontract.

DOD contractors at all three CMMC levels will be required to submit an annual reaffirmation that they comply with applicable cybersecurity safeguarding requirements.

These requirements will greatly increase the costs of complying with existing cybersecurity controls by requiring contractors to invest significant time and resources to demonstrate that they meet these controls, and by increasing the legal risk of noncompliance.

The CMMC program will be phased in over a four-year period, beginning when the final version of the DFARS CMMC rule comes into effect in early spring. That said, contractors should begin preparing now, and should take note of three key areas: third-party assessments, yearly affirmations and impact on subcontractors.

External Assessment and Certification

External assessment is central to the CMMC program that exists at both Level 2 and 3. Level 2 third-party assessments will be conducted by a CMMC third-party assessment organization, or C3PAO, who will analyze whether contractors meet the 110 security controls of the National Institute of Standards and Technology Special Publication 800-171, or NIST SP 800-171.

Level 3 third-party assessments will be conducted by the Defense Contract Management Agency's Defense Industrial Base Cybersecurity Assessment Center, or DIBCAC. To meet Level 3 requirements, a contractor must first meet the requirements of Level 2, as well as 24 additional requirements of NIST Special Publication 800-172, published in February

2021.

One challenge that the DOD and DOD contractors will have to confront, which is reflected in the comments to the final rule, is the scarcity of third-party assessors. The DOD estimates that approximately 8,350 medium and large entities will need to receive this C3PAO Level 2 assessment, 135 of which are expected to occur in the first year alone.[2]

Although the final rule sets out a phased-in approach, contracting officers will be permitted to require Level 2, third-party assessment as soon as implementation begins in early spring. Official C3PAO assessments will not be available until next month, only several months before the CMMC program launches.

The final rule addresses this likely bottleneck by stating that the "CMMC program depends on the supply and demand dynamics of the free market, enabling it to naturally scale and adapt to capacity requirements."[3] This adds little substantive assurance that the supply of assessors will be able to handle the flood of contractors seeking assessment. The final rule also fails to address concerns regarding a lack of C3PAOs for foreign contractors, who will also be required to meet certifications regardless of the availability of assessors.

Level 2 and Level 3 contractors that are at least 80% compliant with the additional controls will be eligible for conditional certification by establishing a plan of action and milestones, or POAM. Contractors with a conditional certification are eligible to receive DOD contracts but must close out their POAMs within 180 days or lose their certification.

Except for Level 2 contractors that are permitted to self-assess, verification of full compliance must be made by a C3PAO or by the DIBCAC, as appropriate. This temporary expedient is not available for Level 1 contractors, which must fully comply with the 15 controls specified in FAR 52.204-21 without exception.

Given the C3PAO backlog, and the fact that conditional certification based on a POAM will only be valid for 180 days, contractors should start the process of seeking third-party assessment early. Not only will early action be critical to avoiding long waiting lists for assessment, but they will also be critical for ensuring compliance with another part of the CMMC scheme, yearly affirmations.

Annual Affirmations

Third-party assessment will be crucial for ensuring cybersecurity compliance, particularly as the CMMC program requires yearly affirmations of compliance. Unfortunately, contractors currently appear ill-equipped to properly self-assess the 110 requirements from NIST SP 800-171 under DFARS 252.204-7012.

A study of 300 DOD contractors, published in September, found that while seven in 10 respondents self-assessed as compliant, the average score of the respondents was actually -12 out of 110.[4]

While knowledge of cybersecurity requirements is likely to increase with the rollout of the CMMC program, contractors that misrepresent their compliance in their CMMC yearly affirmations based on an improper self-assessment could face liability under the False Claims Act.

The CMMC program requires annual affirmations of compliance, in addition to the triennial certifications required at CMMC Level 2 and 3. Needless to say, mistaken affirmations that a

contractor is compliant with all applicable cybersecurity controls will expose contractors to liability under the FCA.

Additionally, the final rule warns that a "new CMMC assessment may be required if significant architectural or boundary changes are made to the previous Assessment Scope. Examples include, but are not limited to, expansions of networks or mergers and acquisitions." Accordingly, a company that undergoes such changes should not reaffirm compliance until a new assessment has been performed.

At this stage, it is unclear which changes rise to the level of "significant architectural or boundary changes." To get ahead of this issue, companies that anticipate making significant changes to their IT infrastructure — for instance, based on a corporate transaction — should plan so that they can expeditiously update their self-assessment or certification, if necessary.

The degree of FCA risk that contractors face from noncompliance with cybersecurity requirements has been subject to debate, with recent developments indicating it is becoming an area of priority for federal investigators.

The U.S. Department of Justice announced the launch of the Civil Cyber-Fraud Initiative in October 2021 to crack down on noncompliance with federal cybersecurity requirements.[5] Although this initiative was highly publicized and widely discussed in the government contracts community, only a handful of settlements and prosecutions have been publicly announced, and smaller DOD contractors have not been targeted for enforcement action.

Nonetheless, the DOJ announced last month that Pennsylvania State University had agreed to pay $1.25 million to resolve allegations that it had violated the FCA by failing to comply with DOD cybersecurity requirements.[6]

In addition, in August the DOJ filed a complaint-in-intervention in an FCA lawsuit against Georgia Institute of Technology, alleging that the university submitted a false assessment of its cybersecurity compliance to the DOD.[7] Georgia Tech faces more than $90 million in potential treble damages under the FCA.

Additional investigations are presumably underway, and the annual affirmations required under the CMMC program will give the DOJ additional leverage to pursue FCA claims.

At the same time, external certification may reduce exposure to FCA liability. Unless a contractor deviates or fails to maintain the cybersecurity controls described in its system security plan, it should be able to use external certification by a C3PAO or a DIBCAC as a possible shield against allegations that it recklessly or intentionally failed to comply with the cybersecurity requirements.

Accordingly, although obtaining external certification is costly, contractors may benefit from doing so, not just by retaining their eligibility to receive significant DOD contracts — in what is likely to be a narrower pool of competitors — but potentially by receiving protection against FCA liability. Although some uncertainty exists over which CMMC Level 2 contracts will require third-party certification, this potential benefit provides another reason to embrace the use of third-party assessors as early as possible.

Impact on Subcontractors

The CMMC program is set to affect over 220,000 contractors across the DIB.[8] It applies to all DOD contractors, including small business and commercial contractors, and flows down to subcontractors. Additionally, the final rule clarifies that foreign companies will be required to comply with CMMC to receive a DOD contract or subcontract. Only supply contracts that are solely for commercial off-the-shelf items are exempt from the CMMC requirements.

This comprehensive coverage reflects the DOD's concern that cyber "attacks not only focus on the large prime contractors, but also target subcontractors that make up the lower tiers of the DOD supply chain."[9] Therefore, at a minimum, subcontractors who will process, store or transmit federal contract information must have a Level 1 assessment, and those who process, store or transmit controlled unclassified information must have a minimum of a self or C3PAO assessment.

This level of security will come at a large cost to subcontractors, many of whom are small and may not currently have the resources allocated for cybersecurity protections. For example, the DOD projects that small businesses will face a cost of $104,670 for Level 2 C3PAO assessment every three years.[10]

The DOD notes that this estimate excludes the costs of implementing or maintaining cybersecurity compliance, because those measures are already required by previous DFARS and FAR requirements.

Again though, studies show that largely contractors are not as compliant as they believe, and the rollout of the CMMC program, with its greater chance of FCA violations, will require investment by contractors into cybersecurity implementation and maintenance.

Ensuring subcontractor compliance will be challenging for prime contractors. Unlike size representations that are publicly accessible in the system for award management, CMMC assessments in the supplier performance risk system and the enterprise mission assurance support service are accessible only by the government: A company can only view its own certification in SPRS or eMASS.

Prime contractors, then, will need to obtain proof of compliance directly from their subcontractors, perhaps by requiring a printout or certification demonstrating compliance as a subcontract deliverable.

Additionally, although the CMMC rule requires compliance at the time of award — not at the time of offer — contractors without external certification at the time of offer are unlikely to obtain it by time of award unless they initiated the process months before submitting their proposals. Accordingly, prime contractors will likely require prospective subcontractors to have their certification in hand as a prerequisite for teaming together.

This creates even greater urgency for subcontractors, which will need to assess the resources required to become compliant at the appropriate level, decide whether it is economically feasible and act quickly to obtain external certification if they decide to remain in the DIB. The shrinking DIB has been the subject of much attention in the defense community, and given the costs of compliance, we expect the DIB to continue consolidating, as smaller businesses that are unable to afford external certification exit the market.[11]

Conclusion

The CMMC program will present numerous challenges and impose enormous costs on defense contractors, particularly on small businesses. However, we do not expect these

challenges and costs to remain limited to DOD contractors for long. Currently, two proposed rules are in their final stages of review to alter portions of the FAR.[12] Our understanding is that these rules will require compliance with many, if not all, of the controls in NIST SP 800-171.

In that sense, the rollout of the CMMC program may be just a preview of what is likely to be required across the procurement space, as the U.S. federal government takes greater action to protect U.S. information in its contracting.

Although these additional compliance challenges and costs are significant, contractors that obtain external certification will not only receive continued access to lucrative defense contracts but will benefit from a narrower pool of competitors and should be better able to manage FCA risk stemming from cybersecurity noncompliance.

And when the FAR analogue to the DFARS cybersecurity rule becomes effective, DOD contractors that are CMMC compliant will be at a competitive advantage to civilian contractors that have not yet begun the process of complying with NIST SP 800-171.

Roger V. Abbott is a principal, Adam A. Bartolanzo is counsel and Kathryn J. Carlson is a law graduate at Miles & Stockbridge PC.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] https://www.federalregister.gov/documents/2024/10/15/2024-22905/cybersecurity-maturity-model-certification-cmmc-program

[2] https://www.federalregister.gov/documents/2024/10/15/2024-22905/cybersecurity-maturity-model-certification-cmmc-program

[3] https://www.federalregister.gov/documents/2024/10/15/2024-22905/cybersecurity-maturity-model-certification-cmmc-program

[4] https://cybersheath.com/resources/downloads/defense-on-the-brink-the-perilous-state-of-cybersecurity-across-the-dib/#register

[5] https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative

[6] https://www.justice.gov/opa/pr/pennsylvania-state-university-agrees-pay-125m-resolve-false-claims-act-allegations-relating

[7] https://www.law360.com/articles/1872779/federal-gov-t-hits-georgia-tech-with-cybersecurity-fca-suit.

[8] https://www.federalregister.gov/documents/2024/10/15/2024-22905/cybersecurity-maturity-model-certification-cmmc-program

[9] https://www.federalregister.gov/documents/2024/10/15/2024-22905/cybersecurity-

maturity-model-certification-cmmc-program

[10] https://www.federalregister.gov/documents/2024/10/15/2024-22905/cybersecurity-maturity-model-certification-cmmc-program (table 10).

[11] https://federalnewsnetwork.com/defense-main/2024/09/a-closer-look-at-the-shrinking-defense-industrial-base/.

[12] 88 FR 68402 and 88 FR 68055.