How DOD Can Improve Flexibility Under Proposed Cyber Rule

By **Joshua Duvall and Sandeep Kathuria** (February 21, 2024)

Joshua Duvall

Sandeep Kathuria

In late December, the U.S. Department of Defense published for public comment its proposed rule regarding the latest iteration of the Cybersecurity Maturity Model Certification, or CMMC, program.

A significant effort to shore up supply chain cybersecurity by the DOD, it is anticipated that the CMMC program will apply to an estimated 221,286 companies in the defense industrial base when finalized and fully rolled out.

Briefly, the CMMC is designed to ensure full implementation of 110 security controls developed by the National Institute of Standards and Technology in Special Publication 800-171 Rev. 2, which has been incorporated in most DOD contracts through an existing regulation, Defense Federal Acquisition Regulation Supplement 252.204-7012.

While the CMMC undoubtedly is an important initiative — and one that the authors want to see succeed — the DOD should carefully address some of the more nuanced aspects of the CMMC program to avoid unintended consequences. In that respect, one maxim comes to mind: Perfection should not be the enemy of the good.

While much has been written and said about CMMC, this article focuses on avoiding a major potential pitfall as proposed under the CMMC program regulations.

Specifically, by proposing to severely limit contractor use of plans of actions and milestones, or POA&Ms, the DOD would effectively constrain the application of NIST SP 800-171r2 Control 3.12.2, "Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems."

This security control is important — as all of them are — because it provides contractors with a means to correct ongoing or emergent issues without being considered to fall out of compliance with their DOD contracts.

By limiting the application of this NIST-approved control, the DOD risks not only reduced competition and resulting higher prices, but also the loss of critical and innovative suppliers in the defense supply chain needed to help deliver products and services to DOD components.

Below we discuss the current POA&M scheme under the CMMC program and offer alternatives for how the DOD might revise its approach to ensure that these risks do not materialize.

Unreasonable Restrictions on Plans of Actions and Milestones

For CMMC Level 2, which is estimated to eventually apply to 76,598 government contractors, the DOD has proposed that (1) POA&Ms will only be permitted where the assessment score is greater than or equal to 88 points, or .8 of 110; (2) that none of the

security requirements on the POA&M may have a score greater than 1, with one exception; and (3) where certain security requirements are not included in the POA&M.

The proposed rule also includes a mandatory 180-day close-out window for POA&Ms, with no provision for extension. Failure to meet these POA&M restrictions could lead government contractors and subcontractors to be ineligible for contract awards, which would be a significant departure from current practice and a potentially harsh result.

As proposed, the POA&M requirements may be unreasonably restrictive for many companies, which ultimately could affect competition for defense contracts and the maintenance of the DOD supply base. In particular, new entrants to government contracting, small businesses and commercial entities may need to rely on POA&Ms as their organizations increase cybersecurity maturity as defined by the DOD.

A more flexible approach would benefit these entities, and indeed the DOD, by ensuring that potential barriers to entry to defense contracting are not overly burdensome. Indeed, it is worth noting that a recent report by the Atlantic Council found that the DOD's industrial base has already shrunk 40% over the past decade,[1] meaning that this problem could be exacerbated if cybersecurity standards, particularly with regard to POA&Ms, are set too high and too fast by the DOD.

As recognized by NIST, a comprehensive cybersecurity regime is not static; rather, it involves an organization's efforts to implement processes, procedures and technologies, among other things, to guard against unwanted or malicious attacks or occurrences that may affect the confidentiality, availability or integrity of an organization's data or systems.[2]

This fluidity is underscored in NIST SP 800-171r2 not only under Control 3.12.3, "Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls," but also under Control 3.14.1, "Identify, report, and correct system flaws in a timely manner." These controls, and others, contemplate continuous monitoring of dynamic information systems.

The controls therefore implicitly identify an important component of the cybersecurity risk management framework: An organization's cybersecurity regime is — and should always be — changing and improving. POA&Ms under 3.12.2, in turn, recognize this reality by creating a mechanism by which an organization will meet any unimplemented security requirements or any "planned mitigations."

The proposed CMMC program, therefore, does not provide for the necessary flexibility for government contractors to appropriately manage risk in a dynamic environment. In that regard, the CMMC program provides that POA&Ms may only be used for the easiest to meet requirements, and not the more difficult — and perhaps costlier — 3- and 5-point controls.

In other words, to be eligible for a POA&M, the proposed rule states that "[n]one of the security requirements included in the POA&M have a point value of greater than 1 as specified in the CMMC Scoring Methodology," except for one requirement, encryption, which can be either a 1 or 3.

Under the proposed CMMC scoring approach, 1-point controls are perhaps the easiest for an organization seeking certification, or OSC, to meet, while the 3- and 5-point requirements up the ante. While the authors recognize the importance of 5-point controls and acknowledge that the absence of such controls could lead to increased cyber risk, the DOD

also should consider the manner in which companies are working to improve their cyber postures and maturity.

The DOD should likewise consider the fact that the CMMC program itself also requires all security controls not met to be implemented no later than 180 days from receipt of a conditional assessment. That time will go by fast and not all companies will have the resources to close every POA&M in short order.

To address the foregoing issues, the DOD should delete any references to specific security requirements to be eligible for a POA&M and permit POA&Ms where a contractor simply meets the minimum scoring threshold of 88 points, or .8 of 110.[3] This would foster flexibility and promote a fulsome defense industrial base by enabling more OSCs to achieve a conditional assessment, which the proposed rule ties to contract eligibility.

The DOD can always seek, in the procurement process, to verify CMMC requirements that are met prior to award or include specific requirements in solicitations. And, where such requirements are not met and that OSC has been awarded a contract with a conditional assessment, the proposed rule does provide recourse in the form of "standard contractual remedies."

Similar problems exist for CMMC Level 3, as the proposed rule not only requires a minimum score of 20 points, or .8 of 24, but also dictates — similar to CMMC Level 2 — what security requirements may not be in a POA&M. This too is problematic because proposed language for CMMC Level 3 states that OSCs must "complete and implement all Level 3 security requirements" prior to initiating a CMMC Level 3 certification assessment.

Under this scheme, an OSC could, in good faith, complete all Level 3 requirements but then be denied a conditional assessment where one of the not met requirements appears in the list of requirements that are not allowed be in a CMMC Level 3 POA&M. This again could unreasonably restrict competition to the detriment of the DOD.

To address these concerns, the DOD should remove the specific references and allow OSCs to achieve a conditional assessment under CMMC Level 3 where any combination of security requirements meets the scoring threshold.

In that regard, given that a requirement not met largely could be based on minor implementation issues, as opposed to not implementing the requirement at all, the DOD also should consider lowering the threshold percentage to .6 or .7, which, again, would foster flexibility and promote a fulsome defense industrial base by ensuring robust participation for defense contracts that require a CMMC Level 3 certification.

To be sure, however, the issues with CMMC Level 3, as with Level 2, are not just confined to how and when a POA&M should apply, they also extend to the POA&M close-out process, which the DOD also should fine tune to avoid more unintended consequences.

With respect to the 180-day POA&M close-out window, the proposed rule does not address the scenario where the 180-day window lapses without any fault of the OSC. The proposed rule states that an OSC must close out their POA&Ms within 180 days or else their conditional certifications will expire.

However, the proposed rule is silent on what happens when the OSC submits its POA&M close-out information to their CMMC third-party assessment organization or Defense Industrial Base Cybersecurity Assessment Center, but that the C3PAO or DIBCAC is unable

to timely complete the request within the 180-day period.

Such a scenario may occur where, for example, the C3PAO or DIBCAC do not have the resources to timely complete an OSC's closeout request. OSCs should not be faced with the steep consequence of having their conditional certifications expire — and thus lose their eligibility for contract awards — because of delays outside their control. There should be a mechanism to extend the 180-day deadline.

Finally, it is worth reemphasizing that POA&Ms are contemplated under one of the 110 security controls under NIST SP 800-171r2 — Control 3.12.2 — which is incorporated by reference by the DOD under DFARS 252.254-7012.

Because POA&Ms are part of the 800-171r2 framework, even for government contractors that have fully implemented all NIST controls and have received a final certification assessment, these companies should still have the ability to continue to adopt POA&Ms in between triennial certification assessments without being considered by the DOD to have fallen out of their continuing compliance obligations under the proposed rule. To the extent that the proposed rule is not clear on the link between POA&Ms and continuing compliance obligations, the DOD should provide clarity.

Indeed, through a contractor's continuous monitoring efforts, as the proposed rule touches upon, post-final certification assessment POA&Ms may be needed to address temporary deficiencies or changes that in many cases arise outside the contractor's control.

Without clearly permitting contractors to use POA&Ms for their continuing compliance obligations, there is a risk that some companies may ignore new risks and system vulnerabilities or delay adopting new technologies in order to remain eligible for defense contracts for the duration of their three-year final certification assessment or longer.

Such an approach would not adequately protect information systems with covered defense information and thus would defeat the purpose of the DOD's cybersecurity compliance regime.

Joshua B. Duvall is a partner at Maynard Nexsen PC.

Sandeep Kathuria is an attorney at L3Harris Technologies Inc.

[1] Atlantic CouncilCommission on Defense Innovation Adoption: Final report - Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/report/atlantic-council-commission-on-defense-innovation-adoption/.

[2] It's worth noting that while NIST SP 800-171r2 states that the primary objective of the framework is protecting the confidentiality of CUI, the SP also states that "the objectives of integrity and availability remain a high priority for organizations that are concerned with establishing and maintaining a comprehensive information security program."

[3] Or some other point value to the extent that DOD decides that a lower percentage threshold would be in the best interest of DOD and its mission.