This is Just a Test

Advising Your Client on Real-World Cybersecurity Questions Using Fictional Scenarios Connected to the Department of Defense's Proposed Cybersecurity Maturity Model Program

BY SANDEEP KATHURIA, WITH COMMENTARY BY NKECHI KANU, SUSAN WARSHAW EBNER, AND ALEXANDER CANIZARES

Sandeep Kathuria

Nkechi Kanu

Susan Warshaw Ebner

Alexander Canizares

This article consists of a series of hypothetical scenarios identifying potential implementation issues related to the Cybersecurity Maturity Model Certification (CMMC) program as it is currently constructed (and which may ultimately change via final rulemaking). Sandeep Kathuria crafted the hypotheticals[1] *and then solicited and coordinated commentary from other government contracts attorneys for their advice about how these scenarios should best be handled if clients raised them. To be clear, the scenarios in this hypothetical are fictional, but the practical challenges identified below may yet come to fruition and are inspired in part by existing issues companies face in connection with meeting the government's evolving cybersecurity requirements and/or managing cyber risk.*

Sandeep Kathuria is a government contracts and cybersecurity attorney writing in his personal capacity. As in-house counsel for large defense contractors, he provided comments on the security controls and proposed regulations associated with the Cybersecurity Maturity Model Certification (CMMC) program, organized and attended industry and professional association meetings on CMMC, and coordinated with like-minded colleagues in the defense industrial base to try to improve the program and ensure its success. Nkechi Kanu is counsel in Crowell & Moring's Government Contracts practice group, where she advises government contractors on internal and government investigations arising under the False Claims Act, with a particular focus on alleged noncompliance with cybersecurity requirements. Susan Warshaw Ebner is a partner at Stinson LLP where she co-chairs the Government Contracts and Investigations Practice, counseling and representing clients on complex and emerging issues in government contracts, grants, compliance, audits, investigations, and litigation. Alexander O. Canizares is a partner with Perkins Coie LLP whose practice focuses on representing government contractors and other companies in litigation, investigations, and counseling related to all phases of federal procurement.

CMMC is a program the US Department of Defense (DoD) proposed to establish a third-party certification regime to validate that defense contractors are meeting security requirements to protect controlled unclassified information (CUI) that is processed, stored, or transmitted on their internal information systems. Under the proposed program, third-party certification is only required if a contractor is handling CUI.[2] CMMC is designed to replace or augment DoD's existing system, which relies on contractors' self-attestations of cybersecurity compliance.

CMMC was first announced by the Department of Defense in 2019.[3] Over the following years, DoD developed various iterations of the technical security model and security levels for CMMC. DoD also proposed federal rules that were not finalized. CMMC has been beset with delays in the regulatory process, but progress has been made more recently.

On December 26, 2023, DoD proposed to implement the CMMC program in 32 C.F.R. Part 170, with DoD expressing its intent to develop new defense contracting processes implementing CMMC in a separate 48 C.F.R./ Defense Federal Acquisition Regulation Supplement (DFARS) rulemaking published at a later date.[4] As DoD explained: "[w]hen this 32 CFR CMMC Program rule is finalized, solicitations for defense contracts involving … CUI on a non-Federal system will, in most cases, have a CMMC level and assessment type requirement a contractor must meet to be eligible for a contract award."[5] Only contracts involving CUI will require this third-party assessment, which will be needed to meet Level 2

Published in The Procurement Lawyer, Volume 59, Number 4, Summer 2024. © 2024 by the American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

and serve as the foundation for Level 3, the highest level. DoD estimates that 221,286 companies will be covered by the CMMC program once it has been phased in over the next few years, but only 76,598 of those companies are projected to need a third-party assessment.

When finalized, CMMC will require more robust and consistent security implementation by industry. For example, unlike today, where compliance can be achieved simply by a contractor having a plan to meet a security requirement (referred to as a Plan of Action & Milestones (POA&M)), contractors will be expected under CMMC to meet all of DoD's security requirements to gain a certification to be eligible for defense contracts involving CUI no later than 180 days after their CMMC assessment.[6]

Factual Background for Our Hypothetical Scenarios

For the purpose of the below hypothetical scenarios, assume that on July 1–3, 2024, government regulators met at the Pentagon to discuss the proposed rule docketed as DOD-2023-OS-0063-0001: Cybersecurity Maturity Model Certification (CMMC) Program.[7] These regulators, committed to moving this proposed rule forward, carefully considered the 787 public comments that had been submitted.

Due to the urgency of getting CMMC in effect after more than five years of planning, and also to promote stronger cybersecurity and data protection in the defense industrial base without any further delay, the regulators finalized the proposed CMMC rule with no changes. They simultaneously issued an interim/final rule implementing CMMC in the DFARS based on the model identified in the proposed rule establishing the CMMC program. This created new acquisition and contracting requirements for cybersecurity affirmations of compliance with all of the security requirements incorporated in DFARS 252.204-7012 and obligations to flow down CMMC to subcontractors, among other things.[8]

The following three scenarios are based on the premise that the CMMC program will be implemented without any changes made via rulemaking. It should again be emphasized that this premise was invented for this article to prompt the discussion below.

Hypothetical Scenario #1: The Senior Official

Carson is the Senior Manager for Cybersecurity for Acme Defense Corporation (Acme Defense). She is called into her supervisor's office and told, "Congratulations, Carson; you are our company's new Senior Official for affirming continuing compliance with all CMMC security requirements in accordance with the new 32 C.F.R. § 170.22." Even though Carson has only been in the workforce for a few years, she feels confident in the assignment because she knows Acme Defense had just received a final CMMC Certificate at Level 2 after being assessed by a third party as having successfully implemented all 110 security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 Rev. 2, which is incorporated in DFARS 252.204-7012, and are the requirements that need to be met for a Level 2 CMMC certification.

A mere three hours later, Carson's team learns about a zero-day software vulnerability and that patches will not be available for at least two weeks. The team determines that the most effective way to mitigate the security risk from this vulnerability would be to move to a version of the software that does *not* utilize Federal Information Processing Standard (FIPS) 140-2 validated cryptographic mechanisms to protect CUI.[9] By using a different version of the software, Acme Defense would *temporarily* be out of compliance with a NIST SP 800-171 Rev. 2 security requirement, but the move also would protect Acme Defense's IT environment from a breach based on a security threat that had never before been seen or mitigated. Wanting to ensure that the system remains secure, Carson's team moves to the version of the software that does not utilize FIPS 140-2–approved cryptography.

The head of Acme Defense's government contracts compliance office, Karl, stops by Carson's office the next day. Karl says, "Carson, it is time for Acme Defense to make its affirmation of continuing compliance with our CMMC Certification Assessment and all CMMC Level 2 security requirements. We need to enter this affirmation in the Supplier Performance Risk System (SPRS). You are required to make the affirmation as our Senior Official. It is due today. If we do not submit it, we will become ineligible for government contract awards at CMMC Level 2, including a major award expected tomorrow that is critical to our ongoing business."

Remembering the decision to move to the software that utilizes non-FIPS-validated cryptography, Carson hesitates. Then she suddenly remembers attending a presentation that her company's outside law firm recently gave on CMMC. Carson finds the presentation on her phone and the contact information for one of the attorneys who gave the presentation, Nkechi Kanu from Crowell & Moring LLP. Carson calls Ms. Kanu right away to find out how the company should proceed.

Commentary from Nkechi Kanu (Crowell & Moring LLP) on Scenario #1

If Carson decides to submit an affirmation, the key issue is whether attesting to continuing compliance with Acme Defense's CMMC Certification Assessment and all CMMC Level 2 security requirements could be deemed inaccurate or misleading, potentially giving rise to liability under the civil False Claims Act (FCA). This is the case because the company's decision to move to a new version of software that does not utilize FIPS 140-2–validated cryptography means that Acme Defense would not meet all CMMC Level 2 security requirements. Acme Defense could consider three options to mitigate against this risk.

First, the company could engage with its CMMC Third-Party Assessment Organization (C3PAO) to

Published in The Procurement Lawyer, Volume 59, Number 4, Summer 2024. © 2024 by the American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

determine what impact, if any, temporarily moving to a version of software that did not employ FIPS 140-2 cryptography would have on the C3PAO's previous determination that Acme had implemented all 110 security controls from NIST SP 800-171. The risk that a government customer or enforcement body could interpret or argue that the company's annual attestation was misleading or inaccurate would be mitigated by Carson's good-faith reliance on an accredited third party's determination that the company's decision to install, and temporarily use, the new version of the software does not change or impact the determination that Acme complies with all CMMC Level 2 security requirements. The company should memorialize (in writing) its outreach and the response from its C3PAO to support the company's decision to submit its attestation of continuing compliance.

Second, and to the extent the affirmation submission in the online SPRS provides space for commentary,[10] the company could include a POA&M associated with its "temporary" use of software that does not employ FIPS 140-2–validated cryptography. Indeed, under the framework that preceded the CMMC program, the NIST SP 800-171 DoD Assessment Methodology acknowledged the existence of temporary deficiencies and expressly allowed for contractors to consider the control as "implemented" when assessing its compliance and calculating its score:

> *Temporary deficiencies that are appropriately addressed in plans of action (i.e., include deficiency reviews, milestones, and show progress towards the implementation of corrections to reduce or eliminate identified vulnerabilities) should be assessed as "implemented." For example, when a plan of action addresses a "temporary deficiency" that arises after implementation (e.g., 3.13.11, employ FIPS validated cryptography, had been implemented, but subsequently a patch invalidated the FIPS validation of a particular cryptographic module), the requirement will be scored "as implemented."*[11]

Documenting this analysis and conclusion internally and providing the rationale with the company's affirmation could potentially mitigate against the risk of the government later claiming that Acme Defense's SPRS submission attesting compliance was inaccurate or misleading.

Third, Carson could take a conservative approach to addressing the potential risks around the submission of an inaccurate or misleading attestation, with Carson objecting to completing the affirmation of continuing compliance. Carson's decision would be supported by the limited amount of time that she had to carefully review and vet the company's security posture and compliance with CMMC Level 2 requirements.

Although most companies will need to make several changes to their processes, procedures, and practices that were in place when they obtained their CMMC Level 2 Certificate, the current proposed rule does not provide clarification around what changes might conflict or interfere with continuing compliance with a company's CMMC Certification Assessment and all CMMC Level 2 security requirements. IT systems are dynamic after all. In the final rule (not the hypothetical rule issued on July 3, 2024), the parameters around continuing compliance should be clearly defined and the use of POA&Ms should be incorporated into the CMMC framework to allow companies to submit attestations of continuing compliance with requirements when temporary deficiencies are present, helping to avoid the scenario described here where an attestation could otherwise be deemed to be false based on a good-faith decision to mitigate security risk.

Once you have knowledge of noncompliance issues, you cannot simply ignore them. Instead, any responsible government contractor needs to take steps to address the issues.

Hypothetical Scenario #2: The Critical Supplier

Colin is the subcontracts manager for a large production contract, working for a major aerospace and defense prime contractor, Edison Vandelay Industries (EVI). Some of the parts needed for manufacturing weapons systems are difficult to find but essential to build and sustain such systems. In many cases, EVI uses what it calls "single source" suppliers to procure these parts. Some of these suppliers are direct subcontractors to EVI, while others are two or three tiers down in the supply chain. Not many "single source" suppliers are left in the defense supply chain.

One morning, Colin attends a CMMC training conference. During the conference, the presenter (a consultant) emphasized, "Prime contractors shall require subcontract compliance throughout the supply chain at all tiers with the applicable CMMC level for each subcontract. This is written clearly in the new 32 C.F.R. § 170.23(a)." Colin takes this to mean that prime contractors like EVI are required to police their entire supply chains for CMMC compliance.

Before heading back to his office, Colin pulls up the office address for a second-tier supplier on his phone. It is a company called Bob's Welding Shop. Bob's office is just around the corner from the conference. As such, Colin

Published in The Procurement Lawyer, Volume 59, Number 4, Summer 2024. © 2024 by the American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

thinks this might be a good time for a site visit to talk about cybersecurity.

Colin walks into Bob's Welding Shop's office immediately. There is no visitor log or physical security at all, for that matter. Colin finds the owner of the company, Bob, sitting at his desk and staring at engineering drawings on his computer. Colin sees the screen and immediately discerns that Bob is looking at CUI, which has been clearly marked by the DoD. Colin remembers sharing what looks like the same engineering drawing with his first-tier subcontractor in support of a DoD contract. Because Bob's Welding Shop potentially has CUI in its possession, this means that the company could be subject to CMMC Level 2 requirements.

Colin introduces himself. Bob is gracious and happy to see a representative from the prime contractor at the top of the tier (EVI) rather than the distributor Bob only ever communicates with over email. Colin then asks Bob if he has heard of "CMMC." Bob pauses for a moment, replies that he has heard of it and recognizes that it is important, but emphasizes that such extensive cybersecurity requirements would be too expensive to implement for his little welding shop. When pushed, Bob replies, "Colin, do you want me to go out of business? I can't afford all that. In fact, I rejected a DFARS 252.204-7012 and CMMC flow-down requirement from your first-tier supplier and they said nothing about it. They are just a distributor anyway, and they kept ordering my parts. You need me; no one else makes these parts around here."

Colin scratches his head. He remembers what the CMMC consultant said about requiring compliance at all tiers in the supply chain. Here it is apparent that the second-tier supplier, Bob's Welding Shop, refused to comply, and Colin now has knowledge of that fact. But Colin also knows that Bob is right. There is almost no one else who makes these parts (certainly not in the United States), and it will probably take six months or longer for EVI to find an alternative supplier and onboard the supplier through EVI's elaborate procurement system. This all means that EVI likely could not meet schedule on numerous government contracts and would likely lose money/fee, and that critical weapons systems would not be timely delivered to Ukraine to support the war effort.

Faced with a difficult situation, Colin calls his outside counsel, Susan Warshaw Ebner at Stinson LLP, explaining the situation about the noncompliant second-tier supplier. Colin asks Susan for her recommendations and if there is anything he should have done differently.

Commentary from Susan Warshaw Ebner (Stinson LLP) on Scenario #2

In government contracts, it is unwise to try to put things back in the proverbial box after you have taken them out. Once you have knowledge of noncompliance issues, you cannot simply ignore them. Instead, any responsible government contractor needs to take steps to address the issues. Ignoring the issues could invite negative consequences under the contract or via an enforcement action. A compliance problem does not get better the longer you wait, and can become substantially more costly to remedy, so identifying and addressing the issues promptly is key.

Let's unpack the facts: EVI has a critical supplier at a lower tier (Bob's Welding Shop) that, according to the supplier, does not have the DFARS 252.204-7012 clause in its subcontract or a contractual requirement to comply with CMMC. Under the current CMMC model, at least Level 2 compliance is required of a company that is handling CUI for the DoD under a contract or subcontract. Bob's Welding Shop appears to have received CUI from EVI's first-tier subcontractor. While Bob has acknowledged EVI is the prime on his contract, and he has told Colin that Bob's Welding Shop has not taken steps to implement CMMC Level 2, there is still quite a bit that Colin does not know. Colin does not know for sure which DoD contract terms have flowed down to Bob. Colin also does not know what specific information has been provided to Bob (i.e., whether the drawing on the screen is identical to the one EVI provided to its first-tier subcontractor). Given that Bob is a lower-tier subcontractor, EVI does not have privity of contract with him, so Colin's lack of knowledge here is hardly surprising. However, Colin is on notice that there may be compliance issues and there are multiple regulations to consider.

The existing DoD cybersecurity rules should be the starting point. Indeed, the CMMC proposed rule provides that "[t]he information safeguarding requirements and cyber incident reporting requirements set forth in DFARS clause 252.204-7012 will not be phased out as a result of this rule."[12] Thus, this DFARS clause is still the baseline. Assuming EVI as prime contractor has the DFARS 252.204-7012 clause in its prime contract, then independent of CMMC, there is a requirement for contractors to comply with NIST SP 800-171 and to flow down those requirements to its subcontractors.[13]

There also is a requirement under DFARS 252.204-7012(c)(1) to report to DoD in the event of a cyber incident and to cooperate with the DoD as part of the government's investigation. With our hypothetical scenario, there is no information to suggest that there has been a reportable cyber incident or breach. However, EVI should still investigate further as a proactive measure. The risk of a compromise would seem to be much higher if the CUI has not been safeguarded in accordance with the security requirements of NIST SP 800-171. There is an expectation that EVI as a prime will deliver its products without compromise.

Even if there isn't a "cyber incident" as defined by DFARS 252.204-7012, EVI also has an obligation to determine if there has been a violation of the contract requirements to flow down and to comply with the terms of the contract. In addition to the DFARS 252.204-7012(m) flow-down requirement, CMMC requirements are to be

Published in The Procurement Lawyer, Volume 59, Number 4, Summer 2024. © 2024 by the American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

flowed down to all tiers of subcontractors under proposed 32 C.F.R. § 170.23. As such, EVI would need to assess the extent to which it will need to correct, mitigate, and potentially report the failure to flow down cybersecurity requirements to all tiers. And where EVI might be required to report, EVI should explore the nature and extent of the reporting, to whom the report should be provided, and the required timing of such reporting.

In the here and now, Colin's options with Bob are probably limited. Yes, Colin is in Bob's shop right now. However, Colin does not know for certain if the documentation on the computer screen is from EVI or if the engineering drawings have been modified in any way by the first-tier subcontractor (for example, by redacting information or reducing the CUI provided to Bob). Colin could try to reach out to the first-tier subcontractor/distributor while at the shop with Bob to get to the bottom of this and determine whether the documentation on the screen does, in fact, belong to EVI, and whether the information on the screen is, in fact, CUI. If it is, then steps should be undertaken to address the situation and ensure the security of the CUI going forward.

EVI now is aware that its first-tier subcontractor and Bob's Welding Shop apparently are not complying with the mandatory flow-down requirements under the DFARS including CMMC. EVI should do the following:

1. Check its subcontract to ensure it has flowed down all required clauses, including their flow-down requirements, to the first-tier subcontractor/distributor.[14]
2. Reach out to its first-tier subcontractor to:
   a. identify what flow-down terms the first-tier subcontractor included in Bob's subcontract; and
   b. address the immediate situation to avoid further violations of contract requirements by:
   - finding out what information and documentation the first-tier subcontractor provided to Bob's Welding Shop,
   - finding out the level of Bob's system's compliance with CMMC and other cyber requirements,
   - identifying what materials Bob has delivered and been paid for under that subcontract by the first-tier subcontractor and (through the first-tier subcontractor) to EVI, and
   - determining whether Bob can proceed with performance without the CUI and whether there is a way of providing information in hard copy or by providing Bob with remote access to EVI's information system (or another presumably compliant system) and facility.
3. Above all else, make a timely disclosure to address the situation to the DoD.

EVI now is on notice that, at least with regard to this lower-tier subcontractor, the DFARS 252.204-7012 clause and CMMC requirements have not been flowed down and CUI has potentially been provided to this subcontractor. EVI also should check with the first-tier subcontractor and gather information to determine if there have been other instances where the first-tier subcontractor has not flowed down the required clauses to its subcontractors in the supply chain. EVI should conduct additional due diligence on the first-tier subcontractor, seeking confirmation of its compliance with the DFARS 252.204-7012 clause and CMMC flow-down requirements and assessing the first-tier subcontractor's policies and procedures regarding flow-downs through the supply chain, taking steps to correct or mitigate as necessary.[15]

Because the items being procured from Bob's Welding Shop are critical to the performance and delivery of EVI's weapons systems, and if these types of contracts are priority-rated orders under the Defense Production Act Title I Defense Priorities and Allocations System (DPAS), there could be a number of other competing issues that might need to be considered in determining the steps to take. For example, shutdown/stoppage of Bob's and the first-tier subcontractor's performance could result in non-delivery and noncompliance with a priority-rated order's timely delivery requirements. Addressing the issue of what to do in such a situation is a delicate matter. EVI needs to quickly consider how best to coordinate the handling of the situation by the prime, the subcontractors, and the contracting officer.

In addition to performance issues, the failure to flow down DFARS 252.204-7012 and CMMC as required and the potential improper handling of CUI means that EVI needs to ensure it is not making any deliveries or submitting invoices for payment for this work before disclosing the actual or suspected noncompliance to the DoD. This situation warrants timely disclosure to the contracting officer, but it also is something that potentially should be disclosed to the contracting agency's Office of Inspector General pursuant to the mandatory disclosure rule at FAR 52.203-13(b)(3). Now that EVI is aware of what has been happening with Bob's Welding Shop (even if EVI does not yet have all the facts), EVI still needs to assess the applicability of FAR mandatory disclosure requirements and reduce the risk of violating the FCA. Indeed, EVI's prior performance and prior invoices may have been for work that was not in compliance with the prime contract's cybersecurity requirements. Continuing to perform and invoice at this stage without disclosing the potential issues to the government could be risky. But by making an appropriate disclosure, hopefully with government concurrence and subsequent directions as to how best to manage this issue, EVI may potentially limit its FCA liability.[16] This is an important part of addressing the situation. In fact, the US Department of Justice has a task force actively investigating and seeking damages from contractors for failure to comply with applicable cybersecurity requirements.[17]

In addition to the foregoing, EVI may have recourse

Published in The Procurement Lawyer, Volume 59, Number 4, Summer 2024. © 2024 by the American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

against the first-tier subcontractor/distributor for potentially breaching the first-tier subcontract by failing to flow down DFARS 252.204-7012 and CMMC requirements as required. EVI also may seek further remedies and indemnification from the first-tier subcontractor in the event there is a government audit, investigation, and/or prosecution related to the compliance issues raised in this scenario.

At the risk of stating the obvious, this scenario is one that poses a number of complicated issues, and the specific facts and circumstances always need to be considered in determining how best to address the situation. It is the type of issue that may exist today for some prime and higher-tier contractors under DFARS 252.204-7012, but the stakes will be even higher once CMMC is in effect.

Scenario #3: Dispute Resolution

Your client, Mark and Mindy Incorporated (MMI), is a tech company based in Silicon Valley. MMI has recruited top talent, persuaded them to work long hours by offering unlimited snacks and compelling incentive packages, and developed an innovative artificial intelligence product that commercial and defense end-users are interested in buying right away. While MMI is predominantly a commercial company, MMI is trying to break into government contracting and has a few nontraditional defense contracts already. Because MMI processes CUI under DoD contracts, MMI is required to pursue CMMC at Level 2.

MMI believes its third-party assessor made some errors in its CMMC assessment of MMI, meaning that MMI did not receive the CMMC certificate to which it believes it was entitled. MMI has been unable to timely resolve these issues with the assessor or the CMMC Accreditation Body (known as the Cyber AB), a third-party organization responsible for overseeing the assessment training and accreditation of third-party assessors. MMI is therefore currently ineligible to compete for a major new government contract that it strongly believes it can win based on its unique technical capabilities and competitive pricing strategy. Without this award, MMI may not be able to retain some of its top talent needed to perform its government contracting work because these talented individuals will be sought after for other opportunities, potentially impacting MMI's ability to remain involved in government contracting in the long run.

The RFP was just posted online. MMI is backed by some of the wealthiest and most sophisticated investors in the world. They and the government contracts team at MMI take great pride in their early success in disrupting the traditional aerospace and defense industry. The team believes that the delays in achieving CMMC certification are due to "paperwork problems" unrelated to the strength of MMI's security program and that these problems create an unfair barrier to entry into the defense market. However, the team also has been told by its consultants and strategic advisors that it is important to build and maintain relationships with key customers like the DoD and not to irritate these customers unnecessarily. MMI's general counsel reaches out to MMI's outside counsel, Alexander Canizares from Perkins Coie LLP, for advice. What are MMI's options?

Commentary from Alexander Canizares (Perkins Coie LLP) on Scenario #3

I would advise MMI to focus its efforts on finding a quick resolution to the dispute, given the business's priority to obtain this contract and the need for CMMC certification at the time of award. It is also unlikely that an assessment could be obtained in time from another Third-Party Assessment Organization/C3PAO, but that issue also should be discussed with MMI.

I would focus first on what options exist under the CMMC rule's appeal process, notwithstanding MMI's apparent failure to timely resolve its concerns with the C3PAO. Under the CMMC rule (assuming for the sake of discussion that the final rule—which has yet to be issued as of the time of this writing—simply adopts the proposed rule issued on December 26, 2023), each C3PAO is required to have a "time-bound, internal appeals process to address disputes related to perceived assessor errors, malfeasance, and unethical conduct."[18] But the CMMC rule does not establish any fixed timelines or deadlines for appeals. The rule specifies that requests for appeals "will be reviewed and approved by individual(s) within the C3PAO not involved in the original activities in question."[19] Organizations seeking certification (OSC) "can request a copy of the process from their C3PAO."[20] A C3PAO is charged with "address[ing] all OSC appeals arising from CMMC Level 2 assessment activities" and "[a]ny appeal not resolved by the C3PAO will elevate to the Accreditation Body for final determination."[21] The rule further states that if a dispute regarding assessment findings "cannot be resolved by the C3PAO, it will be escalated to the Accreditation Body," whose decision "will be final."[22] The rule is silent as to other considerations, such as the standard of review to be applied to a C3PAO's judgments by the Accreditation Body. It is also notable that the rule does not set forth any role for DoD in adjudicating or mediating C3PAO/CMMC disputes.

In weighing next steps, MMI should consider the extent to which there is still an opportunity to resolve its dispute with the C3PAO before escalating to the Accreditation Body. I would want to understand what communications have occurred between MMI and the C3PAO. I would want to review the C3PAO's appeal process, the errors in the C3PAO's assessment that MMI identified, and the extent to which the C3PAO has responded to MMI's concerns. I also would want to review the original audit agreement between the C3PAO and MMI to understand what terms govern the assessment process and what rights MMI may have to contest findings. Depending on the facts, further engagement with the C3PAO may be a viable next step.

Published in The Procurement Lawyer, Volume 59, Number 4, Summer 2024. © 2024 by the American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

If discussions with the C3PAO are not fruitful or if time is otherwise too short, MMI should consider bringing an immediate appeal to the Accreditation Body. MMI should be especially thoughtful as to what arguments may be made regarding the C3PAO's "flawed" determination to deny CMMC Level 2 certification. I would want to know more about MMI's concerns about the assessment and the reasons for MMI's inability to timely resolve those concerns with the C3PAO. It would be important to confirm whether MMI timely raised its concerns to the C3PAO or whether MMI was responsible for the lack of timeliness. Nothing in the CMMC rule precludes the Accreditation Body from hearing an argument that a delay should be excused or waived.

The CMMC rule could be invoked to support MMI's arguments to the Accreditation Body. As noted above, the rule gives broad authority to the Accreditation Body, whose decisions regarding appeals "will be final."[23] Also, the rule specifies that the Accreditation Body "shall . . . [r]ender a decision on *all* elevated appeals."[24] As the word "all" indicates, the Accreditation Body arguably is required to resolve all manner of assessment disputes (including, perhaps, a dispute over whether a company's failure to bring an appeal in a timely manner should be excused). This interpretation is further reinforced by the language in the rule stating that "[a]ny appeal not resolved by the C3PAO will elevate to the Accreditation Body for final determination."[25] MMI may want to consider arguing that the Accreditation Body can and should review and correct the C3PAO's alleged errors. To the extent that the timeliness issue was the result of vague language in the C3PAO's own terms for challenging assessments, that too should be highlighted.

Two other considerations bear mentioning. The first is whether DoD may (or should) play a role in resolving an assessment dispute such as this. Although the CMMC rule delegates "final" appeal decisions to the Accreditation Body, DoD arguably may retain authority to become involved in assessment-related disputes in its capacity as the overseer of the CMMC program and the Accreditation Body.[26] Given the language in the CMMC rule, MMI should expect that DoD will likely resist stepping into the middle of adjudicating a particular appeal.

The second consideration is what litigation options could be pursued as a last resort. The standard remedy for disputes under FAR-based contracts—submitting a claim to the contracting officer under the Contract Disputes Act[27] and FAR 52.233-1—seems unlikely to be useful to MMI under the circumstances here, especially given that the contract at issue has yet to be awarded. Might MMI seek relief in a pre-award bid protest before the Government Accountability Office (GAO) or the US Court of Federal Claims (COFC)? Such a challenge may give rise to jurisdictional arguments given the limitations of the GAO and COFC to review bid protests. It is well-settled that the GAO's Bid Protest Regulations do not give it authority to resolve disputes between private parties.[28] And the COFC's jurisdictional statute, the Tucker Act,[29] is likewise limited to claims against the United States. In this respect, the CMMC rule's delegation of final decisions in assessment disputes to the Accreditation Body raises various practical and legal issues. Among those issues (which goes beyond the scope of this commentary) is the extent to which the Administrative Procedure Act (APA)[30] may provide judicial review over CMMC assessment disputes. That statute provides a right of action to a party that has been "adversely affected or aggrieved" by agency action.[31] Whether a contractor might develop arguments challenging the CMMC rule (e.g., perhaps arguing that the rule usurps the government's prerogative to decide whether to de facto debar a given contractor by denying it eligibility from a DoD contract) is far from clear. Overall, I would advise MMI to focus its strategy on hopefully obtaining a quick resolution under CMMC's formal processes, especially given that the litigation options are too uncertain to offer a clear path forward.

Conclusion

The above scenarios illustrate just some of the implementation issues that may play out in practice when CMMC is finalized in federal regulations. While the guidance provided in this article by the commentators is thoughtful and well-supported, reasonable minds may differ as to what approaches would be appropriate under the complex fact patterns. Moreover, as in practice, not every idea the commentators suggest would be certain to be effective. How would you (the reader) address the scenarios if presented by your clients or business partners?

In the first scenario (the Senior Official), Carson is put in a position where she may have to choose between security and compliance. While the scenario is fictional, the situation is not. There may be no easy answer. As identified in the commentary, to manage the risk of this type of scenario occurring once CMMC is in effect, companies should establish processes in advance for compliance reviews prior to making affirmations or attestations of compliance.[32] Individuals selected by their organizations to make cybersecurity attestations should be at a sufficiently high level of the organization. They may need to carefully consider a wide range of information before making attestations of compliance as information systems, cyber threats, and an organization's compliance posture are all constantly changing.

In the second scenario (the Critical Supplier), Colin finds himself in a situation where there could be a tension between successful performance on an important government contract and the need to meet cybersecurity flow-down requirements. Once again, while the scenario was contrived for the article, this is another issue that may arise in practice in some form. With the benefit of hindsight, EVI should have established more consistent processes in advance for vetting and overseeing its own suppliers and requiring those suppliers to flow down

Published in The Procurement Lawyer, Volume 59, Number 4, Summer 2024. © 2024 by the American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

cybersecurity requirements. If those requirements are rejected, as identified in the commentary, there are alternative ways to provide CUI besides sending it to a noncompliant information system such as by transmitting in hard copy. EVI also would have been wise to try to identify alternative sources of supply in general rather than having a potential single point of failure on a critical contract. There are many things that could have been done differently.

In the third scenario (Dispute Resolution), MMI confronts a potential barrier in its ability to compete for defense contracts because CMMC certifications will be go/no-go determinations for contract awards. If companies are not able to timely get required certifications, DoD may not be able to acquire innovative products and services. The reduced competition also may lead to higher prices for the government. In addition to the ideas suggested in the commentary, this is another scenario where the hypothetical client could have benefited from better advance planning related to CMMC.

Of course, notwithstanding the realistic-seeming scenarios above, rulemaking is not final for either the rule in 32 C.F.R. establishing the CMMC program or the 48 C.F.R. rule that would implement CMMC in the DFARS. The substance of the above concerns may have been identified in one form or another in the 787 regulatory comments that were submitted. Accordingly, there is still an opportunity for regulators to refine CMMC to avoid unintended consequences. PL

Endnotes

1. The substance of these scenarios was presented initially by Sandeep Kathuria to the American Bar Association's Public Contract Law Section at the Council meeting held during the Federal Procurement Institute conference in March 2024. The dynamic discussion at the Council meeting led to this article in *The Procurement Lawyer*.

2. Companies handling federal contract information as defined in FAR 52.204-21, which is a broader but generally less sensitive category of information, will only need to self-attest as to their safeguards for such information. Companies handling federal contract information would be required to self-attest to CMMC Level 1.

3. *See* Susan B. Cassidy, *DoD Announces the Cybersecurity Maturity Model Certification (CMMC) Initiative*, Inside Gov't Cont. (July 16, 2019), https://www.insidegovernmentcontracts.com/2019/07/dod-announces-the-cybersecurity-maturity-model-certification-cmmc-initiative/.

4. *See* Dep't of Def., Cybersecurity Maturity Model Certification (CMMC) Program, 88 Fed. Reg. 89,058 (Dec. 26, 2023), https://www.federalregister.gov/documents/2023/12/26/2023-27280 cybersecurity-maturity- model-certification-cmmc-program.

5. *See id.* at 89,059.

6. *See id.* at 89,060.

7. *See id.* at 89,058.

8. In reality, as of May 14, 2024, the Office of Management and Budget's Office of Information and Regulatory Affairs is reviewing the proposed CMMC rule associated with a regulatory case at 2019-D041 (Assessing Contractor Implementation of Cybersecurity Requirements). More information can be found at *Open DFARS Cases as of 6/7/2024*, Dep't of Def., https://www.acq.osd.mil/dpap/dars/opencases/dfarscasenum/dfars.pdf.

9 .The FIPS 140-2 requirement is set forth in NIST SP 800-171 Rev. 2, which is incorporated by reference in DFARS 252.204-7012 and must be met in accordance with the CMMC program in its current proposed form.

10. *See* DoD's Supplier Performance Risk System (SPRS), available at sprs.csd.disa.mil.

11. *See* NIST SP 800-171 DoD Assessment Methodology, Version 1.2.1, at 8 (June 24, 220), https://www.acq.osd.mil/asda/dpc/cp/cyber/docs/safeguarding/NIST-SP-800-171-Assessment-Methodology-Version-1.2.1-6.24.2020.pdf.

12. 88 Fed. Reg. at 89,077.

13. This obligation specifically applies even to subcontractors providing commercial products or commercial services, notwithstanding DFARS 252.244-7000, which otherwise attempts to limit flow-down clauses to commercial subcontractors. DFARS 252.244-7000(a)(1) requires a clause be flowed down when "it is so specified in the particular clause."

14. The requirement for flow-down applies to subcontracts and similar contractual instruments, including, but not limited to, distributors.

15. In light of these potential noncompliance issues, EVI may face challenges obtaining the cooperation of its first-tier subcontractor or Bob's Welding Shop once EVI starts its efforts to uncover facts and make disclosures.

16. *See, e.g.*, Press Release, Dep't of Just., Aerojet Rocketdyne Agrees to Pay $9 Million to Resolve False Claims Act Allegations of Cybersecurity Violations in Federal Government Contracts (July 8, 2022), https://www.justice.gov/opa/pr/aerojet-rocketdyne-agrees-pay-9-million-resolve-false-claims-act-allegations-cybersecurity.

17. Press Release, Dep't of Just., False Claims Act Settlements and Judgments Exceed $2.68 Billion in Fiscal Year 2023 (Feb. 22, 2024), https://www.justice.gov/opa/pr/false-claims-act-settlements-and-judgments-exceed-268-billion-fiscal-year-2023 (Cyber-Fraud Initiative: "The Department's effort to combat cybersecurity threats includes the Civil Cyber-Fraud Initiative, which was announced in October 2021. The Initiative is dedicated to using the False Claims Act to promote cybersecurity compliance by government contractors and grantees by holding them accountable when they knowingly violate applicable cybersecurity requirements.").

18. Dep't of Def., Cybersecurity Maturity Model Certification (CMMC) Program, 88 Fed. Reg. 89,058, 89,070 (Dec. 26, 2023).

19. *Id.*

20. *Id.*

21. 32 C.F.R. § 170.10(b)(19).

22. 88 Fed. Reg. at 89,070.

23. *Id.*

24. 32 C.F.R. § 170.8(b)(16) (emphasis added).

25. *Id.* § 170.10(b)(19).

26. *See id.* § 170.6.

27. 41 U.S.C. §§ 7101 et seq.

28. *See* AVER, LLC, B-419244, at *3 (Comp. Gen. Nov. 2, 2020) ("Our Office generally does not review disputes between private parties that do not involve the procuring agency."); Consultants on Fam. Addiction, B-237494, at n.2 (Comp. Gen. Feb. 21, 1997) (dismissing protest ground "because it lacked any factual basis and concerned a dispute between third parties which our Office does not review").

29. 28 U.S.C. § 1491(b).

30. 5 U.S.C. § 701 et seq.

31. *Id.* § 702.

32. For example, contractors could look to the Truthful Cost and Pricing statute for guidance by analogy. Many contractors do a "sweep" to ensure that cost and pricing data have been disclosed to the government prior to making a certification required by FAR 15.406-2.

Published in The Procurement Lawyer, Volume 59, Number 4, Summer 2024. © 2024 by the American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.