24 Cyber Assurance for Prime Contractors

34 The *FAR* at 40

44 Procurement Compliance Review

ISSUE THEME

SUPPLY CHAIN

CONTRACT MANAGEMENT

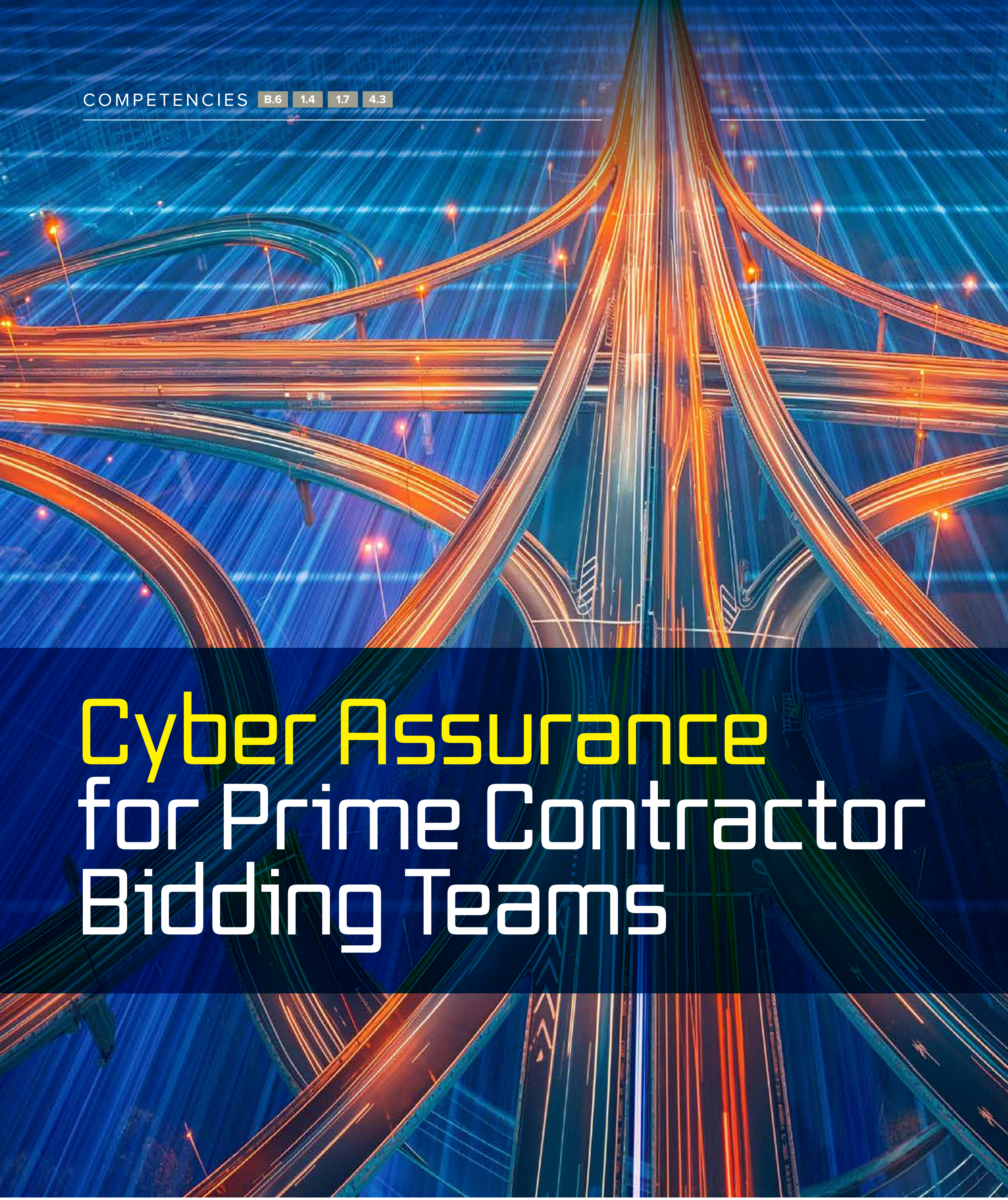
www.ncmahq.org

AUGUST 2024

WEATHERING SUPPLY CHAIN SHOCKWAVES

The path to true supply chain resilience is forged with proactive and reactive contractual solutions.

NCMA®
NATIONAL CONTRACT MANAGEMENT ASSOCIATION
CONNECTING TO
CREATE WHAT'S NEXT



COMPETENCIES B.6 1.4 1.7 4.3

Cyber Assurance for Prime Contractor Bidding Teams

Safeguarding Controlled Unclassified Information (CUI) across the supply chain is critical and the federal government is now moving to implement the Cybersecurity Maturity Model Certification (CMMC) program for Department of Defense contracts and safeguard CUI consistently across a wider range of federal agencies. Prime contractors should increase their due diligence to ensure cyber compliance among subcontractors/suppliers.

By Larry Lieberman

While defense contractors everywhere scramble to get ready for the upcoming Cybersecurity Maturity Model Certification (CMMC) program,[1] there's a lesser-known but potentially greater impact facing most of them: the challenge of assuring that Controlled Unclassified Information (CUI)[2] remains protected across the entire supply chain. CUI is unclassified data sensitive enough to require dissemination controls. It will not matter how well-prepared a CUI-handling contractor is for CMMC if the subcontractors (subs) they share CUI with are not also fully compliant.

Of course, every company doing business with the U.S. Department of Defense (DoD) as a prime contractor (prime) or subcontractor and handling CUI as part of their contract performance should already be aware of and compliant (or working on becoming compliant) with NIST SP 800-171 Revision 2 (R2) cybersecurity requirements for CUI safeguarding.[3] Since the end of 2017, implementation of NIST SP 800-171 on CUI-handling DoD contracts has been mandatory; validating contractor compliance is the goal of the CMMC program.[4]

In May 2024,[5] DoD issued a "class deviation" clarifying that NIST SP 800-171 R2 will remain as the basis for the CMMC program even after the newest revision (R3) takes effect. This means defense contractors across all tiers of the supply chain can be confident in standardizing on the 110 cybersecurity requirements and 320 Assessment Objectives (AO) that are prescribed by NIST SP 800-171 (R2) and its corresponding assessment guide, NIST SP 800-171A.[6] Prime contractors need to ensure their suppliers all understand and address these compliance obligations correctly.

NIST VS. CMMC: WHAT'S THE DIFFERENCE?

Sometimes contractors experience confusion (and/or fatigue) about the differences between the cybersecurity requirements stipulated by the *Federal Acquisition Regulation* (*FAR*), the *Defense Federal Acquisition Regulation Supplement* (*DFARS*), CMMC, and NIST SP 800-171.

To better understand this alphabet soup of clauses and acronyms, keep in mind that *every* federal contract includes FAR clause 52.204-21, prescribing 15 security practices required to ensure Basic Safeguarding of Federal Contract Information (FCI), which includes nearly all contract-related information not intended for public release. DoD contracts add DFARS clause 252.204-7012 on top of that, requiring timely reporting of cyber incidents and adequate safeguarding of Covered Defense Information (CDI), which is CUI with military or space applications.

Adequate safeguarding of CUI on DoD contracts requires implementation of NIST SP 800-171 (R2), which prescribes 110 security practices for safeguarding CUI on non-federal systems. Those 110 requirements include all 15 security practices already mandated by FAR 52.204-21 for all federal contracts.

The DoD's CMMC 2.0 program, currently undergoing final rulemaking, adds more rigorous oversight, assessment, attestation, and certification processes to validate contractor compliance with FCI and CUI safeguarding requirements that already exist in the *FAR* and *DFARS* contract clauses.

CMMC is a three-tiered model in which Level 1 (required for handling FCI) includes all the requirements of FAR 52.204-21, while Level 2 (required for handling CUI) includes all the requirements of NIST SP 800-171 (R2). Level 3, designed only for a small percentage of contracts that are considered highly sensitive, adds some of the "enhanced" requirements prescribed by NIST SP 800-172.

For FCI-handling, CMMC Level 1 requires annual self-assessment and affirmation of compliance by a "senior company official." CMMC Level 2 will require most CUI-handling contractors to start with self-attestation and then obtain third-party certification of their compliance with all of NIST SP 800-171 (R2). Level 3 of CMMC will require a small percentage of contractors to be assessed by the government.

LOOKING ACROSS THE SUPPLY CHAIN

One facet of CMMC that many prime contractors overlook is that their suppliers, subcontractors, vendors, and service providers on DoD contracts that perform any work that involves handling CUI will also be required to prepare for and meet the same NIST SP 800-171 (R2) compliance requirements, all the way down to the "Assessment Objective" level. The bottom line is most of the supply chain is not ready.

Prime contractors have control over their own information systems and their own compliance initiatives, but they do not control their suppliers' systems or operations, and that makes it hard to achieve confidence in supplier compliance status.

By increasing due diligence, insisting on more transparency and cooperation, and providing education and assistance to struggling suppliers, prime contractors can develop greater assurance that suppliers will successfully achieve full compliance with NIST SP 800-171 (R2) and remain eligible for new DoD awards.

Learning how to document their compliance efforts correctly and gather the evidence needed to validate their proper implementation of all assessment objectives ensures suppliers will become better prepared for CMMC and any other cybersecurity compliance programs they may encounter in the future.

SAFEGUARDING CUI: IT'S FOR MORE THAN JUST DOD CONTRACTORS

The term CUI is applicable across the federal information landscape, and multiple federal agencies have CUI safeguarding policies. The National Archives and Records Administration (NARA) maintains a CUI Program Blog[7] that provides links to education, resources and information for all federal contractors that handle CUI.

A draft of the long-anticipated FAR CUI rule expected to require implementation of NIST SP 800-171 for safeguarding CUI in other federal contracts was submitted to the Office of Information and Regulatory Affairs (OIRA) in May 2024 for review prior to publication (see more details in the procurement rules section below).

DoD is leading the charge to improve contractor cybersecurity across the Defense Industrial Base (DIB), but any contractor performing work for other federal agencies or

DoD prime contractors are especially vulnerable to contract risks and liabilities based on non-compliance of their suppliers.

regulated industries such as energy, finance, and health care can benefit from learning how to gather the evidence needed to support a third-party validation of cybersecurity compliance.

While some federal agencies and commercial industries currently accept self-attestation of adherence to cybersecurity standards as the status quo, this simply will not be enough if those contracts adopt CMMC-style third-party cybersecurity assessment requirements that involve evidence-based validation in the future.

FOR DOD CONTRACTS, SUPPLY CHAIN CYBER ASSURANCE IS CRITICAL

DoD primes are especially vulnerable to contract risks and liabilities based on non-compliance of their suppliers. Primes are responsible for ensuring that all CUI-handling suppliers on DoD contracts are compliant with all applicable requirements. This means primes need to establish with high confidence and reasonable assurance that their subcontractors that handle CUI are accurately *saying what they're doing and doing what they're saying*.

Many prime contractors have been distributing letters, inquiries, surveys, and questionnaires to their subs to check on supplier cyber compliance status, but it is insufficient for a supplier or subcontractor to simply state that they're "compliant" or on track for future CMMC certification as part of a response to an inquiry from their prime(s). After all, DoD initially assumed self-attestations of cyber compliance would be an adequate approach to verify prime contractors' compliance, but soon found that it didn't work.[8]

Without requesting adequate substantiation, there is no way for a prime contractor to know whether their supplier's self-attestations are correct. In an alarmingly large number of cases, those attestations unfortunately prove to be inaccurate – and that's just at the first tier of the supply chain. Imagine how much the risk of non-compliance increases as CUI passes down to subsequent tiers below.

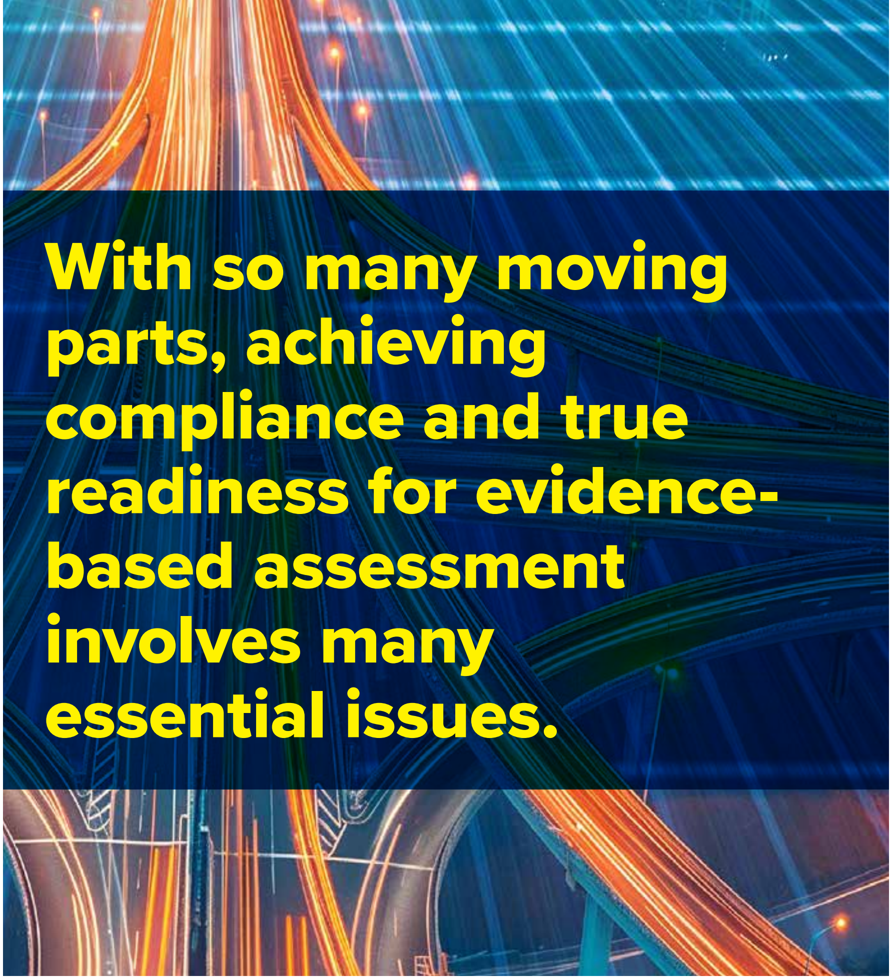
For a prime contractor to gain the proper level of assurance that their suppliers will really, truly be ready for a third-party certification assessment or even to accurately self-assess their compliance with CMMC Level 2 (for handling CUI), additional due diligence is necessary.

Primes need to validate that their suppliers are making adequate progress in implementing the 110 requirements of NIST SP 800-171 (R2) and documenting their implementations properly, by gathering and organizing the evidence an assessor will eventually need to review to confirm satisfaction of each of the 320 Assessment Objectives needed to obtain CMMC Level 2 certification.

Contract managers should coordinate with their procurement and supply chain managers to ensure all CUI-handling suppliers (and all *their* suppliers who also process CUI) are providing adequate validation that they are on track for CMMC in order to develop confidence that those suppliers will be safe to rely on in the future.[9]

THE NEED FOR ASSURANCE ON MULTIPLE FRONTS

Many prime contractors find themselves fighting a battle on two fronts: most are preoccupied with the immediate need to address their own internal compliance, but at the same time are faced with massive risk from their non-compliant subcontractors and suppliers.



With so many moving parts, achieving compliance and true readiness for evidence-based assessment involves many essential issues.

Further complicating the picture is a nascent industry of compliance consultants with varying levels of knowledge and experience. Primes need assurance that their consultants (and those used by their suppliers) are properly vetted to assure they are competent in relevant areas.

So what can a prime contractor do to develop adequate assurance that its suppliers really are on track to meet CMMC requirements at all tiers of the supply chain? One of the most important key points to start with is identifying the flow of CUI across the supply chain, then asking the right questions of the right stakeholders and seeking the right type of information from suppliers about their progress in implementing NIST SP 800-171 requirements.

Suppliers should be ready, willing, and able to offer the right kind of documentation to their primes. For suppliers, responsiveness, transparency, and verifiable effort to achieve adequate levels of readiness will become differentiators that set them apart from less cooperative and poorly prepared competitors.

Contract and procurement managers in organizations that have many suppliers, subcontractors, and vendors should coordinate carefully to identify critical suppliers, accurately evaluate their compliance status, identify non-responsive and high-risk suppliers, and either directly assist or start looking for suitable replacements for critical suppliers that are not likely to achieve compliance.

With so many moving parts, achieving compliance and true readiness for evidence-based assessment involves many essential issues, including:

- ***Assurance that your own organization is on the right path to CMMC Level 2 certification***: Despite what many internal information technology staff and external cyber consultants may claim, the only way to truly assure that your own compliance effort is on track to pass a CMMC certification assessment is to have a CyberAB[10] accredited CMMC Third Party Assessment Organization (C3PAO)[11] or a Registered Practitioner Organization (RPO) with experienced Registered Practitioner Advanced (RPA)[12] personnel perform a readiness assessment at either a medium or high confidence level (i.e., spot-checking requirements or conducting a full evidence-based assessment). Only experienced and proven Lead Certified CMMC Assessor (CCA) personnel can assure 100% validation that all requirements are being met properly and will stand up to the scrutiny of a CMMC Level 2 certification assessment by a C3PAO team driven by a Lead CCA.
- ***Assurance that your own organization is getting correct guidance from consultants***: To ensure correct guidance, it's important to work with a C3PAO or RPO whose consulting staff hold CCA or Registered Practitioner Advanced (RPA) designations. RPAs are trained on CUI while Registered Practitioners (RPs) are trained on CUI and CMMC Level 2, while Registered Practitioners

(RPs) are just trained on FCI and CMMC Level 1. Note that within the CMMC consulting marketplace, some vendors may hold RPO status without having any RPAs, and in some cases even no RPs on staff. Due diligence is important when vetting consultants, and only RPA-accredited or CCA-accredited individuals have received the full CyberAB-sanctioned training to provide accurate guidance on how to properly interpret the requirements, gather and organize evidence, and successfully achieve compliance with all of NIST SP 800-171 (R2).

- ***Assurance that any external service provider (ESP) you are using is also CMMC-ready***: This is an area that has become a major consideration in compliance planning based on the release of the CMMC 2.0 proposed rule in December 2023.[13] The proposed rule states that any external service provider that handles or has access to CUI or provides services used to protect CUI must also obtain the same level of CMMC required by the contract. This narrows the available ESP pool down to a very small number of companies that can be relied upon to provide compliant services.
- ***Assurance that your CUI-handling supply chain (and all ESPs used by those suppliers) are also on the right path – including meeting every requirement described herein, for every CUI-handling supplier***: Any prime or mid-tier sub who shares CUI with lower tier suppliers must also assure that all of its CUI-handling suppliers have each correctly achieved all of the same assurances for their own compliance. Without these assurances, it is not possible to be certain of the risk presented by the supply chain. This is why supply chain cyber assurance is critical to establishing successful bidding teams for future contracts.
- ***Assurance that your entire bidding team is ready for increased self-assessment requirements during Phase 1 of the CMMC rollout***: One of the most surprising aspects of the proposed CMMC

With so many moving parts, achieving compliance and true readiness for evidence-based assessment involves many essential issues.

2.0 ruling is the government's intended implementation schedule[14] and the updated approach to self-assessment as compared with the current type of basic self-assessment required by DFARS 252.204-7019/7020. Under the proposed rule, all new DoD contracts will start including CMMC self-assessment requirements at the appropriate level (Level 1 for FCI-handling and Level 2 for CUI-handling), starting immediately when the ruling becomes effective. The self-assessment for CMMC Level 2 is not just submitting a "score" to SPRS that reflects overall status but is a legal representation that the organization has fully completed its compliance efforts and that the evidence needed to validate all assessment objectives would be available to present to an assessor if required. Prime contractors should be urgently communicating with their suppliers to make sure they are aware of this difference and clear about what self-assessment will entail for CMMC, and they should keep close track of supplier progress.

STRATEGIES FOR DEVELOPING TRUE ASSURANCE OF SUPPLIER CYBER COMPLIANCE SUCCESS

There are two basic approaches recommended for primes that want to validate that their CUI-handling suppliers are on track and likely to be ready for CMMC Level 2 self-assessment or third-party certification in the future:

1. Request that the supplier undergo a full evidence-based CMMC readiness assessment.

   or

2. Request that the supplier undergo a partial "spot-checking" review of supplier status details as a minimum level of assurance that they are indeed on the right track.

The highest-confidence approach is to ask suppliers who self-attest to compliance to undergo a full evidence-based third-party readiness assessment, which is similar to a certification assessment by a CMMC Third-Party Assessment Organization (C3PAO). A full readiness assessment involves a trained assessor or team of assessors reviewing evidence for each of the 320 Assessment Objectives prescribed by NIST SP 800-171A assessment guidance.

The assessment team used for such an effort should be led by a fully credentialed CyberAB Certified CMMC Assessor (CCA) who has been approved by the CyberAB as a Lead Assessor. Uncredentialed IT and cybersecurity vendors that promise to help organizations prepare for CMMC assessment cannot always be relied upon to provide accurate consultation.

If a supplier is not yet ready for a full readiness assessment that validates compliance with all the requirements of NIST SP 800-171, it can still hire a willing C3PAO to conduct a CMMC health check, essentially spot checking a subset of the entire set of requirements to confirm that they are being met correctly. A CMMC health check would be at the discretion of the C3PAO and adhere to a specified scope of work defined by the C3PAO if it is open to this type of engagement, or it may be part of a larger service that it offers.

To achieve a medium level of confidence in a supplier's readiness, a prime can request that the supplier engage with CyberAB accredited consultants, such as a C3PAO or an RPO with RPA staff to review the supplier's SSP and Plan of Action and Milestones (POAM) documentation, verifying that the SSP conforms with NIST SP 800-171 requirements and that the POAM is adequately addressing any unmet requirements.

To make sure suppliers are getting the correct guidance from consultants, they should only work with CyberAB-accredited companies, since the CyberAB is the DoD's designated non-profit administrator of the vast CMMC training, consulting, and certification marketplace. Even companies who handle CUI for non-DoD federal contracts can engage with CyberAB credentialed consultants to ensure their compliance with NIST SP 800-171 is validated.

It is important to note, however, that not all CyberAB accreditations are equal. Consulting companies can become RPOs relatively easily, offering to help Organizations Seeking Certification (OSC) to prepare for CMMC without becoming CMMC-compliant themselves, or even having any highly trained or experienced staff.

The qualifications to become an RPO are far less rigorous than what is required to become a C3PAO, and the qualifications for an individual to become an RP are also far less rigorous than to become an RPA, Certified CMMC Professional (CCP), or CCA. Therefore, to ensure the highest level of confidence (and lowest risk of failure), organizations seeking third party consultation for CMMC preparedness should engage with consultants that are both C3PAO and RPO accredited, whose staff hold RPA (not just RP), CCP, and/or CCA designations and have substantial past experience with NIST assessments.

The pool of available and experienced consultants is limited – as of the time of this writing there are 53 fully accredited C3PAO firms, 318 RPOs, and 138 RPAs (note that the CyberAB site does not list RPAs as a separately searchable category, so companies have to verify with their consultants directly to make sure they have RPAs and not just RPs).

It is true that no supplier is required to engage with any third-party consultant just because a prime contractor recommends (or even demands) it, but it is also true that no prime contractor is obligated to issue subcontracts to a supplier that it has not developed an adequate level of confidence in. Primes can ask suppliers to meet any type of vendor selection criteria they choose, and if a prime contractor wants well vetted subs with a high assurance of CMMC readiness, then they must apply pressure to their suppliers to obtain the right type of help. Without this type of assurance, primes face significantly higher risk.

Primes can and should expect

their suppliers to take their cyber compliance obligations seriously, and do what it takes to ensure readiness. Providing prime contractors with assurance that they are one of the reliable suppliers making adequate progress toward cyber compliance goals should become second nature to any subcontractor working on DoD projects. Preparing properly for DoD requirements will also give those suppliers a head start if similar requirements are adopted by other agencies or industries.

PROCUREMENT RULES ARE CHANGING TO SUPPORT INCREASED SUPPLY CHAIN SECURITY

While the defense industrial base holds its breath waiting for publication of the final CMMC ruling, the gears of government are turning, bringing myriad changes in federal contracting designed to improve security across the DIB and to the broader community of federal contractors.

- ***FAR CUI Proposed Rule:*** Perhaps one of the most significant developments in the nation's move toward increased cybersecurity across all federal contracts is the progress currently being made in establishing new *FAR* rules for safeguarding CUI.[15] The open FAR case number 2017-016 had been lying dormant for years, but in March 2024 a draft proposed FAR CUI rule was released to the Office of Federal Procurement Policy (OFPP) for review, and then in May 2024 the Civilian Agency Acquisition Council (CAAC) sent the proposed FAR CUI rule to OIRA, indicating progress toward publication. It is widely expected that a final FAR CUI rule will establish NIST SP 800-171 as the standard for safeguarding CUI on non-federal systems *across the entire federal contracting landscape.*
- ***DIB CS Program Final Rule:*** This final ruling published in March 2024 opens up the DIB Cybersecurity (CS) program's bilateral information-sharing resources and capabilities to a broader section of the defense contractor community.[16] Previously, access to the DIB CS program was limited to cleared contractors handling classified information. The new ruling makes the program available to all DoD contractors handling CUI, providing contractors with important information to improve their cybersecurity readiness. This ruling will also change the requirement to obtain a Medium Assurance Certificate for access to the DIBNet cyber incident reporting portal;[17] access will instead be granted through registration with the Procurement Integrated Enterprise Environment (PIEE).[18] This may be a small step, but it eases the burden on small- and medium-sized subcontractors by providing an easier way to prepare for incident reporting and gives them access to threat information-sharing resources.
- ***FAR Part 40:*** Another recent change to the federal procurement process was quietly introduced in April 2024 with the issuance of a final ruling to add a new FAR part 40.[19] This new ruling does not implement any new policies or procedures at this time, but it does create a new *FAR* part to accommodate new rules related to a wide array of requirements focused on managing information security and supply chain security. Over time, the government procurement community will leverage this new *FAR* part as a location to cover broad security requirements that apply across a wide range of acquisitions. For contractors and subcontractors this means that the government is putting the framework in place to increase emphasis on information security and supply chain security.

These various machinations across the federal procurement community, in conjunction with the upcoming changes to CFR Title 48[20] and CFR Title 32[21] in support of the CMMC program, and the DOJ's Civil Cyber Fraud Initiative,[22] which is leveraging the False Claims Act (FCA)[23] to prosecute companies that misrepresent their cybersecurity status, all point to broader application and enforcement of contractor and subcontractor cybersecurity requirements.

Primes who wait until the last minute to verify the status of their critical suppliers will face serious impacts to their DoD contracting eligibility; but suppliers who engage with accredited consultants and prepare accurately for evidence-based assessment will find themselves in a very favorable position when the CMMC program rules become effective.

Companies that don’t get serious about compliance for themselves and their suppliers will likely end up wishing they had done more while there was still time.

CONCLUSION: SUPPLY CHAIN CYBER ASSURANCE REQUIRES MORE THAN JUST QUESTIONNAIRES!

All indications point to the government’s intent to implement the CMMC program in exactly or very close to the way it has been proposed, and to expand efforts to safeguard CUI consistently across a wider range of federal agencies. Companies that don’t get serious about compliance for themselves and their suppliers will likely end up wishing they had done more while there was still time.

Primes should increase the due diligence they apply to their situational awareness of supplier cyber compliance status and incentivize their critical suppliers to take action. When primes develop strong relationships of trust and collaboration with their suppliers, the entire supply chain will benefit and our nation will move closer to achieving its national security objectives. **CM**

Larry Lieberman is a subject matter expert and educational content developer at eResilience who has helped produce dozens of national educational webinars on DFARS/NIST/CMMC compliance in conjunction with the Cyber Collaboration Center. These webinars have been widely attended and highly rated by thousands of DIB contractors. For free CMMC supply chain compliance training for prime contractor procurement teams, please email a request to info@eresilience.com.

ENDNOTES

[1] https://dodcio.defense.gov/CMMC/About/

[2] https://www.archives.gov/cui

[3] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf (note that R2 has been withdrawn and replaced by R3, however R2 will remain in effect for the DoD’s CMMC program indefinitely until further notice)

[4] For more information on the history, details, and status of the CMMC program see “*The Maturity of Supply Chain Security - The Impact of the Cybersecurity Maturity Model Certification on the Defense Industrial Base*” by Michael Gruden, et. al in the May 2024 issue of NCMA *Contract Management* Magazine. Accessible at https://ncmahq.org/Shared_Content/CM-Magazine/CM-Magazine-May-2024/The-Maturity-of-Supply-Chain-Security.aspx

[5] https://www.defense.gov/News/Releases/Release/Article/3763953/department-of-defense-issues-class-deviation-on-cybersecurity-standards-for-cov/

[6] https://csrc.nist.gov/pubs/sp/800/171/a/final

[7] https://isoo.blogs.archives.gov/about-the-carter-chronicle/

[8] https://media.defense.gov/2019/Jul/25/2002162077/-1/-1/1/DODIG-2019-105.PDF

[9] For more details on this process, prime contractor procurement teams can access additional briefings, case studies, and free CMMC supply chain compliance training by sending an email request to info@eresilience.com.

[10] https://cyberab.org/

[11] https://cyberab.org/CMMC-Ecosystem/Ecosystem-Roles/Assessing-and-Certification

[12] https://cyberab.org/CMMC-Ecosystem/Ecosystem-roles/Consulting-and-Implementation

[13] https://www.federalregister.gov/documents/2023/12/26/2023-27280/cybersecurity-maturity-model-certification-cmmc-program

[14] https://federalnewsnetwork.com/defense-news/2023/12/dod-outlines-four-phase-approach-to-implement-cmmc-in-proposed-rule/

[15] https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202310&RIN=9000-AN56

[16] https://www.govinfo.gov/content/pkg/FR-2024-03-12/pdf/2024-04752.pdf

[17] https://dibnet.dod.mil/dibnet/

[18] https://piee.eb.mil/

[19] https://www.federalregister.gov/documents/2024/04/01/2024-06411/federal-acquisition-regulation-establishing-federal-acquisition-regulation-part-40

[20] https://www.ecfr.gov/current/title-48

[21] https://www.ecfr.gov/current/title-32

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

[23] https://www.justice.gov/civil/false-claims-act