SUPPLY CHAIN MANAGEMENT

CONTRACT MANAGEMENT

www.ncmahq.org

SEPTEMBER 2023

Information technology negotiator Nick Traboulay lifts the curtain on how companies qualify suppliers, make deals, gather market intelligence, and get inside the heads of sales reps.

Managing Suppliers: The Industry View

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

COMPETENCIES 1.4 B.5 4.3 B.6

Double Trouble

Defense prime contractors must ensure their own compliance with complicated cyber requirements while also policing their subcontractors.

By Larry Lieberman

There is risky business ahead for defense contractors that share controlled unclassified information (CUI)[1] with their subcontractors.

Most prime contractors working on Department of Defense (DoD) projects are aware of strict *Defense Federal Acquisition Regulation Supplement* (*DFARS*) cybersecurity compliance requirements. They also know that scrutiny and enforcement is on the rise due to the Cybersecurity Maturity Model Certification (CMMC) initiative.[2] But few realize how much jeopardy they face when it comes to tracking and assessing subcontractors' compliance.

Getting ready for CMMC is top of mind for most large DoD contractors. However, it's often overlooked or misunderstood by small- and medium-sized companies within the supply chain.

A good starting point for companies wrestling with cyber compliance is to carefully review the language of the relevant *DFARS* clauses, and make plans to address each one. This is critical for prime contractors with a significant number of CUI-handling suppliers. All those suppliers must get prepared for third-party CMMC Level 2[3] certification.

Contractors frequently underestimate the effort required for certification. They often are not aware they must prepare specific, detailed evidence for hundreds of items the third-party assessors will validate. Proactive primes are waking up to the importance of ensuring key suppliers are on track to meet the massive need for evidence of compliance.

To prepare for the coming enforcement of cybersecurity requirements, it is useful to review key points within *DFARS* clauses 252.204-7012 / 7019 / 7020. Also relevant are anticipated prime and subcontractor obligations relating to DFARS 252.204-7021 (CMMC).[4] Once companies identify key liabilities for failing to ensure that they, and all of their CUI-handling subcontractors, completely address cyber regulations, they will want to reduce the risks of supplier noncompliance. This article will recommend best practices for minimizing those risks.

At the heart of the cyber regulations is a requirement for prime contractors to flow requirements down to their subcontractors and ensure compliance across the supply chain before sharing CUI. Only contractors and subcontractors handling CUI are obligated to safeguard it, implement NIST SP 800-171[5] security requirements (also known as "practices"), adhere to strict cyber incident reporting rules, and prepare for third-party CMMC assessment and certification of cyber compliance.

One of the first and most important activities for CUI-handling contractors should be determining what CUI is being handled, and with whom it is being shared. Once the CUI chain of custody is clear, prime contractors can more accurately track and manage compliance responsibilities across the supply chain.

Key Points in the Cyber Clauses

Contractors should understand, remember, and address these points in *DFARS* cyber clauses and the DoD's NIST SP 800-171 Assessment Methodology:

- ► Contractors must flow DFARS 252.204-7012 *Safeguarding Covered Defense Information and Cyber Incident Reporting*[6] down to their subs, and those subs must flow it down to their lower-tier suppliers. At minimum, all CUI-handling parties across the supply chain must implement NIST SP 800-171 security practices and have a conforming system security plan (SSP),[7] and plan of action and milestones (POAM)[8] documentation in place. Every contractor working with CUI also must obtain a medium assurance certificate[9] from one of the DoD's External Certification Authorities (ECA).[10] The certificate is required for mandatory reporting to the DoD in case of a cyber incident. Contractors must report any cyber incident affecting the covered contractor information system (CCIS)[11] to the DoD's Cyber Crime Center (DC3) through the DIBNet portal[12] within 72 hours of discovery.
- ► DFARS 252.204-7019[13] requires all CUI-handling DoD contractors and subcontractors to conduct a NIST SP 800-171 "Basic Assessment." The aggregated compliance score must be submitted to the Supplier Performance Risk System (SPRS), along with an estimated completion date for implementing all remaining items in the POAM, before being awarded any new CUI-handling contracts or subcontracts.
- ► DFARS 252.204-7020[14] makes prime contractors liable for ensuring their subcontractors submit NIST SP 800-171 Basic Assessment reports to SPRS before awarding any new subcontracts that involve handling CUI. This clause puts primes at extreme risk of noncompliance if they share CUI with subcontractors without verifying the subs have successfully reported to SPRS.
- ► DFARS 252.204-7021 *Cybersecurity Maturity Model Certification Requirements*,[15] published in 2020, introduced the CMMC program. This clause establishes the expectation that CMMC requirements (once implemented into a contract) will be pre-award obligations that every FCI/CUI-handling member of the bidding team must meet before contract award.
- ► The DoD NIST SP 800-171 Assessment Methodology[16] provides a scoring formula for contractors to self-assess their compliance and report that status to SPRS. The methodology also introduces three levels of assessment that the government may implement to get more information about a contractor's NIST SP 800-171 compliance status. Basic Assessment involves self-reporting of compliance status. Medium Assessment involves government review of the contractor's SSP. High Assessment involves evidence-based assessment of all security requirement implementations. An often-overlooked

The Crucial Role of Procurement Preparedness:

Supporting Humanitarian Assistance and Disaster Response

Sponsored by Amazon Business

In times of crisis, the ability of federal, state and local government agencies to respond swiftly and effectively is crucial. While emergency disaster preparedness encompasses various aspects, one often overlooked component is procurement preparedness. Establishing robust procurement processes and frameworks is essential for public sector agencies to acquire the necessary goods and services promptly during emergencies.

Understanding Procurement Preparedness

Procurement preparedness involves strategic planning and readiness within public sector agencies to procure goods and services efficiently related to Humanitarian Assistance and Disaster (HADR). It encompasses establishing frameworks, systems, and partnerships that allow agencies to access necessary resources swiftly while maintaining transparency and streamlining procurement processes. Here's why procurement preparedness is essential for public sector agencies:

Swift Response:
In times of crisis, time is of the essence. Adequate procurement preparedness ensures that agencies promptly respond by procuring essential supplies, such as medical supplies, communication equipment, food, water, and other critical resources, without unnecessary delays. Being prepared minimizes administrative hurdles and enables agencies to address urgent needs promptly.

Resource Optimization:
Disasters often lead to increased demand and potential price increases for essential resources. By embracing procurement preparedness, agencies can establish budgets, develop supplier networks, and engage in bulk purchasing arrangements in advance. This proactive approach optimizes resource allocation, helps control costs, and avoids unnecessary competition for scarce resources.

Federal Micro-Purchases for Contingency Contracting:
Micro-purchases, as defined under FAR 2.101, allow federal agencies to procure goods and services up to a specific dollar threshold (currently $10,000) without requiring competitive bids. During emergencies, this process becomes particularly valuable, enabling agencies to procure necessary supplies from qualified sellers. Micro-purchases eliminate red tape and expedite the procurement process, facilitating rapid response efforts.

Transparency and Accountability:
Maintaining transparency in procurement processes is crucial for government agencies, especially during emergencies. By establishing clear guidelines, ensuring documentation, and incorporating appropriate oversight mechanisms, agencies uphold public trust and prevent any perception of impropriety. A transparent procurement system also promotes accountability and reduces the risk of fraud or corruption.

Best Practices for Procurement Preparedness

To enhance procurement preparedness and maximize the benefits of micro-purchases for contingency contracting, agencies can adopt the following best practices:

Comprehensive Planning:
Develop comprehensive procurement plans tailored explicitly to HADR scenarios. These plans should include clear roles and responsibilities, establish a framework for decision-making, and outline the necessary steps for expedited procurement processes during emergencies.

Prequalified Supplier Pool:
Maintain an up-to-date database of prequalified suppliers who can provide critical goods and services during emergencies. This ensures that agencies can access a list of vetted vendors who can be quickly engaged during a crisis.

Develop Contingency Plans:
Create contingency plans that address potential disruptions in supply chains during emergencies. Identify alternative sources of supply and establish agreements with backup suppliers to ensure the continuity of critical resources. These plans should account for various disaster scenarios and outline alternative procurement methods when standard processes are not feasible.

Technology Integration:
Leverage technology to streamline procurement processes and facilitate transparency. Implement e-procurement systems, with integrations into partners like Amazon Business, that enable competitive pricing, track and monitor purchasing patterns, and efficiently manage your cashflow. Automation reduces administrative burdens, ensures accuracy, and improves the speed of procurement operations and audit readiness.

Collaborative Partnerships:
Establish partnerships and collaborations with other government agencies, private sector entities, and nonprofit organizations. These relationships foster information sharing, resource pooling, and coordinated efforts during emergencies. Collaborative partnerships enhance the overall resilience and effectiveness of disaster response and recovery operations.

Monitoring and Evaluation:
Regularly evaluate the effectiveness of procurement processes and emergency response efforts. Analyze data and feedback to identify areas for improvement and implement necessary adjustments. Continuous monitoring and evaluation help optimize procurement practices, enhance preparedness, and drive efficiency in future emergencies.

Be prepared with Amazon Business

No matter how prepared your agency becomes, you can’t prevent an unexpected disaster, but you can be prepared for one. Amazon Business is proud to support government organizations on the front lines with access to critical supplies and resources to help solve procurement challenges.

amazon business

Visit business.amazon.com/government to learn more

> aspect of the DoD Assessment Methodology is that section 2.c clarifies that a prime contractor may use the same methodology to assess its subcontractors. It is fully within a prime contractor's rights to require evidence of compliance from subcontractors and conduct assessments of subcontractors before sharing CUI with them. Subs should insist on confidentiality and non-disclosure agreements yet be prepared to share compliance status information with prime contractors if and when requested.

It's essential that primes and their subs work collaboratively to address problems associated with understanding and successfully navigating current cybersecurity clauses. Cooperation will also be needed to prepare for even greater scrutiny and effort under the CMMC program.

"The prime contractor is responsible for ensuring the entire bidding team is CUI compliant. Prime contractors are at increased risk if they fail to conduct adequate due diligence on their subcontractors' compliance status."

What Is Ahead Under CMMC?

Under the CMMC 2.0 model,[17] prime contractors will still be responsible for obtaining CMMC certification. They also must flow down that requirement down to subcontractors. Once CMMC requirements start appearing in contracts, prime contractors must ensure that any subcontractor handling CUI has obtained CMMC certification at the prescribed level prior to awarding it a subcontract.

Because CMMC will be a pre-award requirement for all participants, all CUI-handling primes and subcontractors should be working now toward implementing NIST SP 800-171. They should also be gathering the evidence needed to prepare for third-party assessment.

Keep in mind that CMMC *does not add any new requirements.* It creates a certification model to ensure that CUI-handling contractors are implementing the safeguarding practices they are supposed to already have in place. CMMC adds oversight and enforcement to ensure that all CUI-handling contractors are implementing the existing NIST SP 800-171 requirements.

There's a very real risk to a prime's future DoD business if they or their supply chain are noncompliant.

The Risk Is Real

Primes have good reason to be careful about ensuring cyber compliance across the supply chain. Ultimately, the prime contractor is responsible for ensuring the entire bidding team is CUI compliant. Prime contractors are at increased risk if they fail to conduct adequate due diligence on their subcontractors' compliance status.

Robert Metzger, with the law firm RJO, described the urgency of CMMC requirements during the NCMA CMMC training webinar in June 2023. He explained that the Department of Justice (DOJ) has been stepping up enforcement of cyber compliance through the 2021 Civil Cyber Fraud Initiative. The DOJ intends to use the False Claims Act (FCA) to seek what may be substantial penalties against DoD contractors that misrepresent or mischaracterize their own compliance or the compliance of their suppliers.

In addition to the FCA, Metzger said "there are contractual consequences of non-compliance. The risk is real." As an example, he cited the importance of making progress on plans of action involving implementation of NIST SP 800-171.

The expected completion date for implementation of a POAM is shared with the government when a company performs a self-assessment and submits it to the DoD Supplier Performance Risk System (SPRS). At that point, the completion date may become a contractual obligation the government can act upon if missed.

"DoD has advised that failure to have or make progress on a plan to implement NIST SP 800-171 requirements may be considered a material breach of contract requirements." Metzger says. "Remedies for such a breach may include withholding progress payments, forgoing remaining contract options, and potentially terminating the contract in part or whole. I would not want to chance it."

Metzger went on to emphasize the importance of cyber incident reporting.

"You should know that there is an important obligation to report cyber incidents within 72 hours of discovery," Metzger explains. "If you fail to report an incident when you should have, you could get in trouble under the False Claims Act."

Increased scrutiny from the government may bring increased exposure for DoD contractors, as the urgency around compliance continues to escalate. Ultimately, the DoD has the authority to investigate noncompliance. According to Metzger, it's even possible that in extreme cases a company could face suspension or debarment. This could happen if a company represented it was meeting requirements, and it was not, and a breach occurred that produced real injury to the DoD.

Companies should avoid these risks by ensuring they – and their subcontractors – address the requirements correctly and report accurately.

Dangerous Blind Spots

In addition to the risks all contractors face preparing for CMMC and correctly interpreting, implementing, and maintaining their own compliance, there are "blind spot" risks for prime contractors involving their supply chains. These blind spots create potential danger for contractors that fail to address supply chain cyber risk management. Blind spots include not realizing that many suppliers handling CUI might not be able to achieve CMMC Level 2 certification on their own.

When prime contractor executives have committed the resources needed to prepare properly for CMMC, it can be a damaging blow to lose contract opportunities because critical suppliers fail to also address CMMC requirements and are found to be noncompliant.

Primes may also find additional scrutiny on the horizon from the DCMA Defense Industrial Base Cybersecurity Assessment Center (DIBCAC), as it continues to evaluate risk across the DoD supply chain. According to the DIBCAC, "DCMA places an emphasis on prevention of defects in deliverables by ensuring that contractors monitor and control their supply chain by verifying that contractually required quality management systems are in place and followed. While cybersecurity has different terminology and technologies, it shares a common governance structure with most other business systems employed by a contractor. To this end, DCMA will begin inspecting how prime contractors ensure that their supply chain remains compliant with DFARS 252.204-7012 and taking appropriate measures when a contractor does not control their supply chain."

With the increasing emphasis on cyber compliance across the DIB, it's critical for prime contractors to develop adequate situational awareness of their suppliers' compliance status. What programs should be put in place to track and assess supplier compliance? Which suppliers are more likely or less likely to obtain certification at the required level? Which suppliers will be easiest or hardest to replace?

Keen situational awareness and effective supply chain cyber risk management dramatically improve a prime's chances of winning new business and being able to deliver on new contracts that require fully compliant bidding teams. Primes should be prepared to lose some suppliers to noncompliance. Plans should be in place now for how they will handle attrition and bring in compliant replacements.

Another hurdle primes face is

educating suppliers to understand the effort required to obtain CMMC Level 2 certification. Preparing for a third-party CMMC assessment requires significant gathering of evidence over weeks or even months. NIST SP 800-171A and the CMMC Level 2 Assessment Guide are documents that both provide a list of the 320 assessment objectives associated with the 110 security requirements established by NIST SP 800-171. An assessor will review the 320 separate assessment objectives (minus any that are nonapplicable) to validate that each requirement or practice has been met.

In order to pass a third-party assessment, a CUI-handling contractor or subcontractor will have to present evidence for every relevant assessment objective pertaining to each requirement. This is why it's so critical to refer to NIST SP 800-171A assessment guidance[18] when developing plans for implementing security requirements. Suppliers must ensure they can provide an evidentiary artifact for every assessment objective for the assessor to review to confirm that each requirement has been met.

It is easy to miss key assessment objectives. Companies often struggle to generate adequate documentation.

For example, the SSP requirement[19] (NIST SP 800-171 item 3.12.4) includes eight separate assessment objectives that are specified in NIST 800-171A. If even one is not met, the SSP will be found nonconforming. This means the company's basic assessment score posted to SPRS will be invalid until any necessary corrections are made. The problem is compounded for prime contractors that want to ensure the accuracy of their own and their subcontractors' scores and reports in SPRS.

Extensive evaluation of small- to medium-sized companies by the DCMA DIBCAC[20] shows that many, if not most, do not have NIST SP 800-171-conforming SSPs.

An SSP that is missing key elements will not satisfy the SSP requirement. One common omission is simply stating "met" or "not met" for each requirement instead of providing a description of how each requirement is implemented. In a strictly "pass/fail" evaluation based on meeting all assessment objectives, a nonconforming SSP counts the same as no SSP. Technically, this could invalidate the SPRS report, potentially rendering a contractor or subcontractor ineligible for a contract award.

Failing to satisfy the SSP requirement also could leave a company exposed to FCA liability for mischaracterizing its compliance status.

CMMC Level 2 assessments start with the SSP review. Clearly, it's in each contractor's best interest to gather evidence and make course corrections where needed to ensure its SSP(s) stand up to assessors' scrutiny.

Limit CMMC Impact

To minimize potential organizational impacts, it's important to connect key stakeholders to meet regularly and oversee the compliance effort. CUI compliance is not just an IT issue. All the players affected should be involved and know their roles and responsibilities. Coordinate among program and contract managers, procurement, security, legal counsel, and especially executives who might not realize the potential impact all of this may have on their businesses.

Another best practice is to start with a CUI flow analysis. Confirm what CUI you're handling and who you're sharing it with. You may be able to limit the impact of CMMC requirements by constraining your CUI-handling security boundary to an "enclave." This is a segmented, separate computing environment for storing and processing CUI.

Establishing a completely separate enclave environment and strictly limiting all CUI handling to the enclave can eliminate the footprint of CUI on the rest of your company's network. This can reduce the scope of your CUI handling to a smaller system and reduce the cost and complexity of compliance.

Remember that even if your company successfully addresses all of these requirements, you will still need to ensure that any CUI-handling subcontractors in lower tiers do the same. Primes often fail to plan adequately for this. Companies commonly task an IT manager with ensuring compliance for their own organization. Keep in mind that IT leaders aren't likely to have monitoring subcontractors' compliance top of mind. They may not be aware of the contractual obligations and liabilities placed on primes that require them to flow down the clauses and ensure subcontractor compliance.

Brief senior executives on CMMC and CUI. All CMMC Level 1, and in some cases Level 2, attestations must be made by senior officials with binding signature authority.

It may not be easy, but with effort and focus on the assessment objectives, it's definitely possible to meet all of the requirements and succeed in cyber compliance. CM

Larry Lieberman is a Cyber Evangelist at eResilience, a division of Referentia Systems, where he is involved in communications, business development, and outreach/education. Lieberman has developed and co-produced dozens of cybersecurity compliance webinars and training events attended by thousands of large and small contractors throughout the defense industrial base. Contact him at larry@eresilience.com.

> CUI compliance is not just an IT issue. . . . Coordinate among program and contract managers, procurement, security, legal counsel, and especially executives.

ENDNOTES

1 Controlled Unclassified Information (CUI), requires safeguarding or dissemination controls but is not classified. In DFARS clause 252.204-7012, CUI with military or space applications is referred to as "Covered Defense Information" (CDI). Further details on CUI are available at the National Archives website at https://www.archives.gov/cui/about. The DoD also provides more details on CUI at https://www.dodcui.mil/

2 The Cybersecurity Maturity Model Certification (CMMC) program is intended to enforce the protection of controlled unclassified information throughout the Defense Industrial Base (DIB). CMMC version 1.0 was published as an interim rule in 2020, and in 2021 the DoD announced an updated version 2.0 in response to public comments. Final rulemaking is currently in progress and expected to be completed by late 2024. Once rulemaking is completed the CMMC requirements can begin appearing in contracts through DFARS 252.204-7021.

3 CMMC Version 2.0 includes three levels. Level 1 is equivalent to the 15 basic safeguarding requirements for Federal Contract Information (FCI) currently in place under FAR 52.204-21. Level 2 is equivalent to the 110 safeguarding requirements for Controlled Unclassified Information (CUI) described by NIST SP 800-171 and currently required by DFARS 252.204-7012. Level 3 is reserved for highly sensitive contracts that will require implementation of all of NIST SP 800-171 as well as some additional enhanced requirements described in NIST SP 800-172. While CMMC Level 2 does not add new requirements beyond what CUI-handling contractors already are supposed to be doing under DFARS 252.204-7012, most contractors have not fully implemented those requirements, and CMMC adds a 3rd party certification process for Levels 2 and 3, to ensure that DIB contractors are meeting all of the CUI safeguarding obligations established by DFARS. Level 1 of CMMC 2.0 will require a self-attestation, asserted by a Senior Company Official with binding signature authority. In most cases Level 2 will require a third-party certification by a C3PAO (CMMC Third-Party Assessment Organization). Level 3 will require all of Level 2 plus additional assessment of enhanced requirements, to be performed by the DIBCAC. The certification process for Levels 2 and 3 means contractors must prepare substantial evidence and documentation to present to assessors, rather than just implement the specified security practices.

4 https://www.acquisition.gov/dfars/252.204-7021-cybersecuritymaturity-model-certification-requirements.

5 NIST SP 800-171 *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* lists 110 cybersecurity requirements that DoD contractors or subcontractors who have DFARS clause 252.204-7012 in their contracts are required to implement if they are handling CUI. Revision 2 is the most current version at the time of this writing. Revision 3 has been published in draft form but has not yet been finalized. Link to the current version at https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

6 https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-

cyber-incident-reporting.

7 A system security plan (SSP) is a formal document that provides an overview of the security requirements for an information system and describes the security controls implemented to meet those requirements.

8 An SSP template is available from NIST in the "Supplemental Material" section of the "Documentation" list at https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

9 A Plan of Action and Milestones (POAM) is a document for a system that "identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones." A POAM template is available from NIST in the "Supplemental Material" section of the "Documentation" list at https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

10 DoD ECA Medium Assurance certificates are issued under the Department of Defense External Certificate Authority (ECA) program and are used to conduct business with the DoD and other government entities. CUI-handling organizations must have a Medium Assurance Certificate in place in order report any cyber incident to the DoD Cyber Crime Center (DC3). In accordance with DFARS 252.204-7012, cyber incidents must be reported within 72 hours from discovery, so it is important to already have the Medium Assurance Certificate in place before storing or processing any CUI. For more information, visit https://dibnet.dod.mil/portal/intranet/ and select "Obtain a Medium Assurance Certificate"

11 The DoD has established the External Certification Authority (ECA) program to support the issuance of DoD-approved certificates to industry partners and other external entities and organizations. For more information visit https://public.cyber.mil/eca/

12 Under FAR 52.204-21 *Basic Safeguarding of Covered Contractor Information Systems*, a Covered Contractor Information System (CCIS) is any information system that stores or processes Federal Contract Information (FCI). FCI includes information not intended for public release, provided by or generated for the government under a contract (see https://www.acquisition.gov/far/52.204-21). CUI is a subset of FCI. Under DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting, "Covered contractor information system" means an unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information (CDI). CDI is CUI with military or space applications. When CUI is present on a company network, the boundary of that network and any interconnected systems is a CCIS. If all CUI storage and processing is strictly limited to a separate, segregated enclave environment, then the enclave is the CCIS that would be subject to the requirements of DFARS cybersecurity clauses. A system that does not store or process CUI but does store or process FCI is subject to the FAR 52.204-21 clause.

13 https://dibnet.dod.mil

14 https://www.acquisition.gov/dfars/252.204-7019-notice-nistsp-800-171-dod-assessment-requirements.

15 https://www.acquisition.gov/dfars/252.204-7020-nist-sp-800-171dod-assessment-requirements.

16 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

17 The DoD NIST SP 800-171 Assessment Methodology enables a strategic assessment of a contractor's implementation of NIST SP 800-171. The methodology provides a formula for scoring contractor compliance with NIST SP 800-171 security requirements on a weighted basis, and defines multiple levels of assessment that can be conducted by the government to assess contractor compliance. The methodology also can be used by prime contractors to assess the compliance status of their subcontractors. A copy of the Assessment Methodology can be found at 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

18 The CMMC 2.0 model reduced the number of CMMC certification levels from five to three. Level 1 is required for handling Federal Contract Information (FCI) and is self-attested by a senior company official. Level 2 is required for handling CUI and will typically require a third-party assessment. Level 3 is only for highly sensitive contracts that need enhanced security requirements. In addition to reducing the number of certification levels from five to three, CMMC 2.0 also removed some of the requirements, or "practices" initially stipulated for CUI handling, and made Level 2 consistent with and limited to the requirements of NIST SP 800-171.

19 NIST SP 800-171A is the Assessment Guide published by NIST to provide federal and nonfederal organizations with assessment procedures and a methodology that can be employed to conduct assessment of the CUI security requirements in NIST SP 800-171 *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171A.pdf

20 According to NIST SP 800-171 (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf), item 3.12.4 on page 35, CUI-handling contractors must "develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems". The NIST SP 800-171A (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171A.pdf) Assessment Guide, section 3.12.4 on page 52, specifies eight separate assessment objectives that an assessor would need to validate based on available evidence, to confirm that the contractor has satisfactorily implemented the NIST SP 800-171 item 3.12.4 requirement.

21 The Defense Contract Management Agency (DCMA)'s Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) is leading the DoD's contractor cybersecurity risk mitigation efforts. DIBCAC developed the DoD NIST SP 800-171 Assessment Methodology and assesses contractor compliance with DFARS cybersecurity requirements on an ongoing basis. For more information visit https://www.dcma.mil/DIBCAC/