# How Contractors Can Prep For DOD Cybersecurity Rule

By **Beth Waller and Patrick Austin** (July 25, 2024)

Beth Waller

Patrick Austin

The proverbial clock is ticking for defense contractors and subcontractors to strengthen their compliance posture in preparation for the rollout of the highly anticipated Cybersecurity Maturity Model Certification program, or CMMC 2.0.[1]

The U.S. Department of Defense issued a proposed rule to implement CMMC 2.0, which included a timeline for implementation to occur at some point in early 2025. Considering we're more than halfway through 2024, the window of time to try and get CMMC compliant may be starting to close.

**Overview of CMMC 2.0**

The framework for CMMC 2.0 is made up of three "levels" of security controls that defense contractors and subcontractors will be expected to meet based on the sensitivity of information a contractor accesses during the contract.

In preparation for the arrival of CMMC 2.0, defense contractors and subcontractors need to be proactive and start familiarizing themselves with the specific requirements associated with each CMMC level. Below, we detail what will be expected of a defense contractor at each level of CMMC 2.0.

For context, the CMMC program is structured like a pyramid, with the strictest standards expected to apply only to a small subset of defense contractors and subcontractors.[2]

Let's dive deeper into each CMMC level.

**CMMC Level 1**

CMMC Level 1 is expected to apply to all defense contractors and subcontractors that obtain defense contracts involving federal contract information. There is an exception for DOD contracts exclusively for commercially available off-the-shelf items.

FCI is considered information not intended for public release provided by or generated for the federal government under a contract to develop or deliver a product or service to the government.[3] Examples of FCI include:

- Contracts;
- Statements of work;
- Technical drawings; and
- Communications between the government and contractor or subcontractor.

Considering its broad definition, defense contractors should be prepared to encounter FCI in most DOD contracts. As a result, they need to take steps to comply with CMMC Level 1.

To comply with CMMC Level 1, defense contractors are obligated to implement 15 security requirements set forth in Federal Acquisition Regulation Clause 52.204-21(b)(1), "Basic Safeguarding of Covered Contractor Information Systems," for contractor information systems that process, store or transmit FCI.[4]

The FAR requirements include, but are not limited to, the following:

- Protocols to restrict system access;
- User authentication and system sanitization procedures; and
- Protections to combat malicious code.

The FAR security requirements have been in place since 2016, which is why there is a general expectation that companies performing contracts for the federal government will have a compliance framework in place to satisfy the 15 security requirements.

In addition to the FAR security requirements, defense contractors will be required to perform an annual self-assessment of each information system that stores, processes or transmits FCI, which must be submitted to the DOD's supplier performance risk system.[5]

Along with proper submission of assessment results, a senior official from the company must affirm compliance with the CMMC Level 1 security requirements on an annual basis.

The importance of complying with the FAR security requirements cannot be understated. According to the proposed rule, defense contractors that fail to meet even one security requirement will be deemed noncompliant with CMMC Level 1 and, therefore, ineligible to bid on contracts requiring CMMC Level 1 compliance.

And it only gets tougher from here.

**CMMC Level 2**

CMMC Level 2 applies to all defense contractors and subcontractors that obtain DOD contracts involving controlled unclassified information. For context, CUI is information the government creates or possesses, or that an entity creates or possesses for or on behalf of the government, that a law, regulation, or government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.[6]

Since CMMC Level 2 applies to contracts with CUI, it likely means that contractors will need to be prepared to confirm they meet the security requirements set forth in Defense Federal Acquisition Regulation Supplement 252.204-7012,[7], which align with standards set forth in the National Institute of Standards and Technology Special Publication 800-171 Revision 2.[8]

Defense contractors and subcontractors performing a contract with CMMC Level 2 controls must complete either a self-assessment or a Level 2 certification assessment to ensure implementation of all Level 2 security requirements.

The other option is to engage with a third party — known as a third-party assessment organization, or C3PAO — to conduct a certification assessment. The advantage of a C3PAO assessment is that the results remain valid for three years (as opposed to having to continually self-certify multiple times per year).

**CMMC Level 3**

CMMC Level 3 is intended for defense contractors and subcontractors with access to high-priority CUI. To comply with CMMC Level 3, contractors must secure a CMMC Level 2 certification, specifically a C3PAO assessment, meaning a Level 2 self-assessment is insufficient.

In addition, contractors must implement the 24 security requirements of NIST SP 800-172,[9] along with the requirements detailed in Defense Federal Acquisition Regulation Supplement 252.204-7012. Defense contractors must also pass a CMMC Level 3 Certification assessment to evaluate the applicable contractor information systems to determine compliance with NIST SP 800-172 controls.

The DOD does not expect a significant number of contractors to pursue or meet the standards set forth for CMMC Level 3. For example, in the CMMC proposed rule, the DOD estimates that less than 1% of defense contractors are expected to obtain a CMMC Level 3 certification once CMMC 2.0 is fully effective.

**Preparing for CMMC 2.0**

Defense contractors and contractors must closely examine the contractual requirements that will be imposed on them once CMMC 2.0 is fully implemented, and take proactive steps to strengthen their compliance posture.

Below are some general tips to help prepare your company for CMMC 2.0.

***Conduct a CMMC compliance audit.***

Defense contractors should consider conducting an audit to assess where they meet relevant CMMC security standards. For example, an audit can help identify where federal information — e.g., FCI and/or CUI — is maintained in the organization's internal databases and systems.

If the organization manages CUI, then the audit could indicate any potential gaps in meeting CMMC Level 2 certification standards. In addition, defense contractors should consider engaging outside counsel to perform such a compliance audit/assessment. Utilizing outside counsel could potentially allow the organization to protect the audit results under the attorney-client privilege.

***Do not rely on plans of action and milestones.***

Defense contractors handling CUI must be prepared to rely less on plans of action and milestones, or POA&Ms, to help bridge the gap when specific security requirements are unmet.

For context, a POA&M is a document identifying tasks that need to be completed to comply with specific security controls in a contractor's system security plan. POA&Ms set forth the resources required to achieve those tasks and associated milestones.

However, CMMC 2.0 will impose restrictions on the use of POA&Ms to achieve CMMC certification. For example, POA&Ms for defense contractors subject to CMMC Level 1 will not be permitted. Contractors subject to CMMC Level 2 can use POA&Ms, but only for specific controls.

Furthermore, if a contractor submits a POA&M, they will only be afforded 180 days to achieve full compliance. Once the 180-day deadline passes, the contractor will need to return to the drawing board and restart the CMMC certification process.

***Ensure accurate affirmations.***

For senior officials of contractors and subcontractors, it is extremely important to ensure CMMC affirmations are accurate.

Misrepresentations associated with such affirmations could allow the federal government to take adverse action against your company, including possible contract termination, issuance of a negative past performance rating, and/or pursuing monetary damages through a claim submitted under the False Claims Act.

As a result, CMMC affirmations need to be taken seriously and made in a manner that is consistent with the contractor's overall CMMC compliance program.

**Looking Ahead**

CMMC 2.0 is expected to be implemented by early 2025, though the DOD stated a phased implementation is expected. For example, CMMC requirements will not immediately be included in all defense contract solicitations. Rather, CMMC requirements are expected to become standard in contract solicitations issued on or after Oct. 1, 2026.

Now is the time for defense contractors and subcontractors to analyze their existing security compliance posture and determine whether there are any significant gaps that would make complying with CMMC 2.0 challenging.

---

*Beth Burgin Waller is a principal and chair of the cybersecurity and data privacy practice at Woods Rogers Vandeventer Black PLC.*

*Patrick J. Austin is of counsel at the firm.*



[1] Cybersecurity Maturity Model Certification (CMMC) Program, 88 Fed. Reg. 89,058 (Dec. 26, 2023).https://www.govinfo.gov/content/pkg/FR-2023-12-26/pdf/2023-27280.pdf.

[2] Id. at 89,088.

[3] 48 C.F.R. § 4.1901.

[4] Other examples of the 15 FAR security requirements include, but are not limited to: identifying, reporting, and correcting information and information system flaws in a timely manner; monitoring, controlling, and protecting organizational communications at the external boundaries and key internal boundaries of the information systems; and controlling information posted or processed on publicly accessible information systems.

See https://www.acquisition.gov/far/52.204-21.

[5] https://www.sprs.csd.disa.mil/.

[6] See 32 C.F.R. § 2002.4(h). There are 20 categories of CUI, which includes information related to technical information with military or space application, export-controlled information, intelligence, procurements, and so forth.

[7] See https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting.

[8] NIST recently rolled out a Rev. 3 of SP 800-171, but the CMMC proposed rule specifically references SP 800-171 Rev. 2.
See https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf.

[9] NIST's Enhanced Security Requirements for Protecting Controlled Unclassified Information. See https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-172.pdf.