Deloitte.

Cybersecurity Maturity Model Certification (CMMC)

The release of the Cybersecurity Maturity Model Certification (CMMC) brings changes to the Department of Defense (DoD) Supply Chain for both contractors and subcontractors. As CMMC will be a requirement to do business with DoD, it is critical for DoD contractors to understand what CMMC means for their organizations and begin preparing now.

The CMMC model was designed with a focus on protecting Federal Contract Information (FCI) and Controlled Unclassified Information (CUI).

Encompasses various requirement families (14) and practices aligned with National Institute of Standards and Technology (NIST) standards (NIST Special Publication (SP) 800-171 & 172).

Consists of three levels of maturity. As the levels progress, so do the number of requirements (e.g., Level 1 consists of 15 requirements, while Level 3 consists of 134 requirements making it the most secure).

Once CMMC is codified, certain DoD contractors will be required to undergo an assessment by a CMMC Third-Party Assessment Organization (C3PAO) or the government and obtain a CMMC. Other DoD contractors will be required to self-assess and self-attest annually.

Applicable to DoD prime contractors and subcontractors.

Examples of Controlled Unclassified Information (CUI)

- Military personnel records
- Health Information (e.g., patient data and records)
- International Traffic in Arms Regulations (ITAR) data covered on the US Munitions List
- North Atlantic Treaty Organization (NATO) restricted data
- Controlled Technical Information (e.g., engineering data and drawings)
- DoD Critical Infrastructure Security Information

Connect with us

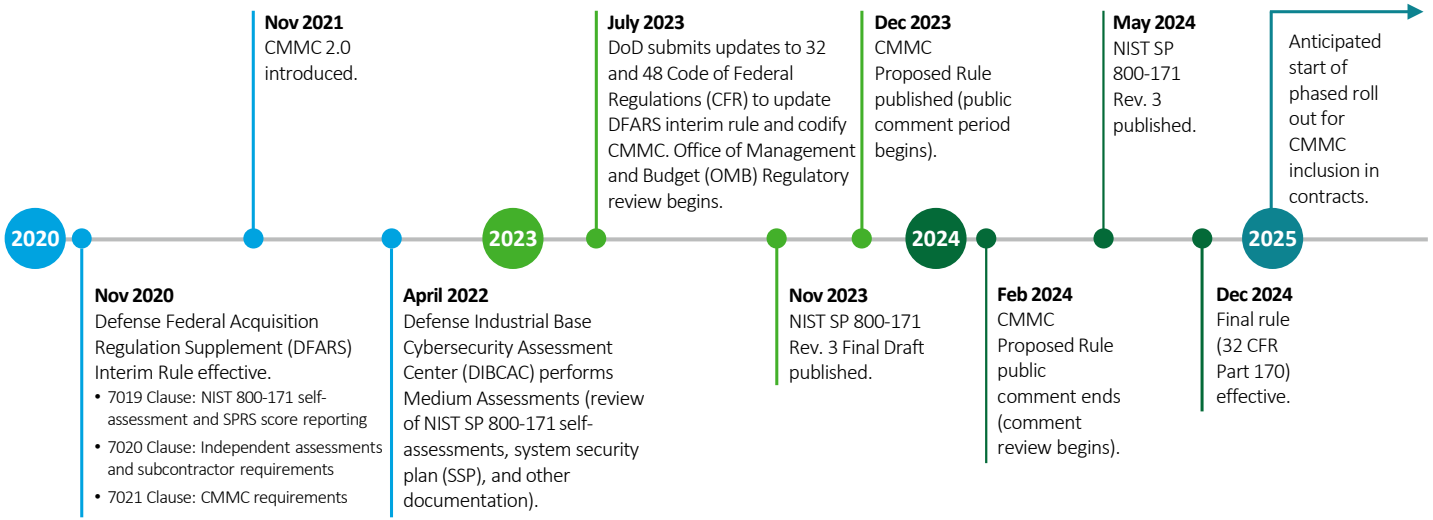
Alan Faver
Partner
Deloitte & Touche LLP
afaver@deloitte.com

Charan Ahluwalia
Principal
Deloitte & Touche LLP
cahluwalia@deloitte.com

Keith Thompson
Managing Director
Deloitte & Touche LLP
keithompson@deloitte.com

Mika Alexoudis
Senior Manager
Deloitte & Touche LLP
malexoudis@deloitte.com

CMMC Timeline



Why now? While there may be some time until CMMC is codified, it is critical to act now because (1) Readiness can be time consuming and require a high level of commitment; and (2) Relevant requirements (e.g., DFARS) related to the protection of FCI/CUI are already in place and applicable to DoD contractors.

5 Updates You Should Know		5 Actions You Should Take
If you are serving the DoD in any capacity (prime or sub-contractor), CUI likely exists within your environment	1	Determine your CUI footprint by collaborating with relevant stakeholders across your organization (e.g., IT, Procurement, Contracting, Legal) to understand how your organization engages with federal customers – including the product and/or services provided as well as possible CUI-relevant data elements.
A detailed view of your CUI footprint is required to (1) categorize your assets and (2) define your CMMC scope	2	Perform CUI Discovery, evaluate results, and categorize assets using the CMMC assessment guide (e.g., CUI Asset, Security Protection Asset (SPA), Contractor Risk Managed Asset (CRMA)).
You are required to provide a Supplier Performance Risk System (SPRS) score related to NIST SP 800-171.	3	Perform an assessment against the applicable requirements (e.g., 110 NIST SP 800-171 controls) to identify compliance gaps and improvement opportunities.
NIST SP 800-171 and CMMC readiness and remediation activities will potentially need to be completed before undergoing a C3PAO assessment in 2025	4	Based on the assessment results, create a remediation roadmap that lays out actions needed to properly address gaps and preparation for the CMMC assessment.
NIST SP 800-171 alignment is required for your suppliers and CMMC will potentially be required for your suppliers in 2025.	5	Review the contractual flow down requirements that are applicable to your suppliers and develop supply chain risk management protocols to address cybersecurity risk within your supply chain.