CMMC and CUI

09.2025

32 CFR Part 170, NIST SP 800-171, FAR DFARS

Issue

The Cybersecurity Maturity Model Certification (**CMMC**) Program, effective 16.12.2024, mandates the **U.S. Department of Defense'** (**DoD**) **cybersecurity compliance for the Defense Industrial Base** (**DIB**). It rolls out in 4 phases (2024–2027) with 5 maturity levels, starting with self-assessment (2024) and **culminating in full certification by 2027** to protect DoD controlled information.

Objective



The higher a DIB organization is **CMMC certified**, the more **U.S. Government contracts** it will be eligible to bid on. DoD contractors and subcontractors handling Controlled Unclassified Information (**CUI**) must achieve at least CMMC Level 3 certification by December 2026, and **properly handle such sensitive information** where existing.

Key Takeaways

1. Definitions
   - **Key regulatory definitions** such as, but not limited to, Covered Contractors, Covered Defense Information, Federal Contract Information (**FCI**), Controlled Unclassified Information (**CUI**), Nonfederal IT Systems and Organizations, Commercially Available Off-The-Shelf items, Micro-Purchase Thresholds
2. Security Requirements
   - **Basic Security Requirements** as laid down by Federal Acquisition Regulations (**FAR**) clause **52.204-21** to protect information systems against cyber-incidents
   - **Safeguard of Covered Defense Information** as laid down by Federal Defense Federal Acquisition Regulation Supplement (**DFARS**) clause **252.204-7012** : Derived Security Requirements
3. Information Systems
   - **Identify and differentiate** internal information systems (or components) from external information systems (or components)
   - Focus on **internal information systems** for the adoption and implementation of Basic Security Requirements and Derived Security Requirements. *NB: exemptions exist.*
   - Understand **dissemination risk** of relevant FCI to external information systems by exerting **adequate due diligence** thereof
4. Federal Contract Information
   - **Identify FCI residing into internal information systems** (BOTH classified as per Executive Order n°13526 AND unclassified – **CUI**)
   - **Mark** them according to DoD instructions
   - **Identify and mark FCI released to third parties**, if any.

Target Audience

- Applies to **both domestic and foreign contractors**
- Applies to all (**defense-related**) information that qualifies as CUI
- Applies at **all contractual levels**, from prime contractors with U.S. DoD to sub-tiers contactors subject to prime's FAR DFARS clauses flowdown

Non-Compliant ?

No more access to DOD solicitations (contracts) **depending on CMMC-certificate level achieved** (whether as prime of subcontractor). Level 3 will be the minimum.

Key Dates

- 12/2026: CMMC level 3 certification deadline and **specific award limitation**
- 12/2027: **no more access to DoD contracts** if not CMMC level 3-certified

To Do

- **Identify** whether you are a Covered Contractor and are aware of the CMMC Program
- **Understand** whether you **handle FCI and CUI**, now or in the future and whether you are (or will be) subject to control obligations therefrom
- **Map your internal IT systems** to determine their CMMC readiness as well as your third parties'
- **Raise awareness** and **update** your IT systems, if need be, as well as your policies and processes **for compliant CUI handling**

Support

Non-exhaustive examples

- **D-Wise Strategy**: review DoD contract information and perform CUI marking gap analysis (CUI Audit)
- **D-Wise Consult**: what is FCI/CUI minimization ?
- **D-Wise Implementation**: decision tree to determine related CUI markings, associated distribution statement (export control), retention and destruction policies
- **D-Wise Academy**: on-site training on CUI recognition, creation and proper handling
- **D-Wise News**: monitoring of any regulatory update