Holland & Hart

Nicole Vele

Of Counsel
202.289.3496
Washington, DC
navele@hollandhart.com

A Defense Contractor's Guide to CMMC, DFARS, and FAR Requirements

Insight — June 3, 2025

CyberNINES

This article, co-authored by CyberNINES CEO Scott Singer, originally appeared in CyberNINES on June 2, 2025 and is reprinted with permission. All rights reserved.

Cyber-attacks against America's defense industrial base are becoming more sophisticated and more frequent. To reduce the risk of sensitive national security information landing in the hands of bad actors, the Department of Defense requires all defense contractors and subcontractors to protect their networks with specified network security requirements.[1] So, whether your company stores Controlled Unclassified Information (CUI) and Federal Contract Information (FCI) or merely transmits it via your company's unclassified information system, you are required to comply with the Department of Defense's (DoD) Cybersecurity Maturity Model Certification (CMMC) Program.[2]

Finalized on December 16, 2024, and anticipated to be written into contracts starting in September 2025, the DoD's CMMC Program has three certification levels: **(1)** CMMC Level 1 (Self-Assessment); CMMC Level 2 (Self-Assessment) & **(2)** CMMC Level 2 (Certification); and **(3)** CMMC Level 3 (Certification). The CMMC Level required of your information system is based on your company's contracts. Upon release this fall of the contract clause associated with CMMC, companies will initially be required to self-attest to either CMMC Level 1 or Level 2. DoD will have the option to require CMMC Level 2 certification in the first year, but after that it will be phased over time into all contracts.

- If your awards require you (or your subcontractor) to **process, store, or transmit only FCI** in your information system, the appropriate assessment requirement is CMMC Level 1 (Self-Assessment).[3]
- If your contract involves covered defense information (CDI) to include CUI, that will be processed, stored, or transmitted on your information system, then your system will need a CMMC Level 2 certification.[4]
- CMMC Level 3 assessments are required when your contract contains CUI associated with mission critical or unique technologies and programs that are processed, stored, or transmitted on your information system and DoD policy requires the

application of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-172.[5]

As important as these rules are, it's not always easy to navigate them. To ensure you are ready to meet CMMC's rigorous standards, this article will highlight the Federal Acquisition Regulations (FAR) and Defense Federal Acquisition Regulations Supplement (DFARS) clauses in your contracts that govern CMMC, provide some practical advice for understanding the basics of compliance under each clause, and discuss the risks associated with non-compliance.

Despite the complexities associated with effective cybersecurity, you will only find a handful of clauses in your federal contracts that discuss the safeguarding requirements and procedures for contractor-owned or -operated information systems. The first clause we will discuss is FAR 52.204-21. This clause became effective June 15, 2016, and it, along with FAR 4.19,[6] set the baseline safeguarding requirements for all contractor-owned or -operated information systems that process, store, or transmit FCI.[7]

FAR 52.204-21 Basic Safeguarding of Covered Contractor Information Systems

Per FAR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems, there are fifteen security controls *(figure 1)* that covered contractors and subcontractors must employ to safeguard their information systems if they want to work with the federal government. These requirements were meant to include the most basic safeguards that a prudent businessperson would exercise even if a federal regulation did not exist.

	FAR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems Securit
1	Limit information system access to authorized users, processe authorized users, or devices (including other information syst
2	Limit information system access to the types of transactions a authorized users are permitted to execute
3	Verify and control/limit connections to and use of external inf
4	Control information posted or processed on publicly accessibl
5	Identify information system users, processes acting on behalf
6	Authenticate (or verify) the identities of those users, processe prerequisite to allowing access to organizational information s
7	Sanitize or destroy information system media containing Fede Information before disposal or release for reuse
8	Limit physical access to organizational information systems, e respective operating environments to authorized individuals
9	Escort visitors and monitor visitor activity, maintain audit logs control and manage physical access devices
10	Monitor, control, and protect organizational communications (*i.e.*, information transmitted or received by organizational inf external boundaries and key internal boundaries of the inform
11	Implement subnetworks for publicly accessible system compo or logically separated from internal networks
12	Identify, report, and correct information and information syst manner
13	Provide protection from malicious code at appropriate locatio organizational information systems
14	Update malicious code protection mechanisms when new rele
15	Perform periodic scans of the information system and real-tim external sources as files are downloaded, opened, or executed

Figure 1 - FAR 52.204-21 Security Controls

DFARS 252.204-7012: Safeguarding Covered Defense Information and Cyber Incident Reporting

Holland & Hart