Non-Compliance with CMMC Could Put Your DoD Contracts at Risk

August 27, 2025
By Edward Tolchin

This past month, the Department of Defense sent the final rule for the new Cybersecurity Maturity Model Certification (CMMC) program under the Federal Acquisition Regulation to the Office of Information and Regulatory Affairs for review. This action precedes the inclusion of the new rule in Department of Defense contracts beginning this autumn. So, it is time to get into compliance for all who have been delaying the inevitable.

Below is a quick review of these requirements.

Background

CMMC is designed to bolster the cybersecurity posture of the DoD's supply chain by validating that DoD contractors and subcontractors possess the necessary cybersecurity practices and processes to safeguard Federal Contract Information (FCI) and various kinds of Controlled Unclassified Information (CUI). CMMC introduces a tiered, certification-based approach, ranging from Level 1 (basic cybersecurity practices for FCI) to Level 2 (advanced practices for most CUI), and Level 3 (expert practices for sensitive CUI).

Why is This Important?

Contractors and subcontractors must attain the appropriate CMMC level aligned with the security requirements of their contracts to bid and work on DoD projects. In addition to the cybersecurity and reputational risks of non-compliance, if contractors and subcontractors fib or cut corners, they could face False Claims Act (FCA) liability, including draconian damage and penalty assessments. One disgruntled employee who decides to bring an FCA complaint can cost a company significant pain.

Contracts Covered by CMMC

The CMMC requirement applies to DoD acquisitions that involve the handling of FCI and CUI.

- Major Contract Programs: Contracts for the procurement of defense systems, weapons, military equipment, and related services that require access to CUI or FCI will be directly impacted. This includes a broad spectrum of procurement categories across the DoD, from large-scale hardware contracts to software development and services.
- Subcontractors and Supply Chain: Importantly, the rule also extends to subcontractors at all tiers. This flow-down creates a ripple effect throughout the defense supply chain.

Contracts Not Subject to CMMC

While the rule is broad, it does not universally apply to all federal contracts.

- FAR Part 12 Commercial Item Contracts: Some commercial item contracts purchased under FAR Part 12 may be excluded unless the scope involves sensitive information or national security concerns.
- Contracts with No Access to CUI or FCI: Contracts that do not involve access to or handling of CUI/FCI will not be subject to CMMC requirements.
- Other Exceptions: The FAR Council has provisions for exemptions for technical or administrative reasons, but these are limited and require justification.

What is FCI

If you are a contractor or subcontractor that handles controlled information such as CUI, you likely have some sophistication regarding cybersecurity. But those with FCI may not be aware that they have protectible information, and most medium and larger-sized DoD contracts will have FCI.

- FCI refers to information that is not intended for public release but is provided by the federal government to a contractor or subcontractor for the purpose of fulfilling a federal contract. It includes data that is critical to the performance of government contracts.
- Examples include technical data (e.g., details about a supplier's hardware specifications), contract schedules and milestones (e.g., timelines for delivering military equipment), and financial or administrative information shared with contractors.
- Typical Contracts:
  - Smaller contracts
  - Basic supply chain activities

FCI Requires Level 1: Basic Cyber Hygiene

Key Requirements:

- Implementation of basic controls, including access only by authorized users, maintaining identification and authentication, and physical protection of information systems.
- Practices include routine login credentials, portable device protections, and basic awareness training.
- Annual self-assessment and annual affirmation of compliance with CMMC requirements.

What is CUI

- It's not classified information, but it is information that requires safeguarding pursuant to various laws, regulations, and government policy.
- Examples include information about physical security, system vulnerability, or operational issues.

CUI Requires Level 2 (Intermediate) or Level 3 (Expert) Processes

- Level 2: Intermediate Cyber Hygiene
  - Practices: 110 practices, aligned with NIST SP 800-171 security requirements.
  - Focus: Establishing more disciplined cybersecurity processes and practices suitable for organizations handling CUI.
  - Third-party assessments are required for certification at this level.

- Level 3: Expert Cyber Hygiene
  - Practices: Over 130 security controls, closely aligned with NIST SP 800-171, plus some additional practices.
  - Focus: A mature, enterprise-wide cybersecurity program.
  - This will apply only to a limited number of contractors with larger, more sensitive defense contracts that require higher levels of CUI protection.
  - Third-party assessment is required.