**Defense Contractors Take Notice: The Cybersecurity Requirements of the CMMC are Now Effective**

**Authors:** Matthew D. Dunn (mdunn@clm.com), Jonathan Trafimow (trafimow@clm.com), Kevin M. Simpson (simpson@clm.com).

Many defense contractors are already aware that the U.S. Department of Defense (DoD)[1] has implemented robust cybersecurity requirements for defense contractors that handle controlled unclassified information (CUI)[2] and federal contract information (FCI).[3] However, they may not be aware of those specific requirements and the risks of noncompliance. This short article provides a basic overview.

DoD's Cybersecurity Maturity Model Certification (CMMC) framework, which went into effect in November 2025, requires certification by a qualified third-party certification organization (C3PAO),[4] annual affirmations of compliance by the contractor (including certification of subcontractor compliance), and compliance with stringent technical requirements, all depending on the type of information the contractor must process under its DoD contract or subcontract. Previously, contractors were able to self-certify, but now they may be required to engage third parties to obtain certification. Full implementation will involve a phased rollout over three years.

The framework was established to protect the defense industrial base (DIB) from cybersecurity attacks. Certification and compliance under the CMMC framework are a condition for contract awards, extensions, and renewals. Contractors also face exposure to enforcement actions and other penalties for misrepresentations in connection with the program.

## I. THE CMMC PROGRAM

DoD announced the CMMC program in 2019 and issued an initial version in November 2020. The initial CMMC Program Rule came into effect in December 2024, establishing the technical requirements, certification levels, and assessment methodologies. The now-effective final rule does not replace any of the previously existing cybersecurity requirements. Instead, it supplements them in a formalized verification and certification framework.[5]

The CMMC program comprises three certification levels, each corresponding to the sensitivity of information handled with differing compliance

requirements. For each level, contractors must maintain a current CMMC status in the DoD's Supplier Performance Risk System (SPRS) and submit annual affirmations of continuous compliance. The CMMC Program Office or the specific military branch, program office, or DoD agency that is sponsoring and requesting a particular project (the "requiring activity") determines which CMMC level applies to a given requirement.

Contractors should also be aware that in January 2026, the General Services Administration (GSA)[6] issued new security assessment requirements for protecting CUI. Because the GSA is involved in other government contracts and its heightened standards are based on revisions to the same NIST SP 800-171 which the CMMC is based on in part,[7] it is likely that DoD may implement the new GSA standards into the CMMC and so compliance with the more stringent GSA standards might save on compliance costs down the line.

## II. CONTRACTOR ELIGIBILITY AND PRE-AWARD REQUIREMENTS

DFARS 252.204-7021 and 252.204-7025, the new federal defense contract clauses that are part of the final rule, explicitly provide that a contractor will not be eligible for an award if it does not have: (1) a current CMMC status entered in SPRS at the required level; and (2) a current affirmation of continuous compliance in SPRS for each contractor information system that will process, store, or transmit FCI or CUI. DoD also requires that contractors have the required certification at the time of award, rather than at proposal submission or post-award. Contracting officers are barred from awarding, extending, or exercising options on contracts unless SPRS reflects the contractor's current CMMC status at the appropriate level.

In addition, prime contractors will now be expected to verify directly with subcontractors that the subcontractors are complying with CMMC requirements. This may require the prime contractor to impose contractual requirements on subcontractors, including certifications, representations, or audit rights in subcontract agreements.

## III. ENFORCEMENT AND LEGAL RISK

The intersection of CMMC and the False Claims Act (FCA), 31 U.S.C. § 3729, represents arguably the most significant legal risk for defense contractors. The DOJ, under its Civil Cyber-Fraud Initiative (CCFI) launched in October

2021, has aggressively pursued contractors who misrepresent cybersecurity compliance.

In fiscal year 2025, DOJ recovered more than $52 million across nine cybersecurity-related FCA settlements, with total recoveries more than tripling in each of the past two years. Notable 2025 settlements under the interim rule for falsely certifying compliance or failing to implement requirements include:

(1) Health Net Federal Services (HNFS) / Centene Corporation (February 2025): $11.25 million settlement where the government alleged that HNFS failed to meet certain cybersecurity controls and falsely certified compliance with them in annual reports. HNFS also allegedly ignored reports from third-party security auditors and their own internal audit department of cybersecurity risks on HNFS' networks and systems. Centene, as HNFS' corporate parent following its acquisition of all issued and outstanding shares of HNFS, assumed the liabilities.[8]

(2) MORSECORP, Inc. (March 2025): $4.6 million settlement where the government alleged that MORSE failed to implement certain technical requirements of the CMMC program. MORSE also allegedly used a third-party company to host emails without requiring and ensuring that the third party met security requirements.[9]

(3) Raytheon / RTX Corporation / Nightwing Group LLC / Nightwing Intelligence Solutions, LLC (May 2025): $8.4 million settlement where the government, under whistleblower provisions, alleged that Raytheon and related entities failed to ensure that an internal system, used for twenty-nine DoD contracts and subcontracts, complied with CMMC cybersecurity requirements.[10]

As demonstrated with current CMMC enforcement, contractors failing to take steps to implement the technical requirements of the program wherever sensitive information could be processed in completing DoD contracts or subcontracts, relying on assessments conducted by improperly accredited assessors or C3PAOs, ignoring reports of internal or third party cyber-compliance auditors, or neglecting due diligence in corporate transactions where these compliance issues loom, could trigger retroactive FCA exposure for the period when the contractor represented compliance based on an invalid assessment. In an M&A context, purchasers could also inherit

exposure for periods when the acquired company failed to comply or falsely represented compliance.

Beyond FCA liability, noncompliance may result in invalidated certifications affecting contract eligibility, contract termination, negative past performance ratings, suspension, and debarment proceedings.

## IV. RECOMMENDATIONS

### A. For Companies Preparing for Certification

1. Assess the CMMC level that likely will apply, conduct an immediate gap assessment against the applicable standards, and develop a remediation roadmap.
2. Engage legal counsel to conduct a cybersecurity readiness review. Take steps to identify and protect sensitive gap analyses while maintaining attorney-client privilege. Identify and remediate deficiencies before they become enforcement liabilities.
3. Ensure SPRS entries are accurate and current.
4. If necessary to comply with the contractor's CMMC level, identify and hire a qualified C3PAO. Generally, do this early, as assessment capacity may be constrained during the initial rollout period.
5. Designate and train an affirming official who understands the legal significance of annual affirmations and the FCA implications of inaccurate certifications.

### B. For Prime Contractors Managing Subcontractor Compliance

1. Revise standard subcontract terms to incorporate flow-down language, including representations and warranties regarding CMMC status, SPRS affirmations, and audit rights.
2. Establish a subcontractor cybersecurity verification program that includes pre-award confirmation of CMMC status, periodic compliance certifications, and contractual remedies for noncompliance.
3. Consider compartmentalizing access to CUI to limit the scope of information that flows down to subcontractors, thereby potentially reducing the CMMC level required at lower tiers.
4. Monitor subcontractor conditional certifications and confirm timely POA&M closeout to prevent lapses that could affect prime contractor performance.

### C. General Risk Mitigation Strategies

1. Treat CMMC compliance as a legal and enterprise risk management priority, not solely an IT initiative. Involve legal, compliance, and executive leadership.
2. Implement internal controls for continuous compliance monitoring, including automated tracking of SPRS submissions, affirmation deadlines, and certification expiration dates.
3. Establish a robust internal whistleblower response program. The majority of FCA cybersecurity settlements have originated from qui tam complaints filed by former employees.
4. Consider voluntary self-disclosure of compliance gaps. DOJ has recognized cooperation credit in multiple settlements, and timely self-disclosure may significantly reduce penalties.
5. Build cybersecurity compliance into M&A due diligence. DOJ's 2025 enforcement activity included holding an acquirer liable for an acquiree's cybersecurity violations, making pre-acquisition CMMC compliance assessment essential.

## V. CONCLUSION

Defense contractors and subcontractors at every tier should act now to assess their compliance posture, remediate gaps, and establish the systems and processes necessary to achieve and maintain certification. Those who treat CMMC as a strategic priority will mitigate legal risk and position themselves competitively in an increasingly security-conscious procurement environment. Legal counsel and a qualified C3PAO are important to this compliance.

---

[1] Currently referred to as the Department of War, however, the regulations refer to DoD.

[2] 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." 32 CFR § 2002.4(h).

[3] FCI is "information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product

or service to the Government, excluding information provided by the Government to the public (such as that on public websites) or simple transactional information, such as that necessary to process payments." 48 CFR § 4.1901.

[4] C3PAOs are authorized by the CMMC Accreditation Body, Inc. to conduct cybersecurity assessments and certify compliance with the CMMC.

[5] Helpful overviews of the CMMC currently in effect are available on the DoD's website: https://dodcio.defense.gov/cmmc/About/ and https://business.defense.gov/Programs/Cyber-Security-Resources/CMMC-20/.

[6] The GSA is an independent federal agency that acts as a centralized business, procurement, and property management arm of the federal government.

[7] The CMMC also implements requirements from NIST SP 800-172.

[8] https://www.justice.gov/opa/pr/health-net-federal-services-llc-and-centene-corporation-agree-pay-over-11-million-resolve

[9] https://www.justice.gov/usao-ma/pr/defense-contractor-morsecorp-inc-agrees-pay-46-million-settle-cybersecurity-fraud

[10] https://www.justice.gov/usao-dc/pr/raytheon-companies-and-nightwing-group-pay-84-million-resolve-false-claims-act