Pachter and Johnson in Law360: Cybersecurity Rule for DOD Contractors Creates New Risks

October 21, 2025 John Pachter, Richard Johnson

PRACTICES Government Contracts Transactions, Government Contracts

Haynes Boone Senior Counsel John Pachter and Richard Johnson authored an article for *Law360* after the U.S. Department of Defense has finalized its Cybersecurity Maturity Model Certification (CMMC) program, requiring nearly all defense contractors and subcontractors to meet strict data security standards and annually affirm full compliance, which is creating significant new compliance burdens and potential legal risks across the defense supply chain.

Read an excerpt below.

On Oct. 15, 2024, the U.S. Department of Defense established a major new program of standards for the security of contractor and supplier data systems. The new requirements establish the Cybersecurity Maturity Model Certification program. While the October 2024 rule established the program, it did not include a clause applying it to contractors and subcontractors.

This second step required a separate action amending the Defense Federal Acquisition Regulation Supplement. On Sept. 9, the DOD released the DFARS clause, locking the CMMC system in place for virtually all prime contractors and subcontractors.

DOD's Authority to Impose the New System
Prior to issuance of the DFARS clause, the DOD imposed the new system under its general contracting authority by specifying in Title 32 of the Code of Federal Regulations, Section 170, that no DOD contract would be valid absent CMMC compliance in any case where new prime contracts would involve possession of certain unclassified information transmitted or stored on prime contractor IT systems.

Now, under the new DFARS clause, prime contractors and higher-tier subcontractors will be contractually obligated to pass the clause down through the contracting chain. If they fail to do so, they will be answerable to the DOD for breach, and the DOD may be able to withhold or retrieve from the subcontractor government-owned or controlled data necessary for subcontract performance.

However, as in the case of certified cost or pricing data — formerly the Truth in Negotiations Act — and many other similar requirements, the government may not proceed directly against subcontractors to impose or enforce the CMMC rule's requirements.

The CMMC Program in Outline
This is not the place for treatment of the CMMC requirements, which are complex, numerous and extensive. Nevertheless, some aspects of the CMMC provisions require special attention.

Of critical importance is determining when a particular contractor data system falls under the CMMC rule. This occurs whenever the data system processes, stores or transmits either of two types of information: federal contract information or controlled unclassified information.

The definitions of FCI and CUI in DFARS 252.204-7021(a), however, are open-ended and subject to revision or expansion at any time, creating a risk that additional contractor data systems could become subject to the CMMC rule at some point during contract performance.

FCI is defined as "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."

CUI is defined as "information the Government creates or possesses, or information an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Governmentwide policy requires or permits an agency to handle using safeguarding or dissemination controls."

Both definitions exclude information an entity possesses or maintains in its own systems that did not come from, "or was not created or possessed by or for an executive branch agency."

To read the full article from *Law360*, click here.