Skadden

Cybersecurity and Data Privacy Update

August 12, 2024

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on the last page or call your regular Skadden contact.

One Manhattan West
New York, NY 10001
212.735.3000

1440 New York Ave., N.W.
Washington, D.C. 20005
202.371.7000

155 N. Wacker Drive
Chicago, IL 60606
312.407.0700

How Defense Contractors Can Prepare Now for CMMC Implementation

Key Points

- Defense contractors should begin preparing for Cybersecurity Maturity Model Certification (CMMC) implementation, expected to begin taking effect early in 2025, based on a proposed rule published in December 2023 setting out three levels of controls (Levels).
- Cybersecurity controls for Levels 1 and 2 contracts are already in effect through existing regulations, but contractors for Level 3 contracts will be required to comply with additional cybersecurity controls yet to be published.
- New assessment and attestation requirements for each CMMC Level will be phased in over a three-year period and will apply to new contracts and option years under current contracts.
- Defense contractors should be evaluating their government business now to: identify their expected CMMC Level; communicate requirements to key subcontractors and assess their status of compliance; develop an IT security strategy to meet cybersecurity reporting; and implement internal processes and procedures to comply with expected audits and attestation requirements.
- Establishing a compliance program is critical because the Department of Justice has been pursuing cases under the False Claims Act where there have been cybersecurity breaches.

The Department of Defense (DoD) is currently reviewing and adjudicating the public comments received in response to its proposed regulations implementing its Cybersecurity Maturity Model Certification 2.0 program (CMMC). Those regulations (Proposed Rule), published December 26, 2023, will establish new verification mechanisms to ensure compliance with DoD cybersecurity requirements prior to award and during contract performance.

Under the CMMC program, all defense contracts will be assigned one of three cybersecurity levels. Levels 1 and 2 are mapped to pre-existing cybersecurity controls outlined in the Federal Acquisition Regulations (FAR) and the Defense Supplement (DFAR) associated with federal contract information (FCI) and controlled unclassified information (CUI), while Level 3, reserved for the most sensitive contracts, will face additional controls beyond those for Level 2.

The Proposed Rule also adds new assessment and attestation requirements associated with each CMMC Level, as discussed below. Affected contractors should be assessing their current compliance with existing cybersecurity controls and preparing for the full set of CMMC compliance requirements before they become effective. The final rule is currently anticipated to be published at the end of 2024 or beginning of 2025, although dates have slipped in the past.

How Defense Contractors Can Prepare Now for CMMC Implementation

CMMC Levels

Starting on the effective date, and in accordance with the phased implementation plan, defense contracts will each be assigned a CMMC Level that will indicate the cybersecurity controls required to receive and perform on the contract.

Most contracts will be assigned Level 1 or 2, which adopt existing cybersecurity controls under FAR (FARs 52.204-21 Basic Safeguarding) and DFAR (DFARs 252.204-7012 Safeguarding Covered Defense Information and Cyber Reporting) for FCI and CUI, respectively. Contractors are already subject to these cybersecurity standards.

The Proposed Rule outlines additional controls for Level 3 contracts, which build upon Level 2 requirements by adding controls based on National Institute of Standards and Technology (NIST) Special Publication (SP) 800-172.

Contractors can anticipate their CMMC Level now by conducting a review of their current government contracts and assessing existing cybersecurity requirements against the criteria for the CMMC Levels outlined in the Proposed Rule. Contractors should also be assessing their material subcontractors' compliance to the extent subcontracts require CMMC compliance. Once implemented, prime contractors will not be able to contract with subcontractors that do not comply with applicable CMMC requirements.

While DFARs 252.204-7012 currently allow contractors to meet the cybersecurity standards through a mixture of implementation of NIST SP 800-171 controls and a plan of action and milestones (POAM), the Proposed Rule would establish a 180-day deadline for closing out any outstanding POAMs. Thus, full compliance with all 110 NIST SP 800-171 controls will be required unless deviations have otherwise been approved.

Importantly, NIST released a new version of NIST SP 800-171 controls, version 3, in May 2024, which prompted DoD to issue a class deviation on May 2, 2024, allowing contractors to meet the DFARs requirement by complying with version 2. Affected contracts will include clause "252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting (DEVIATION 2024-O0013)" incorporating this deviation. The class deviation contains no expiration date.

Assessment and Attestation Requirements

The assessment requirements for each CMMC Level will dictate the frequency of assessments. Maintaining a current assessment will be required for contract award.

Level 1 contracts will require contractors and subcontractors to self-assess compliance with applicable security controls. Level 2 contracts will require on a triennial basis either a (1) self-assessment of compliance or (2) a certification assessment from an approved independent third party. Third parties conducting the assessment will need to be accredited through the CMMC Accreditation Body. Third parties have already begun to receive accreditation or are in the process of being accredited.

Level 3 contracts will require both a Level 2 third-party certification assessment and a government-led assessment to ensure compliance with applicable Level 3 controls.

In addition to compliance assessments, all CMMC levels will require a senior official of a contractor to provide an annual affirmation of compliance with applicable cybersecurity requirements. It will be important for contractors to begin mapping their covered systems and establish internal compliance policies to ensure accuracy of those attestations.

Compliance and Reporting

All assessments and attestations will be electronically submitted to DoD's Supplier Performance Risk Systems (SPRS). Upon full implementation of the program, contract and applicable subcontract awards will be conditioned on a contractor or subcontractor meeting the applicable assessment and attestations requirements. Self-assessments are uploaded by the contractor while third-party assessments are reported by the approved third-party assessor. All requirements for Level 2 and 3 contractors will flow down to applicable subcontractors at all tiers of the supply chain that store, process or transmit CUI. Prime or higher level contractors would be required to confirm that their applicable subcontractors have current SPRS scores prior to subcontract award.

Failure To Comply

Contractors that fail to comply with these requirements will become ineligible for applicable contracts and could face False Claims Act liability for failing to implement appropriate controls while performing on contracts subject to the rules, or misreporting compliance through SPRS. The Department of Justice's Civil Cyber-Fraud initiative has been employing the False Claims Act to pursue cybersecurity-related fraud by government contractors and grant recipients, which includes contractors that knowingly misrepresent their cybersecurity practices or protocols. False Claims Act liability can result in millions of dollars in civil penalties and suspension and debarment proceedings.

How Defense Contractors Can Prepare Now for CMMC Implementation

See our August 5, 2024, client alert "DOJ Launches Corporate Whistleblower Awards Pilot Program and Announces a New Incentive for Self-Reports."

Timing

The Proposed Rule outlines four phases for implementation over a three-year span starting on the effective date. Importantly, the effective date is not expected to fall in 2024, because both the Proposed Rule codifying the CMMC program requirements and the implementing regulations through the DFARs need to be finalized first.

Although DoD has not officially indicated when it will release the final rule implementing CMMC 2.0, observers expect DoD to finalize the rule by the beginning of calendar year 2025 with an effective date likely 30 to 60 days afterwards. Once in effect, contractors can expect to start seeing CMMC Level assignments in new solicitations and, eventually, in option years for existing contracts.

While CMMC is specific to defense contracts, contractors with other federal agencies will likely start to see similar programs in the coming years as the U.S. government seeks to harden its supply chains against cybersecurity attacks. Within DoD, CMMC Program is part of a larger initiative to secure the supply chain broadly from risks stemming from cybersecurity, foreign-sourced products, and services from persons or countries of concern, or more recently, from foreign ownership, control or influence. See our July 24, 2024, client alert "Declassified: DoD Extends Its Vetting of Foreign-Owned and -Controlled Contractors To Cover Some Unclassified Contracts."

While it is unlikely that CMMC will radically impact existing defense contractors that are already required to meet most cyber-security controls, the CMMC program may create cost challenges for new entrants to the defense supply chain, which will not only need to meet the CMMC requirements but more broadly DoD's expansive supply chain security requirements.

Contacts

Michael E. Leiter
Partner / Washington, D.C.
202.371.7540
michael.leiter@skadden.com

William E. Ridgway
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

David A. Simon
Partner / Washington, D.C.
202.371.7120
david.simon@skadden.com

Joshua Silverstein
Counsel / Washington, D.C.
202.371.7148
joshua.silverstein@skadden.com

Tatiana O. Sullivan
Counsel / Washington, D.C.
202.371.7063
tatiana.sullivan@skadden.com

Jacob F. Bell
Associate / Washington, D.C.
202.371.7367
jacob.bell@skadden.com

Jake O. Seaboch
Law Clerk / New York
212.735.2038
jake.seaboch@skadden.com