Updates
November 26, 2019
New Cybersecurity Certification Framework Will Have Significant Impact on Defense Contractors

The U.S. Department of Defense (DOD) is forging ahead in its plan to adopt a new framework for cybersecurity, with significant ramifications for all defense contractors, including subcontractors.

On November 8, 2019, DOD released Version 0.6 of its Cybersecurity Maturity Model Certification (CMMC). DOD anticipates releasing the final model in January 2020 and including it in federal solicitations starting in fall 2020.

Intended to protect DOD's supply chain against increasing cyber threats, CMMC will have a significant impact on contractors. Each of DOD's 300,000-plus contractors and suppliers will need to be certified according to a new, unified cybersecurity framework.

This update provides an overview of CMMC and its significance. It also highlights key aspects of Version 0.6 and identifies important questions that remain open.

DOD's Existing Framework Based on Self-Assessments

The existing cybersecurity framework for defense contractors is derived from various sources. Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012 requires that contractors implement the National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-171, which lists controls intended to safeguard Controlled Unclassified Information (CUI) residing on contractor systems. CUI is broadly defined as any information that law, regulation or governmentwide policy requires to have safeguarding or disseminating controls. CUI does not include classified information.

Among other things, NIST SP 800-171 requires contractors to develop, document and update system security plans. It also requires that contractors develop and implement plans to correct deficiencies and to reduce or eliminate vulnerabilities in their systems.

Under DFARS 252.204-7012, contractors must provide adequate security on their information systems. They also must rapidly report cyber incidents to DOD. The Federal Acquisition Regulation (FAR) also has "basic safeguarding requirements" for contractors' information systems set forth in FAR 52.204-21.

To date, contractors have largely been allowed to determine for themselves how to implement NIST SP 800-171. In a September 2017 guidance, DOD explained that it is the contractor's responsibility to implement NIST SP 800-171 and that third-party assessments of compliance are not required.

CMMC: Single, Unified Standard With Third-Party Verification

DOD has been developing CMMC with the input of industry, university-affiliated research centers, federally-funded research and development centers, and other stakeholders. The rollout process has shifted into a higher gear recently in anticipation of final release of the model.

CMMC reflects DOD's assessment that cybersecurity is an increasingly urgent threat and that protecting against loss of CUI within the defense industrial base is critical to national security. Version 0.6 asserts that cybersecurity "must become a foundation of DoD acquisition." DOD cites estimates that the global cost of

cybercrime each year is approximately $600 billion.

CMMC will create a single, unified standard, borrowing from various existing cybersecurity controls. Defense contractors will be required to hold a CMMC certificate at the specified level to be eligible for award of DOD contracts. All companies conducting business with DOD will have to be certified, including subcontractors and companies that do not even handle CUI.

There will be five certification levels ranging from Level 1 (Basic Cybersecurity Hygiene) to Level 5 (Advanced/Progressive). Each level has its own practices and processes.

In September 2019, DOD released Version 0.4 for public comment. Based on these comments, Version 0.6 updates Levels 1 through 3 but omits Levels 4 and 5. According to DOD, Levels 4 and 5 will be addressed in the next public release.

CMMC categorizes cybersecurity best practices into 17 domains. Examples of domains are Access Control, Risk Management and Incident Response. Each domain is broken further into capabilities and even further into practices and processes. The practices and processes are the activities required to achieve specific capabilities for each of the five maturity levels of CMMC. Thus, to be certified at a given CMMC level, companies will have to demonstrate that they comply with the practices and processes for that level.

Third-Party Assessments and Certifications

The process of certifying contractors' compliance with each of the CMMC levels will be performed by a Third-Party Assessment Organization that will assess the maturity of a company's cybersecurity practices and processes and grant or deny certifications. Contractors will have to coordinate directly with these organizations to request and schedule an assessment.

Each Third-Party Assessment Organization must be accredited by an Accreditation Body, a yet-to-be-created non-governmental entity that will manage and operate CMMC. The Accreditation Body will set the terms and conditions for accrediting Third-Party Assessment Organizations and establish processes for things such as quality control, auditor training and dispute resolution. On November 19, 2019, DOD held a "kickoff meeting" with interested parties regarding the establishment of the Accreditation Body.

DOD intends to identify the required CMMC level in DOD solicitations and to use the level as a go/no go decision in the source selection process. Thus, companies will only be able to be considered for solicitations for which they have the proper certification level or higher. Without the proper CMMC certification, a company will not be eligible to receive the DOD contract.

CMMC Levels 1 Through 3

Version 0.6 provides greater insight into the differences between Levels 1, 2 and 3 as follows:

- To comply with Level 1, companies will have to implement the basic security controls set forth in FAR 52.204-21, the "basic safeguarding" clause. Version 0.6 states that Level 1 practices are foundational and must be completed by all certified organizations. Version 0.6 maps the Level 1 practices to the specific requirements in FAR 52.204-21 and to particular requirements in NIST SP 800-171.
- Level 2 focuses on "intermediate cyber hygiene" and requires more advanced practices to protect and to sustain assets against cyber threats. Companies certified at Level 2 will be expected to establish and

document standard operating procedures, policies and strategic plans for cybersecurity.
- Level 3 companies will have "good cyber hygiene" and must meet the security requirements in NIST SP 800-171 Rev. 1. Organizations that will generate or require access to CUI will need a Level 3 certification. Companies certified at Level 3 must have a basic ability to protect and sustain an organization's assets and CUI, but may have challenges defending against advanced persistent threats, according to the draft model.
- Levels 4 and 5 apply to organizations with a "substantial and proactive cybersecurity program" that allows them to address the changing tactics, techniques and procedures used by advanced persistent threats.

An appendix to Version 0.6 lists the practices applicable to each CMMC level and offers examples of policies and practices for Level 1.

Implications for Contractors and Open Questions

The establishment of a new, single and unified standard has the promise of bringing greater clarity and predictability to a highly complex and evolving area involving multiple standards issued by multiple bodies. CMMC's establishment of a go/no-go test for all DOD contractors will also introduce a significant new step in the source selection process that stops short of making cybersecurity compliance a factor to be evaluated like other non-price factors.

Industry and other stakeholders have raised a number of concerns and questions about CMMC and its implementation. For example:

- **Impact on small businesses and commercial suppliers:** CMMC does not have exceptions for commercial suppliers or small businesses. Although DOD's goal is for CMMC to be cost effective and affordable for small businesses to implement at the lower CMMC levels, certification and compliance are likely to challenge many suppliers.
- **Identification of the relevant controls:** To help identify what controls apply to them, companies should scrutinize the differences between CMMC's unified standard and presently applicable controls. CMMC incorporates dozens of practices from NIST SP 800-171 that currently apply to contracts under the DFARS, but also borrows standards from the United Kingdom and Australia that are less familiar to contractors.
- **Subcontractor flow-down issues:** There are questions regarding the flow down of certification requirements to subcontractors and lower tier subcontractors and the responsibilities of prime contractors and subcontractors for lower tier subcontractors. For example: will subcontractors at each tier need to satisfy the same level as the prime?
- **Quality control:** Significant questions remain regarding the CMMC Accreditation Body, including what processes the body will put in place to ensure quality control of third-party assessments of companies' cybersecurity practices and processes.
- **Identification of the level for a given procurement:** DOD states that the CMMC level will be specified in Sections L and M of solicitations. This introduces an element of uncertainty. It is unclear what standards agencies will apply in the selection of a CMMC level for a specific solicitation. It also is unclear to what extent each military department will follow a standard level selection approach.
- **Cost allowability:** Compliance costs could be significant. DOD has stated that cybersecurity compliance will be an allowable cost but has yet to offer details. One question is whether contractors will have any means of recovering pre-award costs to bring their systems into compliance with CMMC in a particular procurement.
- **Disputes and protests:** There are questions as to whether and in what form disputes may be resolved, especially to the extent that third-party assessors will be private companies. The Contract Disputes Act only applies to suits against the government. Another issue is to what extent the General Accountability

Office and U.S. Court of Federal Claims will have jurisdiction to hear cybersecurity-related bid protests under the CMMC framework.
- **Non-DOD and intelligence community contracts:** At least for now, CMMC does not apply to non-DOD agencies and does not provide controls for classified systems. Different cyber approaches among defense and civilian agencies could pose a problem.
- **Consequences for failure to meet cybersecurity requirements:** Companies certified at a given level could face serious risks if they fail to meet cybersecurity requirements. For example, in July 2019, there was an $8.6 million settlement resolving a *qui tam* relator's suit under the False Claims Act based on alleged cybersecurity non-compliance.

In anticipation of CMMC's release next year, companies should familiarize themselves with Version 0.6 and ensure that they are taking steps to prepare for CMMC to the extent possible, including identifying which CMMC level(s) will likely apply to them and their suppliers.

Authors

Explore more in

Government Contracts Privacy & Security

Related insights

Update

HHS Proposal To Strengthen HIPAA Security Rule

Update

California Court of Appeal Casts Doubt on Legality of Municipality’s Voter ID Law