Understanding the CMMC's New Regulatory Reality for Government Contractors

Jun 26, 2020

Categories:

Blogs
Technology Blog

Every year approximately $600 billion, or 1% of the global gross domestic product, is lost through cyber theft.[1] Right now, there are other nations that have weapon systems with exactly the same flaws as the United States' weapon systems—which suggests the nation's weapon designs are being stolen.[2] While the dangers of cybercrime have been present for many years, the coronavirus pandemic has increased the opportunities for cybercriminals to take advantage of the increased number of internet users online with weak cybersecurity.[3]

Aware of this continued threat to national cybersecurity, the Department of Defense (DoD) created the Cybersecurity Model Maturity Certification (CMMC), with the goal of improving the overall cybersecurity of the DoD. Improved cybersecurity reduces the risk of adversaries stealing and benefiting from the nation's cyber developments and states secrets, and, moreover, protects controlled unclassified information (CUI) from getting into the hands of adversaries.

This article provides an overview of the CMMC, issues that have arisen since DoD announced these new regulations, and ways that individual government contractors facing a new regulatory reality in 2020 can improve their cybersecurity in the short-term and long-term.

Overview of the Cybersecurity Model Maturity Certification

The development of the CMMC began several years ago when DoD directed its government contractors to adopt stronger cybersecurity practices through the NIST 800-171 standard. This standard required any non-federal computer system used by a DoD contractor to store, process, or transmit CUI to provide security protection for such systems. CMMC takes this one step further.

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

FBT Gibbons

DoD will now require companies bidding on defense contracts to certify that they meet the basic level of cybersecurity standards articulated in the CMMC. This unified cybersecurity standard, which debuted as "Version 1.0" on January 31, 2020, will be incorporated into Federal Acquisition Regulations and used as a requirement for contract awarding.

The CMMC gives the DoD a mechanism to certify the cyber readiness of the largest defense contractors ("primes"), as well as the smaller businesses that subcontract with the primes. Primes and subcontractors will not be required to have the same level of CMMC certification to win a contract, but the extent of required subcontractor compliance is unclear.[4]

Every contract—from other transactions agreements to Small Business Innovation Research (SBIR) contracts and even grants—will be marked with a corresponding CMMC level that bidding contractors must meet to bid for a contract.[5] Every one of the more than 350,000 defense contractors will need to be certified under CMMC.

DoD contractors and potential contractors should immediately learn the CMMC's requirements and prepare for the certification process and long-term compliance.

CMMC Third-Party Assessment Organizations

All government contractors working with the DoD will need to become CMMC-certified by passing an independent CMMC certification to verify they have met the appropriate level of cybersecurity for their business. DoD will not be certifying potential defense contractors for CMMC on its own. Nor will companies be charged with the task of self-certification.

Rather, contractors will be certified by a CMMC Third-Party Assessment Organization (C3PAO), which will not be in privity with the DoD. The certification process is a private transaction between the defense contractor and the C3PAO. The C3PAOs will not be able to offer products to the companies they vet, to eliminate conflicts of interest. The assessors will only be allowed to charge contractors for the service of testing their networks. Any solutions to the

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

problems they find will have to be bought separately on the CMMC board's marketplace.

The CMMC Accreditation Board ("Accreditation Board") is the newly created independent non-profit organization made up of 13 members of the defense industrial base, the cybersecurity community, and the academic community, and is responsible for the quality, training, and administration of the C3PAOs.

CMMC Pushback and Other Issues

The rollout of the CMMC has hit some snags since it began in January. A coalition of technology trade associations was so concerned with the rollout of the new cybersecurity standards and certification process that they penned a letter to DoD leaders stressing the need for clarification as to how to prepare. The group cited concerns that current implementation plans lack enough clarity and predictability in key areas and, as a result, may unnecessarily generate confusion, delay and associated costs.

Concerns have also been raised over the uniformity of requirements for similarly situated projects where each contracting officer can establish certain requirements on its own, and subcontractors will not be required to match primes. Multiple authorities could set different level requirements for substantially similar services, resulting in a departure from the uniformity the CMMC seeks to perpetuate. Here is a closer look at the complications that continue to mire rollout of the CMMC:

COVID-19. While the COVID-19 pandemic has slowed down the work across much of the United States, the DoD is adamant that the need for cybersecurity is more important now than ever. And this is true— adversaries are using this unprecedented time to attack companies, particularly small businesses. In one case, ransomware cost a small business $200,000 to acquire the decryption key.[6] Eighty percent of the firms that the DoD partners with are small businesses, which have been hit the hardest financially by COVID-19.[7]

No guidance has been issued as to how training, compliance, and audits will occur during the pandemic when most of the workforce

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

is still at home. However, DoD is continuing with the timeline mentioned above and shows no sign of slowing down with CMMC implementation, even though U.S. cybersecurity remains vulnerable.

The pandemic has greatly increased the need generally for technologies that support secure videoconferencing, virtual events and multimember online meetings throughout all industries, including defense contractors. This is compounded by the vulnerability of U.S. cybersecurity as Chinese hackers target American universities, pharmaceutical and other healthcare firms in a bid to steal intellectual property related to coronavirus treatments and vaccines.8

Rapid Change and Little Guidance. The rollout of the CMMC has been off to a turbulent start. On April 22, 2020, the Accreditation Board posted an RFP requesting proposals as to how the board, the assessors, DoD officials and the contractors themselves can continuously monitor open-source information about companies' cybersecurity and be notified if they are slipping below standards. The Accreditation Board is said to be seeking a cloud-based tool that will essentially offer dashboards for the parties to monitor.

However, the surprise RFP had a tight nine-day response window with no corresponding request for information or other publicized market research. This has prompted some members of the cyber community to conclude that the RFP was written with specific companies in mind. Additionally, confusion exists as to who will fund this cloud-based tool, as DoD has been clear that it will not fund these efforts, nor will it provide funding to the Accreditation Board to avoid conflicts of interest.

The Accreditation Board's request for monitoring technology comes before it has released information on the standards and training of C3PAOs, which some members of the cyber community find to be putting the cart before the horse.

The confusion about standards and compliance has already led to fraud. Some entities are claiming to be C3PAOs capable of providing companies with the CMMC certification. The

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

Accreditation Board has not yet established its program, nor conducted any training or certification of C3PAOs. Once it does, it will establish a CMMC Marketplace that will list approved C3PAOs. Any entity claiming to engage in review and certification now cannot validly or legally certify any contractor. They may be entities seeking to access your systems and information for unlawful purposes.

General Applicability. It is unclear at this point who is required to comply with the CMMC. Guidance is changing daily. For example, on May 5, 2020, DoD announced that the CMMC would not apply to commercial off-the-shelf (COTS) suppliers, like Microsoft that supplies pre-packaged software for DoD.[9] This exception makes sense, particularly since COTS suppliers generally do not handle CUI. Despite this exception, companies should not assume that they or their subcontractors will fall under this or any other exemption without explicit guidance from DoD. Notably, subcontractors that handle CUI are going to be held to the same standard as prime contractors and, because of the flow-down of certain regulations, may still be required to comply to some extent, even if the subcontractor does not handle CUI to the same extent as the prime.

Cost. The Accreditation Board is working to align CMMC with the Federal Risk and Authorization Management Program (FedRAMP), to minimize the economic burden of working with the government by avoiding two separate, mandated certification processes. DoD has promised reciprocity to FedRAMP-certified contractors, but how much reciprocity exactly is still unclear.

For DoD contracts eligible for cost-reimbursement, the CMMC Maturity Level will be contained in sections L and M of an RFP, making cybersecurity an "allowable cost." For smaller government contractors who do not pursue cost-reimbursement contracts, there will be few avenues for relief. Contractors who work on fixed-price or time and materials contracts will be forced to build the cost of cybersecurity compliance into their cost of doing business, thereby increasing rates.

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

Most defense contractors will only need to meet Level 1, Basic Cyber Hygiene, which is the lowest standard with only 17 required practices. The cost to maintain Level 1 for three years is approximately $3,000 or about $1,000 per year.

Preparing for CMMC Compliance

There is no final guidance about the certification process from the Accreditation Board. Until then, government contractors should stay ahead of the transition. There are important steps that contractors can take now to prepare and, later, make minor changes as needed.

Evaluate current systems. After examining current guidance on cyber and data security, contractors should evaluate their systems. Importantly, a contractor should determine the scope of CUI that is handled at the company and how much of the company is working with this type of information. This initial step will influence the rest of the evaluation. For example, some companies are handling very basic information and need only consider achieving Level 1 CMMC compliance (e.g., proper firewalls, anti-virus, and back-ups). Other companies will determine that their systems are handling CUI that will require the whole organization or, possibly, only a small subset of the organization to be Level 3 compliant. If only a small subset of the company needs to be compliant, this could be a significant cost- and time-saving alternative for small or midsize businesses.

Develop a plan of action. Once a contractor is familiar with current guidance and has evaluated its current systems, the company should determine the gaps between where it is and where it wants to be. Then, the contractor should create a plan that documents each step that has been and will be taken to achieve compliance, as well as the timeline to achieve compliance and the resource requirements needed to do so. Even after the plan is implemented, contractors should have a mechanism to continuously monitor their systems to evaluate whether there are any weaknesses that need to be remediated and additional controls put in place. Subsequent changes to the system may have to be documented in the contractor's System Security Plan (SSP), a document that notes any substantial changes a company makes to its security profile or

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

processes.

Conclusion

As these requirements and guidance are rapidly changing, it is important to seek guidance from cybersecurity experts and legal counsel that specialize in this area. Frost Brown Todd stands ready to support your company's efforts to comply with the CMMC.

For more information, contact Zenobia Bivens or any attorney in Frost Brown Todd's Government Contracting or Privacy & Data Security practice groups.

---

[1] https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf?utm_source=Press&utm_campaign=bb9303ae70-EMAIL_CAMPAIGN_2018_02_21&utm_medium=email

[2] https://www.afcea.org/content/pandemic-offers-opportunity-prepare-meet-cmmc-requirements

[3] http://www.unicri.it/news/article/covid19_cyber_crime

[4] https://www.cmmcab.org/cmmc-standard

[5] A narrow exception exists for Companies that solely produce Commercial-Off-The-Shelf (COTS) products, who will be required to comply with CMMC certification. Examples of potentially CMMC-exempt contractors are chicken suppliers or fuel producers. https://www.acq.osd.mil/dpap/Docs/cotsreport.pdf

[6] https://www.afcea.org/content/pandemic-offers-opportunity-prepare-meet-cmmc-requirements

[7] https://www.afcea.org/content/pandemic-offers-opportunity-prepare-meet-cmmc-requirements

[8] https://www.wsj.com/articles/chinese-iranian-hacking-may-be-hampering-search-for-coronavirus-vaccine-officials-say-11589362205

[9] https://www.acq.osd.mil/cmmc/faq.html

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

FBT Gibbons

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

FBT Gibbons