Westlaw Today
powered by Reuters

The road to CMMC: where we started and where we are headed

By Michael G. Gruden, Esq., Maida Lerner, Esq., Jake Harrison, Esq., and Alexis Ward, Esq., Crowell & Moring LLP

MARCH 30, 2023

Anyone who has followed the U.S. Government's tireless efforts to regulate the cybersecurity protecting its sensitive information knows that it has been a long and winding road to its current juncture of releasing an updated cyber compliance paradigm — the Cybersecurity Maturity Model Certification (CMMC) — later this spring.

CMMC is a DoD certification program designed to measure a federal government contractor's cybersecurity maturity. The anticipated CMMC proposed rule is expected to lead the way for companies looking to comply with the government's ever-evolving information security requirements. While CMMC will directly impact federal government contractors that handle unclassified information requiring safeguarding, the broader cybersecurity community, information technology (IT) marketplace and commercial sector at large will feel the heat as well.

Herein we highlight the path that the CMMC rulemaking will likely take and provide a Cybersecurity Roadmap of the Top 5 Action Items that various stakeholders may contemplate as they review and consider strengthening their own cybersecurity compliance regardless of whether they engage in direct government contracting, thus implicating CMMC, or not.

Where we started

The Department of Defense's (DoD's) effort to address complex and evolving cybersecurity threats has been quite a journey. There were more than a few forks and detours along the way, and there are assuredly twists and turns to come. The path to CMMC 2.0 can be traced back through four Defense Federal Acquisition Regulation Supplement (DFARS) clauses.

The DFARS clauses

DFARS 7012

DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting Clause (DFARS 7012), was DoD's first major foray into mandating cybersecurity standards for government defense contractors handling unclassified but sensitive government information.

First introduced in 2013, DoD tinkered with the DFARS 7012 language several times before it took a strategic step in attempting to encourage government contractors to implement the security requirements by imposing a mandatory implementation deadline of December 31, 2017. Since then, DoD incorporated DFARS 7012 into almost all DoD contracts.

DFARS 7012 refers to the information it protects as "covered defense information" or "CDI," but DoD has worked to phase out CDI in favor of "controlled unclassified information," "DoD CUI," or "CUI," in an effort to standardize its terminology with the broader federal government.

The anticipated CMMC proposed rule is expected to lead the way for companies looking to comply with the government's ever-evolving information security requirements.

Generally, DFARS 7012 aims to protect CUI by obligating contractors who handle CUI to comply with the security requirements found in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171.[1]

DFARS 7019 and 7020

In September 2020, DoD released an Interim Rule on assessing contractor implementation of cybersecurity requirements, including DFARS 252.204-7019 (DFARS 7019) and DFARS 252.204-2020 (DFARS 7020). With these new clauses, DoD attempted to add teeth to the DFARS 7012 security requirements, wanting to encourage higher rates of compliance.

DFARS 7019 and 7020 introduced an accountability mechanism to help DoD audit contractors' NIST SP 800-171 compliance. Together, the clauses obligate contractors to maintain a record of their NIST 800-171 compliance within the Supplier Performance Risk System (SPRS), accessible by DoD personnel, and to update their compliance status every three years.[2]

DFARS 7020 distinguished between basic assessments, which can be satisfied by the contractor submitting a self-assessment before

contract award, and DoD-conducted medium/high assessments, a more rigorous assessment carried out after contract award if a contractor is handling especially sensitive or high-value CUI.[3] CMMC's certification model borrows heavily from this three-tiered assessment program, discussed in more detail below.

DFARS 7021

While the DFARS 7012 and NIST SP 800-171 security requirements were meant to safeguard sensitive data, over time DoD realized that they were not working as intended. Despite its December 2017 implementation deadline, DoD found that its contractors were not consistently implementing the requirements, and that the risk of sensitive data loss remained high.[4]

CMMC certification may require a reconfiguration of a contractor's current IT infrastructure.

DoD faced an incentive issue. The DFARS 7012 clause does not require DoD to verify contractors' implementation of NIST SP 800-171 prior to contract award, so some contractors simply did not implement them at all, and many that did implement the requirements did not do so adequately. Thus, alongside DFARS 7019 and 7020, DoD published DFARS 252.204-7021 (DFARS 7021), containing the original CMMC Framework.

Most notably, unlike DFARS 7012, DFARS 7021 requires contractors to possess a current CMMC certification at the contract's requisite CMMC level prior to contract award and to maintain that certification for the duration of the contract.[5]

CMMC

CMMC 1.0

In January 2020, DoD introduced the (now defunct) CMMC Version 1.0, which included five levels of CMMC certification based on maturity processes and cybersecurity controls. Certification would have been available at one of five levels, based on the sensitivity of the information expected to be handled under contract performance.

As its name perhaps foreshadowed, CMMC 1.0 is not where the road ends. Like DoD cybersecurity efforts before it, CMMC has evolved to keep up with new threats and risks to networks housing sensitive government information. In March 2021, DoD began an internal review of CMMC 1.0, engaging industry to help shape the beleaguered program.

CMMC 2.0

In November 2021, DoD announced CMMC Version 2.0, incorporating findings from its internal review and feedback from industry. DoD has explained CMMC 2.0 compliance (and thus DFARS 252.204-7021 compliance) will not be required until DoD completes this new round of rulemaking. DoD originally expected rulemaking to conclude in November 2023 and currently is sticking by that timeline in spite of recent delays to the rulemaking process.

CMMC 2.0 generally includes three CMMC levels of certification as follows.

CMMC Level 1, Foundational — Contractors must implement the 17 controls from NIST SP 800-171 enumerated in FAR 52.204-21 and submit an annual self-assessment to the DoD through the Supplier Performance Risk System (SPRS).

CMMC Level 2, Advanced — Contractors must implement the 110 controls in NIST SP 800-171 and submit an annual self-assessment or, if required to handle as yet undefined "critical national security information," a triennial independent assessment performed by a private entity certified by the DoD as a third-party assessor (known as a "Third Party Assessment Organization" or "C3PAO").

CMMC Level 3, Expert — Contractors must implement the 110 controls in NIST SP 800- 171 and a yet to be determined subset of controls from NIST SP 800-172 before undergoing a triennial government-led assessment.

Under the current Version 2.0, compliance will continue to be required prior to award through solicitation and contract terms.

DoD is currently working to finalize the scope and applicable controls for these levels. Importantly, the controls applicable at each level may change when NIST finalizes its pending revisions to SP 800-171, which are expected as soon as Spring 2023.

DoD has also indicated that it will recognize reciprocity between CMMC and other domestic cybersecurity standards such as the Federal Risk and Authorization Management Program (FedRAMP)[6], and it is looking into reciprocity with International Organization for Standardization (ISO) frameworks and other international cybersecurity standards.

Where we are headed

Impact on defense contractors

Defense contractors may have to shift gears to handle the impacts of the anticipated final version of CMMC 2.0, including how they incorporate cybersecurity within their businesses — in their planning, in their infrastructure, and in their relationships with subcontractors.

The final requirements will likely no longer allow these contractors to be backseat drivers when it comes to their own compliance, including how they implement protocols to assess their own compliance with NIST SP 800-171.

One way may be to engage outside help from Registered Provider Organizations (RPOs), including select law firms, who are able to provide pre-assessment guidance to government contractors in the process of obtaining CMMC certification. These RPOs can also assist contractors if issues are discovered through the certification process.

CMMC certification may also require a reconfiguration of a contractor's current IT infrastructure. Because CMMC requires CUI to be handled and stored in sufficiently protected environments, companies will now need a deep understanding of their network

set up and data flows to assess and maintain compliance and may need to build an appropriate infrastructure or partner with qualified vendors to house their CUI in environments that have the required protections in place.

Finally, contractors may not only be responsible for their own cybersecurity journey — they may also need to pave the road for their subcontractors. Contractors will be responsible for ensuring that subcontractors employ the adequate CMMC level to handle the information being exchanged between the contractor and the subcontractor.

Again, this will require contractors to have a deep understanding of their own data, as well as their relationship with the subcontractor. The contractor will need to understand what data is being flowed to the subcontractor and what level of CMMC certification is required to handle that data. Contractors that are accustomed to riding solo may now need to join the carpool lane.

Impact on industry

Even more than for individual defense contractors, CMMC will likely change the path for the defense industry as a whole. While the focused and unified heightening of cybersecurity standards is expected to have a positive impact on supply chain security, the final CMMC requirements may alter the way defense contractors engage industry at large.

For example, cloud service providers and software providers will need to assess their product offerings to ensure their ability to meet the government's requirements (e.g., FedRAMP Moderate baseline, NIST Secure Software Development Framework (SSDF), etc.) and continue providing technology for defense contractors.

CMMC is expected to define a baseline level of cybersecurity across the defense industry that will help ensure some level of protection across the entire supply chain against cybersecurity threat actors.

Minimizing risk of cyber threats at every step of the supply chain will establish a new standard for federal cybersecurity, and in turn create commercial best practices — increasing security along the supply chain and minimizing points of weakness for threat actors to exploit.

However, reciprocally, the finalized CMMC requirements may increase exposure to defense contractors across the industry by shifting the responsibility of that cybersecurity to the contractors. The industry will now have a greater responsibility to understand their own data and data flows in order to ensure full compliance with the required controls.

A contractor that self-certifies its compliance with CMMC additionally may risk False Claims Act action if its self-certification comes into question, especially under the Justice Department's Civil Cyber Fraud Initiative.

In response to the heightened requirements of CMMC, companies that develop products and technology that support these contractors may need to reroute as well. These providers will need to be aware of developments in the CMMC requirements and be proactive in designing sufficiently protected technology or obtaining their own required certifications.

For example, cloud service providers that plan to work with contractors covered by CMMC will be required to be FedRAMP moderate or equivalent. These second-hand requirements could become a major detour for many services providers across the industry.

Cybersecurity roadmap: top 5 action items

Regardless of where they are on the road to cybersecurity compliance, there are several steps that companies can take now to ensure they are going in the right direction in meeting the CMMC rule and also in developing a compliant cybersecurity program generally lest they end up on the road less traveled.

1. Know your data and your network

In order to implement the cybersecurity infrastructure best suited to meet a business' operational and legal requirements, it is important to understand what categories of regulated data are handled and need to be protected in accordance with government and contractual obligations.

A contractor that self-certifies its compliance with CMMC additionally may risk False Claims Act action if its self-certification comes into question.

For example, does the company possess personally identifiable or biometric data that could implicate state or international privacy laws? Does it handle federally regulated data, such as CUI, that carry specific marking and handling requirements? Are subsets of CUI, such as Export Controlled Information or Naval Nuclear Propulsion Information, on company networks that need to be protected from access by foreign nationals?

Until a company understands what data is handled and the associated regulatory and cybersecurity requirements, it is unclear which direction a company needs to go.

2. Review your contracts

A thorough review of each contract is essential to understand what categories of regulated or proprietary data may be generated or transmitted as part of contract performance. In addition, commercial and government contracts are increasingly including custom cybersecurity, data privacy and incident reporting provisions. Beyond standard cybersecurity frameworks (e.g., NIST CSF, ISO 27001, SOC 2, NIST SP 800-171, etc.) many contracts are now including tailored provisions that add to or enhanced these preexisting standards.

Without careful analysis of each agreement, a company may overlook, for example, that it has only 24 hours to report an incident or that all customer data must be treated as CUI. Particular requirements, such as these examples, form the roadmap that should direct a company's cybersecurity strategy.

3. Consider an enclave

Depending upon the volume of regulated data a company possesses and the stringency of the cyber requirements, a company may consider erecting an enclave to house its regulated data. Where companies have a significant commercial presence apart from their business containing regulated data, they often find it tenable to segment their regulated data from the rest of their network.

The benefits of segmentation are two-fold — 1) it reduces legal risk by constricting the data and network subject to select cybersecurity and incident reporting requirements; and 2) it streamlines the implementation of technical and administrative solutions, decreasing resource costs.

4. Conduct privileged compliance assessments

The regulated data that each company possesses becomes its individual North Star, guiding it towards a cybersecurity regime tailored to protect their information assets. Once a company understands its regulated data and the boundaries of the network, it should pressure test its ability to meet the applicable requirements to protect that data. This validation is often most effective when conducted by an external third-party and under attorney client privilege.

Using counsel with technical capabilities to conduct the assessment or to direct the assessments by third parties can benefit companies if needed to demonstrate to customers and the government that an independent assessment was conducted and also to mitigate the risk of having to disclose assessment findings in litigation or during an investigation.

5. Develop & refine corporate policies

While technical solutions are integral to any cyber strategy, a company's cybersecurity is only as effective as the policies it adopts governing the use of such technology and regulating data traversing it. Companies should establish a practice of devising robust internal cybersecurity policies, incident response plans and other governance documents. Then, the task is to train on and test these policies and plans to help ensure their effectiveness.

These activities can help provide evidence of a company's diligent approach to cybersecurity as, increasingly, government regulators, assessing whether companies are protecting sensitive data, are asking companies whether they have developed and are complying with their own cybersecurity and incident response policies and procedures.

Conclusion

While there remains uncertainty where CMMC's anticipated proposed rule will lead companies seeking to comply with its requirements, the steps outlined above are actions each company can take in order to navigate their own journey towards cybersecurity compliance.

Notes

[1] *See* DFARS 252.204-7012(b)(2).

[2] *See* DFARS 252.204-7019(b); DFARS 252.204-7020(d).

[3] DFARS 252.204-7019(d)(1)-(2).

[4] Dep't of Def. Office of Inspector General, *Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems DODIG-2019-105* (July 23, 2019).

[5] DFARS 252.204-7021(b).

[6] FedRAMP is a Federal government program that provides a standardized approach to security assessment, authorization, and continuous monitoring for commercial cloud products and services sold to the government.

About the authors




(L-R) **Michael G. Gruden**, a counsel at **Crowell & Moring LLP**'s Washington, D.C., office, is a registered practitioner under the Cybersecurity Maturity Model Certification framework, a former Pentagon information technology acquisition branch chief and a former contracting officer at the U.S. Defense Department and the U.S. Department of Homeland Security. He can be reached at mgruden@crowell.com. **Maida Lerner** is senior counsel at the firm's Washington, D.C., office and part of its privacy and cybersecurity and government contracts groups. She advises clients on government contracts, transportation and manufacturing, in the areas of cybersecurity and privacy compliance. She can be reached at mlerner@crowell.com. **Jake Harrison**, an associate at the firm's Washington, D.C., office, counsels government contractors on compliance and regulatory issues, with a focus on cybersecurity and data privacy compliance. He can be reached at jharrison@crowell.com. **Alexis Ward** is an associate in the firm's Los Angeles office and a member of its privacy and cybersecurity and government contracts groups. She can be reached at award@crowell.com. The authors would like to thank partner Evan D. Wolff for his contribution to this article.

This article was first published on Westlaw Today on March 30, 2023.