Deloitte.

DoD contractor and subcontractor alert
February 2020

DoD contractor and subcontractor alert

Cybersecurity Maturity Model Certification (CMMC)

Introduction

With the release of the Cybersecurity Maturity Model Certification (CMMC), major changes are coming to the Department of Defense (DoD) supply chain this year for both contractors and subcontractors (referred to as "contractors" herein). CMMC v1.0 was published in January 2020, and the requirements will be defined in the DoD's RFIs and RFPs targeted for inclusion beginning in June and September 2020, respectively.

Here's what you should know.

What is it?

On October 21, 2016, the DoD adopted a final rule amending the Defense Federal Acquisition Regulation Supplement (DFARS) that required new cybersecurity safeguards and cyber incident reporting for certain types of controlled unclassified information (CUI)[1] for all DoD contractors by December 31, 2017. As this deadline has passed, and various requirements have been established since, the DoD has shifted its focus to the development of a broad cybersecurity model derived from various standards and leading practices. Through collaboration with DoD stakeholders, CMMC was designed to be that model and will be essential in the effort to make security the foundation of DoD acquisition. The CMMC model consists of five maturity levels, ranging from level 1 to level 5, comprising increasing requirements at each successive level—level 5 having the most requirements and being considered the most secure. While CMMC shares certain aspects with its predecessors (such as DFARS), one of the notable differences with CMMC is that self-attestation will not be permitted (that is, third party certification will be required). An accreditation body will be established in the coming months to train and certify the third party auditors responsible for performing CMMC certifications for DoD contractors.

What does the CMMC model cover?

The CMMC model was designed with a focus on protecting federal contract information (FCI) and CUI. CMMC v1.0 encompasses 17 cybersecurity domains, ranging from access control to situational awareness. These domains consist of 43 capabilities that are supported by 171 practices derived from various cybersecurity frameworks and leading practices. CMMC consists of five levels of maturity with varying levels of adoption (for example, level 1 requires only 17 practices, while level 5 requires all 171 practices).[2.] The level of maturity required will depend on the sensitivity of the DoD information that is being handled; for example, companies that handle highly sensitive information must have a level 5 certification.

Cybersecurity risk must be proactively managed and, for those in the DoD supply chain, CMMC creates a clear and measurable cybersecurity requirement that must be assessed by a third party.

Who must comply?

In support of the DoD's initiative to make cybersecurity an integral part of the acquisition process, all contractors in the supply chain must adhere to the defined requirements (meaning a contractor can bid on a contract, but they cannot be awarded the contract until they reach the requisite certification level). Level 1 will be the minimum requirement for all contractors, with higher levels being specified in the respective RFI or RFP.

Why now?

Recent incidents have brought the cybersecurity weaknesses of defense contractors and subcontractors to light. To address these vulnerabilities and the increasing cybersecurity risks, the DoD has made cybersecurity compliance a critical and mandatory part of the acquisition process.

What's next?

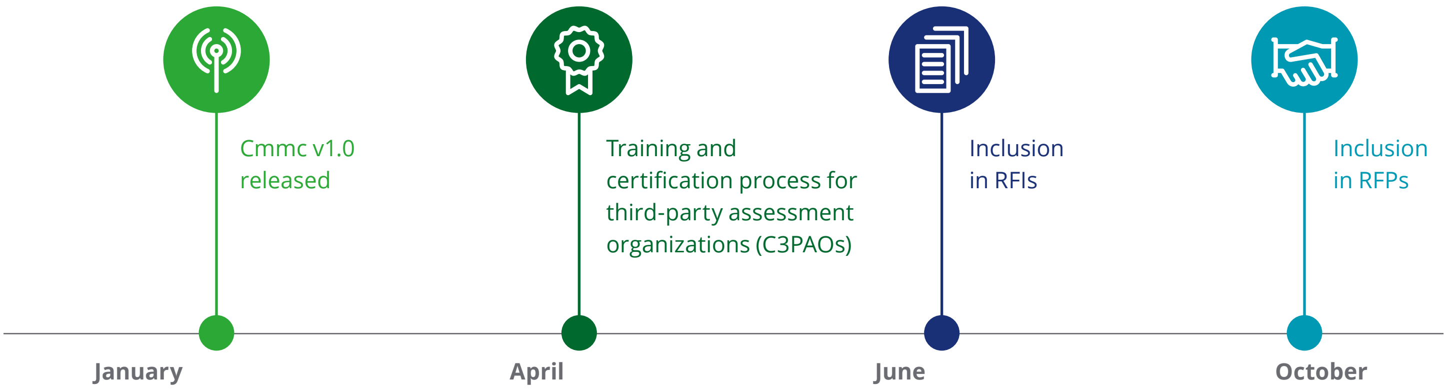
In spring 2020, it is expected that the CMMC Accreditation Board will be formed, and this board is expected to be the governing body around CMMC Third Party Assessment Organizations (C3PAO). These C3PAOs are expected to undergo training and adhere to various certification requirements in order to assess DoD contractors in the future. Additionally, it is expected that DoD contractors will be required to undergo an audit by a C3PAO and obtain a Cybersecurity Maturity Model Certification by mid-to-late 2020.

Challenges

Now more than ever, information security leaders are challenged by evolving information security requirements, as well as the threat of intrusion and data leakage. Contractors are ultimately responsible for addressing the risks specific to their business environments and providing adequate security. To safeguard CUI and adhere to the incident reporting requirements, contractors are required to identify CUI and take the applicable steps to protect that information. Some common pitfalls associated with this requirement include:

- CUI identification
- Media protection and tagging
- Training, policies, and procedure development and implementation

CMMC 2020 timeline



January: Cmmc v1.0 released

April: Training and certification process for third-party assessment organizations (C3PAOs)

June: Inclusion in RFIs

October: Inclusion in RFPs

How Deloitte can help

We take a business-focused, broad approach that supports cost savings, productivity, and risk-reduction goals. We encourage DoD contractors to take a proactive and sustainable approach in order to meet the CMMC requirements. Deloitte can help in various ways, including the following:

Readiness services

Our professionals can assist with achieving compliance by assessing existing processes and controls against the CMMC framework to identify if deficiencies exist. If deficiencies are identified, we can assist with the development of plans of action and remediation activities to address deficiencies.

Supply chain illumination

Aside from the CMMC requirements that contractors must address for their own organization, there is a business imperative to also consider the indirect risk of supply chain disruption. As subcontractors play a critical role in the supply chain, many companies will need to assess and respond to the risk of their subcontractors not being able to comply with their respective CMMC requirements on a given contract. If a vital subcontractor cannot meet the defined CMMC requirements, that subcontractor cannot be used for the respective contract—potentially causing serious supply chain disruptions for the prime contractor. This risk can be of particular concern, as even the identification of relevant subcontractors and service providers throughout the supply chain can be an extremely complex and challenging task. Leveraging a breadth of experience and technical resources, we can help to identify, map, and profile your supply chain to provide transparency and valuable data points to support mitigation of supply chain disruption.

CUI discovery

With the complexity of today's computing landscape, the end-to-end identification of where CUI could reside or where it is transmitted from can quickly become a daunting task. We can assist with inventorying the relevant portions of the landscape housing or transmitting CUI—creating a roadmap for your compliance program.

System security plan and POAM development

Development of a system security plan that is updated periodically to reflect changes in the organization's environment is essential in a well-maintained environment. Plans of action and milestones (POAM) are also developed to mitigate unimplemented security requirements and can be combined into this document. We can assist in the development and documentation of the system security plan and POAM, as well as perform a review to update an existing plan.

CMMC certification support

Certifications and audits can be time-consuming, and difficult to support amid fulfilling day-to-day business activities and having the appropriate individuals to interface with the certifiers can significantly contribute to the outcome of your certification. We have extensive experience in both performing and supporting certifications and audits and can help with preparation for the certification, engaging with your certifiers, and responding to any findings identified.

Incident damage assessment

In the event of an incident where CUI may have been compromised, we can assist with the damage assessment and the archival of evidence that may be requested by the DoD.

Market recognition

Deloitte in aerospace and defense

Deloitte Touche Tohmatsu Limited (DTTL) member firms serve 95 percent of Fortune 500 Aerospace and Defense companies.

Global reach

Deloitte's A&D practice consists of more than 600 professionals in the United States and more than 1,500 across the Global network, many of whom have experience in industry or in the military.

Deloitte is a member of the following organizations:

Aerospace Industries Association (AIA), National Defense Industrial Association (NDIA), Space Foundation, and Professional Services Council (PSC).

Let’s talk

Click here to email our team or contact any of the individuals below.

Curtis Stewart
Managing Director
CMMC A&IA
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
+1 703 251 1782
custewart@deloitte.com

Alan Faver
Partner
Aerospace & Defense
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
+1 404 220 1701
afaver@deloitte.com

Jeff Lucy
Managing Director
CMMC Cyber
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
+1 704 785 0345
jlucy@deloitte.com

Keith Thompson
Senior Manager
CMMC Delivery
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
+1 703 405 3717
keithompson@deloitte.com

Louverture C. Jones
Senior Manager
CMMC Delivery
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
+1 305 808 2548
loujones@deloitte.com

Mika Alexoudis
Manager
CMMC Delivery
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
+1 919 616 7109
malexoudis@deloitte.com

Endnotes

1. US Department of Defense, *Implementation of DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting*, September 21, 2017, https://www.acq.osd.mil/dpap/policy/policyvault/USA002829-17-DPAP.pdf, accessed January 2020.

2. 2. US Department of Defense, *Cybersecurity Maturity Model Certification*, January 30, 2020, https://www.acq.osd.mil/cmmc/docs/ CMMC_Model_Main_20200203.pdf, accessed February 2020.

About Deloitte
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the “Deloitte” name in the United States, and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.