Deloitte.

00:03
00:05
00:02
00:01
00:04

CMMC is here . . .
Are you ready?

The release of the Cybersecurity Maturity Model Certification (CMMC) brings major changes to the Department of Defense (DoD) Supply Chain for both contractors and subcontractors. As CMMC will be a requirement to do business with the DoD, it is critical for DoD contractors to understand what CMMC means for their organizations and begin preparing now.

DoD contractors and subcontractors must meet various requirements focused on safeguarding Controlled Unclassified Information (CUI) and Federal Contract Information (FCI). Those handling CUI or FCI must undergo an assessment by a CMMC Third-Party Assessment Organization (C3PAO) to validate compliance with these requirements.

Here’s an overview of the timing to help keep you on track.

CMMC timeline
Office of the Secretary of Defense (OSD) activity/milestone

DIB timeline
Defense Industrial Base (DIB) activity/milestone

January 2020

CMMC v1.0 released

- Plans of actions and milestones (POA&M) review
- Define CUI boundary
- Revisit system security plan (SSP)

Spring 2020

CMMC Accreditation Body (AB) formed

CMMC readiness assessments begin

Summer 2020

Provisional Assessor Program begins

Fall 2020

DoD issued interim rule (effective 11/30/2020, which includes requirements for DoD contractors)

Winter 2020/2021

Targeted inclusion of CMMC requirement in select RFIs/ RFPs begin

Targeted roll out of CMMC certified training

C3PAO certifications begin

Winter 2021/2022

Why now?

On September 29, 2020, the DoD published an interim rule (effective November 30, 2020) codifying: (1) the NIST SP 800-171 DoD Assessment Methodology; and (2) the CMMC Framework. Building onto DFARS clause 252.204-7012, the interim rule includes the following[1]:

- DFARS provision 252.204-7019, which requires contractors to complete a NIST 800-171 assessment at least every three years and post the results the Supplier Performance Risk System (SPRS) in order to be considered for award.

- DFARS clause 252.204-7020, which requires contractors to provide the DoD access to their systems, facilities, and personnel in order to validate NIST 800-171 compliance via independent assessment. Additionally, contractors are responsible for ensuring that their subcontractors supporting a potential DoD contract also have completed a NIST 800-171 assessment and have posted the results to SPRS prior to award.
- DFARS clause 252.204-7021, which covers the implementation of the CMMC requirements.

While the CMMC requirement may not yet be included in a contract that you are interested in pursuing, the interim requirement is applicable now so you should not wait to prepare. Additionally, taking early action to prepare for the DoD assessment is a step toward CMMC compliance – as the foundation of CMMC is based on the NIST 800-171 requirements.

What can you be doing right now?

In preparation for CMMC, organizations across the Defense Industrial Base (DIB) are taking a serious look at their controls surrounding NIST 800-171 and beginning to understand the differences between NIST 800-171 and CMMC. Some specific areas of focus for DoD contractors include the following:

Define your CUI boundary – In order to understand what level of CMMC you might need, start by understanding your CUI boundary and the types of information that are passing through your environment.

Revisit your system security plan (SSP) – In previous versions of the DFARS clause, DoD contractors were required to develop and maintain a SSP. Now is good time to review and update your SSP, because this will be an integral part of your CMMC assessment.

Revisit your POA&M – If you've performed a self-assessment, you should have developed a POA&M that outlines gaps and your plan to close those gaps. Before going into your CMMC assessment, you should close outstanding gaps and review and update your POA&M.

Common 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.

Common challenges associated with these requirements include:

- **CUI Identification and management**
- **Media protection and tagging**
- **Training, policies, and procedure development and implementation**
- **Supply chain/subcontractor risk mitigation**

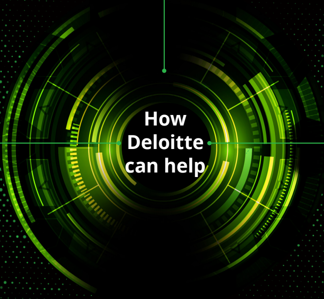
How might this affect you?

CMMC will be required for all* DoD contractors (prime and subs) to do business with DoD. Potential implications of noncompliance could include the following:

- **Revenue loss**
- **Reputational damages through adverse performance reviews**
- **Supply chain disruption**
- **Proposal exclusion**

---

*DoD has stated that companies that solely produce Commercial-Off-The-Shelf (COTS) products do not require a CMMC certification. However, other aspects of the contract may deem such companies CMMC relevant and should be considered on a case-by-case basis. https://www.acq.osd.mil/cmmc/faq.html



How Deloitte can help

Deloitte takes 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 to achieving the CMMC requirements on an ongoing basis.

Deloitte is recognized globally as a leader in cybersecurity risk services. Our vast team of cybersecurity professionals serves thousands of clients worldwide in both the public and private sectors, including various DoD agencies and companies in the DIB. We have a variety of solutions that can be tailored to meet specific cybersecurity needs on the path to CMMC compliance.

Readiness Services – Deloitte can assist DoD contractors with achieving CMMC compliance by assessing existing processes and controls against the CMMC framework to identify if deficiencies exist.

Remediation Services – After organizations undergo a readiness assessment, a Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) audit, or an official assessment from a C3PAO, Deloitte can provide a number of remediation services to help organizations meet CMMC requirements.

Supply Chain Risk Management Services – Aside from the CMMC requirements that contractors need to address for their own organization, there is a business imperative to also consider the indirect risk of supply chain disruption due to the noncompliance of supply chain partners and subcontracters. Deloitte can offer various services to assist DoD contractors with managing the CMMC-related risks within their supply chain.

Cyber Managed Services – Organizations can struggle with resources, tools, and skill sets to implement ongoing cybersecurity platforms. Our team of professionals can provide ongoing managed services to help with these challenges.

Certification Services – Deloitte is in the process with the AB to become a C3PAO and expects to be credentialled in 2021. Stay tuned for updates on this service.

CMMC Program Management and Optimization – CMMC is the tipping point for organizations to start thinking holistically about their overall government contract compliance program – enabling sustainable growth for both DoD-specific business operations and the entire organization. We can help organizations think through their compliance program and provide guidance on how to best derive value from optimizing the management of it.

Products and Solutions Readiness and Management – Consider your products and solutions delivered into the Defense Industrial Base that may need to be CMMC compliant. Failing to adhere to such requirements could result in significant revenue loss, which is why it is critical to proactively prepare and manage compliance around your products and/or services.

CMMC for Cloud and Digitization of Products and Processes – As many organizations are moving toward digitization and a cloud environment, CMMC compliance should be a top-of-mind issue. Wherever you may be in the process, the Deloitte team can provide valuable insight and assistance on your path to CMMC compliance.

Year 1 highlights

CMMC v1.02 was published in March 2020, and provides insight into the CMMC requirements (e.g., practices, processes).

The AB began accepting C3PAO applications in June 2020.

On August 31, 2020, the Accreditation Body (AB) kicked off its Provisional Assessor Program, which is a pilot program intended to be foundational to the official C3PAO training program. We are pleased to announce that Deloitte professionals were among those selected to participate in this program.

The AB began authorization of C3PAOs in June 2021. These organizations will be permitted to assess DoD contractors who wish to obtain a CMMC.

The first round of DoD contractors are expected to undergo an audit by a C3PAO and obtain a CMMC in 2021.

00:03
00:05
00:02
00:01

Contact us to learn more about how we can help you be prepared for CMMC.

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

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

Charan Ahluwalia
Principal
CMMC Government and Public Services
Deloitte LLP
+1 347 237 7834
cahluwalia@deloitte.com

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

---

[1] US Department of Defense, Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019–D041), September 29, 2020, https://www.govinfo.gov/content/pkg/FR-2020-09-29/pdf/2020-21123.pdf, accessed April 2021.

This document contains general information only and Deloitte Risk & Financial Advisory is not, by means of this document, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This document is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional adviser. Deloitte Risk and Financial Advisory shall not be responsible for any loss sustained by any person who relies on this document.

As used in this document, “Deloitte” or “Deloitte Risk and Financial Advisory” means Deloitte & Touche LLP, which provides audit and risk advisory services; Deloitte Financial Advisory Services LLP, which provides forensic, dispute, and other consulting services; and its affiliate, Deloitte Transactions and Business Analytics LLP, which provides a wide range of advisory and analytics services. These entities are separate subsidiaries of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2021 Deloitte Development LLC. All rights reserved.