CYBERSECURITY MATURITY MODEL CERTIFICATION PROGRAM

About

The Cybersecurity Maturity Model Certification (CMMC) Program is designed to enhance the protection of FCI and CUI processed, stored, or transmitted on defense contractor or subcontractor information systems.

Applicability

All Department of Defense (DoD) contracts and subcontracts that will process, store, or transmit FCI or CUI on contractor information systems. Includes commercial item contracts and subcontracts (except contracts exclusively for commercially available off-the-shelf (COTS) items) above the micro-purchase threshold.

Relevant Terms (32 CFR 170.4(b))

- **CMMC Third-Party Assessment Organizations (C3PAOs):** Organization accredited to conduct CMMC Level 2 Certification Assessments.
- **Cloud Service Provider (CSP)**: External company providing platform, infrastructure, applications, and/or storage services for its clients.
- **Contractor Risk Managed Assets**: Assets that can, but are not intended to, process, store, or transmit CUI because of security policies, procedures, and practices in place.
- **Controlled Unclassified Information (CUI)**: Information the government creates or possesses, or that an entity creates or possesses for or on behalf of the government, that a law, regulation, or government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. *See* 32 CFR § 2002.4(h).
- **External Service Provider (ESP)**: External people, technology, or facilities an organization utilizes for the provision and management of comprehensive IT and/or cybersecurity services on behalf of the organization.
- **Federal Contract Information (FCI)**: Information not intended for public release that is provided by or generated for the government under a contract to develop or deliver a product or service to the government. *See* 48 CFR § 4.1901.
- **Internet of Things (IoT)**: The network of devices that contain the hardware, software, firmware, and actuators that allow the devices to connect, interact, and freely exchange data and information. *See* NIST SP 800–172A.
- **Operational Technology (OT)**: Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment).
- **Plan of Action & Milestones (POA&Ms)**: A document that identifies tasks needing to be accomplished.
- **Security Protection Assets**: Assets that provide security functions or capabilities to the organization's CMMC Assessment Scope, irrespective of whether or not these assets process, store, or transmit CUI.
- **Specialized Assets**: Assets that can process, store, or transmit CUI but are unable to be fully secured, including IoT devices, Industrial Internet of Things (IIoT) devices, OT, Government Furnished Equipment, Restricted Information Systems, and Test Equipment.

Current Security Regulation & Requirements: FAR 52.204-21; DFARS 252.204-7012; NIST SP 800-171; NIST SP 800-172

McCarter & English
Government Contracts & Export Controls Group

Alexander W. Major
amajor@mccarter.com

Franklin C. Turner
fturner@mccarter.com

Cara Wulf
cwulf@mccarter.com

Tiffany Hubbard
thubbard@mccarter.com

Maria Panichelli
mpanichelli@mccarter.com

CMMC Level	In-Scope Assets	Security Requirements	POA&Ms	Out-of-Scope Assets*	Assessment/Affirmation Frequency
1	All assets that process, store, or transmit FCI	FAR 52.204-21	Not allowed	IoT devices, OT, and Government-Furnished Equipment	Self-assessment required annually Affirmation by a contractor senior official completed annually
2	• All assets that process, store or transmit CUI • Security Protection Assets • Contractor Risk Managed Assets • Specialized Assets • ESPs • CSPs**	FAR 52.204-21 DFARS 252.204-7012 NIST SP 800-171 Rev 2	Allowed subject to certain limitations and deficiencies identified; must be remediated within 180 days	• Assets that cannot process, store, or transmit CUI and do not provide security protections for CUI assets • Assets that are physically or logically separated from CUI assets	Assessments (self- or performed by a C3PAO required triennially) Affirmation by contractor senior official completed annually
3	• All assets that process, store, or transmit CUI • Security Protection Assets • Contractor Risk Managed Assets • Specialized Assets • ESPs • CSPs**	DFARS 252.204-7012 NIST SP 800-171 Rev 2 NIST SP 800-172	Allowed subject to certain limitations and deficiencies identified; must be remediated within 180 days	• Assets that cannot process, store, or transmit CUI and do not provide security protections for CUI assets • Assets that are physically or logically separated from CUI assets	DoD-led assessment required triennially Affirmation by contractor senior official completed annually

*Assets that fall into any in-scope asset category cannot be considered an out-of-scope asset.

**Contractors/subcontractors undergoing a CMMC Level 2 or 3 assessment may use a CSP to process, store, or transmit CUI in the execution of a contract or subcontract, provided the CSP either (1) is FedRAMP Authorized at the FedRAMP Moderate (or higher) baseline in accordance with the FedRAMP Marketplace, or (2) if not FedRAMP Authorized at the FedRAMP Moderate (or higher) baseline, meets security requirements equivalent to those established by the FedRAMP Moderate (or higher) baseline.

THE CMMC PROGRAM: 10 THINGS FOR THE C-SUITE

McCarter & English
Government Contracts & Export Controls Group

Alexander W. Major
amajor@mccarter.com

Franklin C. Turner
fturner@mccarter.com

Cara Wulf
cwulf@mccarter.com

Tiffany Hubbard
thubbard@mccarter.com

Maria Panichelli
mpanichelli@mccarter.com

10 Things Your C-Suite Should Know About CMMC

1. CMMC is a cybersecurity compliance regime that augments what is required by contractors and subcontractors doing business with the DoD.
2. CMMC will apply via phased rollout to contracts and subcontracts that involve the processing, storing, or transmittal of any information not intended for public release that is provided by or generated for the government under a contract to develop or deliver a product or service to the government.
3. CMMC does not apply to (1) contracts below the micro-purchase threshold (currently $10,000 in 2024) or (2) contracts exclusively for COTS items, defined generally as any item of supply (including construction material) that is (a) a commercial item, (b) sold in substantial quantities in the commercial marketplace, and (c) offered to the government, under a contract or subcontract at any tier, without modification, in the same form in which it is sold in the commercial marketplace.
4. CUI includes a wide variety of information the government creates or possesses, or that an entity creates or possesses for or on behalf of the government, that a law, regulation, or government-wide policy requires or permits an agency to handle using express safeguarding or dissemination controls.
5. CMMC has three levels of requirements that DoD program managers will identify in solicitations based on the supplies and/or services being sought.
6. CMMC Level 1 requirements are expected to apply to non-COTS DoD contracts over the micro-purchase threshold where the need to process, store, or transmit any CUI is not intended or expected.
7. CMMC Level 2 requirements are expected to apply to non-COTS DoD contracts over the micro-purchase threshold where the need to process, store, or transmit any information that a law, regulation, or government-wide policy requires or permits an agency to handle using express safeguarding or dissemination controls is intended or expected.
8. CMMC Level 3 requirements are expected to apply to non-COTS DoD contracts over the micro-purchase threshold where the use of express safeguarding or dissemination controls that are intended or expected to be used to process, store, or transmit any information that a law, regulation, or government-wide policy requires or permits an agency to be protected from an adversary possessing sophisticated levels of expertise and significant resources that allow it to create opportunities to achieve its objectives by using multiple attack vectors (the Advanced Persistent Threat).
9. Costly and lengthy self- or third-party assessments, senior affirmations, and certifications given to the DoD will be required and DoD audits should be expected.
10. CMMC requirements will need to be flown down to vendors and subcontractors at all tiers.

10 Questions the C-Suite Should Be Asking About CMMC

1. Is our company a DoD contractor, subcontractor, or supplier?
2. Do we have a CUI policy?
3. Are the clauses found at FAR 52.204-21, DFARS 252.204-7012, and/or DFARS 252.204-7021 resident in or referenced by any of our existing contracts, subcontracts, or supply/vendor agreements?
4. Does our System Security Plan reflect that our information system network is properly suited for segmentation in case we need to isolate DoD contract information?
5. How have we made any representations, via contract acceptance and invoicing, submissions pursuant to DFARS 252.204-7019 and -7020, cyber incident reporting pursuant to DFARS 252.204-7012, etc., to the DoD related to our cybersecurity?
6. What, if any, representations have we made to our stockholders/partners/subcontractors/prime contractors related to our cybersecurity?
7. Are we using or intending to use in performance of a DoD contract a CSP to process, store, or transmit CUI or an ESP for the provision and management of comprehensive IT and/or cybersecurity services that will process, store, or transmit CUI or Security Protection Data on ESP assets?
8. How are we sure that our domestic and foreign supply chain is able to comport with the requirements resident in CMMC?
9. What changes are we prepared to make in our subcontractor responsibility and award assessments that comport with CMMC?
10. Are we using or intending to use in performance of a DoD contract or provide to the DoD IoT devices, IIoT devices, OT, Government Furnished Equipment, Restricted Information Systems, or Test Equipment?

10 Questions for Which There Are No Current Answers About CMMC

1. How much is all this going to cost?
2. When will this be final and in my contract/subcontract?
3. How do I know for sure what CMMC level will apply to me, my contract, or the products/services I supply?
4. When can I get formally certified by a third-party assessment organization?
5. Can I be assured that the DoD will properly mark material they intend to be protected or define the required CMMC level for all tiers of subcontractors?
6. What is the impact should a prime contractor not properly or adequately identify the appropriate CMMC level in its subcontract?
7. What happens should a prime or subcontractor not be able to locate or identify a CMMC-compliant source?
8. How do I know if I'm being targeted by an adversary that possesses sophisticated levels of expertise and significant resources that allow it to create opportunities to achieve its objectives by using multiple attack vectors (an "Advanced Persistent Threat")?
9. What triggers, if any, can cause CMMC requirements to escalate/decrease among the three levels over time?
10. Are there remedies available to challenge a negative CMMC Certification Assessment beyond the accreditation body's final decision on elevated appeals?