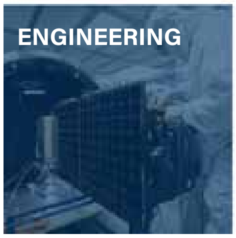
CMMC Quick Reference Guide

MIT Lincoln Laboratory is a Department of Defense Federally Funded Research and Development Center (FFRDC)



Overview of MIT Lincoln Laboratory

Mission: MIT Lincoln Laboratory researches and develops advanced technologies to meet critical national security needs. What sets us apart from many national research and development (R&D) laboratories is an emphasis on building operational prototypes of the systems we design. Read more

At the Laboratory, research and development begins with difficult problems that we believe technology can solve. Our researchers work in cross-disciplinary teams that leverage the latest technical advances to develop innovative solutions. Read more

Vision and Values:

- Our vision is to be the nation's premier laboratory that develops advanced technology and system prototypes for national security challenges.
- We value Integrity, Excellence, and Innovation - How we approach our work.

How can you work with us?

- Research and development partners: We work with government, industry, academia, and not-for-profits to develop technologies that meet national security needs.
- Lincoln Laboratory has a robust program designed to maximize opportunities for small businesses to participate in Laboratory acquisitions and obtain funding awards. Read more

Overview of The Contracting Services Department (CSD)

The mission of MIT Lincoln Laboratory's Contracting Services Department is to provide optimal contracting solutions through guidance, service, and partnership to further the Laboratory's mission of advancing technology for national security.

- Guidance — We help Laboratory staff, and our external customers navigate the complex processes our programs require.
- Service — We strive for an exceptional customer experience, every time.
- Partnership — We collaborate to obtain the best results.

Contact Us
244 Wood Street
Lexington, MA 02421-6426

LINCOLN LABORATORY
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

Cybersecurity Maturity Model Certification Overview

Cybersecurity Maturity Model Certification (CMMC) is a framework developed by the Department of Defense (DoD) to ensure that contractors meet specific cybersecurity standards to protect sensitive information throughout the DoD's supply chain. CMMC applies to contracts involving Federal Contract Information (FCI) or Controlled Unclassified Information (CUI), for both prime contractors and subcontractors. CMMC compliance will be required for relevant Laboratory suppliers engaged in new contracts enacted after the rule takes effect. The date for supplier compliance has not yet been announced by the DoD.

There are three levels of CMMC compliance, and the required level is determined by the sensitivity of the information the contractor or subcontractor handles. CMMC requirements will be incorporated into all DoD contracts above the micro-purchase threshold (MPT) whenever the contractor or subcontractor provides information systems that "process, store, or transmit" FCI or CUI. Contracts exclusively for commercially available off-the-shelf (COTS) items are exempt from CMMC requirements, although there is no exception for FAR Part 12 for commercial products or services contracts. FAR Part 12 implements the Federal Government's preference for the acquisition of commercial products and commercial services by establishing acquisition policies closely resembling those of the commercial marketplace.

Contact us: CMMCSupplierCompliance@ll.mit.edu

Check out the: Small Business Program Office CMMC Resource Letter

Contact Us
244 Wood Street
Lexington, MA 02421-6426

LINCOLN LABORATORY
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

Frequently Asked Questions

Cybersecurity Maturity Model Certification (CMMC) Questions

1. **Does my company need to become CMMC compliant?**
   - If your company processes, stores, or transmits CUI or FCI, and your company intends to bid on any DoD contracts in the near future (2026), including contracts with MIT Lincoln Laboratory, you must achieve CMMC Level 2, or 3 certifications.
   - If your company works with FCI, but does not process, store, or transmit CUI then your company must achieve CMMC Level 1 certification.
2. **What level of CMMC compliance should my company strive for?**
   - It depends upon what type of information your company processes, stores, or transmits.
   - In addition, as a subcontractor to any prime contractor, the DoD mandates that prime contractors not only meet CMMC requirements themselves but also ensure that their subcontractors, who process, store, or transmit information, also comply with the same (or a higher level) of CMMC certification.
3. **Is there support or resources available from MIT Lincoln Laboratory to assist suppliers in achieving CMMC compliance?**
   - There are several resources that are available to guide you through the CMMC compliance process. You can find more details on CMMC requirements and available support through the official DOD CMMC website: https://dodcio.defense.gov/CMMC/.
   - Additionally, the Procurement Technical Assistance Centers (PTACs) offer free and low-cost support to businesses navigating cybersecurity and compliance requirements: https://www.aptac-us.org/.
   - The DoD CUI Program website includes detailed CUI information.
4. **Where can my company find CMMC Third Party Assessment Organizations (C3PAOs)?**
   - The CyberAB Marketplace lists all C3PAOs. Please note inclusion on this list does not constitute an endorsement or recommendation from MIT Lincoln Laboratory. We encourage all of our partners to do their own research to identify which resource(s) meets their company's needs.
5. **What is Federal Contract Infromation (FCI)?**
   - FCI is contained in contract documents. This information is confidential and intended for internal use only, never for public dissemination.
     - Information provided by or generated for the Government, via a contract where the contractor develops a product or service for the Government.
     - Not always marked, but is subject to CMMC.
6. **What is Controlled Unclassified Infromation (CUI)?**
   - A category of information that represents a specific subset of FCI, necessitating enhanced protective measures and subject to additional controls mandated by the DoD.
   - Characteristics can include diagrams, drawings, parts, etc., used on military equipment.
   - Encryption of CUI is mandatory.
   - Should always be marked as CUI information.

Frequently Asked Questions

7. **Are there any contractual or financial implications for subcontractors who do not meet the CMMC compliance requirements?**
    - Beginning in FY 2026, CMMC Flowdown requirements will require a current CMMC certificate at or above CMMC Level 2 for suppliers that handle CUI, as well as annual affirmations of continuing compliance as a requirement for contract award.
8. **What is the overall approach or strategy that MIT Lincoln Laboratory is taking to ensure CMMC compliance across its supplier base?**
    - The Laboratory is taking a proactive and collaborative approach to ensure CMMC compliance across our supplier base, recognizing the critical role that suppliers play in maintaining the cybersecurity posture of the defense industrial base.
9. **What Level of CMMC certification is MIT LL seeking?**
    - Currently Level 2.
    - The Lab anticipates that a Level 3 certification will be required in some specific instances.
10. **What are the implications for my company, as a supplier to MIT LL, given that MIT LL is seeking a Level 2 CMMC Certification?**
    - When a prime contractor is required to be CMMC Level 2 certified, all subcontractors that will process, store, or transmit CUI related to that contract must also achieve at least CMMC Level 2 certification; there are clauses that will be flowed down.
11. **What is Flowdown and why does it matter?**
    - CMMC flowdown refers to the clauses in the prime contract that are also included in DoD subcontracts to ensure subcontractors meet CMMC cybersecurity requirements.
    - The DoD's purpose of requiring flowdown is to create a secure supply chain, as vulnerabilities in any part of the chain would compromise CUI.
12. **How much will it cost to obtain CMMC certification?**
    - Several factors need to be considered when budgeting for CMMC certification, including:
        - The level of certification you intend to achieve.
        - If your company is already compliant with any of the DoD's cybersecurity-related standards.
        - If you plan to become certified by either a Certified Third-party Assessment Organization (C3PAO*) or a "Defense Industrial Base Cybersecurity Assessment Center" (DIBCAC**).
13. **How long will it take to become CMMC compliant?**
    - It depends upon:
        - The level of CMMC certification your company is seeking.
        - If your company has already met and maintained a NIST 800-171 assessment in the Supplier Performance Risk System (SPRS).
        - The number of resources your company allocates to achieving the desired level of CMMC certification.
        - On average, it can take 12-18 months to prepare for a Level 2 certification, and then your company needs to engage with a Certified Third-party Assessment Organization (C3PAO), which can take up to six additional monthscompany needs to engage with a Certified Third-party Assessment Organization (C3PAO), which can take up to six additional months.

14. How long is CMMC certification valid?

- Level 1 certification requires an annual self-assessment and affirmation of compliance with the 15 cybersecurity standards detailed in FAR 52:204-21: Basic Safeguarding of Covered Contractor Information Systems. Upon successful completion of the assessment, the supplier must enter their affirmation into SPRS.
- Level 2 certification requires compliance with 110 cybersecurity standards aligned with NIST SP 800-17 R2: Protecting Controlled Unclassified Information in Non-federal Systems and Organizations, as well as with the standards required for Level 1. Level 2 certification is assessed by a Certified Third-Party Assessment Organization (C3PAO). Level 2 certifications awarded by a C3PAO are valid for three years but must be self-affirmed annually with scores entered into SPRS.
- All CMMC Level 3 certifications are valid for 3 years, provided:
  - The contractor or subcontractor is in full compliance with Level 1 and Level 2 certifications and meets an additional 24 DoD-selected requirements as detailed in NIST SP 800-172: *Enhanced Security Requirements for Protecting Unclassified Information*. An assessment by the Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) is required for Level 3 certification, as well as annual self-assessments.

15. How do you renew a Level 3 certification?

- To renew a Level 3 Certification, a triennial government-led assessment and attestation are required.

16. Where can I find the CMMC requirements for each level of CMMC compliance?

- Level 3: https://csrc.nist.gov/pubs/sp/800/171/r3/final
- Level 2: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r3.pdf
- Level 1: https://www.acquisition.gov/far/52.204-21

17. Are the levels of CMMC successive to one another?

- Yes.
- To achieve a CMMC Level 2 certification, your company must comply with the 15 Cybersecurity practices of a Level 1 certification.
- To achieve a Level 3 certification, your company must comply with the 15 Cybersecurity practices for a Level 1 certification, and the 110 practices defined in NIST SP 800-171R2 for a Level 2 certification.

18. What if my company stores, transmits, or receives information using a Cloud Provider?

- The Federal Risk and Authorization Management Program, known as FedRAMP, is a government-wide program that provides a standardized approach to assessing and authorizing the security of cloud services:
  - When a DoD contractor or subcontractor uses a Cloud Service Provider (CSP) to process, store, or transmit Controlled Unclassified Information, the CSP must be FedRAMP-authorized at the Moderate level or higher or meet FedRAMP Moderate equivalency requirements.*
  - If CUI is not processed, stored, or transmitted in the cloud, FedRAMP authorization is not required.

Additional information can be found in the DoD's FedRAMP Authorization and Equivalency briefing - https://dodcio.defense.gov/Portals/0/Documents/CMMC/FedRAMP-AuthorizationEquivalency.pdf

19. Is FedRAMP required for all Cloud Providers?

- FedRAMP is a mandatory security certification for Cloud providers who want to store US government data from a government agency
- DoD contractors and subcontractors are required to protect CUI using FedRAMP Moderate controls. One way of accomplishing this is through a FedRAMP Moderate authorized service. (https://marketplace.fedramp.gov/products). https://marketplace.fedramp.gov/products
- Another way of accomplishing this is by ensuring FedRAMP moderate equivalency of the cloud service (https://dodcio.defense.gov/Portals/0/Documents/CMMC/FedRAMP-Authorization Equivalency.pdf)

20. My company uses a Managed Service Provider (or Managed Security Service Provider). Do they need to be CMMC certified?

- The DoD uses the term External Service Provider (ESP) as "external people, technology, or facilities that an organization utilizes for provision and management of IT and/or cybersecurity services on behalf of the organization."
- In the CMMC Program, CUI or Security Protection Data (e.g., log data, configuration data), must be processed, stored, or transmitted on the ESP assets to be considered an ESP.
- Please see the CMMC Level 2 Scoping Guide (v2.13, page 9) for additional External Service Provider Considerations (https://dodcio.defense.gov/CMMC/Resources-Documentation/)

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited. This material is based upon work supported by the Department of the Air Force under Air Force Contract No. FA8702-15-D-0001. Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Department of the Air Force.