Updated November 2025

Cybersecurity Maturity Model Certification (CMMC)

Your comprehensive guide to CMMC preparation, implementation, and certification success.

NSF.ORG

“November 10, 2025, marks the start of CMMC certification being a requirement in new Department of War contracts for organizations handling sensitive information.”

What is CMMC?

The CMMC (Cybersecurity Maturity Model Certification) is an assessment framework developed by the U.S. Department of War (DoW) to enhance the cybersecurity of its suppliers, collectively known as the Defense Industrial Base (DIB).

The program was launched as a response to the growing number of cyberattacks targeting defense contractors, which jeopardize sensitive data and pose significant risks to national security. Its goal is to provide a structured certification process to verify that Department of War contractors can comply with information security standards—such as NIST SP 800-171 and DFARS (Defense Federal Acquisition Regulation Supplement) 252.204-7012—to safeguard CUI (Controlled Unclassified Information) and FCI (Federal Contract Information).

If you are part of the Defense Industrial Base (DIB) or intend to join it (in 2021, the DoW awarded more than $154 billion in prime contracts to small businesses), you will need to comply with CMMC. It is estimated that over 300,000 organizations will be affected. Those that fail to comply will be excluded from existing DoW contracts and will not be able to compete for new business.

CMMC Services from NSF

NSF has the experience and expertise to work with you on your CMMC journey. We are an authorized C3PAO and is listed on the Cyber AB Marketplace, the official accreditation body for the CMMC program. We were also the first to be authorized in Michigan.

Our services include:

- **Mock CMMC assessments:** This may seem like an additional step, but completing this can lead to significant time and cost savings down the line, as it can help organizations gain a clearer understanding of specific types of evidence assessors expect for each assessment objective.
- **Phase 1 CMMC pre-assessments:** DIB contractors pursuing Level 2 CMMC certification must pass the Phase 1 pre-assessment before they can move on to the Phase 2 CMMC assessment. The goal of this mandatory readiness check is to confirm that organizations have all the necessary documentation for the formal Phase 2 CMMC assessment.
- **Formal Phase 2 CMMC assessments:** NSF assessors will conduct the CMMC assessment. This includes 110 security requirements; each associated with one or more assessment objectives - 320 in total. After a rigorous assessment process, and subject to the requirements being met for a Final CMMC Level 2 certification, the organization is awarded a three-year CMMC certification.

Don’t underestimate the effort required for CMMC compliance. Ensure you have the necessary resources and that leadership is engaged and prepared to provide ongoing support. **Talk to NSF.**

CMMC Objectives

To strengthen the cybersecurity maturity of DIB organizations, the CMMC framework aims to achieve several objectives:

Mitigate cyber risks:

CMMC provides a consistent set of cybersecurity requirements to safeguard CUI and FCI and reduce the likelihood of successful attacks on Department of War contractors.

Enhance trust:

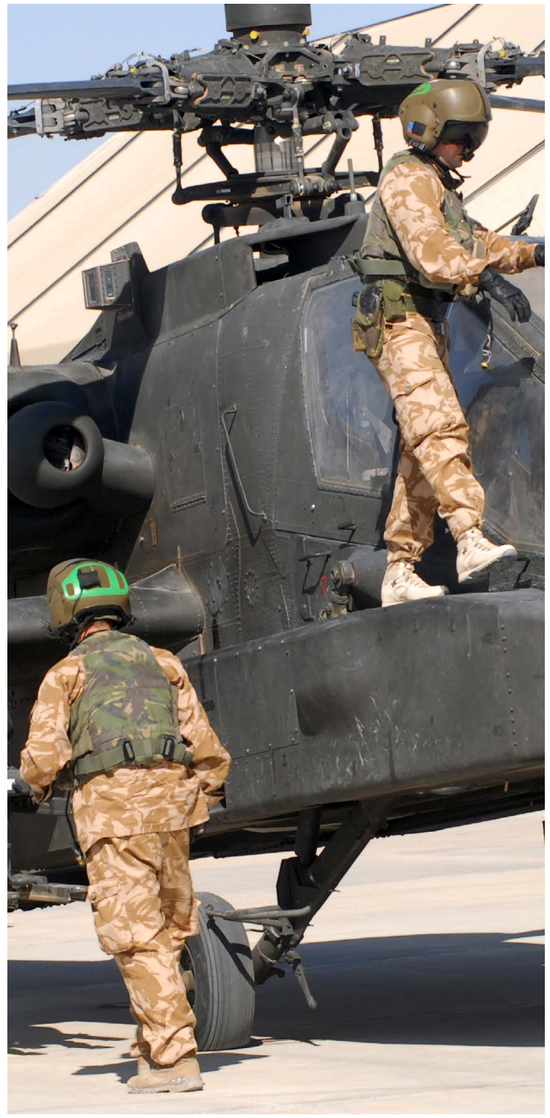
Compliance with CMMC requirements allows organizations to demonstrate their commitment to cybersecurity maturity, fostering trust among government agencies, contractors, and subcontractors.

Facilitate compliance:

To help organizations streamline the compliance process, the CMMC model has been simplified since its launch, with the reduction of compliance levels and the introduction of a three-year implementation plan.

Enhance security across the supply chain:

With its gradual extension to all organizations within the DIB, the CMMC model enhances the security of the entire supply chain. This collaborative approach ensures safeguards are implemented at every level, reducing risks from data breaches.

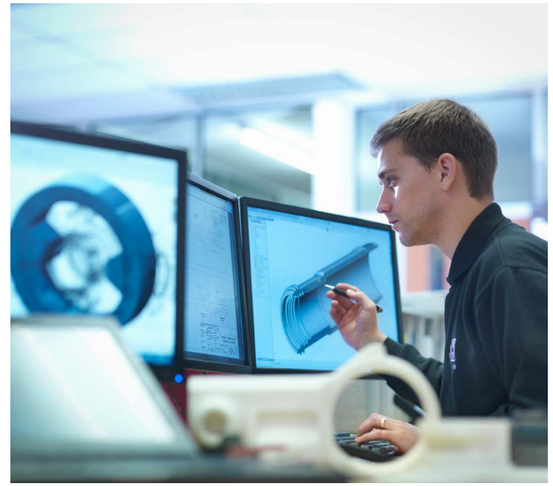


How the CMMC Model is Structured

The CMMC model is based on two rules:

- 32 CFR, defines the CMMC requirements. It was published on December 16, 2024.
- 48 CFR, defines when and how CMMC requirements will appear on DIB contracts. It came into effect from November 10, 2025.

32 CFR organizes CMMC into three levels, each representing a different degree of cybersecurity maturity. Your organization's required level will depend on the type of information your organization will be handling and the level of threat risk.



	Who must comply	Requirements	Assessment
Level 3	DIB contractors that handle CUI and manage critical systems identified by the Department of War.	134 requirements: 110 from Level 2, plus 24 based on NIST 800-172.	• DIBCAC assessment every three years • Annual affirmation.
Level 2	DIB contractors that handle CUI (Controlled Unclassified Information).	110 requirements: 15 from Level 1 included in NIST SP 800-171 r2.	• C3PAO assessment every three years or • Self-assessment every three years for select programs • Annual affirmation.
Level 1	DIB contractors that handle FCI (Federal Contract Information).	15 requirements based on FAR 52.204-21.	• Annual self-assessment • Annual affirmation.

The model is designed to allow organizations to progress through the levels as they enhance their cybersecurity capabilities. Most organizations will aim for Level 2, while those handling significant amounts of CUI may need to achieve Level 3.

Each Level requires more time, likely more cost, and a deeper understanding of the organization's cybersecurity posture.

“Achieving CMMC certification is a significant endeavor, and insufficient preparation could result in delays in obtaining certification and potentially lost business opportunities.”

How the CMMC Certification Process Works

The CMMC certification process consists of the following steps:

1

CMMC self-assessment. All DIB organizations, regardless of their required CMMC level, must conduct a thorough self-assessment to evaluate their current cybersecurity maturity practices against CMMC requirements and identify areas for improvement. For Level 1 and a subset of organizations requiring Level 2, an annual self-assessment will be sufficient to satisfy CMMC requirements.

2

Third-party assessment. Organizations requiring Level 2 and those requiring Level 3 must pass a third-party assessment to certify compliance with CMMC requirements. For Level 2, the assessment is conducted by a C3PAO (CMMC Third-Party Assessor Organization), while Level 3 requires an assessment by the DIBCAC, the Defense Industrial Base Cybersecurity Assessment Center of the DoW. Marine Corps, Air Force and entities such as Space Force, the U.S. Coast Guard and the National Guard. In 2025, this was renamed the “Department of War”.

3

CMMC certification. If the assessment is successful, organizations receive their CMMC certification. This certification is valid for three years, after which organizations must undergo re-assessment to maintain their CMMC status.

4

CMMC affirmation. All organizations, regardless of their level, need to submit an affirmation into SPRS (Supplier Performance Risk System) annually. The affirmation validates to the Department of War that they are actively maintaining compliance with their CMMC level status.delivery, and maintenance of military weapons systems, subsystems, and components or parts.

How to Prepare for CMMC

To meet CMMC requirements follow the steps below:

1

Asess your current cybersecurity posture. Conduct a thorough review of your existing systems, policies, processes, practices and technical controls to identify gaps within the relevant CMMC level requirements. Key areas of focus include access control, incident response, asset management, and configuration management. NIST 800-171 Rev 2 can be used

2

Develop a detailed remediation plan. The main elements of this plan are; a) prioritizing gaps to address areas that pose the greatest risk and are essential for CMMC compliance; b) assigning responsibilities; c) setting deadlines; d) allocating resources to effectively address each gap; e) regularly tracking progress to stay on course.

3

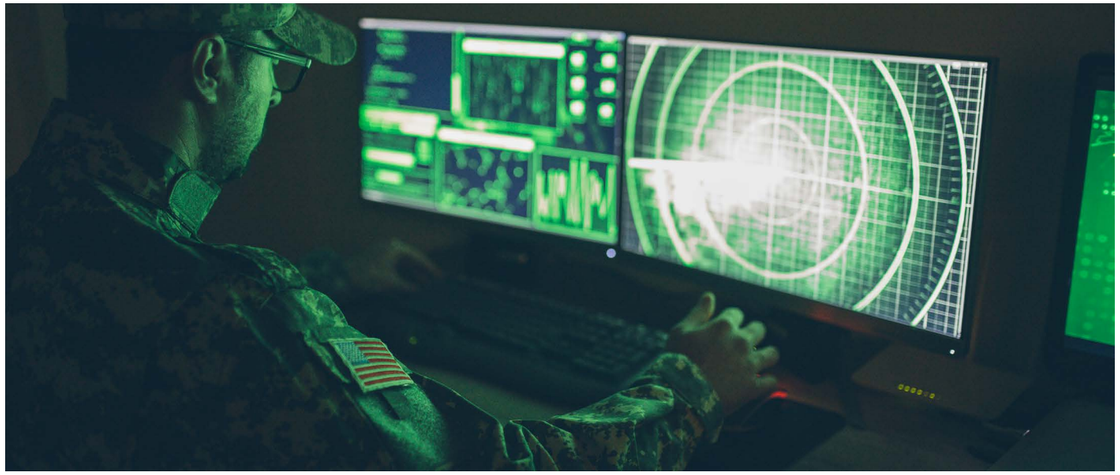
Train your staff. Ensure that all employees are aware of CMMC requirements and understand their roles in maintaining compliance.

4

Document everything. Properly document your cybersecurity policies, procedures and controls to demonstrate compliance.

5

Get ready for the assessment. When ready for the assessment, ensure that everything is up to date and easily accessible for the assessment team.



How CMMC will be Implemented?

The CMMC program is now being implemented as 48 CFR came into effect on November 10, 2025. The requirements of each phase will apply to all contracts, whether new or existing, even if the contract does not explicitly include them. It is the responsibility of the prime contractor to flow down CMMC requirements to all subcontractors.

Phase 1 – Initial Implementation	November 10, 2025	Applicable solicitations will require Level 1 or Level 2 self-assessment.
Phase 2	Begins one year after Phase 1.	Applicable solicitations will require Level 2 certification.
Phase 3	Begins one year after Phase 2.	Applicable solicitations will require Level 3 certification.
Phase 4 – Full Implementation	Begins one year after Phase 3.	All solicitations will include applicable CMMC level requirements was a condition of contract award.

Please note: Department of War may implement CMMC requirements in advance of the planned phase in some procurements.

Challenges in Implementing CMMC

While CMMC offers numerous benefits, organizations may face challenges in its implementation.

Resource constraints. Many organizations, particularly small and medium-sized businesses (SMBs), may lack the resources to meet the stringent requirements of CMMC. This can create barriers to compliance and hinder their ability to compete for government contracts.

Complexity of requirements. The multi-tiered structure of CMMC can be complex. It can be challenging for organizations to understand the specific requirements for each level, implement the necessary practices and navigate the certification process.

Evolving threat landscape. CMMC requires organizations to invest resources in ongoing assessments and improvements, to adapt their cybersecurity practices as cyber threats continue to evolve.

About False Starts

DIB contractors pursuing Level 2 CMMC certification must pass the Phase 1 pre-assessment before they can move on to the Phase 2 CMMC assessment. Failing this step results in what's been called a "false start."

As more OSCs (Organizations Seeking Certification) begin the CMMC certification process, cases of false starts have increased.

Failure to pass the pre-assessment means the scope of the assessment could not be determined and these organizations will likely need to re-do the pre-assessment. This can cause delays to the organizations CMMC certification timeline.

False starts are preventable with proper preparation. For organizations planning CMMC Level 2 certification, NSF can provide expert guidance, as well as mock assessments to identify potential issues early and avoid costly delays.

History and Evolution of CMMC

The origins of CMMC date back to 2015, when the DoW strengthened DFARS 252.204-7012—the clause that focuses on protecting CUI—and the National Institute of Standards and Technology published NIST SP 800-171, which provides the cybersecurity framework to comply with 252.204-7012.

CMMC 1.0 was launched in 2019 with five levels. CMMC 2.0 - announced in 2021 - introduced important improvements:

- It reduced maturity levels from five to three.
- It aligned with NIST SP 800-171.
- It increased the application of self-assessment instead of third-party assessment for lower-risk organizations.

These changes were formalized in December 2024, when CMMC was launched.

November 10, 2025, marked the start of CMMC certification being a requirement in new Department of War contracts for organizations handling sensitive information. This is when 48 CFR, the CMMC Final Rule, took effect.

Your top CMMC Questions Answered

How much does CMMC cost? That will depend on multiple factors, including the CMMC level and the complexity of the Organization Seeking Certification (OSC).

Is self-certification allowed? Yes, self-certification is permitted for CMMC Level 1 and a subset of Level 2 organizations. This must be renewed annually.

Who performs the CMMC assessment? For applicable Level 2 compliance, assessments are conducted by authorized third-party assessors like NSF. Level 3 assessments are performed by the DoW through the Defense Contract Management Agency (DCMA) or the Defense Counterintelligence and Security Agency (DCSA).

How long does the certification process take? Timelines depend on your organization's complexity and the required CMMC level. Make sure you factor in plenty of time, as we estimate that it will take most organizations at least six months to prepare.

What happens if I fail an assessment? You will have 180 days to close out Plan of Action & Milestones (POA&M) requirements as permitted in §170.21(a)(2) for reassessment. Assessors cannot provide recommendations related to any findings.

CMMC Glossary of Terms

CMMC: Cybersecurity Maturity Model Certification.

DoW: Department of Defense. Responsible for overseeing government agencies and functions related to national security and the U.S. Armed Forces, which include the Army, Navy, Marine Corps, Air Force and entities such as Space Force, the U.S. Coast Guard and the National Guard. In 2025, this was renamed the "Department of War" (DoW).

CUI: Controlled Unclassified Information. A safeguarding system for information that, although not considered "classified," is still sensitive and requires protection.

DIB: Defense Industrial Base. The worldwide industrial complex that supports R&D, design, production, delivery, and maintenance of military weapons systems, subsystems, and components or parts.

C3PAO: CMMC Third-Party Assessor Organization. An organization (NSF is one of them) authorized by the CMMC Accreditation Body (CMMC-AB) to conduct assessments that evaluate a contractor's cybersecurity maturity.

DFARS: Defense Federal Acquisition Supplement. A set of additional requirements for contractors working with the Department of War, supplementing the Federal Acquisition Regulation (FAR).

FCI: Federal Classified Information. Non-public information provided by or generated for the Federal Government under a contract.

DIBCAC: Defense Industrial Base Cybersecurity Assessment Center. A Department of War organization focused on evaluating contractors' cybersecurity protections.

DIBCAC assessment: A comprehensive review of an organization's cybersecurity infrastructure to identify weaknesses and recommend improvements.

POAMs: Plans of Action and Milestones. A document outlining tasks to be completed, resources needed, milestones, and deadlines for achieving cybersecurity goals.

False Start: Failure to pass the Phase 1 pre-assessment step required for DIB contractors pursuing Level 2 CMMC certification. This must be passed before an organization can move to the Phase 2 CMMC assessment.

Why Choose NSF for CMMC Certification?

Organizations are recommended to start their preparations for CMMC compliance as early as possible, not only to have enough time to address challenges, but also to secure an assessment date and avoid bottlenecks as C3PAOs start to fill their calendars.

As an authorized C3PAO, NSF is here to support you through this process from assessment to certification. We are listed in the CyberAB Marketplace and we are ready to work with organizations of all sizes.

Four reasons to choose NSF for your CMMC compliance:

- **Dedicated professionals.** Our team includes several Lead CMMC Certified Assessors (CCAs), and CMMC Certified Professionals (CCPs).
- **Auditing know-how.** Our assessors are fully qualified lead auditors for ISO/IEC 27001 and NIST 800-171.
- **Information security expertise.** In addition to CMMC, we provide certifications for ISO/IEC 27001 and NIST 800-171—the frameworks that form the foundation of CMMC—as well as ISO/IEC 20000-1 and CSA STAR.
- **Independent accreditation.** We are accredited to ISO/IEC 17021, certifying the competence, consistency and impartiality of our auditing services, and hold ISO/IEC 27001 certification, the international standard for information security management systems.

We can also deliver additional services, such as an information security gap assessment to help you understand the areas where you may need to build resilience.

For a complete overview of our information security services, visit nsf.org

NSF
789 N. Dixboro Road Ann Arbor, MI 48105 USA
www.nsf.org

NSF.ORG