Main Sail's

CMMC 2.0 GUIDE

Everything you should know to effectively
prepare for Cybersecurity Maturity
Model Certification 2.0

Main Sail's CMMC 2.0 Guide

Are you trying to navigate the DoD's Cybersecurity Maturity Model Certification (CMMC) 2.0 requirements?

Your organization is not the only one which may need some guidance and assistance with the changes announced on November 4, 2021. CMMC 1.0 was originally implemented by the DoD in January of 2020 as the cybersecurity certification requirement for DoD contractors going forward. It heavily relies on NIST National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, and CMMC 2.0 will heavily rely on it as well.

Main Sail's CMMC 2.0 Guide will provide you with excellent information including:

- Defining CMMC 2.0 and the proposed changes made on November 4, 2021
- Context into the creation of and revisions to CMMC 2.0
- Defining Controlled Unclassified Information (CUI)
- Relationship between CMMC 2.0 and NIST SP 800-171
- The three proposed CMMC 2.0 levels
- Why you should move forward with your implementation of NIST SP 800-171 now
- The benefits of working with Main Sail to assist with your implementation of NIST SP 800-171 and prep for CMMC 2.0 when approved

Main Sail's CMMC 2.0 Preparedness Assessment can get you on track for your CMMC 2.0 Certified Third-Party Assessment or self-assessment!

Our team of experts has 30+ years of experience in the areas of IT Audit, IT Compliance, Cybersecurity, and Remediation. We hope you find our guide helpful and informative. Please feel free to contact us if you have any questions.

About Us

Main Sail, LLC is an ISO 9001:2015 Certified, Veteran-Owned Small Business, providing a wide range of business services to commercial and government clients, centered on the latest enterprise technologies, process improvement, and management disciplines.

Questions?
We're here to help.

Contact us to set up a free consultation today!
mainsail@mainsailgroup.com
216-472-5100

Main Sail's

CMMC 2.0 Guide

CMMC 2.0 & NIST SP 800-171 Guide

Everything you should know to effectively prepare for Cybersecurity Maturity Model Certification

There is a lot of buzz regarding the CMMC Certification Process. You may be wondering:

- What are the new CMMC 2.0 changes?
- What are the next steps in the certification process?
- How does NIST SP 800-171 factor into the process?

Small and mid-sized organizations may find themselves overwhelmed with how to reach CMMC 2.0 compliance. Main Sail is here to support you by providing consultative services to get you on track.

The requirement to implement the 110 cybersecurity controls in NIST SP 800-171 has been in place since the end of 2017. Because the DoD wasn't aggressive in enforcing it, most contractors need to catch up to where they should have already been by 2017. This fact is regardless of the announcement about CMMC 2.0.

The updates in CMMC 2.0 are intended to make the process more streamlined, reliable, and flexible.

What is CMMC 2.0?

According to the Office of the Under Secretary of Defense for Acquisition & Sustainment, CMMC 2.0 is a unifying standard for the implementation of cybersecurity across the Defense Industrial Base (DIB). The framework includes a comprehensive and scalable certification element to verify the implementation of processes and practices associated with the achievement of a cybersecurity maturity level. CMMC 2.0 is designed to provide increased assurance to the Department that a DIB company can adequately protect sensitive unclassified information, including information flow down to subcontractors in a multi-tier supply chain.

In November 2021, the Department announced CMMC 2.0, an updated program structure and requirements designed to achieve the primary goals of the internal review:

- Safeguard sensitive information to enable and protect the warfighter
- Dynamically enhance DIB cybersecurity to meet evolving threats
- Ensure accountability while minimizing barriers to compliance with DoD requirements
- Contribute towards instilling a collaborative culture of cybersecurity and cyber resilience
- Maintain public trust through high professional and ethical standards

Main Sail Cybersecurity
mainsail@mainsailgroup.com
www.mainsailgroup.com
216-472-5100

CMMC Implementation

The CMMC 2.0 proposed approval process will take between 9-24 months from November of 2021.

However, your organization needs to work toward NIST SP 800-171 compliancy regardless of this approval timeline.

Don't wait - get your organization NIST SP 800-171 compliant. NIST SP 800-171 compliance will not only meet the DoD requirements, but your organization will also reduce exploitable vulnerabilities by following the framework NOW.

NIST SP 800-171 provides best practices and processes, and can be an integral part of your overall cybersecurity plan. In addition to meeting the DoD requirements, NIST SP 800-171 will help reduce the risk of cybersecurity breaches.

Below are some stats on the critical state of cybersecurity:

Every minute, **$3.0+** million is lost to cybercrime

As of 2021, the average cost of a data breach was **$4.42** million

The average time to identify and contain a breach in 2020 was a staggering **280** days

Phishing attacks account for more than **80%** of reported security incidents

92% of malware is delivered by email

The US has the world's highest data breach costs, with the average attack costing **$8.6** million

Cybercrime is projected to cost the world **$10.5** trillion annually by 2025

Main Sail Cybersecurity
mainsail@mainsailgroup.com
www.mainsailgroup.com
216-472-5100

MAIN sail®

Why Was CMMC Created?

The key reason behind CMMC 2.0 is protection of Controlled Unclassified Information (CUI). CUI is government created or owned information that requires safeguarding or dissemination controls consistent with applicable laws, regulations, and government wide policies.

CUI *is not* classified information. It is *not* corporate intellectual property unless created for or included in requirements related to a government contract. Because there are fewer controls over CUI compared to classified information, CUI is the path of least resistance for adversaries. Loss of aggregated CUI is one of the most significant risks to national security.

CHECK OUT THIS CUI

REFERENCE GUIDE

FOR MORE INFO

All defense contractors, large and small, will be required to implement cybersecurity controls and be third-party or self-assessed.

A perfect 100% assessment score of the implementation of the appropriate CMMC 2.0 level controls will be required for certification by the CMMC-AB, meaning that contractors will not be able to delay the implementation of controls, as they can now.

DFARS Clause 252.204-7012 and NIST SP 800-171 cybersecurity requirements for primes and subcontractors are mandatory.

CMMC 2.0 and NIST SP 800-171

Before getting into more details about CMMC 2.0, here is some information about NIST SP 800-171 and how the DoD's requirements evolved into CMMC. 2.0 This will give you more context on the differences between NIST SP 800-171 and CMMC 2.0.

NIST SP 800-171 was developed in response to the Federal Information Security Management Act. Both NIST SP 800-171 and CMMC 2.0 protect CUI.

Background of NIST SP 800-171

DFARS Clause 252.204-7012 mandated that government contractors must implement NIST SP 800-171 to protect sensitive, but unclassified information. Flowdown of this requirement from prime contractors to sub-contractors meant that most companies doing business with the government were to implement NIST SP 800-171. However, the lack of compliance with this mandate led the DoD to release CMMC in an effort to combat this issue through the use of third-party assessments.

NIST SP 800-171 contains the recommended security requirements for protecting the confidentiality of CUI in nonfederal systems and organizations. This framework designates basic and derived requirements. The basic security requirements are obtained from FIPS 200, which provides the high-level and fundamental security requirements for federal information and systems. The derived security requirements, which supplement the basic security requirements, are taken from the security controls in NIST SP 800-53. These security requirements are tailored to eliminate the requirements that are uniquely federal, not directly related to protecting the confidentiality of CUI, or are expected to be routinely satisfied by non-federal organizations without specification. This is where NIST SP 800-171 comes from.

The NIST SP 800-171 Control Families consist of: Access Control, Audit and Accountability, Awareness and Training, Configuration Management, Identification and Authentication, Incident Response, Maintenance, Media Protection, Personnel Security, Physical Protection, Risk Assessment, Security Assessment, System and Information Integrity, and Systems and Communications Protection.

CMMC 2.0 Level 2 includes all 110 requirements that originate from NIST SP 800-171, with the intent that CMMC 2.0 will replace the requirement of compliance with NIST SP 800-171 when the rulemaking process is complete. By leveraging the work that's already been done to implement NIST SP 800-171, contractors will be set up for success when CMMC 2.0 rulemaking is complete.

Main Sail's

CMMC 2.0 Guide

The Three CMMC 2.0 Levels

In November 2021, the DoD released CMMC 2.0, which replaces CMMC 1.0.

CMMC 2.0 Level 1: 17 practices (mapped to Federal Acquisition Regulation (FAR) 52.204-21)

CMMC 2.0 Level 2: 110 practices (aligned with the 110 controls from NIST SP 800-171)

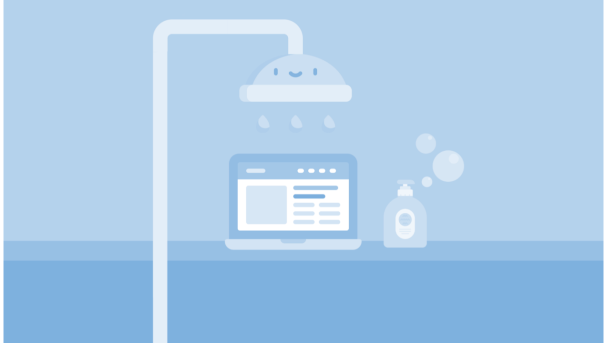
CMMC 2.0 Level 3: 110+ practices (based on NIST SP 800-172). Currently still under development.

Foundational (Level 1): Basic Cyber Hygiene

An organization must demonstrate the very basics of cybersecurity in the form of consistent practices for protecting Federal Contract Information (FCI). For example, using antivirus software or requiring employee password changes on a regular basis. Level 1 is certified through annual self-assessments.

Advanced (Level 2): Good Cyber Hygiene

An organization has an institutionalized management plan in place to implement and maintain best practices for protecting CUI, including all NIST SP 800-171 Revision 2 requirements. Level 2 is certified through triennial third-party assessments for critical national security information or annual self-assessments for select programs.



Expert (Level 3): Advanced Cybersecurity Program

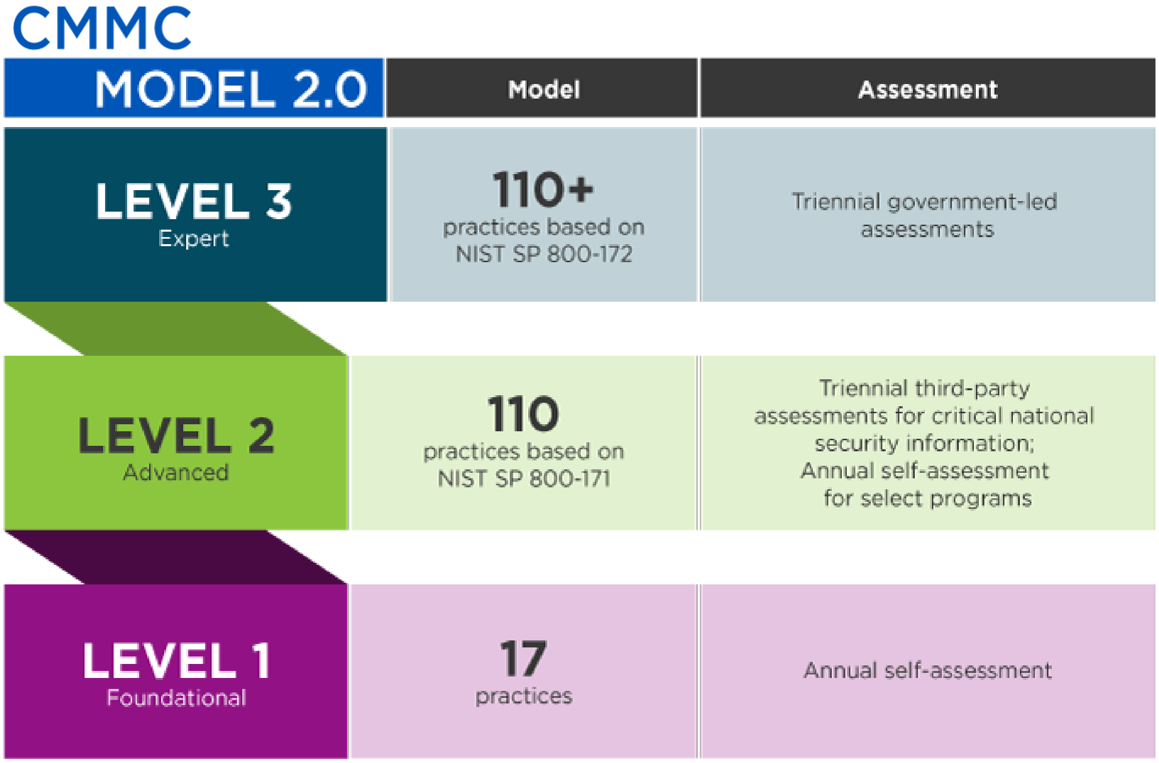
An organization must achieve organization-wide standardization, implementation, and optimization of its cybersecurity management plan, processes, and best practices. Level 3 is still under development, but includes continual improvement type and enhanced process for identifying and combating APTs. Level 3 is certified through triennial government-led assessments.

Main Sail Cybersecurity
mainsail@mainsailgroup.com
www.mainsailgroup.com
216-472-5100

MAIN sail®

The CMMC 2.0 Levels

Organizations handling very basic information will only need to achieve Level 1 certification. For others who are handling CUI, the process is more involved. These contractors will need to achieve at least CMMC level 2. Below are more details on the 3 CMMC levels:



CMMC MODEL 2.0	Model	Assessment
LEVEL 3 Expert	110+ practices based on NIST SP 800-172	Triennial government-led assessments
LEVEL 2 Advanced	110 practices based on NIST SP 800-171	Triennial third-party assessments for critical national security information; Annual self-assessment for select programs
LEVEL 1 Foundational	17 practices	Annual self-assessment

What Do I Need to Do to Prepare?

The preparation for the assessment can be overwhelming, requires your organization to gather a great deal of documentation, and will also require interviewing several members of your team across the organization. You will also need to work with your suppliers and contractors during the course of your prep work to gather information and documentation. Conducting your own preparation could take months. Don't worry, your NIST SP 800-171 compliance efforts will not go to waste.

Tapping our expertise gained from our 30 years of experience will enable you to quickly and efficiently comply with requirements and pass any assessment in a cost effective manner.

CMMC 2.0 is still an evolving model, but there is a practical and efficient way to move beyond product vendor promises and follow a strategy that guarantees long term success.

Main Sail's

CMMC 2.0 Guide

Preparing for CMMC 2.0

Main Sail can help your organization prepare for your assessment utilizing our CMMC 2.0 Preparedness Assessment services offering. Our methodology is outlined below.

- How to leverage your NIST SP 800-171 compliance efforts in preparation for CMMC 2.0
- The relationship between NIST SP 800-171 and CMMC 2.0
- What your System Security Plan (SSP) should include
- What Plan of Action & Milestones (POAM) are and how they are best utilized
- How the requirements can be implemented in a way that enables CMMC 2.0 validation
- Interviewing the key stakeholders
- Review of your cybersecurity practices, procedures and posture
- Penetration Testing
- Assistance with remediation of areas of concern
- Applying our best practices from 30+ years of experience with IT Audit, Compliance, and Cybersecurity
- Full documentation of our findings

Even if you are not currently a DoD contractor, passing the CMMC 2.0 assessment is a good business practice for improving your cybersecurity posture. It will guide you to put into place good cyber hygiene practices which include the building blocks of People, Process, and Technology.

PROCESS

PEOPLE

TECHNOLOGY

Main Sail Cybersecurity
mainsail@mainsailgroup.com
www.mainsailgroup.com
216-472-5100

Main Sail's

CMMC 2.0 Guide

People, Process, and Technology

What is Meant by
People, Process, and Technology?

With cybersecurity, the reference to People, Process, and Technology is used to summarize the best practices, skills, and tools needed to build and maintain good cyber hygiene.

People:

Are your People prepared for cybersecurity breaches and do they have the ability to recognize potential threats? Do they understand and utilize the processes and technology in place to prevent attacks? Do they have access to training for recognizing potential threats?

Process:

What is the Process to prevent breaches in the first place? What is the process once a breach occurs? Is the plan well formulated and documented? Does the organization have a complete understanding of the IT environment overall? What is the vendor team in place to help respond to cybersecurity events?

Technology:

There are hundreds of Technology solutions in the marketplace that address cybersecurity. Some essentials include anti-virus, malware protection, firewalls, SIEM tools, multi-factor authentication, identity and access management, and training tools among others. Needless to say there are several factors to consider before investing in technology.

Main Sail offers a holistic approach to assist you with your preparation for NIST SP 800-171 compliance and CMMC 2.0 assessment. We also partner with an ecosystem of solutions partners with best-in-class products and services you may need to assist with and meet your NIST SP 800-171 and CMMC 2.0 requirements.

Please contact us at mainsail@mainsailgroup.com for more information and a free consultation!

Main Sail Cybersecurity
mainsail@mainsailgroup.com
www.mainsailgroup.com
216-472-5100