NetworkTitan

GUIDE TO CMMC 2.0 COMPLIANCE

April 2025

www.NetworkTitan.com
619-255-2621

NetworkTitan

Table of Contents

About the Author:

Mike Hughes, CMMC Registered Practitioner, is the Founder and President of Network Titan, LLC. Since 2006, Mike has been providing top-tier IT Support and Cybersecurity Services to Southern California small and medium sized businesses and government contractors. Mike explains his success has been built on a 'customer first' approach and retaining highly skilled teams with the utmost integrity. Mike's experience supporting clients with NIST compliance and CMMC dates back to their infancy in government contracting and he is considered to be one of the top CMMC compliancy experts in the field.

He can be reached at mike@NetworkTitan.com and 619-255-2621.

NetworkTitan

Introduction

The Cybersecurity Maturity Model Certification 2.0 (CMMC) continues to evolve since the initial version was introduced in November of 2020. The Department of Defense (DoD) has even since dropped the "2.0" tag, but what hasn't changed is the primary goal of the program; to protect the DoD from cyber damage at the hands of the DIB (Defense Industrial Base) – specifically the hands of DoD suppliers and subcontractors (non-federal entities) while they 'handle' sensitive government information in the course of doing business. In essence, the goal is to protect the entire DIB from rising security threats and highly sophisticated cyber attacks so that the DoD, and the warfighter, are ultimately protected.

It's incumbent upon everyone in the DIB, at any level, to understand cyber risks, remediate and migrate toward compliance today. Actually, yesterday. CMMC provides a framework for accountability – not always crystal clear – but a roadmap to better protecting FCI (Federal Contract Information) and CUI (Controlled Unclassified Information). And although CMMC is currently being phased in, it is closer than it's ever been. It is recommended everyone in the DIB supply chain work to attain compliance now.

As a Cybersecurity and Managed IT Service Provider (MSP), our goal is to simplify the complexities of CMMC compliance for our customers. This Guide will give you a basic understanding of CMMC 2.0 and steps your organization can take now toward reaching compliance.

Be sure to take a look at the Abbreviations and Resources in this Guide and, if your organization qualifies, take advantage of our comprehensive CMMC Readiness Check.

What Is CMMC 2.0 And Who Needs It?

CMMC is a certification program for organizations in the government supply chain requiring compliance with a set of unified information security standards and best practices to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI).

CMMC 2.0 has streamlined security requirements into 3 distinctly different and progressive "levels" based on the security requirements from FAR 52.204.12, *Basic Safeguarding of Covered Contractor Information Systems*, NIST SP 800-171 r2, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, and a subset of the requirements from NIST SP 800-172, *Enhanced Security Requirements for Protecting Controlled Unclassified Information: A supplement to NIST SP 800-171* which demonstrate that an organization has implemented the defined cybersecurity practices. At each level, the number of best practices and requirements increase. The level (1, 2 or 3) your organization needs to attain will be specified in a solicitation or RFI (Request For Information). We can help you determine your "level." It will be based on the type of information you handle and the type of contract vehicles you participate in. It goes without saying that ANY organization can benefit from CMMC compliance, but most companies will fall into Level 1 or Level 2.

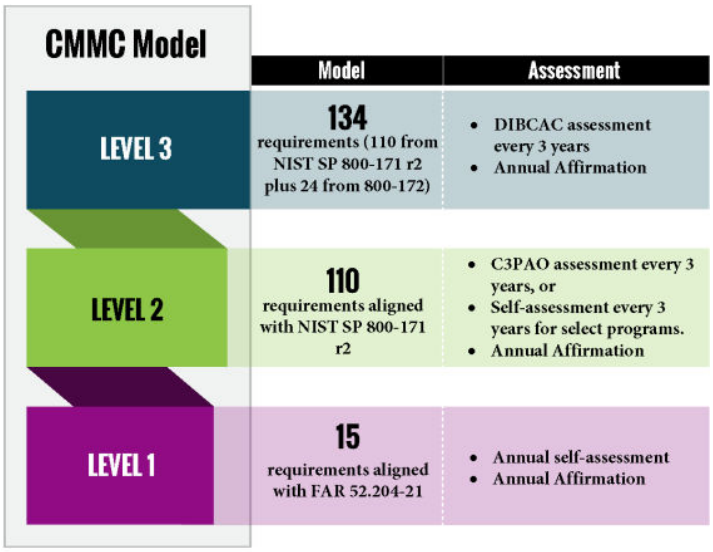
CMMC 2.0 Levels

The practices and protocols for each CMMC Level are cumulative. To demonstrate achievement at any Level, you must also demonstrate achievement of the preceding lower Level. All levels require annual affirmation.

Level 1: Foundational. Contractors can securely handle (process, store or transmit) FCI (Federal Contract Information), have implemented the 15 defined cybersecurity practices in the "Far Clause" (CFR 52.204.-21), and will conduct annual self-assessments.

Level 2: Advanced. Contractors can securely handle CUI (Controlled Unclassified Information), have implemented the 110 defined cybersecurity requirements specified in NIST SP-800-171 r2 and additionally, every 3 years, must conduct a 3rd Party Assessment from a certified C3PAO (3rd Party Assessor Organization) unless they fit into an "non-prioritized acquisitions" exception.

Level 3: Expert. Contractors can securely handle highly sensitive information critical to national security, have implemented the 110 defined cybersecurity requirements in Level 2 plus further controls from NIST 800-172, and additionally, every 3 years they must undergo a DIBCAC assessment.



When Will I Need To Comply?

Network Titan has been actively supporting the CMMC mandate and NIST 800-171 for clients since the beginning, prior to 2016. The stop-and-go journey has finally become solidified and there is a phased in timeline for compliance. It's past time to get your CMMC efforts organized for contracts and awards.

CMMC compliance will be phased in over a 3-year time frame with full implementation by 2028. Businesses in the supply chain need to be hyper-focused compliance *today*.

What About Subcontractors?

If a subcontractor provides their products or services to a government contractor, they too, will need to comply with CMMC protocols. The "flow down" of DFARS clause 252.204-7012 puts an additional burden on prime contractors to confirm their subs also comply with CMMC.

Meeting the CMMC compliance requirements will demonstrate a sub's "suitability" as a partner with prime contractors. Some Primes are already requiring CMMC readiness from their Subs. Meeting CMMC requirements creates a greater demand for your products or services in the marketplace.

What Is Self-Attestation or Self-Assessment?

Required for Level 1 and a sub-set of Level 2, Self-Attestation is a comprehensive report, affirmed by a senior company official, which contains the findings of a self-assessment. This document verifies and validates that a company is meeting and has fulfilled the objectives of the CMMC Level 1 practices (and protection of FCI). NIST 800-171A describes various assessment methods which can be utilized in a self-assessment to determine if a contractor meets the intent of all Level 1 practices with a "MET" or "NOT APPLICABLE" finding.

What Is The False Claims Act and The Civil Cyber-Fraud Initiative?

The Department of Justice created the Civil Cyber-Fraud Initiative in 2021 to combat new and evolving cyber threats. Combined with the False Claims Act (aka the "Lincoln Law," which is the Fed's primary litigation tool against persons and companies that defraud the government), the Civil Cyber-Fraud Initiative allows the government to impose hefty fines in cases where an organization misrepresents their cybersecurity practices or knowingly violates obligations to monitor and report cybersecurity incidents and breaches. ***Settlements and judgements, as of January 2025, have exceeded $2.9 billion!*** This means defense contractors must have the data and documentation to prove comprehensive cybersecurity practices and protocols are in place including accurate System Security Plans and Plans of Actions and Milestones.

How Long Will It Take To Become Compliant?

Your company size, complexity and current cybersecurity stance are only a few of the many factors that affect how long it will take to you become CMMC 2.0 compliant. It would not be unusual for the process to take many months to over a year to complete. You can become compliant and *additionally* get "Certified" after a C3PAO conducts an assessment. Currently there are only about 60 to 70 C3PAOs in the world that are certified, so there may be a backlog as contractors race toward certification. If you are unsure of where your organization stands, it is recommended to get an objective, external readiness assessment.

How Much Will It Cost?

Way back in 2020, Katie Arrington, current DoD CISO, estimated that C3PAOs would charge $3,000 to $4,000 to assess and certify compliance at the previous CMMC 1.0 Level 1 (keep in mind she was not estimating the cost *to become* compliant but rather what C3PAO's would charge to certify compliance). Today that figure doesn't apply. The cost to become compliant is not fixed and varies significantly based on many factors including:

- The CMMC level being pursued: Higher levels require more stringent controls and therefore involve greater costs.
- The size and complexity or your organization: Larger organizations with multiple locations and more complex IT infrastructures will face higher costs.
- Your current Cybersecurity stance: Companies that already have strong security "maturity," aligned with NIST 800-171, will likely have lower certification costs.

Network Titan can give you guidance on costs based on your unique factors. The time and resources needed for self-assessments, documentation, and implementation of security requirements all factor into pricing for an organization to become compliant. Also important to understand is that compliancy is an ongoing effort, not a one-and-done exercise. Maintaining compliance requires ongoing maintenance. Partnering with a reputable, experienced Managed Service Provider can help keep your organization in compliance year after year.

The reality is that if an organization wants to continue to do business with the government, in *any* capacity in the supply chain, CMMC is not optional, **compliance is mandatory**. A company will either be compliant or not. It is incredibly important to get organized now and to systematically review and improve every internal IT process to be prepared for certification.

Where Is CMMC Headed Now?

CMMC 3.0 is likely on its way as we speak, as maintaining cyber security at all levels is a fluid and dynamic effort. Feedback from the DIB and findings from C3PAO audits will drive additional revisions to the current CMMC 2.0 framework. Public comments for NIST SP 800-171 revision 3 are closed (Revision 2 currently supersedes ALL versions per DFARS 252.204-7012 DEVIATION 2024-O0013), but any changes will only build upon current the controls and practices.

Self-Assessments are probably on the way out as the DoD moves to a more verifiable system of compliance through 3rd party assessments. The focus will be on "maturity" and assessors will look for evidence that an organization has consistently managed required security controls, not just that they can pass a test at a specific moment.

CMMC will need to evolve to keep pace with the ever-changing cyber threat landscape, most likely with updates to framework security controls, integrating with other security frameworks and adding zero-trust principles.

What Is A SPRS Score?

The Supplier Performance Risk System (often pronounced like a cowboy's 'spurs') uses statistical algorithms to provide contracting officials a score for the overall assessment of a supplier's performance and risk. Using this "Supplier Risk Score," contracting officials can identify "high risk" suppliers.

DoD suppliers are responsible for entering their Assessment Methodology score into the SPRS website (scores range between -203 and +110). A supplier must have a CAGE Code, complete a NIST SP 800-171 DoD Assessment Methodology and an SSP, prior to logging on to enter their results of a self-assessment.

After a contractor successfully enters their score, the SPRS website provides storage and retrieval for the NIST SP 800-171 assessment results. Suppliers can view and update their company information and address potential inaccuracies.

What Steps Should You Be Taking Now

1. Get an unbiased CMMC Readiness Check / IT Risk Assessment.
2. Evaluate your current cybersecurity tools and technologies.
3. Create or update your SSP (Security System Plan).
4. Implement authentication / encryption / monitoring.

Network Titan's Process Gets You Ready for Certification

1. We perform a detailed analysis of your current environment and cybersecurity practices.
2. We identify deficiencies within the CMMC framework that will prevent compliance.
3. We explain and clarify the exact remediation steps needed to achieve compliance based on your required certification level and current cybersecurity stance.
4. We implement all technical requirements you need for compliance *prior* to hiring a C3PAO for CMMC assessment and certification.

Get An Unbiased CMMC Readiness Check from Network Titan

Network Titan can assist you to determine "where" you are now in the CMMC 2.0 readiness process, including exactly what you will need to become compliant and then lead you there.

Certification is conducted by a C3PAO. This 3rd Party Assessor Organization does not assist you in *becoming compliant*, they merely certify that you are (or aren't). Of course, you can pay them to conduct a certification, however if you fail, you are left in the same position as when you started, except, of course, for the fees you paid to them.

For more information and to discuss your unique situation, contact Network Titan at 619-255-2621. Or go to www.NetworkTitan.com/cmmc

What Is An SSP?

A System Security Plan is a step-by-step process guide that describes how your organization protects FCI and CUI to reduce cybersecurity risks. It is a requirement for all levels of CMMC 2.0.

An SSP is a document that describes how an organization meets the security requirements for a system or how an organization plans to meet the requirements. In particular, the SSP describes the system boundary; the environment in which the system operates; how the security requirements are implemented; and the relationships with or connections to other systems.

What Is a POA&M?

Plan of Action and Milestones. This document addresses and tracks progress on certain CMMC requirements that your company hasn't achieved yet (weaknesses), but will "within a clearly defined timeline," so you can still perform on a contract.

A POA&M is not an excuse for security shortfalls. Covering all requirements for full CMMC compliance, at any level, is an ongoing, company-wide effort that requires systematic review and remediation. The POA&M provides your company with documentation on necessary tasks to achieve compliance on a particular security control or "weakness" as identified by an internal review or outside auditor. Importantly, each task includes who is responsible and a completion date for the corrective action. Milestones further help to manage corrective actions in phases until the security control is achieved.

The POA&M is considered a crucial document demonstrating your commitment to secure your information systems. The POA&M, like the SSP, is a living document that is continually in use, updated and revised.

What Is FCI?

As defined in the "FAR Clause" 52.204.21 Basic Safeguarding of Covered Contractor Information

> *Federal contract information* means 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, but not including information provided by the Government to the public (such as on public websites) or simple transactional information, such as necessary to process payments.

Basically, FCI is any information from the Government provided in a contract. Therefore, any supplier that has been awarded a contract or participates in one, is required to protect FCI using the defined safeguards in the FAR Clause which correspond to the controls of CMMC 2.0 Level 1.

What Is CUI?

As defined by the National Archives and Records Administration (NARA) About Controlled Unclassified Information (CUI)

> Controlled Unclassified Information (CUI) is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended.

CUI falls into various groups, categories and subcategories. While working within the government supply chain, it's necessary to use, store, generate and share information that requires some level of protection from unauthorized access or release. Defining the CUI your company uses and has access to, as well as how it is handled, is a very detailed and critical component of CMMC 2.0 Levels 2 and 3.

Examples of CUI for a DoD contractor - manufacturer:

Blueprints, engineering drawings, technical specifications or other data related to the design, production, build, assembly or repair of military equipment or systems.

Examples of CUI for a DoD contractor - aerospace:

Data collected during flight testing of military aircraft or drones, such as performance metrics, sensor readings, and system responses, as well as analysis and reports derived from this data.

NetworkTitan

Abbreviations

AC Access Control

AES Advanced Encryption Standard

API Application Programming Interface

APT Advanced Persistent Threat

C3PAO CMMC Third-Party Assessment Organization

CAGE Code Commercial And Government Entry

CIO Chief Information Officer

CIS Computer Information System

CMMC Cybersecurity Maturity Model Certification

CNC Computerized Numerical Control

CUI Controlled Unclassified Information

CTI Controlled Technical Information

CVE Common Vulnerabilities and Exposures

CWE Common Weakness Enumeration

DCISE DIB Collaborative Information Sharing Environment

DFARS Defense Federal Acquisition Regulation Supplement

DHC Device Health Check

DIB Defense Industrial Base

DIBCAC Defense Industrial Base Cybersecurity Assessment Center

DKIM Domain Key Identified Mail

DMARC Domain-based Message Authentication, Reporting, and Conformance

DNS Domain Name System

DNSSEC Domain Name System Security

DOD Department of Defense

ESP External Service Provider

FAR Federal Acquisition Regulation

FCI Federal Contract Information

FDDI Fiber Distributed Data Interface

FDE Full Disk Encryption

FedRAMP Federal Risk and Authorization Management Program

FIPS Federal Information Processing Standard

FTP File Transfer Protocol

IC3 Internet Crime Complaint Center

ICS Industrial Control Systems

IDS Intrusion Detection System

IIoT Industrial Internet of Things

IoT Internet of Things

IP Internet Protocol

IPSec Internet Protocol Security

ISAC Information Sharing and Analysis Center

ISDN Integrated Services Digital Network

LAN Local Area Network

MAC Media Access Control

MDM Mobile Device Management

MEP Manufacturing Extension Partnership

MFA Multifactor Authentication

NARA National Archives and Records Administration

NAS Networked Attached Storage

NIST National Institute of Standards and Technology

NSA National Security Agency

Abbreviations (continued)

NTP Network Time Protocol

OMB Office of Management and Budget

OSA Organization Seeking Assessment

OSC Organization Seeking Certification

OT Operational Technology

PII Personal Identifiable Information

PIV Personal Identity Verification

PI Performance Information

PKI Public Key Infrastructure

PLC Programmable Logic Controller

POA&M Plan of Action & Milestones

RADIUS Remote Authentication Dial-in User Service

RMM Resilience Management Model

RM Risk Management

RPO Recovery Point Objectives

RPO Registered Provider Organization

RTO Recovery Time Objectives

SCADA Supervisory Control and Data Acquisition

SCRIM Supply Chain Risk Management

SI System and Information Integrity

SIEM Security Integration and Event Management

SMS Short Message Service

SOC Security Operations Center

SPF Sender Policy Framework

SPRS Supplier Performance Risk System

SSC Secure Socket Layer

SSP System Security Plan

SP Special Publication

TLS Transport Layer Security

URL Universal Resource Locator (aka Uniform Resource Locator)

UTC Coordinated Universal Time

VLAN Virtual Local Area Network

VoIP Voice over Internet Protocol

VPN Virtual Private Network

WAP Wireless Access Point

WPA2-PSK WiFi Protected Access-Pre-shared Key

RESOURCES

What is CMMC https://dodcio.defense.gov/CMMC/

NIST SP 800-171 Assessment Methodology Version 1.2.1 https://www.acquisition.gov/dfars/252.204-7020-nist-sp-800-171dod-assessment-requirements.

FAR Clause 52.204.21 https://www.acquisition.gov/far/52.204-21?searchTerms=204.21

Self-Assessments https://dodcio.defense.gov/CMMC/Assessments/

Supplier Performance Risk System (SPRS) FAQs https://www.sprs.csd.disa.mil/faqs.htm