Do I Need Cybersecurity Maturity Model Certification (CMMC) and Why?

Bit About Me

Peter Bagley
CISSP, CMMC- RP, CEH, CHFI,
ITIL, CCNA, Security +

- Retired Army after 21 years
- Defense Contractor – CACI, Tampa, FL
- College Professor – St. Petersburg College, St. Petersburg, FL
- Founder/Chief Information Officer (CIO) of B&B Cyber Solutions LLC
    - Cybersecurity Consulting/Training
    - Career Coaching
    - CMMC Support

What You'll Learn

1. The relationship between **FAR and DFARS** relating to CUI
2. **CMMC Ecosystem** - Cyber AB's role and purpose supporting CMMC
3. Explain the differences between the **NIST 800-171** Rev 2, 171A and NIST 800-172, 172A and how the Cyber AB (previously AB-CMMC) supports the program
4. The Cyber AB individual certification types RP, CCP, and CCA and organizations seeking certifications (OSCs) and CMMC Third-Party Assessment Organizations (C3PAOs)
5. CMMC certification process
6. Discuss the CMMC Levels 1 & 2 assessment process and the 14 NIST 800-171 controls
7. Steps to CMMC Readiness and the Supplier Performance Risk System (SPRS) process

FAR CLAUSE 52.204-21

- The original concept for basic cyber security across federal suppliers is contained in the Federal Acquisition Regulation (FAR) Clause 52.204-21. It has ***15 basic cybersecurity controls*** required to be implemented by a contractor as part of the contract award. The CMMC Level 1, basic FAR safeguards are translated to the 17 Level 1 practices.

- This will also support the protection of federal contract information (FCI).

FAR CLAUSE 52.204-21

FEDERAL ACQUISITION REGULATION (FAR) CLAUSE 52.204-21

BASIC SAFEGUARDING OF COVERED CONTRACTOR INFORMATION SYSTEMS

15 Basic Controls

- Limit access to authorized users, processes, or devices
- Limit access to the type of actions that authorized users are permitted to execute
- Identify information system users, processes, or devices
- Authenticate identities of users, processes, or devices prior to allowing access
- Escort visitors, monitor visitor activity, maintain audit logs of visitor activity, and control and manage physical access devices
- Verify and control (or limit) connections to external information systems
- Control information posted or processed on publicly accessible systems
- Sanitize or destroy media containing Federal Contract Information
- Limit physical access to information systems, equipment, and operating environment to authorized individuals
- Perform periodic scans of the system and real-time scans of files from external sources as files are downloaded, opened, or executed
- Monitor, control, and protect organizational communications
- Implement subnetworks for publicly accessible system components that are separated from internal networks
- Identify, report, and correct information and system flaws in a timely manner;
- Provide protection from malicious code
- Update malicious code protection mechanisms when new releases are available

DFARS 252.204.7012

- *"The **Defense Federal Acquisition Regulation Supplement (DFARS)** to the Federal Acquisition Regulation (FAR) is administered by the Department of Defense (DoD). The **DFARS implements and supplements the FAR.** The DFARS contains requirements of law, DoD-wide policies, delegations of FAR authorities, deviations from FAR requirements, and policies/procedures that have a significant effect on the public."*

DFARS 252.204.7012

DFARS Clause 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting

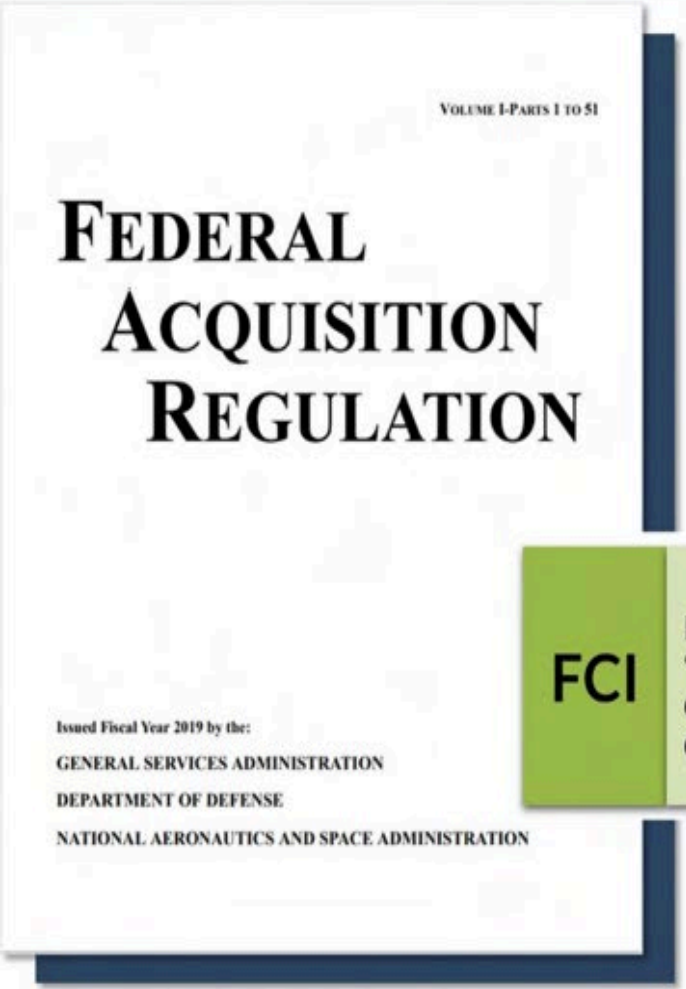
- (b)(2) For covered contractor information systems that are not part of an IT service or system operated on behalf of the Government and therefore are not subject to the security requirement specified at paragraph (b)(1) of this clause, the following security requirements apply:
  - **(i)** The covered contractor information system shall be subject to the security requirements in National Institute of Standards and Technology **(NIST) Special Publication (SP) 800-171**, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" (available via the internet at http://dx.doi.org/10.6028/NIST.SP.800-171) in effect at the time the solicitation is issued or as authorized by the Contracting Officer.

DFARS 252.204.7012

DFARS Clause 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting

- (b)(2) For covered contractor information systems that are not part of an IT service or system operated on behalf of the Government and therefore are not subject to the security requirement specified at paragraph (b)(1) of this clause, the following security requirements apply:
  - **(ii)(A)** The Contractor shall implement NIST SP 800-171, as soon as practical, but not later than December 31, 2017. For all contracts awarded prior to October 1, 2017, the Contractor shall notify the DoD CIO via email at osd.dibcsia@mail.mil **within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award.**

FEDERAL CONTRACT INFORMATION (FCI)


VOLUME I-PARTS 1 TO 51

FEDERAL ACQUISITION REGULATION

Issued Fiscal Year 2019 by the:

GENERAL SERVICES ADMINISTRATION

DEPARTMENT OF DEFENSE

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

Executive Branch contracts are primarily based around the **FAR (Federal Acquisition Regulations)**, which defines the legal and additional requirements necessary to do business with the Executive Branch.

FCI

FCI (Federal Contract Information) is defined as:
"Information, not intended for public release, provided by, or generated for the Government under a contract to develop or deliver a product or service to the Government"

CONTROLLED UNCLASSIFIED INFORMATION (CUI)

CUI

CUI (Controlled Unclassified Information is defined as:
"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."

Law, regulation, or Government-wide policy may require or permit safeguarding or dissemination controls in three ways:

- Requiring or permitting agencies to control or protect the information but providing no specific controls, which makes the information CUI Basic
- Requiring or permitting agencies to control or protect the information and providing specific controls for doing so, which makes the information CUI Specified
- Requiring or permitting agencies to control the information and specifying only some of those controls, which makes the information CUI Specified, but with CUI Basic controls where the authority does not specify

CMMC Program

- The CMMC program was initially launched as CMMC 1.0 in January 2020, but it was revised and updated to CMMC 2.0 in November 2021. The CMMC 2.0 program is the next iteration of the CMMC cybersecurity model.

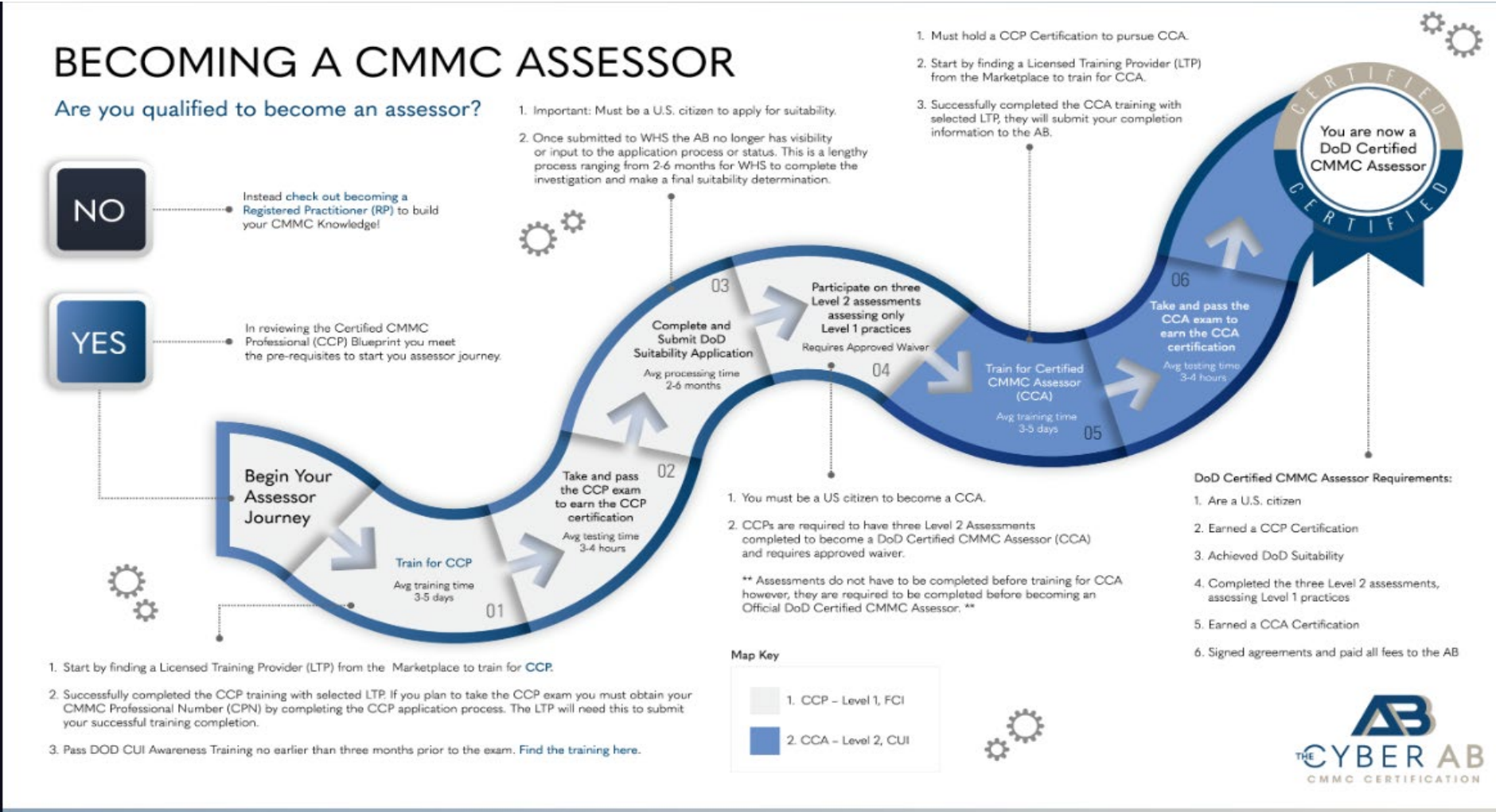
- The CMMC 2.0 program aims to simplify the compliance process, reduce the cost and burden for small and medium-sized businesses, and enhance the security posture of the Defense Industrial Base (DIB).

- The DoD mandates its implementation across the Defense Industrial Base, underlining its critical role in protecting sensitive information integral to national security.

The CMMC Ecosystem

The CMMC Ecosystem is designed as a decentralized program that fosters competition and cost reduction for OSCs. The CMMC Model is the core of the CMMC Ecosystem, defines the overall certification requirements, and covers a wide range of contractor types.

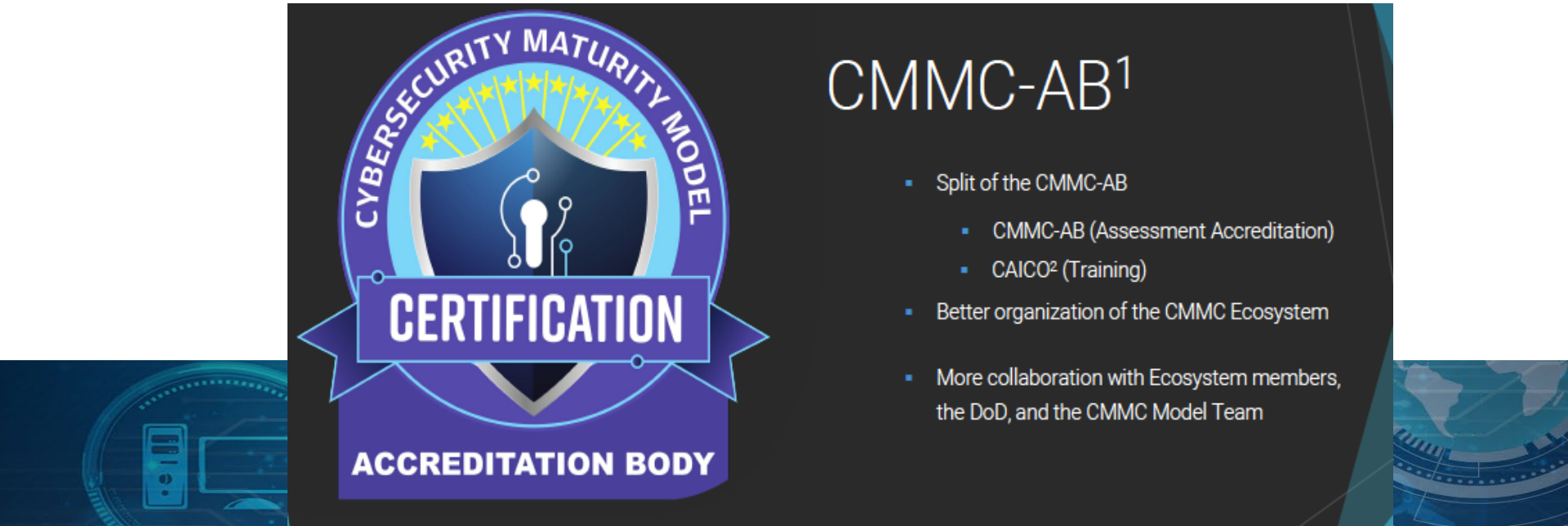
Cyber AB CMMC Assessor



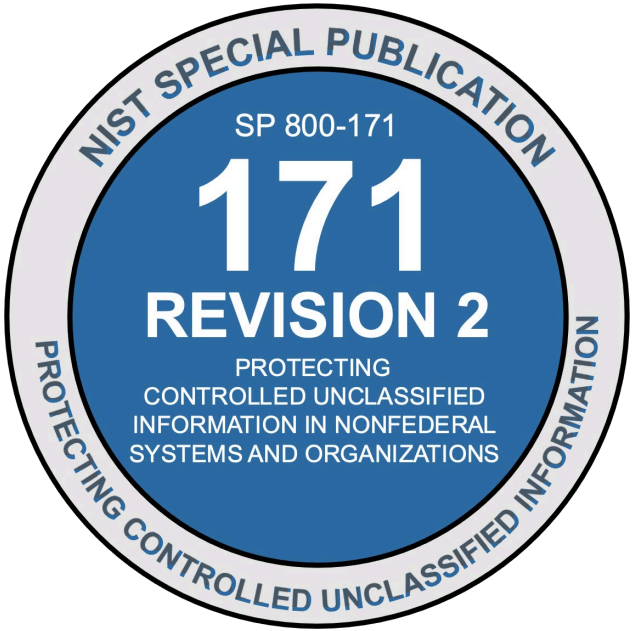
Cyber AB
CMMC Third-Party Assessment Organizations (C3PAOs)

- The Cyber AB is the official accreditation body of the CMMC Ecosystem and the sole authorized nongovernmental partner of the DoD in implementing and overseeing the CMMC conformance regime.

- The primary mission of the Cyber AB is to authorize and accredit the C3PAOs that conduct CMMC assessments of companies within the DIB. Manages the CMMC ecosystem for the DoD.



NIST SP 800-171 Rev. 2 vs. NIST SP 800-171A



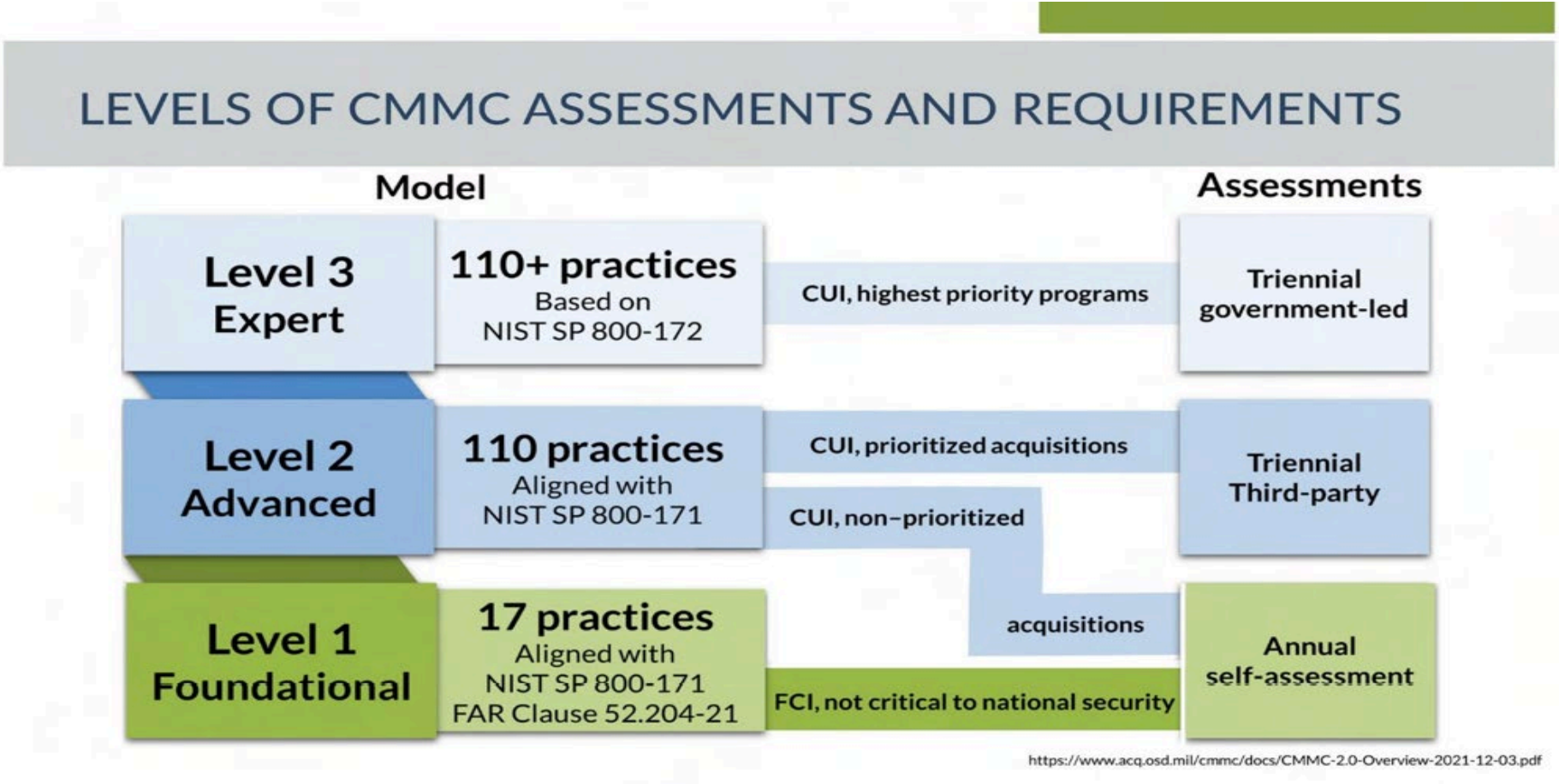
- 110 requirements

- 320 assessment objectives

CMMC Framework for NIST SP 800-171 Rev. 2 and NIST SP 800-172

The CMMC framework consists of the security requirements from ***NIST SP 800-171 Rev. 2 (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 Special Publication 800-171***). The framework is organized into domains, which map directly to the NIST SP 800-171 Rev. 2 families, and there are three levels within CMMC—Levels 1, 2, and 3.

CMMC Levels


LEVELS OF CMMC ASSESSMENTS AND REQUIREMENTS
Model
Assessments
Level 3
Expert
110+ practices
Based on
NIST SP 800-172
CUI, highest priority programs
Triennial
government-led
Level 2
Advanced
110 practices
Aligned with
NIST SP 800-171
CUI, prioritized acquisitions
CUI, non-prioritized
Triennial
Third-party
Level 1
Foundational
17 practices
Aligned with
NIST SP 800-171
FAR Clause 52.204-21
acquisitions
FCI, not critical to national security
Annual
self-assessment
https://www.acq.osd.mil/cmmc/docs/CMMC-2.0-Overview-2021-12-03.pdf

CMMC Models Structure

- ***Level 1: Basic***. This level covers the basic security requirements for protecting FCI, which is information not intended for public release. It is based on the 17 basic requirements from NIST SP 800-171.

- ***Level 2: Intermediate***. This level covers the intermediate security requirements for protecting CUI. The security objective at this level is to protect CUI from unauthorized disclosure, modification, or exfiltration. It is based on the 110 requirements from NIST SP 800-171 plus 21 additional practices from NIST SP 800-172.

- ***Level 3: Advanced***. This level covers the enhanced security requirements for protecting CUI that is associated with a critical program or a high-value asset. It is based on the 131 requirements from NIST SP 800-171 and 800-172 plus 34 additional practices from NIST SP 800-172. The expected threat at this level is from the advanced persistent threat or a comparable adversary who uses state-of-the-art tools and techniques.

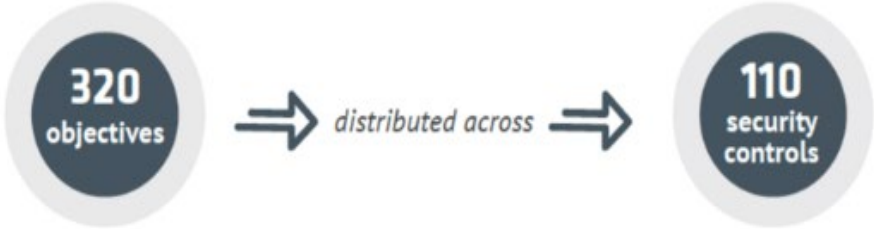
CMMC Level 1

CMMC Level 1 (Foundational): At Level 1, organizations must demonstrate performance of basic cyber hygiene practices to protect FCI.

Level 1 requirements are specified in FAR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems. That clause identifies 17 cyber hygiene practices distributed across six domains.

CMMC Level 2

NIST SP 800-171 assessors will review compliance with:



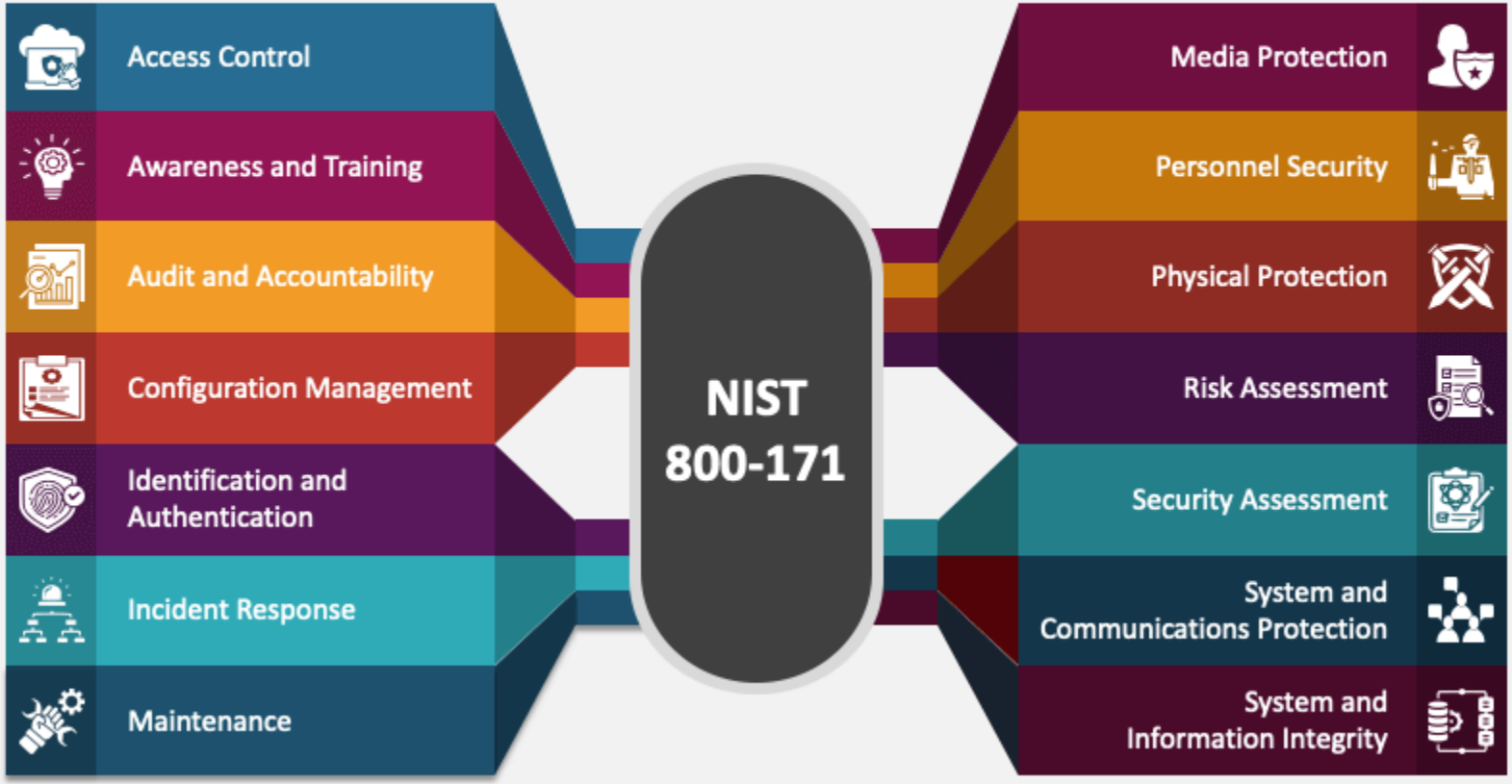
Each security control has anywhere from one to 15 objectives. Every *objective* associated with a *control* must be met for that control to be satisfied. For example:

CMMC Level 2: Requirements align with NIST SP 800-171, Protecting Controlled Unclassified Information [CUI] in Nonfederal Systems and Organizations.

NIST SP 800-171 identifies 110 cybersecurity controls distributed across 14 domains, including the six noted for Level 1 plus an additional eight domains.

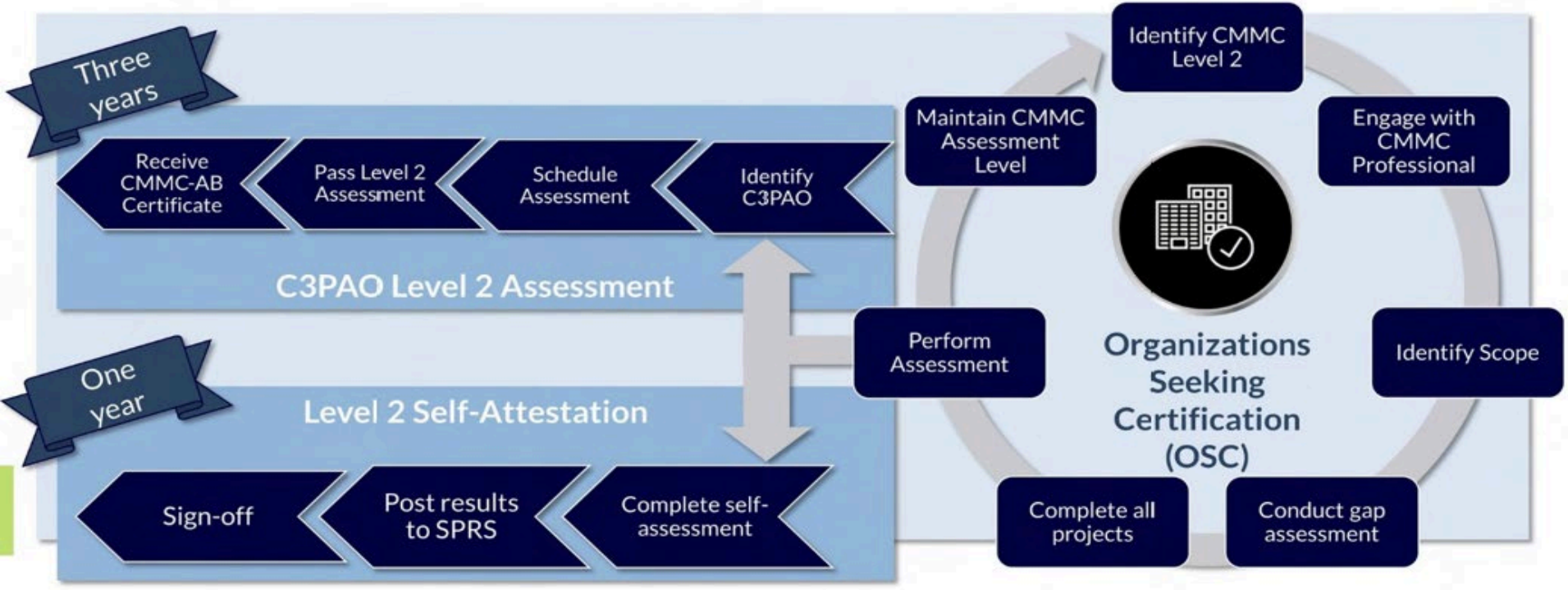
NIST 800-171

What are the NIST 800-171 Controls?



ORGANIZATIONS SEEKING CERTIFICATION (OSC) AT LEVEL 2

Purpose | Requirements | Benefits



5 Steps to CMMC Readiness

1. START PREPARING TODAY

Acting now is key to success. There is no standard time frame for how long the CMMC process takes. It may take smaller companies less time than a larger or more sophisticated organization. And depending upon what level criteria you must meet, putting together the required documentation, such as a gap analysis and Plan of Action and Milestones (POAM) (see more on this in step 5), can take six to nine months alone. If you fail the audit, you may be able to correct any deficiencies found in the assessment

2. CONDUCT A SELF-ASSESSMENT

To help streamline the CMMC process, the DoD requests that you complete a self-assessment before scheduling your CMMC assessment. Conducting self-audits or self-assessments in advance will also help you cut down on CMMC certification costs.

3. CONSULT WITH A CMMC PROFESSIONAL OR C3PAO

While the DoD has a website that vendors can use for guidance, contact information, and to submit assessments, consulting with a firm that provides CMMC assessment, or a certified third-party assessor (C3PAO), is also a good idea. The agency or assessor you contact can tell you precisely what your assessment will entail and advise you on how to prepare.

5 Steps to CMMC Readiness

4. PREPARE FOR YOUR CMMC AUDIT

Only a CP3AO is qualified to perform a CMMC audit. The extent of your audit will depend on the maturity level for which your organization wishes to be certified. The assessor will first speak with you to determine your needs and request any documents required to evaluate your controls for protecting FCI or CUI. They will also inquire about the systems you are using and what services you are providing and supplying to the DoD. These documents may include diagrams of your environment, risk assessments, data from vulnerability scans, and a list of in-scope controls.

5. SUBMIT YOUR CMMC ASSESSMENT

There is a scoring process in place that the DoD looks at when you submit your CMMC assessment. The scores based on the following three things:

1. Your self-assessment.
2. Your System Security Plan: A detailed document including all 130 CMMC required controls tied to the 14 control families, as well as relevant attachments. This must be submitted in the DoD's template.
3. Your POAM: This document outlines where you have gaps in your environment, processes, infrastructure, policies, and procedures. This must be submitted in the DoD's template.

Demonstrating compliance with CMMC requires ongoing monitoring and evidence, which may be required weekly, monthly, or quarterly, depending on the level of CMMC certification.

CMMC Framework for NIST SP 800-171 rev. 2 & NIST SP 800-172

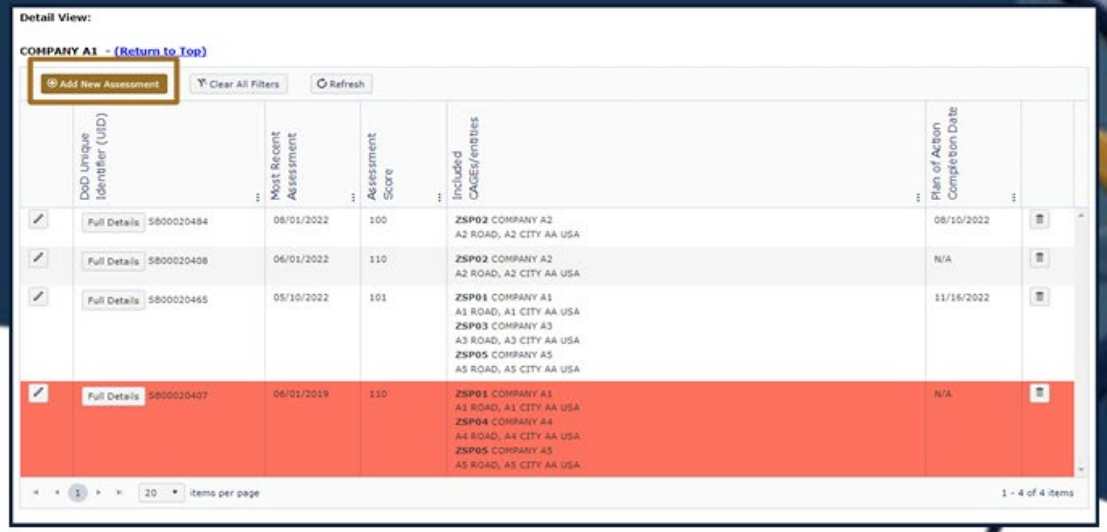
Aspect	NIST 800-171 (Original)	NIST 800-172
Purpose	Protecting CUI in nonfederal systems and organizations.	Enhanced security requirements for protecting CUI, specifically tailored for organizations working with the DoD.
Applicability	Nonfederal systems and organizations.	Organizations dealing with the DoD.
Security Requirements	Establishes a baseline of security requirements.	Builds upon NIST 800-171, with additional security requirements and controls.
Defense Supply Chain	Not specifically focused on the defense supply chain.	Designed to safeguard CUI in the defense supply chain.
Compliance Requirements	Applies to a broader range of organizations.	Targeted at contractors and entities working with the U.S. DoD.
Relationship to NIST 800-171	Serves as a foundation for security practices.	An extension with more stringent requirements, expanding on NIST 800-171.

Supplier Performance Risk System (SPRS)

The SPRS is a self-certification scoring method based on the NIST 800-171 control framework. It provides contracting officials with a score of the overall risk of the supplier. SPRS scores must be supplied to the DoD using the designated systems. Current scores must be maintained and cannot be more than 3 years old.

Detail View

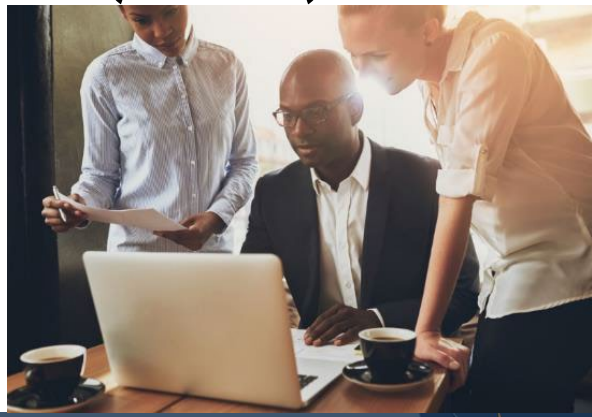
SPRS Cyber Vendor Users may enter NIST SP 800-171 Assessment details for their company



Click the +Add New Assessment button to begin entering data.

Supplier Performance Risk System (SPRS)

- The SPRS score is essentially a numerical grade that is entered into the DoD SPRS application. It is a component of the scoring that the DoD leverages for reviewing and assessing the supplier's stance.
- The DoD is now using the SPRS score as a major component of a supplier's CMMC evaluation. Your SPRS score will fall somewhere in a range from -203 to 110. The score is based on value points assigned to each of the controls in the CMMC standard.
- There are 110 controls, and the maximum SPRS score is 110. Those control items range across 14 areas related to the cybersecurity of your organization — for example, access control, configuration management, identification and authentication, incident response, system and information integrity, and more.



Assessment Entry Input

Step 1: Enter Assessment Date

NIST SP 800-171 DOD ASSESSMENT

Company Name:	COMPANY A1
HLO CAGE Code:	ZSP01
Confidence Level:	BASIC
Assessment Standard:	NIST SP 800-171

Enter Assessment Details

Assessment Date:

Score:

Assessing Scope: -Select-

Plan of Action Completion Date:

System Security Plan (SSP) Assessed:

SSP Version/Revision:

SSP Date:

Open CAGE Hierarchy

Included CAGE(s):

Include HLO

Save

CMMC FAQs

- **WHAT DO I NEED TO BE COMPLIANT WITH CMMC?**

  To be compliant with CMMC, you must comply with NIST 800-171 in addition to the 14 CMMC control family requirements. You must also acquire certification from a C3PAO assessment and certification for your maturity level.

- **HOW MUCH DOES CMMC COMPLIANCE COST?**

  The cost of CMMC compliance varies from organization to organization, depending on your cybersecurity posture and the maturity level for which you wish to achieve certification.

- **WHAT ARE THE STEPS TO BECOMING CMMC COMPLIANT?**

  1. Engage with the DoD
  2. Establish a procurement account and obtain and active status
  3. Conduct a self-assessment
  4. Understand the scope of the assessment
  5. Develop a plan
  6. Submit your assessment scope
  7. Demonstrate CMMC readiness and remediation
  8. Get a C3PAO assessment
  9. Pass (or fail) certification

- **WHAT ARE THE CMMC COMPLIANCE DEADLINES?**

  CMMC compliance will be phased into DoD contracts over the next few years. All contracts will require certification by October 25, 2025.

Resources

DoD CIO

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

NIST SP 800-171 Rev 2 and NIST SP 800-172

https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final

https://csrc.nist.gov/news/2022/nist-releases-sp-800-172a

Cyber AB

https://cyberab.org/About-Us/Overview

SPRS

https://www.sprs.csd.disa.mil/

LinkedIn Address:
www.linkedin.com/in/peterbagley-fl
Email: bbcyberfl@gmail.com