



CYBER  **FLORIDA**
AT THE UNIVERSITY OF SOUTH FLORIDA

EDUCATION | RESEARCH | OUTREACH

Cybersecurity Maturity Model Certification (CMMC)

Presented to

8(a) Firms in the U.S. Small Business Administration

North and South Florida Districts



What we'll cover today

1. Introduction
2. Overview of CMMC
3. CMMC contracts language in FAR and DFARS
4. CUI and NIST SP 800-171, 800-171A, 800-172
5. Achieving CMMC levels 1 and 2
6. CMMC 1.0, 2.0 timeline, implementation, and cost
7. Resources
8. Introduction to Cyber Florida Programs (time allowing)



Cyber Florida Point of Contact:

Kate Whitaker

Associate Director for Outreach

Cyber Florida: The Florida Center for Cybersecurity

whitakerk@cyberflorida.org

Today's Presenter:

Andy Seely

Cyber Florida Consultant

andy@sonador.com



<https://www.cyberflorida.org>





U.S. Small Business
Administration

Companies in this session work in ...

- Construction, environmental, engineering, equipment, manufacturing
- Audio-visual, physical security
- Healthcare and medical
- Legal, accounting, management
- IT, software, cybersecurity, training

Some companies in this session have Defense and Federal contracts including ...

- SEAPORT NXG
- SEWP
- ITES 3
- GSA MAS
- STARS III
- Construction contracts

Companies in this session need to prepare to meet CMMC requirements to do business in future Defense contracts



If you only have time for one slide

CMMC is a program for ensuring contractor protections of Federal Contract Information (FCI) and Controlled Unclassified Information (CUI).

CMMC 2.0 is an enforcement of NIST SP 800-171/171A/172 and *expected to be a burden*.

CMMC is a contract requirement. If your contract doesn't include DFARS 252.204-7021 today then you don't have a CMMC requirement in your current contract.

If you do not already have DFARS language requiring CMMC in your existing contracts, then you are not in the CMMC 1.0 pilot program.

Defense contracts *already* require NIST SP 800-171 compliance via DFARS 252.204-7012. Federal contracts require cybersecurity hygiene via FAR 52.204-21.

CMMC 2.0 compliance will be required for all new Defense contracts starting in the coming year (or two) -- **compliance will be required in order to submit a bid for new contracts**. Start now: Scope, staffing, gap analysis, remediation, reporting.

CMMC 2.0 Level 1 is a **self-assessment** focused on 15 requirements for FCI protections.

CMMC 2.0 Level 2 is a **3rd party assessment** focused on 110 requirements for FCI and CUI defined in NIST SP 800-171r2 and SP 800-171A

CMMC 2.0 Level 3 is a **government-run assessment** focused on 110 requirements for FCI, CUI, AND advanced guidance from NIST SP 800-172.



CMMC at a Glance

Cybersecurity Maturity Model Certification (CMMC) is a formal framework for accountability of a contractor's cybersecurity hygiene.

CMMC will enforce compliance of NIST SP 800-171, SP 800-171A, SP 800-172 on contractor-owned systems.

Applies to contractor's own systems where Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) are processed.

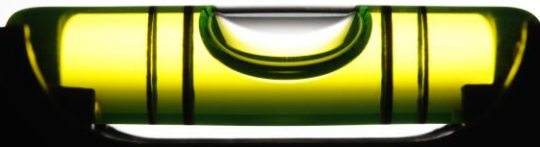
Does *not* apply to government-owned systems operated by contractors and managed via RMF and NIST SP 800-53.



- NIST defines the details for CUI cybersecurity hygiene.
- DoD CIO defines the CMMC program to implement the NIST details.
- OUSD A&S defines the requirement to comply with the CMMC program.
- Cyber AB defines who is qualified to certify CMMC program compliance.
- You achieve CMMC certification and win work with DoD !

Why CMMC? Why Now?

- The DIB is a popular attack vector to get at the DoD.
- Intellectual Property theft damages U.S. economy and erodes U.S. competitive advantage.
- Continues increased cybersecurity hardening trends following RMF, NIST SP 800-171, and DFARS 252.204-712.
- Streamlines and standardizes cybersecurity practices across the DIB to create a common baseline.
- Aligns with broader Federal efforts to protect Critical Infrastructure and sensitive Federal data.
- Reduces DoD cybersecurity risk for complex supply chains and vendor relationships.



CMMC applies to you if you...

➔ Process, store, or transmit information that meets the definition of FCI or CUI on contractor information systems as part of an awarded prime or subcontract.

This is true regardless of the size of your company.

➔ CMMC will not apply if your company provides services to operate and maintain government-owned networks.

➔ Contracts or orders that are exclusively for commercial off-the-shelf (COTS) items or are valued at or below the micro-purchase threshold do not require CMMC.

*** If your company processes FCI on your company network as a function of selling COTS, then CMMC Level 1 DOES apply ***

When in doubt, check your contract!



A Quick Look at Relevant Contract Language

FAR 52.204-21

DFARS 252.204-7012

DFARS 252.204-7019

DFARS 252.204-7021



FAR 52.204-21

Basic Safeguarding of Covered Contractor Information Systems.

(1) The Contractor shall apply the following basic safeguarding requirements and procedures to protect covered contractor information systems. Requirements and procedures for basic safeguarding of covered contractor information systems shall include, at a minimum, the following security controls:

(i) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

(ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

(x) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.

(xi) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

(xii) Identify, report, and correct information and information system flaws in a timely manner.

(xiii) Provide protection from malicious code at appropriate locations within organizational information systems.

(xiv) Update malicious code protection mechanisms when new releases are available.

(xv) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.



DFARS 252.204-7012

(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) Except as provided in paragraph (b)(2)(ii) of this clause, 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 7012 directs the contractor to implement NIST 800-171, build a System Security Plan (SSP) that describes how you have implemented NIST 800-171, create a Plan of Action and Milestones (POA&M) that describes where you have not yet implemented NIST 800-171 as well as how and when you plan to meet its requirements, create an incident response plan (IRP), and other requirements.

Note that you can be compliant with DFARS 7012 even if you have not yet implemented all 110 controls in NIST 800-171. The POA&M provides some flexibility.

<https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting>.



What About Cloud?

From DFARS 252.204-7012:

(D) If the Contractor intends to use an **external cloud service provider to store, process, or transmit any covered defense information in performance of this contract**, the Contractor shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (**FedRAMP Moderate** baseline (<https://www.fedramp.gov/documents-templates/>) and that the cloud service provider complies with requirements in paragraphs (c) through (g) of this clause for cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment.

[https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting.](https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting)



DFARS 252.204-7019 pairs with 204-7012

NOTICE OF NIST SP 800–171 DOD ASSESSMENT REQUIREMENTS (NOV 2023)

(a) Definitions.

“Basic Assessment”, “Medium Assessment”, and “High Assessment” have the meaning given in the clause 252.204-7020, NIST SP 800-171 DoD Assessments.

“Covered contractor information system” has the meaning given in the clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, of this solicitation.

(b) Requirement. In order to be considered for award, if the Offeror is required to implement NIST SP 800–171, the Offeror shall have a current assessment (i.e., not more than 3 years old unless a lesser time is specified in the solicitation) (see 252.204–7020) for each covered contractor information system that is relevant to the offer, contract, task order, or delivery order. The Basic, Medium, and High NIST SP 800–171 DoD Assessments are described in the NIST SP 800–171 DoD Assessment Methodology located at <https://www.acq.osd.mil/asda/dpc/cp/cyber/docs/safeguarding/NIST-SP-800-171-Assessment-Methodology-Version-1.2.1-6.24.2020.pdf> ..



Example from Recent FEDSIM Task Order Request

I.4 DEFENSE FEDERAL ACQUISITION REGULATION SUPPLEMENT (DFARS) CLAUSES INCORPORATED BY REFERENCE

The full text of a clause may be accessed electronically at the DFARS website: [acquisition.gov/dfars](https://www.acquisition.gov/dfars)

SECTION K – REPRESENTATIONS, CERTIFICATIONS, AND OTHER STATEMENTS OF OFFERORS OR RESPONDENTS

DFARS 252.204-7019 NOTICE OF NIST SP 800-171 DOD ASSESSMENT REQUIREMENTS (MAR 2022)

(a) *Definitions.*

“Basic Assessment”, “Medium Assessment”, and “High Assessment” have the meaning given in the clause 252.204-7020, NIST SP 800-171 DoD Assessments.

“Covered contractor information system” has the meaning given in the clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, of this solicitation.

- (b) *Requirement.* In order to be considered for award, if the Offeror is required to implement NIST SP 800-171, the Offeror shall have a current assessment (i.e., not more than 3 years old unless a lesser time is specified in the solicitation) (see 252.204-7020) for each covered contractor information system that is relevant to the offer, contract, task order, or delivery order. The Basic, Medium, and High NIST SP 800-171 DoD Assessments are described in the NIST SP 800-171 DoD Assessment Methodology located at <https://www.acq.osd.mil/asda/dpc/cp/cyber/safeguarding.html#nistSP800171>.

C.5.1.11 SUBTASK 1.11 – ESTABLISH AND MAINTAIN TO MANAGEMENT PORTAL

The objective of the TO management portal is to introduce efficiencies and streamline the flow of TO information. It will also provide a central location for the Government and contractor to access management-level information regarding the status of TO activities.

The contractor shall provide, implement, and maintain a secure, web-based portal capability that provides program management views/reporting, tracks metrics, and stores artifacts at the unclassified level. Government-approved contractor personnel and Government personnel shall have access to the portal worldwide. The contractor shall coordinate with the Government to facilitate access issues should Government network locations prevent or prohibit access. The portal content shall be maintained and revised throughout the duration of the TO. The contractor shall implement cybersecurity best practices that comply with DoD’s Cybersecurity Maturity Model to protect the portal system and all data contained within the portal.

The web-based portal shall have the capability to be certified up to Controlled Unclassified Information (CUI) in the event that an operational need arises requiring the storing or processing of CUI. The contractor shall not store or process CUI per Defense Federal Acquisition Regulation Supplement (DFARS) 204.73 – Safeguarding Covered Defense Information and Cyber Incident Reporting without the approval of the FEDSIM CO.

SECTION I – CONTRACT CLAUSES

DFARS	TITLE	DATE
252.204-7009	Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information	JAN 2023
252.204-7012	Safeguarding Covered Defense Information and Cyber Incident Reporting	JAN 2023
252.204-7018	Prohibition on the Acquisition of Covered Defense Telecommunications Equipment or Services	JAN 2023
252.204-7020	NIST SP 800-171 DoD Assessment Requirements	JAN 2023
	Item Unique Identification and Valuation	



Example from Recent NIWC Atlantic PWS

8.4.2 Safeguards

The contractor shall protect Government information and shall be able to provide documentation (e.g., Systems Security Plan (SSP)) validating they are complying with the requirement in accordance with DFARS 252.204-7012. Subcontractors are subject to DFARS requirements only when performance will involve operationally critical support or covered defense information. The contractor and all applicable subcontractors shall abide by the following safeguards:

8.4.2.1 Do not process DoD information on public computers (e.g., those available for use by the general public in kiosks or hotel business centers) or computers that do not have access control.

8.4.2.2 Protect information by at least one physical or electronic barrier (e.g., locked container or room, login and password) when not under direct individual control.

8.4.2.3 Sanitize media (e.g., overwrite, reformat, or degauss) before external release or disposal.

8.4.2.4 Encrypt all information that has been identified as controlled unclassified information (CUI) when it is stored on mobile computing devices such as laptops and personal digital assistants, or removable storage media such as portable hard drives and digital optical disks, using DoD Authorized Data-at-Rest encryption technology. Thumb drives are not authorized for DoD work, storage, or transfer. Use GSA Awarded DAR solutions (GSA # 10359) complying with ASD-NII/DOD-CIO Memorandum, "Encryption of Sensitive Unclassified Data-at-Rest on Mobile

8.5 ENHANCED SECURITY CONTROLS

Controlled unclassified information (CUI), as defined in DoDI 5200.48, is applicable to this contract. Pursuant to DFARS 252.204-7012, prior to the processing, storing, or transmitting of CUI on an unclassified information system and IT asset that is owned, or operated by or for the contractor, the contractor shall meet the following enhanced security controls.

8.5.1 Systems Security Plan and Plan of Action and Milestones (SSP/POA&M) Reviews

8.5.1.1 Within thirty (30) days of task order award, the contractor shall make its System Security Plan(s) (SSP(s)) for its covered contractor information system(s) available for review by the Government at the contractor's facility. The SSP(s) shall implement the security requirements in DFARS 252.204-7012, which is included in this task order. The contractor shall fully cooperate in the Government's review of the SSPs at the contractor's facility.

8.5.1.2 If the Government determines that the SSP(s) does not adequately implement the requirements of DFARS 252.204-7012 then the Government will notify the contractor of each identified deficiency. The contractor shall correct any identified deficiencies within thirty (30) days of notification by the Government. The Contracting Officer may provide for a correction period longer than thirty (30) days and, in such a case, may require the contractor to submit a plan of action and milestones (POA&M) for the correction of the identified deficiencies. The contractor shall immediately notify the Contracting Officer of any failure or anticipated failure to meet a milestone and provide an updated POA&M.

8.5.2 Compliance to NIST 800-171

8.5.2.1 The contractor shall fully implement the CUI Security Requirements (Requirements) and associated Relevant Security Controls (Controls) in NIST Special Publication 800-171 (Rev. 1) (NIST SP 800-171), or establish a SSP(s) and POA&M that varies from NIST 800-171 only in accordance with DFARS 252.204-7012(b)(2), for all covered contractor information systems affecting this task order.

8.5.2.2 Notwithstanding the allowance for such variation, the contractor shall identify in any SSP and POA&M their plans to implement the following, at a minimum:

(a) Implement Control 3.5.3 (Multi-factor authentication). This means that multi-factor authentication is required for all users, privileged and unprivileged accounts that log into a network. In other words, any system that is not standalone should be required to utilize acceptable multi-factor authentication. For legacy systems and systems that cannot support this requirement, such as

9.0 GOVERNMENT FURNISHED INFORMATION (GFI)

For the purposes of this task order, Government Furnished Information (GFI) includes manuals, technical specifications, software, software licenses, maps, building designs, schedules, drawings, test data, etc. provided to contractors for performance on this task order. Depending on information contained in a document, the contractor shall comply with additional controls (e.g., completion of a Non-Disclosure Agreements, etc.) for access and distribution. The Government will mark any CUI which includes unclassified covered defense information and unclassified controlled technical information provided to the contractor. For any missing markings, contractor shall request appropriate marking from the Government.



DFARS 252.204-7021



DFARS

Change Number: DFARS Change 05/30/2024
Effective Date: 05/30/2024

CYBERSECURITY MATURITY MODEL CERTIFICATION REQUIREMENTS (JAN 2023)

- (a) Scope. The Cybersecurity Maturity Model Certification (CMMC) CMMC is a framework that measures a contractor's cybersecurity maturity to include the implementation of cybersecurity practices and institutionalization of processes
- (b) Requirements. **The Contractor shall have a current (i.e. not older than 3 years) CMMC certificate** at the CMMC level required by this contract and maintain the CMMC certificate at the required level for the duration of the contract.
- (c) Subcontracts. The Contractor shall—
 - (1) Insert the substance of this clause, including this paragraph (c), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial products or commercial services, excluding commercially available off-the-shelf items; and
 - (2) Prior to awarding to a subcontractor, ensure that the subcontractor has a current (i.e., not older than 3 years) CMMC certificate at the CMMC level that is appropriate for the information that is being flowed down to the subcontractor.



A Look at CUI, NIST SP 800-171, and CMMC Levels



Defining CUI

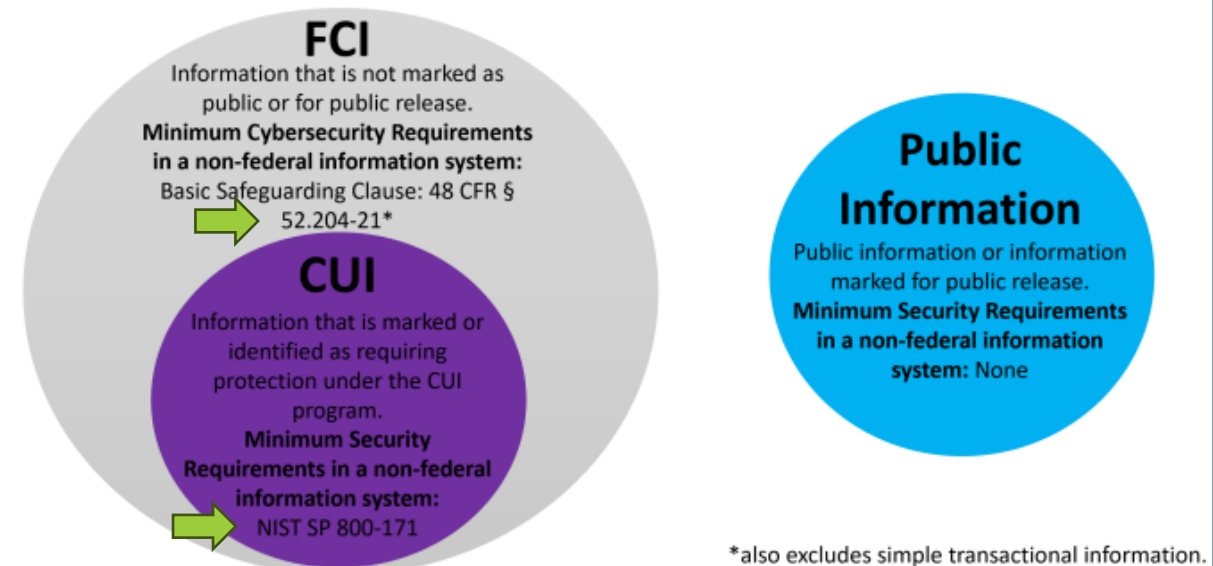


NATIONAL ARCHIVES

The National Archives and Records Administration (NARA) serves as the Controlled Unclassified Information (CUI) Program's Executive Agent and has delegated CUI Executive Agent responsibilities to the Director of the Information Security Oversight Office (ISOO). As the CUI Executive Agent, ISOO issues guidance to Federal agencies on safeguarding and marking CUI.

<https://www.archives.gov/guidance/cui-guidance>

Information that is collected, created, or received pursuant to a government contract



<https://isoo.blogs.archives.gov/2020/06/19/%E2%80%8Bfci-and-cui-what-is-the-difference/>

Defining CUI

CUI categories are grouped by organizational indices:

- Critical Infrastructure
- Defense
- Export Control
- Financial
- Immigration
- Intelligence
- International Agreements
- Law Enforcement
- Legal
- Natural and Cultural Resources
- NATO
- Nuclear
- Patent
- Privacy
- Procurement and Acquisition
- Proprietary Business Information
- Provisional
- Statistical
- Tax
- Transportation

Each organizational index has one or more specific CUI categories. For example, Defense includes:

- Controlled Technical Information
- DoD Critical Infrastructure Security Information
- Privileged Safety Information
- Naval Nuclear Propulsion Information
- Unclassified Controlled Nuclear Information – Defense



NIST SP 800-171

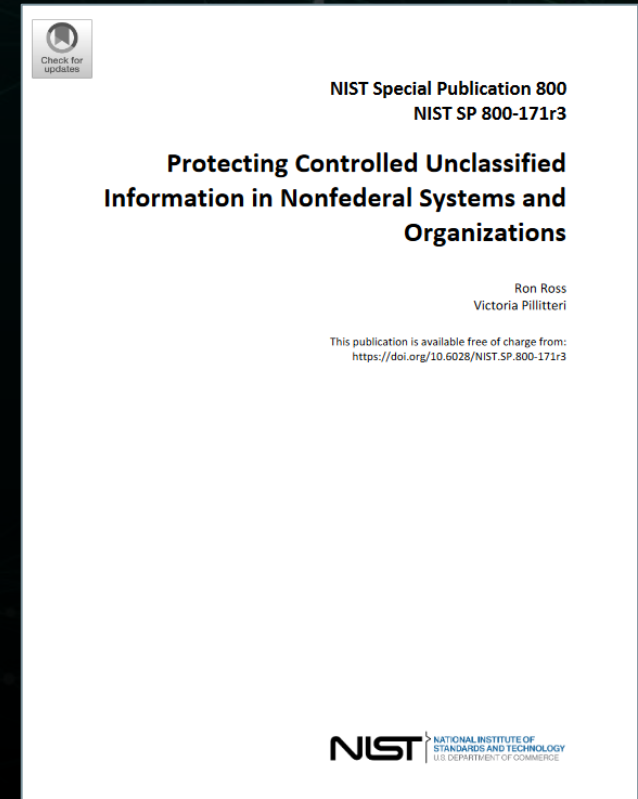
“The protection of Controlled Unclassified Information (CUI) resident in nonfederal systems and organizations is of paramount importance to federal agencies and can directly impact the ability of the federal government to successfully conduct its essential missions and functions. This publication provides agencies with recommended security requirements for protecting the confidentiality of CUI when the information is resident in nonfederal systems and organizations; when the nonfederal organization is not collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency; and where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category listed in the CUI Registry. The requirements apply to all components of nonfederal systems and organizations that process, store, and/or transmit CUI, or that provide protection for such components. The security requirements are intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations.”



NIST SP 800-171

110 controls in 17 control families

- Access Control
- Awareness and Training
- Audit and Accountability
- Assessment, Authorization and Monitoring
- Configuration Management
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Physical and Environmental Protection
- Planning
- Personnel Security
- Risk Assessment
- System and Services Acquisition
- System and Communications Protection
- System and Information Integrity
- Supply Chain Risk Management



NIST SP 800-171A

This publication provides organizations with **assessment procedures and a methodology** that can be used to conduct assessments of the security requirements in NIST Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. The assessment procedures are flexible and can be customized to the needs of organizations and assessors. Assessments can be conducted as independent, third-party assessments or as government-sponsored assessments.

03.01.07 Least Privilege – Privileged Functions

ASSESSMENT OBJECTIVE

Determine if:

A.03.01.07.a: non-privileged users are prevented from executing privileged functions.

A.03.01.07.b: the execution of privileged functions is logged.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: access control policy and procedures; procedures for least privilege; system design documentation; system configuration settings; system audit records; list of audited events; list of privileged functions to be audited and associated user account assignments; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with responsibilities for reviewing least privileges; personnel with information security responsibilities; system developers; system administrators]

Test

[SELECT FROM: mechanisms for auditing the execution of least privilege functions; mechanisms for implementing least privilege functions for non-privileged users]

REFERENCES

Source Assessment Procedures: [AC-06\(09\)](#), [AC-06\(10\)](#)

320 assessment objectives
for 110 controls in 17
control families



NIST SP 800-172

“In certain situations, CUI may be associated with a **critical program or a high value asset**. These critical programs and high value assets are potential targets for the **advanced persistent threat (APT)**. An APT is an adversary or adversarial group that possesses the expertise and resources that allow it to create opportunities to achieve its objectives by using multiple attack vectors, including cyber, physical, and deception. The APT objectives include establishing a foothold within the infrastructure of targeted organizations for purposes of exfiltrating information; undermining or impeding critical aspects of a mission, function, program, or organization; or positioning itself to carry out these objectives in the future. The APT pursues its objectives repeatedly over an extended period, adapts to defenders’ efforts to resist it, and is determined to maintain the level of interaction needed to execute its objectives. While the category of CUI itself does not require greater protection, **CUI associated with critical programs or high value assets is at greater risk because the APT is more likely to target such information** and therefore requires additional protection.”



NIST Special Publication 800-172

Enhanced Security Requirements for Protecting Controlled Unclassified Information

A Supplement to NIST Special Publication 800-171

RON ROSS
VICTORIA PILLITTERI
*Computer Security Division
National Institute of Standards and Technology*

GARY GUISSANIE
RYAN WAGNER
Institute for Defense Analyses

RICHARD GRAUBART
DEB BODEAU
The MITRE Corporation

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.800-172>

February 2021











U.S. Department of Commerce
Wynn Coggins, Acting Secretary

National Institute of Standards and Technology
James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce
for Standards and Technology & Director, National Institute of Standards and Technology

<https://csrc.nist.gov/Pubs/sp/800/172/Final>

CMMC vs RMF

DOD Risk Management Framework Applicable to DOD components	CMMC 2.0 Framework Applicable to defense contractors
 Risk-based framework	 Compliance-based framework
 266 <i>optional</i> security controls selected based on risk	 110 <i>mandatory</i> security requirements
 Plans of Action and Milestones <i>allowed</i> for systems that do not comply with security controls	 <i>Limited allowance</i> of Plans of Action and Milestones for systems that do not comply with security controls ^a
 Does not have waiver restrictions	 Very limited use of waivers with restrictions to mitigate Controlled Unclassified Information (CUI) risk

Source: GAO analysis of Department of Defense (DOD) information. | GAO-22-105259

^aAccording to DOD's CMMC documents, the department intends to limit the use of plans of action and milestones by limiting the duration (potentially 180 days), not allowing plans of action and milestones for highest-weighted requirements, and establishing a minimum-score requirement.



CMMC Levels

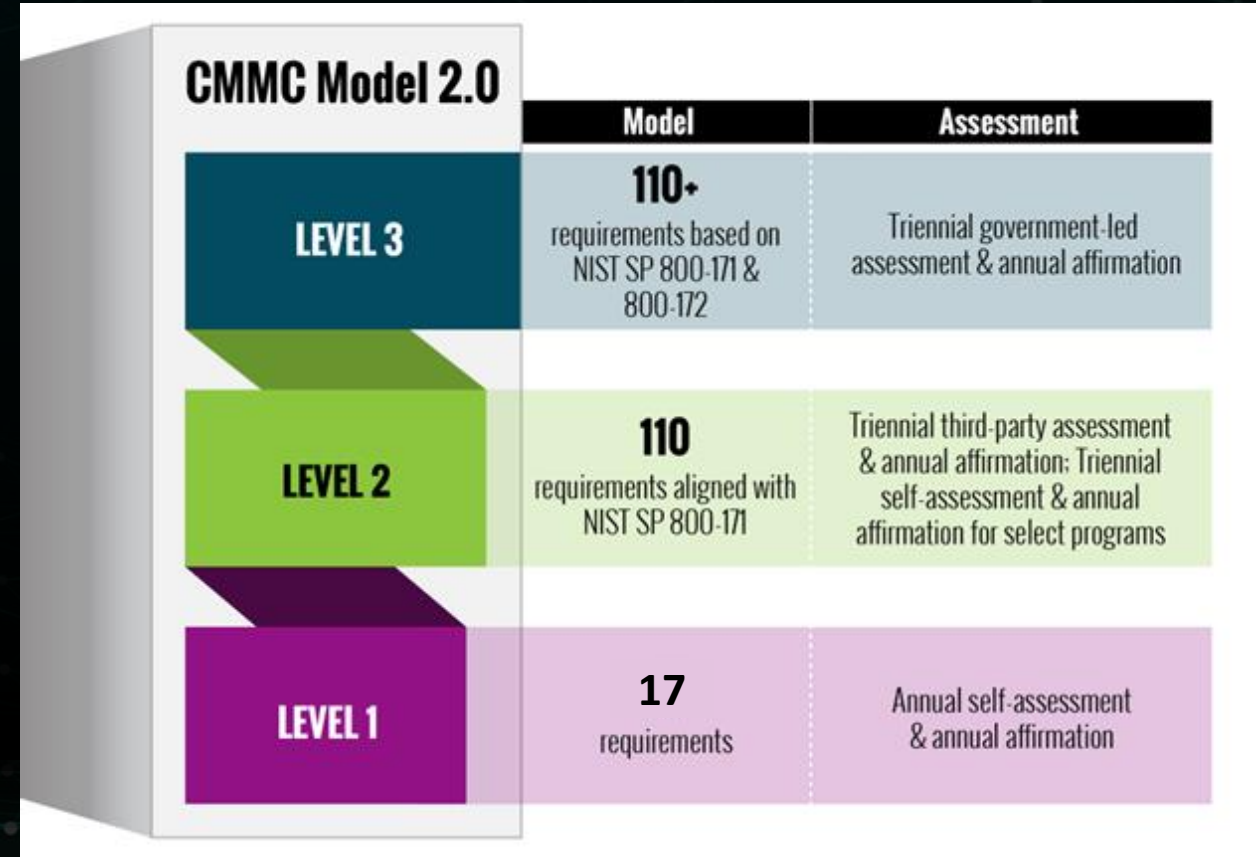
Cybersecurity Maturity Model Certification (CMMC) Model Overview

https://dodcio.defense.gov/Portals/0/Documents/CMMC/ModelOverview_V2.0_FINAL2_20211202_508.pdf

Level 1 (17 practices). An organization must demonstrate basic cyber hygiene practices to protect Federal Contract Information (FCI).

Level 2 (110 practices). An organization must have an institutionalized management plan to implement good cyber hygiene practices to safeguard CUI, including 110 NIST 800-171 r2 controls and 320 800-171A objectives.

Level 3 (Optimizing 110+ practices). An organization must have standardized and optimized processes in place and additional enhanced practices that detect and respond to changing tactics, techniques and procedures (TTPs) of advanced persistent threats (APTs). Implements NIST 800-172.



CMMC Level 1

CMMC Self Assessment Scope – level 1

<https://dodcio.defense.gov/Portals/0/Documents/CMMC/Scope Level1 V2.0 FINAL 20211202 508.pdf>

CMMC Self-Assessment Guide - level 1

<https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG Level1 V2.0 FinalDraft 20211210 508.pdf>

Results are documented in SSP and POA&M, self-reported in Supplier Performance Risk System.

Limited to these controls:

AC: AC.L1-3.1.1, AC.L1-3.1.2, AC.L1-3.1.20, AC.L1-3.1.22

IA: IA.L1-3.5.1, IA.L1-3.5.2

MP: MP.L1-3.8.3

PE: PE.L1-3.10.1, PE.L1-3.10.3, PE.L1-3.10.4, PE.L1-3.10.5

SC: SC.L1-3.13.1, SC.L1-3.13.5

SI: SI.L1-3.14.1, SI.L1-3.14.2, SI.L1-3.14.4, SI.L1-3.14.5

Note the dates: These guides are from Dec 2021 and were built during CMMC 1.0. Expect updated guidance after CMMC 2.0 rule-making is finalized.



CMMC Level 2

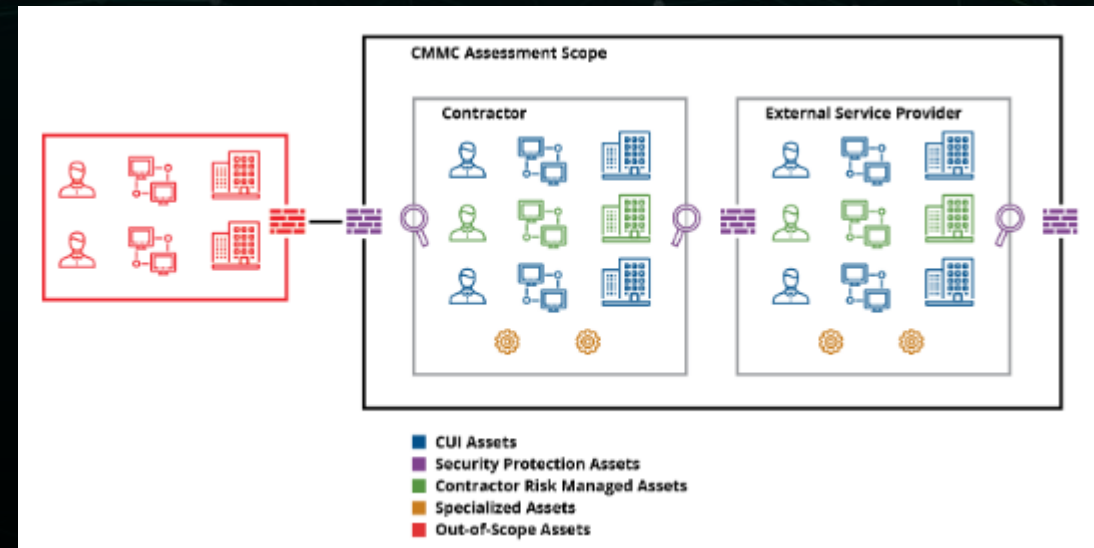
CMMC Assessment Scope - Level 2

https://dodcio.defense.gov/Portals/0/Documents/CMMC/Scope_Level2_V2.0_FINAL_20211202_508.pdf

CMMC Assessment Guide - Level 2

https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level2_MasterV2.0_FINAL_202112016_508.pdf

Results are documented in a CMMC Certificate provided by the [C3PAO](#).



“Certified Assessors will use the assessment methods as defined in this guide to conduct CMMC Level 2 assessments. Certified Assessors will review information and evidence to independently verify that a contractor meets the stated assessment objectives for all of the required practices.”



Role of System Security Plan in CMMC

The SSP is essential for CMMC. It describes the CUI protection program and enumerates each of the SP 800-171 controls. SP 800-171A should guide the minimum SSP requirements.

It's common to have a 200~300 page SSP. If your SSP is under 100 pages you might be lacking sufficient detail.

The SSP will be supported by additional documents like an IRP.

The SSP itself is CUI, in the Security Protection Data category.

NIST offers an SSP template as a starting point.

<<Insert name>> SYSTEM SECURITY PLAN Last Updated: <<Insert date>>

1. SYSTEM IDENTIFICATION

1.1. System Name/Title: [State the name of the system. Spell out acronyms.]

1.1.1. System Categorization: Moderate Impact for Confidentiality

1.1.2. System Unique Identifier: [Insert the System Unique Identifier]

1.2. Responsible Organization:

Name:	
Address:	
Phone:	

1.2.1. Information Owner (CUI):

Name:	
Title:	
Office Address:	
Work Phone:	
e-Mail Address:	

1.2.1.1. System Owner (CUI):

Name:	
Title:	

3.1. Access Control

3.1.1. Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).

Implemented Planned to be Implemented Not Applicable | Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.2. Limit system access to the types of transactions and functions that authorized users are permitted to execute.

Implemented Planned to be Implemented Not Applicable | Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.3. Control the flow of CUI in accordance with approved authorizations.

Implemented Planned to be Implemented Not Applicable | Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.4. Separate the duties of individuals to reduce the risk of malevolent activity without collusion.

Implemented Planned to be Implemented Not Applicable | Current implementation or planned implementation details. If "Not Applicable," provide rationale.



Supplier Performance Risk System

SPRS is the system used to report compliance with NIST SP 800-171 and CMMC.

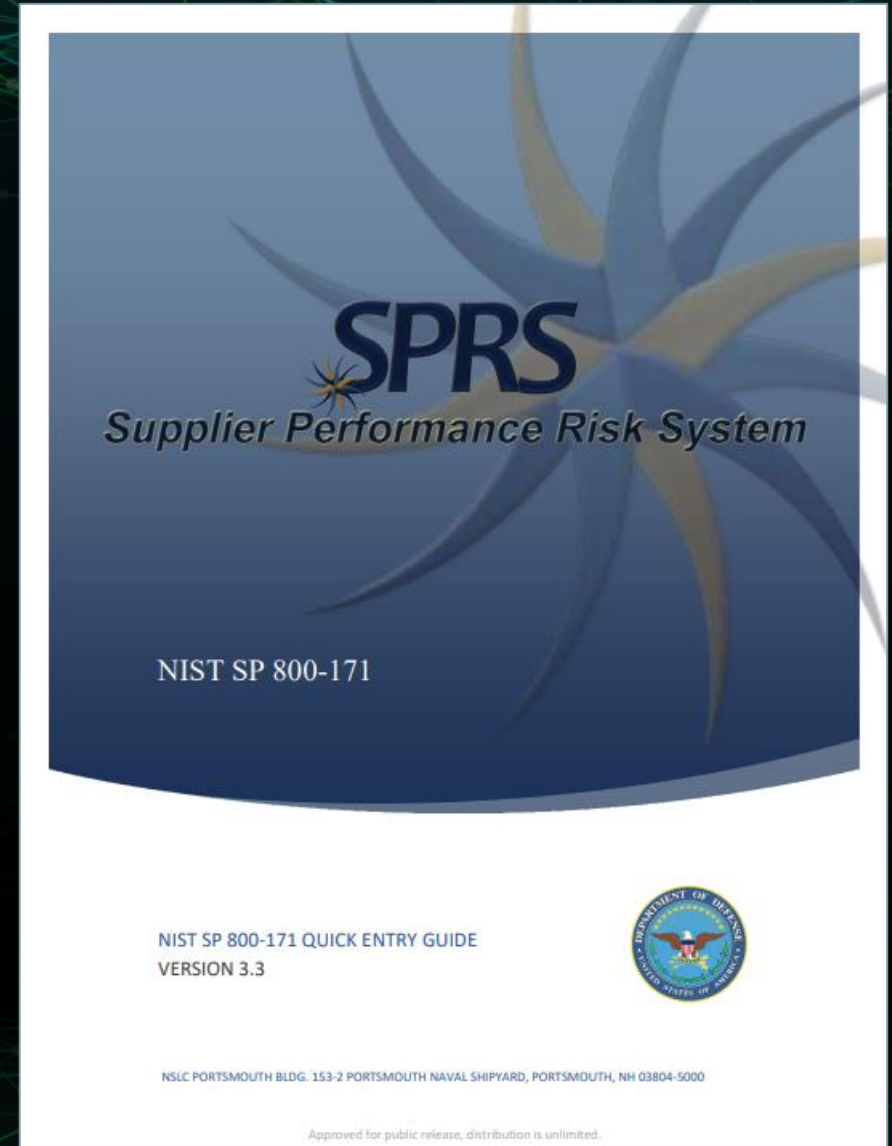
Example language from a recent GSA Alliant II Task Order Request:

L.5.1.12 NOTICE OF NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) SP 800-171 DOD ASSESSMENT REQUIREMENTS (TAB L)

The offeror shall provide a copy (screenshot is acceptable) of its assessment in the Supplier Performance Risk System (SPRS) per DFARS 252.204-7019 provision.

L.5.1.13 COST/PRICE ASSUMPTIONS (TAB M)

This Quick Entry Guide provided by DISA is from August 2021, gives screen shots and step by step for setting up and submitting assessment results.



Timelines, Paths to Certification, and Cost



Path to and Problems with Certification

When to start? Now. Yesterday, if possible.

- Some estimates suggest that NIST SP 800-171 implementation for 50-100 person companies starting from scratch will average 12-18 months
- Required for new contracts 9~12 months from now ... the heat is on!
- Significant DIB criticism that CMMC is an **undue burden on small businesses** (and on large businesses)

If you do not have a robust cybersecurity team, get help!

- There are a LOT of companies selling help – **due diligence** is important
- Start with scoping
- Do a gap analysis
- Perform a self assessment

Certified 3rd Party Assessment Organization (C3PAO) required to issue a CMMC Level 2 certification

- Check the listing in the **CMMC AB Marketplace**:
<https://cyberab.org/Catalog#!/c/s/Results/Format/list/Page/1/Size/9/Sort/NameAscending?term=tampa>

The Cyber AB is the official accrediting body for CMMC assessors

A Key Note:

Don't spend money you don't need to spend

- ✓ *Vet your vendors*
- ✓ *Get a gap analysis*
- ✓ *Do a self assessment*
- ✓ *Understand your contract requirements*
- ✓ *Ensure your C3PAO is certified*
- ✓ *Build your organic cybersecurity workforce*



Cyber AB and CMMC Roles

The Cyber AB is the official accreditation body of the Cybersecurity Maturity Model Certification (CMMC) Ecosystem and the sole authorized non-governmental partner of the U.S. Department of Defense in implementing and overseeing the CMMC conformance regime. <https://cyberab.org/>

Registered Practitioner (RP): An individual who has attended training and passed tests demonstrating knowledge of CMMC levels. Valuable for preparation and consulting. Can help with self-assessment. Can not provide CMMC certification or letter of attestation.

Registered Practitioner Organization (RPO): An organization that provides RP personnel for consulting and non-certified advisory roles.

Certified CMMC Professional (CCP): Has been trained, evaluated, and authorized to provide certifications for CMMC Level 1. While Level 1 is self-assessment, a CCP providing that assessment may add additional value to an organization.

Certified CMMC Assessor (CCA): Has been trained, evaluated, and authorized to provide certifications for CMMC Level 2. Only a CCA may provide this certification service.

CMMC 3rd Party Assessment Organization (C3PAO): A company that employs CCA and CCP personnel to conduct independent assessments and provide CMMC certifications.

Note that an RP, CCP, or CCA who assists an organization in preparation for an assessment may not also participate in that assessment.



Cyber AB Assessors

Find accredited assessors: <https://cyberab.org/Catalog>

BECOMING A CMMC ASSESSOR

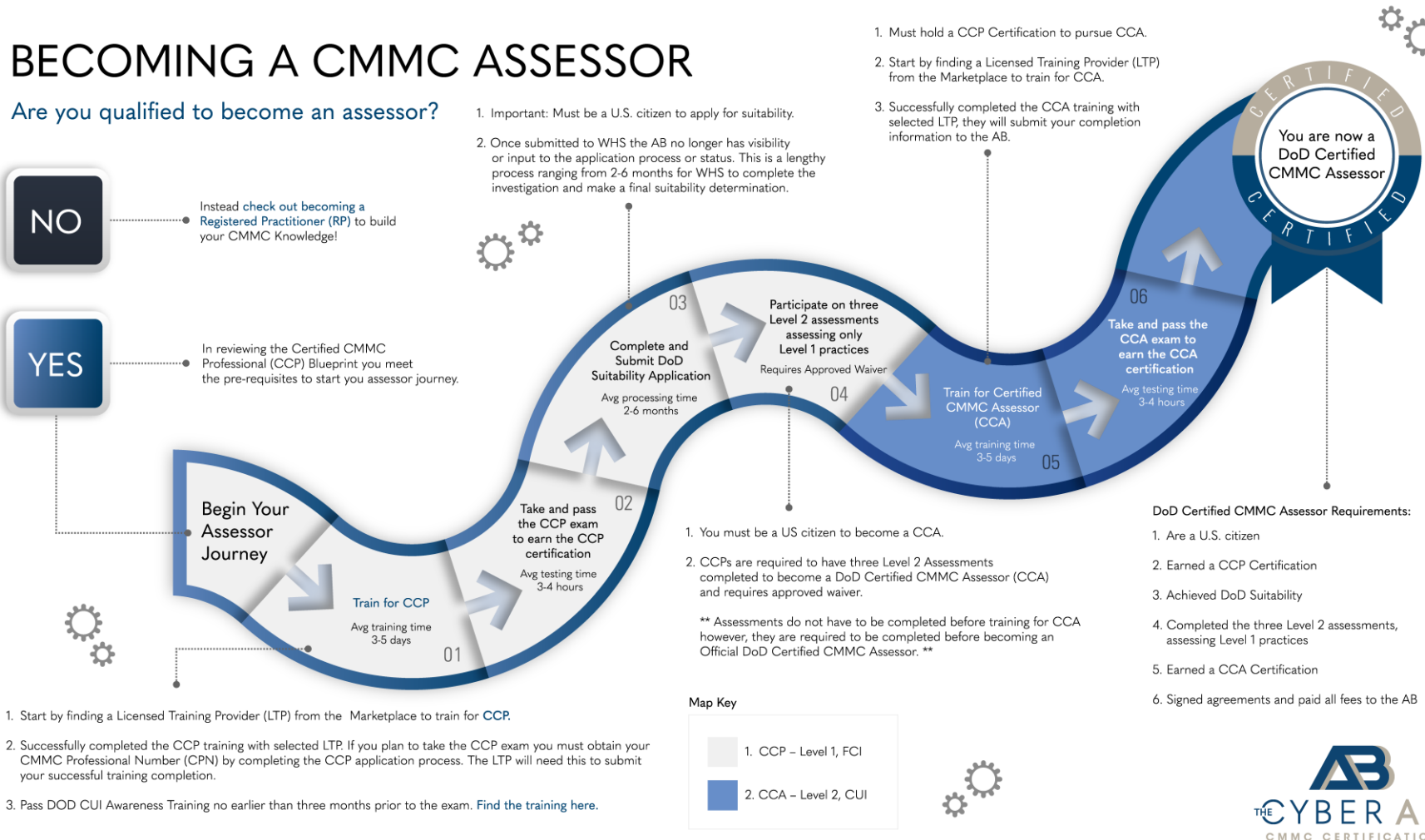
Are you qualified to become an assessor?

NO

Instead check out becoming a Registered Practitioner (RP) to build your CMMC Knowledge!

YES

In reviewing the Certified CMMC Professional (CCP) Blueprint you meet the pre-requisites to start your assessor journey.



1. Important: Must be a U.S. citizen to apply for suitability.
2. Once submitted to WHS the AB no longer has visibility or input to the application process or status. This is a lengthy process ranging from 2-6 months for WHS to complete the investigation and make a final suitability determination.

1. Must hold a CCP Certification to pursue CCA.
2. Start by finding a Licensed Training Provider (LTP) from the Marketplace to train for CCA.
3. Successfully completed the CCA training with selected LTP, they will submit your completion information to the AB.

1. Start by finding a Licensed Training Provider (LTP) from the Marketplace to train for CCP.
2. Successfully completed the CCP training with selected LTP. If you plan to take the CCP exam you must obtain your CMMC Professional Number (CPN) by completing the CCP application process. The LTP will need this to submit your successful training completion.
3. Pass DOD CUI Awareness Training no earlier than three months prior to the exam. [Find the training here.](#)

Map Key

- 1. CCP - Level 1, FCI
- 2. CCA - Level 2, CUI

1. You must be a US citizen to become a CCA.
 2. CCPs are required to have three Level 2 Assessments completed to become a DoD Certified CMMC Assessor (CCA) and requires approved waiver.
- ** Assessments do not have to be completed before training for CCA however, they are required to be completed before becoming an Official DoD Certified CMMC Assessor. **

- DoD Certified CMMC Assessor Requirements:**
1. Are a U.S. citizen
 2. Earned a CCP Certification
 3. Achieved DoD Suitability
 4. Completed the three Level 2 assessments, assessing Level 1 practices
 5. Earned a CCA Certification
 6. Signed agreements and paid all fees to the AB



CMMC History

CMMC 1.0 was developed by OUSD for Acquisition and Sustainment in 2019, building on the previous guidance of the Federal Information Security Management Act (FISMA), the Federal Information Processing Standards (FIPS), and language in the Defense Federal Acquisition Regulation Supplement (DFARS)

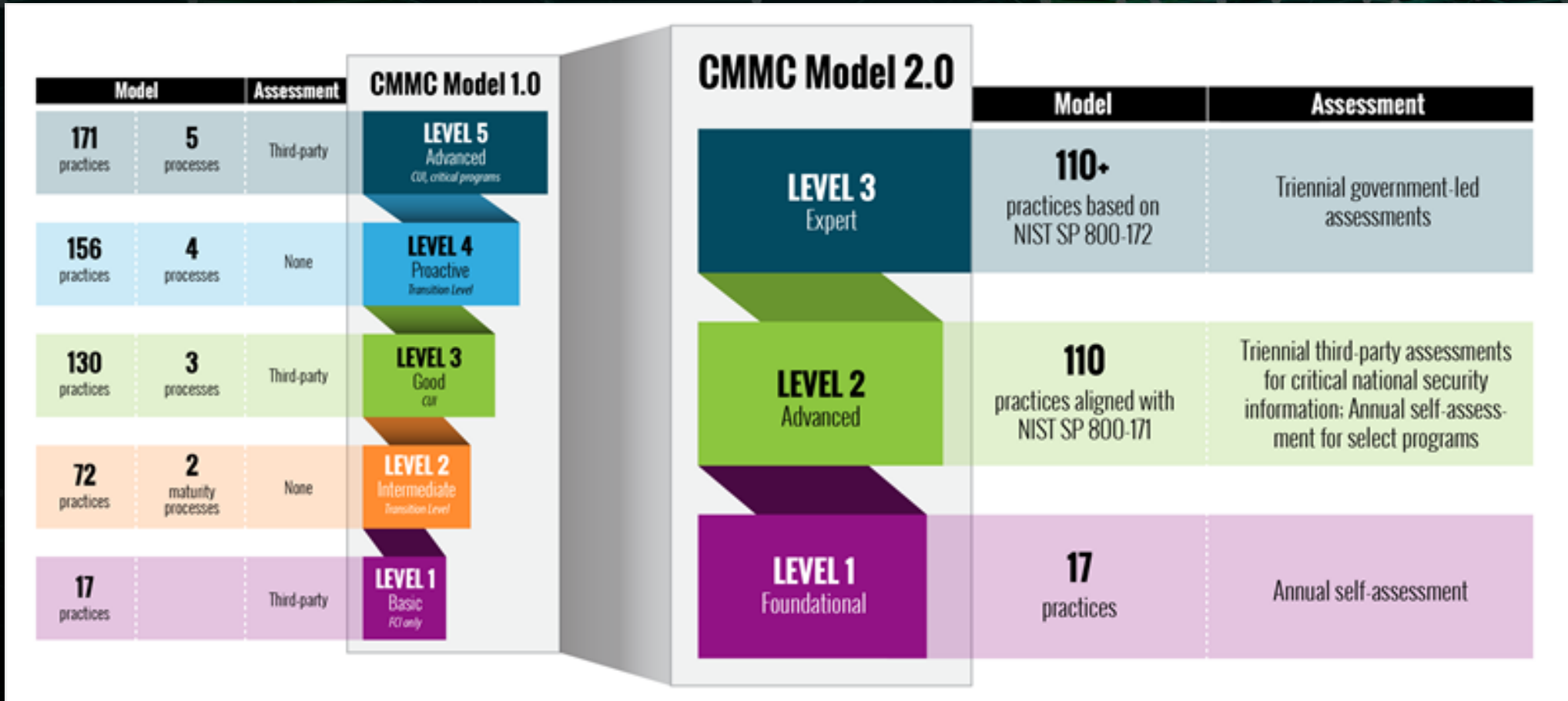
CMMC 2.0 refines and streamlines the 1.0 framework; the rulemaking process expected to complete this year

CMMC requirements expected to be baked-in with DFARS contract clauses in all future defense contracts

A Key Note: NIST SP 800-171 compliance is already required by DFARS
CMMC is an additional framework of compliance oversight and accountability



CMMC 1.0 to 2.0 Transition



CMMC 2.0

Code of Federal Regulations rule-making public comment period closed earlier this year

“DoD is proposing to establish requirements for a comprehensive and scalable assessment mechanism to ensure defense contractors and subcontractors have, as part of the Cybersecurity Maturity Model Certification (CMMC) Program, implemented required security measures to expand application of existing security requirements for Federal Contract Information (FCI) and add new Controlled Unclassified Information (CUI) security requirements for certain priority programs. DoD currently requires covered defense contractors and subcontractors to implement the security protections set forth in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800–171 Rev 2 to provide adequate security for sensitive unclassified DoD information that is processed, stored, or transmitted on contractor information systems and to document their implementation status, including any plans of action for any NIST SP 800–171 Rev 2 requirement not yet implemented, in a System Security Plan (SSP). **The CMMC Program provides the Department the mechanism needed to verify that a defense contractor or subcontractor has implemented the security requirements at each CMMC Level and is maintaining that status across the contract period of performance, as required.**”



CMMC Timeline

Mid 2022 – 20 C3PAOs “authorized,” but cannot yet perform CMMC assessments.

Mid 2022 – Mid 2023: A few C3PAOs were allowed to do “joint” assessments of 800-171 alongside the Defense Industrial Base Cybersecurity Assessment Center (DIBCAC). These are not CMMC assessments.

Mid 2022 – About 100 CMMC Assessors certified but cannot yet perform CMMC assessments.

Late 2023 – New DFARS rule enforcing CMMC was published in draft. 26 December DoD submitted the proposed rule for CMMC 2.0 to the Federal Register. <https://www.govinfo.gov/content/pkg/FR-2023-12-26/pdf/2023-27280.pdf>

26 February: Public Comments period closed. <https://www.regulations.gov/docket/DOD-2023-OS-0063>

Now → 27 June: DoD submitted CMMC 2.0 under Title 32 (National Defense) to Information and Regulatory Affairs in OMB as final step before public release. Expect 3~4 months review, go-live early 2025 in Title 48 (FAR) <https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202404&RIN=0790-AL49>

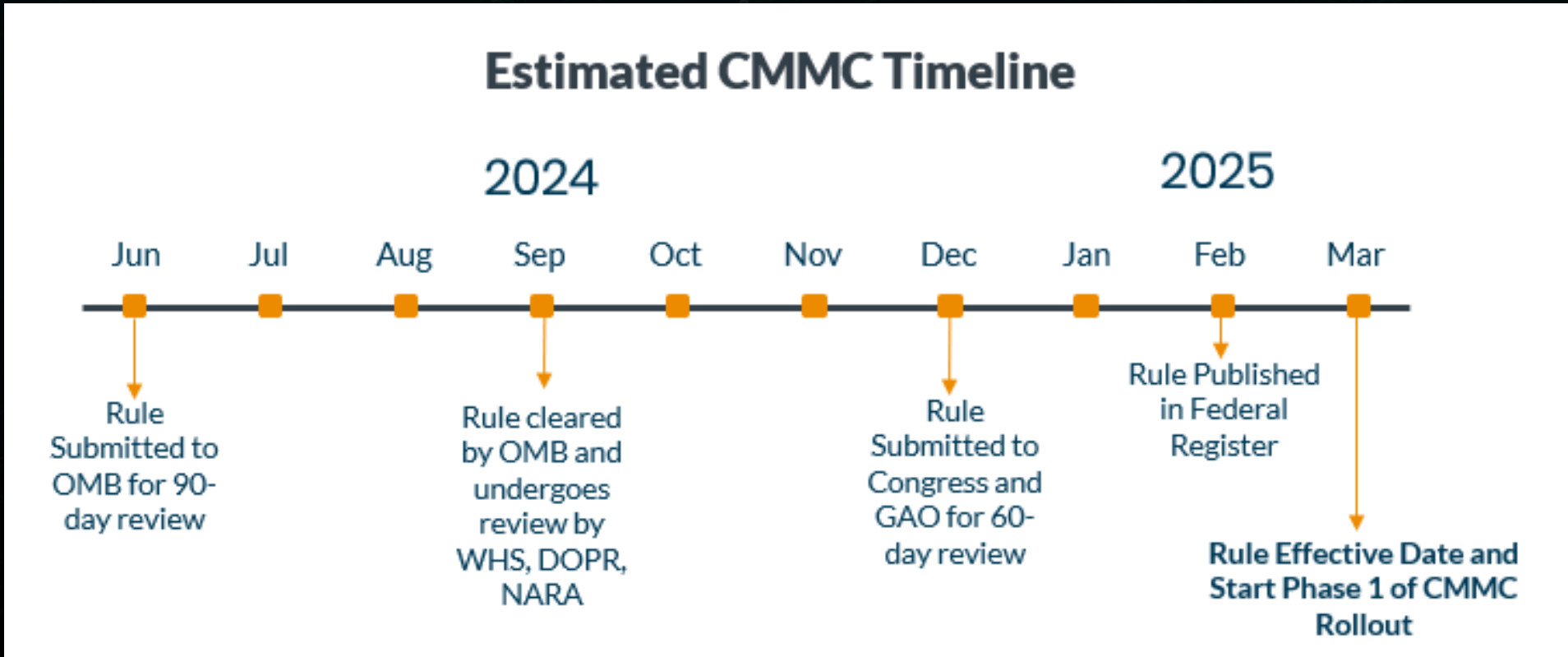
Impacts your business → Mid 2025 – contracts requiring CMMC Level 1 self-assessment released.

→ Late 2025 – contracts requiring CMMC Level 2 certification assessments released.

Mid 2026 – contracts requiring CMMC Level 3 certification assessments released.



CMMC Timeline



The Cost of CMMC

“DoD's Office of Small Business and Technology Partnerships (OSBTP) is working to provide SBIR/STTR programs with support for CMMC implementation through the use of Technical and Business Assistance. The SBA's affiliation rules are codified at 13 CFR 121.103, available at <https://www.ecfr.gov/current/title-13/chapter-I/part-121>. Any change to the SBA's affiliation rules is outside the scope of this rulemaking.”
(There is no obvious mention of this assistance in <https://business.defense.gov/>)

<https://www.federalregister.gov/documents/2023/12/26/2023-27280/cybersecurity-maturity-model-certification-cmmc-program>

“A Level 2 self-assessment and related affirmations are estimated to cost over **\$37,000** for small entities and nearly **\$49,000** for larger entities (including the triennial assessment and affirmation and two additional annual affirmations). A Level 2 certification assessment is projected to cost nearly **\$105,000** for small entities and approximately **\$118,000** for larger entities (including the triennial assessment and affirmation and two additional annual affirmations).”

<https://defensescoop.com/2023/12/28/cmmc-implementation-cost-estimates/>



The Cost of CMMC

“Average Burden per Response (CMMC Level 2): 525.955 hours.” (Back of the envelope: \$100/hour burdened rate, \$52,600 ?)

<https://www.regulations.gov/document/DOD-2023-OS-0063-0374>

The Department will publish a comprehensive cost analysis associated with each level of CMMC 2.0 as part of rulemaking. Costs are **projected to be significantly lower relative to CMMC 1.0** because the Department intends to (a) streamline requirements at all levels, eliminating CMMC-unique practices and maturity processes, (b) allow companies associated with the new Level 1 (Foundational) and some Level 2 (Advanced) acquisition programs to perform self-assessments rather than third-party assessments, and (c) increase oversight of the third-party assessment ecosystem.

<https://dodcio.defense.gov/CMMC/about/>



The Cost of CMMC

DoD CIO CMMC FAQ

Q. How much will it cost to implement CMMC 2.0?

A. The Department will publish a comprehensive cost analysis associated with each level of CMMC 2.0 as part of rulemaking. It is important to note that **costs to implement cybersecurity controls are incurred due to the need to comply with contract requirements for safeguarding information, as defined in FAR 52.204-21, and DFARS 252.204-7012, and are not considered to be costs for implementing CMMC**, which is a program to assess the degree to which those underlying security requirements have been met.

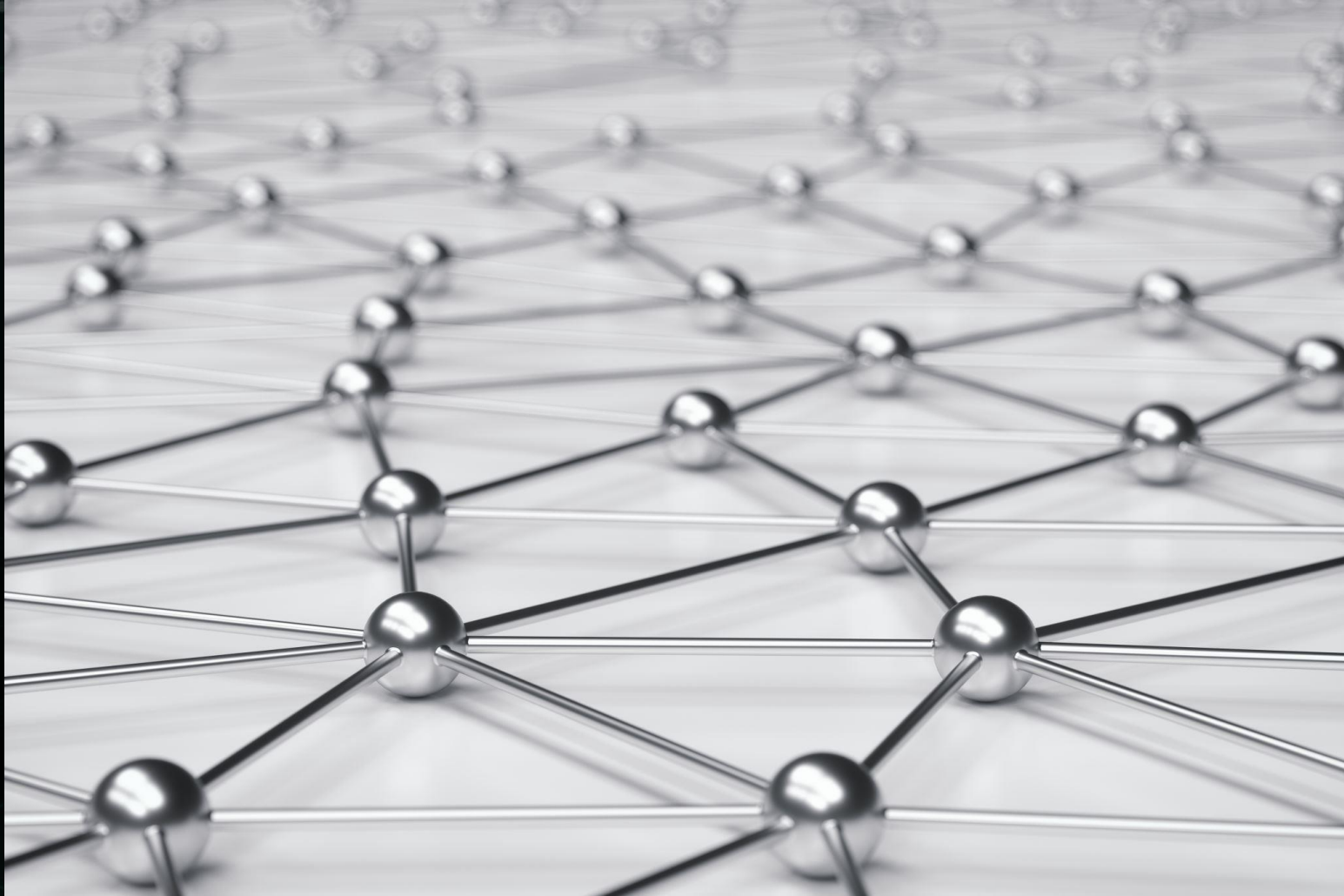
(If CMMC costs are allowable, do they impact overall price and LPTA competitions?)

<https://dodcio.defense.gov/CMMC/FAQ/>

All sources hint that cost estimates are strictly for CMMC compliance efforts, and not for underlying NIST SP 800-171 compliance activities.



Resources and Last Words



Resources

Explore free services provided by NSA, DoD, and NIST

NATIONAL SECURITY AGENCY (NSA) CYBERSECURITY COLLABORATION CENTER <https://www.nsa.gov/About/Cybersecurity-Collaboration-Center/>

- Protective Domain Name System (PDNS)
- Attack Surface Management
- Threat Intelligence Collaboration

DC3/DOD DEFENSE INDUSTRIAL BASE COLLABORATIVE INFORMATION SHARING ENVIRONMENT (DCISE) <https://www.dc3.mil/>

- Real-time monitoring of network traffic, threat detection, and alerts; option to block malicious traffic
- CYBER RESILIENCE ANALYSIS (CRA)
- ADVERSARY EMULATION (AE)

PROJECT SPECTRUM <https://www.projectspectrum.io/#/>

BLUE CYBER INITIATIVE <https://www.safcn.af.mil/CISO/Small-Business-Cybersecurity-Information/>

NIST CUI POA&M Template: <https://csrc.nist.gov/files/pubs/sp/800/171/r2/upd1/final/docs/cui-plan-of-action-template-final.docx>

NIST CUI SSP Template: <https://csrc.nist.gov/files/pubs/sp/800/171/r2/upd1/final/docs/cui-ssp-template-final.docx>



Resources

Be aware of vendors pushing the **urgency of CMMC** in order to capitalize on your uncertainty. The National Defense Information Sharing and Analysis Center published an easy “**C3PAO Shopping Guide for Small & Medium-Sized Businesses**” https://ndisac.org/wp-content/uploads/2024/03/ND-ISAC_C3PAO-Shopping-Guide-for-SMBs_v12_13MAR2024.pdf

There are valuable resources at the CMMC Information Institute, including an **excellent self assessment tool** and a nice CMMC Assessment Lifecycle info-chart. <https://cmmcinfo.org/>

CMMC Center of Awesomeness is a really good and really fun resource. “CMMC is punishment for the DIB blowing off the DoD's requirements to comply with NIST 800-171 requirements to protect Controlled Unclassified Information (CUI). The DoD went from self-certification to a pathological focus on perfection.” The **Awesomeness Spreadsheet** and the **Kill Chain** are very useful. <https://cmmc-coa.com/>

“CMMC CON 2024” is a virtual event that might be vendor-heavy, but still interesting (and free): <https://registration-cmmccon.cybersheath.com/>

“Secure the DIB Summer Camp” is a virtual event by Summit7 that looks interesting (and is also free): <https://www.summit7.us/securethedib>



Last Words on CMMC for Florida 8(a) firms

- ✓ Practice good cybersecurity hygiene regardless of what your contracts require
- ✓ Understand your contracts and what they require
- ✓ Talk to your primes and understand their expectations
- ✓ Talk to your subs and let them know your expectations
- ✓ Look at your in-house skills, out-source if necessary
- ✓ Scope your requirement and potential FCI and CUI
- ✓ Do a gap assessment
- ✓ Make a CMMC assessment readiness plan that gets you to the right level by early / mid-2025
- ✓ Join CMMC forums and mailing lists and stay informed of program changes
- ✓ Execute the plan and be ready to win new work in 2025!



Introduction to Cyber Florida

Cyber Florida programs that directly support 8(a) firms in Florida
Cyber Florida programs that directly support public sector organizations
(and indirectly benefit 8(a) firms!)



WHO ARE WE?

- 28 Full-Time Staff Members
- 16 Student Team Members
- 5 Faculty Academic Directors



WHAT ARE WE DOING?

GRANT-FUNDED & STATE INITIATIVES

Florida's Cybersecurity Critical Infrastructure Risk Assessment

Conduct a voluntary cybersecurity risk assessment for Florida-based public and private critical infrastructure organizations

Statewide Cybersecurity Training Program

Provide cybersecurity awareness and training courses tailored to job roles for all public-sector employees

Cyber Range (HB 5001)

Provide a cost-effective, realistic cybersecurity training environment for city, county, and local governments

CyberWorks: Cybersecurity Workforce Development (NCAE)

Prepare veterans and transitioning first responders for jobs in cybersecurity



WHAT ARE WE DOING?

ONGOING PROGRAMS

Operation K12

Infuse cybersecurity awareness and career preparation throughout the Florida education system

Seed Fund Pilot Program

Supports Florida-based researchers and emerging entrepreneurs in commercializing their cybersecurity technical innovations, launching new businesses, and helping secure critical infrastructure

Policy & Research

Fund and facilitate research and help guide public policy by educating both the decision-makers and the public on best practices and policy initiatives

SOCAP: Security Operations Center Apprenticeship Program

Provide hands-on experience to complement degree programs and services to support the public sector



CRITICAL INFRASTRUCTURE PROTECTION (CIP) PROGRAM

- Free online cyber risk assessment funded and authorized by the State of Florida
- New entry-level assessment (20 questions) to identify vulnerabilities
- Free resources for public and private sector critical infrastructure organizations, such as incident response plans and subscriptions to INL cyber workforce enhancement programs

COMING SOON:

- Adopt and implement a Florida-Specific Cybersecurity Maturity Model for critical infrastructure providers
- Close the maturity gap for “basic” ransomware readiness
- Continue to expand and mature existing critical infrastructure cybersecurity initiatives via CI mapping and analysis
- Construct and maintain a comprehensive list of critical infrastructure entities operating in the state for sampling and communication purposes (intel sharing)



powered by **CYBER FLORIDA AT USF + SIMSPACE**

ARCS  **RANGE**

ALIGNED REALISTIC CYBERATTACK SIMULATION RANGE

RANGE FEATURES

- Florida County and Local government IT and cybersecurity personnel - public sector focused
- Cyber Range as a Service (CRaaS), 100% cloud-based training model
- No cost for public sector users
- Supports Statewide Training Program

KEY MILESTONES

- ✓ Feb 2024: SimSpace selected as vendor; soft launch
- ✓ 27 March 2024: Ribbon cutting/formal launch
- ✓ Currently 145 users across 17 counties on ARCS Range



CYBER FLORIDA FIRSTLINE

No-cost education & training
for Florida's public sector

\$30M in non-recurring funding
from the Florida Legislature to
provide no-cost cyber education
and training to every Florida
state, county, and municipal
government employee

PROGRAM FEATURES

- Courses tailored to work roles: general awareness, managerial/executive, technical
- Courses offered online (synchronous and asynchronous) and in-person at locations throughout the state to minimize travel
- Catalog includes
 - Industry certification prep courses plus exam vouchers to upskill Florida's technical professionals
 - Specialized training for law enforcement
 - In-person tabletop exercises through NUARI's DECIDE platform

PROGRAM PARTNERS





- Grant-supported
- Industry partners include JPMorgan Chase, ReliaQuest, KnowBe4, Amazon Web Services, VMWare, Rapid7, Cisco, Raytheon, OPSWAT, GuidePoint
- **NICE Work Role:** Cyber Defence Analyst
- **Enrollment:** Two cohorts per year, 30-40 students per cohort
- **Courses/Badges:** Network Fundamentals, Cyber Defense Fundamentals
- **Industry Certifications:**
 - CompTIA Network+
 - CompTIA Cybersecurity Analyst (CySA+)
 - CompTIA Security+



OPERATION **K12** **POWERED BY** **CYBER FLORIDA**

- Youth Engagement
- Educator Professional Development
- Curriculum Development

PROGRAM HIGHLIGHTS

- Active in districts across Florida through a tiered support system, as well as several other states, territories, and even countries
- Cybersecurity Essentials Course (including lesson plans, presentations, labs, tests, and activities) preps for industry certification exam
- CyberHub virtual lab environment provided at no cost
- Speakers Bureau, monthly webinars, Slack channel w/150 users
- Collaboration Center housed in Canvas provides curriculum guides, demos, exam prep, career resources
- Second Annual CyberLaunch Statewide High School Competition 4 April 2025



SEED FUND PILOT PROGRAM

- \$750,000
- Collaboration with Tech Incubators and Accelerators
- In consultation with the Florida Cybersecurity Advisory Council
- Modeled after federal SBIR/STTR programs
- Preparing for Year 2, 2024-2025

Company	Remarks	Domain
ChainHealth	USF faculty (Cyber Florida, CAS) Well-developed go-to-market strategy	Secure personal medical data sharing using BlockChain
Monic.ai	USF alumni \$250k in other seed funding already secured, some customers	Automated training co-pilot using private LLM
OverwatchOT	USF alum Founder previously helped Cyber Florida	Automated cybersecurity audit
ThreatShield	FIU faculty Potentially relevant to Federal Government	Automated threat detection for zero-day attacks





Security Operations Center Apprentice Program

Provides hands-on cyber threat monitoring, digital forensics, and reporting skills for up to 20 USF students each year

SERVICES OFFERED/STUDENT LEARNING OBJECTIVES

- Digital forensics, including enterprise and mobile devices
- Incident response (remote triage assistance)
- Malware analysis
- Log management and review/log collection and analysis
- Cybersecurity projects, assessments, and consulting
- Coming soon: vulnerability assessment and penetration testing



SUMMARY

CYBER FLORIDA IS FULLY ENGAGED

Risk Assessment

Training

ARCS Range

Workforce Development

Education and Training Capacity building

A STATEWIDE RESOURCE

Engaged across the State

Public and Private Sectors

HELPING TO MAKE FLORIDA THE LEADING STATE IN CYBERSECURITY

