NORTH CAROLINA MILITARY BUSINESS CENTER

CYBERSECURITY MATURITY MODEL CERTIFICATION V1.02

What is CMMC?

- Unified cybersecurity standard for DoD acquisitions – eliminates confusion created by multiple regulations
- Protects Federal Contract Information [FCI]– unclassified information that is to be protected from public disclosure, and Controlled Unclassified Information [CUI]– information that requires safeguarding or dissemination controls
- A quality management system for cybersecurity – not a checklist. Compliance to CMMC is not an IT task, it's a management task. As with other quality management systems and maturity models, it requires a culture change.
- Based on CMMI – developed by Carnegie Mellon and Johns Hopkins

Why Do We Need CMMC?

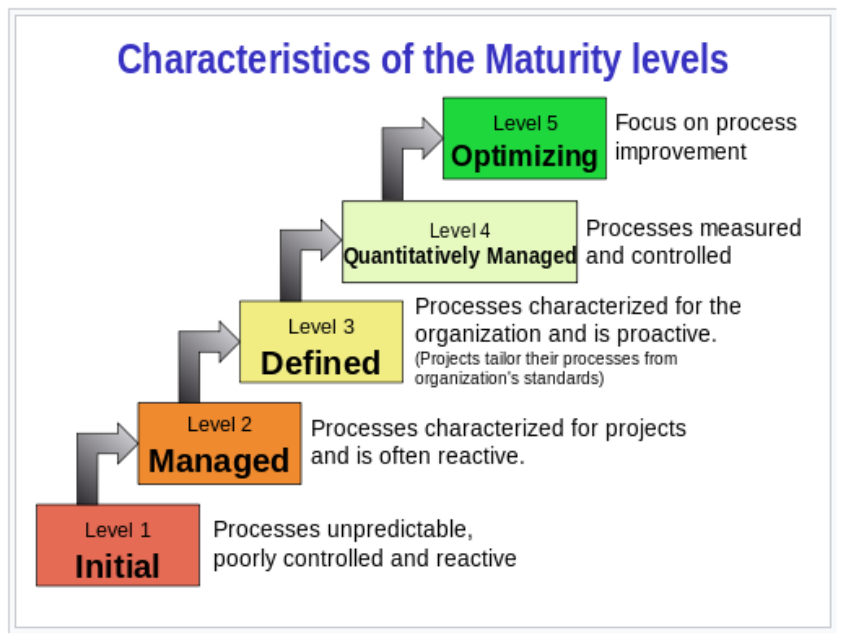
- 70% to 80% of DoD data resides on contractors' networks - and there are over 300,000 companies in the DIB
- $600B [1% of GDP] is lost to cyber theft each year to our adversaries
- Half of all cyber attacks are targeted at small businesses, and some never recover due to the high cost of a cyber attack
- DFARS 252.204-7012 allowed companies to "self-attest" to compliance with NIST SP 800-171
- Current cybersecurity requirements don't go far enough to protect CUI [NIST SP 800-171 and 48 CFR 52.204-21 (FAR)]
- Part of "supply chain illumination"

Who Has to Comply with CMMC?

- Any organization in the DoD supply chain that processes, stores and/or transmits FCI or CUI
- Any organization that provides protection for FCI or CUI. Note: that includes Managed Service Providers

What is a Maturity Model?

- Provides a benchmark against which an organization can evaluate the current level of capability of it's processes, practices and methods, and set goals and priorities for improvement; measure for the extent to which an activity is ingrained in the operations of an organization. The more deeply ingrained the more likely it is that the outcomes will be consistent, repeatable and of high quality.



Domains, Capabilities, Processes and Practices

CMMC Model V 1.02 encompasses the following:

- 17 capability domains
- 43 capabilities
- 5 processes across 5 levels to measure process maturity
- 171 practices across five levels to measure technical capabilities. Note: Practices are cumulative, e.g. Level 5 includes all the practices from Levels 1 – 4, plus adds an additional 15 for a total of 171 practices

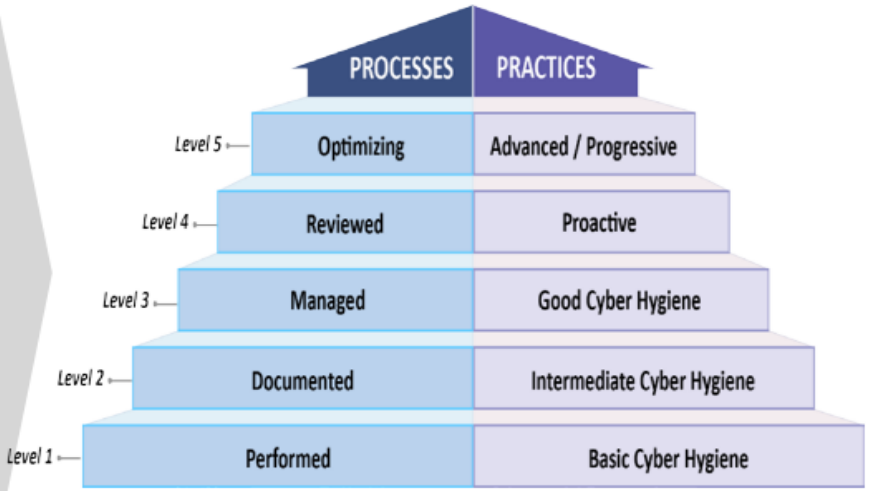
CMMC Level	Practices	Processes
Level 1	17	-
Level 2	55	2
Level 3	58	1
Level 4	26	1
Level 5	15	1

CMMC Model Structure

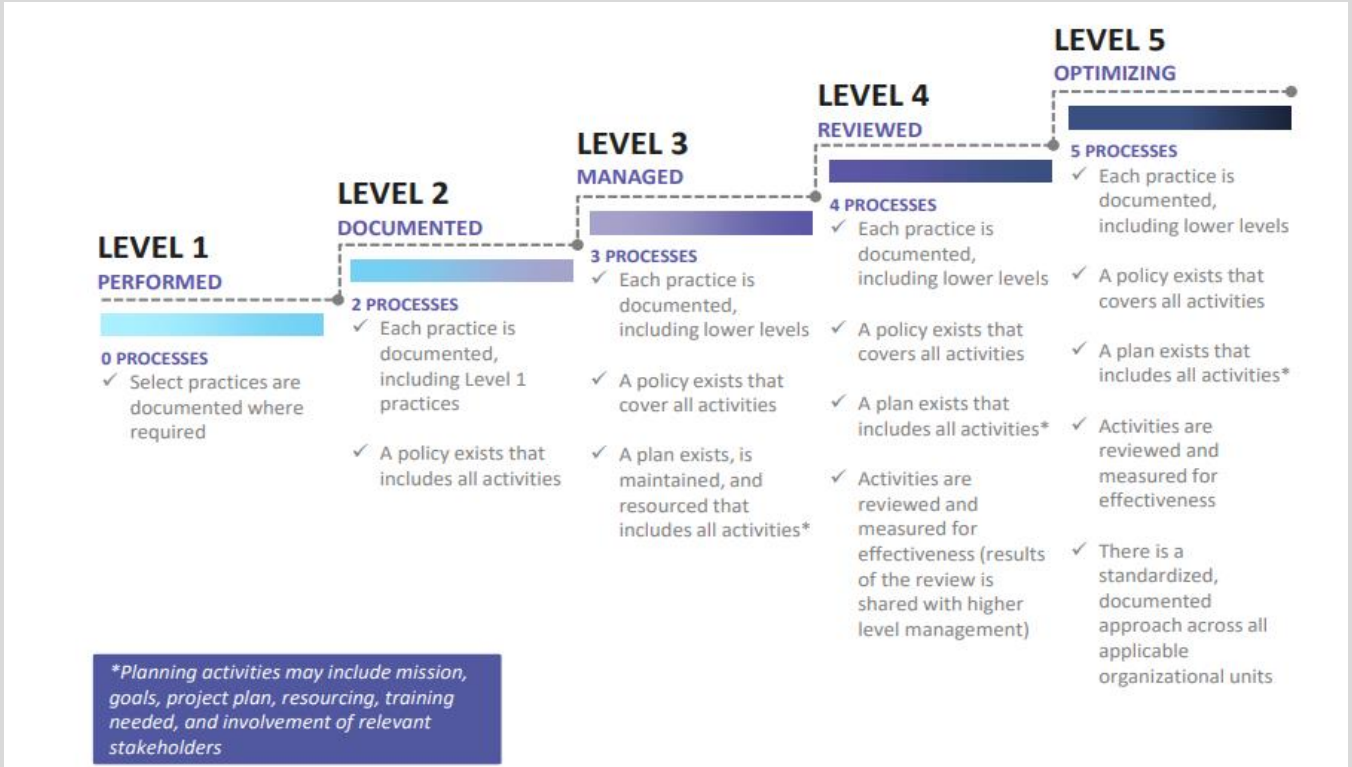
17 Capability Domains

Access Control (AC)	Incident Response (IR)	Risk Management (RM)
Asset Management (AM)	Maintenance (MA)	Security Assessment (CA)
Awareness and Training (AT)	Media Protection (MP)	Situational Awareness (SA)
Audit and Accountability (AU)	Personnel Security (PS)	System and Communications Protection (SC)
Configuration Management (CM)	Physical Protection (PE)	System and Information Integrity (SI)
Identification and Authentication (IA)	Recovery (RE)	

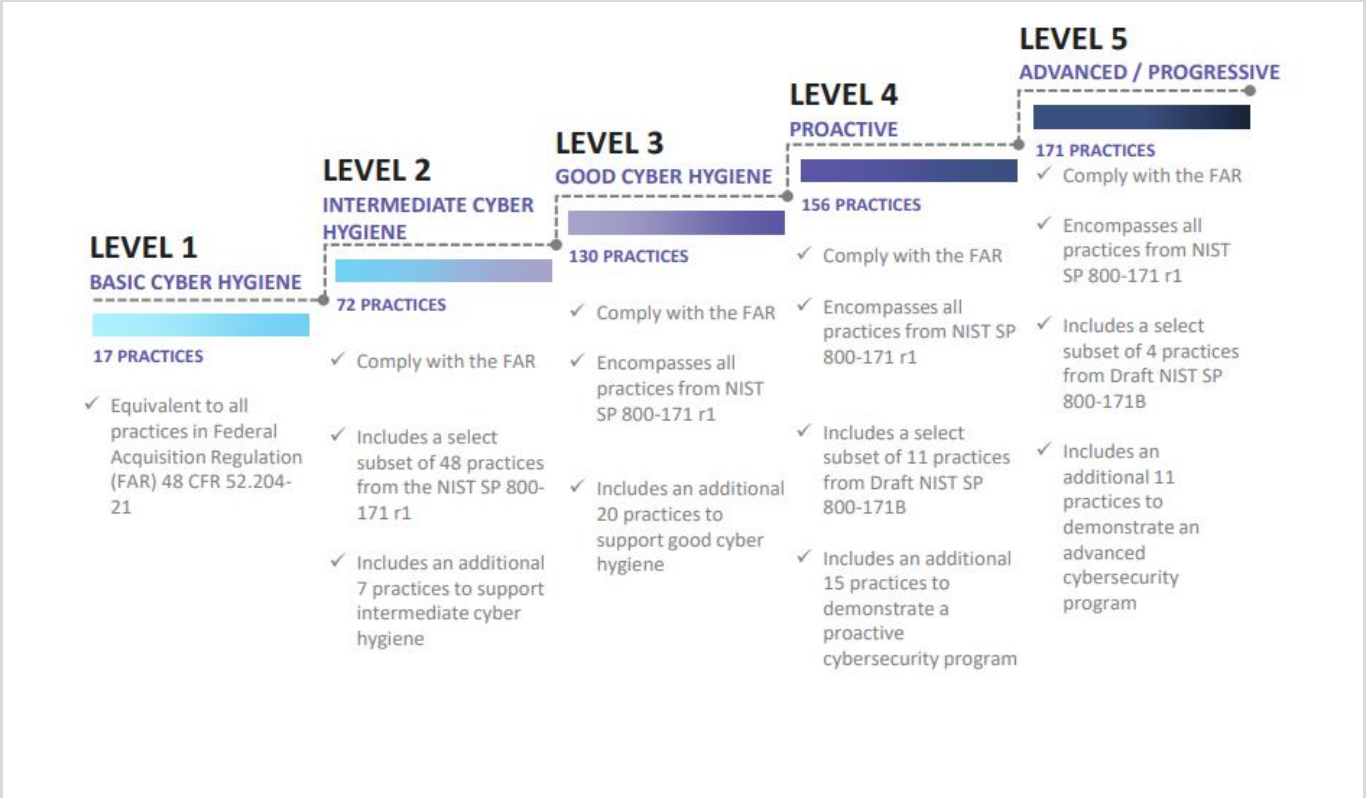
CMMC model with 5 levels measures cybersecurity maturity



CMMC Maturity Process Progression



CMMC Practices Progression



CMMC Capabilities

Domain	Capability
Access Control (AC)	• Establish system access requirements • Control internal system access • Control remote system access • Limit data access to authorized users and processes
Asset Management (AM)	• Identify and document assets
Audit and Accountability (AU)	• Define audit requirements • Perform auditing • Identify and protect audit information • Review and manage audit logs
Awareness and Training (AT)	• Conduct security awareness activities • Conduct training
Configuration Management (CM)	• Establish configuration baselines • Perform configuration and change management
Identification and Authentication (IA)	• Grant access to authenticated entities
Incident Response (IR)	• Plan incident response • Detect and report events • Develop and implement a response to a declared incident • Perform post incident reviews • Test incident response
Maintenance (MA)	• Manage maintenance
Media Protection (MP)	• Identify and mark media • Protect and control media • Sanitize media • Protect media during transport

CMMC Practices – Example

ACCESS CONTROL (AC)

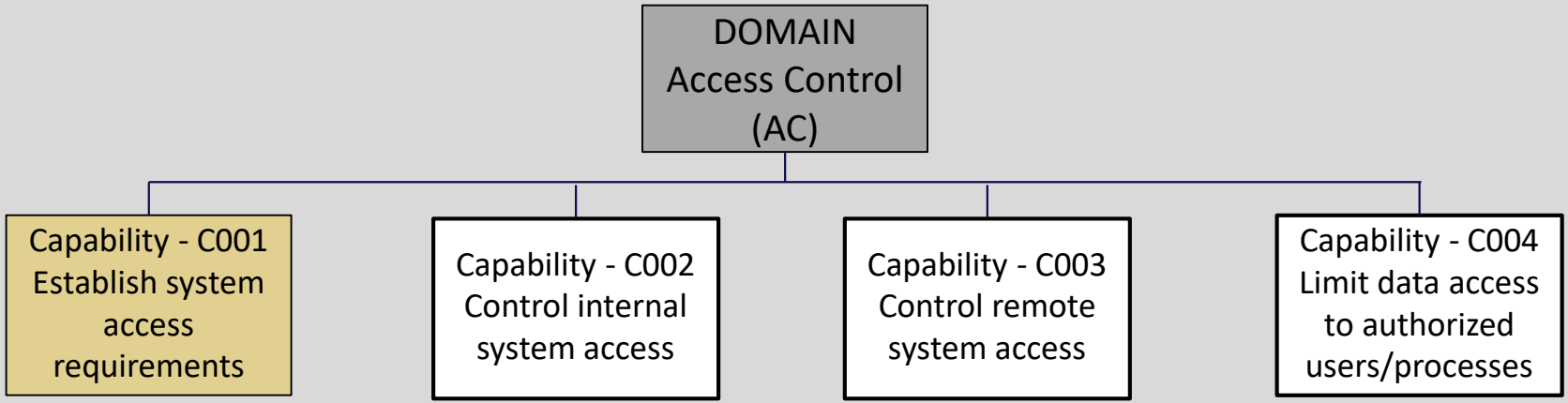
Level 1

AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
AC.1.003	Verify and control/limit connections to and use of external information systems.
AC.1.004	Control information posted or processed on publicly accessible information systems.

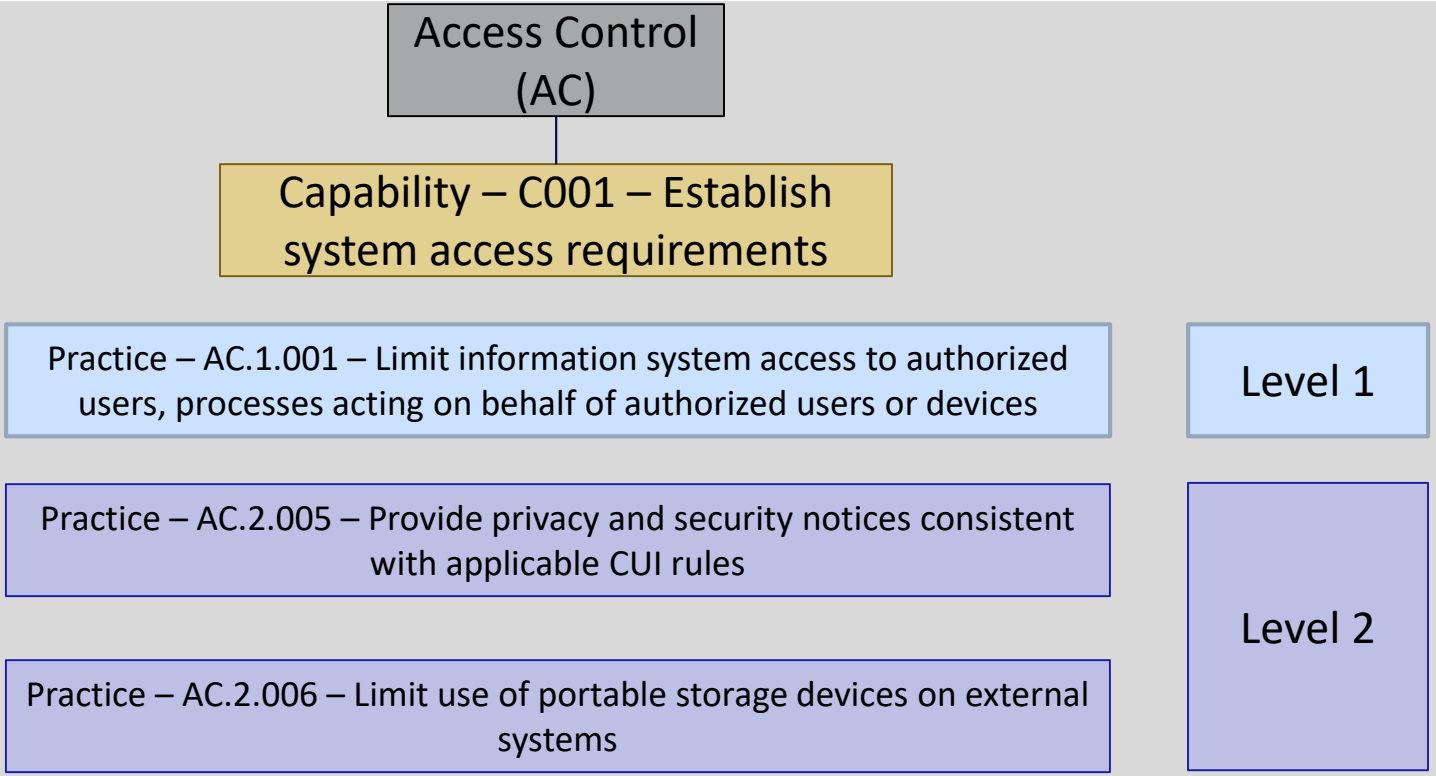
Level 2

AC.2.005	Provide privacy and security notices consistent with applicable CUI rules.
AC.2.006	Limit use of portable storage devices on external systems.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.
AC.2.008	Use non-privileged accounts or roles when accessing nonsecurity functions.
AC.2.009	Limit unsuccessful logon attempts.
AC.2.010	Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.
AC.2.011	Authorize wireless access prior to allowing such connections.
AC.2.013	Monitor and control remote access sessions.
AC.2.015	Route remote access via managed access control points.
AC.2.016	Control the flow of CUI in accordance with approved authorizations.

Example – Access Control Domain



Example – AC – C001



Example – Domain, Capability, Practices

ACCESS CONTROL (AC)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C001 Establish system access requirements	AC.1.001 Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). • FAR Clause 52.204-21 b.1.i • NIST SP 800-171 Rev 1 3.1.1 • CIS Controls v7.1 1.4, 1.6, 5.1, 14.6, 15.10, 16.8, 16.9, 16.11 • NIST CSF v1.1 PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-6, PR.PT-3, PR.PT-4 • CERT RMM v1.2 TM:SG4.SP1 • NIST SP 800-53 Rev 4 AC-2, AC-3, AC-17 • AU ACSC Essential Eight	AC.2.005 Provide privacy and security notices consistent with applicable CUI rules. • NIST SP 800-171 Rev 1 3.1.9 • NIST SP 800-53 Rev 4 AC-8			
		AC.2.006 Limit use of portable storage devices on external systems. • NIST SP 800-171 Rev 1 3.1.21 • CIS Controls v7.1 13.7, 13.8, 13.9 • NIST CSF v1.1 ID.AM-4, PR.PT-2 • NIST SP 800-53 Rev 4 AC-20(2)			

Access Control – C002 - Practices

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C002 Control internal system access	AC.1.002 Limit information system access to the types of transactions and functions that authorized users are permitted to execute. • FAR Clause 52.204-21 b.1.ii • NIST SP 800-171 Rev 1 3.1.2 • CIS Controls v7.1 1.4, 1.6, 5.1, 8.5, 14.6, 15.10, 16.8, 16.9, 16.11 • NIST CSF v1.1 PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-6, PR.PT-3, PR.PT-4 • CERT RMM v1.2 TM:SG4.SP1 • NIST SP 800-53 Rev 4 AC-2, AC-3, AC-17	AC.2.007 Employ the principle of least privilege, including for specific security functions and privileged accounts. • NIST SP 800-171 Rev 1 3.1.5 • CIS Controls v7.1 14.6 • NIST CSF v1.1 PR.AC-4 • CERT RMM v1.2 KIM:SG4.SP1 • NIST SP 800-53 Rev 4 AC-6, AC-6(1), AC-6(5) • UK NCSC Cyber Essentials	AC.3.017 Separate the duties of individuals to reduce the risk of malevolent activity without collusion. • NIST SP 800-171 Rev 1 3.1.4 • NIST CSF v1.1 PR.AC-4 • NIST SP 800-53 Rev 4 AC-5	AC.4.023 Control information flows between security domains on connected systems. • CMMC modification of Draft NIST SP 800-171B 3.1.3e • CIS Controls v7.1 12.1, 12.2, 13.1, 13.3, 14.1, 14.2, 14.5, 14.6, 14.7, 15.6, 15.10 • NIST CSF v1.1 ID.AM-3, PR.AC-5, PR.DS-5, PR.PT-4, DE.AE-1 • NIST SP 800-53 Rev 4 AC-4, AC-4(1), AC-4(6), AC-4(8), AC-4(12), AC-4(13), AC-4(15), AC-4(20), SC-46	AC.5.024 Identify and mitigate risk associated with unidentified wireless access points connected to the network. • CMMC • CIS Controls v7.1 15.3 • NIST CSF v1.1 PR.DS-5, DE.AE-1, DE.CM-7 • NIST SP 800-53 Rev 4 SI-4(14)
		AC.2.008 Use non-privileged accounts or roles when accessing nonsecurity functions. • NIST SP 800-171 Rev 1 3.1.6 • CIS Controls v7.1 4.3, 4.6 • NIST CSF v1.1 PR.AC-4 • NIST SP 800-53 Rev 4 AC-6(2) • UK NCSC Cyber Essentials	AC.3.018 Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs. • NIST SP 800-171 Rev 1 3.1.7 • NIST CSF v1.1 PR.AC-4 • CERT RMM v1.2 KIM:SG4.SP1 • NIST SP 800-53 Rev 4 AC-6(9), AC-6(10)	AC.4.025 Periodically review and update CUI program access permissions. • CMMC	
		AC.2.009 Limit unsuccessful logon attempts. • NIST SP 800-171 Rev 1 3.1.8 • NIST CSF v1.1 PR.AC-7 • NIST SP 800-53 Rev 4 AC-7	AC.3.019 Terminate (automatically) user sessions after a defined condition. • NIST SP 800-171 Rev 1 3.1.11 • CIS Controls v7.1 16.7, 16.11 • NIST SP 800-53 Rev 4 AC-12		
		AC.2.010 Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity. • NIST SP 800-171 Rev 1 3.1.10 • CIS Controls v7.1 16.11 • NIST SP 800-53 Rev 4 AC-11, AC-11(1)	AC.3.012 Protect wireless access using authentication and encryption. • NIST SP 800-171 Rev 1 3.1.17 • CIS Controls v7.1 15.7, 15.8 • NIST CSF v1.1 PR.PT-4 • CERT RMM v1.2 KIM:SG4.SP1 • NIST SP 800-53 Rev 4 AC-18(1)		

How CMMC Will Be Managed

- CMMC Accreditation Body [CMMC-AB] – will oversee the training, quality, and administration of third party assessment organizations. CAB consists of 13 individuals from industry, the cybersecurity community, and academia.
- CMMC Third Party Assessment Organizations [C3PAOs] will be assessors – will be assessed and trained by the CMMC-AB
- CMMC Training – the Defense Acquisition University [DAU] will be performing training for contractors and acquisition professionals starting in July 2020. PTACs will also provide training events and seminars to assist small businesses
- CMMC Marketplace Portal – companies will use to schedule their audits
- CMMC Flow-down – level flow-down will follow the FCI/CUI. If a contractor won't receive or touch CUI, then most likely will be required to meet Level 1

CMMC Structure

- **Certified Professional (CP)** – trained, tested, and certified professionals who demonstrate a working knowledge of the CMMC model. CPs can support organizations working towards CMMC compliance. This is the base individual certification offered by CMMC-AB and a prerequisite for achieving all other certifications. CPs are not CMMC-AB employees.

- **Certified Assessor (CA)** – Trained, tested, and certified professionals authorized by CMMC-AB to deliver assessments under a contract with a Certified Third-Party Organization (C3PAO). CAs are not CMMC-AB employees.

CMMC Structure

- **Certified 3rd Party Assessment Organization (“C3PAO”)** – An Entity with which at least two Assessors is associated and to which a License has been issued.

- **CMMC Certified Entity** – An Entity whose cybersecurity program has received a CMMC Certificate from the CMMC-AB.
- **Trainer** – A person Licensed to provide Training to prospective and current Assessors. The Trainers are not CMMC-AB employees.

- **License** – A document issued to an Assessor, C3PAO, or Trainer, as appropriate, entitling them to perform their duties with respect to the CMMC-AB

CMMC Structure

- **Licensed Partner Publisher (LPP)** – A commercial or academic organization licensed by CMMC-AB to produce training curriculum and materials based on AB Learning Objectives to adequately prepare students for exams, and subsequently employed by an LTP.

- **Licensed Training Provider (LTP)** – A commercial or academic organization that markets, advertises, and delivers CMMC Certified Training using content licensed from LPPs and based on learning objectives and exams from the CMMC-AB. Certified classes delivered by LTPs must be taught or facilitated by CMMC-AB Certified Instructors.

Cost of Certification

- Cost of certification – minimal for Level 1; increase significantly at Level 3 and will be even higher at Levels 4/5
- Costs of CMMC system are allowable and reimbursable – should be like any other OH cost – rolled into rates
- DoD perspective – DFARS has required self attestation to cybersecurity compliance for several years, so companies should already have controls in place if they have worked on defense contracts

CMMC Timeline

- January 31, 2020 – CMMC 1.0 released
- March 18, 2020 – CMMC 1.02 released
- 2nd qtr. 2020 – CMMC marketplace created
- 3rd qtr. 2020 – CMMC requirements in select RFIs; DAU initiates training; new CMMC DFAR regulation rolled out (regulation roll-out may be delayed due to COVID-19). CMMC-AB begins training assessors.
- 4th qtr. 2020 – CMMC requirements in select RFPs, SBIR/STTRs, etc.
- January, 2026 - All new DoD contracts will contain the CMMC requirements

Where Do We Start?

1. *Tone at the top is critical – treat CMMC as an opportunity to do your part to protect National Security.*
2. **LEVEL 1**: Maps to FAR Clause 52.204.21. Basic cyber hygiene. 85% of DIB will be Level 1
3. **LEVELS 2 & 3**: Maps to NIST 800-171 rev. 1, plus additional practices; 48 practices to meet Level 2, additional 45 practices to meet Level 3. No RFPs at Level 2 – considered a "transition" to get to Level 3
4. **LEVELS 4 & 5**: NIST 800-171b – for Advanced Persistent Threats [APT]and High Value Assets [HVA]. Less than 1% of DIB will be Level 4 or 5
5. Use SANS policy templates to develop your company's CMMC program

Key Points

- CMMC certification will be required at time of contract award
- No fines associated with non-compliance
- If a company is believed to never receive or touch CUI, then will be required to meet Level 1
- If there is a chance a company will touch CUI, then they will be required to meet Level 3 [at a minimum]
- SAM registrations will be automatically updated with CMMC Level certification

Looking to the Future

- CMMC will likely replace ISO 27001 and SOC 2
- Other departments of the federal government will likely begin to require compliance to CMMC
- Anticipate CMMC being adopted internationally in 2021
- CMMC-AB working on mapping and reciprocity with ISO 27001 and FEDRAMP

Important Links

- CMMC v1.02 [Right click on link, then select Open Hyperlink]
- CMMC Appendices
- CMMC-Accreditation Body
- FAR Clause 52.204-21
- NIST SP 800-171 r2
- NIST SP 800-171b [for critical programs and high value assets]
- SANS Cybersecurity Policies
- NCSU Cyber Toolkit

NORTH CAROLINA MILITARY BUSINESS CENTER

CYBERSECURITY MATURITY MODEL CERTIFICATION V1.02