ncmbc
CONNECTING BUSINESS AND MILITARY

# NORTH CAROLINA MILITARY BUSINESS CENTER

## DEPT. OF DEFENSE CYBERSECURITY REGULATIONS

INCLUDING

## CYBERSECURITY MATURITY MODEL CERTIFICATION – CMMC

AND

## DFARS 252.204-7012 AND THE DFARS INTERIM RULE

WWW.NCMBC.US

30 November 2020

# Why is Cybersecurity So Important?

***DATA IS THE NEW CURRENCY***

**Rule the data,
rule the world…**

# Cybersecurity Regulations Terminology

- FAR:  Federal Acquisition Regulation – all the regulations associated with federal procurement
- DFARS: Defense Federal Acquisition Regulation Supplement – acquisition regulations for the Dept. of Defense
- NIST SP 800-171:  National Institute of Standards and Technology Special Publication that contains 110 cybersecurity controls

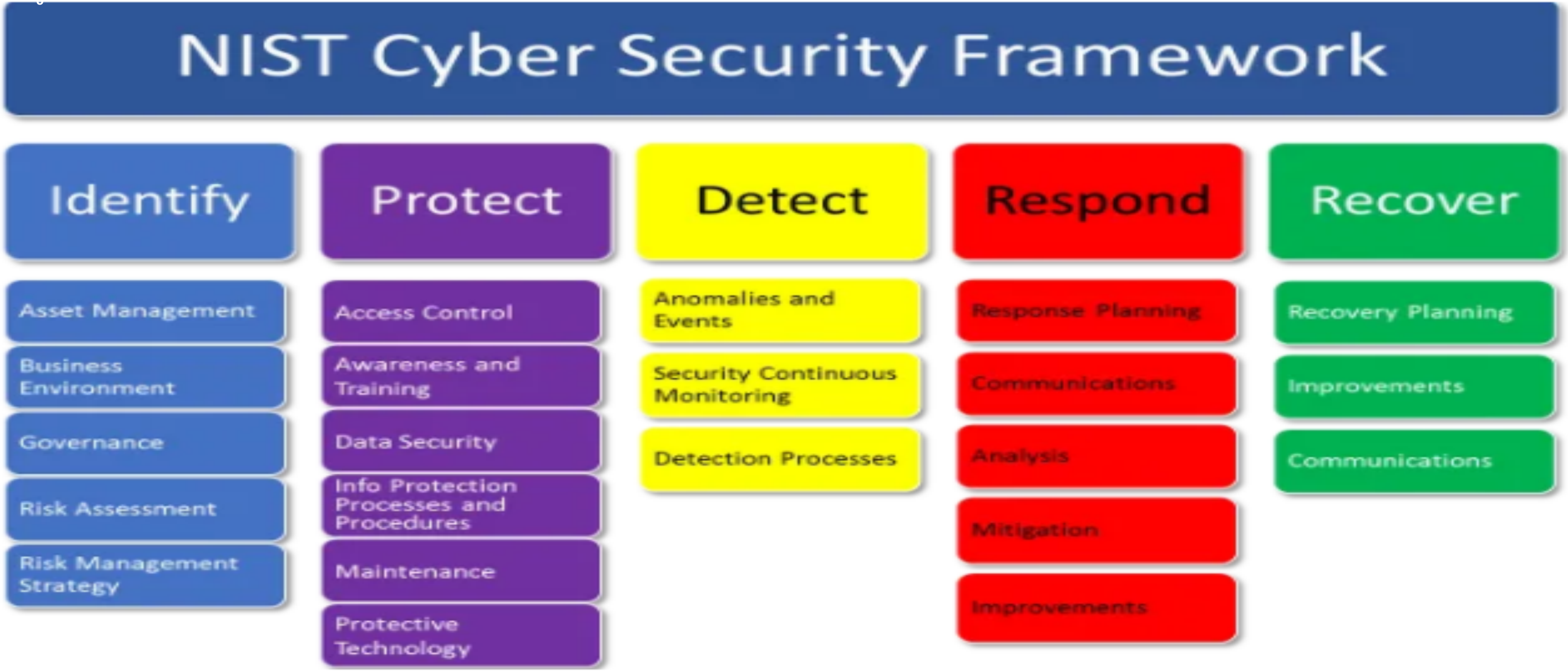
# Cybersecurity Regulations

- **FAR 52.204-21** – “Basic Safeguarding of Covered Contractor Information Systems.” Maps to practices in CMMC Level 1.
- **DFARS 252.204-7012** – “Safeguarding Covered Defense Information and Cyber Incident Reporting.” Requires protection of CUI by compliance to the 110 cybersecurity controls in NIST SP 800-171. Contractors could self-attest to compliance. **Modified by DFARS Interim Rule.**
- **CMMC** – Cybersecurity Maturity Model Certification – requires physical cybersecurity assessment and certification to a CMMC level of maturity. First 15 RFPs will CMMC requirements in 2021.
- **DFARS Interim Rule** – implements CMMC AND modifies DFARS 252.204-7012 to include a self-assessment using the Department of Defense Assessment Methodology, which must be uploaded to the Supplier Performance Risk System. Effective date: 30 Nov 2020. Will be phased-in over a 3-year period.

# What is CMMC?

- Unified cybersecurity standard for DoD acquisitions – eliminates confusion created by multiple regulations. Best cybersecurity practices.
- 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 ***program***. As with other quality management systems and maturity models it requires a culture change.
- Based on CMMI – developed by Carnegie Mellon and Johns Hopkins using the NIST Cybersecurity Framework, NIST SP 800-171 and other cybersecurity regulations.
- **CMMC is foundational** – as important as cost, schedule and performance – non-negotiable.

# NIST Cybersecurity Framework



## NIST Cyber Security Framework

| Identify | Protect | Detect | Respond | Recover |
|---|---|---|---|---|
| Asset Management | Access Control | Anomalies and Events | Response Planning | Recovery Planning |
| Business Environment | Awareness and Training | Security Continuous Monitoring | Communications | Improvements |
| Governance | Data Security | Detection Processes | Analysis | Communications |
| Risk Assessment | Info Protection Processes and Procedures | | Mitigation | |
| Risk Management Strategy | Maintenance | | Improvements | |
| | Protective Technology | | | |

# Why Do We Need CMMC?

- 70% to 80% of DoD data resides on contractors’ networks - and there are over 300,000 companies in the Defense Industrial Base [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 [110 security controls], so companies didn’t comply
- Current cybersecurity requirements don’t go far enough to protect CUI against advanced persistent threats.
- Part of “supply chain illumination” – requires in-person audits - reveal bad actors

# Who Has to Comply with CMMC?

- Any organization in the DoD supply chain that processes, stores and/or transmits FCI or CUI. Includes SBIR/STTR and grant recipients.
- Any organization that provides protection for FCI or CUI. **Note: that includes Managed Service Providers and Cloud Service Providers.**
- 60% of the Defense Industrial Base will need to be compliant with CMMC Level 1; 30% will need to be compliant to CMMC Level 3; less than 2% need to be compliant with CMMC Levels 4 and 5.
- Most Commercial-off-the-Shelf suppliers will not be required to be compliant with CMMC – yet…

# CMMC Timeline

January 31, 2020 – CMMC 1.0 released

March 18, 2020 – CMMC 1.02 released; signed MOU transferring CMMC from DoD to the CMMC-AB

2nd qtr. 2020 – CMMC marketplace created

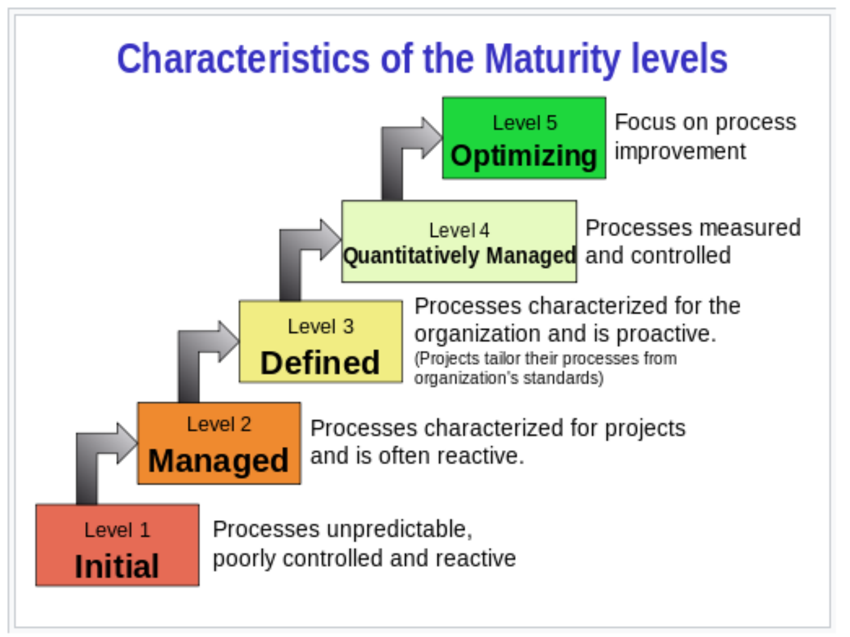
3rd qtr. 2020 – Defense Acquisition University initiates training; CMMC-AB begins training assessors.

4th qtr. 2020 – 1st qtr. 2021 - CMMC DFARS regulation rolled out; CMMC requirements in select RFPs, SBIR/STTRs, grants etc.

October 2025- All new DoD contracts will contain CMMC requirements

# What is a Maturity Model?

- Provides a benchmark against which an organization can evaluate the current level of capability of its 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.



Characteristics of the Maturity levels

Level 5 **Optimizing** – Focus on process improvement

Level 4 **Quantitatively Managed** – Processes measured and controlled

Level 3 **Defined** – Processes characterized for the organization and is proactive. (Projects tailor their processes from organization's standards)

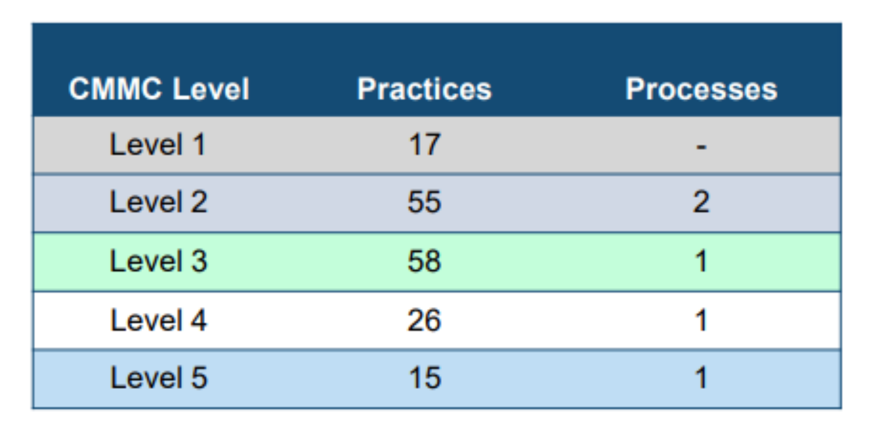
Level 2 **Managed** – Processes characterized for projects and is often reactive.

Level 1 **Initial** – Processes unpredictable, poorly controlled and reactive

# Domains, Capabilities, Processes and Practices

CMMC Model V 1.02 encompasses the following:

- 17 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 adds 15 practices to all the practices in Levels 1 – 4.



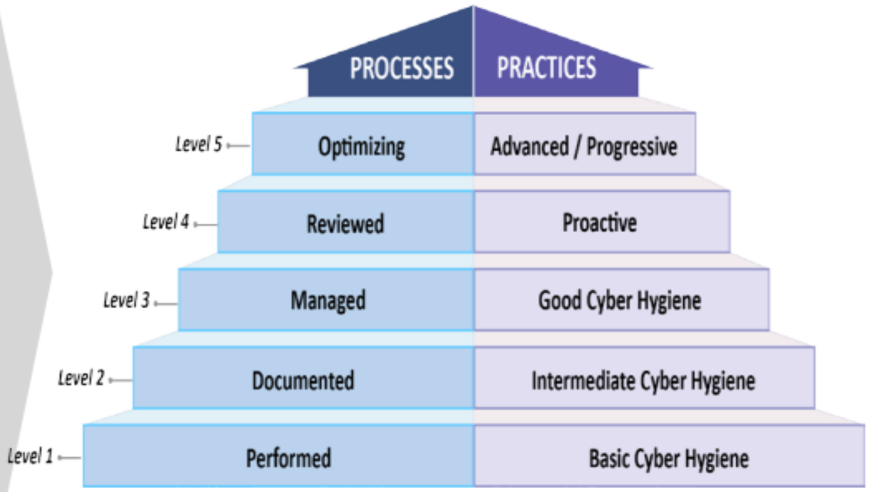
| CMMC Level | Practices | Processes |
|---|---|---|
| Level 1 | 17 | - |
| Level 2 | 55 | 2 |
| Level 3 | 58 | 1 |
| Level 4 | 26 | 1 |
| Level 5 | 15 | 1 |

# CMMC Model Structure

## 17 Capability Domains

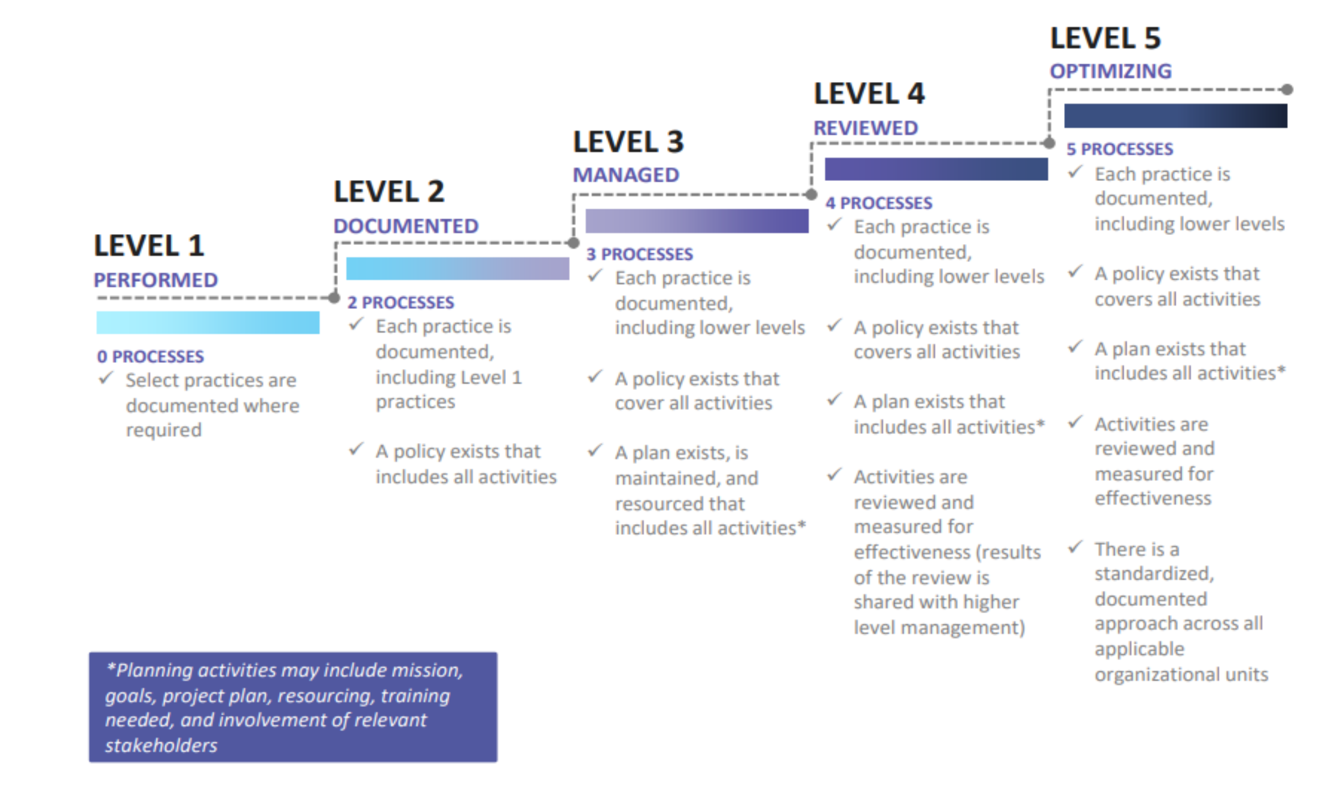
| | | |
|---|---|---|
| Access Control (AC) | Incident Response (IR) | Risk Management (RM) |
| Asset Management (AM) | Maintenance (MA) | Security Assessment (CA) |
| Awareness and Training (AT) | Media Protection (MP) | Situational Awareness (SA) |
| Audit and Accountability (AU) | Personnel Security (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



| | PROCESSES | PRACTICES |
|---|---|---|
| Level 5 | Optimizing | Advanced / Progressive |
| Level 4 | Reviewed | Proactive |
| Level 3 | Managed | Good Cyber Hygiene |
| Level 2 | Documented | Intermediate Cyber Hygiene |
| Level 1 | Performed | Basic Cyber Hygiene |

# CMMC Maturity Process Progression



**LEVEL 1**
**PERFORMED**

**0 PROCESSES**
- ✓ Select practices are documented where required

**LEVEL 2**
**DOCUMENTED**

**2 PROCESSES**
- ✓ Each practice is documented, including Level 1 practices
- ✓ A policy exists that includes all activities

**LEVEL 3**
**MANAGED**

**3 PROCESSES**
- ✓ Each practice is documented, including lower levels
- ✓ A policy exists that cover all activities
- ✓ A plan exists, is maintained, and resourced that includes all activities*

**LEVEL 4**
**REVIEWED**

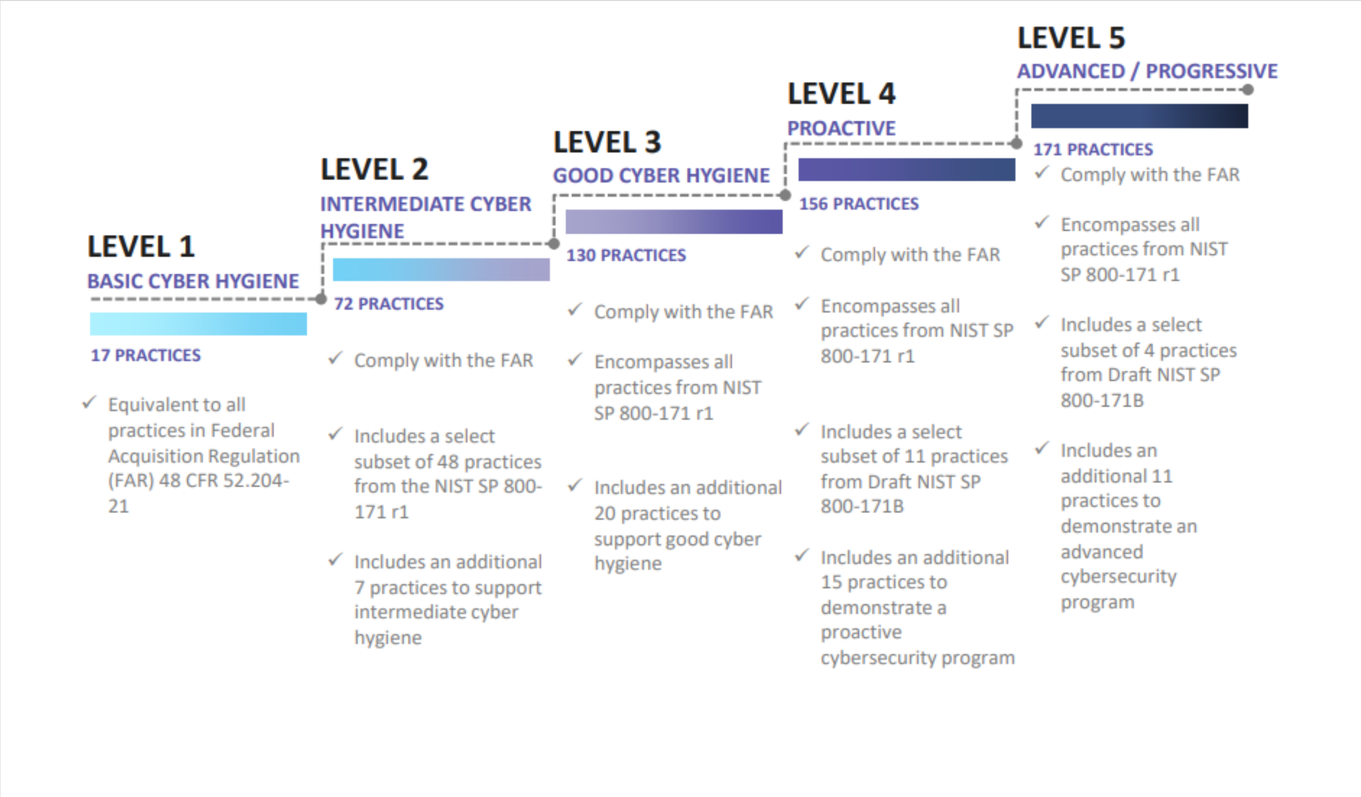
**4 PROCESSES**
- ✓ Each practice is documented, including lower levels
- ✓ A policy exists that covers all activities
- ✓ A plan exists that includes all activities*
- ✓ Activities are reviewed and measured for effectiveness (results of the review is shared with higher level management)

**LEVEL 5**
**OPTIMIZING**

**5 PROCESSES**
- ✓ Each practice is documented, including lower levels
- ✓ A policy exists that covers all activities
- ✓ A plan exists that includes all activities*
- ✓ Activities are reviewed and measured for effectiveness
- ✓ There is a standardized, documented approach across all applicable organizational units

**Planning activities may include mission, goals, project plan, resourcing, training needed, and involvement of relevant stakeholders*

# CMMC Practices Progression



**LEVEL 1**

**BASIC CYBER HYGIENE**

**17 PRACTICES**

- ✓ Equivalent to all practices in Federal Acquisition Regulation (FAR) 48 CFR 52.204-21

**LEVEL 2**

**INTERMEDIATE CYBER HYGIENE**

**72 PRACTICES**

- ✓ Comply with the FAR
- ✓ Includes a select subset of 48 practices from the NIST SP 800-171 r1
- ✓ Includes an additional 7 practices to support intermediate cyber hygiene

**LEVEL 3**

**GOOD CYBER HYGIENE**

**130 PRACTICES**

- ✓ Comply with the FAR
- ✓ Encompasses all practices from NIST SP 800-171 r1
- ✓ Includes an additional 20 practices to support good cyber hygiene

**LEVEL 4**

**PROACTIVE**

**156 PRACTICES**

- ✓ Comply with the FAR
- ✓ Encompasses all practices from NIST SP 800-171 r1
- ✓ Includes a select subset of 11 practices from Draft NIST SP 800-171B
- ✓ Includes an additional 15 practices to demonstrate a proactive cybersecurity program

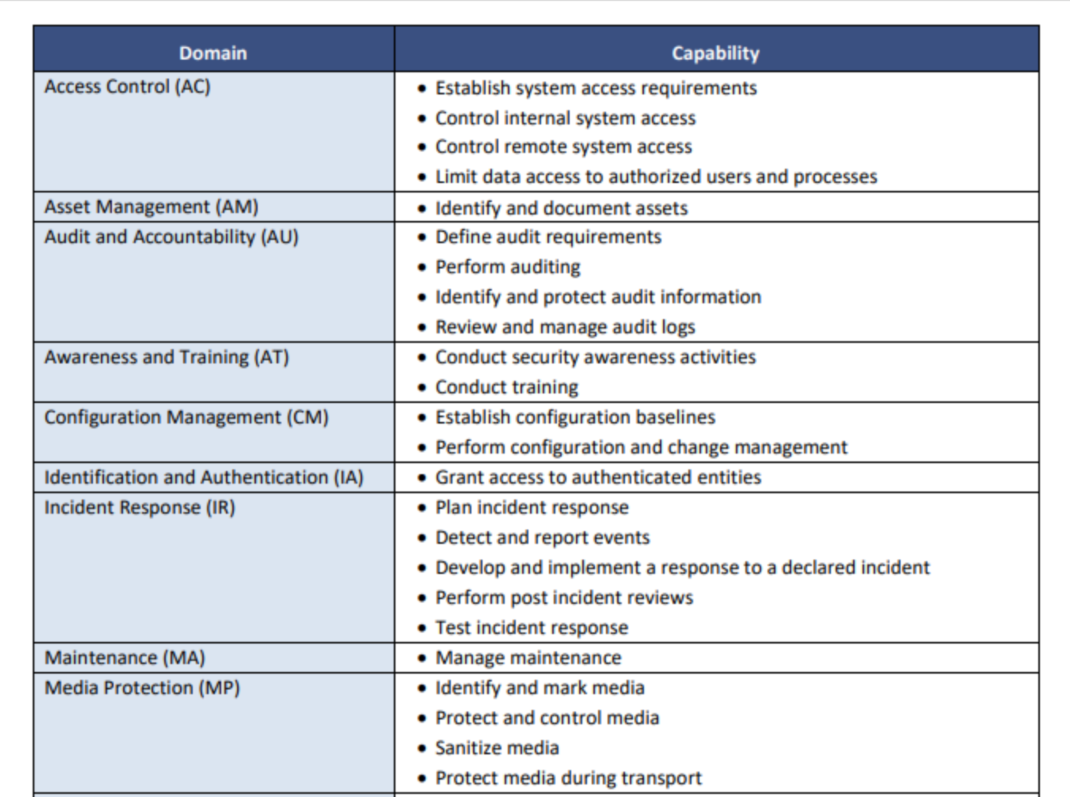
**LEVEL 5**

**ADVANCED / PROGRESSIVE**

**171 PRACTICES**

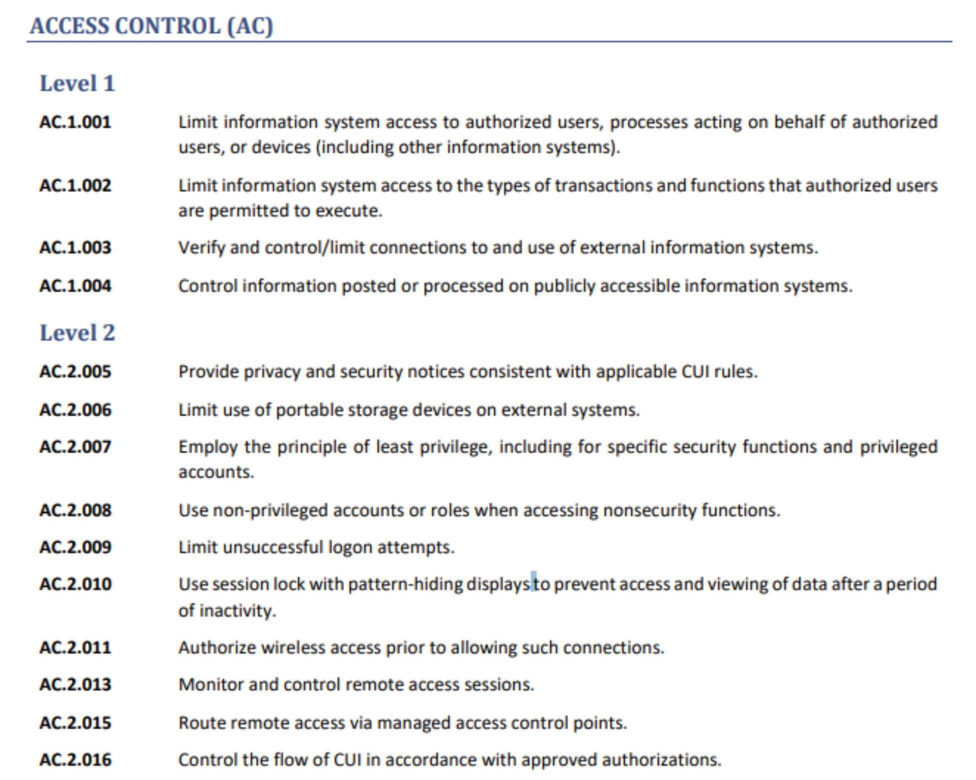
- ✓ Comply with the FAR
- ✓ Encompasses all practices from NIST SP 800-171 r1
- ✓ Includes a select subset of 4 practices from Draft NIST SP 800-171B
- ✓ Includes an additional 11 practices to demonstrate an advanced cybersecurity program

# CMMC Capabilities



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

# CMMC Practices[Controls] – 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.

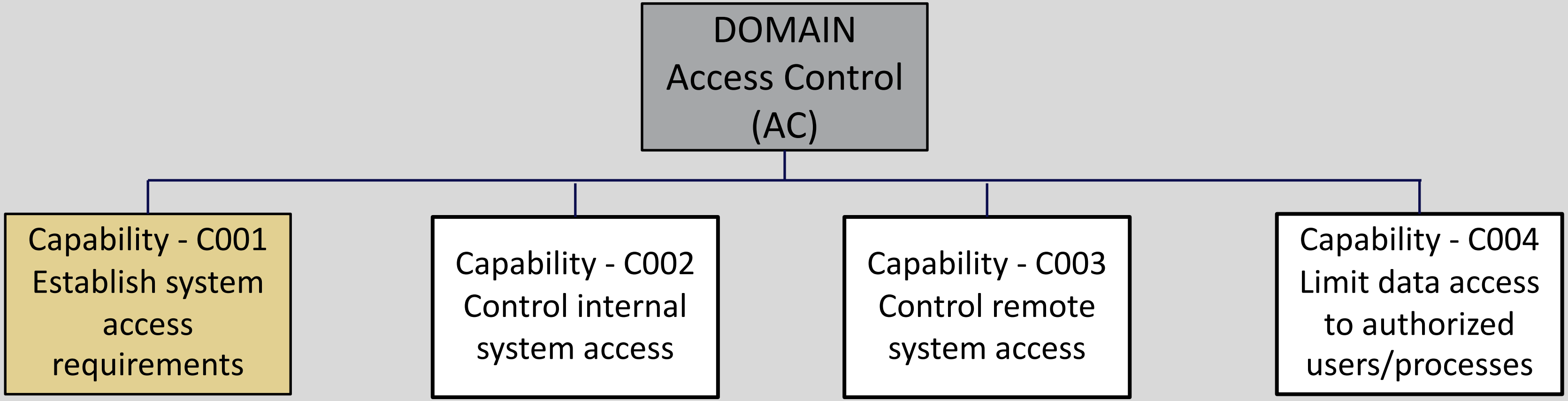
**AC.2.011** Authorize wireless access prior to allowing such connections.

**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



DOMAIN
Access Control
(AC)

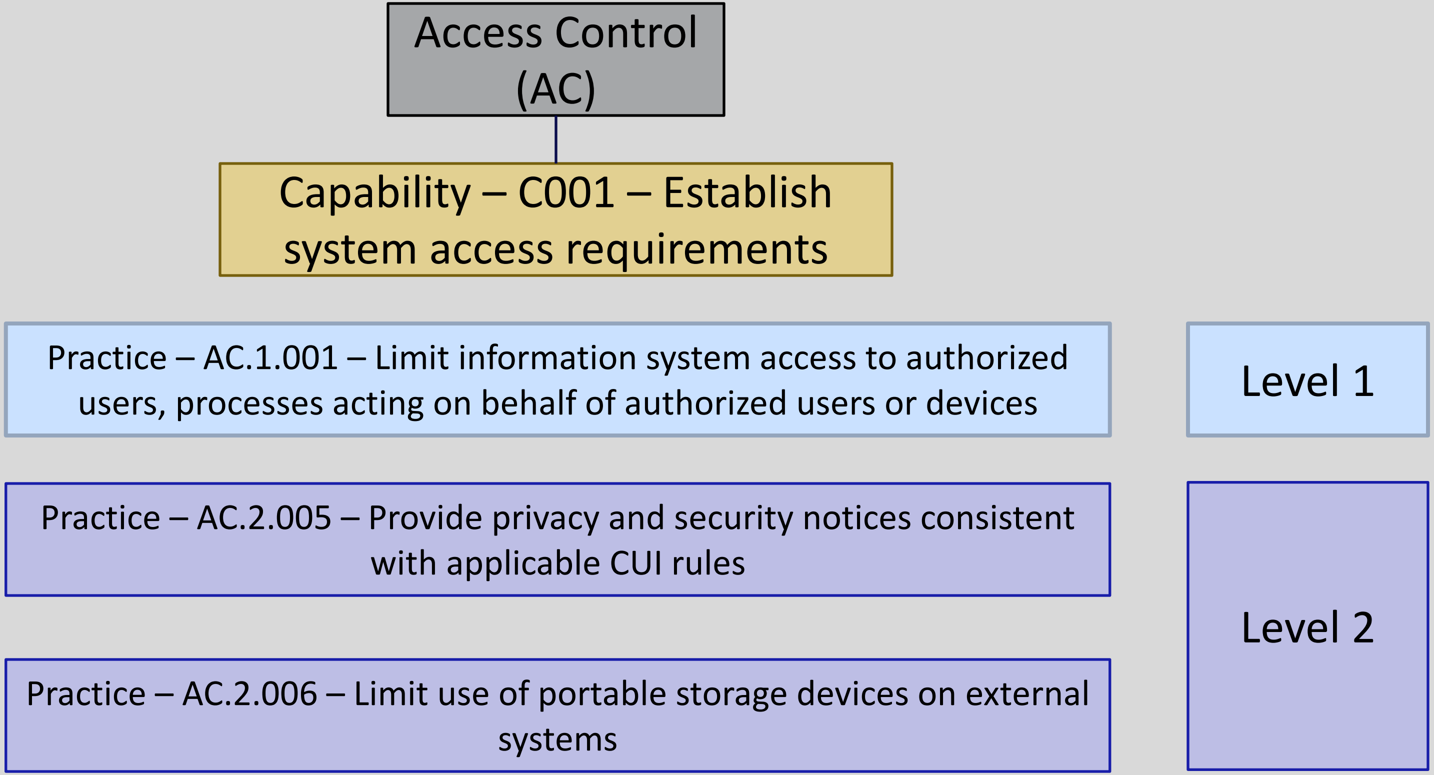
Capability - C001
Establish system access requirements

Capability - C002
Control internal system access

Capability - C003
Control remote system access

Capability - C004
Limit data access to authorized users/processes

# Example – AC – C001



Access Control (AC)

Capability – C001 – Establish system access requirements

Practice – AC.1.001 – Limit information system access to authorized users, processes acting on behalf of authorized users or devices

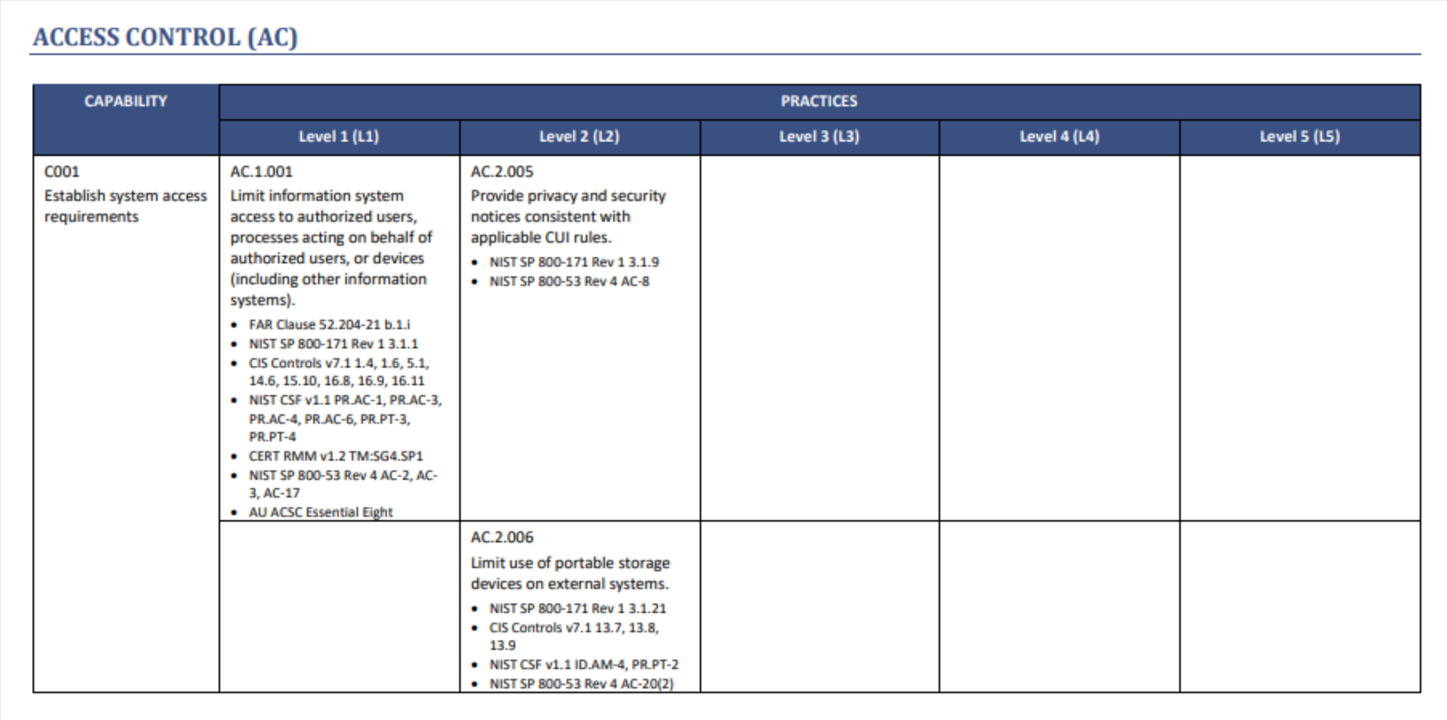
Level 1

Practice – AC.2.005 – Provide privacy and security notices consistent with applicable CUI rules

Practice – AC.2.006 – Limit use of portable storage devices on external systems

Level 2

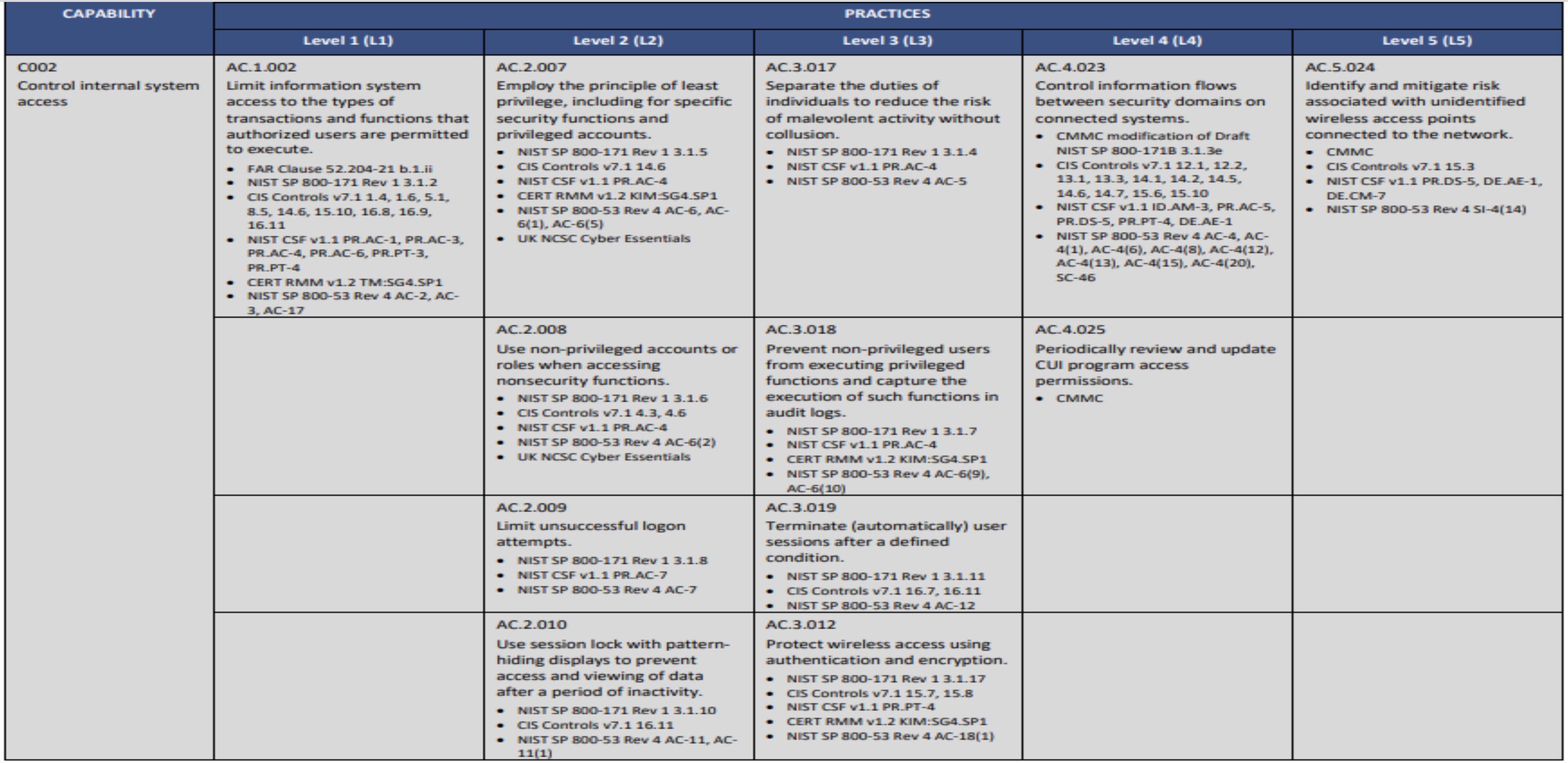
# Example – Domain, Capability, Practices



## ACCESS CONTROL (AC)

| CAPABILITY | PRACTICES | | | | |
|---|---|---|---|---|---|
| | Level 1 (L1) | Level 2 (L2) | Level 3 (L3) | Level 4 (L4) | Level 5 (L5) |
| C001<br>Establish system access requirements | AC.1.001<br>Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).<br>• FAR Clause 52.204-21 b.1.i<br>• NIST SP 800-171 Rev 1 3.1.1<br>• CIS Controls v7.1 1.4, 1.6, 5.1, 14.6, 15.10, 16.8, 16.9, 16.11<br>• NIST CSF v1.1 PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-6, PR.PT-3, PR.PT-4<br>• CERT RMM v1.2 TM:SG4.SP1<br>• NIST SP 800-53 Rev 4 AC-2, AC-3, AC-17<br>• AU ACSC Essential Eight | AC.2.005<br>Provide privacy and security notices consistent with applicable CUI rules.<br>• NIST SP 800-171 Rev 1 3.1.9<br>• NIST SP 800-53 Rev 4 AC-8 | | | |
| | | AC.2.006<br>Limit use of portable storage devices on external systems.<br>• NIST SP 800-171 Rev 1 3.1.21<br>• CIS Controls v7.1 13.7, 13.8, 13.9<br>• NIST CSF v1.1 ID.AM-4, PR.PT-2<br>• 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<br>Control internal system access | AC.1.002<br>Limit information system access to the types of transactions and functions that authorized users are permitted to execute.<br>• FAR Clause 52.204-21 b.1.ii<br>• NIST SP 800-171 Rev 1 3.1.2<br>• CIS Controls v7.1 1.4, 1.6, 5.1, 8.5, 14.6, 15.10, 16.8, 16.9, 16.11<br>• NIST CSF v1.1 PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-6, PR.PT-3, PR.PT-4<br>• CERT RMM v1.2 TM:SG4.SP1<br>• NIST SP 800-53 Rev 4 AC-2, AC-3, AC-17 | AC.2.007<br>Employ the principle of least privilege, including for specific security functions and privileged accounts.<br>• NIST SP 800-171 Rev 1 3.1.5<br>• CIS Controls v7.1 14.6<br>• NIST CSF v1.1 PR.AC-4<br>• CERT RMM v1.2 KIM:SG4.SP1<br>• NIST SP 800-53 Rev 4 AC-6, AC-6(1), AC-6(5)<br>• UK NCSC Cyber Essentials | AC.3.017<br>Separate the duties of individuals to reduce the risk of malevolent activity without collusion.<br>• NIST SP 800-171 Rev 1 3.1.4<br>• NIST CSF v1.1 PR.AC-4<br>• NIST SP 800-53 Rev 4 AC-5 | AC.4.023<br>Control information flows between security domains on connected systems.<br>• CMMC modification of Draft NIST SP 800-171B 3.1.3e<br>• 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<br>• NIST CSF v1.1 ID.AM-3, PR.AC-5, PR.DS-5, PR.PT-4, DE.AE-1<br>• 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<br>Identify and mitigate risk associated with unidentified wireless access points connected to the network.<br>• CMMC<br>• CIS Controls v7.1 15.3<br>• NIST CSF v1.1 PR.DS-5, DE.AE-1, DE.CM-7<br>• NIST SP 800-53 Rev 4 SI-4(14) |
| | | AC.2.008<br>Use non-privileged accounts or roles when accessing nonsecurity functions.<br>• NIST SP 800-171 Rev 1 3.1.6<br>• CIS Controls v7.1 4.3, 4.6<br>• NIST CSF v1.1 PR.AC-4<br>• NIST SP 800-53 Rev 4 AC-6(2)<br>• UK NCSC Cyber Essentials | AC.3.018<br>Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.<br>• NIST SP 800-171 Rev 1 3.1.7<br>• NIST CSF v1.1 PR.AC-4<br>• CERT RMM v1.2 KIM:SG4.SP1<br>• NIST SP 800-53 Rev 4 AC-6(9), AC-6(10) | AC.4.025<br>Periodically review and update CUI program access permissions.<br>• CMMC | |
| | | AC.2.009<br>Limit unsuccessful logon attempts.<br>• NIST SP 800-171 Rev 1 3.1.8<br>• NIST CSF v1.1 PR.AC-7<br>• NIST SP 800-53 Rev 4 AC-7 | AC.3.019<br>Terminate (automatically) user sessions after a defined condition.<br>• NIST SP 800-171 Rev 1 3.1.11<br>• CIS Controls v7.1 16.7, 16.11<br>• NIST SP 800-53 Rev 4 AC-12 | | |
| | | AC.2.010<br>Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.<br>• NIST SP 800-171 Rev 1 3.1.10<br>• CIS Controls v7.1 16.11<br>• NIST SP 800-53 Rev 4 AC-11, AC-11(1) | AC.3.012<br>Protect wireless access using authentication and encryption.<br>• NIST SP 800-171 Rev 1 3.1.17<br>• CIS Controls v7.1 15.7, 15.8<br>• NIST CSF v1.1 PR.PT-4<br>• CERT RMM v1.2 KIM:SG4.SP1<br>• NIST SP 800-53 Rev 4 AC-18(1) | | |

# How CMMC Will Be Managed – CMMC Ecosystem

**CMMC Accreditation Body [CMMC-AB]** – will oversee the training, quality, and administration of third-party assessment organizations (C3PAOs). CMMC-AB consists of 13 individuals from industry, the cybersecurity community, and academia. CMMC-AB is a 501(c)(3) organization – not part of DoD.

**CMMC Third Party Assessment Organization [C3PAOs]** - manage Certified Assessors (CA)

**Certified Assessor (CA)** - certified to assess companies at different levels – CMMC Levels 1, 3 and 5. CAs can also deliver certified CMMC consulting services

**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 – assessments and consulting

**Registered Practitioners (RP) –** trained in CMMC and can consult

# How CMMC Will Be Managed – CMMC Ecosystem

**CMMC Training –** the Defense Acquisition University [DAU] is providing training to acquisition professionals (contracting officers). Several organizations, including the NC Military Business Center and the Procurement Technical Assistance Centers (PTACs) are developing and providing training to assist businesses with compliance. The NCMBC is working with the DAU so the training we provide is consistent with DAU training.

**CMMC Flow-down –** level flow-down will follow the FCI/CUI. If a contractor won't receive, process, house or create CUI, then they will be required to meet CMMC Level 1 requirements. Just because a prime contractors touches CUI, that doesn't mean their subs/suppliers will.

# DFARS 252.204-7012

Currently, most companies that work directly for the DoD have DFARS 252.204-7012 referenced in their contracts. *HOWEVER, that does not necessarily mean you must be compliant with the DFARS clause*. ***Per the Defense Acquisition University [DAU], the DFARS clause should be referenced in all DoD contracts, but does not have to be complied with if the company does not receive, house, process or create Controlled Unclassified Information.*** In general, if you are supply strictly COTS you do not have to comply with cybersecurity requirements.

Remember – DFARS 252.204-7012 = NIST 800 171 [110 cybersecurity controls]

# New DFARS Rule

Since CMMC will not be fully implemented until October of 2025 – meaning the requirements won't be in 100% of the contracts until then – other cybersecurity requirements will be referenced in contracts.

- If the contract requires the contractor to receive, process, house or create CUI, then it will reference the new DFARS Rule which requires that a formal self-assessment to the NIST 800-171 requirements be done and results submitted to the DoD. The new rule is expected to go into effect November 30, 2020.
- If the contract requires the contractor to receive, process, house or create FCI, then the contract will reference FAR 52.204-21, which requires compliance with 17 controls [equivalent to CMMC Level 1]. [Not COTS]

# FAR/DFARS/New DFARS Rule/CMMC

Current state – FAR 52.204-21 in effect for companies touching FCI [equates to the 17 controls in CMMC Level 1]; DFARS 252-204-7012 [all 110 controls in NIST 800-171] in effect for companies touching CUI – self-attestation to compliance.

November 30, 2020 – December 2025 – FAR 52.204-21 in effect for companies touching FCI; NIST controls apply to companies touching CUI, and formal self-assessment results must be provided to the DoD. CMMC rolled out incrementally.

October 2025 and beyond – only CMMC requirements will be in effect.

# NAICS Codes and CUI

The following 5 NAICS codes will be most affected by the DFARS Interim Rule – majority of CUI in these codes

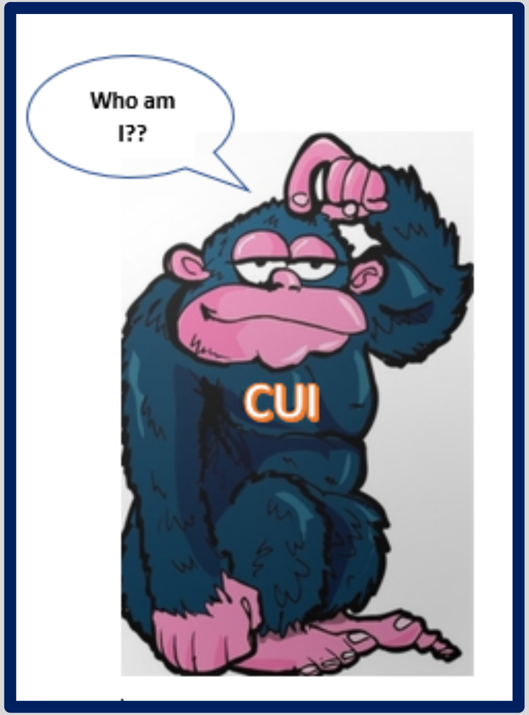
- 541712 - R&D in the Physical, Engineering, and Life Sciences (Except Biotech)
- 541330 – Engineering Services
- 236220 – Commercial and Institutional Building Construction
- 541519 – Other Computer Related Services
- 561210 – Facilities Support Services [base facilities operation support services.]

# CMMC/DFARS

Unfortunately, the contractor is responsible for knowing whether they must be compliant with the DFARS cybersecurity clauses, which means you need to determine if the data is CUI or not.

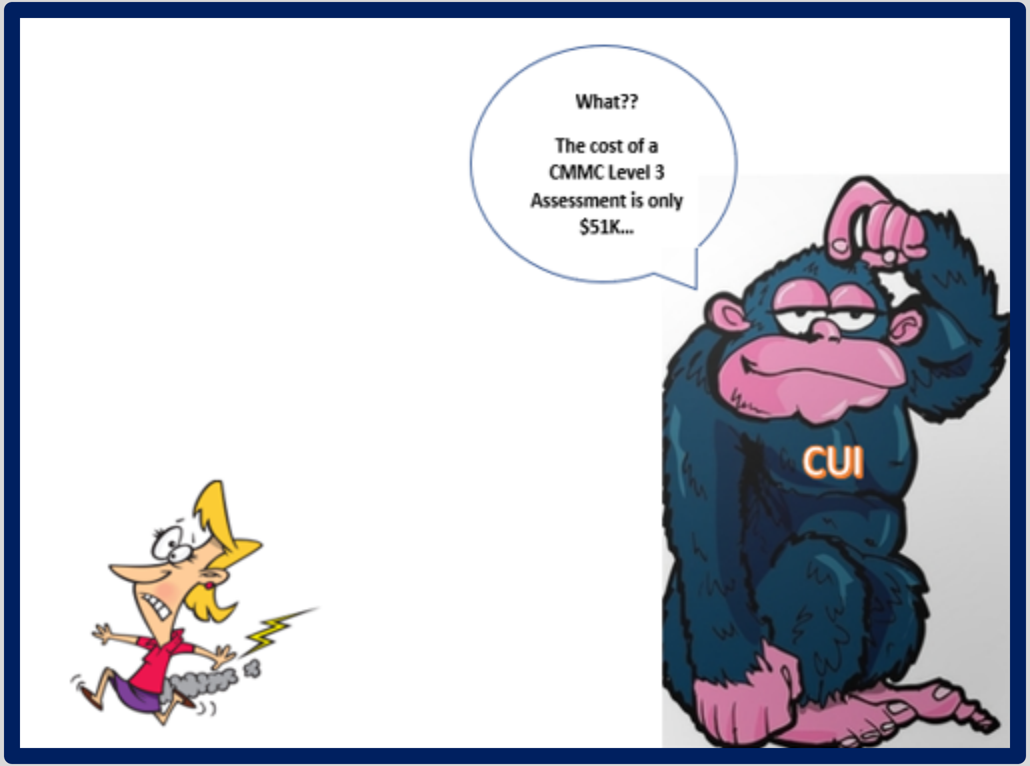
So, how do you know if your company touches CUI?

# CUI – The 900-Pound Gorilla in the Room



- □ Since compliance to NIST 800-171 or CMMC Level 3 is based on the data – CUI, not CUI – it seems logical that there would be a good definition for CUI that everyone could understand…but there isn't.
- □ And, if a company touches CUI, the more expensive it is to set up their cybersecurity system, and the cost of a CMMC Level 3 assessment is exponentially higher than a CMMC Level 1 assessment
- □ So what should we do??

# AVOID CUI!



# AVOID CUI!

- The best way to minimize the cost of securing your network and prevent unauthorized access to CUI is to *avoid touching CUI*. It will require more work on everyone’s part, but it will save time and money, and reduce the risk of our adversaries accessing our data or disrupting our supply chains.
    - Prime contractors - work with your CO/KO to find ways of eliminating the need to receive CUI; for example, discuss the necessity of them sending a complete set of drawings to you. Is it possible to compartmentalize the information sent so that it no longer contains CUI? Can CUI be redacted out of the drawing or information? Is a secure cloud available in which to perform the work? **And figure out ways to eliminate the need for your subs/suppliers to process CUI.**

# AVOID CUI!

Subcontractors/suppliers – you need to collaborate with your primes and ask the same questions. Example:  a prime contractor does not need to send a complete set of drawings to a machine shop that will be fabricating screws. Also, large primes might have secure clouds for sub/suppliers to work in if CUI can't be avoided.

**No CUI = Less Risk and Less Money**

# CUI - COLLABORATION

**Collaboration is the key** – at least until good definitions of CUI are provided or contracts are properly marked.

- Prime contractors should contact their contracting officer[CO/KO] to determine if the contract includes CUI. If the CO/KO doesn’t know, ask them to contact the DoD CUI Office at osd.pentagon.ousd-intel-sec.mbx.dod-cui@mail.mil
- The NCMBC is working with the Defense Acquisition University to make sure they understand the implications of the new cybersecurity standards, as well as the confusion surrounding CUI, so they can provide appropriate training to CO/KOs

# Cost of Certification - CMMC

Recurring costs of implementing CMMC are allowable and reimbursable – should be like any other OH cost – rolled into rates. Non-recurring costs can be billed to the contract directly. Assessment costs amortized over the life of the certification – 3 years.

DoD perspective – *DFARS [NIST 800-171, 110 cybersecurity controls] 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, so non-recurring costs should be minimal.*

# Cost of Certification - CMMC

Assessment costs will increase significantly as CMMC Levels of certification increase. Below are DoD estimates, and include the amount paid to the assessor/team and your time during the audit.

- CMMC Level 1 Assessment - $3000 [no CUI, just FCI]
- CMMC Level 2 Assessment - $23,000 [not sure I see the point in this one since there will be no contracts issued that have CMMC Level 2 compliance requirements]
- CMMC Level 3 Assessment - $51,000 [CUI]
- CMMC Level 4 Assessment - $70,000 [mostly large primes]
- CMMC Level 5 Assessment - $110,000 [for high-value assets and/or advanced persistent threats – mostly large primes]

# Where Do We Start?

1. For company leaders: ***Tone at the top is critical – treat cybersecurity as an opportunity to do your part to protect National Security, which in turn protects our freedoms.***

2. If your company sells strictly COTS, consider working toward CMMC Level 1 compliance. While compliance is not yet required, it could be in the future. Perform a self-assessment to Level 1 requirements. There are only 17 controls/practices in CMMC Level 1.

3. Review your current DoD contracts. If DFARS 252.204-7012 is referenced ***AND*** your CO/KO **states in writing** that your company has/will touch CUI, you need to comply with NIST SP 800-171 as soon as possible if there are unexercised options coming up or you are planning to bid on a contract after 30 Nov 2020. You probably need to find a consultant who is an expert in NIST 800-171 requirements.

# Where Do We Start?

4. Get help from a cybersecurity consultant if you think you need it. *NOTE: at this point, consultants are NOT certified in CMMC, but can help implement the necessary NIST controls – just make sure they are experts in NIST 800-171.*
5. If your contract references FAR 52.204-21, begin working toward compliance to the 17 controls in CMMC Level 1.
6. All other companies in the DIB – begin with compliance to CMMC Level 1
7. Once you feel comfortable that your company is compliant with CMMC Level 1 requirements and you are certain your company will not need to touch CUI, you can contact the CMMC Accreditation Body via the CMMC Marketplace to schedule a compliance assessment. [For companies that only require CMMC Level 1 compliance]. NOTE: It may be several months before the infrastructure is in place to begin assessments.

# Where Do We Start?

8. If you want to go after contracts that will require you to touch CUI, and/or you want to be proactive and get ahead of your competition, begin by working toward CMMC Level 2 compliance. [Note: No RFPs will be issued at CMMC Level 2 – Level 2 is considered a stepping-stone to get to Level 3 - so begin with Level 2 requirements, then move to Level 3. Keep in mind that at Level 2 you are still not compliant with NIST 800-171]. Level 2 has 55 controls in addition to the 17 required at Level 1. In addition, all controls/practices must be documented, and you must have a cybersecurity policy.

# Where Do We Start?

9. CMMC Level 3 requirements include an additional 58 controls/practices, all practices must be documented, you must have a cybersecurity policy and a System Security Plan is required. Remember,  CMMC Level 3 is derived from DFARS 252.204-7012, which requires compliance to NIST 800-171.

   ***CMMC Level 3 = NIST 800-171 [110 controls] + 20 additional controls + PPI + Maturity***

10. Schedule a Level 3 assessment via the CMMC Marketplace. If you attain CMMC Level 3 certification, you will have exceeded the requirements in the DFARS cybersecurity clause.

11. If your company is registered to any quality management systems standards such as ISO 9001 or AS9100 D, your cybersecurity system needs to be integrated into those programs. If your products/services fall under the ITAR, cybersecurity needs to be integrated into that program as well.

# Resources

- For help understanding the requirements for CMMC Level 1, go to https://www.cybernc.us/ and click on Certification Levels, then Level 1 to access "CMMC Level 1 in a Box"
- Cybersecurity Consultants – posted on NCMBC website [consultants have completed an application, but will not be vetted by the NCMBC]
- NCSU Cyber Toolkit – gap analysis tool for compliance with NIST 800-171
- CUI Registry Categories – look at all categories, not just Defense
- Get help from the NCMBC – Laura Rodgers; rodgersl@ncmbc.us

# Key Points - CMMC

- CMMC certification will be required at time of contract award. If you aren’t compliant, you don’t get the award.
- If you provide strictly COTS products, CMMC does not apply
- If a company receives or touches FCI, then it will be required to be certified to CMMC Level 1 [60% of companies in the DIB]
- If a company will touch CUI, then it will be required to be certified to CMMC Level 3 [at a minimum]
- Compliance with CMMC is a HUGE differentiator – companies that aren’t proactive and pursue certification will not get contracts
- Collaboration is the key to avoiding CUI and reducing cybersecurity costs

# Looking to the Future

- Other departments in the federal government will begin to require compliance to CMMC. For example, CMMC requirements will be in the STARS 3 contract.
- Anticipate CMMC being adopted internationally in 2021 or 2022
- CMMC Level 1 may go away since it is seen as basic cyber hygiene. As cyber threats evolve and increase, a higher level of CMMC may be required – even for companies that don't touch CUI.

***This is an opportunity for North Carolina to get ahead of other states that are not coordinating compliance to cybersecurity requirements.***

# Important Links

- □ CMMC v1.02 [
- □ CMMC Appendices – model in table format
- □ CMMC-Accreditation Body – shows CMMC Ecosystem
- □ FAR Clause 52.204-21 [maps to CMMC Level 1]
- □ DFARS 252.204-7012 [maps to NIST 800-171]
- □ NIST SP 800-171 r2
- □ New DFARS Rule

# Network Security is Non-Negotiable

**It's not an option. Our adversaries - particularly China, Russia, North Korea and Iran - are targeting our networks constantly. We simply cannot let them get information that shows our vulnerabilities and/or gives them an advantage. The stakes are way too high.**

ncmbc
CONNECTING BUSINESS AND MILITARY

# NORTH CAROLINA MILITARY BUSINESS CENTER

## DEPT. OF DEFENSE CYBERSECURITY REGULATIONS

INCLUDING

## CYBERSECURITY MATURITY MODEL CERTIFICATION – CMMC

AND

## DFARS 252.204-7012 AND THE DFARS INTERIM RULE

WWW.NCMBC.US

30 November 2020