NORTH CAROLINA MILITARY BUSINESS CENTER

CYBERSECURITY REGULATIONS WORKSHOP

PRESENTED TO:
NC TECH ASSOCIATION

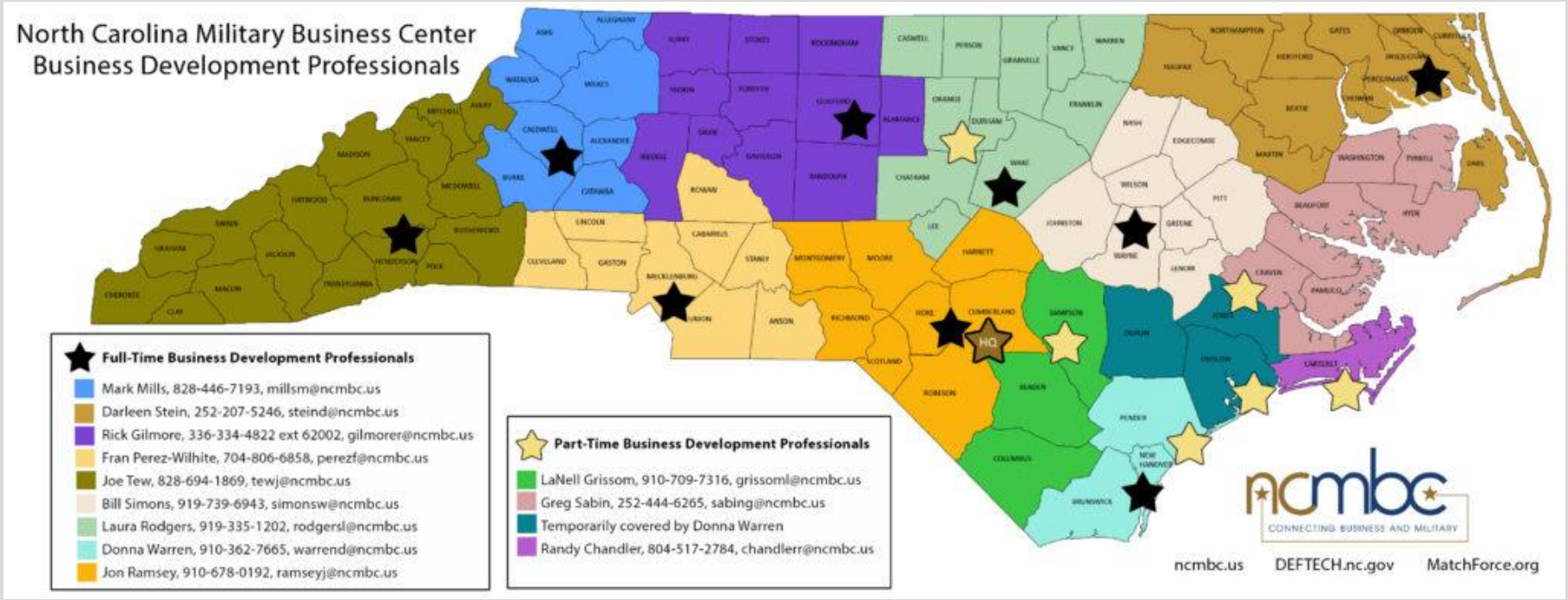
NCMBC

The North Carolina Military Business Center (NCMBC) is a statewide business development and technology transition entity of the North Carolina Community College System, headquartered at Fayetteville Technical Community College.

The mission of the NCMBC is to leverage military and other federal business opportunities to expand the economy, grow jobs and improve quality of life in North Carolina.

https://www.ncmbc.us/

Business Development



Cybersecurity Regulations Workshop

Objective: *NC cyber/IT companies have the necessary skills to assist DoD contractors with compliance to cybersecurity regulations AND to attain certification themselves.*

- Awareness of DoD cybersecurity regulations
- Understand the impact of cybersecurity regulations on NC contractors
- Understand the role of IT/cyber consultants in the cybersecurity/CMMC Ecosystem
- Awareness of cybersecurity resources

Cybersecurity Regulations Terminology

- FAR: Federal Acquisition Regulation – all the regulations associated with federal procurement. Part of the Code of Federal Regulations (CFR)
- 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
- CMMC – Cybersecurity Maturity Model Certification
- Types of information that requires protection:
  - ✓ Federal contract information (FCI)
  - ✓ Controlled unclassified information (CUI)

Awareness - Cybersecurity Regulations

- **FAR 52.204-21** – "Basic Safeguarding of Covered Contractor Information Systems." Maps to 17 practices (controls) in CMMC Level 1. Applies to FCI.
- **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. Protects FCI and CUI. Fifteen RFPs will have CMMC requirements in FY 2021 – will affect approximately 1500 defense contractors, including subs/suppliers. Phased in over the next 4 years.
- **DFARS Interim Rule** – implements CMMC. Also adds "teeth" to 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 (For protection of CUI only). Effective date: 30 Nov 2020. Will be phased-in over a 3-year period.

Awareness - DFARS Interim Rule

- DFARS Interim Rule – 9/29/2020 – added 3 new DFARS clauses in addition to DFARS 252.204 -7012. Applies to companies in the DoD supply chain that touch CUI.
    - 252.204-7019 – added the DoD Assessment Methodology. Companies must now do a self-assessment to NIST 800-171 using the new methodology and upload the score to the Supplier Performance Risk System. Urgent if a contractor has an unexercised option on a current contract and/or plans to bid on a new contract. Applies only to CUI. Must have Plan of Action and Milestones (POAMs) in place for missing controls.
    - 252.204-7020 – provision for DoD auditors to have access to company facilities if it is determined that an audit is needed
    - 252.204-7021 – CMMC

IT/Cybersecurity Role - DFARS Interim Rule

Step 1: Gap assessment

- Resources available to perform a gap assessment:
  - ✓ Project Spectrum – website funded by the DoD. Includes training videos, cybersecurity information and gap analysis tools for DFARS and CMMC. Need to set up a free account.
  - ✓ CISA CSET – gap assessment tool for a variety of regulations, including DFARS and CMMC
  - ✓ NC State University Gap Analysis Tool – downloadable Excel workbook for determining gaps in compliance with the 110 controls in NIST

IT/Cybersecurity Role - DFARS Interim Rule

Step 2: Scoring using the DoD Assessment Methodology

- A perfect score is 110, meaning the contractor has all 110 NIST controls in place.

***NIST SP 800-171 DoD Assessment* Scoring Template**

Security Requirement		Value	Comment
3.1.1*	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	5	
3.1.2*	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	5	
3.1.3	Control the flow of CUI in accordance with approved authorizations.	1	
3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	1	
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	3	
3.1.6	Use non-privileged accounts or roles when accessing non-security functions.	1	
3.1.7	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	1	
3.1.8	Limit unsuccessful logon attempts.	1	

For every control that is not in place, subtract its value from 110 – see figure.

Example: If my company is not compliant with controls 3.1.1 and 3.1.5, subtract 8 points from 110.

IT/Cybersecurity Role - DFARS Interim Rule

Step 3: Develop POAMs for each control that is not performed

- NIST SP 800-171, POAM Template, SSP Template

Step 4: Upload score – and other information to the Supplier Performance Risk System

System Security Plan	CAGE Codes supported by this plan	Brief description of the plan architecture	Date of assessment	Total Score	Date score of 110 will achieved

IT/Cybersecurity Role - DFARS Interim Rule

Step 5: Close out POAMs. Resource: CMMC Awesomeness Technology Solutions

NOTE: Compliance to the DFARS regulations does NOT mean that you are compliant with all 110 controls. Compliance means that you have done a self-assessment, prepared POAMs and have uploaded your score to SPRS.

Step 6: Begin working toward CMMC Level 3 compliance

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.

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, creates, stores and/or transmits FCI or CUI ***on behalf of the DoD.*** 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.** Cloud Service Providers must be the equivalent of FedRAMP “moderate” (CUI).
- 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 (COTS) suppliers will not be required to be compliant with CMMC.

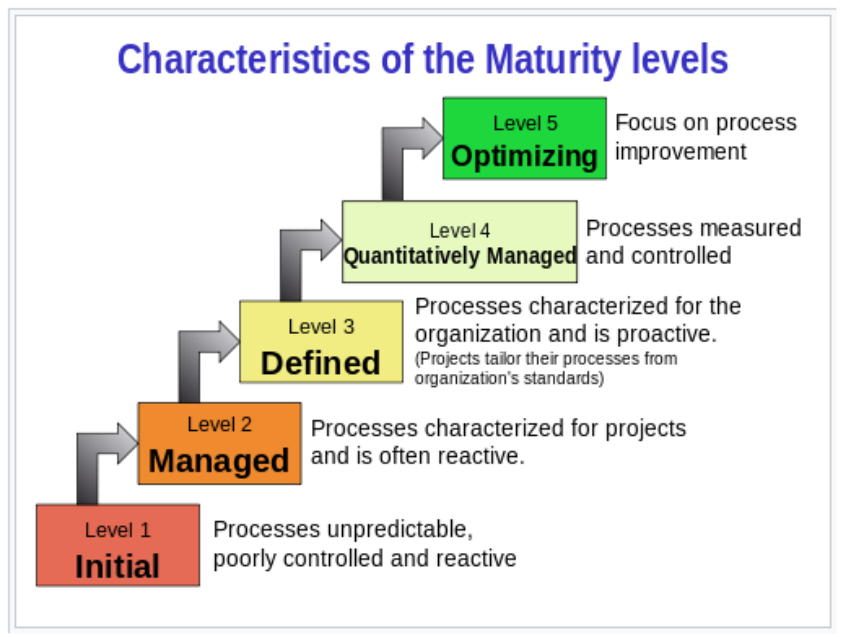
Impact on DoD Contractors

- CMMC assessment and compliance costs are onerous for many small and medium-sized contractors.
  - CMMC Level 3 assessment can cost in excess of $50K; doesn't include the cost of implementing 130 practices/controls and developing a quality management/maturity model framework.
  - CMMC Level 4 assessment can cost in excess of $70K
  - CMMC Level 5 assessment can cost in excess of $110K

Note: assessment costs as well as compliance costs beyond NIST 800-171 can be rolled into rates, which increases the cost of goods/services purchased by the DoD by over $1B per year.

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.



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.

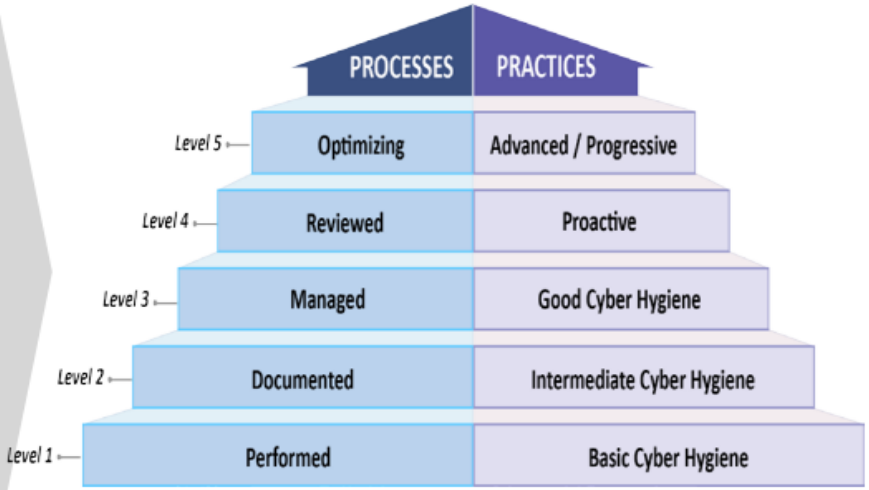
CMMC Level	Practices	Processes
Level 1	17	-
Level 2	55	2
Level 3	58	1
Level 4	26	1
Level 5	15	1

CMMC Model Structure

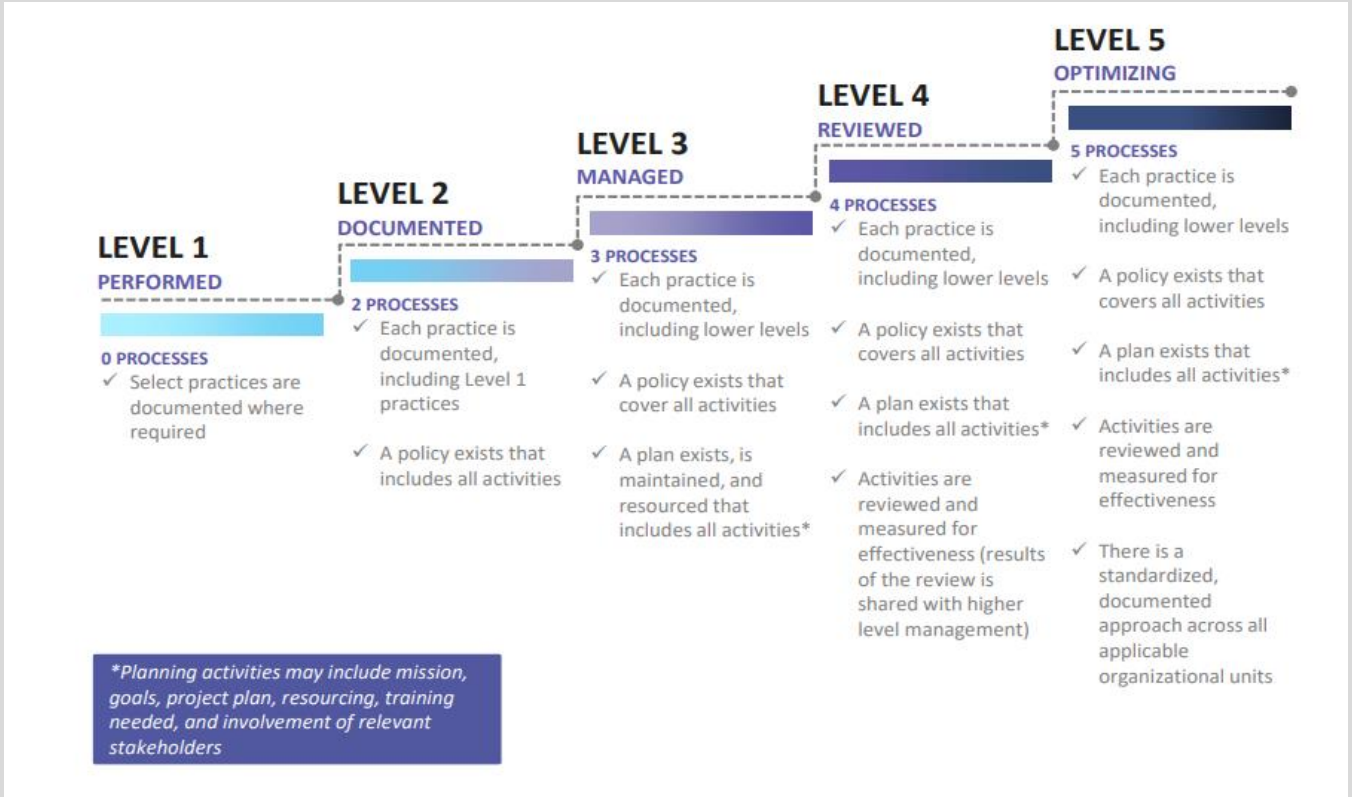
17 Capability Domains

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)	

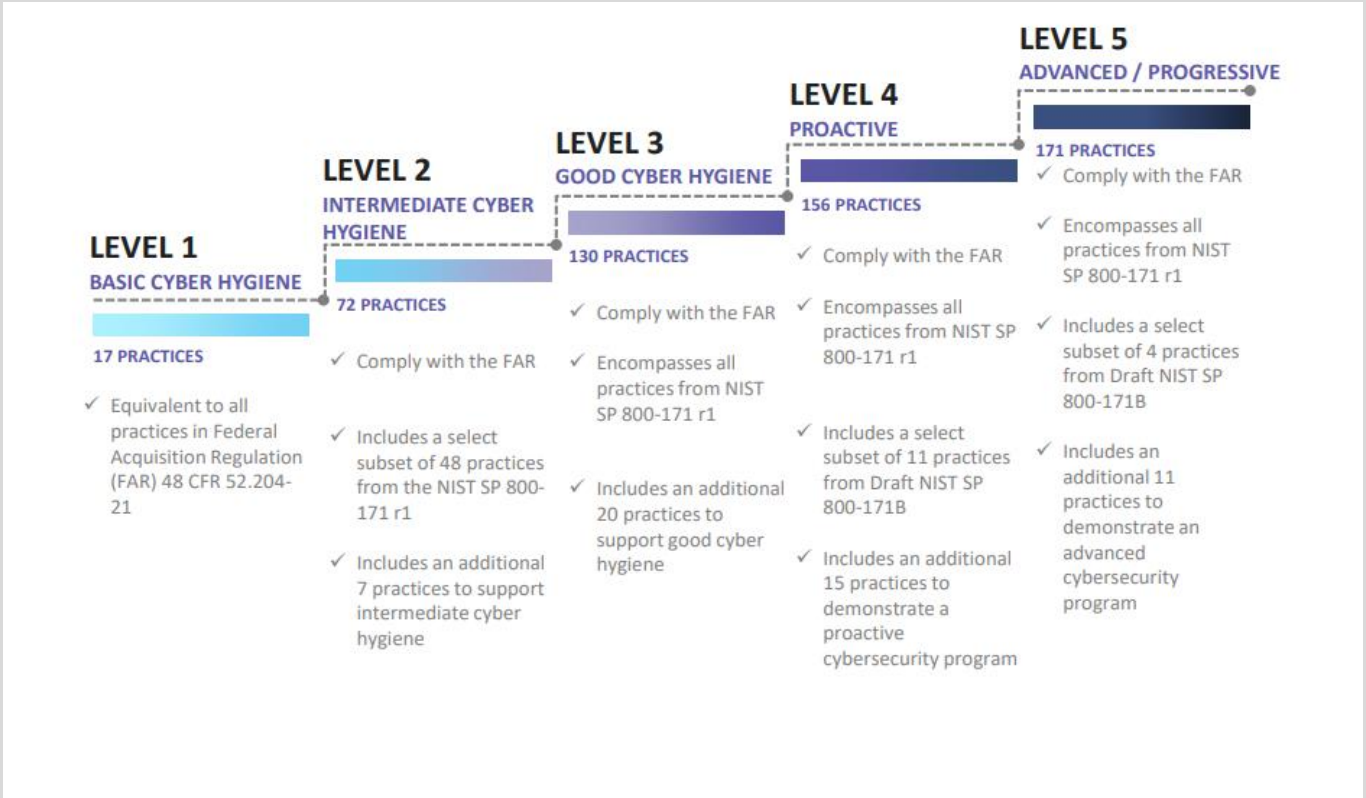
CMMC model with 5 levels measures cybersecurity maturity



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[Controls] – Example

ACCESS CONTROL (AC)

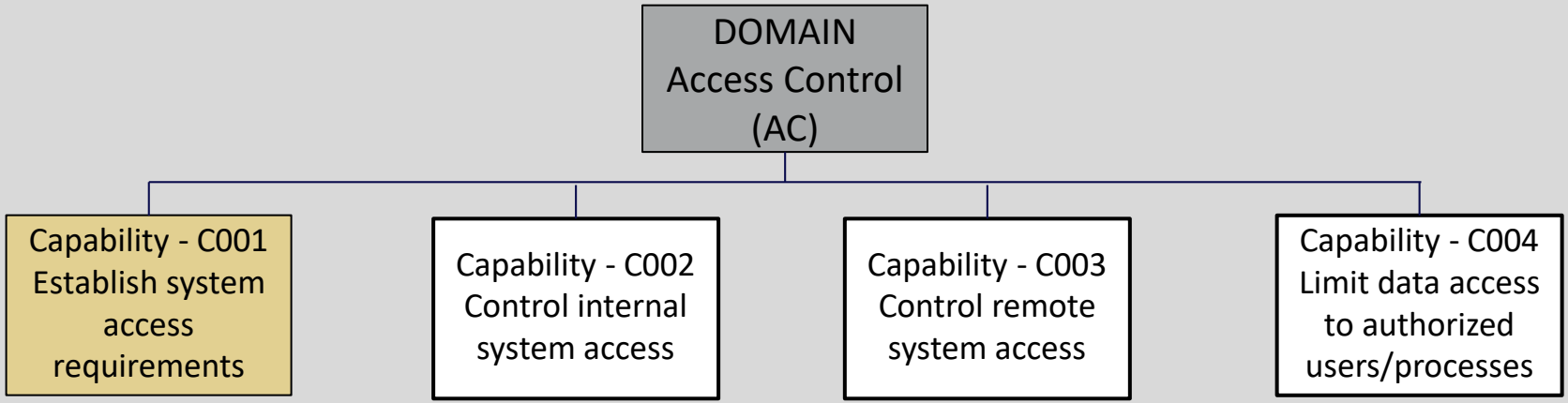
Level 1

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.

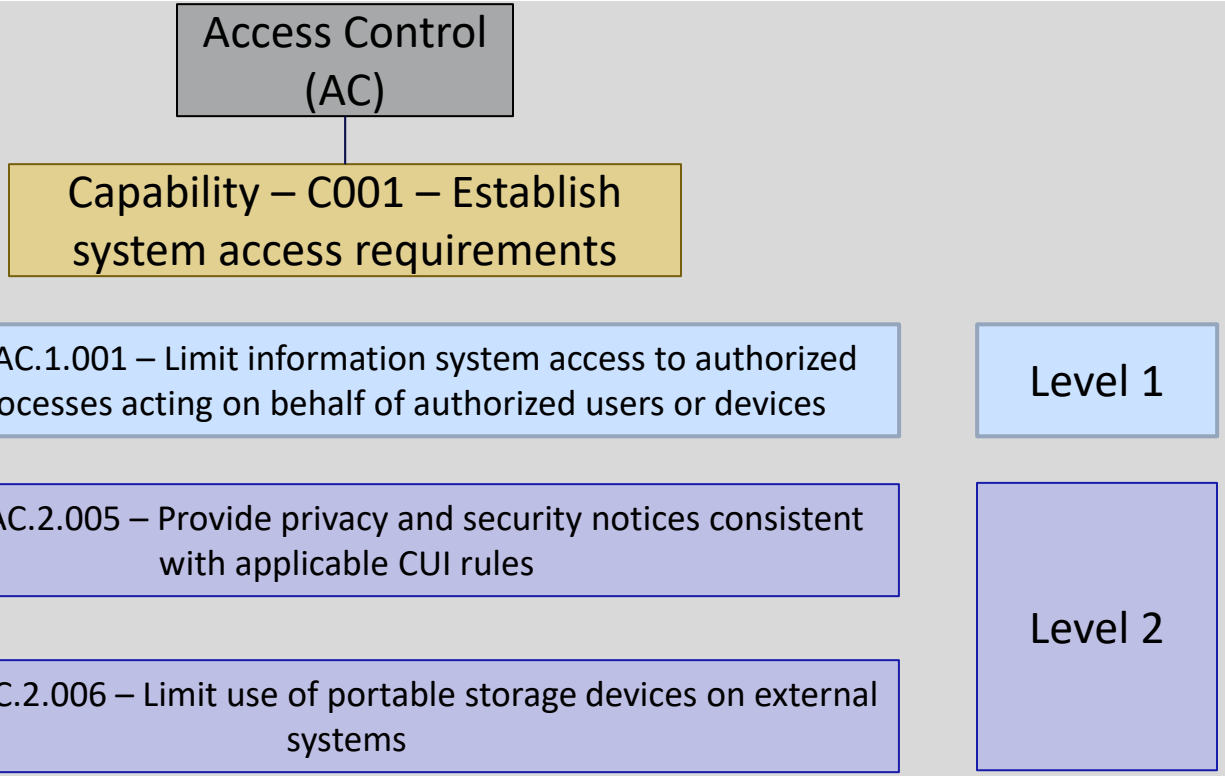
Level 2

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



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)			

Links to CMMC Model & Ecosystem

CMMC – the model in paragraph format and table format, FAQs, Assessment Guides for Levels 1 and 3, and a glossary.

CMMC Ecosystem

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 (40 + hours of training)
- **Registered Practitioners (RP) –** trained in CMMC and can consult but not assess (8 hours of training)

How CMMC Will Be Managed – CMMC Ecosystem

- **Register Provider Organization (RPO) –** organization that can consult but not assess. Manage RPs
- **Organizations Seeking Certification –** organizations in the DoD supply chain and companies/organizations that manage their data
- **Licensed Instructors (LI)** – provide certified training
- **Licensed Training Providers (LTP)** – organizations that hire Licensed Instructors

Cybersecurity Regulations - Update

- CMMC is expected to be in 15 solicitations in FY 2021. First round of pilot programs nominated for consideration:
  - U.S. Navy
    - ✓ *Integrated Common Processor*
    - ✓ *F/A-18E/F Full Mod of the SBAR and Shut off Valve*
    - ✓ *DDG-51 Lead Yard Services / Follow Yard Services*
  - U.S. Air Force
    - ✓ *Mobility Air Force Tactical Data Links*
    - ✓ *Consolidated Broadband Global Area Network Follow-On*
    - ✓ *Azure Cloud Solution*
  - Missile Defense Agency
    - ✓ *Technical Advisory and Assistance Contract*

Looking to the Future

- Other departments in the federal government are looking at requiring compliance to CMMC. For example, CMMC requirements will be in the STARS 3 contract, and DHS will most likely be the next federal agency to adopt CMMC.
- Anticipate CMMC being adopted internationally in 2022 or 2023.
- Will most likely become an international cybersecurity standard.
- 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.

Looking to the Future

CMMC certification will be a **HUGE** differentiator in determining contract award, since certification is required at the time of award.

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

Resource – cyberNC.us

Tour of cyberNC.us – presentations, resources, links

Laura Rodgers - rodgersl@ncmbc.us

Questions

NORTH CAROLINA MILITARY BUSINESS CENTER

CYBERSECURITY REGULATIONS WORKSHOP

PRESENTED TO:
NC TECH ASSOCIATION