“CMMC” Cybersecurity Maturity Model Certification
The Basics

Presented by:

Introduction and Participant Guide

- Things to know before we start
  - Muting
  - Chat function
- Slides will be posted at www.NHEconomy.com/ptac under Training Presentations
- Session is being recorded
  - We will post the recording as soon as we're able

What to Expect from Today's Webinar

- CMMC 101
  - What is it and Why
- CMMC Levels
- DoD Public Briefing overview
- CMMC Accreditation Body and C3PAOs
- Roadmap, what to do now
- Plain language explanations

CMMC 101

- CMMC = "Cybersecurity Maturity Model Certification"
- The CMMC Framework is designed to assess and enhance cybersecurity posture of the Defense Industrial Base (DIB)
- DFARS 252.204-7012: Safeguarding Covered Defense Information and Cyber Incident Reporting is main provision requiring adequate cybersecurity, and Cyber Incident reporting and response
- CMMC builds upon DFARS 252.204-7012 by implementing a verification component with respect to cybersecurity

https://www.acq.osd.mil/cmmc/index.html

CMMC 101

- Concerns that certain unclassified Government information being mishandled
- Increasingly frequent and more sophisticated cyber attacks and intrusions
- The aggregate loss of controlled unclassified information (CUI) from the Defense Industrial Base (DIB) sector increases risk to national economic security and in turn, national security. In order to reduce this risk, the DIB sector must enhance its protection of CUI in its networks.

WHY?

- The Council of Economic Advisers, an agency within the Executive Office of the President, estimates that malicious cyber activity cost the **U.S. economy between $57 billion and $109 Billion in 2016** [Ref: "The Cost of Malicious Cyber Activity to the U.S. Economy, CEA" in February 2018].[1]

[1] https://www.acq.osd.mil/cmmc/faq.html

CUI Controlled Unclassified Information

- Any unclassified information provided by or for the DoD relating to a contract or collected, developed, received, transmitted, used or stores by or for a contractor in performing the contract
- that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended.
- CUI Category List and descriptions: https://www.archives.gov/cui/registry/category-list

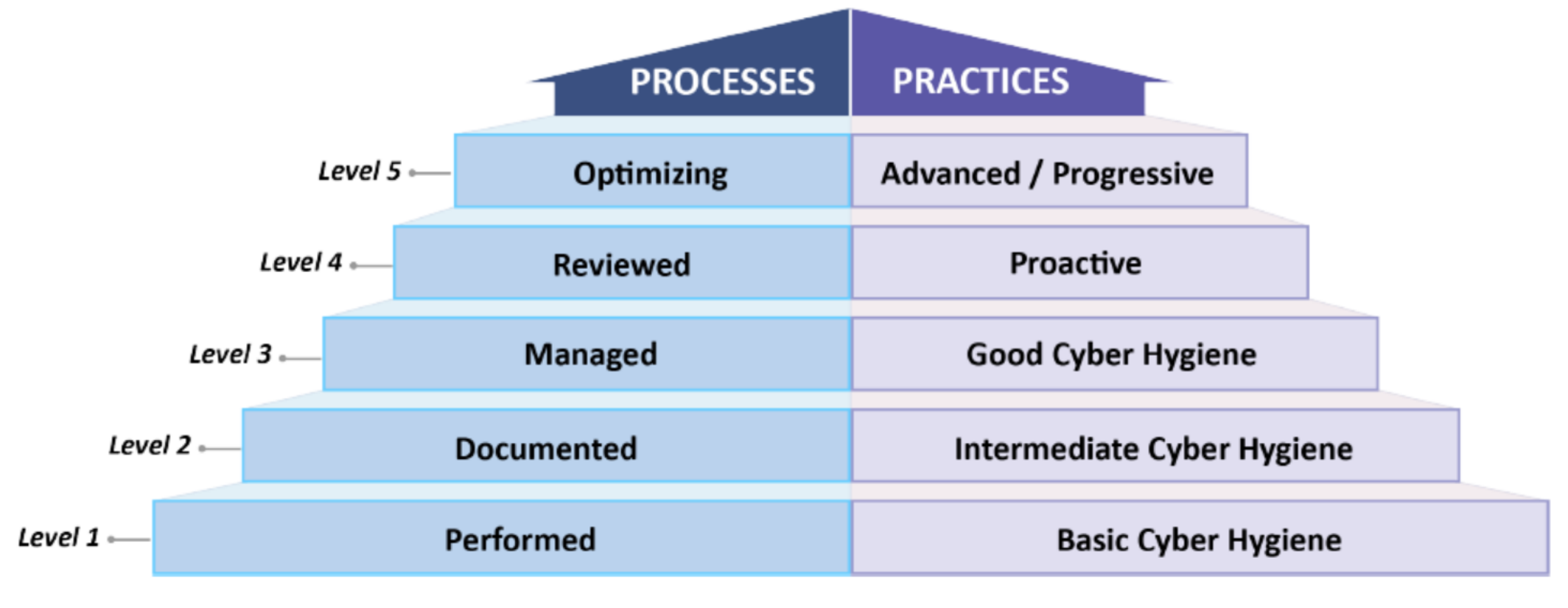
Maturity Levels

- CMMC Model measures cybersecurity maturity with five levels, each level consisting of a set of processes and practices.
- Processes range from Level 1 ‘performed’ to ‘optimizing’ at Level 5
- Practices range from Basic Cyber Hygiene (L1) to Advanced/Progressive (L5)

Maturity Levels

- All Contractors will be need to meet Level 1
  - 17 Practices (FAR 17)
- Level 2 will be required for some CUI Processors
  - 72 Practices (includes some of NIST 800-171)
- Level 3 will be required by all CUI Processors
  - 130 Practices (800-171 + 20 additional)
- Level 4 – APT Targeted Organizations
  - 156 Practices, including enhanced assessment objectives from 800-171B
- Level 5 - APT Targeted Organizations
  - 171 Practices, including enhanced assessment objectives from 800-171B

Maturity Levels



Aligning Levels with Focus

- Level 1: Basic cyber hygiene
  - Safeguard Federal Contract Information (FCI)
- Level 2: Intermediate cyber hygiene
  - Transition step in cybersecurity maturity progression to protect CUI
- Level 3: Good cyber hygiene
  - Protect Controlled Unclassified Information
- Level 4: Proactive
  - Proactive protection of CUI from Advanced Persistent Threats (APTs)
- Level 5: Advanced/Progressive
  - Advanced Protection of CUI and reduce risk of APTs

DOD Public Briefing 01/31/2020

DoD Public Briefing 1-31-20

Without a Secure Foundation All Functions are at Risk

Cost, Schedule, and Performance are only effective in a **SECURE ENVIRONMENT**

CMMC ACCREDITATION BODY

- Establishes and oversees a qualified, trained, and high-fidelity community of assessors that can deliver consistent and informative assessments to participating organizations against a defined set of controls/best practices within the Cybersecurity Maturity Model Certification (CMMC) Program.
- Community of Assessors includes:
  - C3PAOs
  - Certified Assessors
  - Registered Provider Organizations
  - Registered Practitioners

Certified 3rd Party Assessment Organization C3PAO

- **The requirements for becoming a CMMC Third Party Assessment Organization (C3PAO) are not yet established – no third-party entities are currently credentialed to conduct assessments.**
- Must be certified annually
- CMMC AB is developing process for CMMC C3PAO level 3 certification
- At this time C3PAO's must be 100% US Citizen owned (possible changes are being considered)
- Should C3PAO use external cloud service provider to store, process, transmit CUI C3PAO shall require and assure the CSP meets security requirements equivalent to government FedRAMP high baseline impact level 4

Identify desired or required Level of Maturity

- Projects and opportunities you intend to bid/perform on
  - GWACS
- Current security levels implemented
  - If meet Level 3 obtain certification for it!
  - Work towards next level
- It is anticipated that majority of acquisitions will require Level 1 to Level 3, very few will be Level 4 or 5
- FedRAMP and other certification Reciprocity

ROADMAP

- Learn the requirements and conduct an assessment

Requires company buy-in across all functions, including but not limited to:

  - Management
  - Compliance
  - Facilities
  - IT
  - Legal
- Senior Management Responsibility
- SSP and POAM
- Technical Roadmap and Budget

ROADMAP

- Implementation/Remediation
  - Incident Response
  - Risk Management
  - Asset management
  - Employee Awareness and Safe Practices
  - Technology Upgrades

ROADMAP

- Third Party Certification
  - Readiness Assessment
  - Final Preparation
  - Third Party Audit
  - Corrective Action
  - Certification

Perform a (Pre-)Assessment

- Who has access to your data?
- What data do you have access to?
  - All Employees
- Who are your vendors?
- Do you rely on a third party for:
  - IT security services
  - Accounting

Organizational Areas to Review

- CMMC Training (IT, MSP, Management, Employees)
- Documentation (SSP, POAM, Policies)
- Management Process
- Risk Management
- Administrative Controls (Risk, Change and Incident Management)
- Performance Tracking
- Physical security
- Audit Preparation

Technical Areas to Review

- Network Configuration and Management
- Security Information Events Management (SIEM) System, Log Monitoring
- Network Hardware (switches, routers, firewalls, etc)
- Multi-factor authentication
- Antivirus, Backup, Vulnerability Scanning, VPN, Whitelisting/Blacklisting, DLP, IPS, Encryption
- Video Cameras

Opportunities for Involvement

- **Registered Provider Organizations**
  - authorized to represent the organization as familiar with the basic constructs of the CMMC Standard with a CMMC-AB provided logo
  - Deliver **non-certified** CMMC Consulting Services
- **Certified 3rd Party Assessment Organizations**
  - authorized to manage the assessment process.
- **Certified Professionals and Certified Assessors**
  - Credentialed individuals authorized to deliver assessments, training, and consulting.
- **Licensed Partner Publisher**
  - Publishers of educational courses and content who wish to sell such content to education organizations, professional schools or direct to consumer

Interim Rule Sept 29, 2020

- The interim final rule seeks to assess contractor implementation of cybersecurity procedures requirements to further strengthen protection of classified materials throughout the supply chain. The rule allows for a five-year phase-in with different levels of certification requirements for DOD contracts. Additionally, the rule requires some contractors who want medium- or high-level work to open themselves up to a DOD review.
- The new rule also requires that contractors undergo a third-party audit. The rule is written in such a way that most of the auditing will be done by third parties, but some might be done by the Cybersecurity Maturity Model Certification Audit Board itself.
- Comments on the interim final rule are due November 30, 2020.
- Read the *Federal Register* notice here.
- Submit comments here.

What does it mean?

- "Identify, report and correct information and information system flaws in a timely manner"
  - **Patch your Information Systems**
- Provide Protection from malicious code at appropriate organization locations
  - **Install Antivirus**
- Update malicious code protection mechanisms when releases available
  - **Keep Antivirus up-to-date**
- Perform periodic scans of informaitn system and real-time scans of files from external sources as downloaded, opened or executed
  - **Use Antivirus**

What does it mean?

- Sanitize or destroy information system media containing FCI before disposal or release for reuse
  - **Shred documents and wipe hard drives**
- Limit physical access to organizational information systems, equipment and respective operating environments to authorized individuals
  - **Lock doors and windows**
- Escort visitors and monitor visitor activity; maintain audit logs of physical access; control and manage physical access devices
  - **Monitor all entry points, and keep inventory of keys**

What does it mean?

- Control information posted or processed on publicly accessible information systems (and or websites)
  - **Don't post Federal info on Facebook, or other social media**
- Identify and authenticate information system users, processes acting on behalf of users, or devices
  - **Require individual usernames and passwords**
- Limit Information system access to authorized users, processes acting on behalf of authorized users, or devices (incl other information systems)
  - **Control Access to the System**

What does it mean?

- Limit Information system access to types of transactions and functions authorized users are permitted to execute
  - **"Least Privilege"**
- Verify and control/limit connections to and use of external information systems.
  - **Use Firewall**
- 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.
  - **Use Firewall and IDS Tools**

Shameless Commercial

- NH PTAC offers free assistance with all this & more.
- You must have a physical presence in New Hampshire.
- You have to sign up online.
- To continue “active client” status, you have to use us as a resource.

How do I get started with NH PTAC?

- Go to the website and answer our questionnaire (www.nheconomy.com/ptac)
- email us at: govcontracting@livefree.nh.gov
- Meet with us in Concord (currently via Zoom)
- Give us a call at (603) 271-7581
- Request a site visit – we'll come to you.

BEA

New Hampshire
PROCUREMENT TECHNICAL ASSISTANCE CENTER