CMMC Level 3 Readiness Supplier Webinar

"Bridging the Gaps to Accelerate CMMC Preparation"

October 22, 2020

DISCLAIMER

- Webinar content is based on:
  - Office of Under Secretary of Defense (OUSD) CMMC Info
  - National Institute of Standards & Technologies (NIST) publications
  - National Archives & Records Administration (NARA) definitions
  - Defense Industrial Base Sector Coordinating Council (DIB SCC) Supply Chain Task Force - CyberAssist
  - Exostar assessment documentation preparation presentation
  - Observations from Lockheed Martin's suppliers engagements
- Lockheed Martin does not take responsibility for suppliers' certification by the CMMC 3rd Party Assessment Organization (C3PAO)

LEARNING OBJECTIVES

- Provide a baseline understanding of CMMC
- Clarify differences between NIST SP 800-171 & CMMC v1.02 Level 3
- Highlight common NIST interpretation challenges and information sources
- Explain Lockheed Martin's expectation for CMMC deployment
- Prepare for CMMC assessment

CYBERSECURITY MATURITY MODEL CERTIFICATION OVERVIEW

- **What is CMMC?**
  - o New DoD cybersecurity framework to verify the cybersecurity posture of the Defense Industrial Base (DIB)
- **Certification conducted by Certified 3rd Party Assessment Organizations (C3PAO)**
- **Acquisition Go/No-Go Decisions**
- **Supply Chain Flow Down**
  - o Mandatory flow down of CMMC requirements and verify supplier certification level
- **Official CMMC document source**

CMMC Model Framework

Domains (17)	Capabilities (43)	Practices (171)
Key sets of cybersecurity capabilities	Achievements to ensure cybersecurity within each domain	Activities required by level to achieve a capability

CMMC Domains (17)

Asset Control	Asset Management	Audit and Accountability	Awareness and Training	Configuration Management
Identification and Authentication	Incident Response	Maintenance	Media Protection	Personnel Security
Physical Protection	Recovery	Risk Management	Security Assessment	Situational Awareness
	System and Communications Protections	System and Information Integrity		

CMMC Levels (5)

Level 5 Advanced	Advanced Persistent Threats	15 practices	NIST SP 800-171 B and other frameworks
Level 4 Proactive		26 practices	
Level 3 Good	Controlled Unclassified Information (CUI)	58 practices	NIST SP 800-171 R1 and other frameworks
Level 2 Intermediate	Federal Contract Information (FCI)	55 practices	
Level 1 Basic		17 practices	

Source: https://www.acq.osd.mil/cmmc/draft.html

CMMC DEPLOYMENT EXPECTATIONS

- OUSD scheduled release of RFI's with CMMC requirements starting 2020
- OUSD will identify contracts w/CMMC requirements during FY21-25 roll-out
- CMMC rollout expected to complete by 2026

Total Number of New Prime Contracts Awarded Each Year with CMMC Requirement				
FY21	FY22	FY23	FY24	FY25
15	75	250	479	479

- Lockheed Martin working with DoD on Q2 – Q3 2020 pathfinder (Table Top exercises and Mock Assessments) – to inform/influence rule making
- Official CMMC Updates
- Official CMMC FAQ

DO I NEED TO BE CMMC LEVEL 3 COMPLIANT?

- Level 1: Safeguard Federal Contract Information (FCI)
- Level 2: Serve as transition step in cybersecurity maturity progression to protect CUI
- Level 3: Protect Controlled Unclassified Information (CUI)
- Levels 4-5: Protect CUI and reduce risk of Advanced Persistent Threats (APTs)

NATIONAL ARCHIVES

- If you currently receive **Controlled Technical Information (CTI) or CUI** provided by your customer or generated (developed, collected, transmitted or stored) by, or on behalf of, the contractor in support of the performance of the contract.

Examples of CTI:

- Research and engineering data
- Engineering drawings & associated specifications
- Standards, manuals, technical reports & studies
- Computer software executable code & source code

CUI Categories
CUI Training from National Archives

DOD Controlled Unclassified Information (CUI) = Covered Defense Information (CDI)

NIST 800-171 VS. CMMC REQUIREMENTS

NIST 800-171	CMMC Level 3	CMMC Levels 4 & 5
POA&M's allowed	**No** POA&M's allowed	**No** POA&M's allowed
Contract work allowed if controls are not 100% implemented but POA&M's in place	No work allowed until certified that all requirements are implemented	No work allowed until certified that all requirements are implemented
Self-Certification	Certified 3rd party assessment organizations will grant CMMC certifications	Certified 3rd party assessment organizations will grant CMMC certifications
110 Controls	130 Practices (20 additional to NIST 800-171) With additional maturity processes	156 Practices for level 4; 171 Practices for level 5 With additional maturity processes

CMMC Vs. NIST 800-171 and other Frameworks

COMMON NIST INTERPRETATION CHALLENGES

NIST 800-171 Control # (CMMC practice #)	Control Requirement (CMMC Domain)	Clarifying Questions Source: NIST HB 162 -Self-Assessment Handbook For Assessing NIST SP 800-171
3.1.1,.4,.5 (AC 1.001, AC 2.007, AC 3.017)	Access Control (Access Control)	• Do you only grant enough privileges to users to allow them to do their job? • Does the company require users to logon to gain access?
3.2.2 (AT 2.057)	Awareness and Training (Awareness and Training)	• Do employees with security-related duties and responsibilities receive initial and annual training on their operational, managerial, and technical roles and responsibilities? • Does the training cover physical, personnel, and technical safeguards and countermeasures?
3.4.1,.2,.3,.9 (CM.2.061, CM 2.064, CM 2.065, CM 2.063)	Configuration Management (Configuration Management)	• Are baseline configurations developed, documented, and maintained for each information system type? • Are configuration-managed changes to the system audited by company personnel? • Are user controls in place to prohibit the installation of unauthorized software?
3.6.2 (IR 3.098)	Incident Response (Incident Response)	• Is there a company incident response policy which specifically outlines requirements for tracking and reporting of incidents involving CUI to appropriate officials?
3.7.5 (MA 2.113)	Maintenance (Maintenance)	• Does all remote access to a system for maintenance or diagnostics occur via an approved remote solution using multifactor authentication? • Does the system require multifactor authentication for remote access?

COMMON NIST INTERPRETATION CHALLENGES

NIST 800-171 Control # (CMMC practice #)	Control Requirement (CMMC Domain)	Clarifying Questions Source: NIST HB 162 -Self-Assessment Handbook For Assessing NIST SP 800-171
3.8.7,.8 (MP.1.121, MP.3.123)	Media Protection (Media Protection)	• Is the use of writable, removable media restricted on the system? • Do all portable storage devices have identifiable owners?
3.9, 3.10 (PS., PE.)	Personnel Security (Personnel Security)	• Are individuals requiring access screened before access is granted? • Are physical access devices (such as card readers, proximity readers, and locks) maintained and operated per the manufacturer recommendations? • Do all alternate sites where CUI data is stored or processed meet the same physical security requirements as the main site?
3.11 (RM.)	Risk Assessment (Risk Management)	• Does the company have a risk management policy? • Are systems periodically scanned for common and new vulnerabilities? • Do system owners and company managers upon recognition of any vulnerability provide an action plan for remediation, acceptance, avoidance, or transference of the vulnerability risk?
3.12.1 (CA.2.158)	Security Assessment (Security Assessment)	• (NOTE): Companies should ensure that security assessment results are current, relevant to the determination of security requirement effectiveness, and obtained with the appropriate level of assessor independence.

COMMON NIST INTERPRETATION CHALLENGES

NIST 800-171 Control # (CMMC practice #)	Control Requirement (CMMC Domain)	Clarifying Questions Source: NIST HB 162 -Self-Assessment Handbook For Assessing NIST SP 800-171
3.13.12, .13 (SC.2.178, SC.3.188)	System and Communications Protection (System and Communications Protection)	• Have collaborative computing devices (e.g., cameras, microphones, etc.) been configured so they cannot be remotely activated? • Are there defined limits of mobile code usage, established usage restrictions, that specifically authorize use of mobile code (e.g., Java, JavaScript, ActiveX, PDF, Flash, Shockwave, Postscript, VBScript, etc.) within the information system?
3.14.1 (SI.1.210)	System and Information Integrity (System and Information Integrity)	• Are system flaws identified, reported, and corrected within company-defined time periods? • Does the company perform all security-relevant software updates (patching, service packs, hot fixes, and anti-virus signature additions) in response to identified system flaws and vulnerabilities within the timeframe specified in policy or within the system security plan?

MATURITY LEVEL 3 – NOT JUST A CHECKLIST

- **Demonstrate CMMC compliance with effective Policies and Documentation:**
  - Define your organization's response to cyber incidents
  - Develop processes and procedures
    - e.g. CM.3.067: Define, document, approve, and enforce physical and logical access restrictions
  - Outline and clarify procedures for all stakeholders
  - Proper documentation serves as proof of your cybersecurity readiness
- **Assessors might want to see:**
  - Scan results, log files, command media, actual training programs (phishing email tests etc.), physical access restrictions, etc.
- CyberAssist (CMMC help website)
- CMMC Accreditation Body
- Documentation and Policy Requirements

Major Highlights:

- **Additional 20 level 2/3 practices**
  - 130 vs. 110 NIST 800-171
  - Implemented vs. POAM
- **3 Maturity Processes**
  - Demonstrating institutionalization

Source: https://landing.exostar.com/webinar-cmmc-documentation-and-policy-requirements

RELATIONSHIP BETWEEN PRACTICES AND PROCESSES

XX.2.999: Establish a policy that includes XX domain

- Develop and publish organizational policy for the process

XX.2.998: Document the CMMC practices to implement the XX domain policy

- Practices are established, documented, and followed to implement the policy for XX domain

Practices and documentation enforce the policies

XX.3.997: Establish, maintain, and resource a plan that includes XX domain.

- Establish and maintain the plan for performing the process

Resources enable processes

Source: https://landing.exostar.com/webinar-cmmc-documentation-and-policy-requirements

ACCESS CONTROL DOMAIN EXAMPLE

Establish	**AC.2.999: Establish a policy that includes Access Management** • Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) • Work from Home (WfH) and Bring Your Own Device (BYOD) Policies • Remote access policy • Limit information system access to the types of transactions and functions that authorized users are permitted to execute
Document	**AC.2.998: Document the CMMC practices to implement the Access Control policy** • Account Creation Procedure • WFH and BYOD procedures • Defined user roles based on type of work performed
Establish, maintain, and resource	**AC.3.997: Establish, maintain, and resource a plan that includes Access Control** • A project plan for access control activities • Ensuring the workforce implementing the access control activities are qualified • Ensure Access Control activities are budget for • Tools necessary for access control activities are provided and workforce is trained on the tools

Source: https://landing.exostar.com/webinar-cmmc-documentation-and-policy-requirements

KEY CMMC AND CUI INFORMATION SOURCES

- Official CMMC document source
- Official CMMC Updates
- Official CMMC FAQ
- Exostar blog entry on CMMC
- Cyber Assist (CMMC help website)
- CMMC Accreditation Body
- CMMC For Suppliers
- CMMC Vs. NIST 800-171 and other Frameworks
- CUI Categories
- CUI Training from National Archives
- CUI Marking Handbook from National Archives
- NIST HB 162 -Self-Assessment Handbook For Assessing NIST SP 800-171

Q & A

PIRA CET20200500