DFARS Clause 252.204-7012 and the Cybersecurity Maturity Model Certification (CMMC) Webcast Overview

Chris Newborn
DAU Cybersecurity Enterprise Team

Webcast - Why

Targeted for Acquisition Workforce Members (AWF) who are responsible to

- Deliver secure and resilient systems
- Determining cybersecurity requirements

Webcast - Why

Provides a forum to bring the right set of disciplines together to provide clarification regarding

- AWF’s roles & responsibilities implementing the DFARS Clause and transitioning to the CMMC process
- Migration from current security requirements to the new CMMC process
- Challenges & issues concerning the implementation and execution of DFARS Clause on current and future procurements and the migration to the CMMC process

Webcast - Why

This is the first of five webcasts. The remaining webcasts will discuss the following:

- DoDI 5200.48
- NIST 800-171 v1.1
- Request For Information/ Request For Proposal (RFI/RFP) Contract Strategy Considerations
  - CMMC Implementation Process
- Selection of CMMC Levels (I, III, and III+)
  - Sensitivity of the Information
  - Threat Capability

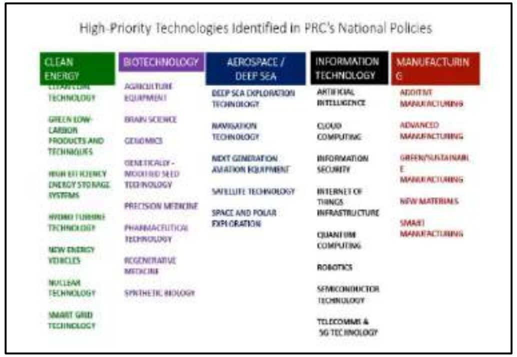
Outline

- **Why DFARS/CMMC**
- **FY20 NDAA**
- **Current Policy - DFARS**
- **Related Policies**
  - DoDI 5200.48
  - DoDI 8582.01
  - Cloud Computing
  - NIST SP 800-171 v1.1 (DAM)
- **Future Process - CMMC**
  - CFR 52.204-201
  - Model Framework
  - Levels & Descriptions
  - Levels & Associated Focus
- **CMMC Accreditation Board**
- **CMMC Schedule**
- **Migration from DFARS to CMMC Level 3**
- **Contractor's Preparation**
- **Summary**

Why DFARS/CMMC

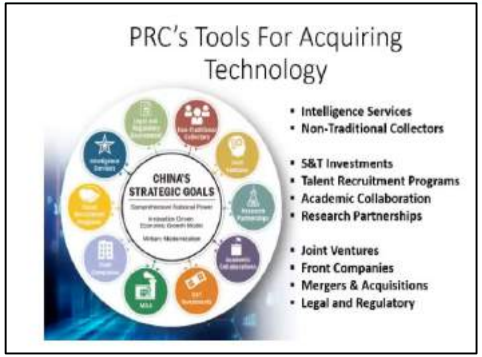
FBI is investigating more than 1,000 cases of Chinese theft of US technology

"They've pioneered an expansive approach to stealing innovation through a wide range of actors, including not just Chinese intelligence services but state-owned enterprises, ostensibly private companies, certain kinds of graduate students and researchers, and a whole variety of other actors all working on their behalf."



High-Priority Technologies Identified in PRC's National Policies

CLEAN ENERGY	BIOTECHNOLOGY	AEROSPACE / DEEP SEA	INFORMATION TECHNOLOGY	MANUFACTURING
CLEAN COAL TECHNOLOGY	AGRICULTURE EQUIPMENT	DEEP SEA EXPLORATION TECHNOLOGY	ARTIFICIAL INTELLIGENCE	ADDITIVE MANUFACTURING
GREEN LOW-CARBON PRODUCTS AND TECHNIQUES	BRAIN SCIENCE	NAVIGATION TECHNOLOGY	CLOUD COMPUTING	ADVANCED MANUFACTURING
HIGH EFFICIENCY ENERGY STORAGE SYSTEMS	GENOMICS	NEXT GENERATION AVIATION EQUIPMENT	INFORMATION SECURITY	GREEN/SUSTAINABLE MANUFACTURING
HYDRO TURBINE TECHNOLOGY	GENETICALLY-MODIFIED SEED TECHNOLOGY	SATELLITE TECHNOLOGY	INTERNET OF THINGS INFRASTRUCTURE	NEW MATERIALS
NEW ENERGY VEHICLES	PRECISION MEDICINE	SPACE AND POLAR EXPLORATION	QUANTUM COMPUTING	SMART MANUFACTURING
NUCLEAR TECHNOLOGY	PHARMACEUTICAL TECHNOLOGY		ROBOTICS	
SMART GRID TECHNOLOGY	REGENERATIVE MEDICINE		SEMICONDUCTOR TECHNOLOGY	
	SYNTHETIC BIOLOGY		TELECOMMS & 5G TECHNOLOGY	



PRC's Tools For Acquiring Technology

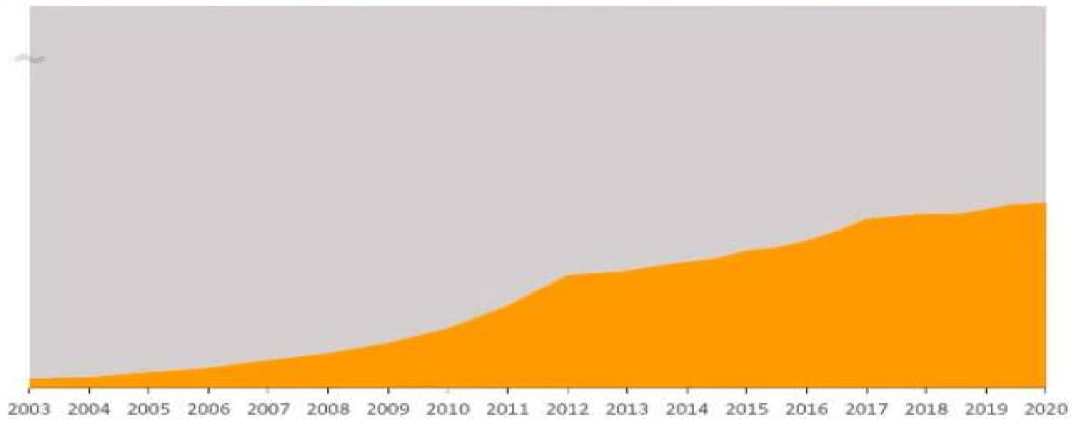
CHINA'S STRATEGIC GOALS
Comprehensive National Power
Innovation Driven Economic Growth Model
Military Modernization
M&A
S&T Investments

- Intelligence Services
- Non-Traditional Collectors

- S&T Investments
- Talent Recruitment Programs
- Academic Collaboration
- Research Partnerships

- Joint Ventures
- Front Companies
- Mergers & Acquisitions
- Legal and Regulatory

FBI Technology Theft Cases Involving China



FY 20 NDAA Section 1648

Required the Secretary of Defense to develop a comprehensive framework to enhance the cybersecurity of the U.S. DIB to address cybersecurity standards, regulations, metrics, ratings, and third-party certifications that prime contractors/ subcontractors must meet to successfully implement the current DFARS Clause 252.204-7012

Cybersecurity Maturity Model Certification (CMMC)

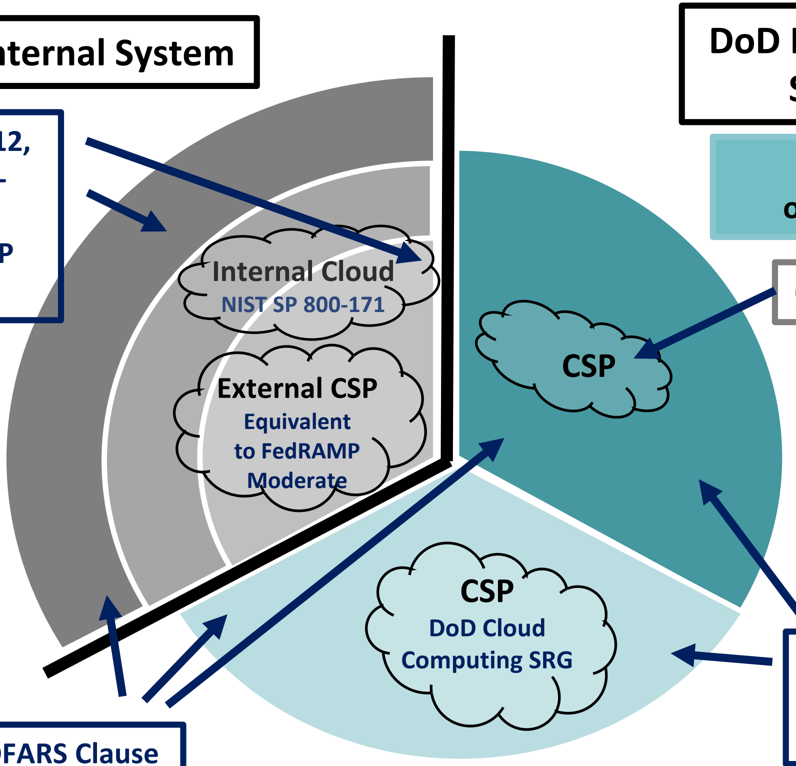
Current Policy – DFARS Clause 252.204-7012

Purpose:

- DFARS Clause 252.204-7012 structured to ensure controlled unclassified DoD information (CUI) residing on contractor's internal information system is safeguarded from cyber incidents, and any consequences associated with the loss of this information are assessed & minimized via cyber incident reporting & damage assessment process
- Providing a single DoD-wide approach to safeguarding covered contractor information systems

Goal: To properly secure sensitive information (CUI) in the Defense Industrial Base (DIB)

PROTECTING THE DOD'S UNCLASSIFIED INFORMATION



Contractor's Internal System

DFARS Clause 252.204-7012, and/or FAR Clause 52.204-21, and security requirements from NIST SP 800-171 apply

Federal Contract Information

Controlled Unclassified Information (USG-wide)

DoD CUI

DFARS Clause 252.239-7018, may apply

DoD Information System

System Operated on Behalf of the DoD

Cloud Service Provider (CSP)

When cloud services are used to process data on the DoD's behalf, DFARS Clause 252.239-7010 and the DoD Cloud Computing SRG apply

Controlled Unclassified Information

Risk Management Framework and 'Authority to Operate' shall apply

DFARS Roles/Responsibilities

Requires the program office/requiring activity to:

- **Mark or otherwise identify** in the contract, task order, or delivery order **CUI** provided to the contractor by or on behalf of, DoD in support of the performance of the contract

Requires the contractor/subcontractor to:

- Provide adequate security to safeguard CUI that resides on or is transiting through a contractor's internal information system or network
- Report cyber incidents that affect a covered contractor information system or the CUI residing therein, or that affect the contractor's ability to perform requirements designated as operationally critical support
- Flow down the clause in subcontracts for operationally critical support, or for which subcontract performance will involve CUI

Related Policies – Controlled Unclassified Information (CUI)

DoDI 5200.48, Controlled Unclassified Information:

- Supersedes DoD Manual 5200.01, Volume 4
- Establishes policy, assigns responsibilities, and prescribes procedures for CUI throughout the DoD IAW DFARS Sections 252.204-7008 and 252.204-7012
- Establishes the official DoD CUI Registry

General DoD CUI Procedures:

- Unclassified information associated with a law, regulation, or government-wide policy and identified as needing safeguarding is considered CUI
  - **DoD CUI replaces all references to Covered Defense Information (CDI)**
  - Authorized holder is responsible for determining whether information in a document or material falls into a CUI category, and applying CUI markings and dissemination instructions accordingly
  - **At minimum, CUI markings for DoD CUI documents will include the acronym "CUI" in the banner and footer of the document (FOUO not valid for new documents)**

Related Policies - Other Transactions

DoDI 8582.01, Security of Non-DoD Information Systems Processing Unclassified Nonpublic DoD Information:

- **Applies to all unclassified non-DoD information systems** (to the extent provided by applicable contracts, grants, or other legal agreements with the DoD) that process, store, or transmit unclassified nonpublic DoD information.
- It is DoD policy that non-DoD information systems provide adequate security for all unclassified nonpublic DoD information. Appropriate requirements must be incorporated into all contracts, grants, and other legal agreements with non-DoD entities
- **Non-DoD information systems processing, storing, or transmitting DoD CUI must be protected in accordance with NIST SP 800-171**
- **Also addresses cyber incident reporting and compliance requirements**

Related Policies - Cloud Computing

Safeguarding DoD CUI and Cyber Incident Reporting 48 CFR Parts 202, 204, 212, and 252, DFARS Clause 252.204-7012

- Applies when a contractor uses an external cloud service provider to store, process, or transmit CUI on the contractor's behalf
- Ensures that the cloud service provider:
  - **Meets requirements equivalent to those established for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline**
  - **Complies with requirements for cyber incident reporting and damage assessment**

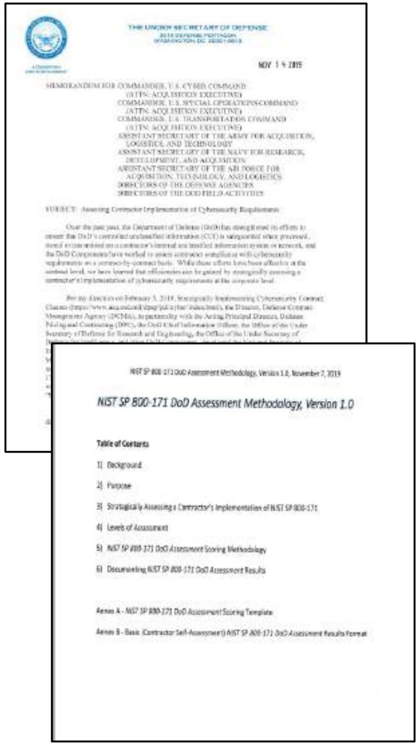
Cloud Computing Services 48 CFR Parts 239 and 252, DFARS Clause 252.239-7010

- Applies when a cloud solution is being used to process data on the DoD's behalf or DoD is contracting with Cloud Service Provider to host/process data in a cloud
- Requires the cloud service provider to:
  - Comply with the DoD Cloud Computing Security Requirements Guide
  - Comply with requirements for cyber incident reporting and damage assessment

Related Policies - DoD Assessment Methodology (DAM) Tool

NIST SP 800-171 v1.1, DoD Assessment Methodology Tool

- A methodology that enables assessment of a contractor's implementation of NIST SP 800-171, a requirement for compliance with DFARS Clause 252.204-7012
- **Consists of three levels of assessments (Basic, Medium, and High) that reflect the depth of the assessment and level of confidence in the assessment results**
- DCMA, Defense Counterintelligence and Security Agency (DCSA) and DoD Components completed High Assessments for the Department's largest contractors; **captured in the Supplier Performance Risk System (SPRS)**
- DoD will use methodology to assess the implementation of NIST SP 800-171 by its prime contractors. Prime contractors may use this methodology to assess the implementation status of NIST SP 800-171 by subcontractors



THE UNDER SECRETARY OF DEFENSE
3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

NOV 1 4 2019

MEMORANDUM FOR COMMANDER, U.S. CYBER COMMAND
(ATTN: ACQUISITION EXECUTIVE)
COMMANDER, U.S. SPECIAL OPERATIONS COMMAND
(ATTN: ACQUISITION EXECUTIVE)
COMMANDER, U.S. TRANSPORTATION COMMAND
(ATTN: ACQUISITION EXECUTIVE)
ASSISTANT SECRETARY OF THE ARMY FOR ACQUISITION, LOGISTICS, AND TECHNOLOGY
ASSISTANT SECRETARY OF THE NAVY FOR RESEARCH, DEVELOPMENT, AND ACQUISITION
ASSISTANT SECRETARY OF THE AIR FORCE FOR ACQUISITION, TECHNOLOGY, AND LOGISTICS
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Assessing Contractor Implementation of Cybersecurity Requirements

Over the past year, the Department of Defense (DoD) has strengthened its efforts to ensure that DoD's controlled unclassified information (CUI) is safeguarded when processed, stored or transmitted on a contractor's internal unclassified information system or network, and the DoD Components have worked to assess contractor compliance with cybersecurity requirements on a contract-by-contract basis. While these efforts have been effective at the contract level, we have learned that efficiencies can be gained by strategically assessing a contractor's implementation of cybersecurity requirements at the corporate level.

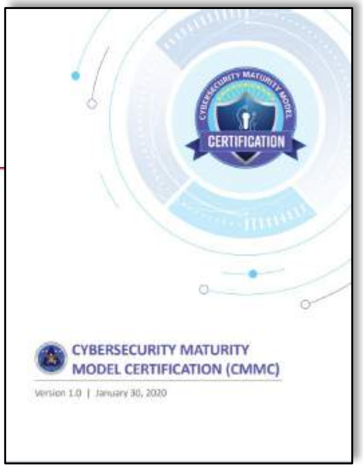
Per my direction on February 5, 2019, Strategically Implementing Cybersecurity Contract Clauses (https://www.acq.osd.mil/dpap/pdi/cyber/index.html), the Director, Defense Contract Management Agency (DCMA), in partnership with the Acting Principal Director, Defense Pricing and Contracting (DPC), the DoD Chief Information Officer, the Office of the Under Secretary of Defense for Research and Engineering, the Office of the Under Secretary of [illegible]

NIST SP 800-171 DoD Assessment Methodology, Version 1.0, November 7, 2019

NIST SP 800-171 DoD Assessment Methodology, Version 1.0

Table of Contents

Future Process - CMMC

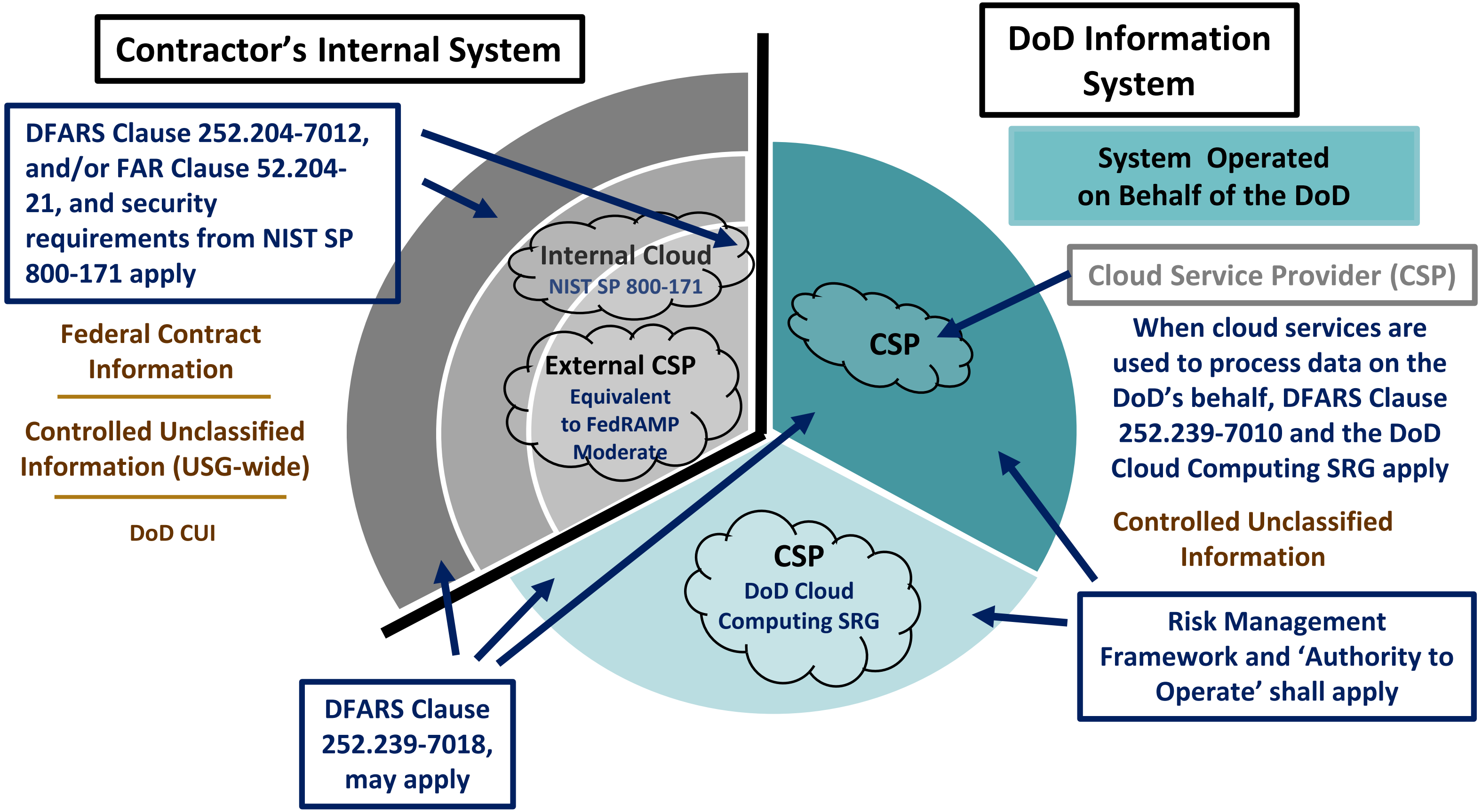


CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)

Version 1.0 | January 30, 2020

- A certification process that measures a Defense Industrial Base (DIB) company's ability to protect **Federal Contract Information (FCI)** & Controlled **Unclassified Information (CUI),** within the supply chain
  - FCI is information provided by or generated for the Government under contract not intended for public release
  - CUI is sensitive information that requires protection under laws, regulations and Government-wide policies
- Combines cybersecurity standards and maps practices and processes to maturity levels; from "basic cyber hygiene" to "highly advanced"
- Builds from existing regulation (48 Code of Federal Regulations (CFR) 52.204-21 & DFARS 252.204-7012)

PROTECTING THE DOD'S UNCLASSIFIED INFORMATION



Contractor's Internal System

DFARS Clause 252.204-7012, and/or FAR Clause 52.204-21, and security requirements from NIST SP 800-171 apply

Federal Contract Information

Controlled Unclassified Information (USG-wide)

DoD CUI

Internal Cloud
NIST SP 800-171

External CSP
Equivalent to FedRAMP Moderate

DFARS Clause 252.239-7018, may apply

DoD Information System

System Operated on Behalf of the DoD

Cloud Service Provider (CSP)

CSP

When cloud services are used to process data on the DoD's behalf, DFARS Clause 252.239-7010 and the DoD Cloud Computing SRG apply

Controlled Unclassified Information

CSP
DoD Cloud Computing SRG

Risk Management Framework and 'Authority to Operate' shall apply

CMMC Roles/Responsibilities

Requires the program office/requiring activity to:

- Identify FCI/CUI Data and Marking Requirements
- Develop/Update Security Classification Guide (SCG)
- Identify CMMC Level(s)

Requires the contractor/subcontractor to:

- Develop/Update Artifacts/Deliverables per RFI/RFP
- Initiate/Hire C3PAO to perform CMMC assessment
- Develop Supply Chain/Tier 1 & below Contractor Support Agreements

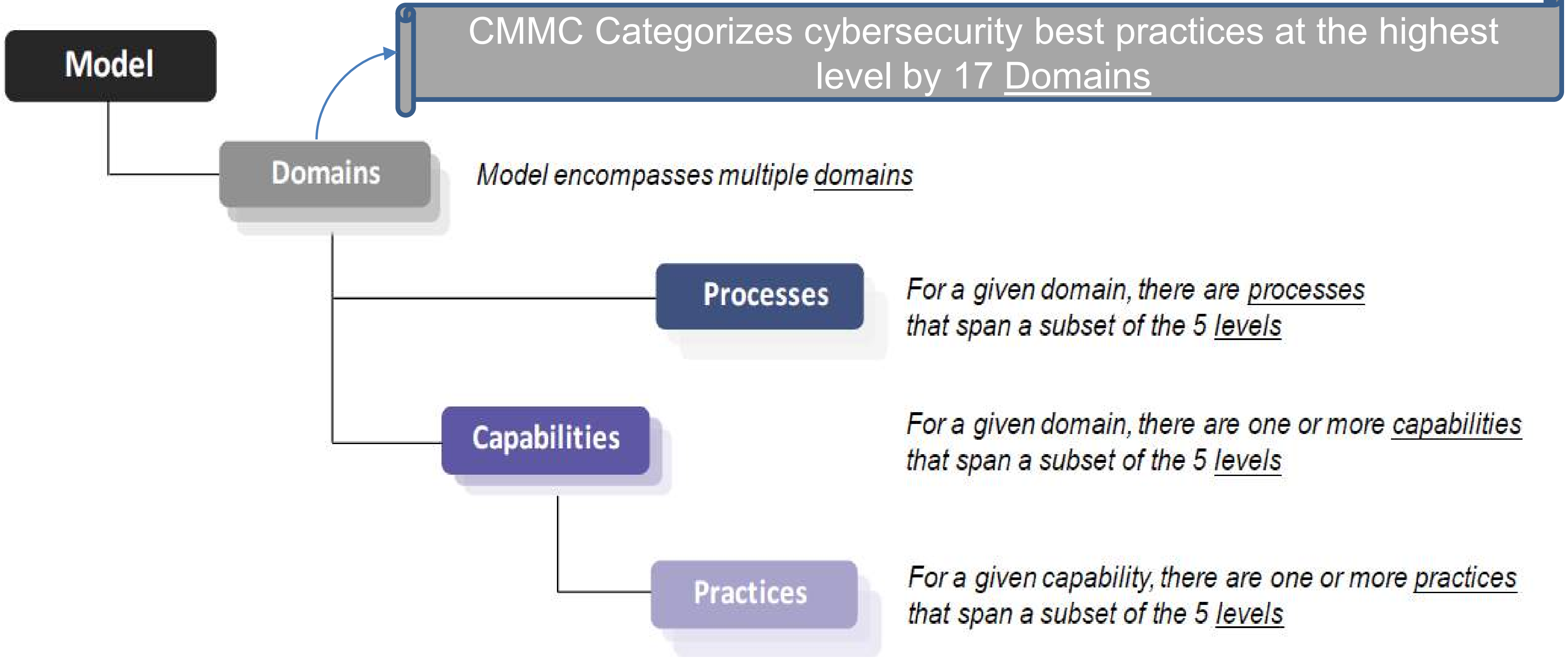
Related Policies - Basic Safeguarding of Covered Contractor Information Systems

Code of Federal Regulations (CFR) 52.204-201, Basic Safeguarding of Covered Contractor Information Systems:

- Covered contractor information system means an information system that is owned or operated by a contractor that processes, stores, or transmits Federal Contract Information (FCI)
- Supplier Requirements:
  - Provide basic security - CFR 52.204-201(b)
    - Limit Access, Authenticate, Sanitize, Monitor, Find/ Fix Flaws, Patch, Detect Malware, Scans, etc.
  - Flow down these requirements to Subcontracts - CFR 52.204-201 (c)

CMMC Model Framework

CMMC Categorizes cybersecurity best practices at the highest level by 17 Domains



Model

Domains

Model encompasses multiple domains

Processes

For a given domain, there are processes that span a subset of the 5 levels

Capabilities

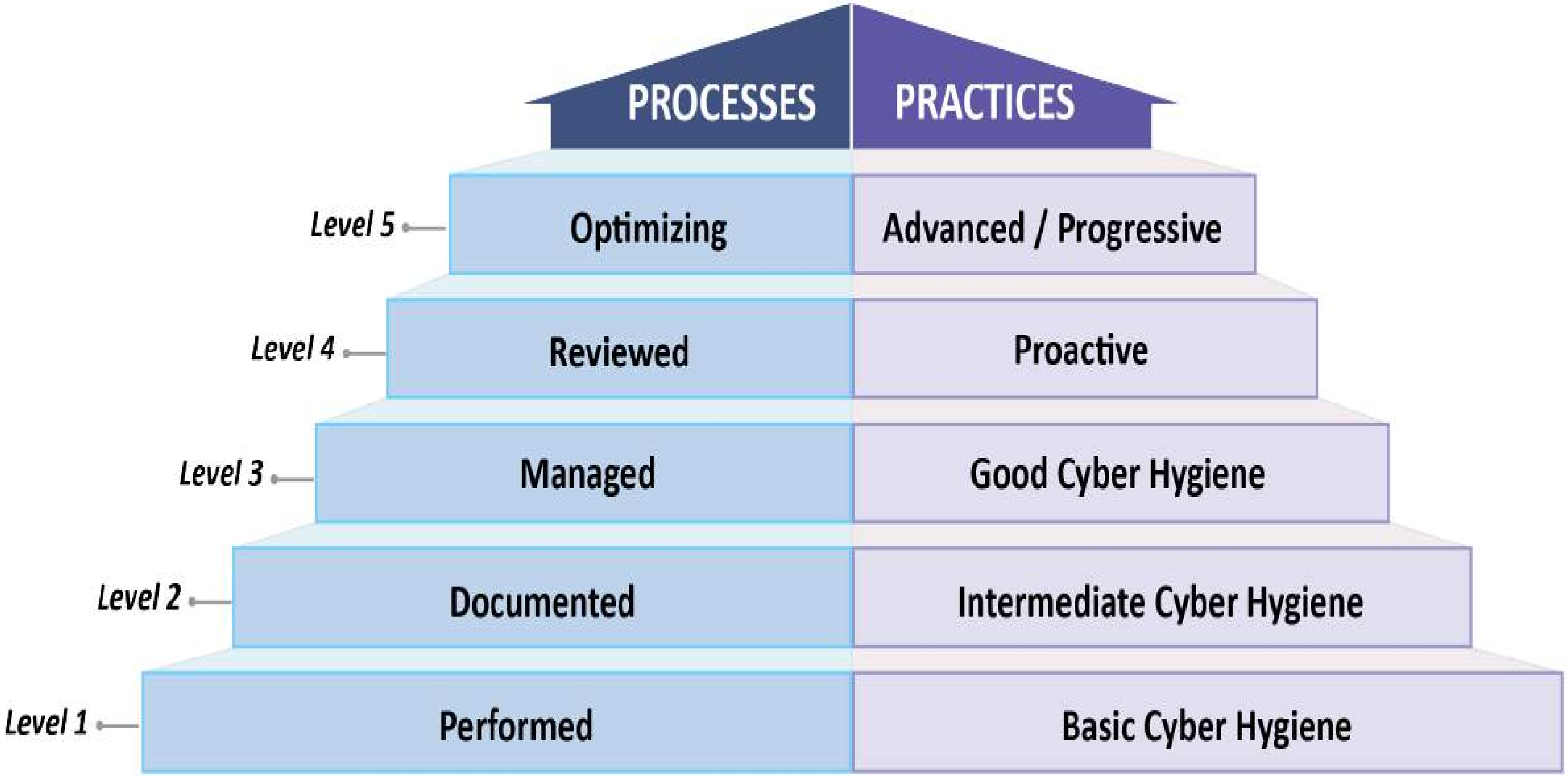
For a given domain, there are one or more capabilities that span a subset of the 5 levels

Practices

For a given capability, there are one or more practices that span a subset of the 5 levels

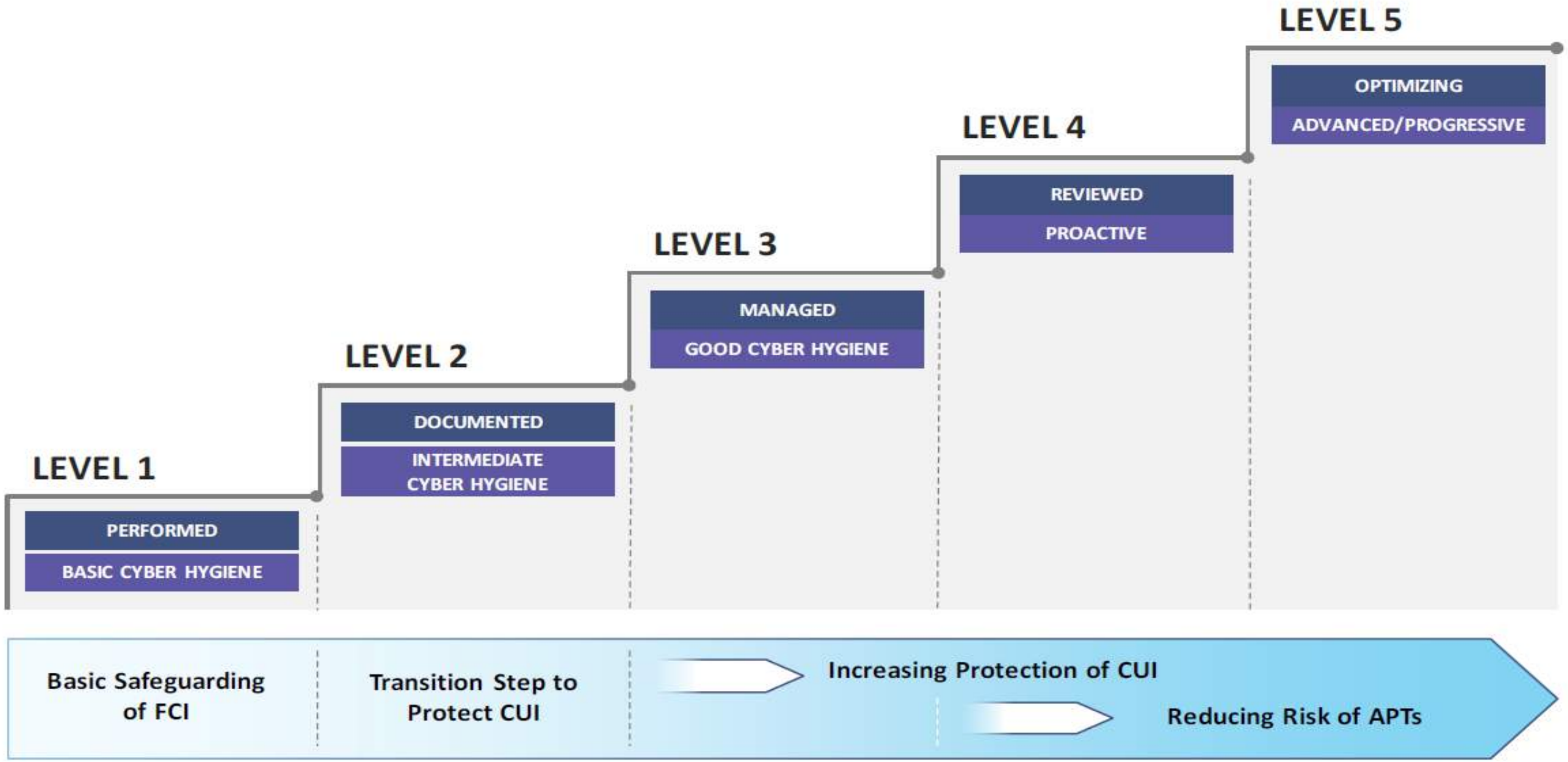
DIB companies will be accredited under the CMMC only if they can demonstrate compliance with the required practices and demonstrate mature processes required for the given CMMC level

CMMC Levels and Descriptions



	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 Levels and Associated Focus



CMMC is designed to provide increased assurance to the DoD that a DIB can adequately protect CUI at a level commensurate with the risk

CMMC Levels Comparison

Levels 1-3: Moderate Threats & Below

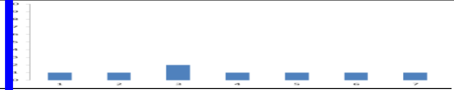
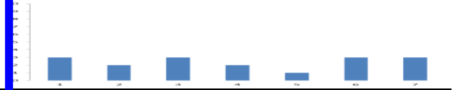
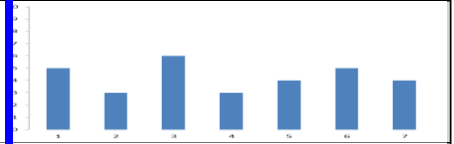
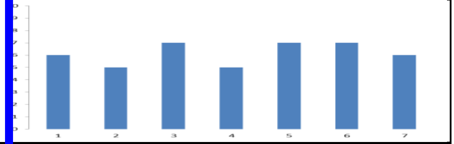
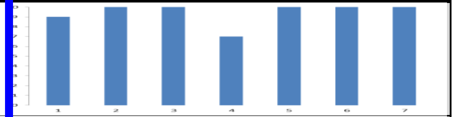
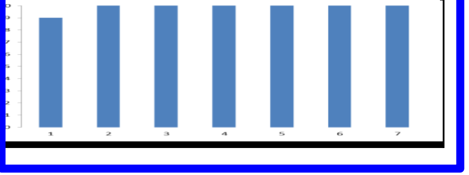
- **Security Requirements:**
  - CFR 52.204-21, DFARS 252.204-7012, NIST SP 800-171
- **Risk Based Approach:**
  - Risk = Consequence * Threat * Vulnerability
- **What is the threat likely to do?**
  - Inventoried assets w/ perimeter defense

Levels 4-5: Advanced Persistent Threats

- **Security Requirements:**
  - Level1-3 + NIST SP 800-172 (171B)
- **Threat Centric Approach**
  - Worst Case Scenario
- **What could the threat do?**
  - Zero trust architecture, analysis, & dynamic defense

CMMC Level	Number of Practices Introduced at CMMC Level	Source			
		48 CFR 52.204-21	NIST SP 800 171	NIST SP 800-172	Other
1	**17**	15	17		
2	**55**		48		7
3	**58**		45		13
4	**26**			11	15
5	**15**			4	11
Total	**171**	**15**	**110**	**15**	**46**

DSB Threat Tiers

Tier	Typical Organizations	Vulnerability Exploitation	Resources	Motivation	Scope of Access	Skills and Capabilities
I	**Script Kiddies**	Exploits pre-existing known vulnerabilities.	$ Hundreds	Bragging rights	Minimal.	
II	**Hackers for hire**	Exploits pre-existing known vulnerabilities.	$ Thousands	Theft/sale of business, financial data	Minimal.	
III	**Small teams of hackers, e.g., non-state actors**	Discovers unknown vulnerabilities	$ Millions	Theft/sale of corporate, govt leaders' personal or organizational data, political impact	Localized or sparse physical presence. Minimal supply chain access.	
IV	**Larger, well-organized teams – criminal, non-state, or state sponsored**	Discovers unknown vulnerabilities	$ Millions	Theft/sale of corporate, govt leaders' personal or organizational data, political impact	Localized or sparse physical presence. Minimal supply chain access.	
V	**Highly capable state actors**	Creates vulnerabilities	$ Billions. Can pursue a <u>few</u> complex attacks concurrently.	Political, military, economic impact	Physically present and/or supplies technology world-wide and in space.	
VI	**Most capable state actors (U.S. rivals)**	Creates vulnerabilities	$ Billions. Can pursue <u>many</u> complex attacks concurrently over a long time	Political, military, economic impact	Physically present and/or supplies technology world-wide and in space.	

CMMC Accreditation Board (CMMC AB)

- CMMC AB is responsible for training and certifying third-party auditors (C3PAO) that will validate cybersecurity practices and compliance of defense contractors
- Consists of 14 members from industry
  - Board Chairman: Ty Shieber, senior director of business development at the University of Virginia's Darden School of Business

CMMC AB – Do’s & Don’ts

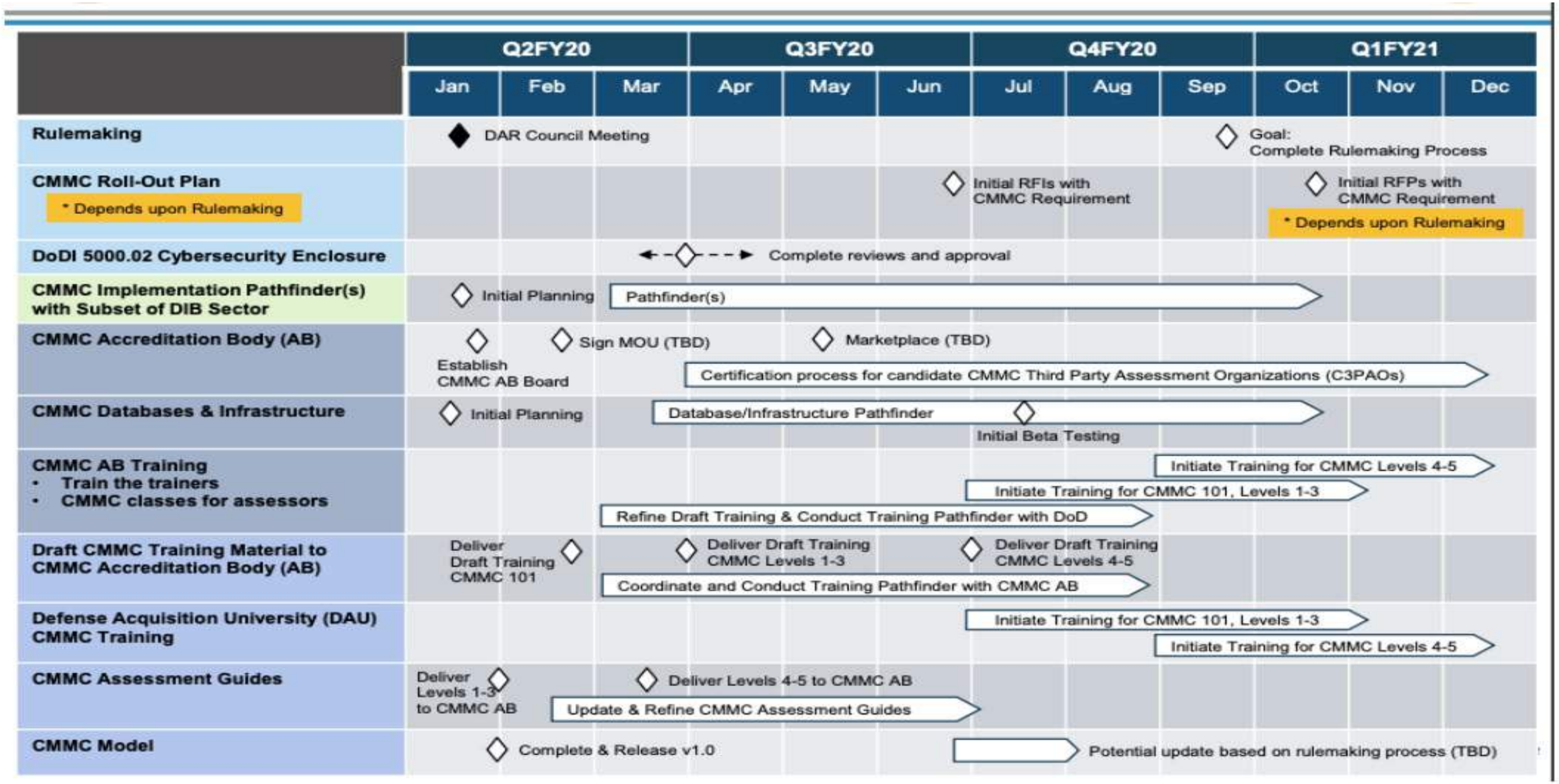
Do's

1. When mentioning CMMC, always place the word DRAFT in front of it, so as not to mislead readers that the standard is complete and released.
2. Share valid information about the CMMC standard acquired from this site or the Official DoD site located at https://www.acq.osd.mil/cmmc/index.html.
3. **Prepare your clients for CMMC by training and educating them for DFARS regulations and NIST 800-171 guidance.** It is the law and there is an increasing number of audits being performed right now, in 2020.
4. Become an expert on CMMC by reading the standard, assessment guidance, and training materials that will be published on https://www.acq.osd.mil/cmmc/index.html. These materials ARE NOT YET AVAILABLE as the standard is not complete and released.

Don'ts

1. Do not state that you are an expert on CMMC. The standard is not yet released. No certified training exists yet.
2. **Currently, DFARS regulation requires self-assessments under NIST 800-171 guidance. Do not focus training on future requirements (CMMC) at the expense of current requirements.**
3. Do not charge clients for workshops, seminars, and training that promise CMMC compliance. The CMMC-AB will provide training and certifications to empower you with those opportunities.
4. Do not sell or promote tools that promise CMMC compliance with certainty. The CMMC-AB will create standards for tool producers to use. For now, ensure that any tools promoted focus first on completed and released standards, or best practices."

CMMC Deployment Schedule



	Q2FY20			Q3FY20			Q4FY20			Q1FY21		
	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Rulemaking	◆ DAR Council Meeting								◇ Goal: Complete Rulemaking Process			
CMMC Roll-Out Plan * Depends upon Rulemaking						◇ Initial RFIs with CMMC Requirement				◇ Initial RFPs with CMMC Requirement * Depends upon Rulemaking		
DoDI 5000.02 Cybersecurity Enclosure			◇ Complete reviews and approval									
CMMC Implementation Pathfinder(s) with Subset of DIB Sector	◇ Initial Planning		Pathfinder(s)									
CMMC Accreditation Body (AB)	◇ Establish CMMC AB Board	◇ Sign MOU (TBD)	Certification process for candidate CMMC Third Party Assessment Organizations (C3PAOs)		◇ Marketplace (TBD)							
CMMC Databases & Infrastructure	◇ Initial Planning		Database/Infrastructure Pathfinder				◇ Initial Beta Testing					
CMMC AB Training • Train the trainers • CMMC classes for assessors			Refine Draft Training & Conduct Training Pathfinder with DoD			Initiate Training for CMMC 101, Levels 1-3		Initiate Training for CMMC Levels 4-5				
Draft CMMC Training Material to CMMC Accreditation Body (AB)		◇ Deliver Draft Training CMMC 101	Coordinate and Conduct Training Pathfinder with CMMC AB ◇ Deliver Draft Training CMMC Levels 1-3			◇ Deliver Draft Training CMMC Levels 4-5						
Defense Acquisition University (DAU) CMMC Training						Initiate Training for CMMC 101, Levels 1-3		Initiate Training for CMMC Levels 4-5				
CMMC Assessment Guides	◇ Deliver Levels 1-3 to CMMC AB	Update & Refine CMMC Assessment Guides	◇ Deliver Levels 4-5 to CMMC AB									
CMMC Model	◇ Complete & Release v1.0					Potential update based on rulemaking process (TBD)						

Cybersecurity Maturity Model Certification (CMMC) timeline

Contractor’s Preparation for CMMC

- DIB legally bound to follow the provisions of DFARS Clause 252.204-7012:
  - Safeguarding DoD CUI
  - Reporting Cyber Incidents
  - Flow-down DFARS Clause to subs/vendors
- Identify/focus efforts on deltas between DFARS Clause and CMMC process
- From the CMMC Accreditation Board:

  “… Do not focus training on future requirements (CMMC) at the expense of current requirements ...“

Summary

- The new CMMC process will eliminate self-certification of compliance
- DIB Contractors will be required to undergo 3rd-party Audits of their IT Systems and Cybersecurity Policies by Independent Assessors (C3PAOs) to receive a CMMC compliance ranging from Level 1 to Level 5
  - All practices for the required CMMC level must be met for contract eligibility (RFI or RFP)
  - Expected to appear in RFPs Sep 2020
  - Compliance expenses are "allowable cost" that may be included in DoD contract bids.
  - Certifications from C3PAO audits good for three years.

For additional questions, please contact Chris Newborn at chris.newborn@dau.edu or 619-370-3076