Assured Information Technology

The Key To Your Information Assurance

Cybersecurity Maturity Model Certification (CMMC) Overview

What you need to know about CMMC and how it effects your company.

28 October 2020

Jason Eddy, President
Joe Pennetti, IT

AIT Engineering

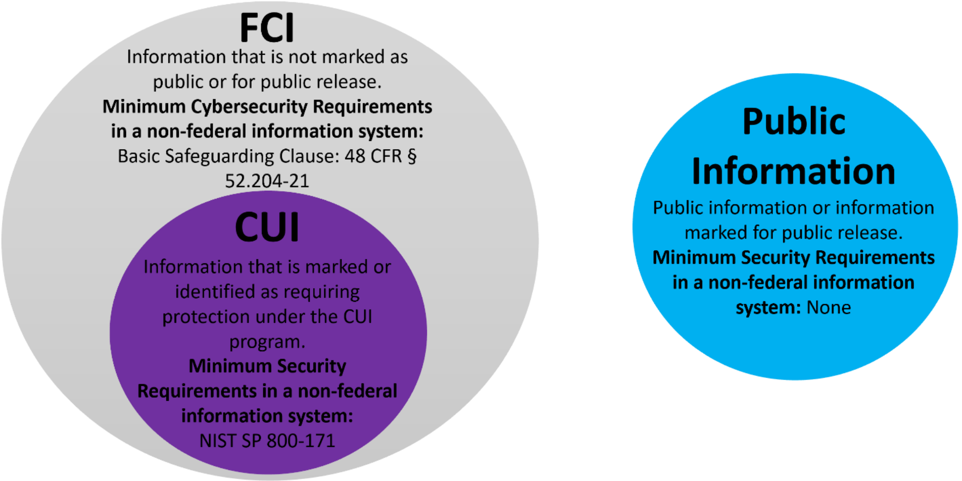
Disclaimer

- In the current state of conflicting information, draft standards, and interim regulations this presentation will attempt to clarify what the CMMC is, how we got here and next steps
- As the compliance landscape changes daily the information in this presentation will likely have a short lifespan. All sources are sited throughout the presentation and a Reference slide summarizes the authoritative sources at the end
- Webinar content is based on:
  - Office of the Under Secretary of Defense for Acquisition & Sustainment CMMC Info
  - National Institute of Standards & Technologies (NIST) publications
  - National Archives & Records Administration (NARA) definitions
  - Defense Acquisition University (DAU) webinar content

IT’S ALL ABOUT THE DATA - FCI and CUI

- Federal Contract Information
  - Information not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public Web sites) or simple transactional information, such as necessary to process payments.
  - Basic safeguarding IAW FAR clause 52.204-21
- Controlled Unclassified Information
  - Information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.
  - Comprehensive safeguarding IAW NIST SP 800-171

Information that is collected, created, or received pursuant to a government contract



FCI
Information that is not marked as public or for public release.
Minimum Cybersecurity Requirements in a non-federal information system: Basic Safeguarding Clause: 48 CFR § 52.204-21

CUI
Information that is marked or identified as requiring protection under the CUI program.
Minimum Security Requirements in a non-federal information system: NIST SP 800-171

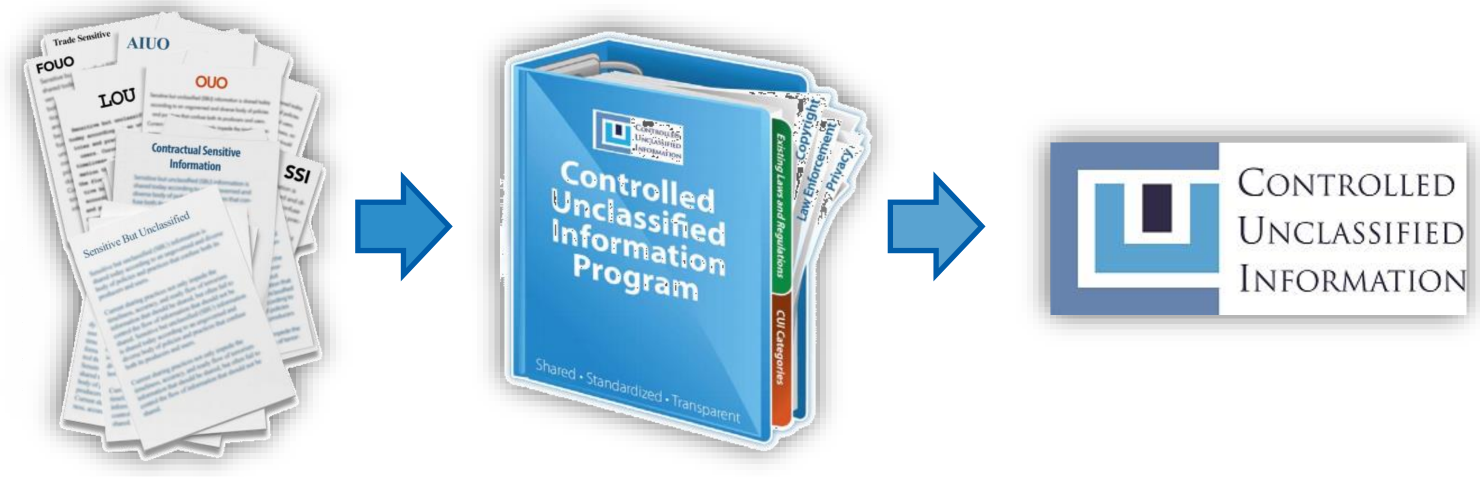
Public Information
Public information or information marked for public release.
Minimum Security Requirements in a non-federal information system: None

All CUI in possession of a Government contractor is FCI, but not all FCI is CUI.

Source: https://www.dau.edu/Lists/Events/Attachments/289/CMMC Webcast 13 October 2020 Final r2.pdf

Controlled Unclassified Information Program

- The CUI Program is an information security reform that standardizes the way the executive branch handles information that requires protection
- Established by Executive Order 13556 on November 4, 2010
- Impacts 100+ departments and agencies within the federal government
  - Also affects foreign governments, state, local, tribal, academia, and businesses


Trade Sensitive
AIUO
FOUO
LOU
OUO
Contractual Sensitive Information
SSI
Sensitive But Unclassified
Controlled Unclassified Information Program
Existing Laws and Regulations
Copyright
Law Enforcement
Privacy
CUI Categories
Shared • Standardized • Transparent
Controlled Unclassified Information

Source: https://www.archives.gov/cui

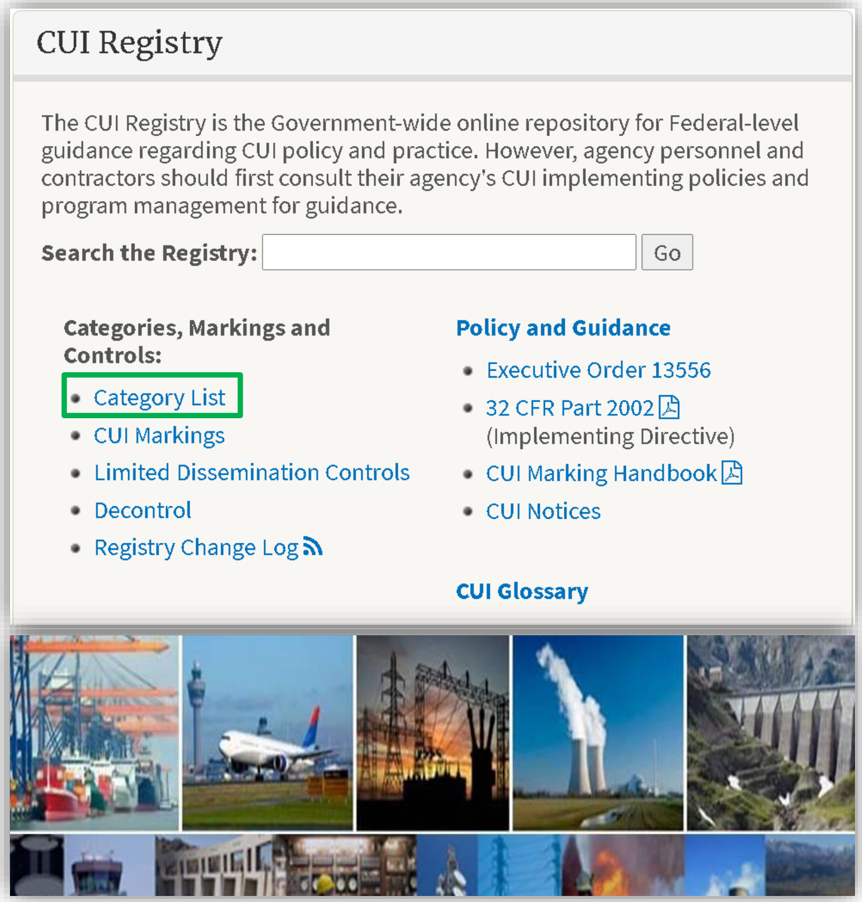
The CUI Registry - DoD Instruction 5200.48

- DoD Instruction 5200.48 (DoDI), Controlled Unclassified Information
- Supersedes DoD Manual 5200.01, Volume 4
- Establishes policy, assigns responsibilities, and prescribes procedures for CUI throughout the DoD IAW Defense Federal Acquisition Regulation Supplement (DFARS) Sections 252.204 7008 and 252.204 7012
- Establishes the official DoD CUI Registry
- General DoD CUI Procedures:
  - 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)

Source: https://www.dau.edu/Lists/Events/Attachments/205/CMMC Webcast Overview 5.13.20.pdf

National Archives and Records Administration (NARA) CUI Registry*

- Defense (most pertinent to DoD)
  - Controlled Technical Information
  - DoD Critical Infrastructure Security Information
  - Naval Nuclear Propulsion Information
  - Unclassified Controlled Nuclear Information - Defense
- Critical Infrastructure
- Export Control
- Financial
- Immigration
- Intelligence
- International Agreements
- Law Enforcement
- Legal
- Natural and Cultural Resources
- NATO
- Nuclear
- Patent
- Privacy
- Procurement and Acquisition
- Proprietary Business Information
- Provisional
- Statistical
- Tax
- Transportation



CUI Registry

The CUI Registry is the Government-wide online repository for Federal-level guidance regarding CUI policy and practice. However, agency personnel and contractors should first consult their agency's CUI implementing policies and program management for guidance.

Search the Registry: [ ] Go

Categories, Markings and Controls:

- Category List
- CUI Markings
- Limited Dissemination Controls
- Decontrol
- Registry Change Log

Policy and Guidance

- Executive Order 13556
- 32 CFR Part 2002 (Implementing Directive)
- CUI Marking Handbook
- CUI Notices

CUI Glossary

*DoD CUI Registry now available as well
https://www.dodcui.mil/Home/DoD-CUI-Registry/

Source: https://www.archives.gov/cui/registry/category-list

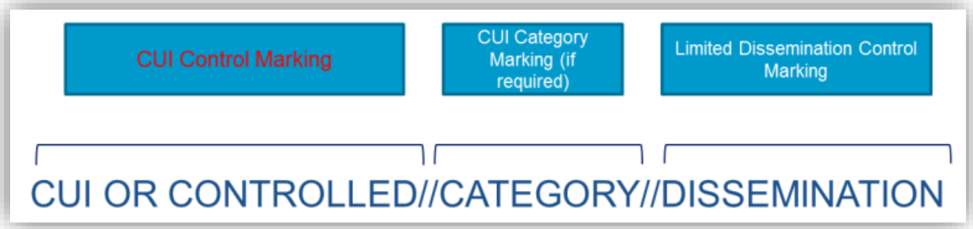
Controlled Technical Information (CTI)

- Controlled Technical Information (CTI)
  - Technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination.
  - Examples include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

Source: https://www.archives.gov/cui/about

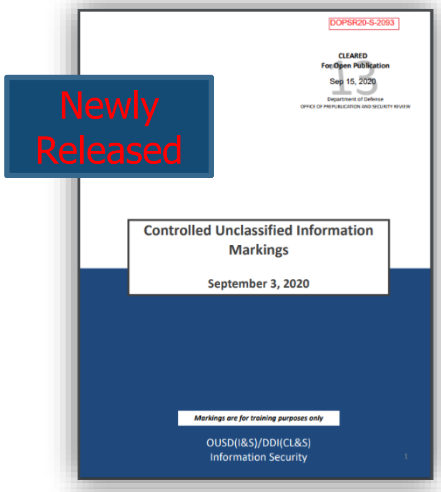
CUI Marking

- Documents / email marked appropriately



CUI Control Marking
CUI Category Marking (if required)
Limited Dissemination Control Marking
CUI OR CONTROLLED//CATEGORY//DISSEMINATION

  - Proper use of CUI Coversheet and/or Labels
  - SF 901 Coversheet
  - SF 902 Media Label
  - SF 903 USB Media Label



Newly Released

DOPSR20-S-2093

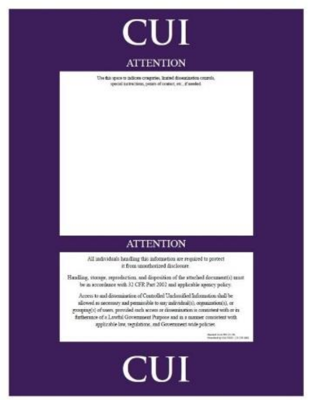
CLEARED
For Open Publication
Sep 15, 2020
Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

Controlled Unclassified Information Markings

September 3, 2020

Markings are for training purposes only

OUSD(I&S)/DDI(CL&S)
Information Security



CUI

ATTENTION

Use this space to indicate categories, limited dissemination controls, special instructions, points of contact, etc., if needed.

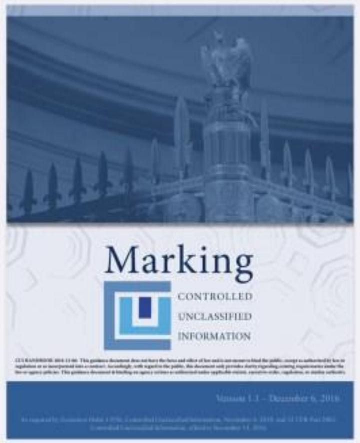
ATTENTION

All individuals handling this information are required to protect it from unauthorized disclosure.

Handling, storage, reproduction, and disposition of the attached document(s) must be in accordance with 32 CFR Part 2002 and applicable agency policy.

Access to and dissemination of Controlled Unclassified Information shall be allowed as necessary and permissible to any individual(s), organization(s), or grouping(s) of users, provided such access or dissemination is consistent with or in furtherance of a Lawful Government Purpose and in a manner consistent with applicable law, regulations, and Government-wide policies.

CUI



Marking

CONTROLLED
UNCLASSIFIED
INFORMATION

Version 1.1 – December 6, 2016

This medium is
CUI
U.S. Government Property

Protect it from unauthorized disclosure in compliance with applicable executive orders, statutes, and regulations.

SF 902 (11-18)

This medium is
CUI
U.S. Government Property

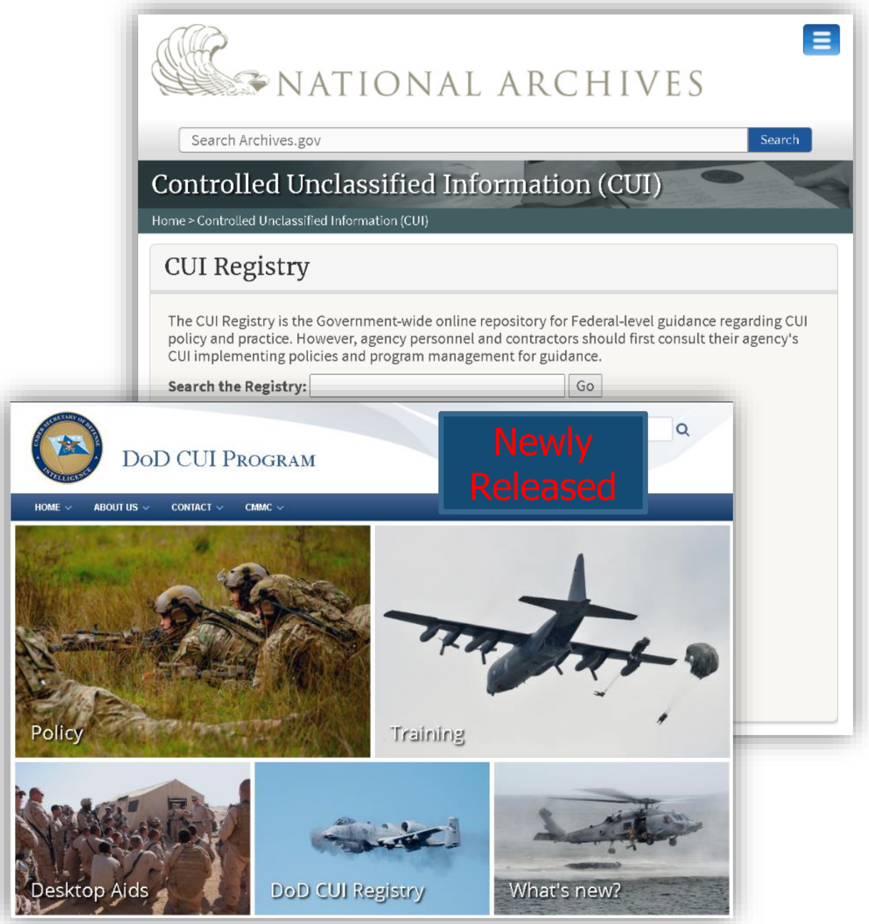
SF 903 (11-18)

Source: https://isoo.blogs.archives.gov/wp-content/uploads/2020/08/Marking-class-presentation-USE-ONLY-.pdf

DoD CUI Program

The DoD CUI Registry:

- Provides an official list of the Indexes and Categories used to identify the various types of CUI used in DoD
- Mirrors the National CUI Registry www.archives.gov/cui
- The registry is located on the NIPRNet Intelink SharePoint site
- Future state of the DoD CUI Registry will be located at https://www.dodcui.mil



Controlled Unclassified Information (CUI)

CUI Registry

The CUI Registry is the Government-wide online repository for Federal-level guidance regarding CUI policy and practice. However, agency personnel and contractors should first consult their agency's CUI implementing policies and program management for guidance.

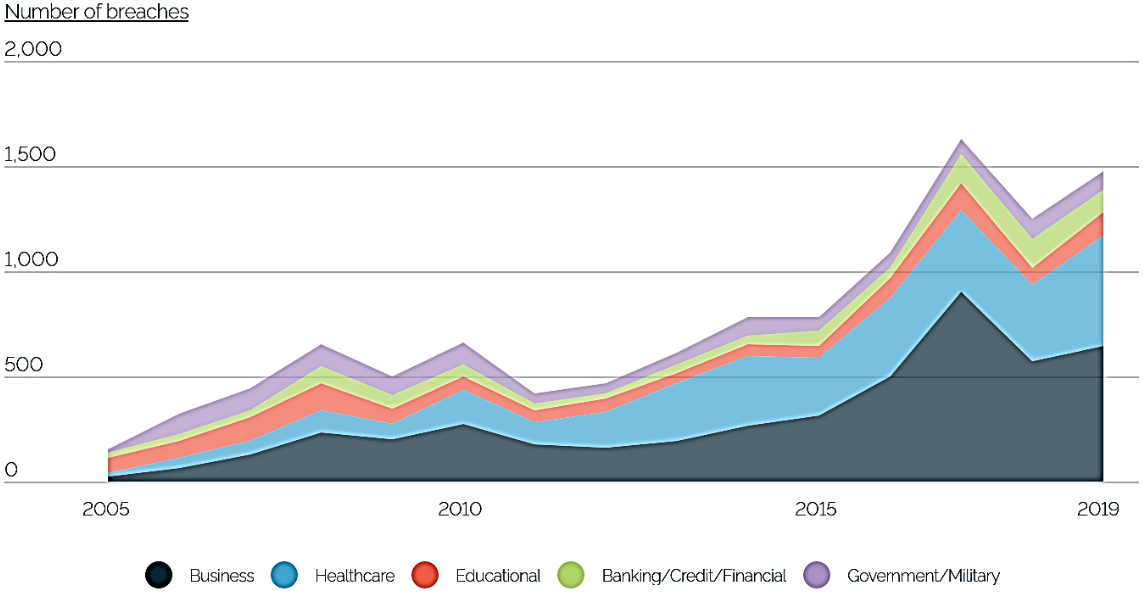
Newly Released

Source: https://www.dodcui.mil/Portals/109/Documents/Desktop Aid Docs/20-S-2093 cleared training guide-13_oct-20.pdf

Why Protect CUI? - Data Breaches

“The protection of Controlled Unclassified Information (CUI) in nonfederal systems and organizations is of paramount importance to federal agencies and can directly impact the ability of the federal government to successfully conduct its assigned missions and business operations.” - NIST Special Publication (SP) 800-171 Protecting Controlled Unclassified Information

“The majority of data breaches stem from hacking and intrusion cases and unauthorized access to records, which comprised more than 75 percent of all data breaches in 2019. On the other hand, employee error and negligence accounted for less than 11 percent of data breaches in 2019.”



Source: Identity Theft Resource Center

Source: https://spanning.com/resources/industry-research/largest-data-breaches-us-history/

Unauthorized Disclosures of CUI

"The loss or improper safeguarding of CUI has a direct impact on national security" - Information Security Oversight Office

- Significant impact of mission capabilities to perform contractual obligations has been significantly degraded due to numerous security breaches involving CUI
- Office of Personnel Management (OPM) Data Breach (2015)
  - Personnel files of 4.2 million former and current government employees.
  - Security clearance background investigation information on 21.5 million individuals

- Anthem / Blue Cross Blue Shield (BCBS) breach
  - Provides insurance for more than 2 million US government employees and 9 million US Government contractors

- Equifax Breach, 147 Million and counting
  - Exposed credit accounts worth of $100B
  - Recent contract award from IRS to provide identity services

Source: https://www.archives.gov/files/cui/documents/unauthorized-disclosures-20170927.pdf

How did we get to CMMC?

USG Supply Chain / Cybersecurity Initiatives

- NIST SP 800-18 Rev 1, Guide for Developing Security Plans for Federal Information Systems, February 24, 2006
- Executive Order 13556: “Controlled Unclassified Information”, November 4, 2010
- FAR Case 2011-020, Basic Safeguarding of Contractor Information Systems, August 24, 2012
- Executive Order 13636: “Improving Critical Infrastructure Cybersecurity”, February 1, 2013
- DFARS Case 2011-D039, Safeguarding Unclassified Controlled Technical Information, November 18, 2013
- Framework for Improving Critical Infrastructure Cybersecurity, February 12, 2014
- NIST Special Publication 800-171 - Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, June 19, 2015
- OMB draft Guidance: “Improving Cybersecurity Protections in Federal Acquisitions”, August 11, 2015
- DFARS Case 2013-D018, Network Penetration Reporting and Contracting for Cloud Services, Interim Rule, August 26, 2015
- DFARS Provision 252.239-7009 - Representation of Use of Cloud Computing, September 1, 2015
- Proposed Rule: Detection and Avoidance of Counterfeit Electronic Parts, September 21, 2015
- DoD Class Deviation - Multifactor authentication (local/network access), October 8, 2015
- OMB Memorandum: “Cybersecurity Strategy and Implementation Plan” (CSIP), October 30, 2015
- NDAA FY 2016 (includes cyber risk assessment), November 1, 2015
- Cybersecurity Information Sharing Act (CISA) signed into law, December 18, 2015
- DFARS Case 2013-D018, Network Penetration Reporting and Contracting for Cloud Services, Interim Rule, December 30, 2015
- Basic Safeguarding of Contractor Information Systems, May 16, 2016
- 32 CFR Part 2002, Controlled Unclassified Information, September 1, 2016
- 32 CFR Part 236, DoD Defense Industrial Base Cybersecurity Activities, October 1, 2016
- DFARS Provision 252.204-7008 - Compliance with Safeguarding Covered Defense Information Controls, October 1, 2016
- DFARS Clause 252.204-7009 - Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information, October 1, 2016
- DFARS Clause 252.239-7010 - Cloud Computing Services, October 1, 2016
- DFARS Case 2013-D018, Network Penetration Reporting and Contracting for Cloud Services, Final Rule, October 21, 2016
- DFARS Rule 239.76 - Cloud Computing, October 21, 2016
- NIST Special Publication 800-171, Revision 1 - Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, December 1, 2016
- DoDI 5000.02, Enclosure 14, Cybersecurity in the Defense Acquisition System, February 1, 2017
- PGI 204.73, December 1, 2017
- DFARS Rule 204.73 - Safeguarding Covered Defense Information and Cyber Incident Reporting, December 28, 2017
- NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information, June 13, 2018
- DCMA updates the Contractor Purchasing System Review (CPSR) Guidebook to incorporate protection of CDI, February 26, 2019
- Assessing Contractor Implementation of Cybersecurity Requirements, November 1, 2019
- DFARS Clause 252.204-7012 - Safeguarding Covered Defense Information and Cyber Incident Reporting, December 1, 2019
- NIST Special Publication 800-171, Revision 2 - Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, February 21, 2020
- DoD Instruction 5200.48 Controlled Unclassified Information (CUI), March 1, 2020
- DoDI 8582.01, Security of Unclassified DoD Information on Non-DoD Information Systems (Under Revision), March 1, 2020
- NIST SP 800-171 DoD Assessment Methodology, June 1, 2020
- DFARS 252.204-7019, Notice of NIST SP800-171 DoD Assessment Requirements, September 29, 2020
- DFARS 252.204-7020, NIST SP800-171 Assessment Requirements, September 29, 2020
- DFARS 252.204-7021, Cybersecurity Maturity Model Certification Requirements, September 29, 2020

Source: https://dodprocurementtoolbox.com/site-pages/cybersecurity-policy-regulations

Contract Requirements (FCI/CUI)

- Revised Contract Requirements (Nov 2019):
  - Federal Acquisition Regulation (FAR) 52.204-21 - (FCI)
  - DoDI 5200.48 -(CUI)
  - DFARS 252.204-7008 - DoD CUI
  - DFARS 252.204-7012 - DoD CUI
- New Contract Requirements (Sept 2020)
  - DFARS 252.204-7019, Notice of NIST SP 800-171 DoD Assessment Requirements
  - DFARS 252.204-7020, NIST SP 800-171 Assessment Requirements
  - DFARS 252.204-7021, CMMC Requirements

Source: https://www.dau.edu/Lists/Events/Attachments/240/CMMC Webcast 19 May 2020.pdf

DFARS Clause 252.204-7008, 7009, & 7012

DFARS Clause 252.204-7008, 7009, & 7012

- MUST be included in ALL contract actions with no exceptions, including, but not limited to:
  - Request for Quote (RFQ) against all GSA Schedule Contracts
  - Request For Information (RFI)
- Scope covers, at a minimum, the following categories
  - Protect all CTI
  - Implement the security requirements specified by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 not later than December 31, 2017
  - Flow down requirements to subcontractors
  - “Rapidly report”, within 72 hours, of discovery of any cyber incident

Source: https://www.dau.edu/Lists/Events/Attachments/276/CMMC Webcast 9.22.20.pptx

DoDI 8582.01

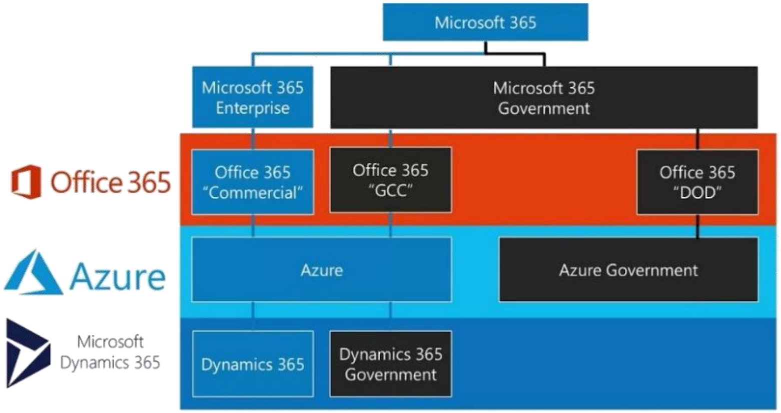
DoDI 8582.01, Security of Non DoD Information Systems Processing Unclassified Nonpublic DoD Information (twin brother of DFARS 252.204-7012)

- 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

Source: https://www.dau.edu/Lists/Events/Attachments/272/CMMC Webcast 8.25.20.pdf

Contractor use of Cloud Computing

- Safeguarding DoD CUI and Cyber Incident Reporting 48 Code of Federal Regulations (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
- Microsoft in-scope cloud services
  - Azure Government
  - Dynamics 365 U.S. Government
  - Intune
  - Office 365 U.S. Government Community Cloud (GCC)
  - Office 365 GCC High, and DoD



Microsoft 365

Microsoft 365 Enterprise

Microsoft 365 Government

Office 365

Office 365 “Commercial”

Office 365 “GCC”

Office 365 “DOD”

Azure

Azure

Azure Government

Microsoft Dynamics 365

Dynamics 365

Dynamics 365 Government

Source: https://www.dau.edu/Lists/Events/Attachments/205/CMMC Webcast Overview 5.13.20.pdf

DFARS Case 2019-D041

- DoD has issued an interim rule to amend the DFARS to implement a DoD Assessment Methodology and Cybersecurity Maturity Model Certification framework in order to assess contractor implementation of cybersecurity requirements and enhance the protection of unclassified information within the DoD supply chain
  - DFARS 252.204-7019, Notice of NIST SP 800-171 DoD Assessment Requirements
  - DFARS 252.204-7020, NIST SP 800-171 Assessment Requirements
  - DFARS 252.204-7021, Cybersecurity Maturity Model Certification Requirements
- Directs the use of the NIST SP 800-171 DoD Assessment Methodology by contractors as well as instructs contracting officers to verify in SPRS that an offeror has a current assessment on record, prior to contract award, if the offeror is required to implement NIST SP 800-171 pursuant to DFARS clause 252.204-7012
- Directs the use of the CMMC framework and requirement to obtain accreditation by a CMMC Third-Party Assessor Organization (C3PAO)

Effective November 30, 2020

SPRS
Supplier Performance Risk System

Guiding the DoD in Responsible Acquisition Decisions

WELCOME

Sources: https://www.govinfo.gov/content/pkg/FR-2020-09-29/pdf/2020-21123.pdf

https://www.regulations.gov/document?D=DARS-2020-0034-0002

DoD Assessment Methodology

NIST SP 800-171, DoD Assessment Methodology (v1.2.1 latest)

- Standard DoD-wide methodology for assessing DoD contractor implementation of the security requirements in NIST SP 800-171
- 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
- Authorized representatives of the contractor may enter results for Basic (self) assessments
- Defense Contract Management Agency's (DCMA) Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) may enter summary results for Medium and High assessments
- DoD will use this 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

Source: https://www.acq.osd.mil/dpap/pdi/cyber/strategically_assessing_contractor_implementation_of_NIST_SP_800-171.html

CMMC

- 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)
- The goal is for CMMC to be cost-effective and affordable for small businesses to implement at the lower CMMC levels.
- The intent is for certified independent 3rd party organizations to conduct audits, inform risk, and grant 3-year certifications of DIB contractors

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

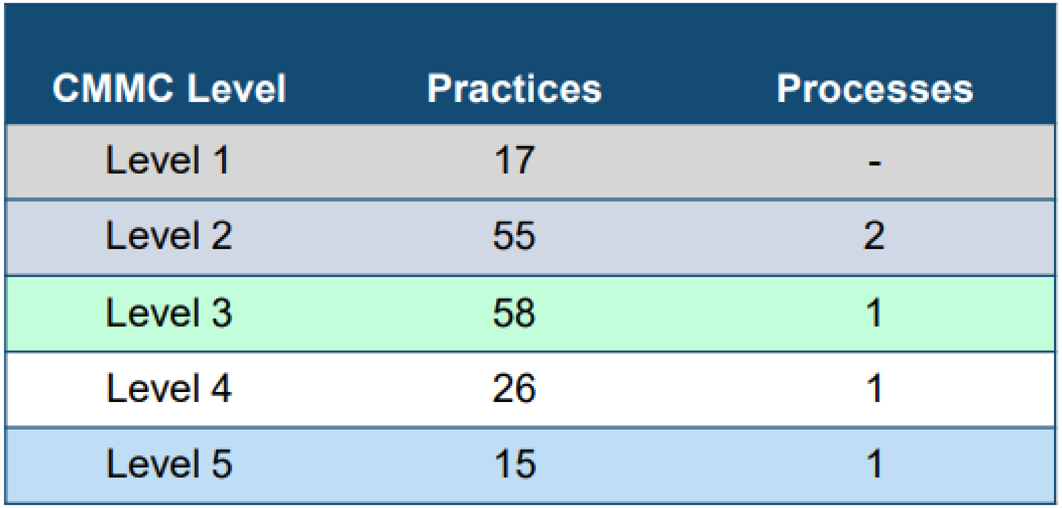
CMMC Suggested Roles/Responsibilities

- Requires the program office/requiring activity to:
  - Identify FCI/CUI Data and Marking Requirements
  - Develop/Update Security Classification Guide (SCG), Work Breakdown Structure (WBS), and Program Protection Plan (PPP)
  - Identify CMMC Level(s)
- Requires the contractor/subcontractor to:
  - Develop/Update Artifacts/Deliverables per RFI/RFP
  - Request C3PAO to perform CMMC assessment
  - Develop Supply Chain/Tier 1 & below Contractor Support Agreements

Source: https://www.dau.edu/Lists/Events/Attachments/289/CMMC Webcast 13 October 2020 Final r2.pdf

CMMC Practices and Processes Focus

- Level 1
  - Safeguard Federal Contract Information
- Level 2
  - Serve as a transition step in cybersecurity maturity progression to protect CUI
- Level 3
  - Protect Controlled Unclassified Information
- Level 4-5
  - Protect CUI and reduce the risk of Advanced Persistent Threats (APTs)
  - Based on a penetration resistant architecture, damage limiting operations, a cyber resilient and survivable design



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

Each level builds on the previous levels.
Practices and processes are cumulative!

Source: https://www.acq.osd.mil/cmmc/docs/CMMC_v1.0_Public_Briefing_20200131_v2.pdf

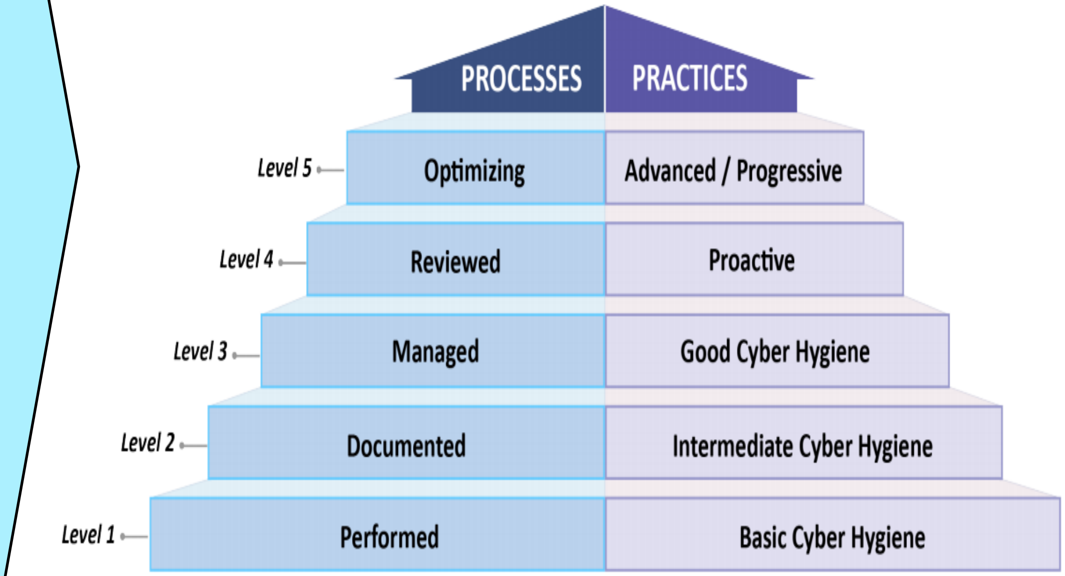
CMMC Domains and Maturity Levels

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) ★	

★ Tied to equivalent 800-53 control family

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

Source: https://www.acq.osd.mil/cmmc/docs/CMMC_v1.0_Public_Briefing_20200131_v2.pdf

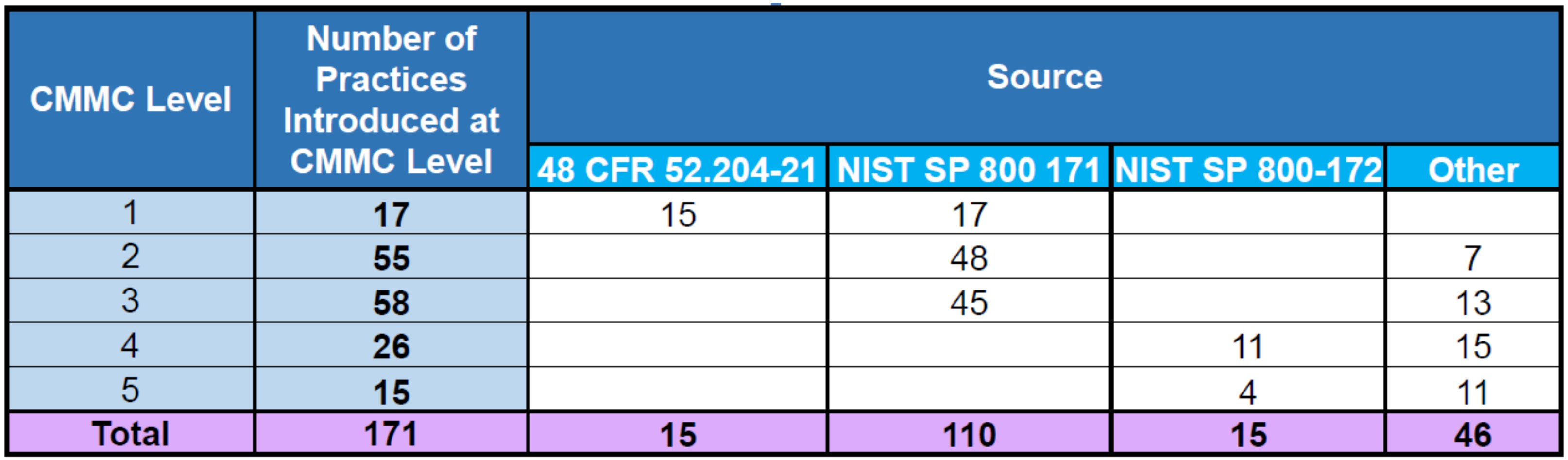
CMMC Levels and Source Requirements

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

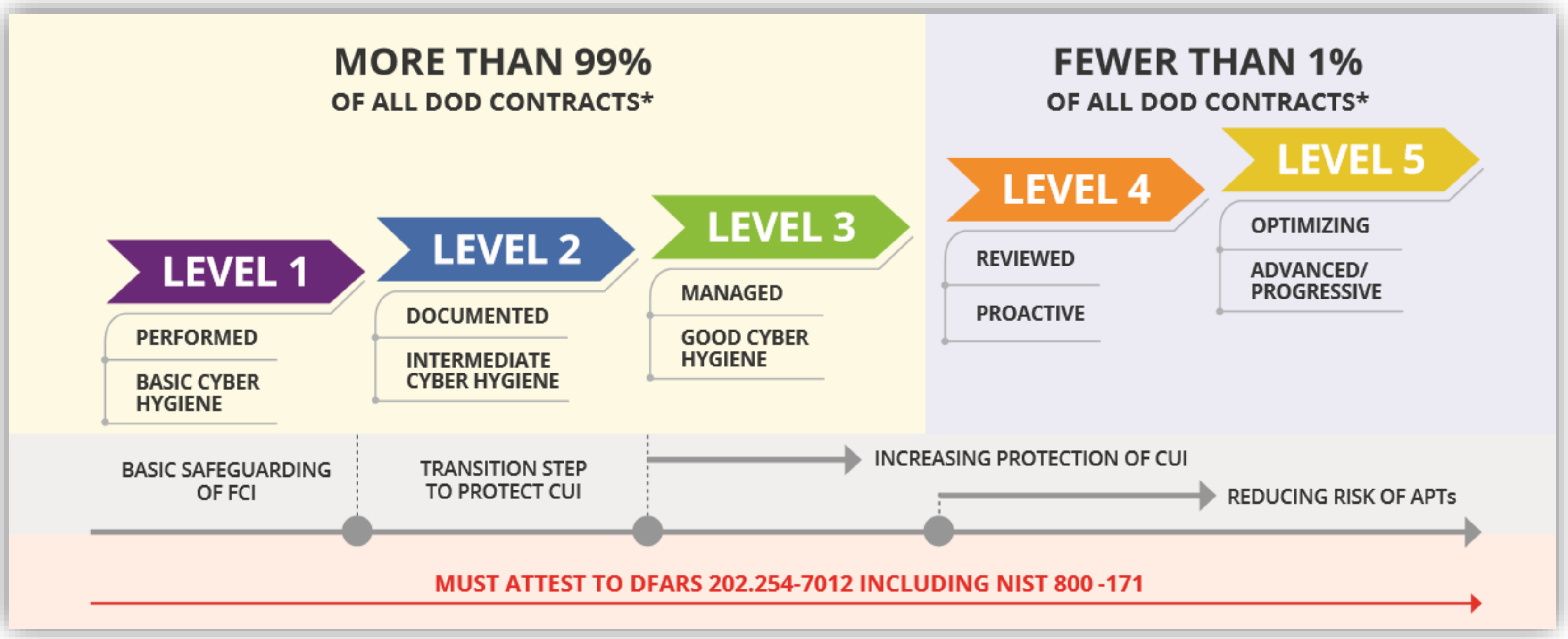
- Security Requirements:
  - Level1-3 + NIST SP 800-172 (171B)
- Threat Centric Approach
  - Worst Case Scenario
- What could the threat do?
  - Zero trust architecture, analysis, & dynamic defense



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**

Source: https://www.dau.edu/Lists/Events/Attachments/289/CMMC Webcast 13 October 2020 Final r2.pdf

What CMMC Levels To Expect

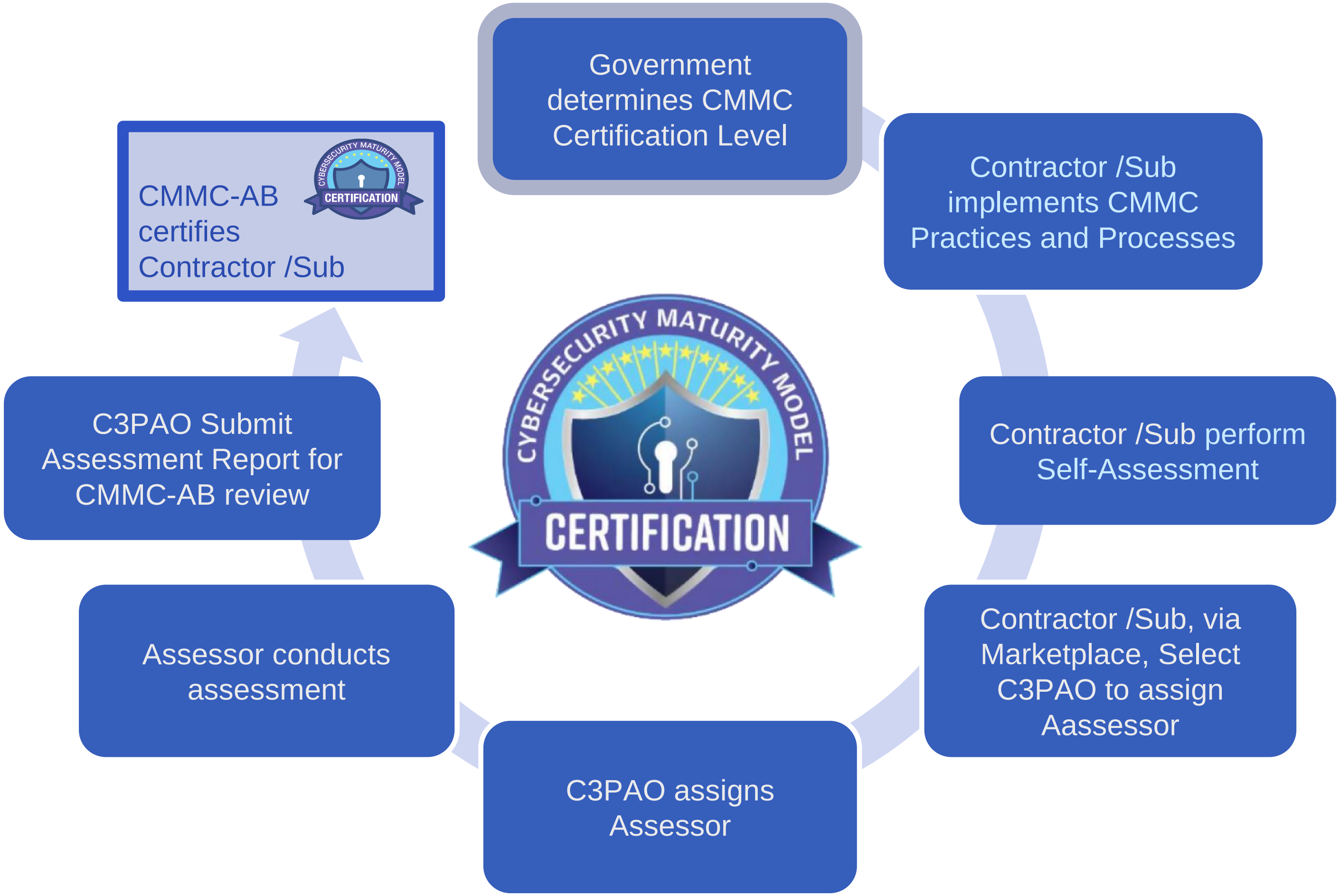


“Every company within the DoD supply chain — not just the defense industrial base, but the 300,000 contractors — are going to have to get certified to do work with the Department of Defense…., and then we can really start looking at our supply chain, where our most and greatest vulnerabilities lie…..It’s going to take time, it’s going to be painful, and it’s going to cost money.”

* Ms. Katie Arrington, CISO in the Office of the Undersecretary of Defense for Acquisition, at the October 2019 Intelligence & National Security Summit

Source: https://adcg.org/binary-new-cybersecurity-compliance-requirements-for-government-contractors

CMMC Certification Process



Government determines CMMC Certification Level

Contractor /Sub implements CMMC Practices and Processes

Contractor /Sub perform Self-Assessment

Contractor /Sub, via Marketplace, Select C3PAO to assign Aassessor

C3PAO assigns Assessor

Assessor conducts assessment

C3PAO Submit Assessment Report for CMMC-AB review

CMMC-AB certifies Contractor /Sub

Source: https://www.dau.edu/Lists/Events/Attachments/276/CMMC Webcast 9.22.20.pptx

Compliance Roadmap

- Accurately Identify FCI/CUI in your environment
  - Identify where the data lives and how it’s used
  - Work on reducing footprint through proper disposal of unneeded data
  - Minimize receipt/generation by ensuring you need the data
  - Investigate benefits of segmenting networks and access to data
  - Establish clear responsibilities regarding data use for employees and 3rd parties
- Consider outsourcing a portion of compliance obligations by storing FCI/CUI in a FedRAMP approved cloud
  - https://marketplace.fedramp.gov
- Review your implementation of NIST SP 800-171 (Self attestation deadline was December 2017)
- Complete, at a minimum, a Basic (self) assessment utilizing the NIST SP 800-171 DoD Assessment Methodology
  - Submit results to the Supplier Performance Risk System (SPRS)
- Plan to schedule a CMMC audit with a CMMC Third Party Assessment Organization (C3PAO)

Expected Challenges

- Non-Technical
  - Clearly identifying CUI when it is received and transferred
  - Identifying and marking all CUI
  - Flowing requirements down through supply chain
  - Budgeting for NIST SP 800-171 / CMMC compliance and certification
  - Frequent changes to regulations and applicability
  - Flow down of excessive requirements from Prime to Subs
- Technical
  - Processing CUI via Email
  - Multi-factor Authentication
  - SEIM Solution
  - Backup Solutions
  - Managing non-supported hardware/software
  - Continuous Monitoring Program

Defense Acquisition University CMMC Webcast Series

Assured Information Technology
The Key To Your Information Assurance

05/13/2020, 12:30 PM	Cybersecurity Maturity Model Certification: Overview and Latest Developments
05/19/2020, 2:00 PM	Cybersecurity Maturity Model Certification : Latest Developments Question and Answer Session
06/03/2020, 12:30 PM	Cybersecurity Maturity Model Certification : Overview and Latest Developments
06/23/2020, 12:00 PM	Cybersecurity Maturity Model Certification: Request for Information/Proposal (RFI/RFP) Contract Strategy Considerations to Implement the CMMC
08/11/2020, 12:30 PM	Cybersecurity Maturity Model Certification: DoD Assessment Methodology Tool Implementation (NIST 800-171 v1.1)
08/25/2020, 12:30 PM	Cybersecurity Maturity Model Certification: Migration from NIST SP 800-171 to the new CMMC process
09/22/2020, 12:30 PM	The Cybersecurity Maturity Model Certification Request for Information/Proposal (RFI/RFP)
10/13/2020, 12:30 PM	The Cybersecurity Maturity Model Certification: Selecting the CMMC level (I, III, and III+) to Protect (FCI) and (CUI)
11/17/2020, 12:30 PM	The Cybersecurity Maturity Model Certification

Source: https://www.dau.edu/dau-webcasts/p/explore-webcast-series

AIT Overview

Assured Information Technology
The Key To Your Information Assurance

- Veteran-owned Small Business Founded in 2011
- Located at 12001 Research Pkwy, Suite 128
- Primarily Focused on Cybersecurity and Information Technology
- Experts in Risk Management Framework (RMF)
- Subject Matter Experts in all related areas
  - Networks (Cisco, Juniper, SonicWall, etc.)
  - Databases (Oracle, SQL, Postgres, NoSQL, Cassandra, etc.)
  - Software Development (Java, C#, C++, etc.)
  - Operating Systems (Windows, Linux, Android, MAC, Apple IOS, etc.)
  - Policy (Configuration Management, Change Control, Software Dev)
  - Compliance (FISMA, Sarbanes Oxley, HIPAA, Penetration testing, etc.)
  - Virtualization (VMware, Hyper-V, Amazon Web Services, Microsoft Azure, etc.)
  - Wireless (802.11, 802.16, Cellular, Bluetooth, Microwaves, etc.)
- AIT personnel achieved over 100 Authority to Operate (ATO) with 100% Success
- Developed and fielded over 30 Cross Domain Solutions (CDS)
- DoD 8570.01-M Certified workforce with DoD, DoS, DHS, DoD contractor and commercial expertise

Team of Cybersecurity process experts and all related technical disciplines

How AIT Can Help

- Consultation to provide assessment framework and compliance roadmap
- Developing Cybersecurity docs toward achieving Accreditation
- Deciphering Requirements versus Directives with RMF, NIST SP 800-171, NARA, DFARS, and NIST 800-53 and 800-37
- Continuous Monitoring Setup Assistance or via Managed Services
  - Extensive Experience with Splunk configurations and monitoring
- Multi-factor authentication analysis and implementation recommendations
- Development and sustainment of required Policies and Procedures
- Tools and automation to assist with compliance and requirements management (Keystone Demo)

Expert support for as much or little as any company requires

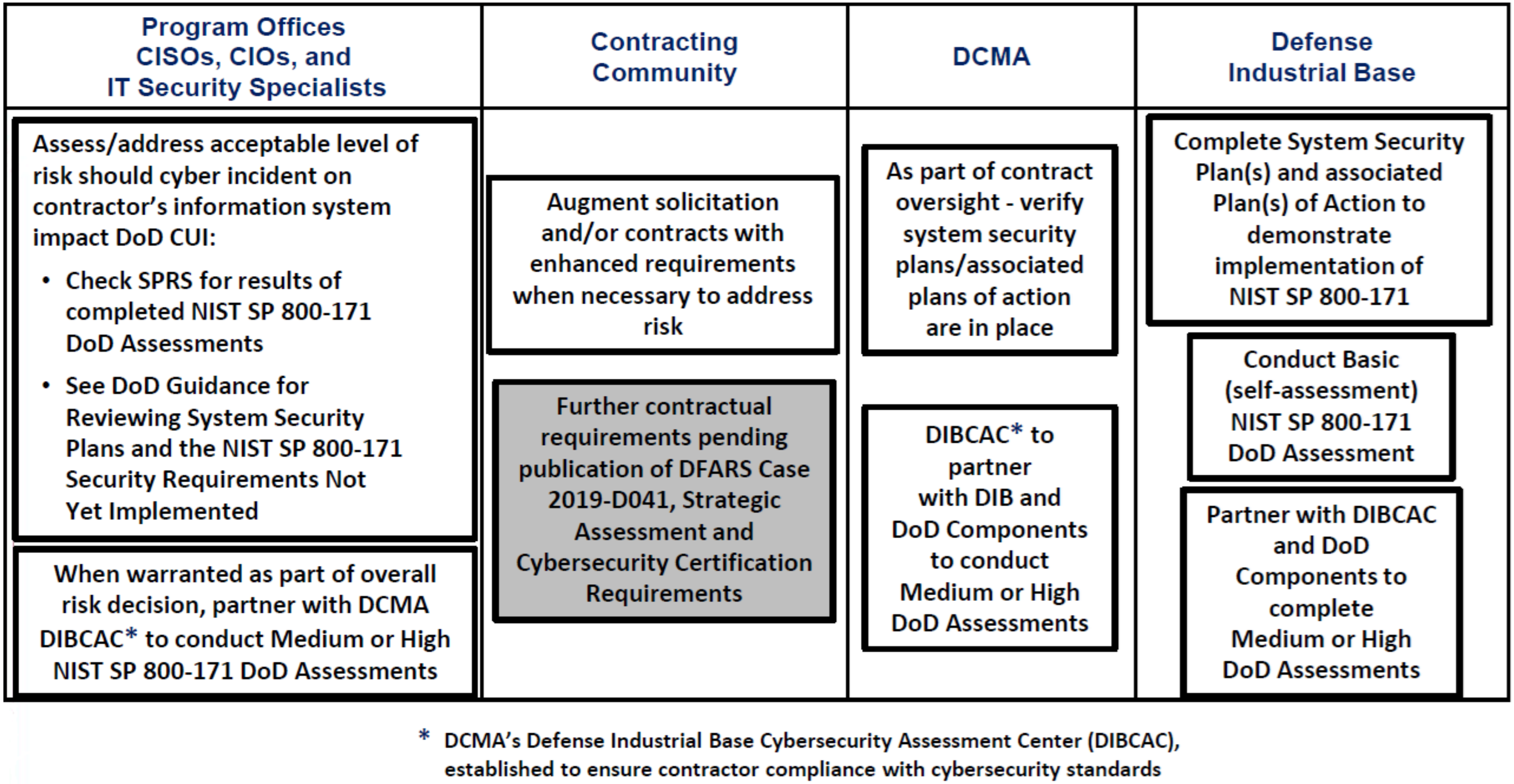
Reference / More Information

- AIT Engineering
  - Jason Eddy
  - Joe Pennetti
- Approved Cloud Service Providers
- CMMC document source
- CMMC Updates
- CMMC FAQ
- CMMC Accreditation Body
- Cyber Assist CMMC Help
- Defense Acquisition University
- DHS Enhanced Cybersecurity Services
- DoD Assessment Methodology
- DoD CUI Program
- DoD CUI Registry
- DoD CUI Marking Aid
- DoD CUI Training
- DoD Cyber Crime Center
- DoD Office of Small Business Programs - Project Spectrum
- NARA CUI Program
- NARA CUI Categories
- NARA CUI Marking Handbook
- NARA CUI Training
- NIST Special Pub 800 Series
- Software Engineering Institute

Terms

- C3PAO: CMMC Third-Party Assessor Organization
- CDI: Covered Defense Information
- CUI: Controlled Unclassified Information
- CFR: Code of Federal Regulations
- DFAR: Defense Federal Acquisition Regulation
- DFARS: Defense Federal Acquisition Regulation Supplement
- DoDI: DoD Instruction
- FAR: Federal Acquisition Regulation
- FCI: Federal Contract Information
- FIPS: Federal Information Processing Standards
- FISMA: Federal Information Systems Modernization Act
- GSA: General Services Administration
- NARA: National Archives & Records Administration
- NIST: National Institute of Standards & Technology
- OMB: Office of Management and Budget
- OPM: Office of Personnel Management
- OUSD A&S: Office of the Under Secretary of Defense for Acquisition & Sustainment

DoD Assessment Stakeholder Roles and Responsibilities

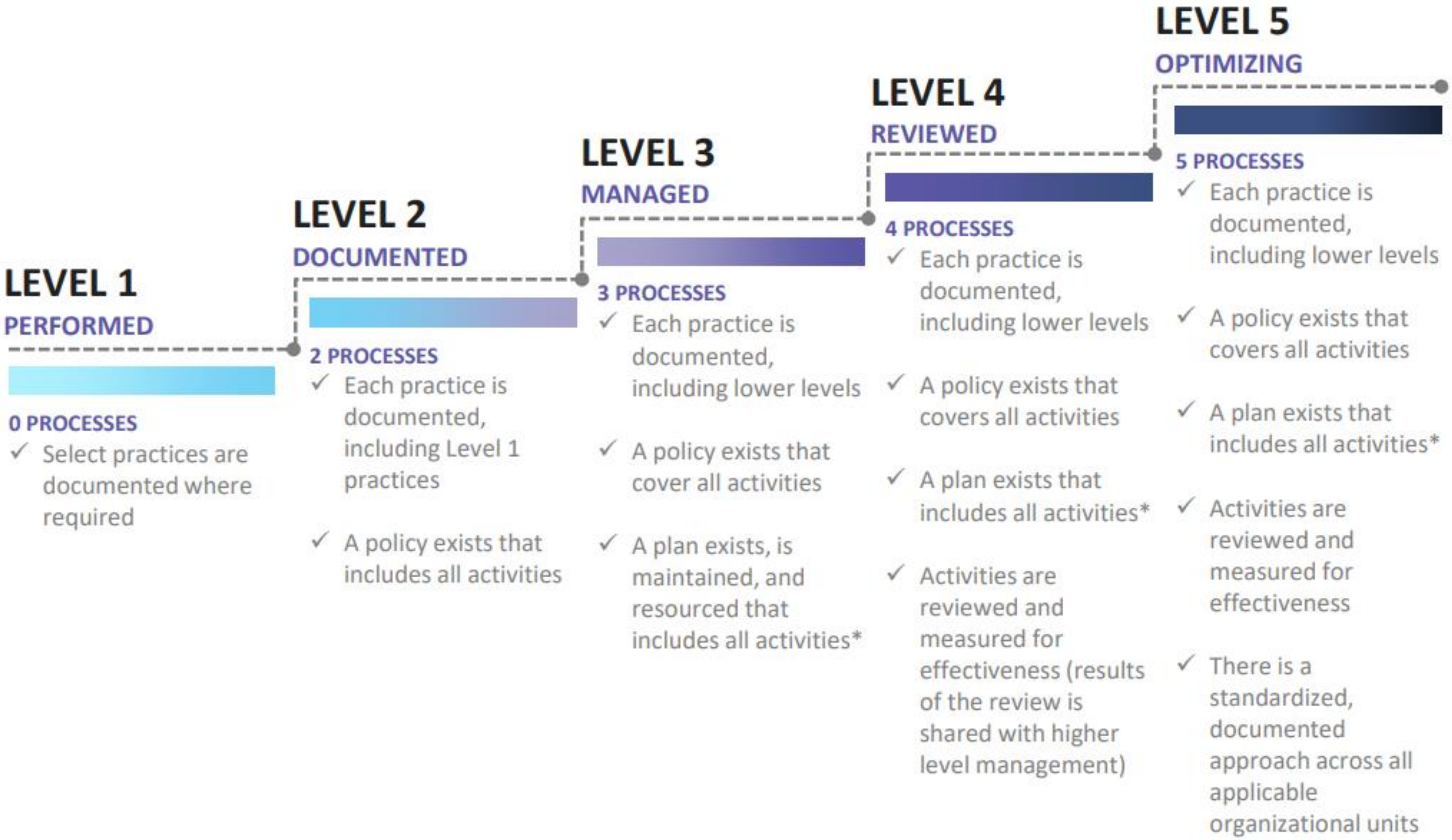


Program Offices CISOs, CIOs, and IT Security Specialists	Contracting Community	DCMA	Defense Industrial Base
Assess/address acceptable level of risk should cyber incident on contractor's information system impact DoD CUI: • Check SPRS for results of completed NIST SP 800-171 DoD Assessments • See DoD Guidance for Reviewing System Security Plans and the NIST SP 800-171 Security Requirements Not Yet Implemented When warranted as part of overall risk decision, partner with DCMA DIBCAC* to conduct Medium or High NIST SP 800-171 DoD Assessments	Augment solicitation and/or contracts with enhanced requirements when necessary to address risk Further contractual requirements pending publication of DFARS Case 2019-D041, Strategic Assessment and Cybersecurity Certification Requirements	As part of contract oversight - verify system security plans/associated plans of action are in place DIBCAC* to partner with DIB and DoD Components to conduct Medium or High DoD Assessments	Complete System Security Plan(s) and associated Plan(s) of Action to demonstrate implementation of NIST SP 800-171 Conduct Basic (self-assessment) NIST SP 800-171 DoD Assessment Partner with DIBCAC and DoD Components to complete Medium or High DoD Assessments

* DCMA's Defense Industrial Base Cybersecurity Assessment Center (DIBCAC), established to ensure contractor compliance with cybersecurity standards

Source: https://www.dau.edu/Lists/Events/Attachments/207/CMMC Webcast 8.11.20.pdf

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

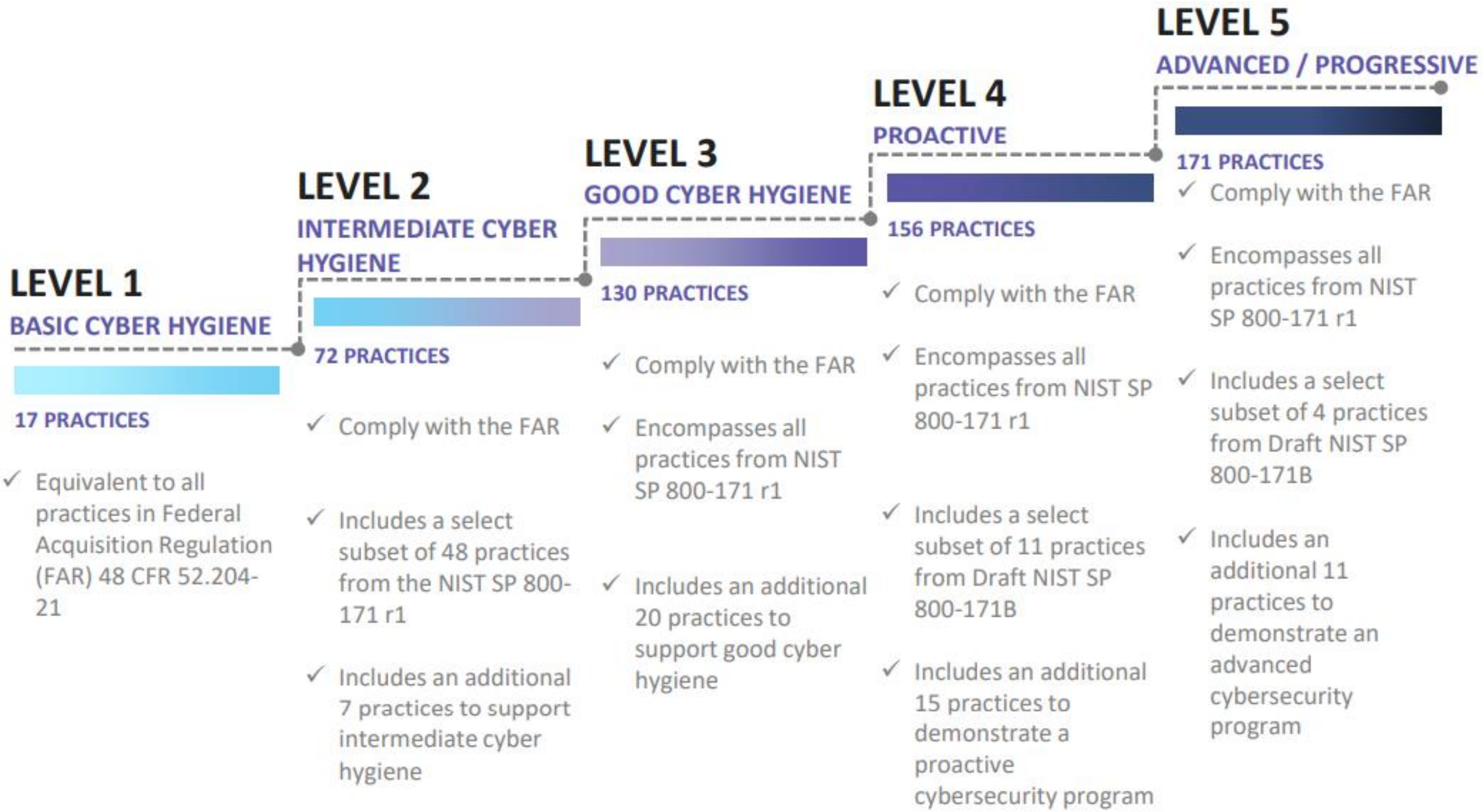
4 PROCESSES
- ✓ Each practice is documented, including lower levels
- ✓ A policy exists that covers all activities
- ✓ A plan exists that includes all activities*
- ✓ Activities are reviewed and measured for effectiveness (results of the review is shared with higher level management)

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

Source: https://www.acq.osd.mil/cmmc/docs/CMMC_v1.0_Public_Briefing_20200131_v2.pdf

CMMC Practice 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

Source: https://www.acq.osd.mil/cmmc/docs/CMMC_v1.0_Public_Briefing_20200131_v2.pdf