Successfully Navigating the CMMC & DOD's New Interim DFARS Rule

Reggie Jones
Partner, Fox Rothschild LLP

Matt Gilbert
Principal, Baker Tilly

Mike Baker
CISO, GDIT

DoD's Goal and the Associated Contract Clauses

The Goal

To promote and achieve:

- Penetration-resistant cyber architecture
- Damage limiting operations
- Designs to achieve cyber resiliency and survivability

NIST 800-172 (Draft), Section 1.1, Lines 255-258 (July 2020)

The Path to Achieve the Goal

- FAR 52.204-21 (Basic Safeguarding of Covered Contractor Information Systems)
- DFARS 252.204-7012 (Safeguarding Covered Defense Information and Cyber Incident Reporting)

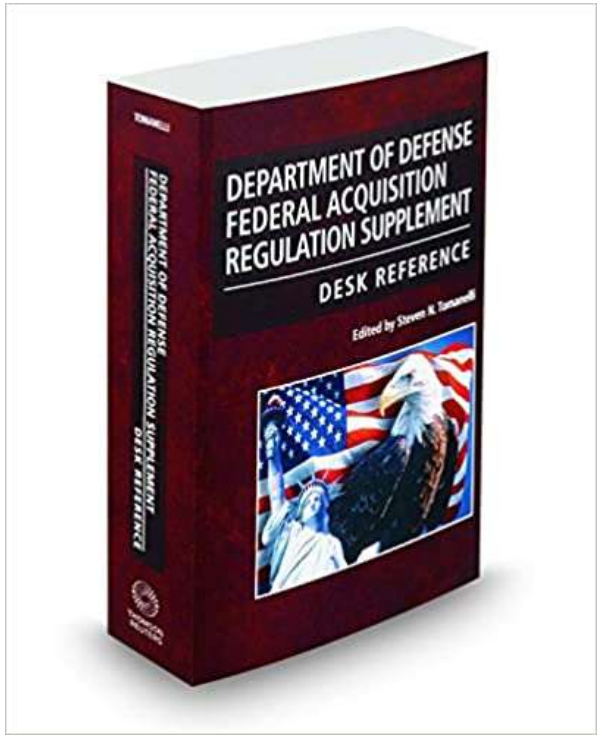
- *New Interim Rule:* DFARS clause 252.204-7019 (Notice of NIST SP 800-171 DoD Assessment Requirements)
- *New Interim Rule:* DFARS clause 252.204-7020, (NIST SP 800-171 DoD Assessment Requirements)
- *New Interim Rule:* DFARS clause 252.204-7021 (Cybersecurity Maturity Model Certification Requirements)

FAR 52.204-21 (Basic Safeguarding of Covered Contractor Information Systems)

- Only covers ***information systems***, not the information contained on those systems
- FAR 52.204-21= CMMC Level 1 (Basic Cybersecurity Hygiene)
- Became final rule in 2016; first contract clause to meaningfully address cybersecurity information systems across all agencies, not just DOD
- 15 basic safeguarding requirements
- No requirements for training, penetration testing, cyber incident reporting or cybersecurity insurance

Safeguarding Covered Defense Information and Cyber Incident Reporting (DFARS 252.204-7012)

- Covers ***information***, not just the ***information system*** itself
- Incorporates NIST SP 800-171
- Requires implementation of 110 security requirements on “covered contractor information systems”
- Document in System Security Plan & Plans of Action & Milestones (POAMs) those requirements not yet implemented and when they will be implemented



What are the Cyber Incident Reporting Requirements?

- Must "***rapidly report***" cyber incident within "***72 hours of discovery***"
  - Report "whatever information is available"
  - Continuing obligation to disclose new information
  - Must preserve and protect images of all known affected information systems for at least 90 days to allow DOD to request the media
- A cyber incident is defined as: "actions taken through the use of computer networks that result in a compromise or an actual or potential adverse effect on an information system and/or the information residing therein"
- Much faster than the mandatory disclosures required under FAR 52.203-13 (Contractor Code of Business Ethics)
- ***Have agreement with third-party forensic consultant already in place!***

What Information Is Covered?

- The clause applies to "all ***covered defense information***" (CDI), which is defined as:
- **Unclassifed Controlled Technical Information (CTI)**
  - https://www.archives.gov/cui/registry/category-detail/controlled-technical-info.html; ***or***
- **Controlled Unclassified Information (CUI)**
  - https://www.archives.gov/cui/registry/category-list
  - Executive Order 13556 defines and calls upon management of CUI

NIST SP 800-171 DoD Assessment Requirements (DFARS 252.204-7019 & 20)

- *New DoD assessment methodology!*
- Requires contractors subject to DFARS 252.204-7012 to self complete a Basic Assessment and upload the resulting score into the Supplier Risk Management System (SPRS) prior to contract award
- Medium and High Assessments may be required and will be completed by the government (DCMA's Defense Industrial Base Cybersecurity Assessment Center or DIBCAC)
- Requires contractors to flow same requirement down to subcontractors in "all subcontracts and other contractual instruments"
  - 7020 Clause for SP 800-171 Assessments
    - "information systems relevant to its offer"
- Transition clause until October 1, 2025

Cybersecurity Maturity Model Certification Requirements (DFARS 252.204-7021)

- *New DoD assessment methodology!*
- Requires contractors to maintain the requisite CMMC level for the duration of the contract
- Establishes the CMMC Accreditation Body (CMMC-AB) and Certified Third Party Assessor Organization (C3PAOs)
- Requires contractors to flow same requirement down to subcontractors in "all subcontracts and other contractual instruments"
  - 7021 Clause for CMMC Requirements
    - "CMMC level that is appropriate for the information"
- *See 85 Fed. Reg. 61,505 (Sept. 29, 2020)*

DOD Instruction 5200.48 (March 6, 2020)

- 5.3.a. – "Whenever DOD provides information to contractors, it must identify whether any of the information is CUI via the contracting vehicle … and mark such documents … ."
- 5.3.b. – "Whenever the DOD provides CUI to, or CUI is generated by, non-DOD entities, protective measures and dissemination controls … will be articulated in the contract."
- Creates a parallel, more detailed DOD CUI registry
- No requirement to remark legacy material unless shared outside of DOD

What is CMMC?

What Is the Cybersecurity Maturity Model Certification (CMMC)?

- A mandatory third-party certification of DoD contractors and subcontractors' information systems that is intended to protect sensitive, but unclassified data against cyber threats (CUI).
- Created with federal funding by:
  - Carnegie Mellon University
  - Johns Hopkins University Applied Physics Laboratory, LLC
- First draft version released in September 2019 (Version 0.4)
- Final version released January 30, 2020
- Requires reassessments/re-certification every 3 years

Why CMMC in addition to staying the 800-171 course?

- Need for more consistency from contractors
  - NIST SP 800-171 requirements were often widely interpreted and companies could extend Plans of Action and Milestones (POA&M) to cover gaps indefinitely
- Findings that contractors were not compliant with NIST SP 800-171
  - "DOD contractors did not consistently implement DoD-mandated system security controls for safeguarding Defense information." (Findings in July 2019 DoD OIG Report)
  - Information losses included theft of transport plane and fighter jet data, among other losses
  - CMMC FAQs: https://www.acq.osd.mil/cmmc/faq.html

CMMC Basics

- 5 maturity levels
- 17 domains
- 171 best practices

- Level 3:
  - NIST 800-171 consists of 110 security requirements
  - CMMC adds 20 practices and 3 processes

CMMC Version 1.0, supra note 46, at 3–4

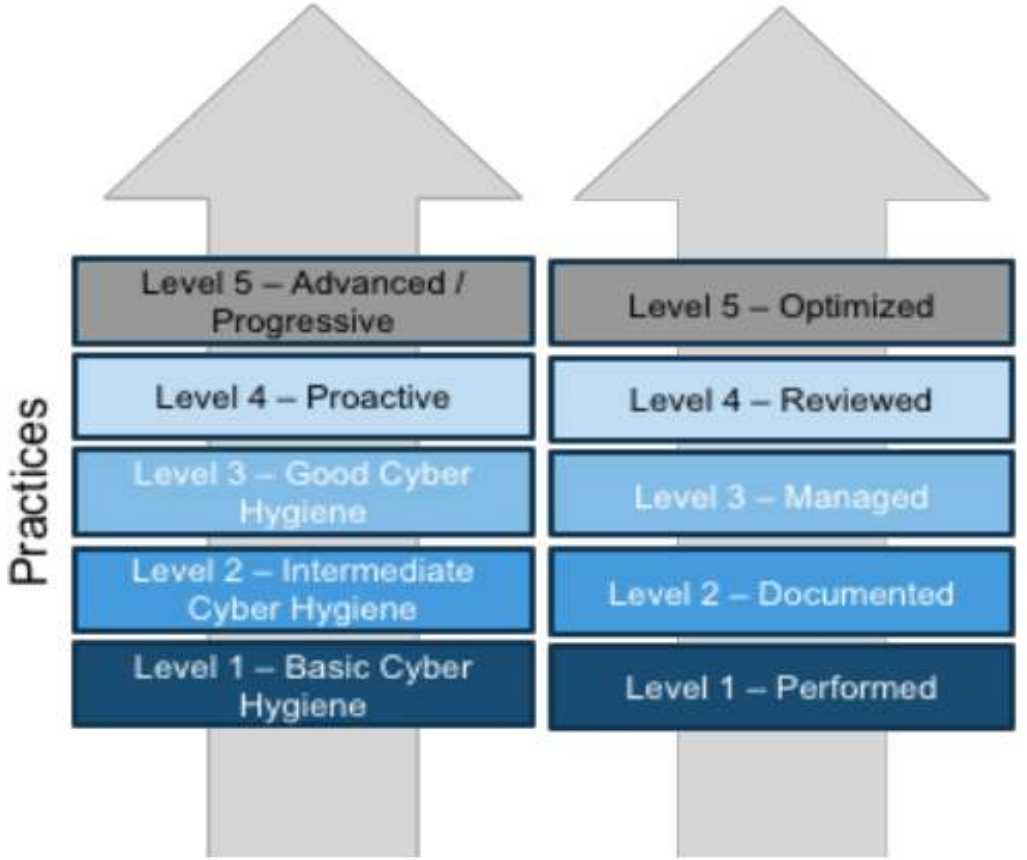


Figure 2. CMMC Level Descriptions

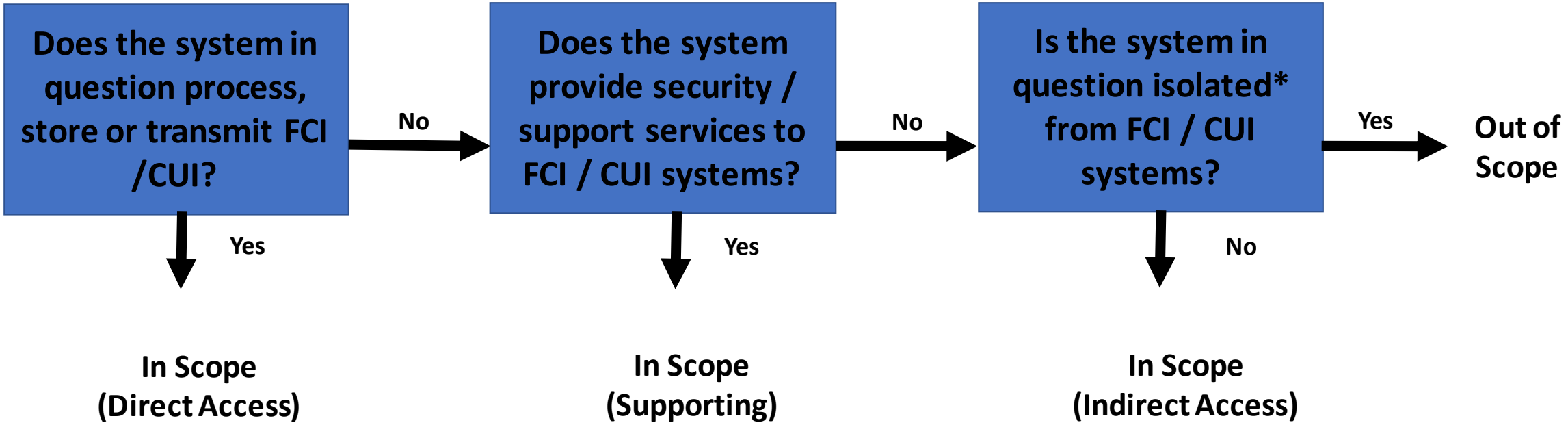
CMMC Domains

Access Control (AC)	Asset Management (AM)	Audit and Accountability (AA)	Awareness and Training (AT)	Configuration Management (CM)
Identification and Authentication (IDA)	Incident Response (IR)	Maintenance (MA)	Media Protection (MP)	Personnel Security (PS)
Physical Protection (PP)	Recovery (RE)	Risk Management (RM)	Security Assessment (SAS)	Situational Awareness (SA)
System and Communications Protections (SCP)	System and Information Integrity (SII)			

CMMC-AB & C3PAOs

Role	Responsibilities
Assessors	Individuals who have successfully completed the background, training, and examination requirements as outlined by the CMMC AB and to whom a license has been issued. Assessors are not employed by the CMMC AB and may or may not be employed by the C3PAO
C3PAO	An entity with which at least two Assessors are associated and to which a license has been issued to engage with OSCs to complete their associated CMMC assessment.
CMMC AB	The accreditation body that 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 CMMC program
Organization Seeking Certification (OSC)	The organization that is going through the CMMC assessment process to receive a level of certification for a given environment(s)

CMMC Scope Determination



Note - Isolated from means it is not on the same network segment, subnet, or VLAN as the FCI / CUI environment and cannot access or connect to systems in the FCI / CUI environment.

Roll Out: Crawl, Walk, Run

CMMC timeline

January 2020

- Official CMMC model released

Spring 2020

- CMMC-AB starting to release assessor and certification program details

July 2020

- CMMC requirements appeared in GSA STARS III and several other RFPs for the Intel Community

August 2020

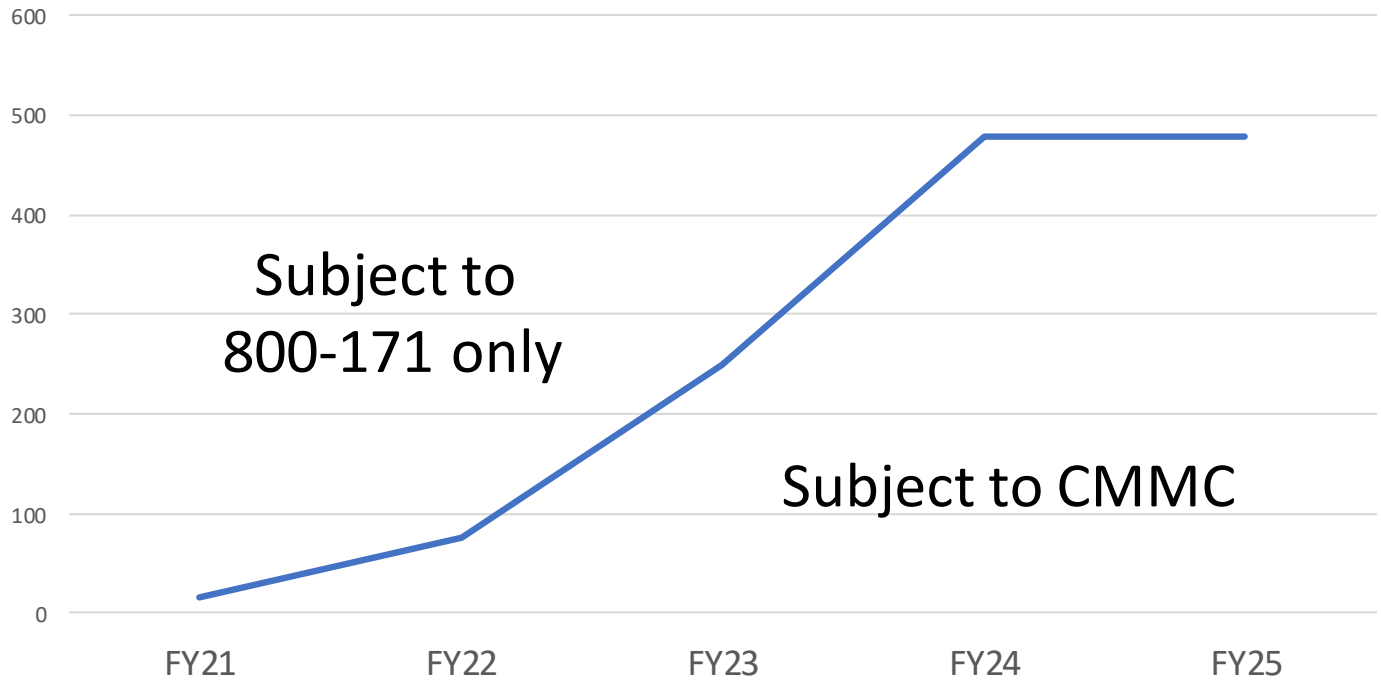
- CMMC provisional assessors
- Training begins for the assessors 8/31 target date

Fall / Winter 2020

- RFPs released with CMMC requirements
- CMMC assessments occurring Level 1 to start then level 3
- Rulemaking for public comment – effective 11/30
- Updates to the assessment method

Roll Out: Crawl, Walk, Run

- 100% CMMC requirement by FY 26 with the exception of commercial off the shelf procurement
- Years between FY 21 and FY 25 will put both obligations on contractors that handle CUI



Values based on DoD presentation on 1/28/2020 – subject to change

Certification & Disputes

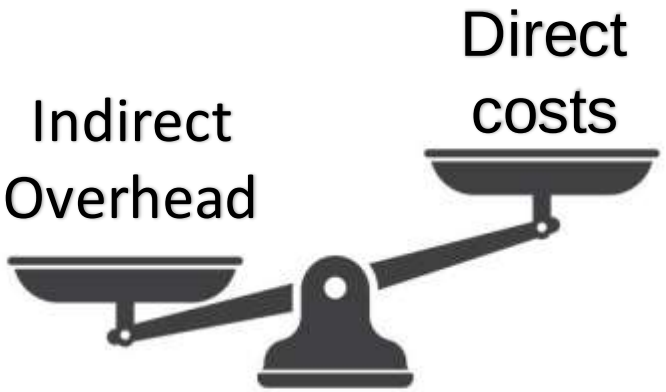
- Certifications and assessments current for three years
  - Agency may modify
- NIST SP 800-171 Assessments
  - Rebuttal process
- CMMC Certifications
  - Submit dispute adjudication request to CMMC-AB
  - May request additional assessment

How Much Will CMMC Cost?

DOD's Estimated Cost of Compliance for Small Entities

Level	Certification Costs (Est.)	Total Annual Assessment Costs (Est.)
1	$2,999.56	$1,000.00
2	$22,466.88	$28,050.00
3	$51,095.60	$60,009.00
4	$70,065.04	$371,786.00
5	$110,090.80	$482,874.00

Who Pays for Certification?



Direct Costs	Indirect Overhead Costs
• Cost of actual certification • Likely to be a few thousand dollars • In-practice cost of having someone from the accreditation body certify your business	• Cost of all of the planning, implementation, etc. it will take to become compliant • Likely several thousand dollars, if not more • Can be added to your indirect overhead overtime • Contractors likely to bear most of the burden

Questions?

Matt Gilbert
Matt.Gilbert@bakertilly.com
410.960.2716

Reggie Jones
rjones@foxrothschild.com
202.461.3111

Mike Baker
Michael.Baker@GDIT.com
703.268.7788