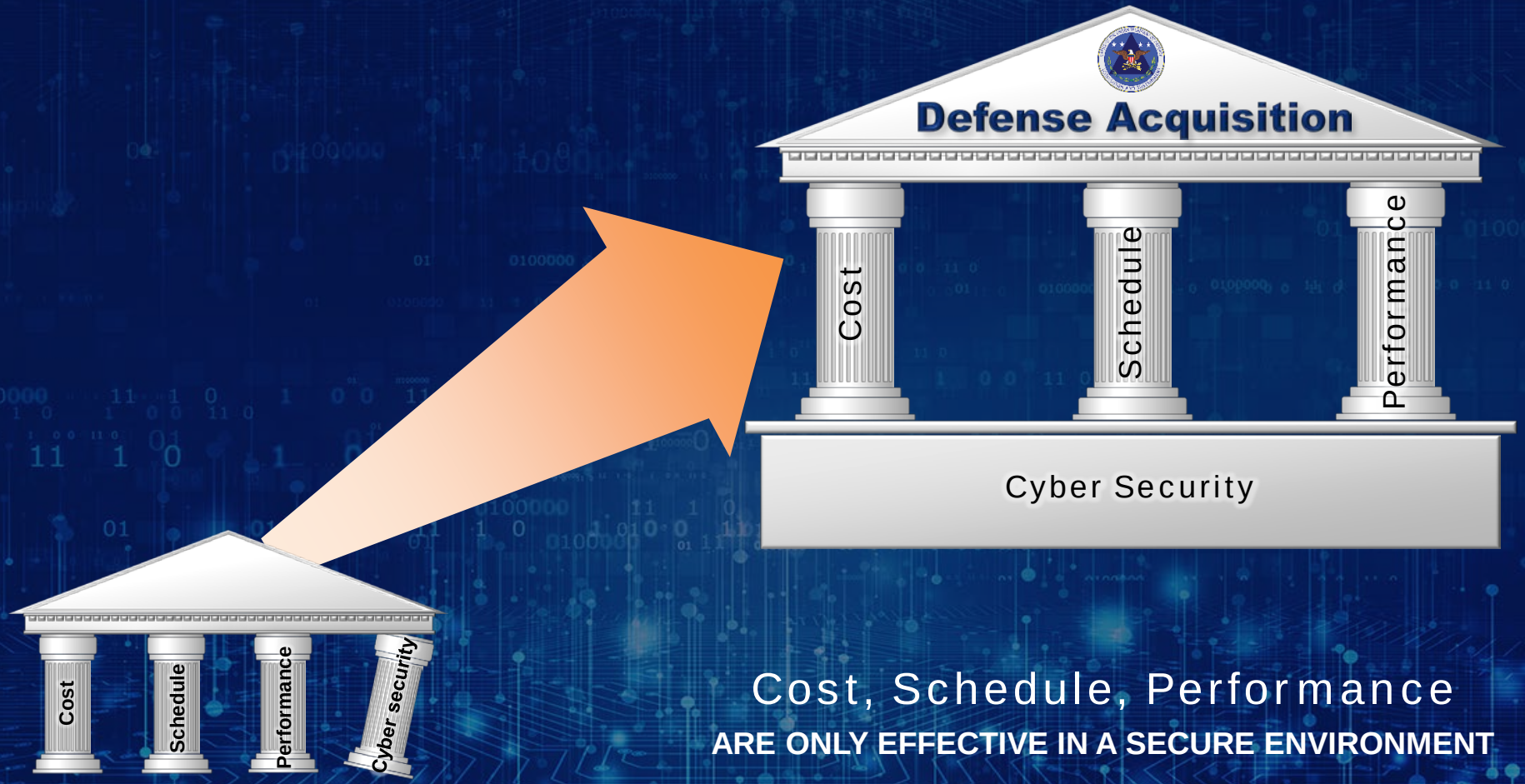
Securing the DoD Supply Chain

Cybersecurity Maturity Model Certification

Ms. Katie Arrington
Chief Information Security Officer
for Acquisition

As of 9 Dec 2019

Without a Secure Foundation
All Functions are at Risk



Cost, Schedule, Performance

ARE ONLY EFFECTIVE IN A SECURE ENVIRONMENT

Draft CMMC Model v0.7 Summary

- **CMMC will be a unified cybersecurity standard for DoD acquisitions**
  - Iterative draft versions are being developed, working towards v1.0 in Jan 2020

- **Draft CMMC Model 1 v0.7 encompasses:**
  - 17 capability domains; 43 capabilities
  - 173 practices across five CMMC levels to measure technical capabilities
  - 9 processes across five CMMC levels to measure process maturity

- **Draft CMMC Model v0.7 focuses on refining Levels 4 and 5**
  - Reduces Levels 4 and 5 by 52% from v0.6 (i.e. removes 46 practices)
  - Provides new draft discussion and clarification content for Level 2, Level 3, and maturity processes

Draft CMMC Model v0.7 Practices and Processes per Level

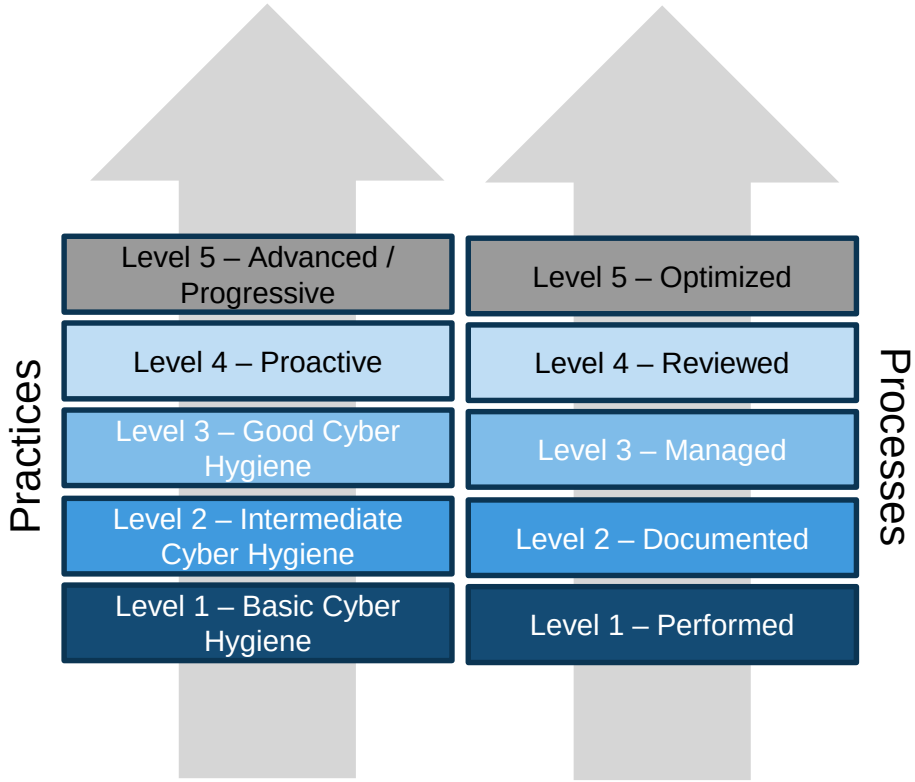
CMMC Level	Practices	Processes
Level 1	17	
Level 2	55	3
Level 3	59	2
Level 4	26	2
Level 5	16	2

CMMC Model Structure

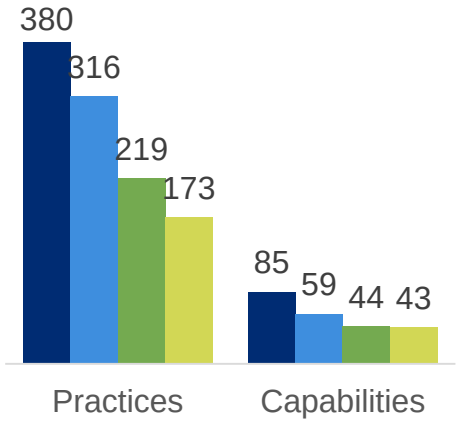
17 Capability Domains (v0.7)

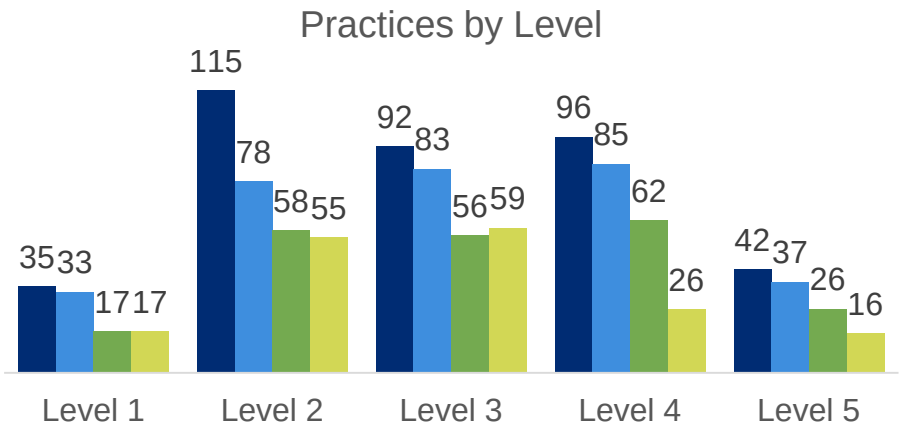
Access Control (AC)	Incident Response (IR)	Risk Management (RM)
Asset Management (AM)	Maintenance (MA)	Security Assessment (SAS)
Awareness and Training (AT)	Media Protection (MP)	Situational Awareness (SA)
Audit and Accountability (AA)	Personnel Security (PS)	System and Communications Protection (SCP)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

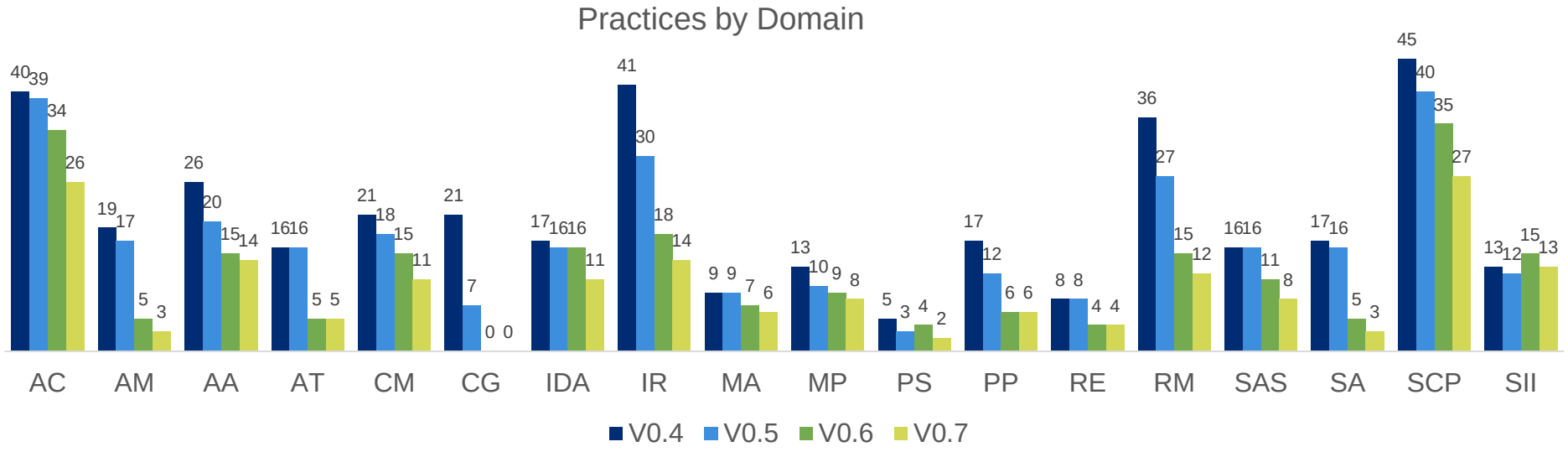
Capabilities are assessed for Practice and Process Maturity



Recent Changes to Draft CMMC Model
v0.4 to v0.5 to v0.6 to v0.7







Draft CMMC Model v0.7 Source Counts

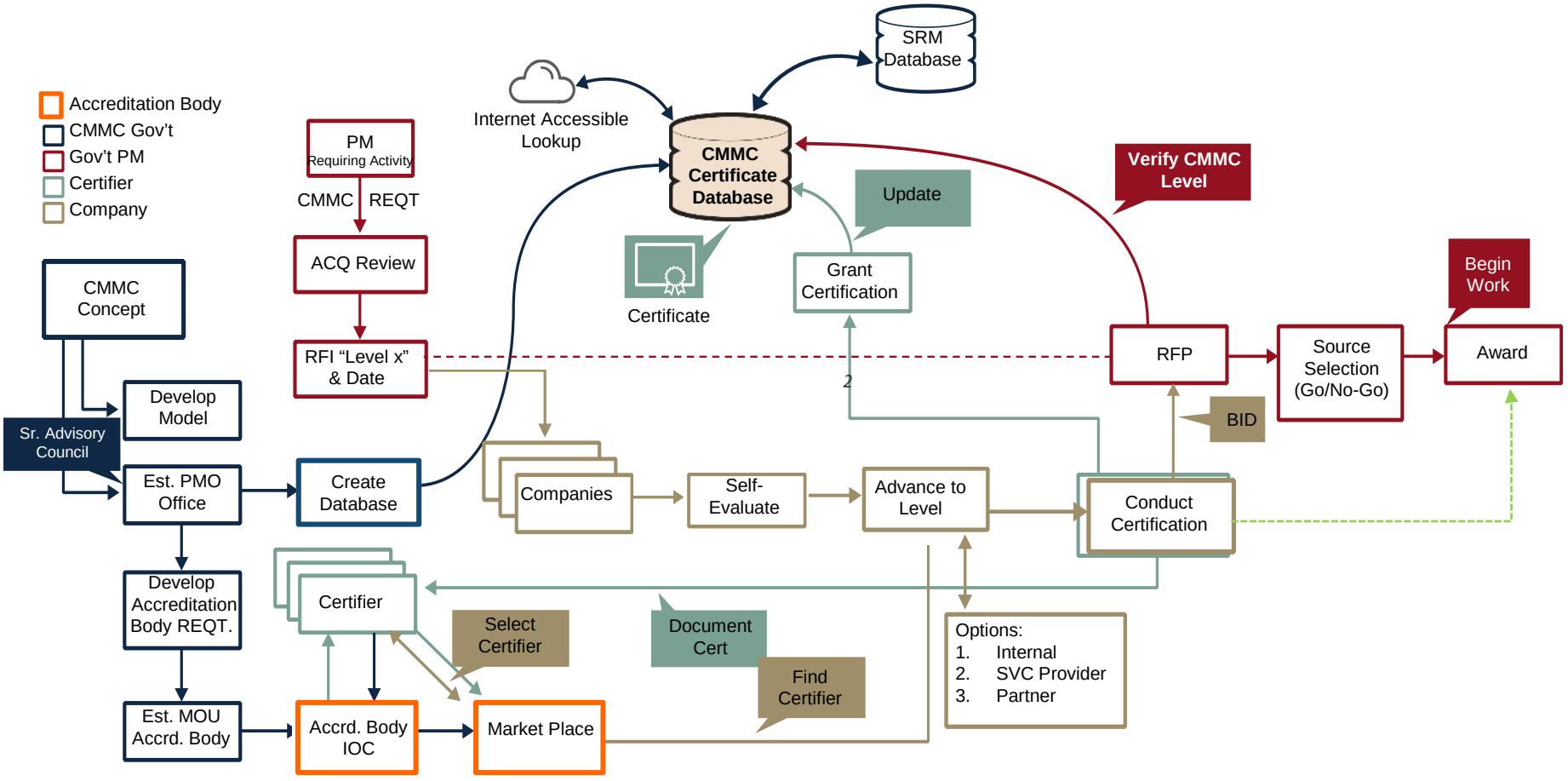
- **Draft CMMC Model leverages multiple sources and references**
  - CMMC Level 1 only includes practices from FAR Clause 52.204-21
  - CMMC Levels 4 and 5 do not include QTY 15 practices from Draft NIST SP 800-171B because of cost or implementation challenges

Draft CMMC Model v0.7: Number of Practices per Source

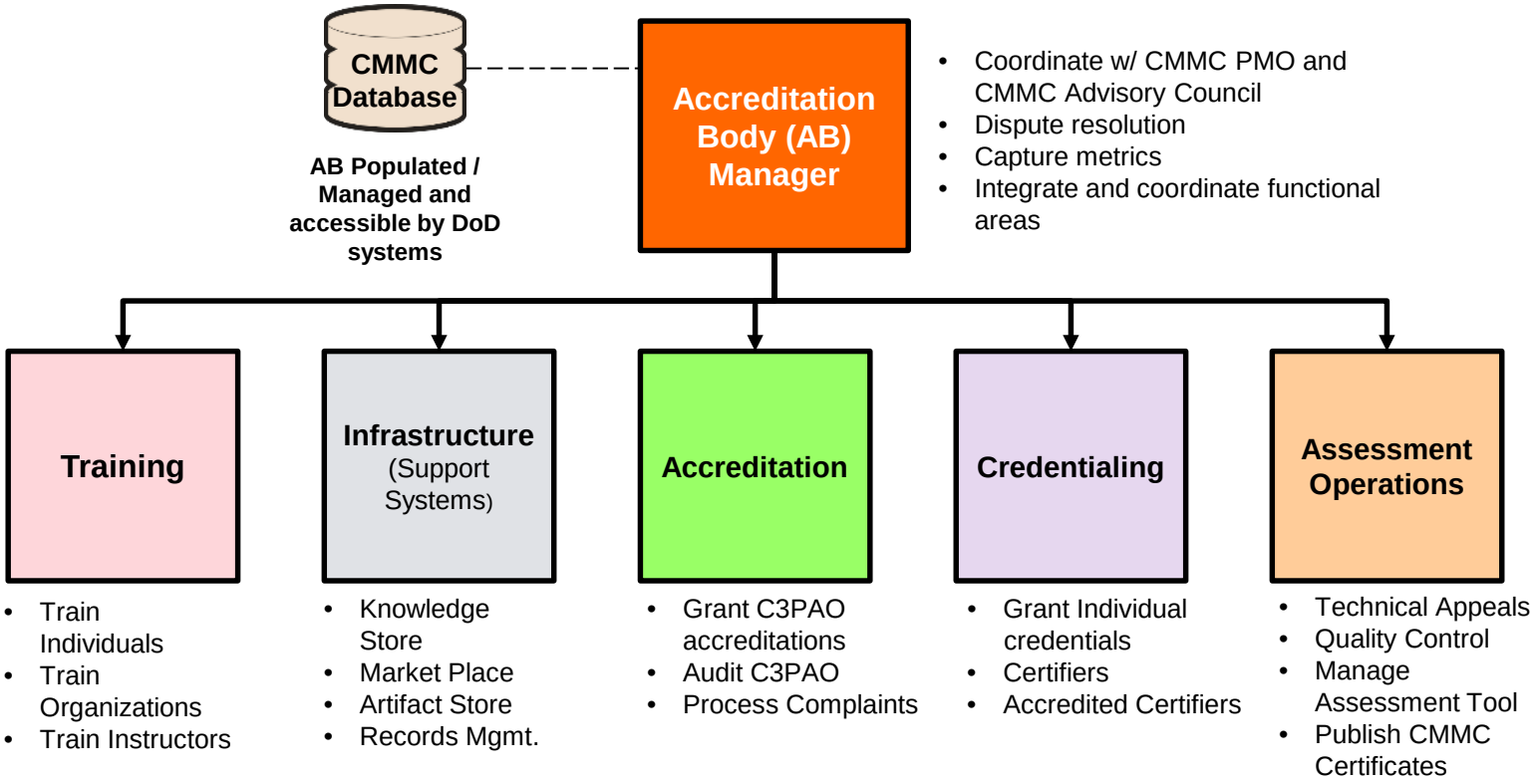
CMMC Level	Total Number Practices per CMMC Level	Source			
		48 CFR 52.204-21	NIST SP 800-171r1	Draft NIST SP 800-171B	Other
Level 1	17	17 *	17	-	-
Level 2	55	-	48	-	7
Level 3	59	-	45	-	14
Level 4	26	-	-	13	13
Level 5	16	-	-	5	11
Excluded	-	-	-	15	-

* Note: QTY 15 safeguarding requirements from FAR clause 52.204-21 correspond to QTY 17 security requirements from NIST SP 800-171r1, and in turn, QTY 17 practices in CMMC

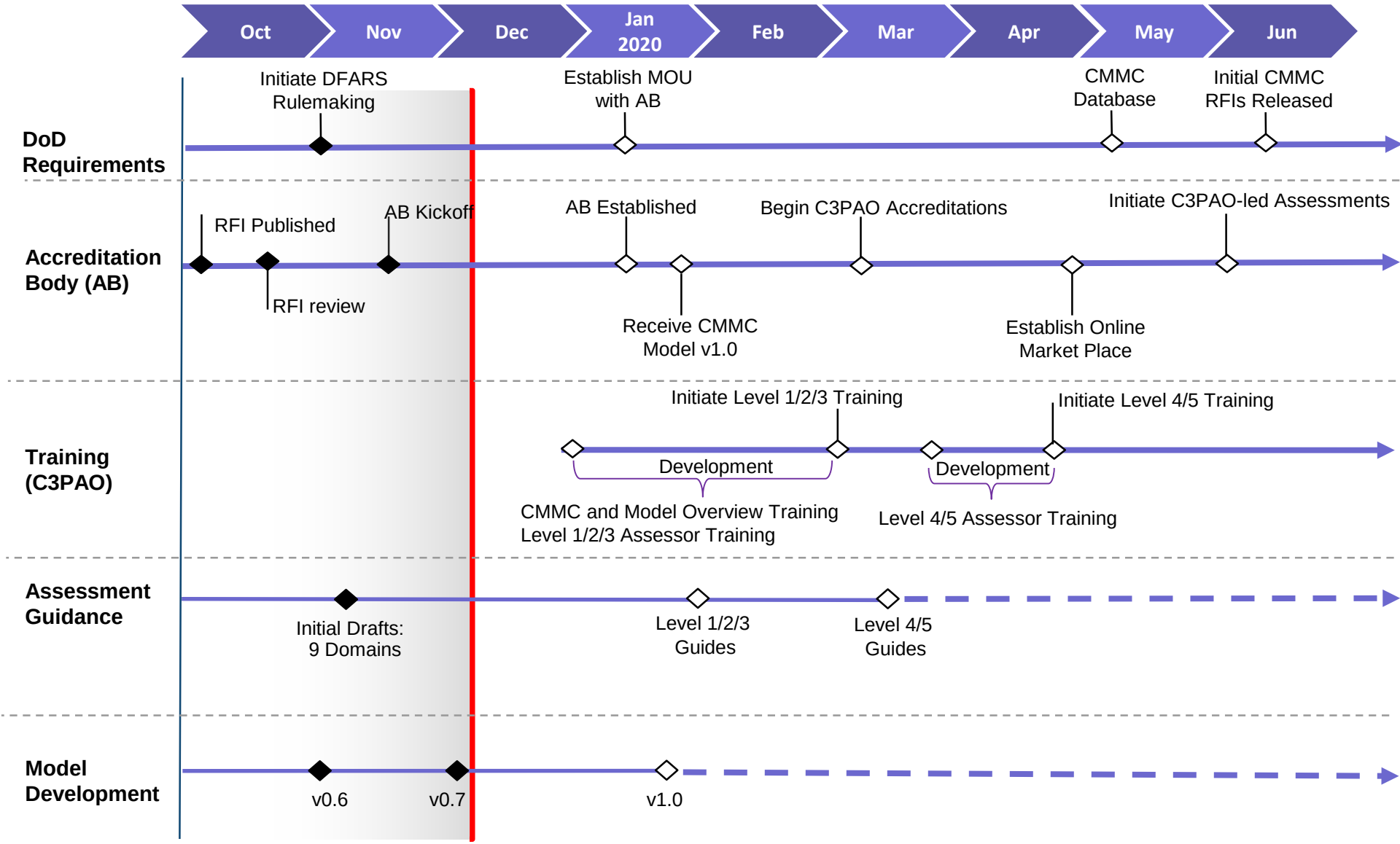
Notional CMMC Implementation Flow



Notional CMMC Accreditation Body Activities



Draft CMMC Development Schedule



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