A DISCUSSION WITH THE CMMC-AB AND DOD

JANUARY TOWN HALL

- Host Opening and Rules of Engagement (Wayne Boline)
- Welcome (Karlton Johnson, Chairman)
- Message from Katie Arrington, DOD CISO
- DOD CMMC Pilot Overview (Diane Knight, DOD)
- Training and Credentialing (Jeff Dalton and Ben Tchoubineh)
- ISO 17011 Accreditation Body Update (Jeff Dalton)
- Q&A (Wayne Boline)
- Wrap Up and Thank you (Karlton Johnson)

TRAINING AND CREDENTIALING **UPDATE**

BEN TCHOUBINEH (TRAINING) | JEFF DALTON (CREDENTIALING)

TRAINING AND CREDENTIALING TOPICS

- Current Numbers of Credentialed Professionals and Organizations
- Licensed Partner Publishers (LPPs)
- Q/A: ProCert
- Exams: Scantron
- Licensed Training Providers – Applications now open
- Provisional Instructors – Coming Soon!
- Rollout Timeline
- AB and CAICO
- ISO 17020 Timeline

CURRENT STATUS OF CREDENTIALS

Credential	December: Total	December : Pending	December: Approved	January Total	January Pending	January Approved
RP	980	511	469	1439	378	1060
RPO	297	46	251	382	43	339
C3PAO	369	349	20	408	355	53
LPP	16	0	16	18	2	16
LTP	0	0	0	22	10	12
Provisional Assessors	100	0	100	100	0	100

CERTIFICATION EXAMS

- Exams being developed by CMMC-AB and Scantron Corporation
  - https://www.scantron.com/
- Currently being developed
  - Certified Professional
  - Certified Assessor Level 1
  - Certified Assessor Level 3
- Will begin development in 2021
  - Certified Assessor Level 5 - Q3 or later
  - Certified Instructor - Q2

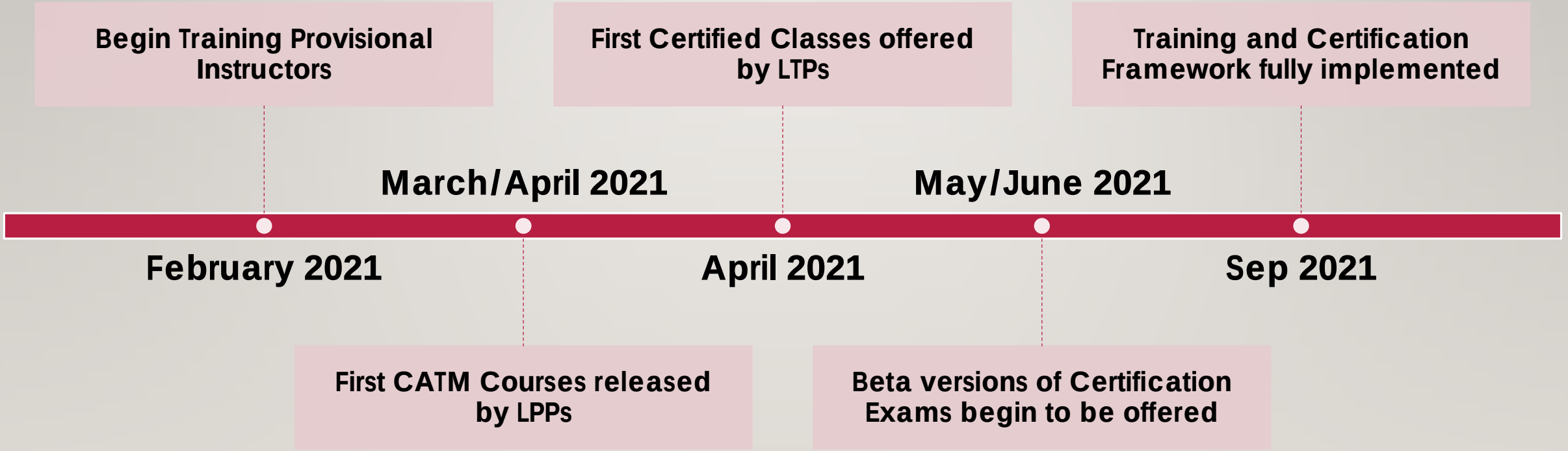
LICENSED TRAINING PROVIDERS

- LTPs will begin offering Certified Classes in Q2 of 2021
- Certified Classes will prepare students for taking the certification exams
- Definition of a Certified Class
  - Taught at an LTP
  - Taught by a CMMC-AB Provisional or Certified Instructor
  - Uses CMMC-AB Approved Training Material (CATM) developed by an LPP
- LTP Applications are now open!
  - https://www.cmmcab.org/ltp-lp

PROVISIONAL INSTRUCTORS

- CMMC-AB will be training Provisional Instructors beginning in February of 2021 and monthly thereafter
- They are highly qualified Assessors who also have significant training experience.
- The CMMC-AB will train instructors on an on-going basis
- If you are interested in being an instructor, please send an email to cmmcsupport@cmmcab.org, mention you are applying to be an instructor, and attach your resume

PROGRAM TIMELINE



CERTIFIED PROFESSIONAL/CERTIFIED ASSESSOR APPLICANTS (CP/CA)

- Many of you have pre-purchased vouchers for the exams at a discounted price.
- You should take training with an LTP once it becomes available in the Spring
  - LTPs will be listed in our Marketplace
- Before the exams become available, we will send you your exam vouchers to be used when scheduling your exam
- Thank you for your patience as we've worked to develop this Training and Certification Framework

…. AND COMING SOON

- **Licensed Software Provider (LSP)**

A Licensed Software Provider will leverage specifications and requirements provided by the CMMC AB to build software solutions that assist Certified Assessors, Certified Professionals, C3PAOs, RPs, and RPOs in delivering consistent, high-quality CMMC Services to their clients.

ISO 17011 RELEASE PLAN

ACCREDITATION BODY (ISO/IEC 17011) RELEASE PLAN

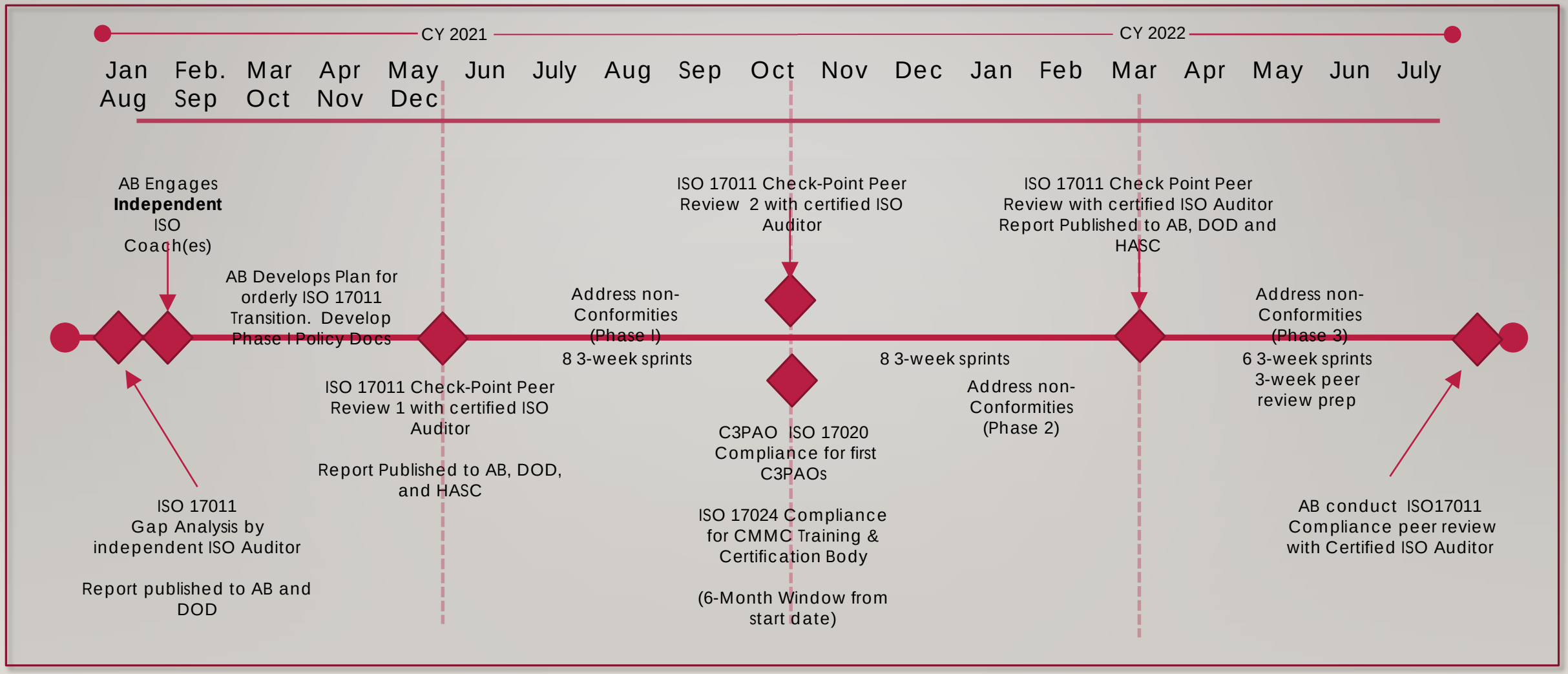
15-DEC 2020. V1.4

COPYRIGHT © 2020 CMMC AB

WHY ARE WE ADOPTING ISO/IEC 17011:2017?

- We are NOT currently an ISO Accreditation Body! But we plan to become one within 24 months.
- ISO/IEC 17011: 2017 is the ISO Standard for Accreditation Bodies
- Once accredited themselves, the CMMC AB will accredit C3PAOs (“inspection bodies”) in both DOD requirements and ISO/IEC 17020 (ISO standard for Certification Bodies). Until then we will accredit C3PAOs to DOD Requirements.
- There will be two separate and distinct lines of business:
  - AB: Responsible for C3PAO vetting, licensing, and Accreditation to DOD Requirements and ISO 17020 (within 24 months), Informal training, RPOs, and registered practitioners
  - CAICO: Responsible for training and testing Certified Assessors and Instructors.
- C3PAOs will need be formally accredited in ISO/IEC 17020 by the CMMC AB within 27 months
- Formally adopting ISO/IEC 17011 and ISO/IEC 17020 will strengthen the independence of the overall ecosystem

CMMC ACCREDITATION BODY ISO/IEC 17011 RELEASE PLAN



Copyright © 2020 CMMC AB

Cybersecurity Maturity Model Certification (CMMC)

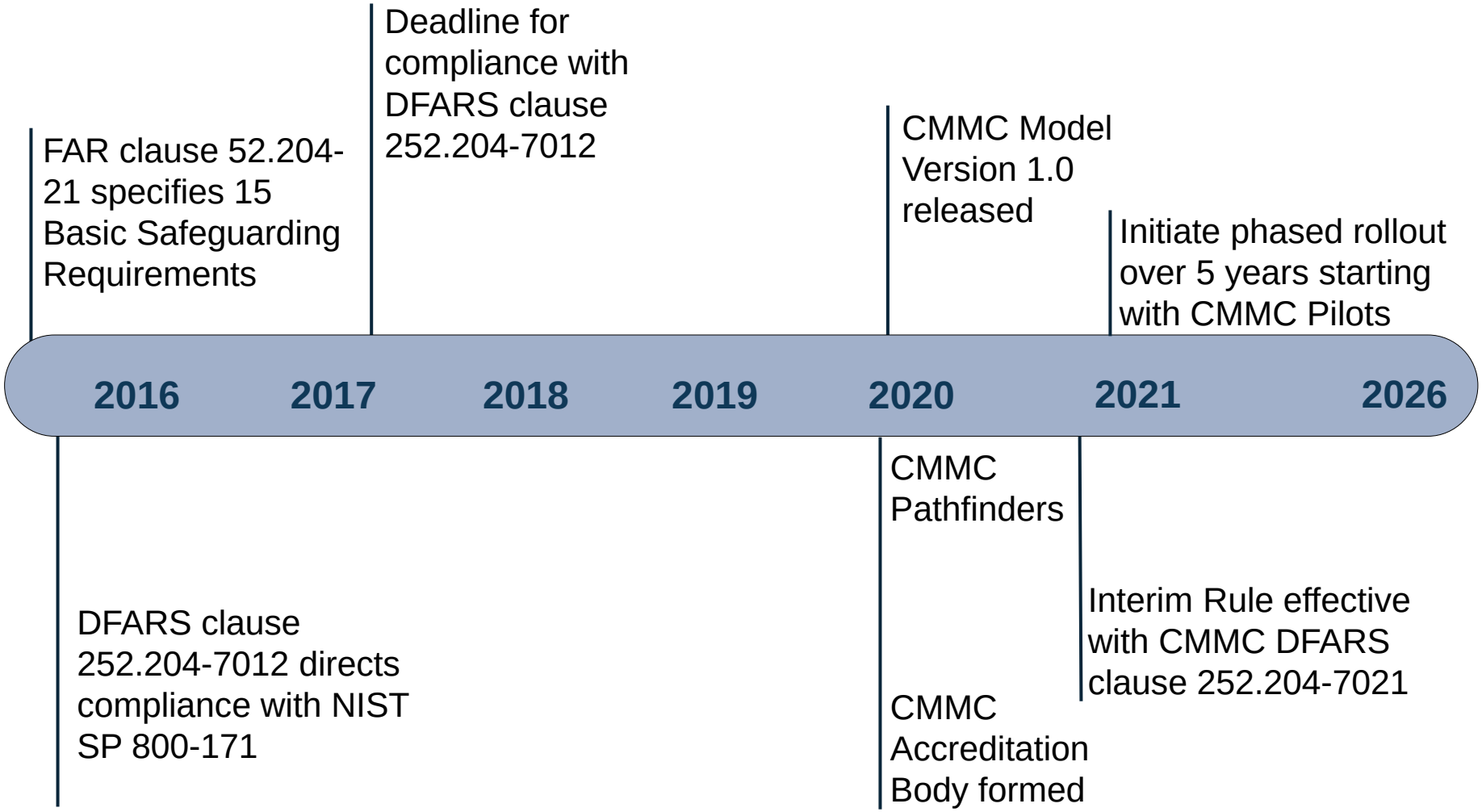
Pilots

CMMC-AB Town Hall Briefing

26 Jan 2021

DISTRIBUTION A. Approved for public release

CMMC Regulatory and Implementation Timeline



DFARS Interim Rule for CMMC in effect; DoD initiating CMMC Pilot Kick Off meetings

DISTRIBUTION A. Approved for public release

DFARS Clause 252.204-7012: The Foundation for CMMC

CMMC complements DFARS clause 252.204-7012: Safeguarding Covered Defense Information [Controlled Unclassified Information (CUI)] and Cyber Incident Reporting

DFARS clause 252.204-7012 requires contractors/subcontractors to:

- Safeguard CUI by implementing cybersecurity requirements in NIST SP 800-171
  - Document in a System Security Plans (SSP) how requirements are implemented
  - Maintain a Plan of Action and Milestones (POAM) for unimplemented requirements
  - Obtain approval from Contracting Officers for any variances or "alternate but equally effective controls" implemented to meet the requirements
- Report cyber incidents (to include lost or stolen devices)*
- Isolate and submit malicious software for analysis*
- Facilitate damage assessments
- Flow down the clause to subcontractors if CUI is conveyed (not applicable to COTS)

Contractors and subcontractors self-attest to compliance

DFARS Case 2019-D041
Assessing Contractor Implementation of Cybersecurity Requirements

The *interim rule* took effect 30 Nov 2020 / DoD implementing a 5-year phased roll-out

DFARS Provision 252.204-7019 Notice of NIST SP 800-171 DoD Assessment Requirements	DFARS Clause 252.204-7020 NIST SP 800-171 DoD Assessment Requirements	DFARS Clause 252.204-7021 Cybersecurity Maturity Model Certification Requirements
Solicitation Notice: Basic Assessment Score required in SPRS for contract award • A NIST SP 800-171 DoD Assessment (Basic, Medium, High) summary level score must be posted into DoD's Suppliers Risk Performance System (SPRS) for the applicable CAGE code and Systems Security Plan • The summary level score must remain current (not older than 3 years unless a lesser time is specified) throughout the life of the contract, task or delivery order	**Basic Assessment Score required in SPRS to be considered for contract award** • Applicable to companies subject to DFARS clause 252.204-7012 • Post award, if DoD deems a Medium or High assessment is necessary due to program sensitivity, provide DoD access to facilities, systems and personnel • Include clause in all subcontracts or other contractual instruments including subcontracts for commercial items • Confirm subcontractor compliance with SPRS reporting if receiving CUI	**Cybersecurity Maturity Model Certification Required by contract award effective 1 Oct 2025** • Until 1 Oct 2025, OUSD(A&S) must approve clause in new acquisitions • Contractor certification level must be maintained for contract duration • Clause must be flowed down; primes must ensure subs are certified at required CMMC level prior to awarding subcontract

- Interim rule clauses are applicable to contracts, task orders and delivery orders
- Not applicable to micro-purchases or solicitations exclusively for the purchase of COTS products

CMMC assessments and certifications required for the applicable enterprise network or network segment where FCI or CUI will be processed, stored, or transmitted in performance of the contract

DISTRIBUTION A. Approved for public release

CMMC Risk Reduction: Pathfinders

- **OUSD(A&S) funded risk reduction activities to inform CMMC implementation**

Missile Defense Agency (MDA) Pathfinder (Apr 2020 – present)

Activity: Mock Assessments
Mock Assessors trained by CMMC-AB
Conducted mock assessments:
- CMMC Level 3 'delta' of prime contractor
- CMMC Level 3 and Level 1 of two subcontractors

Objective
Validate drafted CMMC Assessment Guides and gather lessons learned

Outcome
Identified Lessons Learned to improve draft documentation and assessment processes

Activity: Acquisition Tabletop
Conducted a sequence of evolving TTXs that focus on the DoD's acquisition processes from RFI to post contract award.

Objective
Identify and reduce risks associated with implementing CMMC in future acquisitions

Outcome
Developed exemplar RFI, RFP and flow down language to support contract actions

Defense Logistics Agency (DLA) Pathfinder (Sep 2020 – present)

Planned Activity: Mock Assessments
Conduct two mock assessments:
- CMMC Level 3 of two prime contractors
- Assessed by authorized C3PAOs

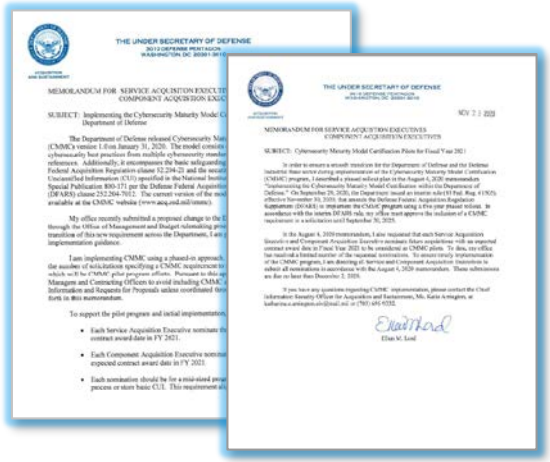
Objective
Identify and reduce risks associated with newly authorized C3PAOs

Mock Assessments are non-attributional, non-punitive and do not result in a certification

DISTRIBUTION A. Approved for public release

CMMC Implementation: Pilots (1 of 2)

- The CMMC Pilot Program supports FY 2020 NDAA, Section 1648 guidance
- USD(A&S) issued memoranda on 4 Aug and 23 Nov 2020 requesting Pilot candidates from the military services and component agencies
- Criteria for candidate programs:
  - FY2021 expected contract award
  - No acquisitions solely for the provision of COTS products or for operational technology systems supporting industrial or manufacturing operations
  - Midsized programs that process, store, or transmit basic CUI



- The initial (7) CMMC Pilot candidates were announced in a DoD press release on 15 Dec 2020
- Candidate acquisitions have now been identified by the Army, Navy, Air Force, Missile Defense Agency, and Defense Logistics Agency
- OUSD(A&S) is exploring additional opportunities to pursue pilots outside of the DoD

OCISO(A&S) plans to begin scheduling kick-off meetings in January 2021.

DISTRIBUTION A. Approved for public release

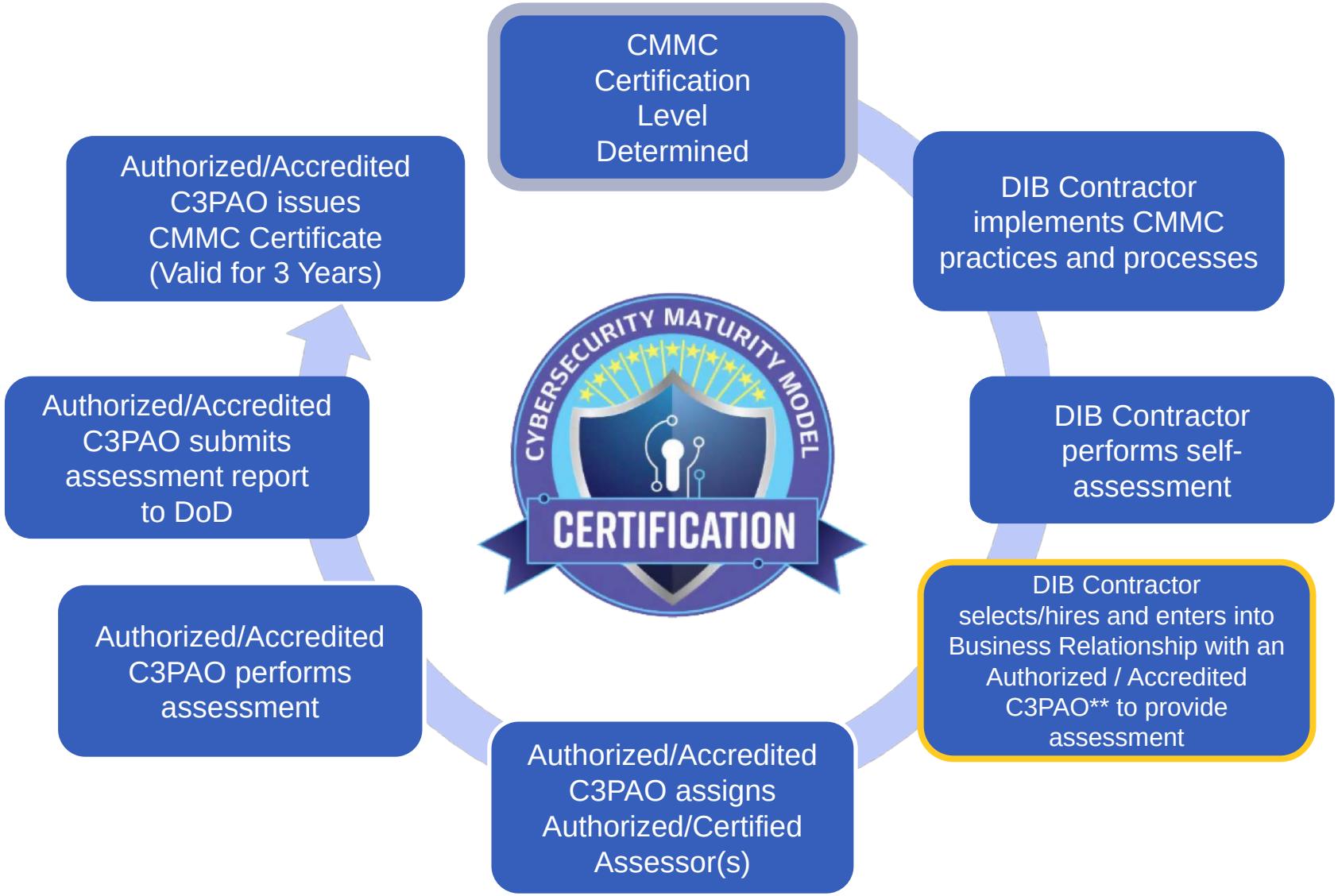
CMMC Implementation: Pilots (2 of 2)

- **The following candidate programs have been identified by Services and Agencies:**

Service or Agency	Program
Army	Foreign Military Sales (FMS) Field Service Representative Support
	Woman, Infant, & Children (WIC) Overseas Program for DHA-J10-TRICARE
	Main Operating Base-Installation Service Nodes (MOB-ISN)
Navy	Integrated Common Processor
	F/A-18E/F Full Mod of SBAR & Shut off Valve
	DDG-51 Lead Yard Services / Follow Yard Services
Air Force	Mobility Air Force Tactical Data Links
	Consolidated Broadband Global Network Area Network Follow-On
	Azure Cloud Solution
Missile Defense Agency	Technical Advisory and Assistance Contract

- **DoD plans to implement CMMC using a phased rollout over five years commencing with a target of up to 15 new acquisitions in FY21:**
  - The rollout ramps up over 5 years with CMMC in up to 475 new prime contracts by FY25
  - Until 1 Oct 2025, OUSD(A&S)/OCISO(A&S) CMMC Office must approve the use of the clause for new acquisitions

DIB Contractor / C3PAO Business Relationship
Basic CMMC Process



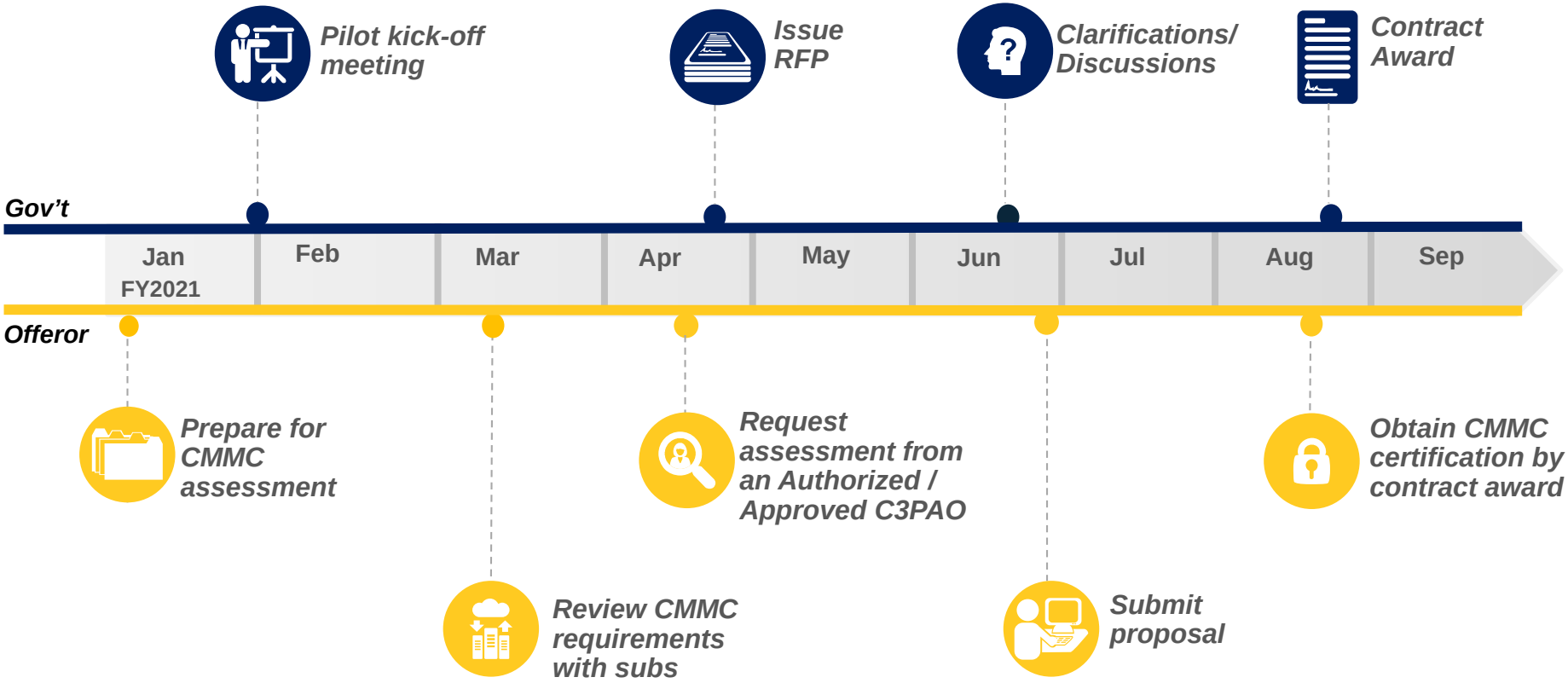
DISTRIBUTION A. Approved for public release

*DIB Contractor is AKA: "OSC – Organization Seeking Certification
**C3PAO – CMMC Third Party Assessment Organization

Notional CMMC Pilot Timeline

KEY PILOT MILESTONES

Below is a notional CMMC Pilot timeline outlining key milestones for the government and offerors:



Pilot acquisitions will require obtaining CMMC Certification by contract award

DISTRIBUTION A. Approved for public release

Pilot Key Takeaways

Until 1 Oct 2025, CMMC requirements will only be included in new acquisitions with the approval of OUSD(A&S) / OCISO(A&S)

CMMC Pilot programs will include applicable CMMC requirements in RFPs

- OUSD(A&S) is not funding CMMC Pilots
- CMMC certification must be met by contract award
- CMMC certification is required of the enterprise network or particular segment where FCI or CUI is processed, stored, or transmitted in performance of the particular contract
- CMMC certification must be maintained for the duration of the contract; recertification may be necessary depending on expiration date of the CMMC certification versus the contract end date

CMMC Pilot contractors will be required to achieve CMMC Certification

- DIB Contractor enters into Business Relationship with an authorized / approved C3PAO
- CMMC certification is achieved by passing a CMMC assessment conducted by C3PAO
- All CMMC practices and processes must be implemented at the required CMMC Level
- CMMC does not allow POAMs
- If there are assessment findings, the contractor will need to remediate to achieve CMMC certification
- CMMC Certification is good for three years

OUSD(A&S) will provide guidance and support during Pilot roll-outs

CMMC References

Source	Significance
DFARS clause 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting, published in Federal Register and effective on 26 August 2015 as interim rule Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013-D018)	*Builds upon the requirements in DFARS clause 252.204-7012, namely the adherence to the assessment requirements in NIST SP 800-171*
DFARS Case 2019-D041: Assessing Contractor Implementation of Cybersecurity Requirements, published in Federal Register on 29 September 2020	*Provides extensive explanations of the rationale behind the new regulatory requirements and how they will be incorporated into new DoD acquisitions containing CUI beginning 1 Oct 2025, among other things*
Press Release Announcing CMMC Pilots for Fiscal Year 2021, published by DoD on 15 December 2020	*The first seven candidate pilots were submitted to OCISO(A&S) by the U.S. Navy, U.S. Air Force, and the Missile Defense Agency*
DoD CMMC website	*Contains links to a variety of resources, such as the CMMC model, CMMC assessment guides (particularly helpful for offerors), and FAQs*
DODI 5000.90 – Cybersecurity for Acquisition Decision Authorities and Program Managers	*Establishes policy, assigns responsibilities, and prescribes procedures for the management of cybersecurity risk by program decision authorities and program managers (PMs) in the DoD acquisition processes*
DoD CUI Program website	*Explains the source and importance of CUI and posts related policies, training, marking aids, as well as the CUI registry and new developments*

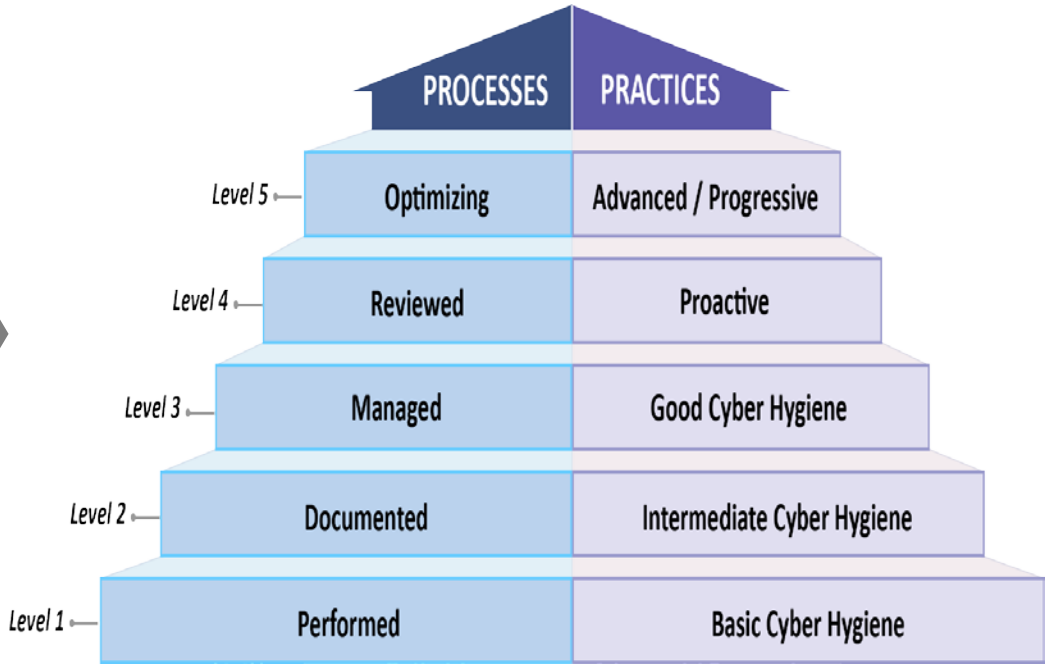
Backups

CMMC Model Structure

17 Capability Domains (v1.0)

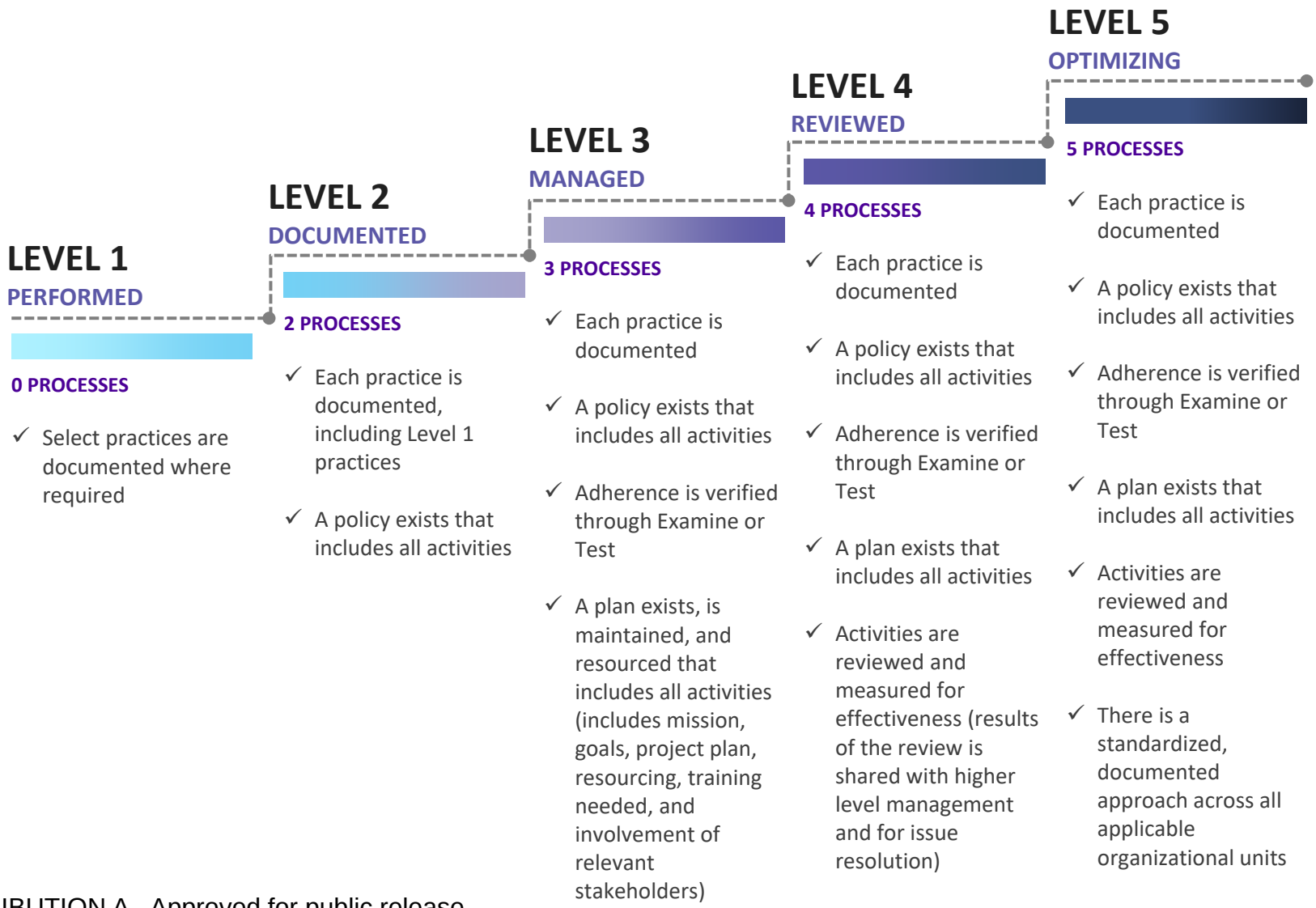
Access Control (AC)	Incident Response (IR)	Risk Management (RM)
Asset Management (AM)	Maintenance (MA)	Security Assessment (SAS)
Awareness and Training (AT)	Media Protection (MP)	Situational Awareness (SA)
Audit and Accountability (AA)	Personnel Security (PS)	System and Communications Protection (SCP)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

CMMC Model with 5 levels with each level consisting of processes and practices



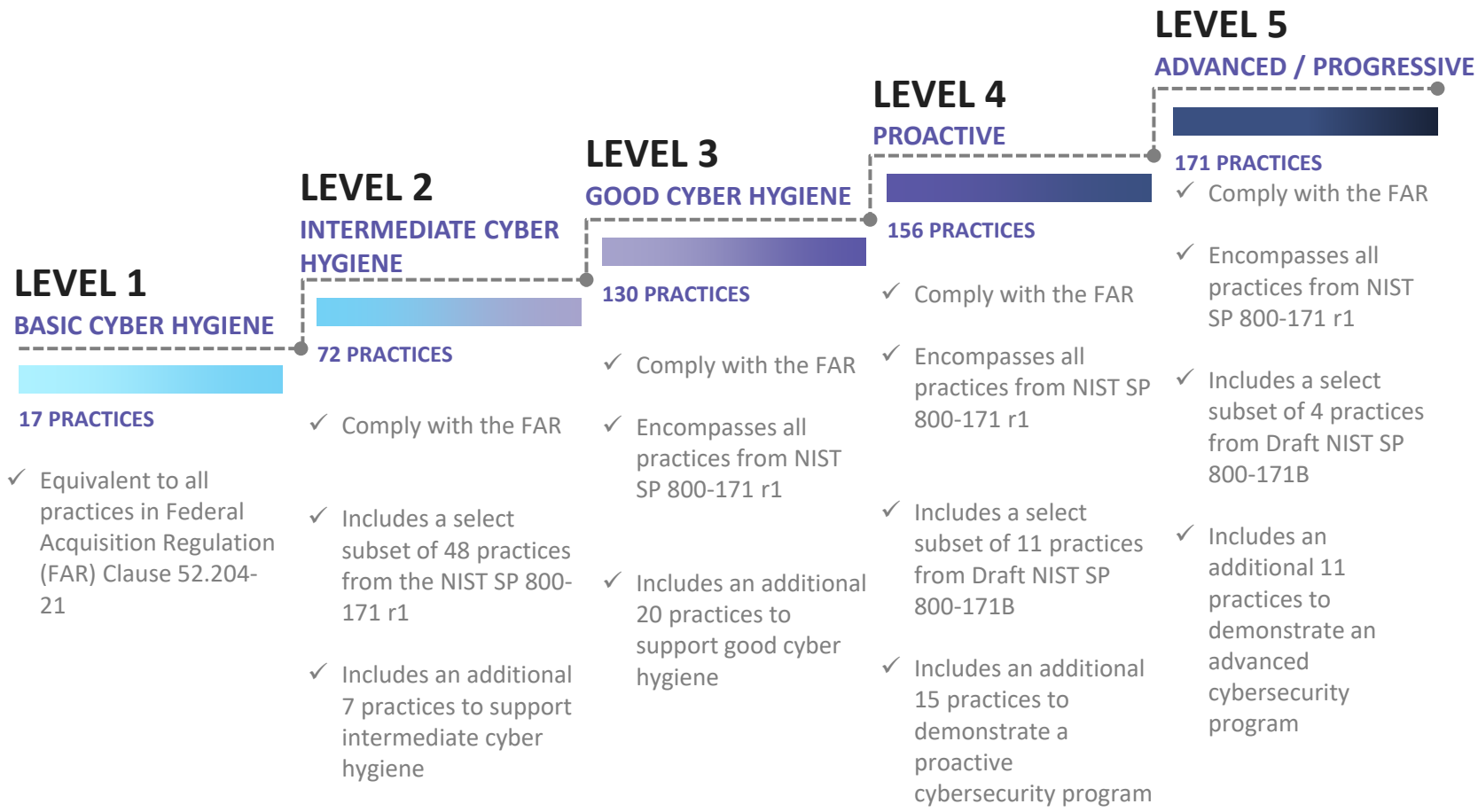
DISTRIBUTION A. Approved for public release

CMMC Maturity Process Progression



DISTRIBUTION A. Approved for public release

CMMC Practice Progression



DISTRIBUTION A. Approved for public release