|TSM|

DRAFT

Industry Courtesy Copy

Department of Defense
Cybersecurity Maturity Model Certification
CMMC v. 1

May 19, 2020

OUTLINE

INTRO

The US Department of Defense (DoD) is going through a game-changing reset with respect to the cybersecurity policy and regulations applicable to the contractor and subcontractor ecosystem.

Until as recent as 2019, conventional thought was to adopt a graduated framework of security requirements depending on the nature of the contract and the size and role of a given contractor / subcontractor. Key to this prior approach was relying on prime contractors and sub contractors to self-certify.

In January 2020, industry news broke that the DoD effectively changed its view and mandated that contracts after October 2020 will incorporate formal third-party audits and verification for the entire DoD supply chain, effectively ending the self-certification approach to cybersecurity.

The following slides are based on independent research and presentations and information provided by Katie Arrington, Special Assistant to the Assistant Secretary of Defense for Acquisition ASD(A) for Cyber, and John Weiler of the CMMC Accreditation Body Board and Derek White of the Beryllium Infosec Collaborative on 11 and 4 May 2020 respectively.

CMMC

Cybersecurity Maturity Model Certification

What is it?

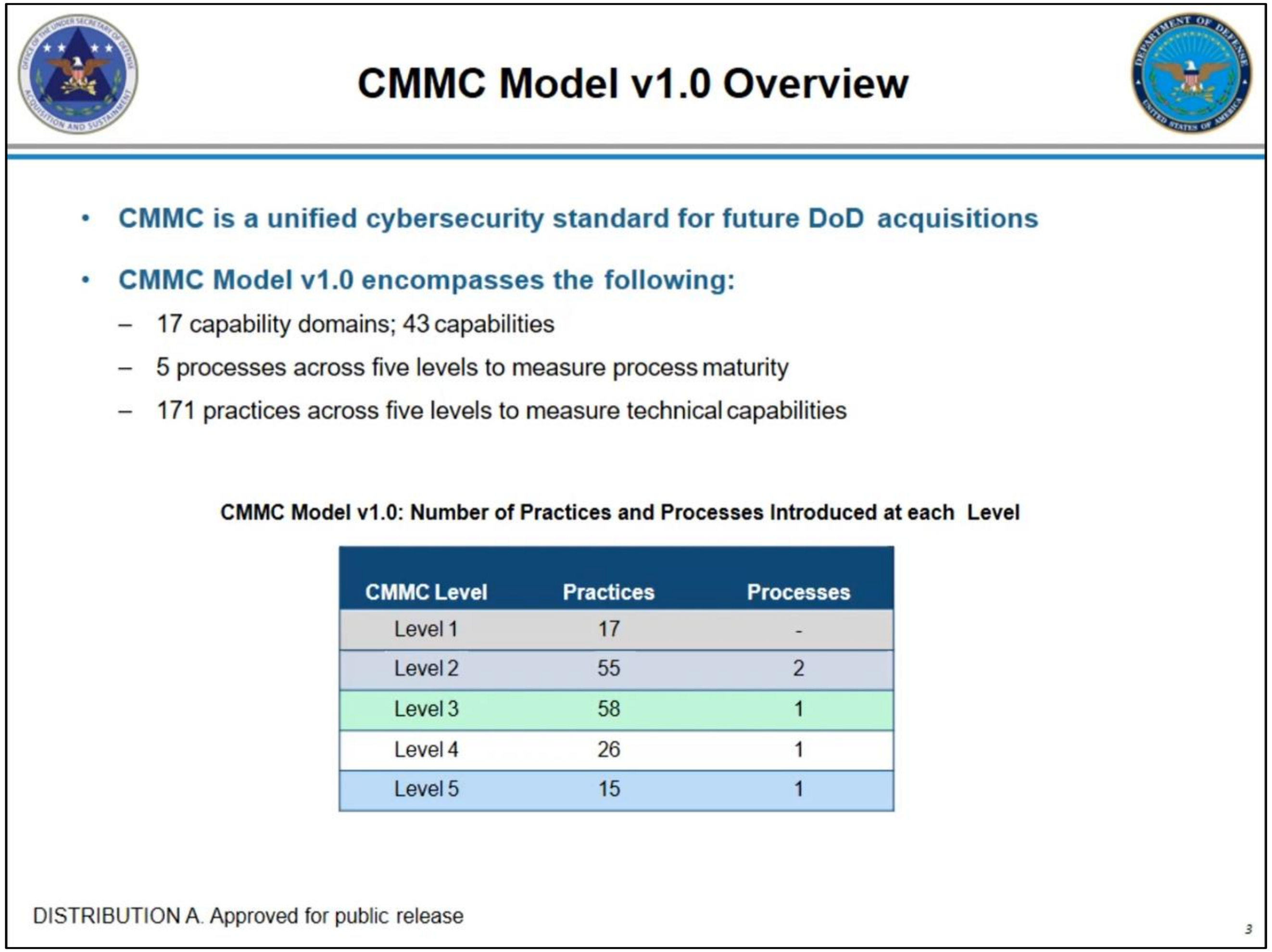
- The CMMC measures cybersecurity maturity, based on the type and sensitivity of information needing to be protected.
- Certification means third-party audit / verification.

Why?

- Each year, more than $600B of intellectual property is stolen from American firms.
- Major national security breaches in recent years, e.g. wholesale theft by Chinese hackers of technical design and specs of key defense aircraft from DoD subcontractors:
  - F-35 Joint Strike Fighter
  - F-22 Raptor
  - MV 22 Osprey

CMMC

Cybersecurity Maturity Model Certification



CMMC Model v1.0 Overview

- CMMC is a unified cybersecurity standard for future DoD acquisitions
- CMMC Model v1.0 encompasses the following:
  - 17 capability domains; 43 capabilities
  - 5 processes across five levels to measure process maturity
  - 171 practices across five levels to measure technical capabilities

CMMC Model v1.0: Number of Practices and Processes Introduced at each Level

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

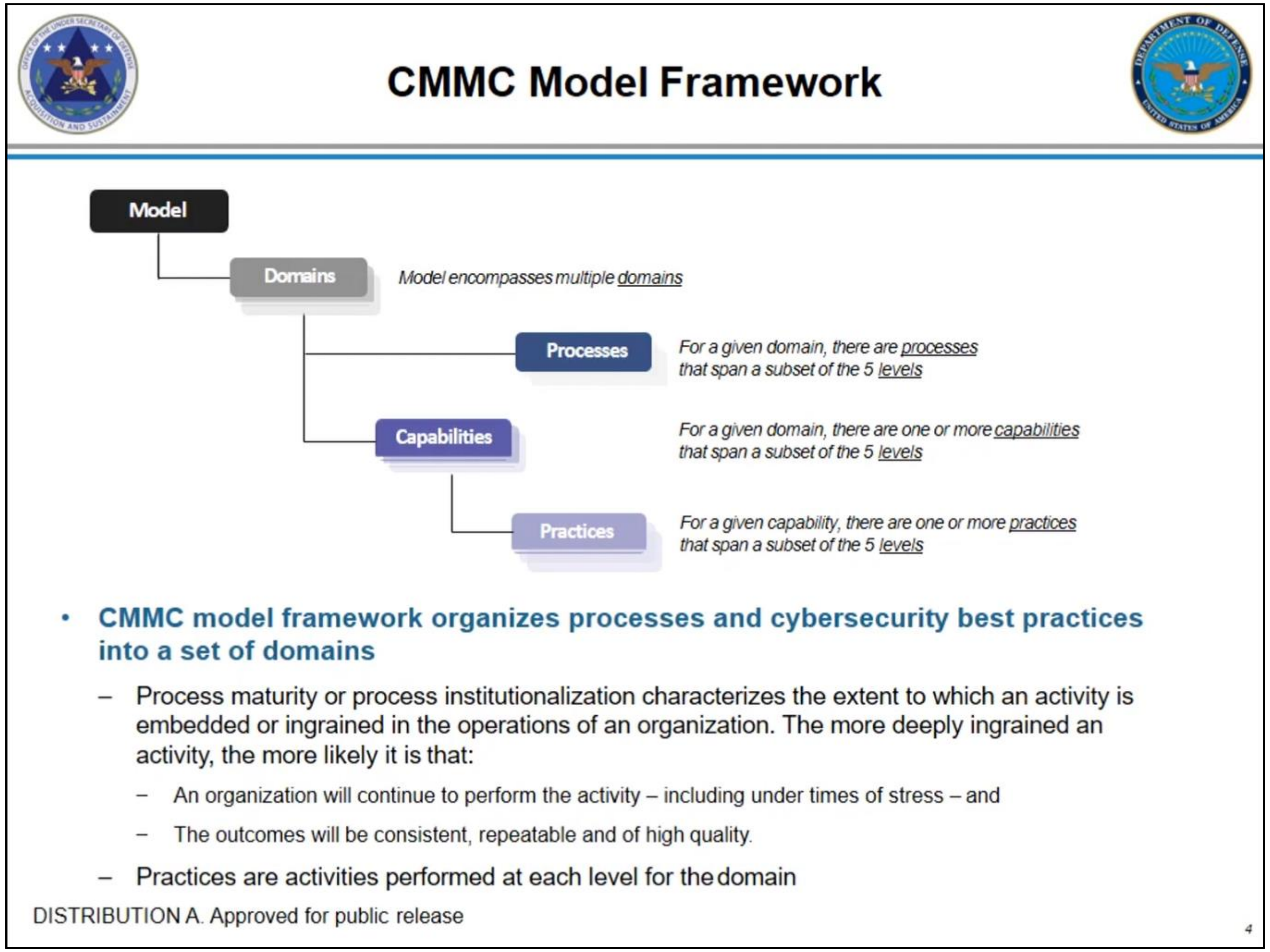
DISTRIBUTION A. Approved for public release

3

- In 2017 NIST published SP 800-171 with contractor security requirements but industry response was not adequate.
- Cybersecurity breaches continued to devolve and nothing seemed to be catching on.
- The new CMMC approach is supposed to be a policy reset.
- Goal is to close huge gap between the policymaker vision for defense industry security practices and the reality of monumental hacks by hostile national intelligence services (e.g. Chinese and others) in recent years.

CMMC

Cybersecurity Maturity Model Certification



CMMC Model Framework

Model
Domains
Processes
Capabilities
Practices

Model encompasses multiple domains

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

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

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

- **CMMC model framework organizes processes and cybersecurity best practices into a set of domains**
  - Process maturity or process institutionalization characterizes the extent to which an activity is embedded or ingrained in the operations of an organization. The more deeply ingrained an activity, the more likely it is that:
    - An organization will continue to perform the activity – including under times of stress – and
    - The outcomes will be consistent, repeatable and of high quality.
  - Practices are activities performed at each level for the domain

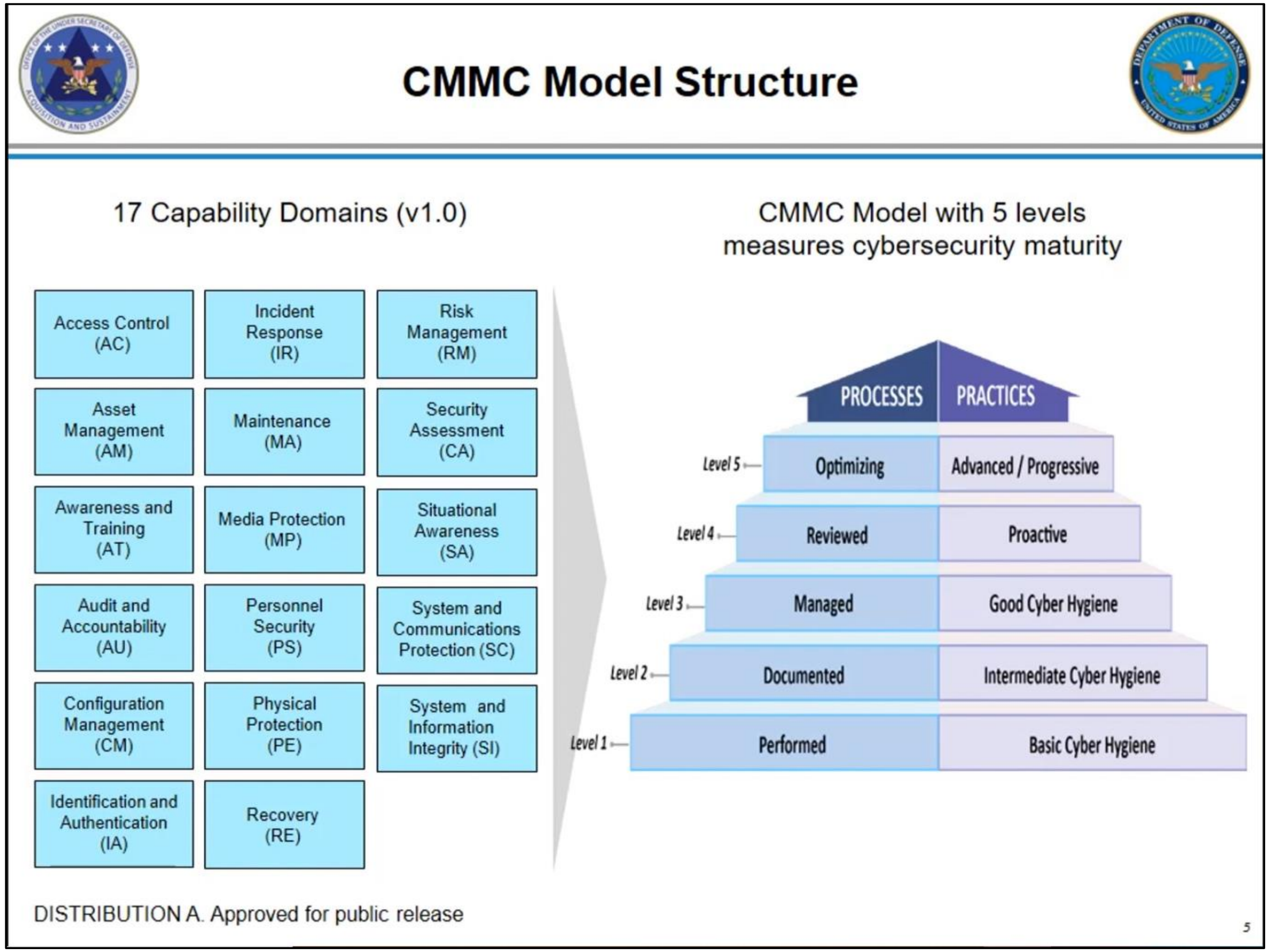
DISTRIBUTION A. Approved for public release

4

- The CMMC model evolved to recognize a one-size fits all approach to cyber security does not work.
- This model is based on maturity of security practices, focused on what DoD needs to protect for a given contract and category of risk.
- The key characteristic of the program is its orientation on processes, capabilities, and practices within 17 domains, and a third-party verification mechanism to assess the maturity across those with respect to efficacy in safeguarding sensitive information.

CMMC

Cybersecurity Maturity Model Certification



CMMC Model Structure

17 Capability Domains (v1.0)

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)	

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

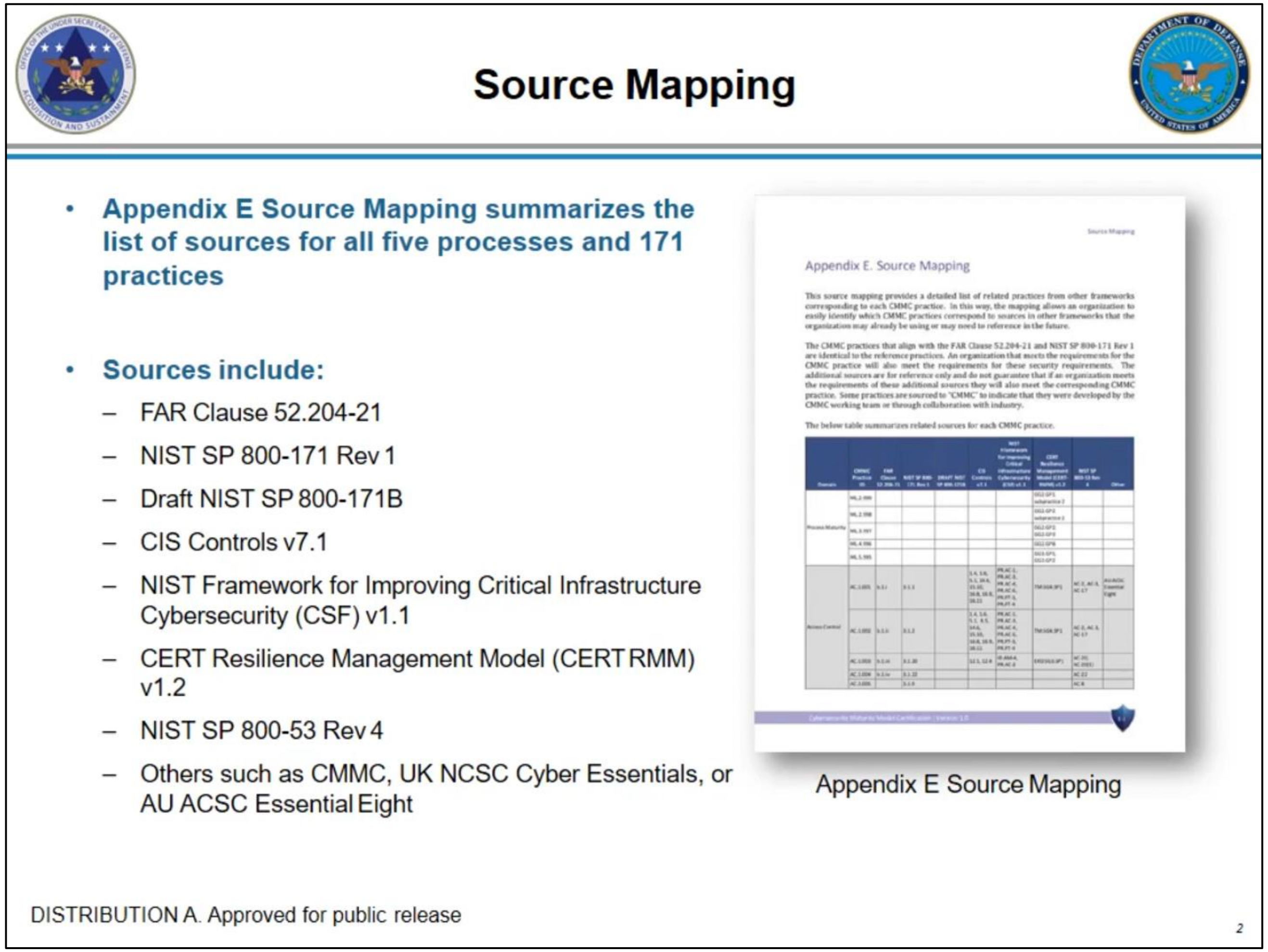
DISTRIBUTION A. Approved for public release

5

- The model is more about promoting critical thinking skills than making a checklist.
- The model made with/for industry in way that is to be digestible for small businesses as well.
- Intent is to roll this out in June ‘20 with RFI to train auditor firms that will certify companies later this year.
- New DFARS rule will come into effect later this year, CMMC requirements to be incorporated in contracts coming out in November.
- Big cultural shift for DoD requiring 3 party certification (after contract award, not prior, however).

CMMC

Cybersecurity Maturity Model Certification



Source Mapping

- Appendix E Source Mapping summarizes the list of sources for all five processes and 171 practices
- Sources include:
  - FAR Clause 52.204-21
  - NIST SP 800-171 Rev 1
  - Draft NIST SP 800-171B
  - CIS Controls v7.1
  - NIST Framework for Improving Critical Infrastructure Cybersecurity (CSF) v1.1
  - CERT Resilience Management Model (CERT RMM) v1.2
  - NIST SP 800-53 Rev 4
  - Others such as CMMC, UK NCSC Cyber Essentials, or AU ACSC Essential Eight

Source Mapping

Appendix E. Source Mapping

This source mapping provides a detailed list of related practices from other frameworks corresponding to each CMMC practice. In this way, the mapping allows an organization to easily identify which CMMC practices correspond to sources in other frameworks that the organization may already be using or may need to reference in the future.

The CMMC practices that align with the FAR Clause 52.204-21 and NIST SP 800-171 Rev 1 are identical to the reference practices. An organization that meets the requirements for the CMMC practice will also meet the requirements for these security requirements. The additional sources are for reference only and do not guarantee that if an organization meets the requirements of these additional sources they will also meet the corresponding CMMC practice. Some practices are sourced to "CMMC" to indicate that they were developed by the CMMC working team or through collaboration with industry.

The below table summarizes related sources for each CMMC practice.

Appendix E Source Mapping

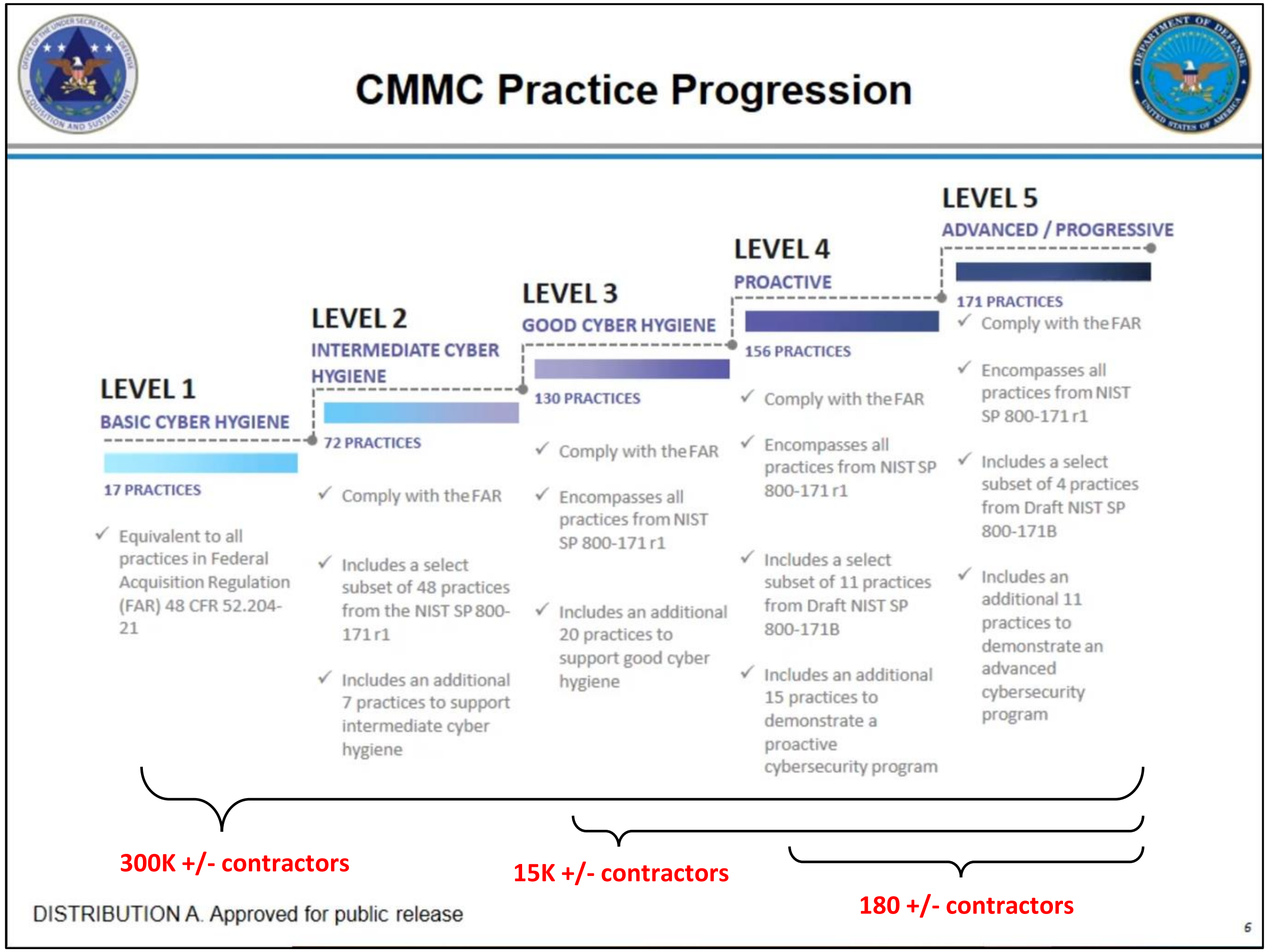
DISTRIBUTION A. Approved for public release

2

- The CMMC framework is based on many existing source regulations/policy documents.
- The process delivering the CMMC involved coordination with industry and academic organizations over the past year.
- Key history:
  - NIST released SP 800-53 in 2005, detailed federal systems security requirements.
  - Executive Order in 2014 mandated security requirements NIST SP 800-171 for contractor systems.
  - DFARS rule in response to 2014 Executive order was DFAR 252.204.701, it applied to any contractor touching controlled unclassified, but was a self-certify approach, which ultimately proved to be inadequate.

CMMC

Cybersecurity Maturity Model Certification



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

300K +/- contractors

15K +/- contractors

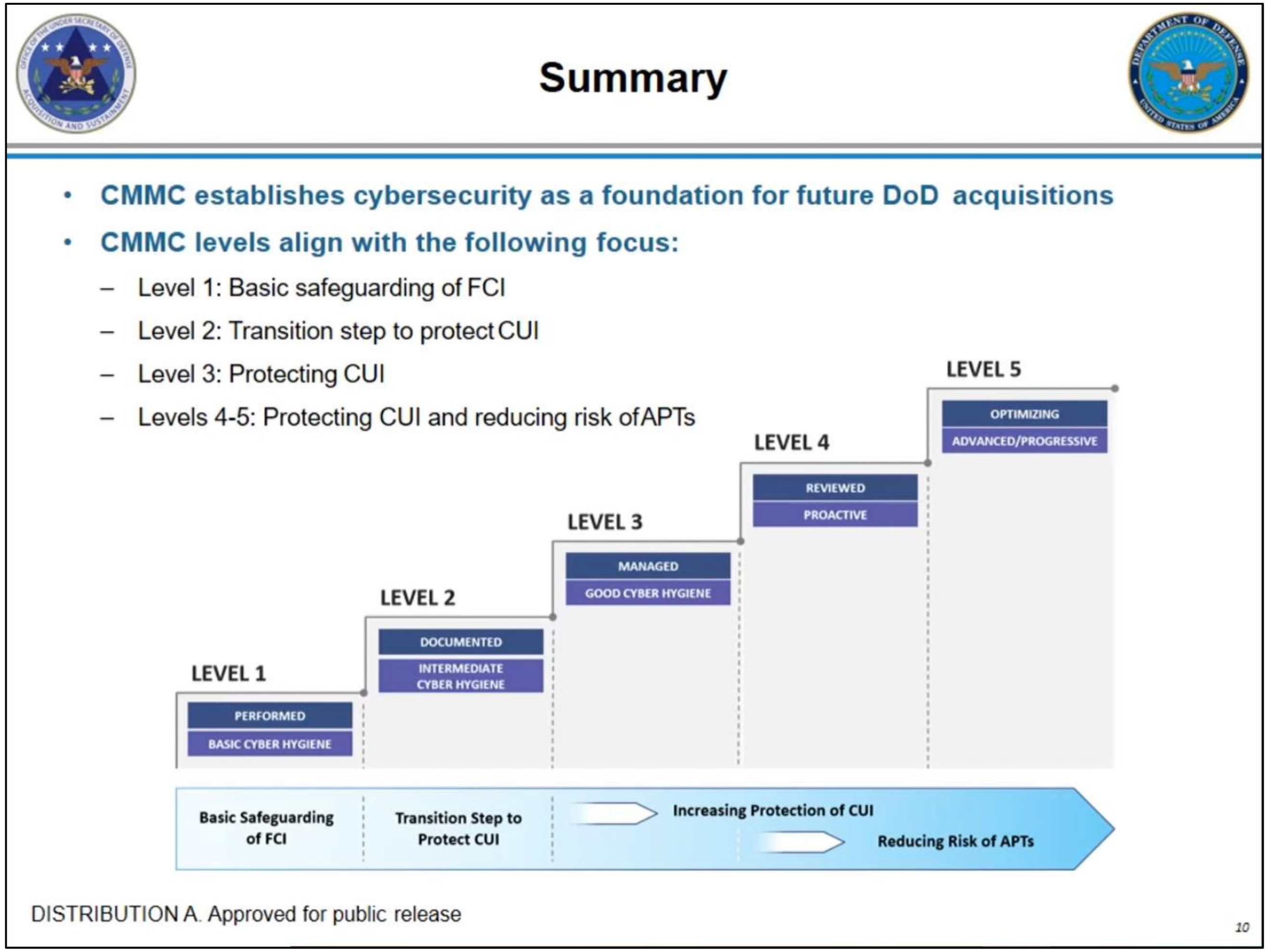
180 +/- contractors

DISTRIBUTION A. Approved for public release

- The Defense Industrial Base (DIB) includes about 300,000 contractors, and ALL will need minimum of Level 1 certification, will involve fee to auditing firm (estimate <$3,000 fee for Level 1).
- Of the DIB, 15,000 will need Level 3 certification…"cleared" defense contractors (holding Controlled Unclassified Information).
- Only 180 will need to get Level 4 or 5 certified due to working with more sensitive information.
- Will take a while to implement, good news is security is an allowable cost to submit as part of proposals.

CMMC

Cybersecurity Maturity Model Certification



Summary

- **CMMC establishes cybersecurity as a foundation for future DoD acquisitions**
- **CMMC levels align with the following focus:**
  - Level 1: Basic safeguarding of FCI
  - Level 2: Transition step to protect CUI
  - Level 3: Protecting CUI
  - Levels 4-5: Protecting CUI and reducing risk of APTs

LEVEL 1: PERFORMED, BASIC CYBER HYGIENE

LEVEL 2: DOCUMENTED, INTERMEDIATE CYBER HYGIENE

LEVEL 3: MANAGED, GOOD CYBER HYGIENE

LEVEL 4: REVIEWED, PROACTIVE

LEVEL 5: OPTIMIZING, ADVANCED/PROGRESSIVE

Basic Safeguarding of FCI | Transition Step to Protect CUI | Increasing Protection of CUI | Reducing Risk of APTs

DISTRIBUTION A. Approved for public release

10

- CMMC requires third party audit of ALL DoD prime and subcontractors <u>every three years</u>.
- Third party certification audit will not only cost money but probably require major transformation of corporate security policies and practices for many firms.
- The federal government’s auditor contract hasn’t been awarded yet (expected late summer).
- More information available at the CMMC accreditation body:

www.cmmcab.org

22FEB21

|TSM|

CAPABILITIES STATEMENT

Jeff Moran
Owner & Project Executive

Biography

30+ years of diverse functional and international experience with TSM Worldwide LLC, Honeywell Aerospace, Ingersoll-Rand, and Deloitte including 14 years of distinguished Regular & Reserve Army service as an apprentice and commissioned Intelligence Officer.

Selected Individual Certifications

FMI – Construction Exec | MCAA-AIPM | USACE/NAVFAC QM
DAU-DSAM | DoD-PPBES | DoD-RMBC | SBA 7J (10+)
Six Sigma Blackbelt | MN State –Tech Dipl (Design, Fab, Svc)
Learning Tree – Systems & Network Security (+4 others)

Education

BSFS, Georgetown University (honors)
MBA, Emory University
Joint LLM MS, Université de Genève-IHEID

Contact Details

+1.763.301.1843 (Mobile)
+1.877.768.4164 (Office/Fax)
jeff@tsmworldwide.com

View profile

LinkedIn

The TSM story began in 2006 after Jeff Moran returned from overseas military duty and completed a multi-year intensive entrepreneurship assistance program sponsored by the Veterans Benefits Administration. TSM has since evolved to conscientiously and creatively partner with clients on a range of specialized challenges and opportunities in construction and manufacturing management. In 2020, TSM completed VA-verification as a Service-Disabled Veteran-Owned Small Business so now also offers strategic venturing services to firms in federal markets. TSM plans to complete SBA HUBZone certification in 2021.

Service Disabled Veteran Owned Small Business
SDVOSB
CVE

Functional & Process Competencies

- Compliance program evaluation, development, management
- Continuous process improvement
- Financial analysis, management accounting, audit, controls
- Interim management & supervision
- Investigative research methods & practices
- Machine shop design and manufacturing service management
- Physical, information, systems, network, & personnel security
- Procurement & related administration and management
- Program/project management (full life-cycle)
- Quality management, audit, & control
- Risk-management & advisory (full spectrum)
- Sales & marketing management
- Strategic ventures & contracts management
- Technical service & manufacturing operations management
- Valuation, estimating, forecasting, and budgeting

Market Segments of Interest

- Aerospace, defense, intelligence
- Correctional, public safety, security
- Federal facilities, institutions, and public buildings
- Manufacturing & building construction management
- Medical, hospitals, patient-care

Selected NAICS Codes

- 236220 | Commercial & Institutional Building Construction
- 238220 | Plumbing, Heating, and Air-Conditioning Contractors
- 332710 | Machine shops
- 423720 | Plumbing & Heating Equipment (Hydronics) Wholesaler
- 423730 | Heating and Cooling Equipment (Air) Wholesaler
- 541611 | Administrative management, related consulting services
- 541614 | Process, distribution, logistics consulting services

Other Certifications / Security Clearance

- VA Verified SDVOSB | HUBZone certification pending
- MN Federal Executive Board-certified (SADBOC)
- Top Secret + clearance expired, reinvestigation pending

CAGE Code	8FQV5
DUNS #	012488963
Web Address	https://tsmworldwide.com
Physical Address	TSM Worldwide LLC 12700 550th Street Rock Creek, MN 55069
Postal Address	TSM Worldwide LLC P.O. Box 141050 Minneapolis, MN 55414

www.tsmworldwide.com