INFORMATION SECURITY & ACQUISITIONS

Mr. David Curry
Chief, Strategic Integration
Directorate of Contracting
U.S. Army Corps of Engineers

31 March 2025

U.S. ARMY

US Army Corps of Engineers®

AGENDA

- Background

- CUI - Controlled Unclassified Information
- NIST - National Institute of Standards and Technology scores
- CMMC - Cybersecurity Maturity Model Certification
- Questions/Discussion

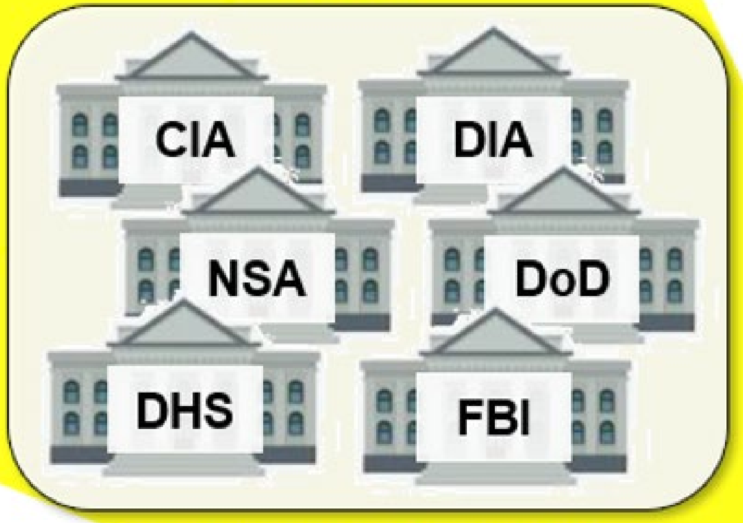
PROBLEM STATEMENT

DoD and the Defense Industrial Base (DIB) face increased security risks due to slow / no compliance with DoD mandates related to Controlled Unclassified Information (CUI).

BACKGROUND

WHY NOW?

1990s



Intelligence Orgs = 17

Today

Our enemies used to target the US intelligence agencies

SWD Contractors = 1800

WHY NOW?

1990s

Intelligence Orgs = 17

They soon realized a MUCH easier target is the Defense Industrial Base.

Today

SWD Contractors = 1800

U.S. ARMY

US Army Corps of Engineers®

HISTORY OF INFOSEC/ CYBERSECURITY

27 MAY 09 – POTUS memo calling for examination of CUI and Interagency Task Force

04 NOV 10 – POTUS issues Executive Order 13556 – Controlled Unclassified Information (CUI)

18 NOV 13 – Final rule passed, NIST SP 800-53, Unclassified Controlled Technical Information

01 AUG 15 – DoD publishes DFARS Clause 252.204-7012 - Safeguarding Unclassified CTI

26 AUG 15 – Interim rule passed, NIST SP 800-171, Covered Defense Information

30 DEC 15 – Interim rule passes, NIST SP 800-171, Operationally Critical Support

14 SEP 16 – 32 CFR Part 2002 introduces the first legal framework for CUI

21 OCT 16 – Final rule passed, NIST SP 800-171

30 OCT 16 – DFARS 252.204-7012 goes into effect

15 NOV 18 – DoD Memo on implementing CUI

06 MAR 20 – DoD Instruction 5200.48 Established DoD CUI Policy

30 NOV 20 – DFARS interim rule goes into effect requiring NIST score in SPRS to receive awards

04 DEC 20 – Director of National Intelligence requests POTUS kill CUI and EO 13556

31 DEC 20 – Deadline for agencies to issue CUI implementation guidance

01 OCT 25 – CMMC goes into full effect, no award without CMMC certification

15yr onramp

WHERE ARE WE TODAY?

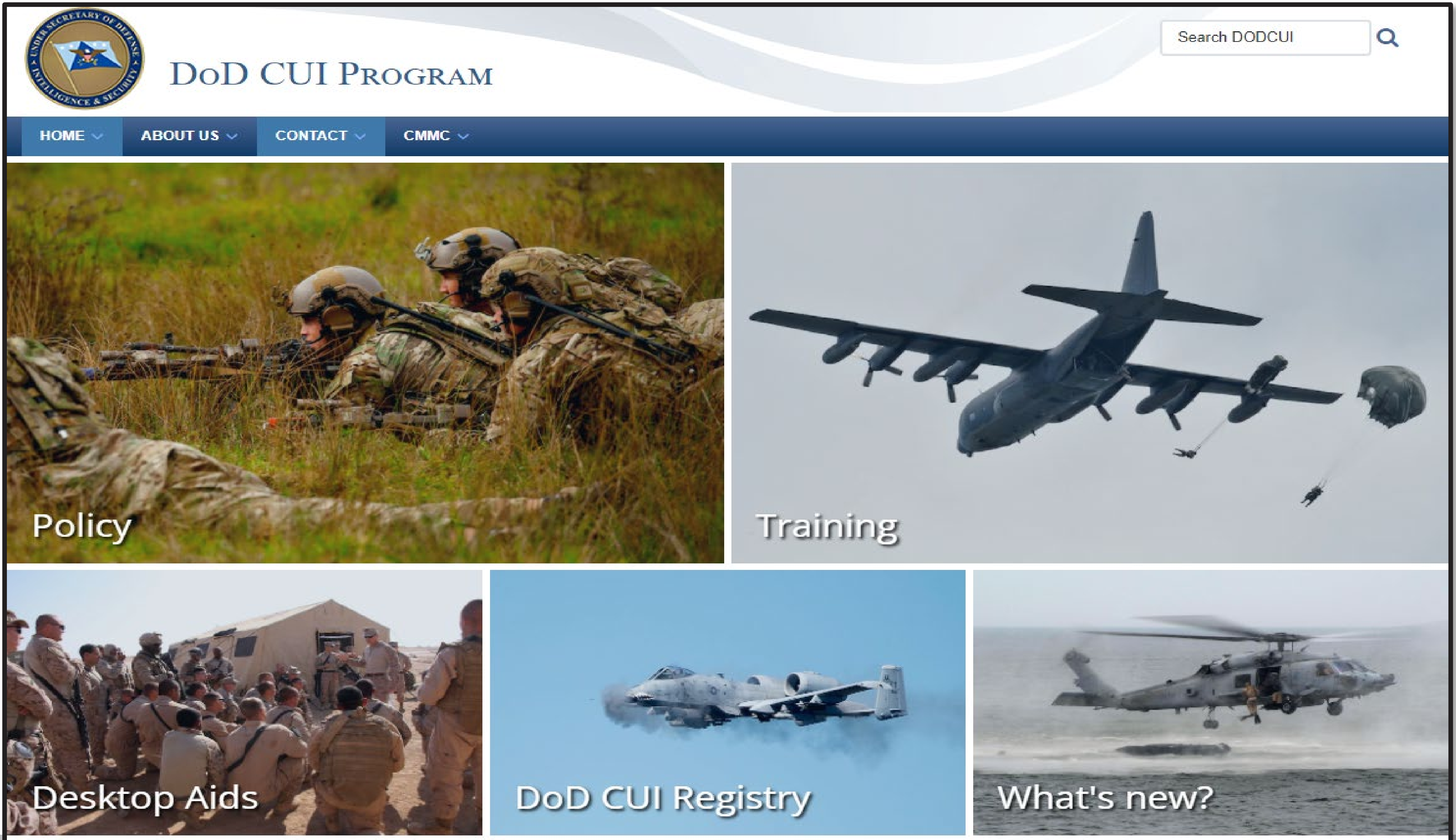
- CUI mandated 10+ years ago, in DoD contracts since 2017
- Still widespread variance in DoD implementation of CUI
- Ex: USACE has no one person identified as CUI owner
- DIB feedback? DoD marks too little info as CUI…or too much
  - Too little = security risk, exposes sensitive information to our enemies
  - Too much = cost risk, DIB charges us and protecting CUI is expensive
- Spotty DIB understanding of CUI and clause requirements
- Ex: few if any in the DIB comply with Cyber Crimes mandate
- Ex: most USACE solicitations are currently silent on CUI
- Two forcing functions will drive DoD/Army/USACE action:
  1) Cybersecurity Maturity Model Certification (CMMC)
  2) Completion of the CUI rule-making process

CUI

WHAT IS CUI ?

Controlled Unclassified Information (CUI) is sensitive info that doesn’t quite rise to the level of classification…but still warrants protection. It is UNCLASSIFIED information that requires identification, marking, safeguarding and dissemination controls required by law, regs and policy. Note, CUI may be created by the Government or DIB contractors.

www.DODCUI.mil



DOD INDEX GROUPS*

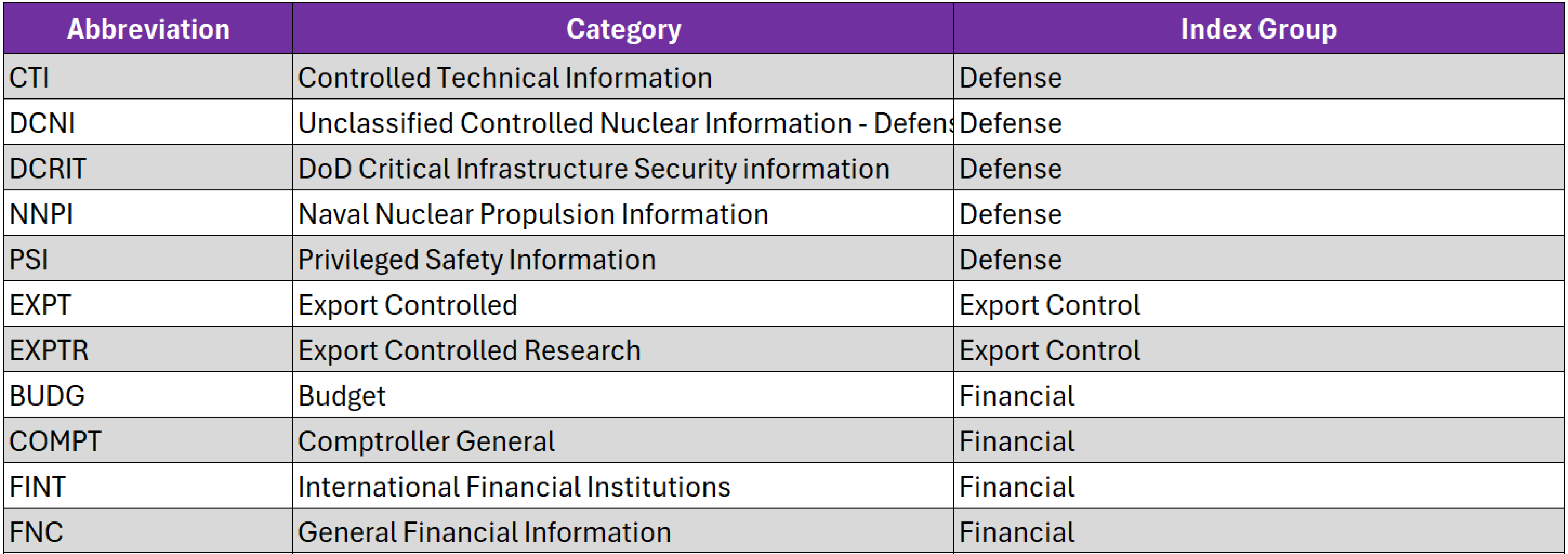
112 “Categories” of CUI across 18 “Index Group”

Critical Infrastructure	Proprietary Business Information	Export Control	Financial	Immigration
Intelligence	International Agreements	Law Enforcement	Legal	Natural and Cultural Resources
Statistical	Nuclear	Patent	Privacy	Procurement and Acquisition
	Tax	Defense	Transportation	

*Note: NARA owns CUI, and lists more categories and groups, but DoD has fewer.

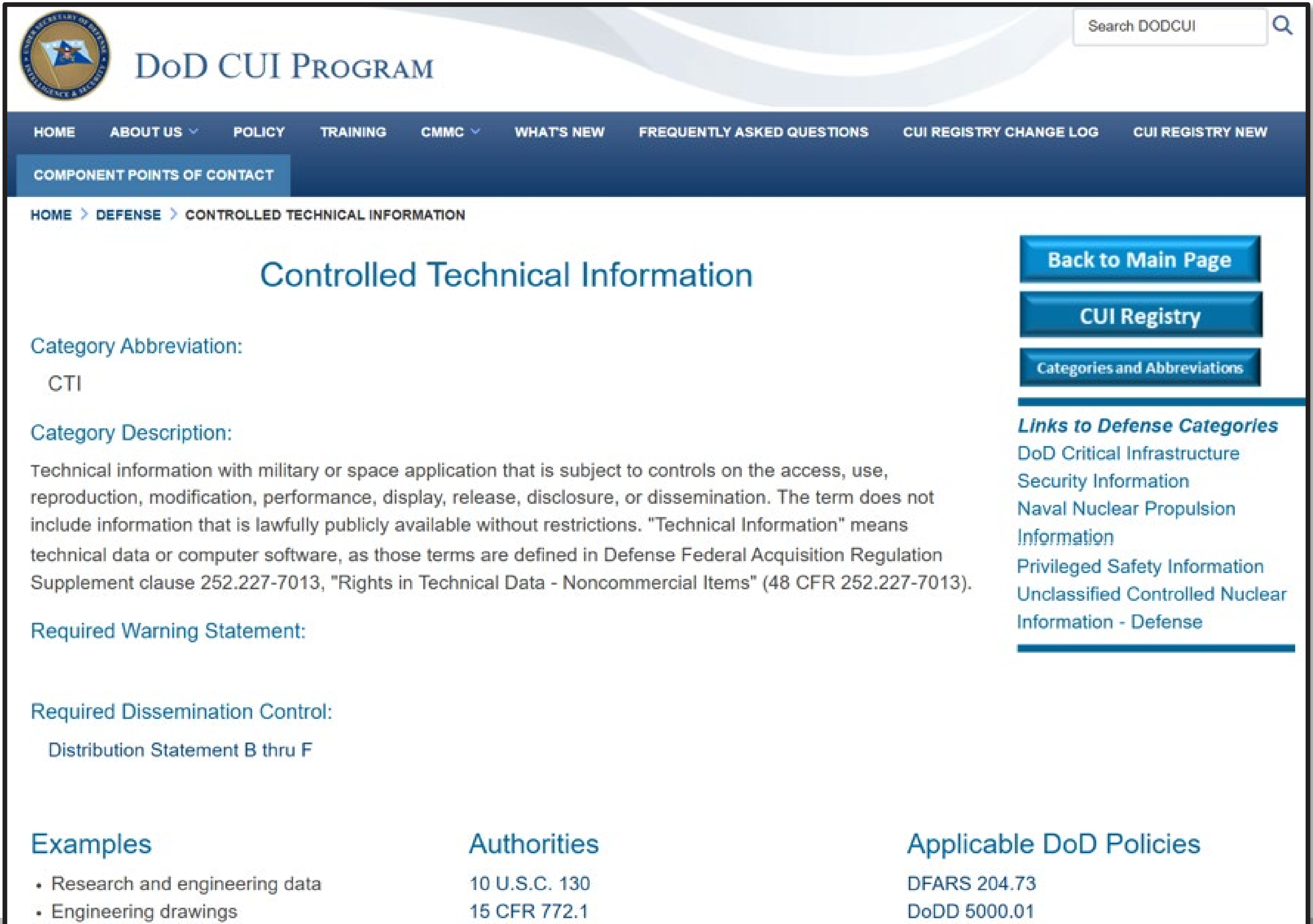
DOD CUI REGISTRY

112 “Categories” of CUI across 18 “Index Group”



Abbreviation	Category	Index Group
CTI	Controlled Technical Information	Defense
DCNI	Unclassified Controlled Nuclear Information - Defens	Defense
DCRIT	DoD Critical Infrastructure Security information	Defense
NNPI	Naval Nuclear Propulsion Information	Defense
PSI	Privileged Safety Information	Defense
EXPT	Export Controlled	Export Control
EXPTR	Export Controlled Research	Export Control
BUDG	Budget	Financial
COMPT	Comptroller General	Financial
FINT	International Financial Institutions	Financial
FNC	General Financial Information	Financial

DOD CUI REGISTRY



Controlled Technical Information

Category Abbreviation:

CTI

Category Description:

Technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. The term does not include information that is lawfully publicly available without restrictions. "Technical Information" means technical data or computer software, as those terms are defined in Defense Federal Acquisition Regulation Supplement clause 252.227-7013, "Rights in Technical Data - Noncommercial Items" (48 CFR 252.227-7013).

Required Warning Statement:

Required Dissemination Control:

Distribution Statement B thru F

Links to Defense Categories

DoD Critical Infrastructure Security Information

Naval Nuclear Propulsion Information

Privileged Safety Information

Unclassified Controlled Nuclear Information - Defense

Examples

- Research and engineering data
- Engineering drawings

Authorities

10 U.S.C. 130

15 CFR 772.1

Applicable DoD Policies

DFARS 204.73

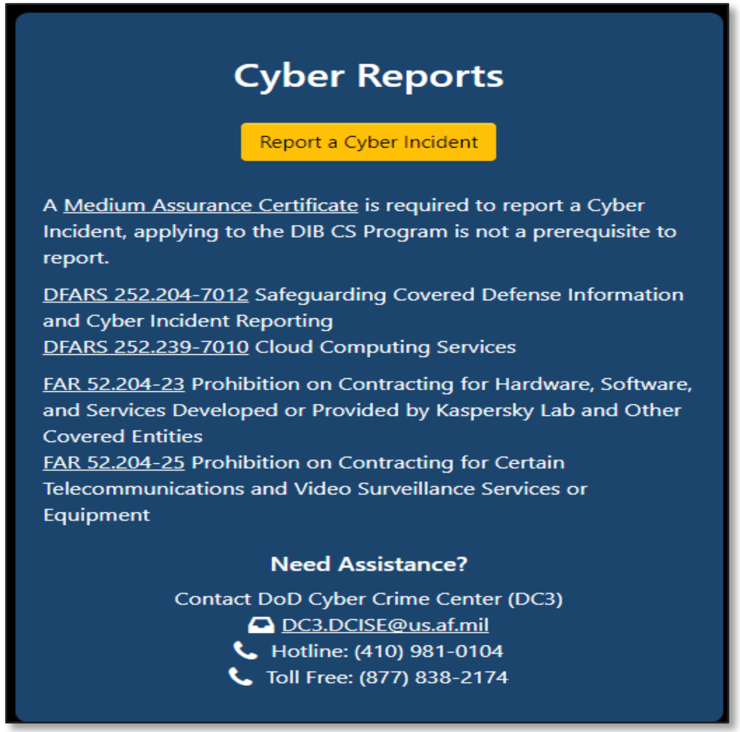
DoDD 5000.01

CUI BASICS

- SHARED responsibility of Government (GOV) and Contractor (DIB) personnel

- GOV responsibilities:
  - Identification
  - Communication
  - Marking
  - Safeguarding

- DIB responsibilities:
  - Marking
  - Safeguarding
  - Reporting – 100%, even suspected cyber incidents to DoD.



Cyber Reports

A Medium Assurance Certificate is required to report a Cyber Incident, applying to the DIB CS Program is not a prerequisite to report.

DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting
DFARS 252.239-7010 Cloud Computing Services

FAR 52.204-23 Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities
FAR 52.204-25 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment

Need Assistance?

Contact DoD Cyber Crime Center (DC3)
DC3.DCISE@us.af.mil
☎ Hotline: (410) 981-0104
☎ Toll Free: (877) 838-2174

- DoD Cyber Crime Center = central node to report incidents: https://dibnet.dod.mil
- Can also report anomalous cyber activity 24/7 to: report@cisa.gov or (888) 282-0870

CUI sounds resource intensive!

YES.

RECENT EXAMPLES

- Ex #1: 2023 Industry Day ~ 500ish companies attending
  - Conducted real time poll:
  - KTRs with a cyber breach / suspected breach in the last 12mos? **475**
  - How many companies reported incident to DoD? **0**
- Ex #2: 2024 Industry Day ~ 500ish companies attending
  - Conducted real time poll:
  - KTRs with a cyber breach / suspected breach in the last 12mos? **486**
  - How many companies reported incident to DoD? **0**
- One WOSB reported she was fully prepped for CUI/CMMC.
- When asked why? “Because I plan to win” – sees it as competitive advantage

…THE CUI ASK

- Designate at least 1 person to own CUI
- Educate org on CUI, what / when / why / how
- Educate industry on what we’re paying them to do
- Study the JAN 2025 Federal Register post on CUI
- Mark and safeguard CUI IAW with regs / statute
- Establish checks / balances to ensure compliance

NIST SCORES

WHAT IS THE NIST REQUIREMENT?

- Rolled out in 2017/2018 timeframe
- NIST SP 800-171 Rev2, “Protecting CUI in Nonfederal Systems and Organizations Security Requirements”
- DoD’s 110 item Microsoft Excel checklist
- KTRs must annually self-assess their cyber hygiene
- KTRs upload their score into PIEE/SPRS
- KOs validate a NIST score is present before award
- KOs download a copy and store it in PCF.
- Scores don’t matter, only that KTR performed the assessment
- NIST is a statutory mandate not a policy initiative

- **No NIST score = No Award**

If a contractor numeric NIST score doesn’t currently matter, then what’s the point?

PRACTICE. PRACTICE. REPEAT.

- The point of NIST scores is **muscle memory**.
- DoD's goal: think about cyber hygiene 1x/year
  - Pay attention to security.
  - Assess your hygiene.
  - Fill your gaps.
  - Report your status.
  - Repeat.
- Just like taxes.

…THE NIST ASK

- Prioritize and support organizational NIST compliance
- Educate your organization on NIST requirements
- Ensure NIST compliance across your portfolio
- Don’t settle for the minimum, meet the intent of NIST
- Implement plan for cyber hygiene before 1 OCT 25

CMMC

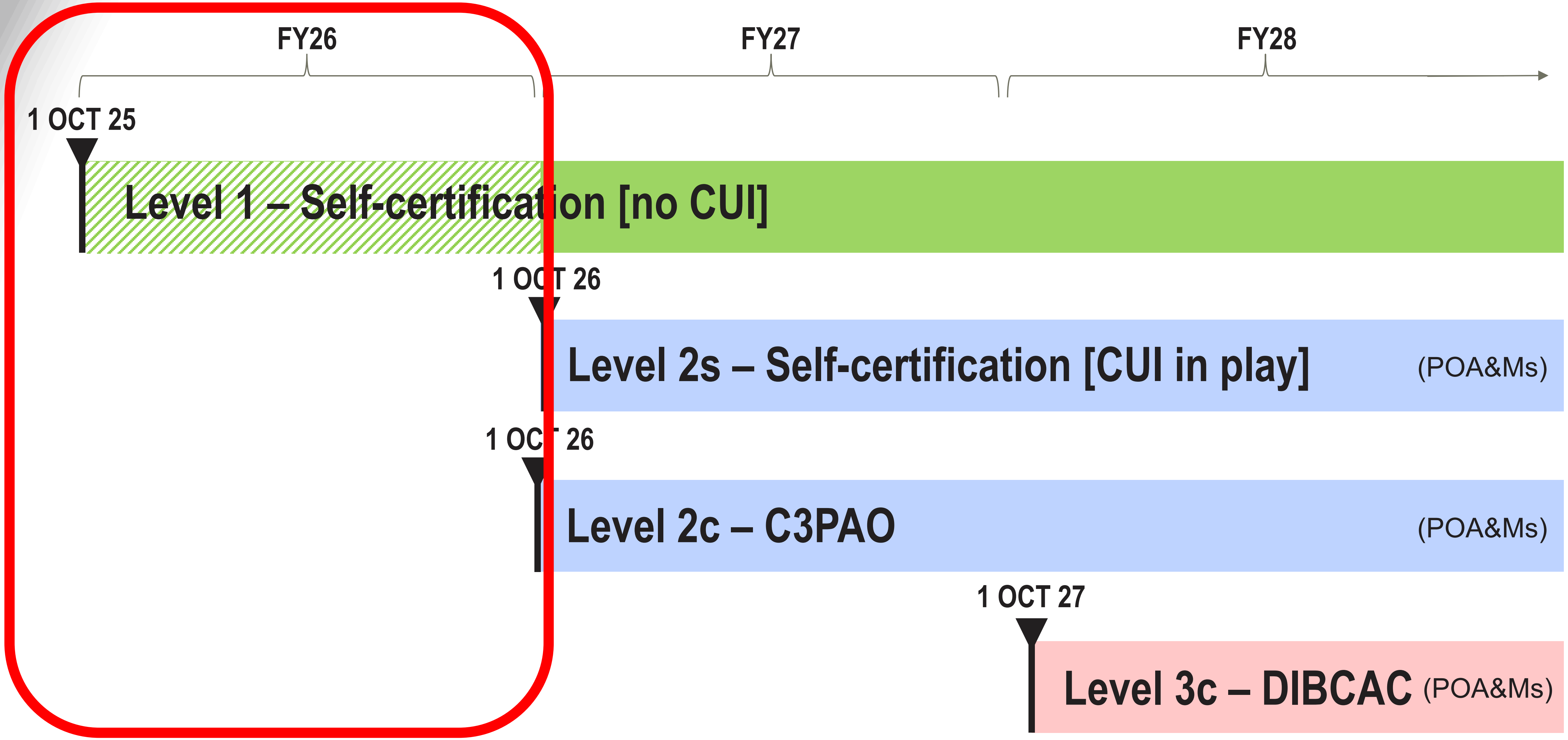
WHAT IS CMMC ?

The Cybersecurity Maturity Model Certification (CMMC) is a new DoD standard to ensure security of Federal Contract Information (FCI) and CUI within the Defense Industrial Base (DIB). Starting 1 OCT 25, certification is mandatory for all DIB contractors.

CMMC BASICS

LEVEL 3	134	Requirements (110 from NIST SP 800-171 R2 plus 24 from NIST SP 800-172)	- DIBCAC certification assessment @ 3yrs - Annual Affirmation	FY28
LEVEL 2	110	Requirements aligned with NIST SP 800-171 R2	- C3PAO cert. @ 3yrs, or - Self-assessment every 3yrs for select programs - Annual Affirmation	FY27
LEVEL 1	17	Requirements aligned with FAR 52.204.21	Annual Self-Assessment Annual Affirmation	FY26

PHASED CMMC IMPLEMENTATION



FY26

FY27

FY28

1 OCT 25

Level 1 – Self-certification [no CUI]

1 OCT 26

Level 2s – Self-certification [CUI in play] (POA&Ms)

1 OCT 26

Level 2c – C3PAO (POA&Ms)

1 OCT 27

Level 3c – DIBCAC (POA&Ms)

Plans of Action and Milestones (POA&Ms)

…THE CMMC ASK

- Prioritize and support CMMC compliance
- Educate your organization on CMMC requirements
- Put in plan to achieve CMMC Level 1 by 1 OCT 25
- Recommend CMMC backcheck metrics, measure progress/risk
- Actively engage with PTACs for Small Business partners
- Cover CMMC in Customer/Partner/Trade Org meetings

IMPLEMENTATION

IMPLEMENTATION LINES OF EFFORT

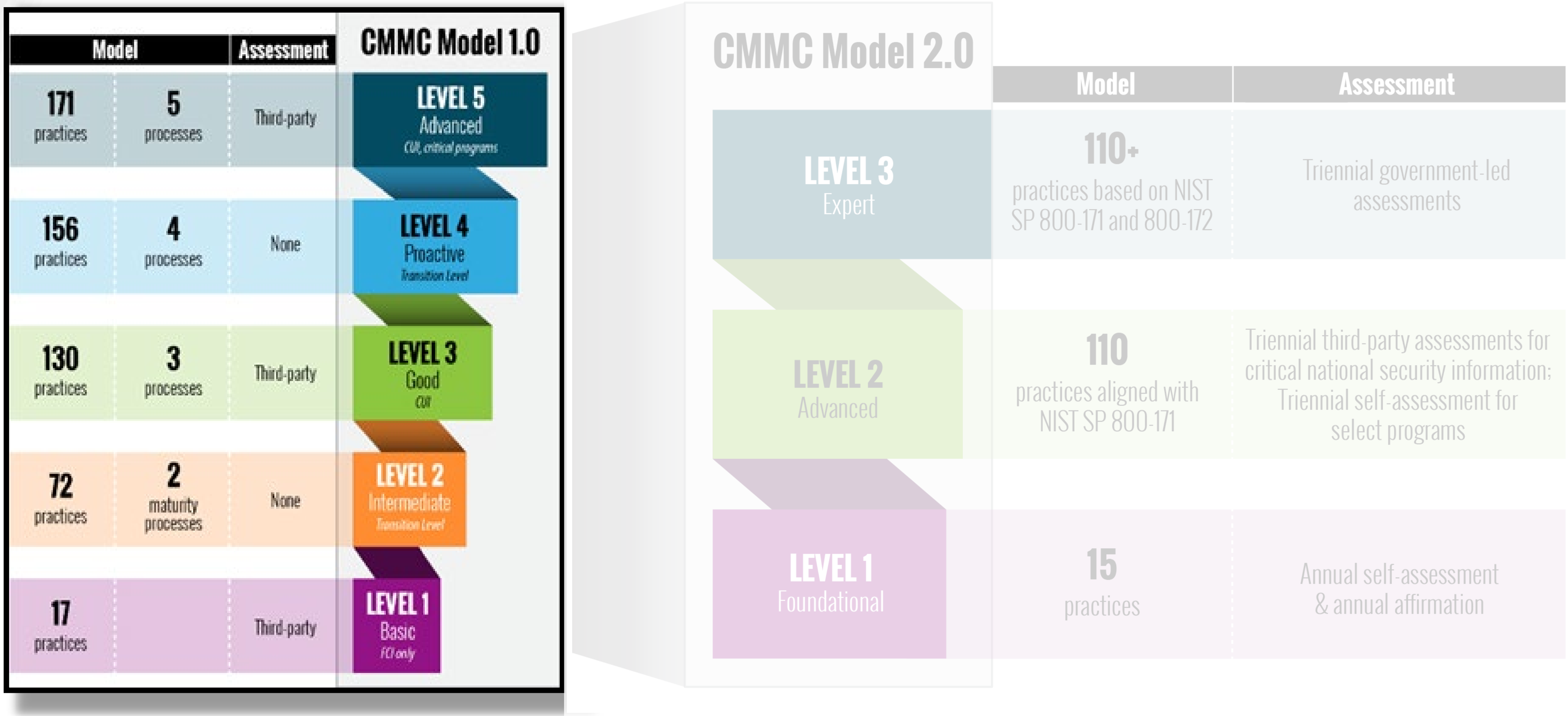
- Form CMMC Task Force [CT]
- HQ OPORD for Commanders [CT]
- DIB training [CT]
- Standardize procedures [CT/EC]
- USACE training [CT]
- Implement oversight [CT]
- Audit of existing:
  - CUI [ALL]
  - Audit existing infrastructure [OPS]
  - Audit existing IT ecosystem [G6]

Q
A

KEY TERMS

- **AI** = Artificial Intelligence
- **AO** = Affirming Official
- **CamoGPT** = Army’s secure CAC-enabled AI tool
- **ChatGPT** = Leading online AI tool
- **CMMC** = Cybersecurity Maturity Model Certification
- **CTI** = Controlled Technical Information (a subset of CUI)
- **CUI** = Controlled Unclassified Information
- **FOUO** = For Official Use Only
- **NIST** = National Institute of Standards and Technology
- **OAS** = Organization Seeking Assessment
- **PIEE** = Procurement Integrated Enterprise Environment
- **SPRS** = Supplier Performance Risk System

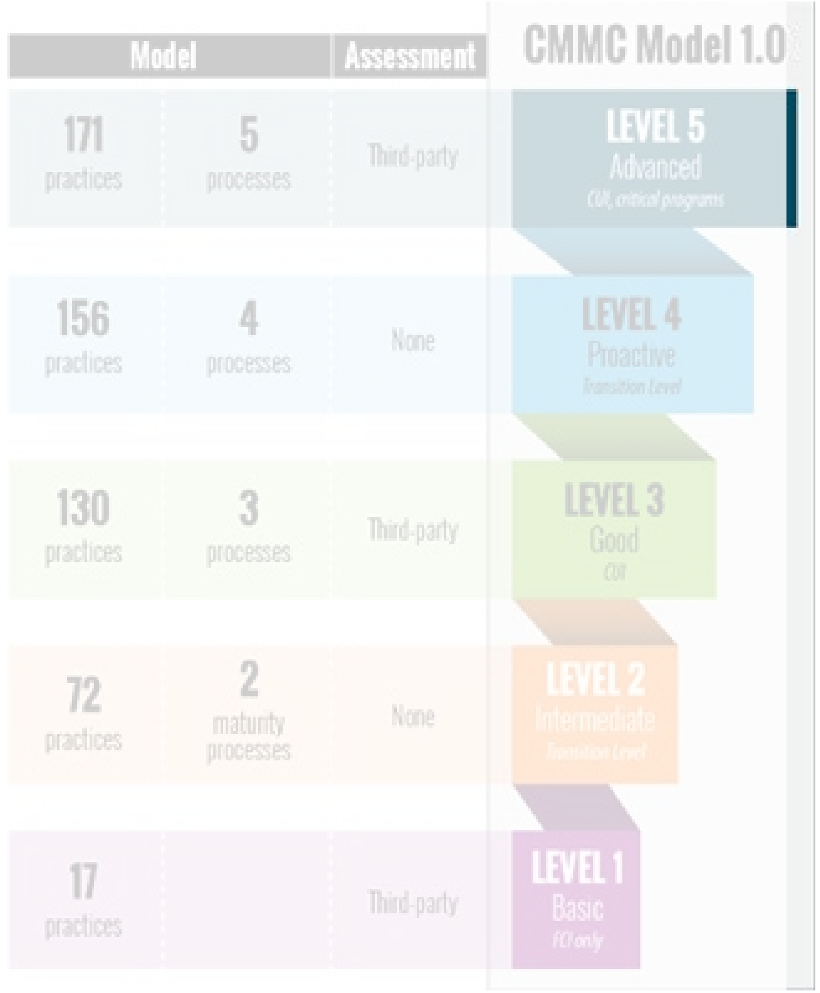
ORIGINAL CMMC FRAMEWORK



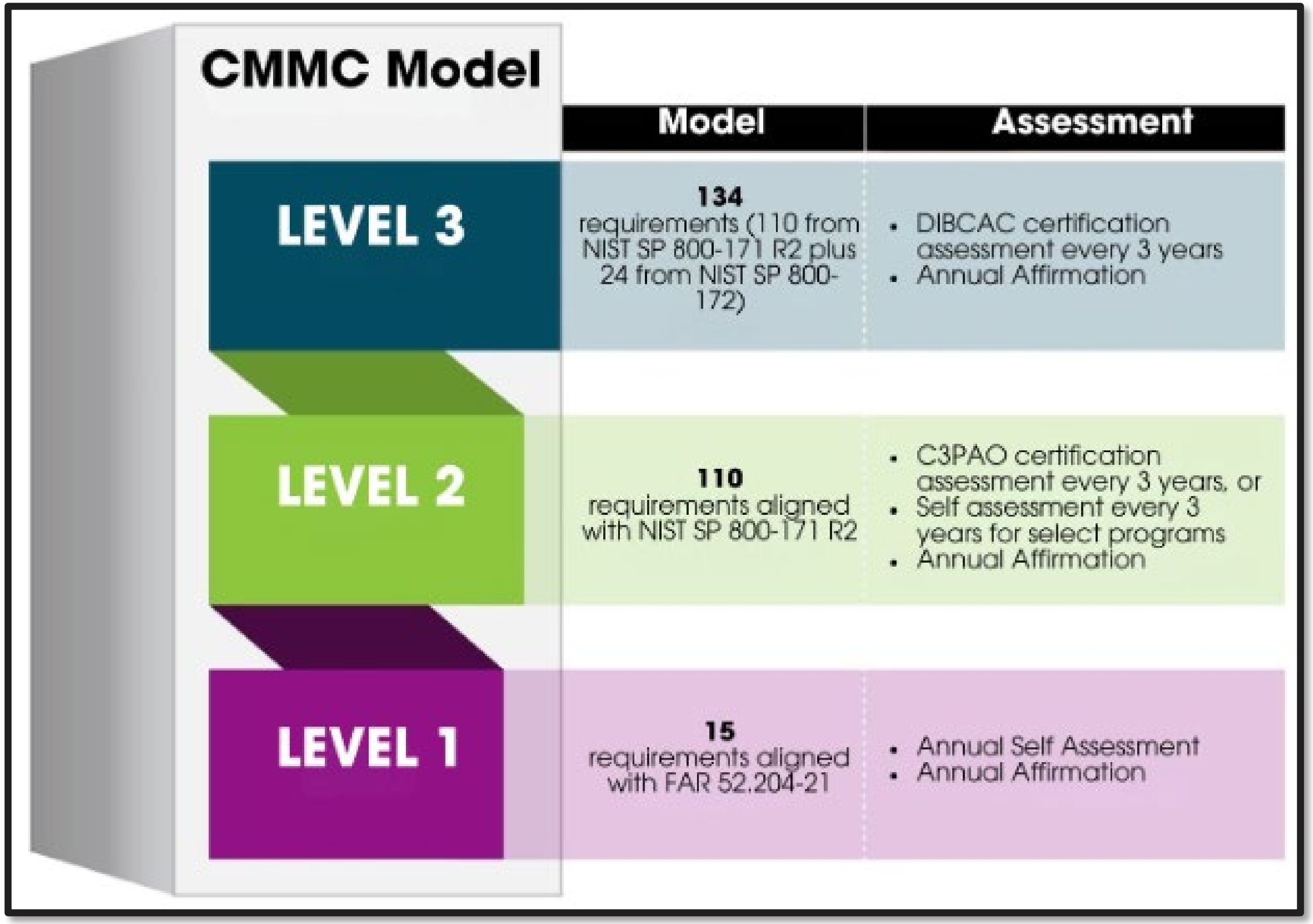
Model		Assessment	CMMC Model 1.0
171 practices	5 processes	Third-party	LEVEL 5 Advanced *CUI, critical programs*
156 practices	4 processes	None	LEVEL 4 Proactive *Transition Level*
130 practices	3 processes	Third-party	LEVEL 3 Good *CUI*
72 practices	2 maturity processes	None	LEVEL 2 Intermediate *Transition Level*
17 practices		Third-party	LEVEL 1 Basic *FCI only*

CMMC Model 2.0	Model	Assessment
LEVEL 3 Expert	110+ practices based on NIST SP 800-171 and 800-172	Triennial government-led assessments
LEVEL 2 Advanced	110 practices aligned with NIST SP 800-171	Triennial third-party assessments for critical national security information; Triennial self-assessment for select programs
LEVEL 1 Foundational	15 practices	Annual self-assessment & annual affirmation

CURRENT CMMC FRAMEWORK

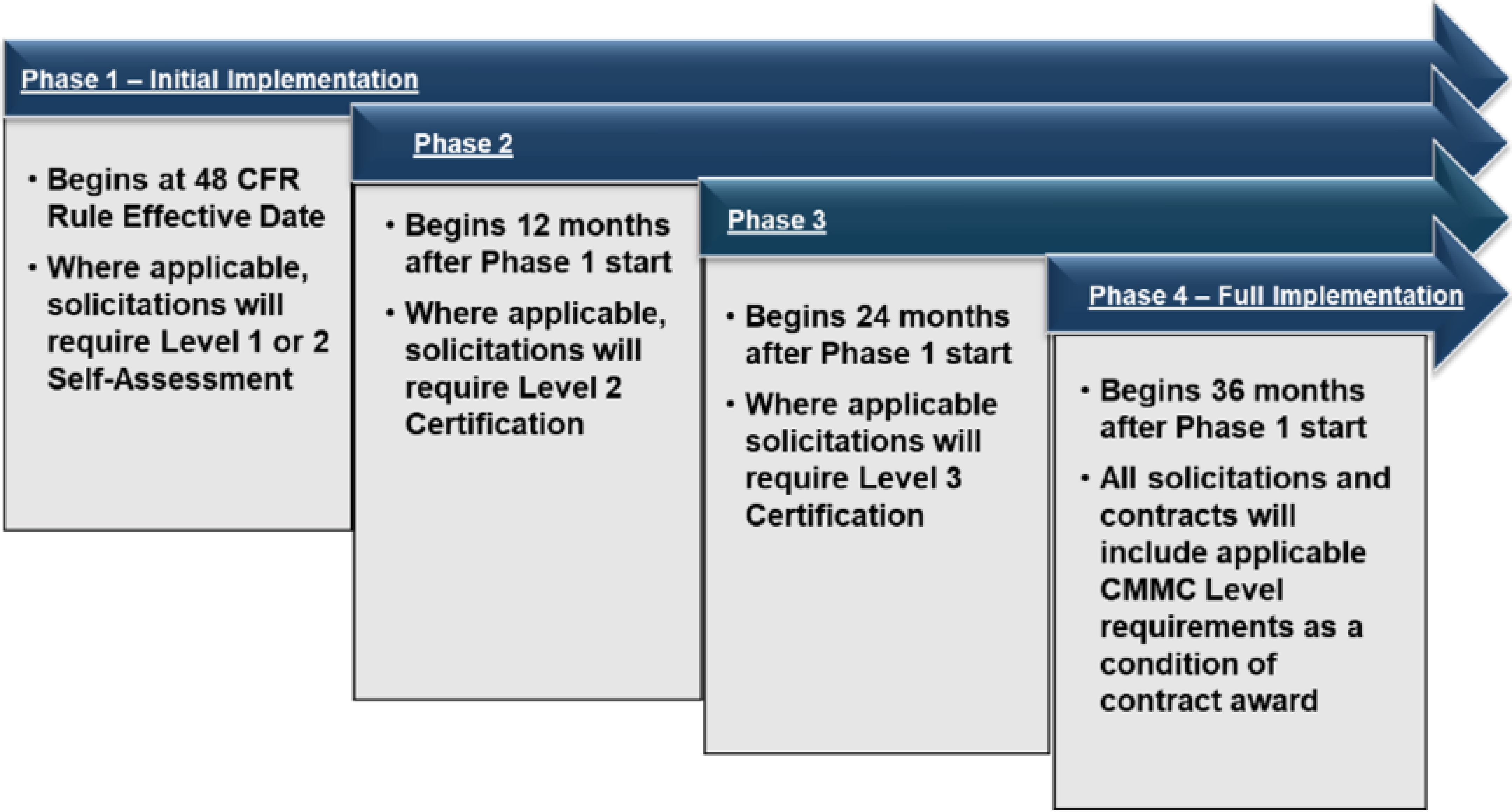


Model		Assessment	CMMC Model 1.0
171 practices	5 processes	Third-party	LEVEL 5 Advanced CUI, critical programs
156 practices	4 processes	None	LEVEL 4 Proactive Transition Level
130 practices	3 processes	Third-party	LEVEL 3 Good CUI
72 practices	2 maturity processes	None	LEVEL 2 Intermediate Transition Level
17 practices		Third-party	LEVEL 1 Basic FCI only



CMMC Model	Model	Assessment
LEVEL 3	**134** requirements (110 from NIST SP 800-171 R2 plus 24 from NIST SP 800-172)	• DIBCAC certification assessment every 3 years • Annual Affirmation
LEVEL 2	**110** requirements aligned with NIST SP 800-171 R2	• C3PAO certification assessment every 3 years, or • Self assessment every 3 years for select programs • Annual Affirmation
LEVEL 1	**15** requirements aligned with FAR 52.204-21	• Annual Self Assessment • Annual Affirmation

PHASED CMMC IMPLEMENTATION



Phase 1 – Initial Implementation

- Begins at 48 CFR Rule Effective Date
- Where applicable, solicitations will require Level 1 or 2 Self-Assessment

Phase 2

- Begins 12 months after Phase 1 start
- Where applicable, solicitations will require Level 2 Certification

Phase 3

- Begins 24 months after Phase 1 start
- Where applicable solicitations will require Level 3 Certification

Phase 4 – Full Implementation

- Begins 36 months after Phase 1 start
- All solicitations and contracts will include applicable CMMC Level requirements as a condition of contract award

U.S. ARMY

US Army Corps of Engineers®

PHASED CMMC IMPLEMENTATION

CMMC Status	Source & Number of Security Reqts.	Assessment Reqts.	Plan of Action & Milestones (POA&M) Reqts.	Affirmation Reqts.
Level 1 (Self)	• 15 required by FAR clause 52.204-21	• Conducted by Organization Seeking Assessment (OSA) annually • Results entered into the Supplier Performance Risk System (SPRS)	• Not permitted	• After each assessment • Entered into SPRS
Level 2 (Self)	• 110 NIST SP 800-171 R2 required by DFARS clause 252.204-7012	• Conducted by OSA every 3 years • Results entered into SPRS • CMMC Status will be valid for three years from the CMMC Status Date as defined in § 170.4	• Permitted as defined in § 170.21(a)(2) and must be closed out within 180 days • Final CMMC Status will be valid for three years from the Conditional CMMC Status Date	• After each assessment and annually thereafter • Assessment will lapse upon failure to annually affirm • Entered into SPRS
Level 2 (C3PAO)	• 110 NIST SP 800-171 R2 required by DFARS clause 252.204-7012	• Conducted by C3PAO every 3 years • Results entered into CMMC Enterprise Mission Assurance Support Service (eMASS) • CMMC Status will be valid for three years from the CMMC Status Date as defined in § 170.4	• Permitted as defined in § 170.21(a)(2) and must be closed out within 180 days • Final CMMC Status will be valid for three years from the Conditional CMMC Status Date	• After each assessment and annually thereafter • Assessment will lapse upon failure to annually affirm • Entered into SPRS
Level 3 (DIBCAC)	• 110 NIST SP 800-171 R2 required by DFARS clause 252.204-7012 • 24 selected from NIST SP 800-172 Feb2021, as detailed in table 1 to § 170.14(c)(4)	• Pre-requisite CMMC Status of Level 2 (C3PAO) for the same CMMC Assessment Scope, for each Level 3 certification assessment • Conducted by DIBCAC every 3 years • Results entered into CMMC eMASS • CMMC Status will be valid for three years from the CMMC Status Date as defined in § 170.4	• Permitted as defined in § 170.21(a)(3) and must be closed out within 180 days • Final CMMC Status will be valid for three years from the Conditional CMMC Status Date	• After each assessment and annually thereafter • Assessment will lapse upon failure to annually affirm • Level 2 (C3PAO) affirmation must also continue to be completed annually • Entered into SPRS

IMMEDIATE (1 MONTH)

- Brief Executive Sponsors
- Recruit team members and finalize charter
- Develop and issue OPORD
- Initiate and issue recurring SAM.gov announcement from HQ
- Develop plug/fill SAM.gov template for use by Districts/Centers
- Webinars: SCOs, RBDs, RPDs, BoBs, KOs
- Develop CMMC flowchart for UAI
- Develop USACE webinar deck
- Develop DIB webinar deck
- Develop Steering Committee IPR template
- HCA email to CT CoP with WARNO and status update
- Conduct IPR #1 with Steering Committee

NEAR TERM (2 MONTH)

- Baseline readiness survey w/ key stakeholder groups
- Webinar: E&C Chiefs
- Webinar: Civilian Deputies (DPMs)
- Develop UAI section for CUI
- Develop UAI section for CMMC
- Update UAI checklists to incorporate CUI and CMMC
- List of active DIB contractors, by USACE org, to CoCOs/DPMs
- CMMC PgM email to CT CoP with status update and DIB list
- HCA email to CT CoP reinforcing OPORD, roles & responsibilities
- Conduct IPR #2 with Steering Committee

SHORT TERM (3 MONTH)

- Incorporate final SF XXX into the UAI
- Issue FRAGO to incorporate SF XXX into HQ guidance
- Brief USACE governance forums: DR-C, BR-C, and ER-C
- Conduct IPR #3 with Steering Committee

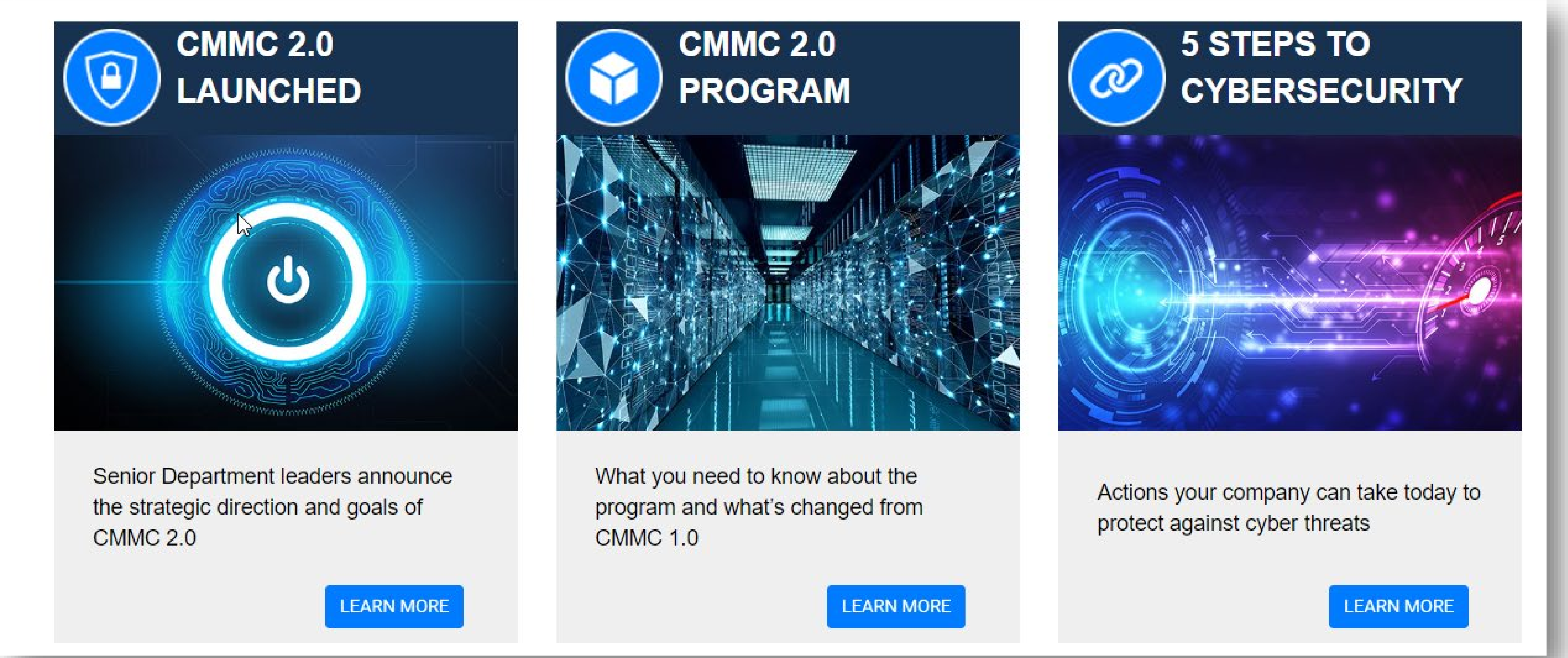
MEDIUM TERM (6 MONTH)

- Capture metrics, report status and compliance in monthly IPRs
- Monitor progress across Districts/Divisions; adjust as needed
- Conduct monthly IPRs with Steering Committee

LONG TERM (FY26 – FY28)

- Develop/field INFOSEC PROSPECT course
- Monthly CT data calls, by org, for non-responsive DIB eliminations
- Monthly BI audit of awards to validate CMMC Level 1 compliance
- Monthly cycle time audit for CMMC waiver requests to HCA
- Monthly report to Director on metrics and compliance
- Bi-annual IPRs with Steering Committee

HTTPS://DODCIO.DEFENSE.GOV/CMMC/



CMMC 2.0 LAUNCHED

Senior Department leaders announce the strategic direction and goals of CMMC 2.0

CMMC 2.0 PROGRAM

What you need to know about the program and what's changed from CMMC 1.0

5 STEPS TO CYBERSECURITY

Actions your company can take today to protect against cyber threats