CMMC IS FINALIZED CMMC IS FINALIZED CMMC IS FINALIZED CMMC IS FINALIZED CMMC IS FINALIZE

SUMMIT7

Live Webinar

# 32 CFR CMMC: Finalized

This is it.
So, now what?

November 7th, 2024 I 10:30 AM CT

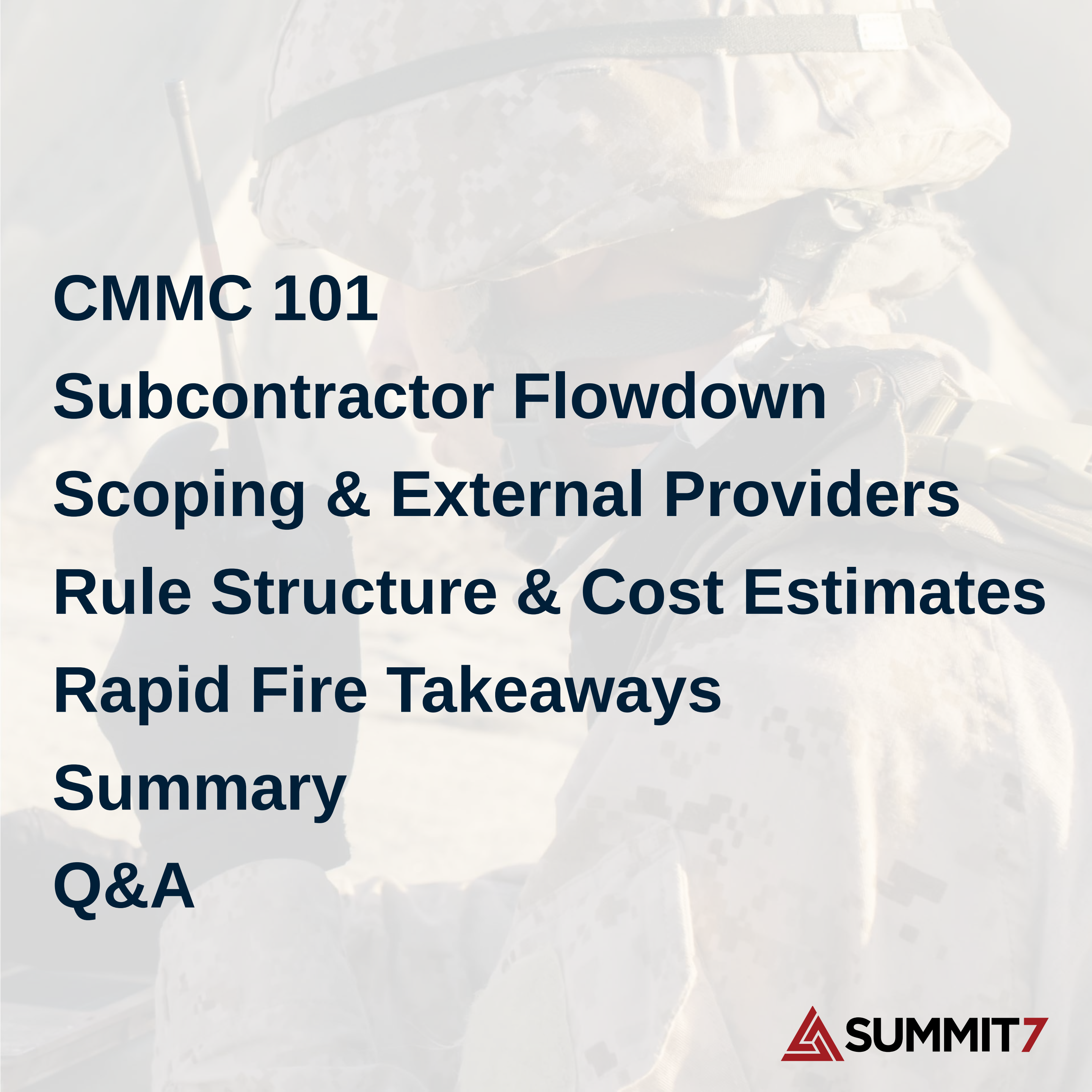
## Presenters:

**Jacob Horne**
*Chief Cybersecurity Evangelist*

**Scott Edwards**
*CEO*

ALIZED CMMC IS FINALIZED CMMC IS FINALIZED CMMC IS FINALIZED CMMC IS FINALIZED CMMC IS FIN

# Agenda



01 CMMC 101

02 Subcontractor Flowdown

03 Scoping & External Providers

04 Rule Structure & Cost Estimates

05 Rapid Fire Takeaways

06 Summary

07 Q&A

SUMMIT7

# CMMC 101

The major elements of a major rule

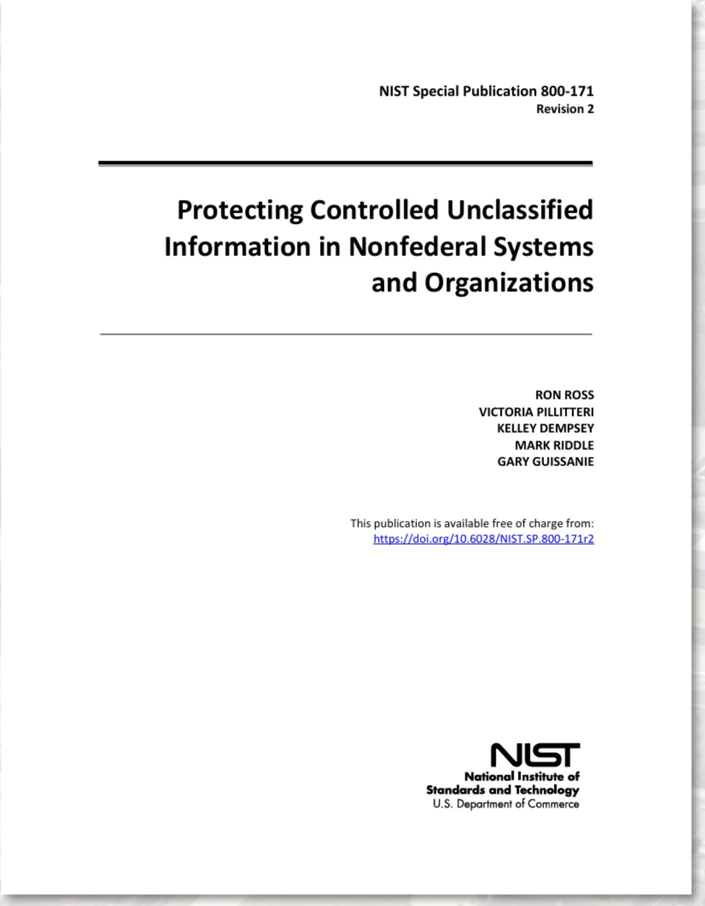
SUMMIT7

# CMMC is a program that verifies cybersecurity requirements

Cybersecurity requirements are imposed through contract clauses

# Those requirements are documented in NIST publications

NIST: The National Institute of Standards and Technology



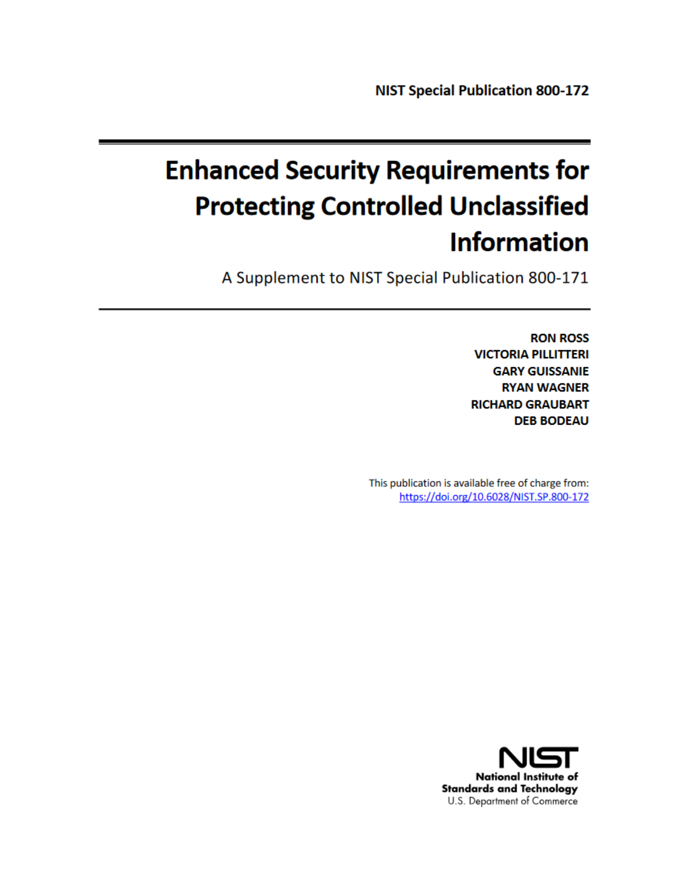
NIST Special Publication 800-171
Revision 2

## Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

RON ROSS
VICTORIA PILLITTERI
KELLEY DEMPSEY
MARK RIDDLE
GARY GUISSANIE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-171r2

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce



NIST Special Publication 800-172

## Enhanced Security Requirements for Protecting Controlled Unclassified Information

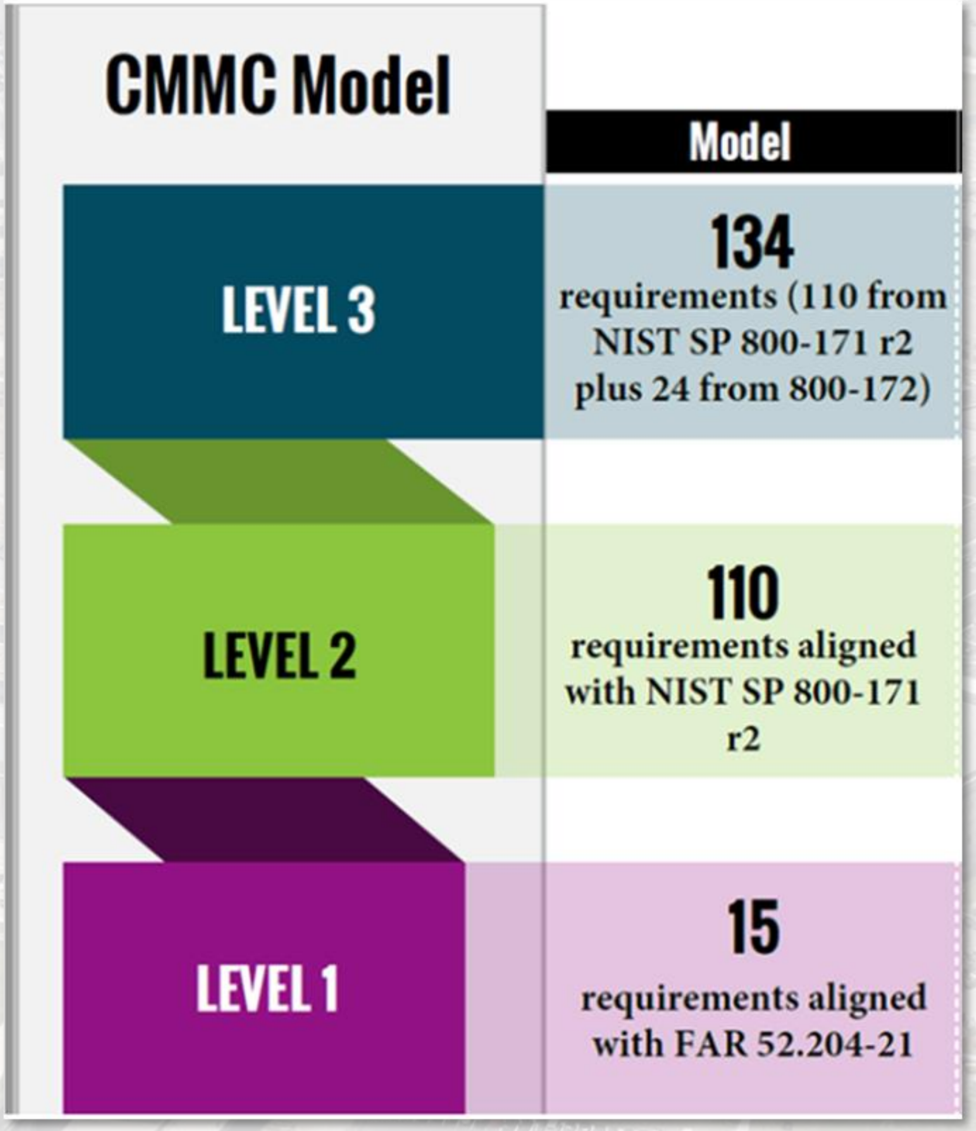
A Supplement to NIST Special Publication 800-171

RON ROSS
VICTORIA PILLITTERI
GARY GUISSANIE
RYAN WAGNER
RICHARD GRAUBART
DEB BODEAU

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-172

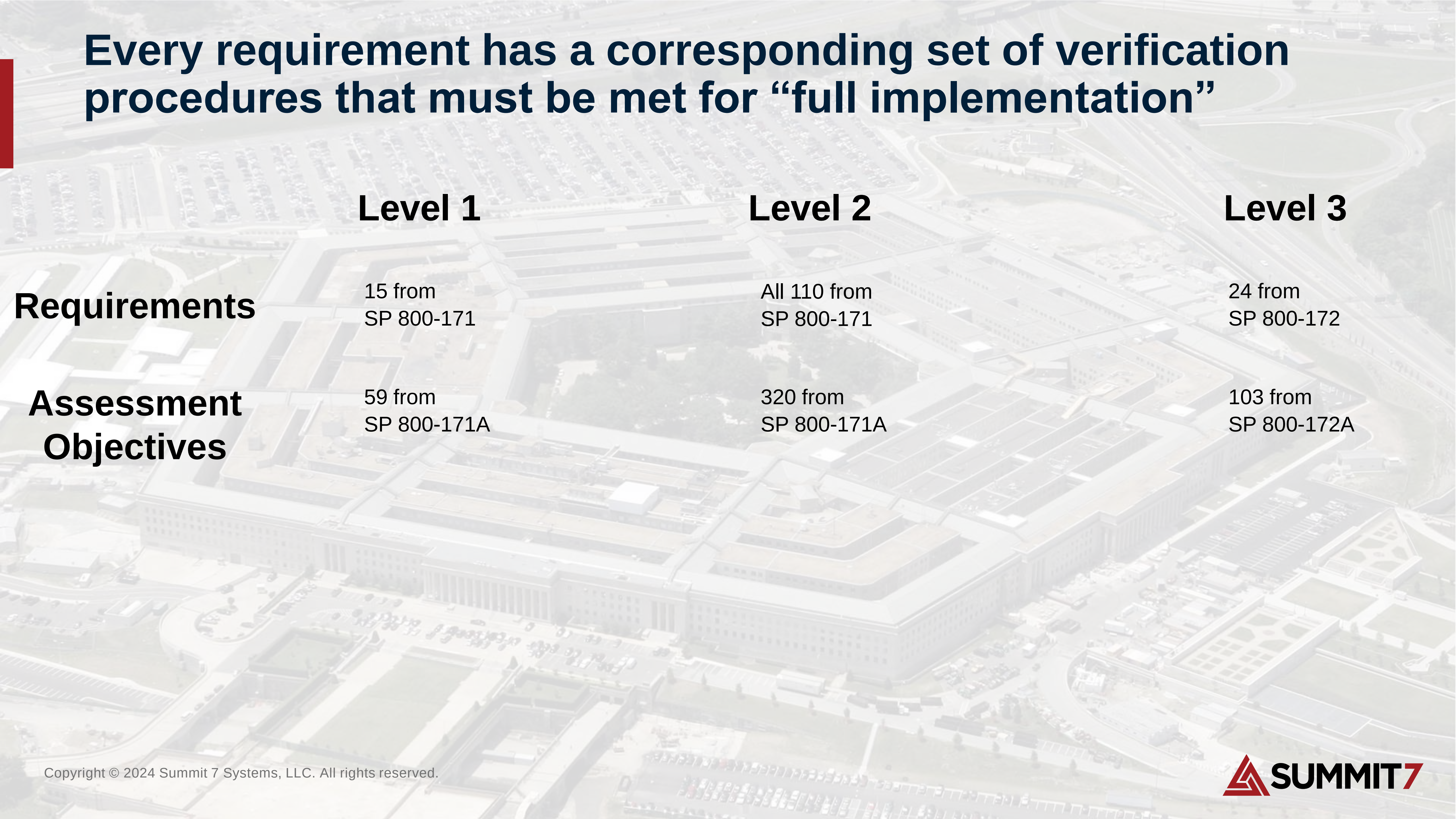
NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

# The CMMC model has 3 levels that correspond to the requirements it verifies



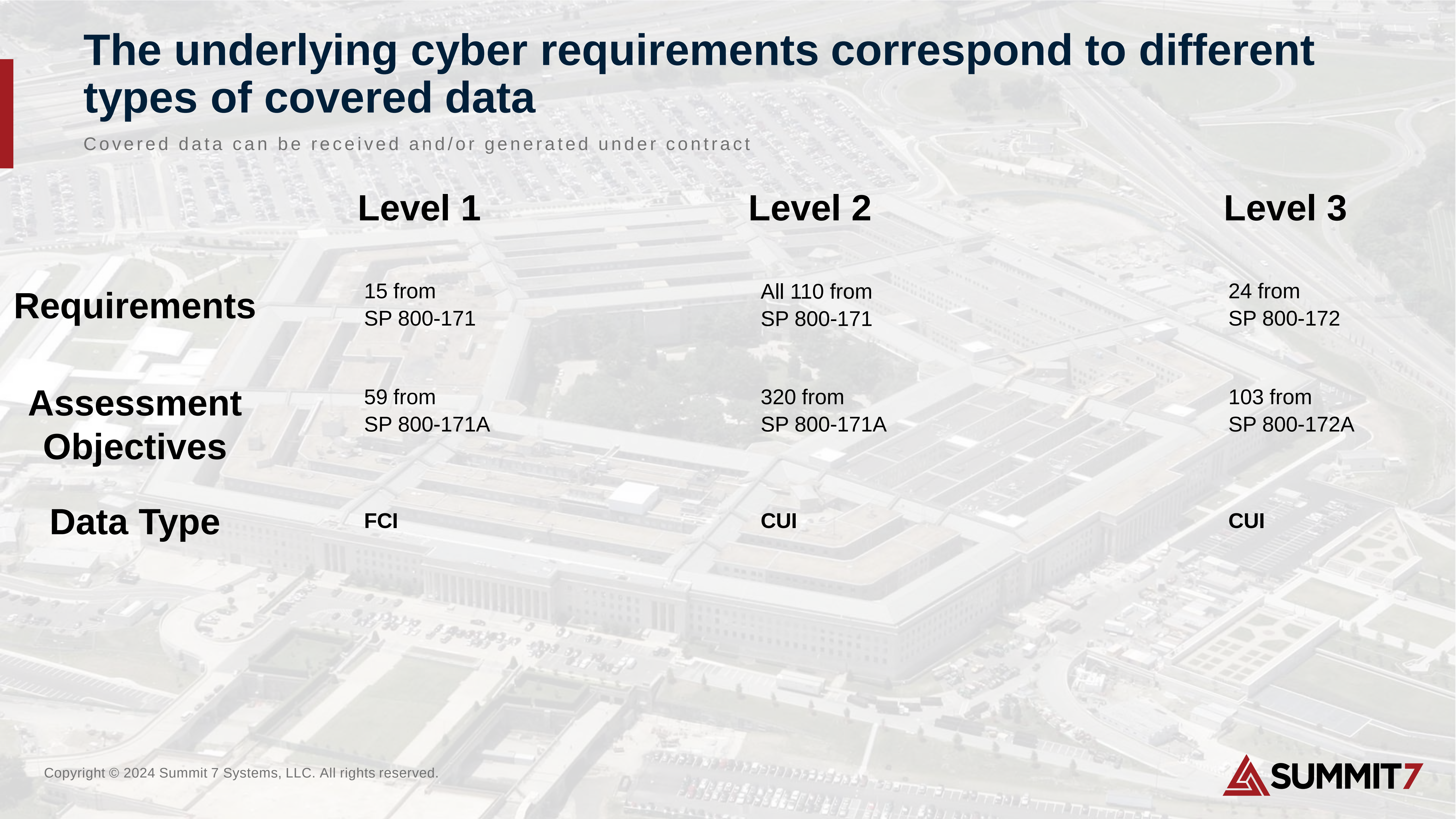
| CMMC Model | Model |
|---|---|
| LEVEL 3 | **134**<br>requirements (110 from NIST SP 800-171 r2 plus 24 from 800-172) |
| LEVEL 2 | **110**<br>requirements aligned with NIST SP 800-171 r2 |
| LEVEL 1 | **15**<br>requirements aligned with FAR 52.204-21 |

# Every requirement has a corresponding set of verification procedures that must be met for “full implementation”



|  | Level 1 | Level 2 | Level 3 |
|---|---|---|---|
| **Requirements** | 15 from<br>SP 800-171 | All 110 from<br>SP 800-171 | 24 from<br>SP 800-172 |
| **Assessment Objectives** | 59 from<br>SP 800-171A | 320 from<br>SP 800-171A | 103 from<br>SP 800-172A |

SUMMIT7

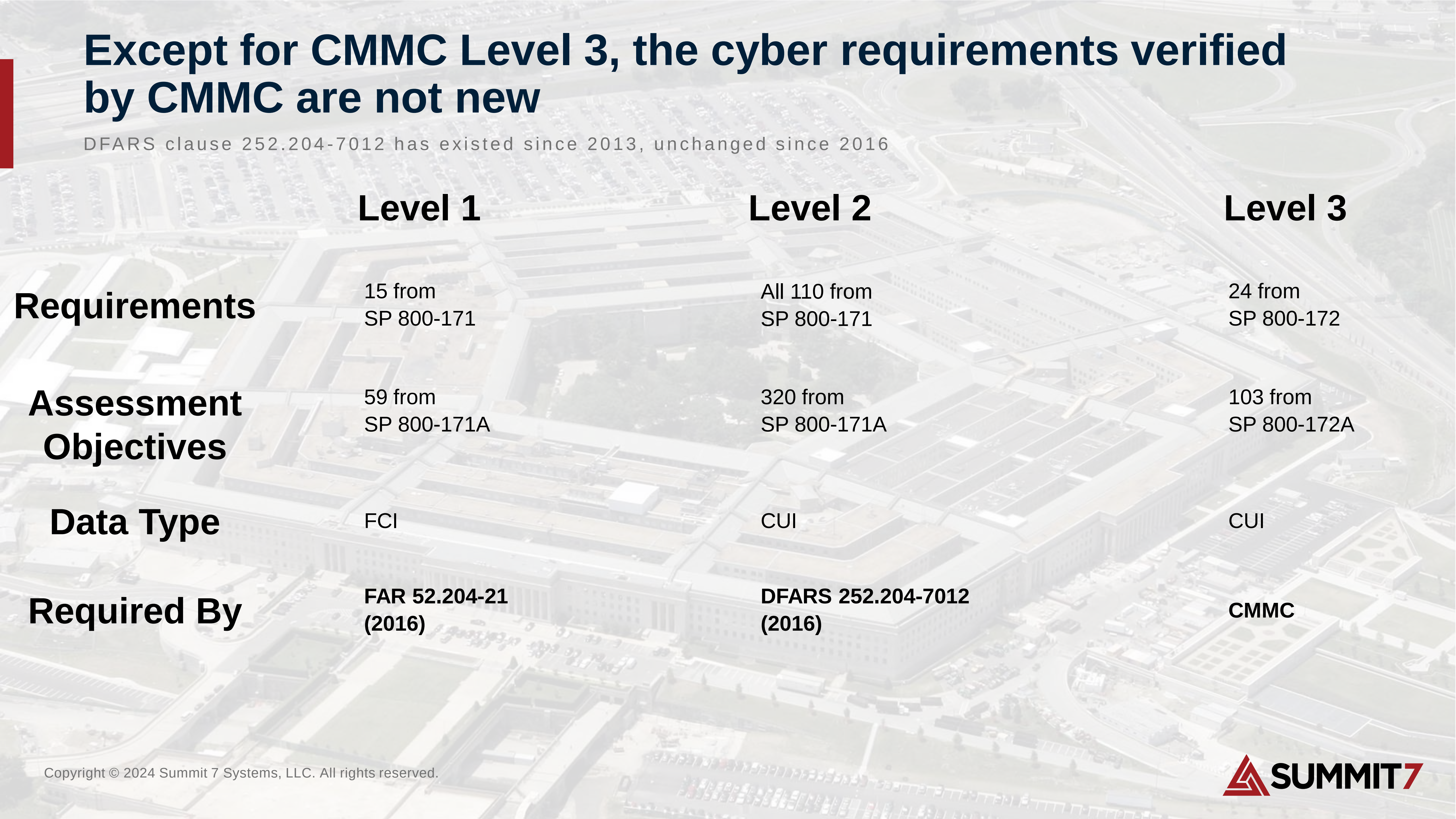


# The underlying cyber requirements correspond to different types of covered data

Covered data can be received and/or generated under contract

| | Level 1 | Level 2 | Level 3 |
|---|---|---|---|
| **Requirements** | 15 from<br>SP 800-171 | All 110 from<br>SP 800-171 | 24 from<br>SP 800-172 |
| **Assessment Objectives** | 59 from<br>SP 800-171A | 320 from<br>SP 800-171A | 103 from<br>SP 800-172A |
| **Data Type** | **FCI** | **CUI** | **CUI** |

SUMMIT7



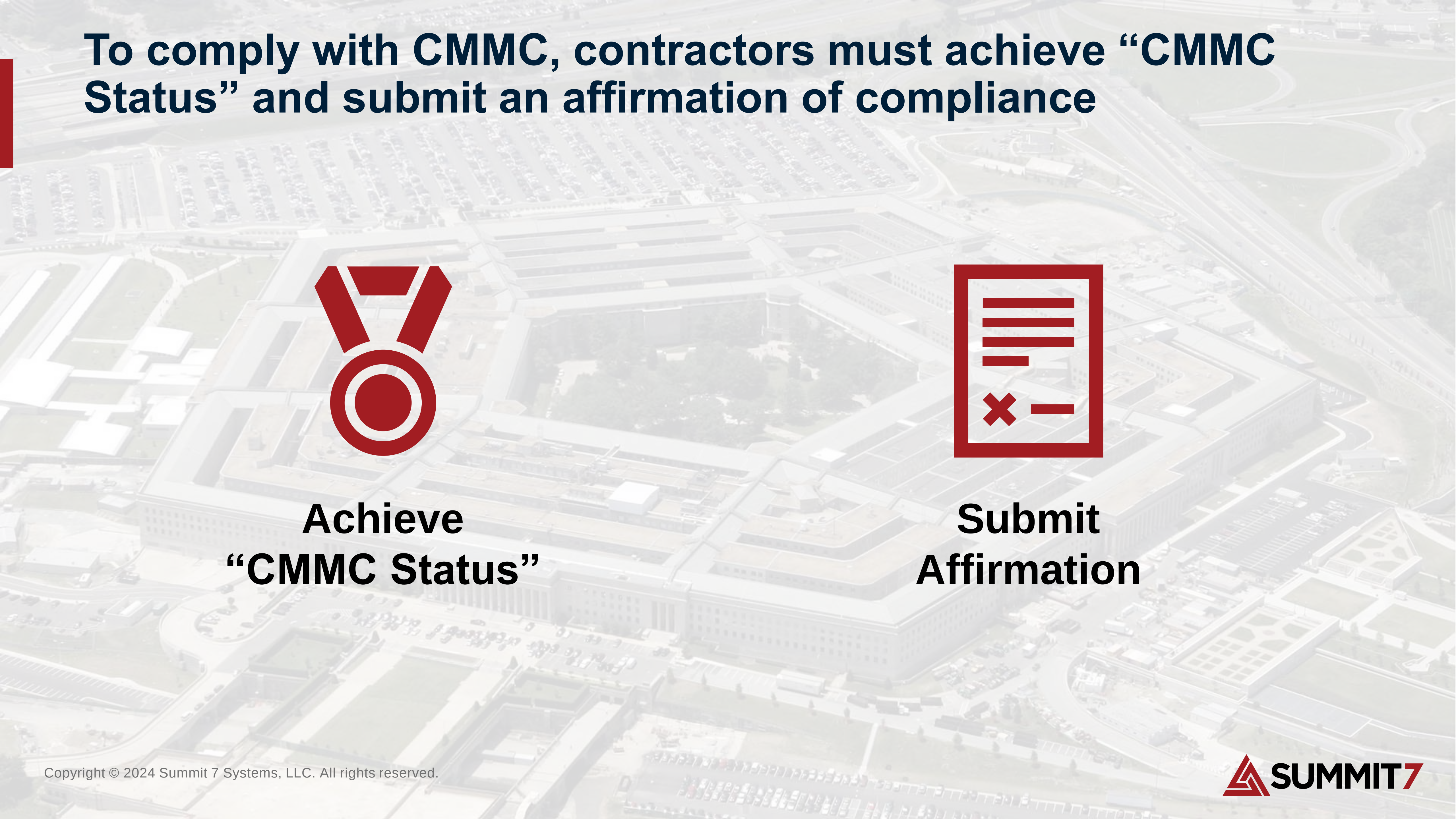
# Except for CMMC Level 3, the cyber requirements verified by CMMC are not new

DFARS clause 252.204-7012 has existed since 2013, unchanged since 2016

| | Level 1 | Level 2 | Level 3 |
|---|---|---|---|
| **Requirements** | 15 from<br>SP 800-171 | All 110 from<br>SP 800-171 | 24 from<br>SP 800-172 |
| **Assessment Objectives** | 59 from<br>SP 800-171A | 320 from<br>SP 800-171A | 103 from<br>SP 800-172A |
| **Data Type** | FCI | CUI | CUI |
| **Required By** | **FAR 52.204-21<br>(2016)** | **DFARS 252.204-7012<br>(2016)** | **CMMC** |

SUMMIT7

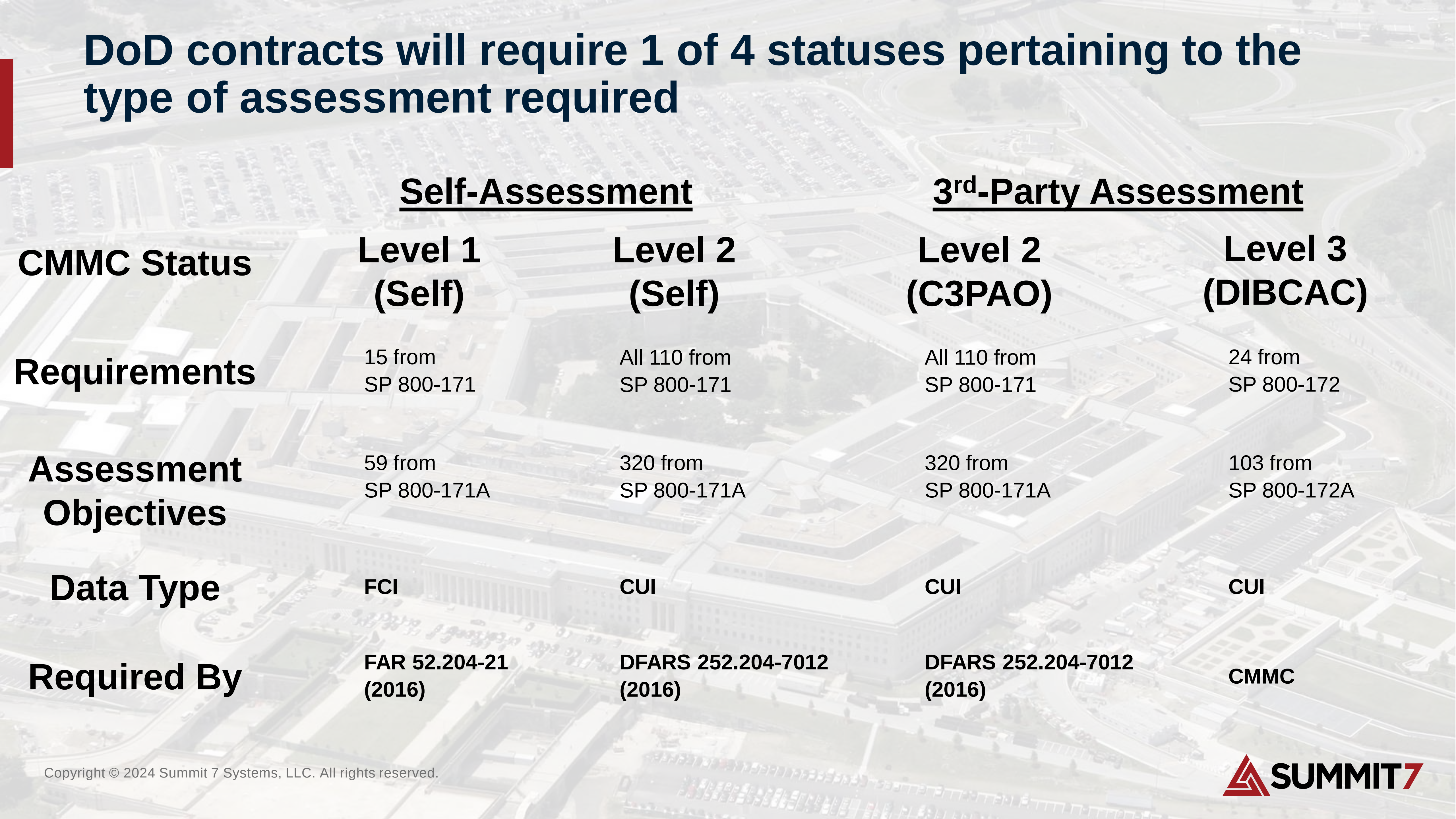
# To comply with CMMC, contractors must achieve “CMMC Status” and submit an affirmation of compliance



Achieve
“CMMC Status”

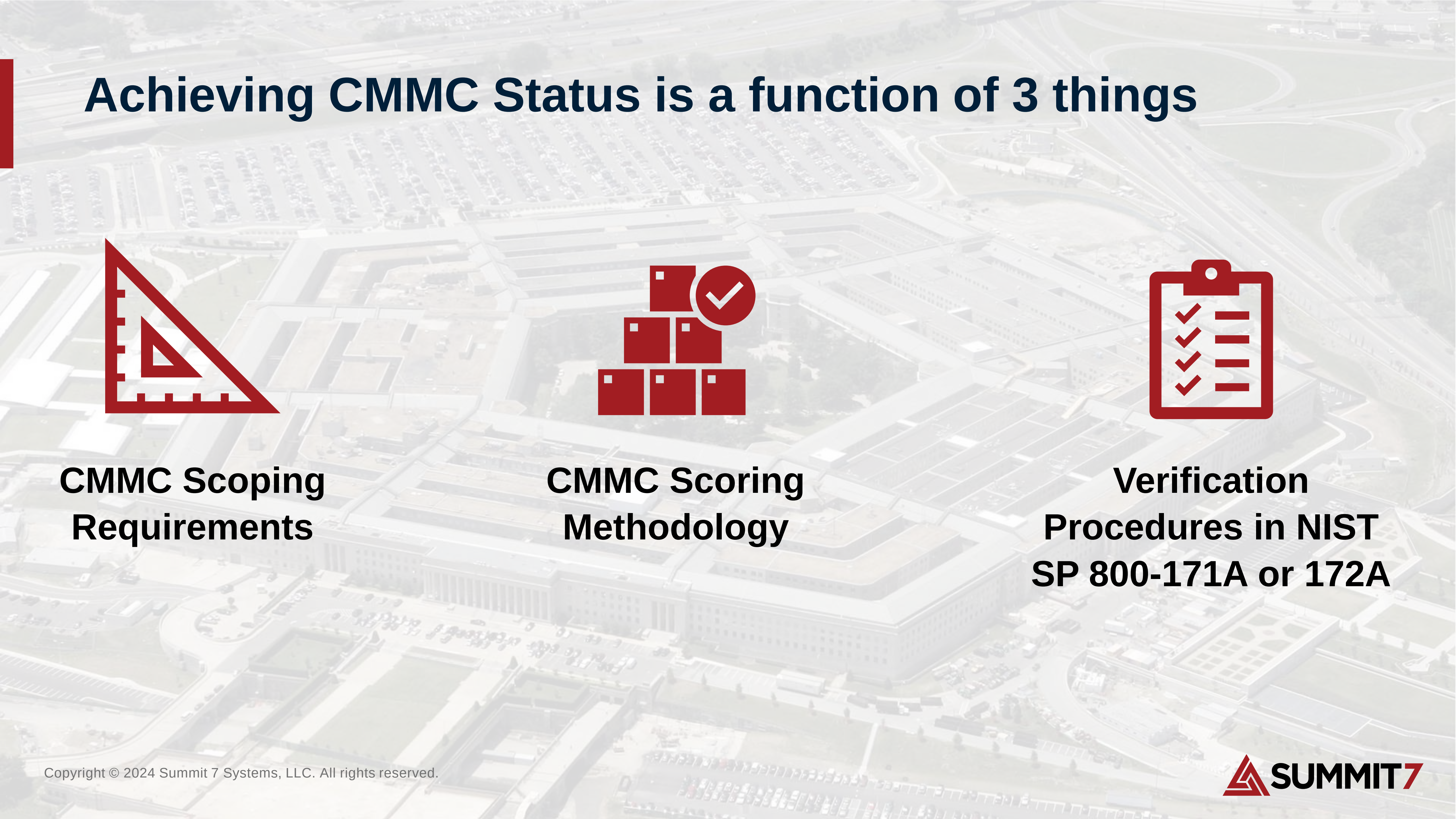
Submit
Affirmation

# DoD contracts will require 1 of 4 statuses pertaining to the type of assessment required



| | **Self-Assessment** | | **3rd-Party Assessment** | |
|---|---|---|---|---|
| **CMMC Status** | **Level 1 (Self)** | **Level 2 (Self)** | **Level 2 (C3PAO)** | **Level 3 (DIBCAC)** |
| **Requirements** | 15 from SP 800-171 | All 110 from SP 800-171 | All 110 from SP 800-171 | 24 from SP 800-172 |
| **Assessment Objectives** | 59 from SP 800-171A | 320 from SP 800-171A | 320 from SP 800-171A | 103 from SP 800-172A |
| **Data Type** | **FCI** | **CUI** | **CUI** | **CUI** |
| **Required By** | **FAR 52.204-21 (2016)** | **DFARS 252.204-7012 (2016)** | **DFARS 252.204-7012 (2016)** | **CMMC** |

SUMMIT7



# Achieving CMMC Status is a function of 3 things

CMMC Scoping Requirements

CMMC Scoring Methodology

Verification Procedures in NIST SP 800-171A or 172A

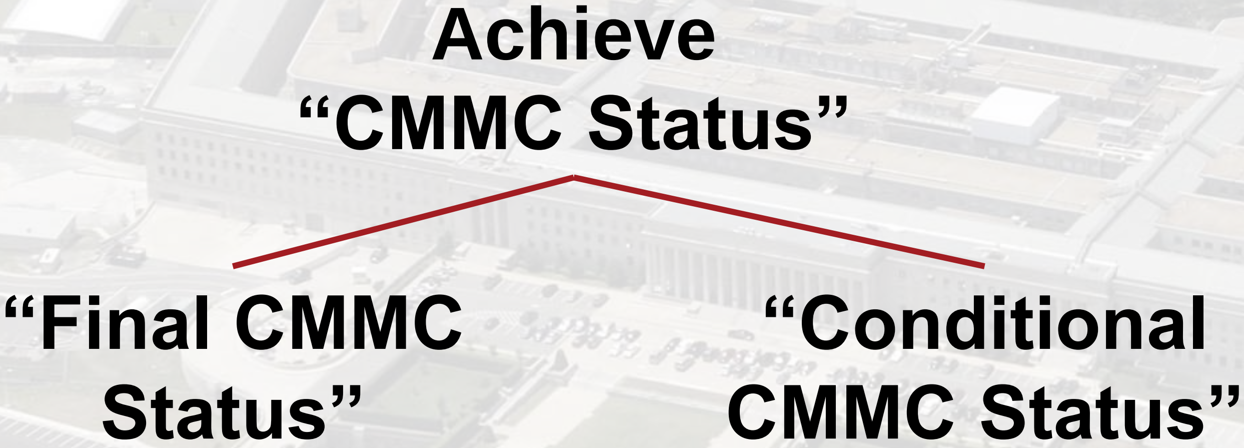
# CMMC Scoring Methodology (§ 170.24)

- Level 1: Score not required; either **MET** or **NOT MET**
- Level 2: Security requirements are valued 1, 3, or 5 points with a range of -203 to 110, with a minimum passing score of 88. Partial credit is allowed for 2 requirements:
  - MFA: 5 points deducted from overall score of 110 if MFA is not implemented or implemented only for general users and not remote and privileged users;
  - MFA: 3 points deducted if MFA is implemented for remote and privileged users but not implemented for general users;
  - FIPS: 5 points deducted from overall score of 110 if no cryptography is employed;
  - FIPS: 3 points deducted if cryptography is employed, but not FIPS validated.
- Level 3: All Level 3 security requirements are valued 1 point with a maximum score of 24. Requires a prerequisite Level 2 score of 110.
- Results for all Levels are posted in SPRS and reviewed by contracting officers and requiring activities.

https://dodcio.defense.gov/cmmc/Resources-Documentation/

# Limited POA&Ms are allowed at CMMC Levels 2 & 3

POA&Ms are not allowed at CMMC Level 1



Achieve “CMMC Status”

“Final CMMC Status”

“Conditional CMMC Status”

Submit Affirmation

SUMMIT7

# CMMC Post-Assessment Remediation

## ❑ CMMC Program will allow limited use of POA&Ms

- POA&Ms are not allowed for CMMC Level 1.
- Refer to § 170.21 of the 32 CFR CMMC Program final rule for CMMC Level 2 and Level 3 POA&Ms requirements, including critical requirements not allowed in a POA&M.

## ❑ Closeout Assessment

- POA&M closeout Self-Assessment is conducted by the OSA.
- POA&M closeout Certification Assessment is conducted by a C3PAO or the DIBCAC.
- POA&Ms must be closed out within 180 days of when the CMMC Assessment results are finalized and submitted to SPRS or CMMC eMASS, as appropriate.

**Failure to close POA&M within 180 days will result in an expired CMMC Status**

https://dodcio.defense.gov/cmmc/Resources-Documentation/

# Contractors must also submit an affirmation of compliance after every assessment and annually thereafter

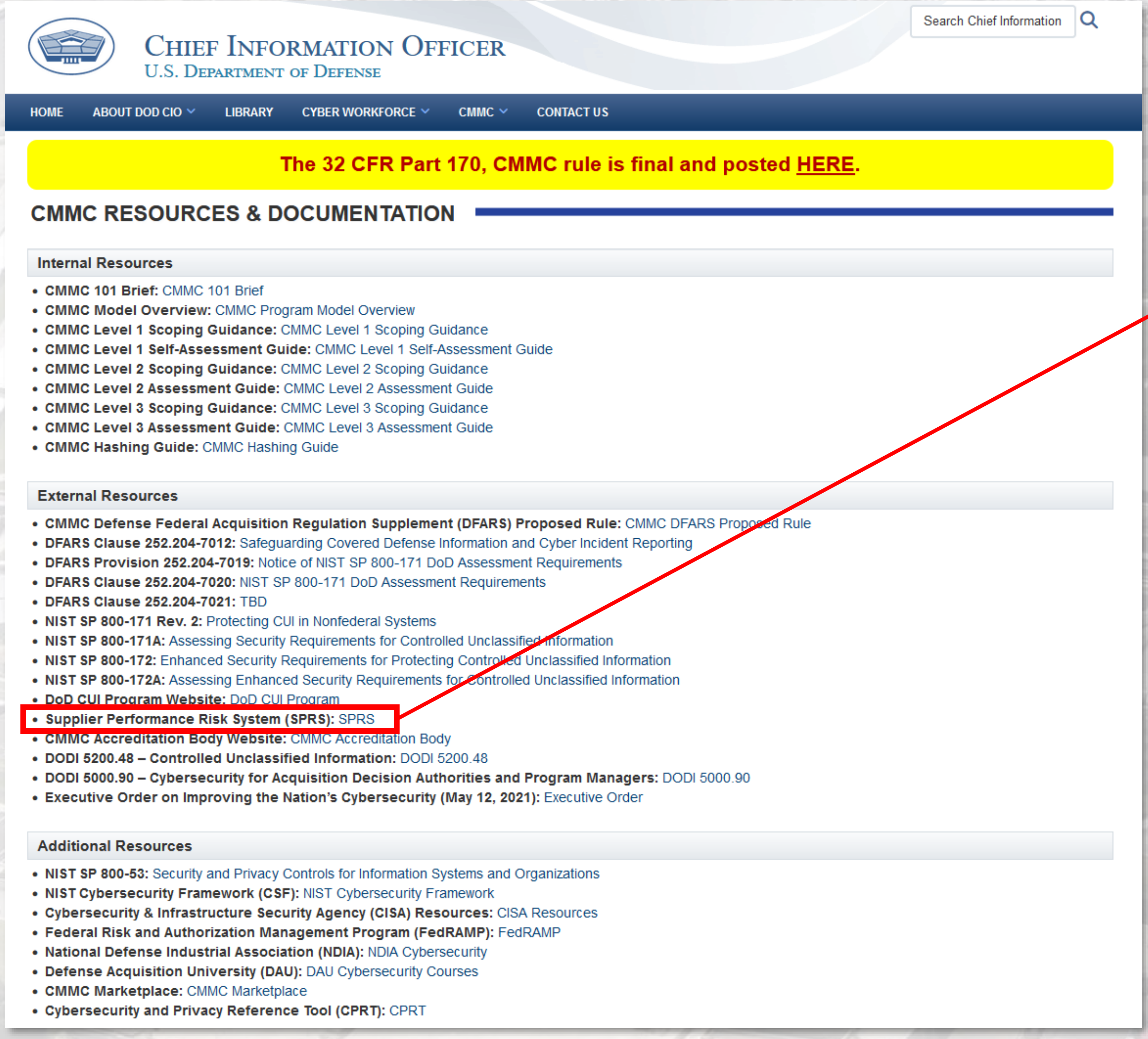
**Affirming Official:** The senior level representative within each OSA who is:

- Responsible for ensuring the OSA’s compliance with the CMMC program requirements and
- Has the authority to affirm the OSA’s continuing compliance

The DoD will verify submission of the affirmation to ensure compliance with CMMC solicitation or contract requirements.

# Assessment results and affirmations are uploaded to the Supplier Performance Risk System (SPRS)

3rd-party assessments results are uploaded to eMASS and transmitted to SPRS



The 32 CFR Part 170, CMMC rule is final and posted HERE.

## CMMC RESOURCES & DOCUMENTATION

### Internal Resources

- **CMMC 101 Brief:** CMMC 101 Brief
- **CMMC Model Overview:** CMMC Program Model Overview
- **CMMC Level 1 Scoping Guidance:** CMMC Level 1 Scoping Guidance
- **CMMC Level 1 Self-Assessment Guide:** CMMC Level 1 Self-Assessment Guide
- **CMMC Level 2 Scoping Guidance:** CMMC Level 2 Scoping Guidance
- **CMMC Level 2 Assessment Guide:** CMMC Level 2 Assessment Guide
- **CMMC Level 3 Scoping Guidance:** CMMC Level 3 Scoping Guidance
- **CMMC Level 3 Assessment Guide:** CMMC Level 3 Assessment Guide
- **CMMC Hashing Guide:** CMMC Hashing Guide

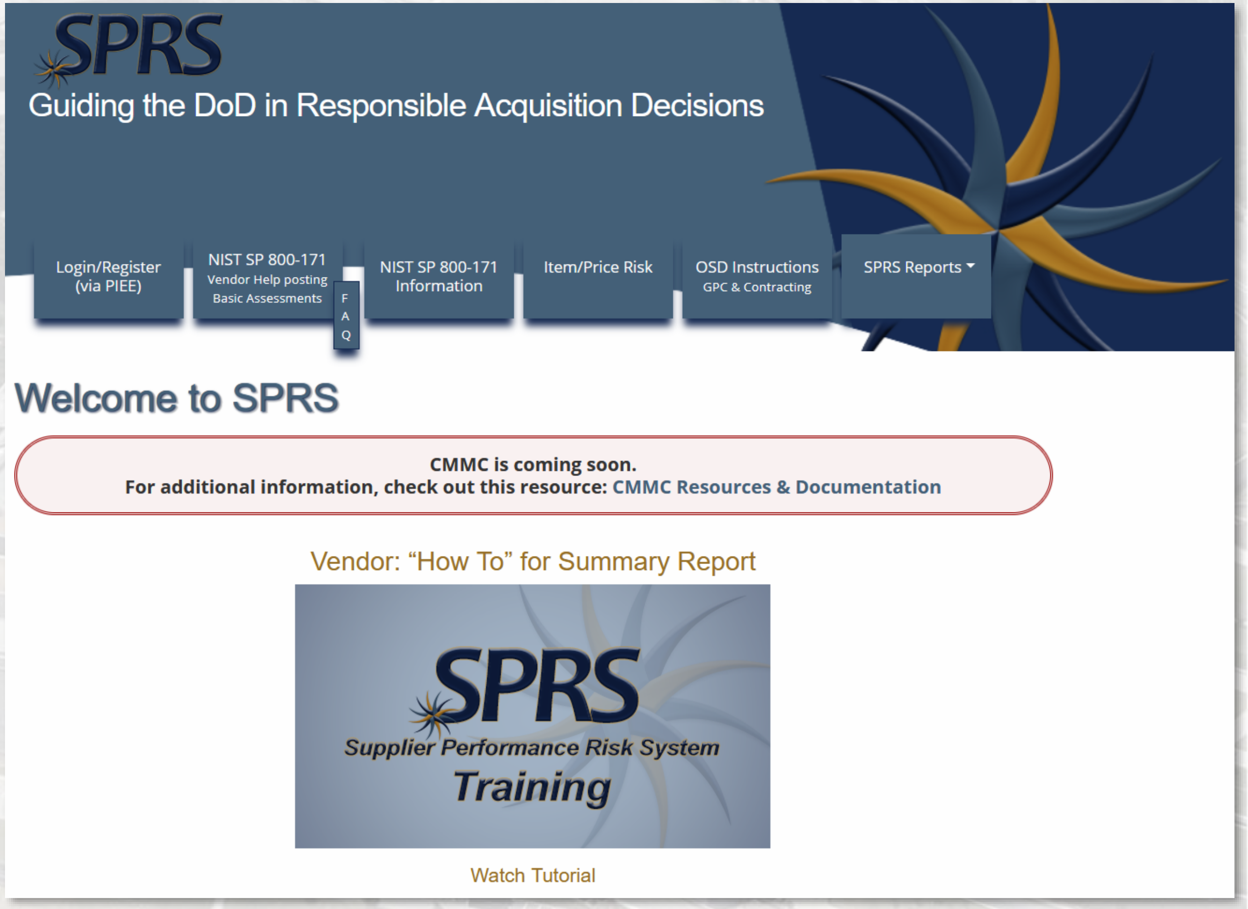
### External Resources

- **CMMC Defense Federal Acquisition Regulation Supplement (DFARS) Proposed Rule:** CMMC DFARS Proposed Rule
- **DFARS Clause 252.204-7012:** Safeguarding Covered Defense Information and Cyber Incident Reporting
- **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:** TBD
- **NIST SP 800-171 Rev. 2:** Protecting CUI in Nonfederal Systems
- **NIST SP 800-171A:** Assessing Security Requirements for Controlled Unclassified Information
- **NIST SP 800-172:** Enhanced Security Requirements for Protecting Controlled Unclassified Information
- **NIST SP 800-172A:** Assessing Enhanced Security Requirements for Controlled Unclassified Information
- **DoD CUI Program Website:** DoD CUI Program
- **Supplier Performance Risk System (SPRS):** SPRS
- **CMMC Accreditation Body Website:** CMMC Accreditation Body
- **DODI 5200.48 – Controlled Unclassified Information:** DODI 5200.48
- **DODI 5000.90 – Cybersecurity for Acquisition Decision Authorities and Program Managers:** DODI 5000.90
- **Executive Order on Improving the Nation's Cybersecurity (May 12, 2021):** Executive Order

### Additional Resources

- **NIST SP 800-53:** Security and Privacy Controls for Information Systems and Organizations
- **NIST Cybersecurity Framework (CSF):** NIST Cybersecurity Framework
- **Cybersecurity & Infrastructure Security Agency (CISA) Resources:** CISA Resources
- **Federal Risk and Authorization Management Program (FedRAMP):** FedRAMP
- **National Defense Industrial Association (NDIA):** NDIA Cybersecurity
- **Defense Acquisition University (DAU):** DAU Cybersecurity Courses
- **CMMC Marketplace:** CMMC Marketplace
- **Cybersecurity and Privacy Reference Tool (CPRT):** CPRT

https://dodcio.defense.gov/cmmc/Resources-Documentation/


SPRS
Guiding the DoD in Responsible Acquisition Decisions
Login/Register (via PIEE)
NIST SP 800-171 Vendor Help posting Basic Assessments
FAQ
NIST SP 800-171 Information
Item/Price Risk
OSD Instructions GPC & Contracting
SPRS Reports
SPRS
Supplier Performance Risk System
Training

## Welcome to SPRS

CMMC is coming soon.
For additional information, check out this resource: CMMC Resources & Documentation

Vendor: "How To" for Summary Report

Watch Tutorial

https://www.sprs.csd.disa.mil/

SUMMIT7

# Additional CMMC features to be aware of

- The DoD reserves the right to conduct DIBCAC assessments as provided for under DFARS clause 252.204-7020.
- Contractors are required to retain artifacts used in assessments for six years.
- There are no exceptions based on business size.
- Waivers are for entire contracts, not individual contractors.

“The decision to rely upon a CMMC Level 2 self-assessment in lieu of a certification assessment is a Government risk-based decision based upon the nature of the effort to be performed and CUI to be shared.

The size of the company with access to the CUI is not a basis for this determination.

The value of information and impact of its loss does not diminish when the information moves to contractors of smaller size.”

**32 CMMC 170 Preamble**

> “Once applicable to a solicitation, there is no process for OSAs to seek waivers of CMMC requirements from the DoD CIO.”

**32 CMMC 170 Preamble**

# CMMC 101

How many will be affected? Who decides? When?

SUMMIT7

# CMMC will affect all defense contractors and subcontractors in some way

Except for awards below the micro-purchase threshold ($10k) and purely COTS products

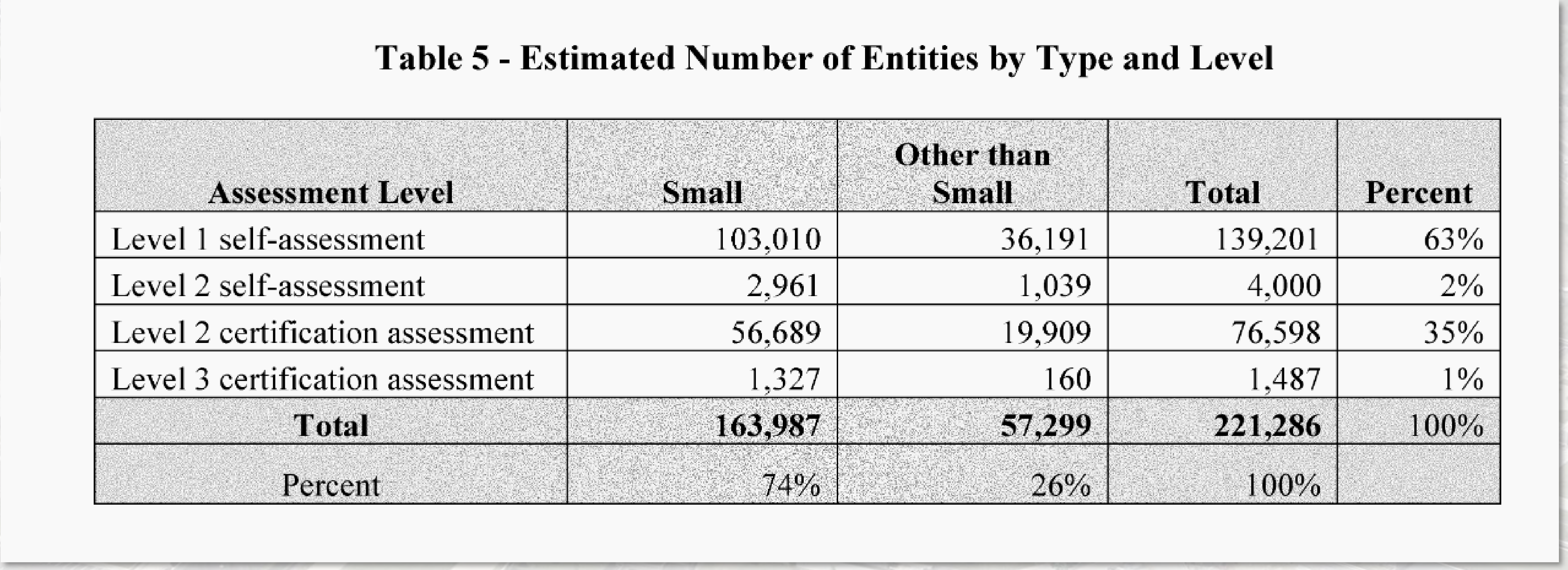


**Table 5 - Estimated Number of Entities by Type and Level**

| Assessment Level | Small | Other than Small | Total | Percent |
|---|---|---|---|---|
| Level 1 self-assessment | 103,010 | 36,191 | 139,201 | 63% |
| Level 2 self-assessment | 2,961 | 1,039 | 4,000 | 2% |
| Level 2 certification assessment | 56,689 | 19,909 | 76,598 | 35% |
| Level 3 certification assessment | 1,327 | 160 | 1,487 | 1% |
| **Total** | **163,987** | **57,299** | **221,286** | 100% |
| Percent | 74% | 26% | 100% | |

# DoD program managers and requiring activities will select the CMMC status that will apply to a procurement

Criticality of the associated mission capability

Type of acquisition program or technology

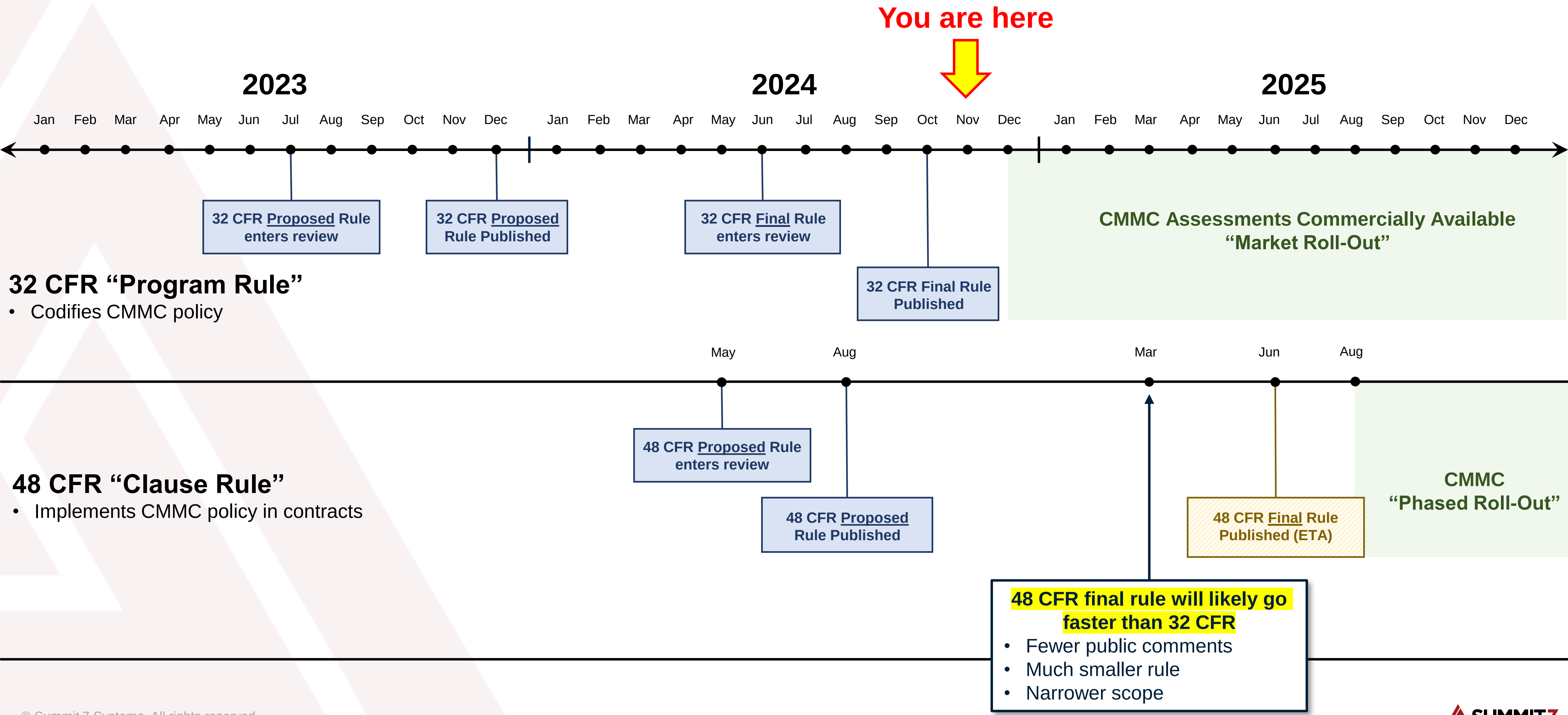
Threat of loss of the FCI or CUI to be shared or generated

Impacts from exploitation of information security deficiencies

Other relevant policies and factors, including Milestone Decision Authority guidance

# 32 CFR CMMC will go into effect 12/16/2024

If the 48 CFR final rule takes as long as 32 CFR, the CMMC phased roll-out will start in August 2025



32 CFR **Proposed** Rule enters review

32 CFR **Proposed** Rule Published

32 CFR **Final** Rule enters review

32 CFR Final Rule Published

CMMC Assessments Commercially Available “Market Roll-Out”

## 32 CFR “Program Rule”

- Codifies CMMC policy

48 CFR **Proposed** Rule enters review

48 CFR **Proposed** Rule Published

48 CFR **Final** Rule Published (ETA)

CMMC “Phased Roll-Out”

## 48 CFR “Clause Rule”

- Implements CMMC policy in contracts

**48 CFR final rule will likely go faster than 32 CFR**

- Fewer public comments
- Much smaller rule
- Narrower scope

# DoD’s phased roll-out and yearly assessment estimates are based on the 48 CFR final rule timeline rather than the 32 CFR final rule

◔

## Phase 1
## ETA: Q2 2025

**Begins on the effective date of the 48 CFR CMMC Rule***

**Level 1 and Level 2 self-assessment** requirements included in all applicable solicitations and contracts as a condition of award**

*DoD discretion: prior to effective date of 48 CFR CMMC

**DoD discretion: Level 2 certification in place of self-assessment

◑

## Phase 2
## ETA: Q2 2026

**Begins 1 calendar year after the start of Phase 1***

**CMMC Level 2** certification in all applicable solicitations and contracts as condition of award**

*DoD discretion: delay inclusion of L2 certification to an option period instead of condition of award

**DoD discretion: Level 3 certification instead

◕

## Phase 3
## ETA: Q2 2027

**Begins 1 calendar year after the start of Phase 2***

**CMMC Level 2 certification in all applicable solicitations and contracts as condition of award or exercise of option period.**

**CMMC Level 3 certification* in all applicable solicitations and contracts as condition of award.**

*DoD discretion: delay inclusion of L3 certification to an option period instead of condition of award

●

## Phase 4
## ETA: Q2 2028

**Begins 1 calendar year after the start of Phase 3**

**CMMC in all applicable solicitations and contracts including options periods on contracts awarded prior to Phase 4.**

# Subcontractor Flow Down

The false hope of CMMC Level 2 Self-Assessment

# If your prime needs Level 2 (C3PAO) status, you will too

The odds of avoiding 3rd-party assessment are too high to gamble on

## From § 170.23 Application to subcontractors

CMMC requirements apply to prime contractors and subcontractors throughout the supply chain at all tiers that will process, store, or transmit any FCI or CUI on contractor information systems in the performance of the DoD contract or subcontract.

Prime contractors shall comply and shall require subcontractors to comply with and to flow down CMMC requirements, such that compliance will be required throughout the supply chain at all tiers with the applicable CMMC level and assessment type for each subcontract as follows…

**If a subcontractor will process, store, or transmit CUI in performance of the subcontract and the associated prime contract has a requirement for a CMMC Status of Level 2 (C3PAO), then the CMMC Status of Level 2 (C3PAO) is the minimum requirement for the subcontractor.**

SUMMIT7

# CMMC Scoping and External Service Providers

# CMMC Scoping is based on asset categorization

Asset categories hinge on the flow of covered data in your organization

Table 3 to § 170.19(c)(1)—CMMC Level 2 Asset Categories and Associated Requirements

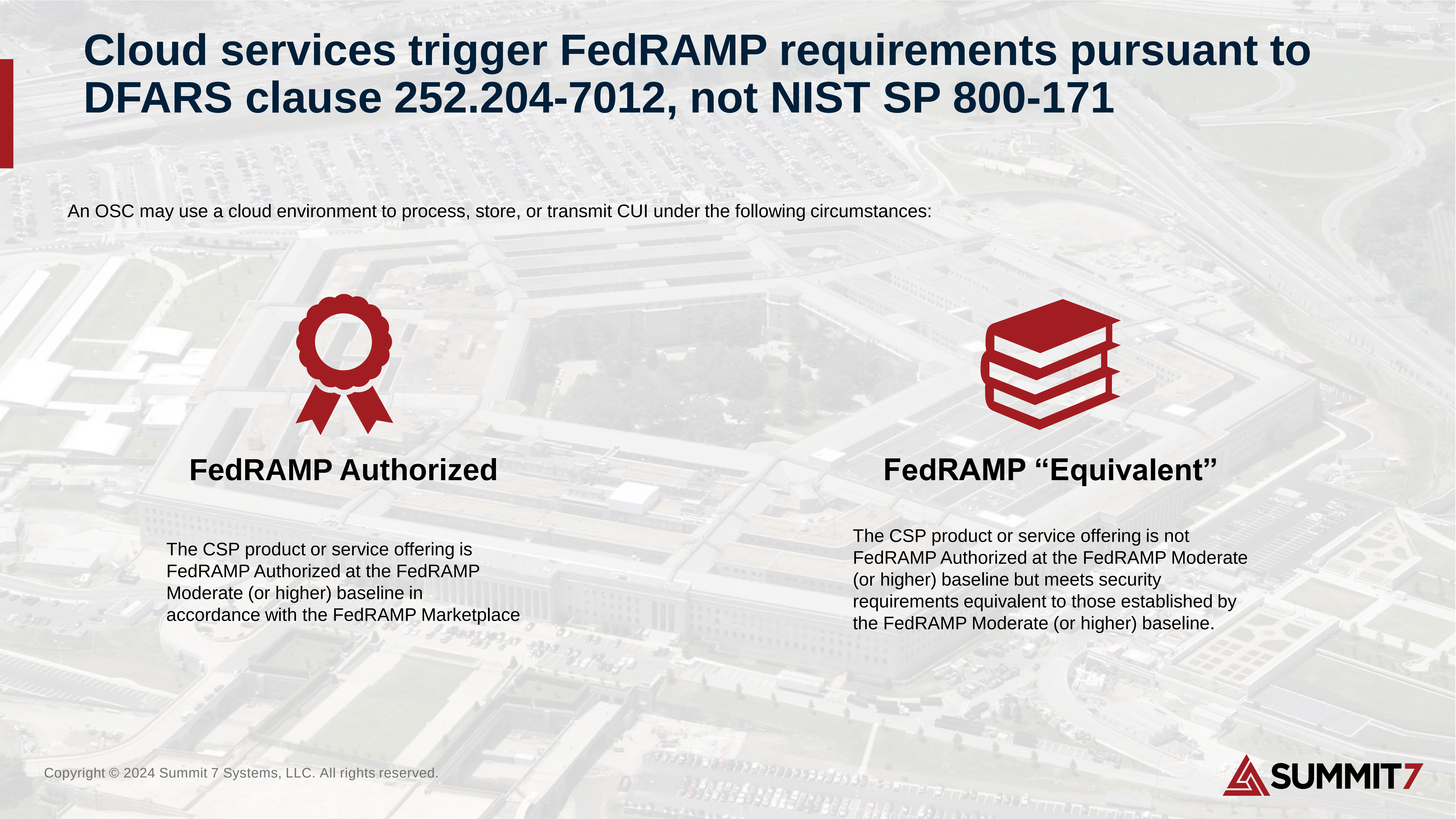
| Asset Category | Asset Description | OSA Requirements | Assessment Reqs | Notes |
|---|---|---|---|---|
| CUI Assets | Assets that process, store, or transmit CUI | • Document in the asset inventory<br>• Document treatment in SSP<br>• Document in network/scope diagram | Assess against all Level 2 security requirements | |
| Security Protection Assets (SPA) | Assets that provide security functions or capabilities to the OSA's CMMC Assessment Scope | • Document in the asset inventory<br>• Document treatment in SSP<br>• Document in network/scope diagram | Assess against all relevant Level 2 security requirements | |
| Contractor Risk Managed Assets (CRMA) | Assets that can, but are not intended to, process, store, or transmit CUI because of security policy, procedures, and practices | • Document in the asset inventory<br>• Document treatment in SSP<br>• Document in network/scope diagram | Review SSP:<br>If sufficient, do not assess<br>Can conduct "limited checks":<br>• Shall not materially increase assessment duration/cost<br>• Conducted against CMMC requirements | Assets are not required to be physically or logically separated from CUI assets. |
| Specialized Assets | Assets that can process, store, or transmit CUI but are unable to be fully secured | • Document in the asset inventory<br>• Document treatment in SSP<br>• Document in network/scope diagram<br>• Show these assets are managed w/ contractor's risk-based treatment | Review SSP<br>Do not assess against CMMC requirements | Examples:<br>• Internet of Things (IoT) devices<br>• Industrial Internet of Things (IIoT) devices<br>• Operational Technology (OT)<br>• Government Furnished Equipment (GFE)<br>• Restricted Information Systems<br>• Test Equipment |
| Out-of-Scope Assets | Assets that cannot process, store, or transmit CUI; and do not provide security protections for CUI Assets | Prepare to justify the inability to process, store, or transmit CUI | None | • Assets that are physically or logically separated from CUI assets<br>• VDI* |

# CMMC Level 3 Scoping is stricter than Level 2

No contractor risk managed assets; Specialized Assets are in-scope

Table 5 to § 170.19(d)(1)—CMMC Level 3 Asset Categories and Associated Requirements

| Asset Category | Asset Description | OSA Requirements | Assessment Reqs | Notes |
|---|---|---|---|---|
| CUI Assets | • Assets that process, store, or transmit CUI<br>• Assets that can, but are not intended to, process, store, or transmit CUI (CRMA) | • Document in the asset inventory<br>• Document treatment in SSP<br>• Document in network/scope diagram | • Limited check against all Level 2 requirements<br>• Assess against all Level 3 requirements | |
| SPA | Assets that provide security functions or capabilities to the OSA's CMMC Assessment Scope | • Document in the asset inventory<br>• Document treatment in SSP<br>• Document in network/scope diagram | • Limited check against all Level 2 requirements<br>• Assess against all relevant Level 3 security requirements | Irrespective of whether or not these assets process, store, or transmit CUI |
| Specialized Assets | Assets that can process, store, or transmit CUI but are unable to be fully secured | • Document in the asset inventory<br>• Document treatment in SSP<br>• Document in network/scope diagram<br>• ~~Show these assets are managed w/ contractor's risk-based treatment~~ | • Limited check against all Level 2 requirements<br>• Assess against all relevant Level 3 security requirements | Intermediary devices are permitted to provide the capability for the specialized asset to meet one or more CMMC security requirements. |
| Out-of-Scope Assets | Assets that cannot process, store, or transmit CUI; and do not provide security protections for CUI Assets | Prepare to justify the inability to process, store, or transmit CUI | None | • Assets that are physically or logically separated from CUI assets<br>• VDI* |



# Cloud services trigger FedRAMP requirements pursuant to DFARS clause 252.204-7012, not NIST SP 800-171

An OSC may use a cloud environment to process, store, or transmit CUI under the following circumstances:

## FedRAMP Authorized

The CSP product or service offering is FedRAMP Authorized at the FedRAMP Moderate (or higher) baseline in accordance with the FedRAMP Marketplace

## FedRAMP “Equivalent”

The CSP product or service offering is not FedRAMP Authorized at the FedRAMP Moderate (or higher) baseline but meets security requirements equivalent to those established by the FedRAMP Moderate (or higher) baseline.

# Which MSP you partner with is the single most important decision you will make on your CMMC journey

75% of the DIB are small businesses and DoD assumes you will leverage an MSP for compliance

**MSPs do not need a CMMC Certification**

**MSPs are part of your assessment scope**

**Significant documentation requirements**

The use of the ESP, its relationship to the OSA, and the services provided are:

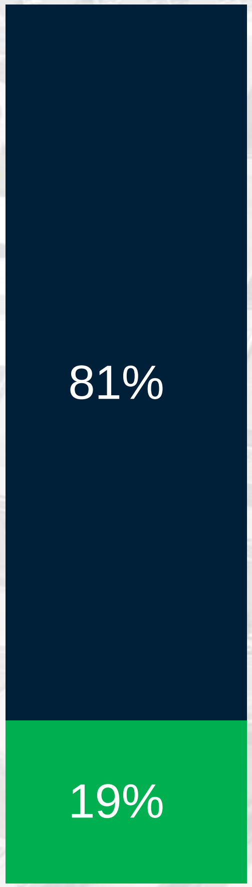
- Documented in the OSA’s System Security Plan and

- Described in the service provider’s:
  - Service description and
  - Customer Responsibility Matrix (CRM)

# Final Rule Structure & CMMC Cost Estimates

# Nowhere in the rule will DoD tell you *how* to implement cybersecurity requirements

32 CFR Final Rule
Composition by Page Count

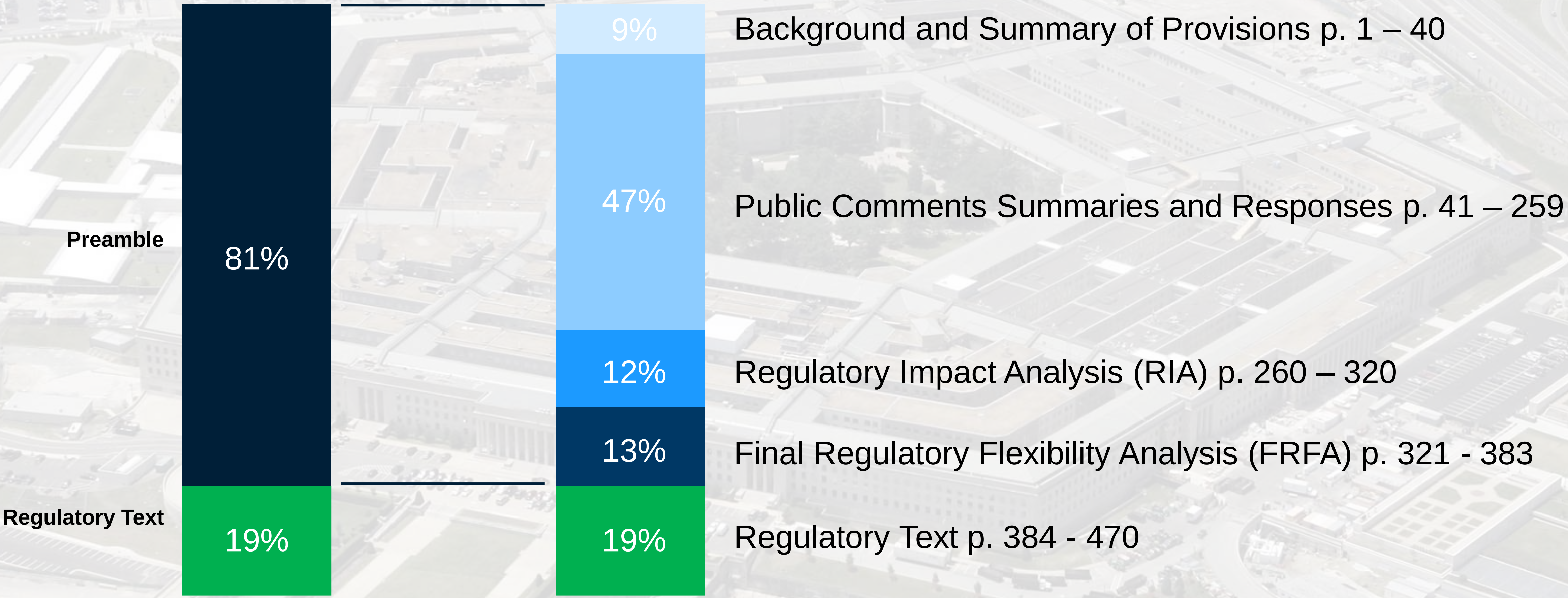


“Preamble” - this part tells you **why**

Regulatory Text - this part tells you **what**

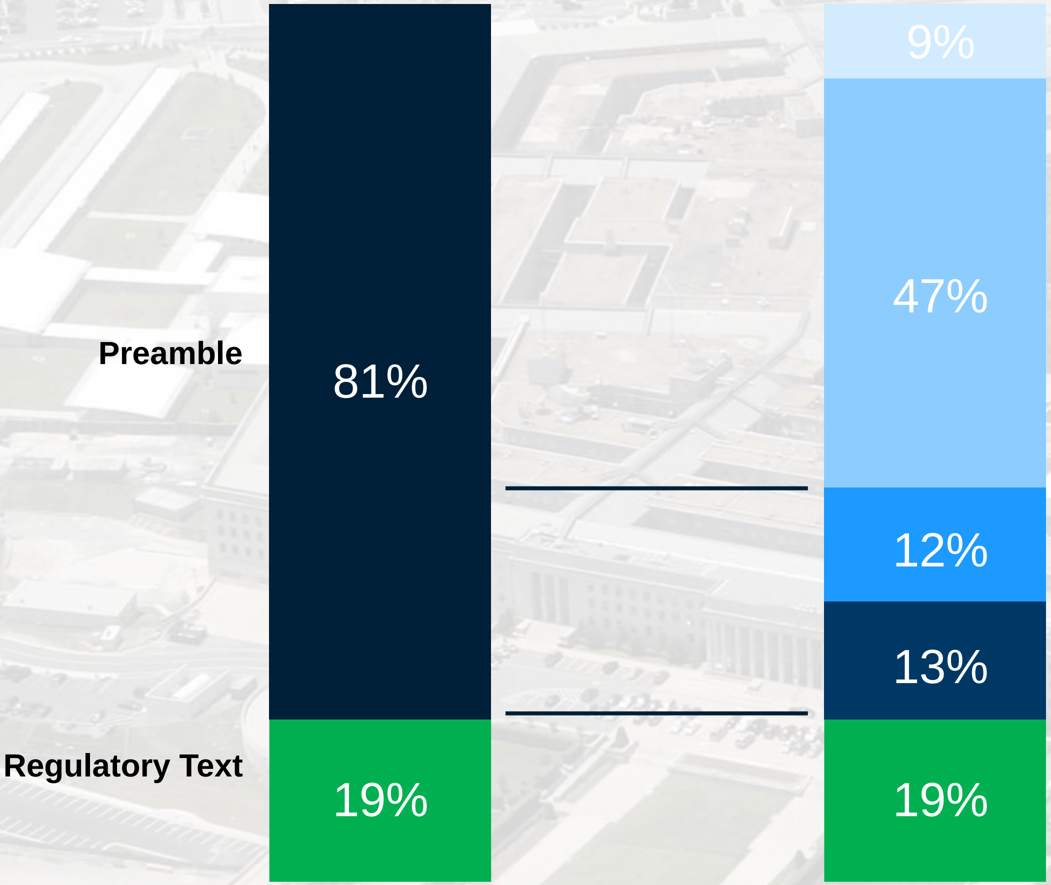
SUMMIT7

## 32 CFR Final Rule Composition by Page Count



# The final rule is identical to the proposed rule under the regulatory hood

32 CFR Final Rule Composition by Page Count



- RIA & FRFA are identical to the December 2023 proposed rule.
- From a regulatory perspective, there are no significant changes.
- Anyone who spent the last 10 months waiting in hopes of major changes made the wrong bet.

# CMMC is a six-figure problem

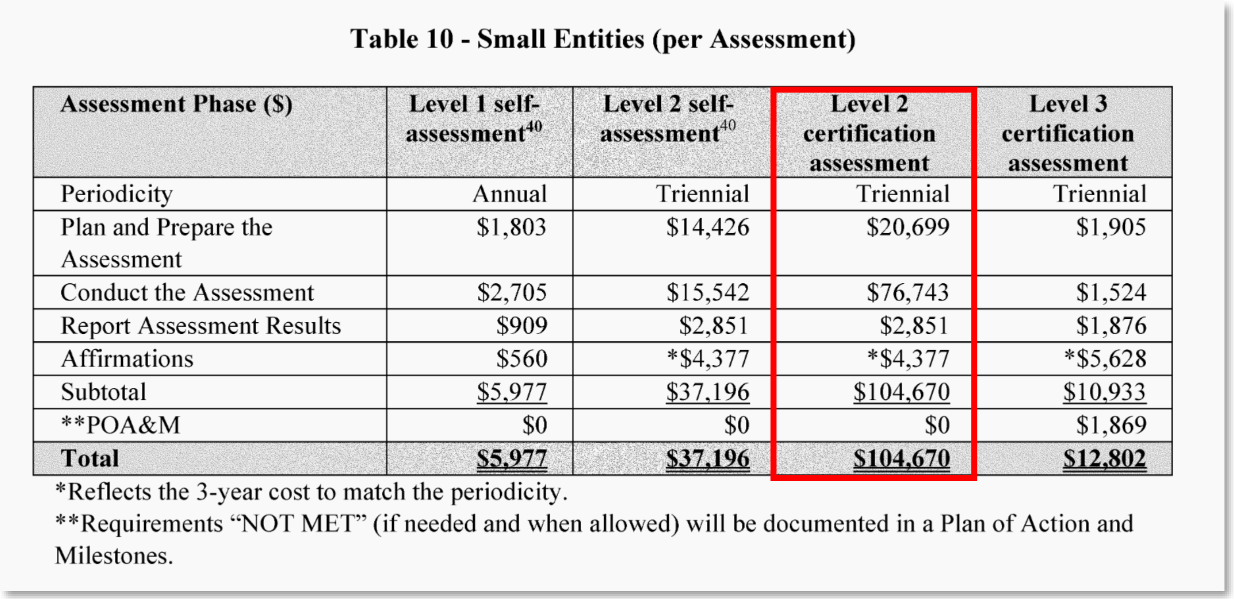


Table 10 - Small Entities (per Assessment)

| Assessment Phase ($) | Level 1 self-assessment[40] | Level 2 self-assessment[40] | Level 2 certification assessment | Level 3 certification assessment |
|---|---|---|---|---|
| Periodicity | Annual | Triennial | Triennial | Triennial |
| Plan and Prepare the Assessment | $1,803 | $14,426 | $20,699 | $1,905 |
| Conduct the Assessment | $2,705 | $15,542 | $76,743 | $1,524 |
| Report Assessment Results | $909 | $2,851 | $2,851 | $1,876 |
| Affirmations | $560 | *$4,377 | *$4,377 | *$5,628 |
| Subtotal | $5,977 | $37,196 | $104,670 | $10,933 |
| **POA&M | $0 | $0 | $0 | $1,869 |
| **Total** | **$5,977** | **$37,196** | **$104,670** | **$12,802** |

*Reflects the 3-year cost to match the periodicity.

**Requirements "NOT MET" (if needed and when allowed) will be documented in a Plan of Action and Milestones.

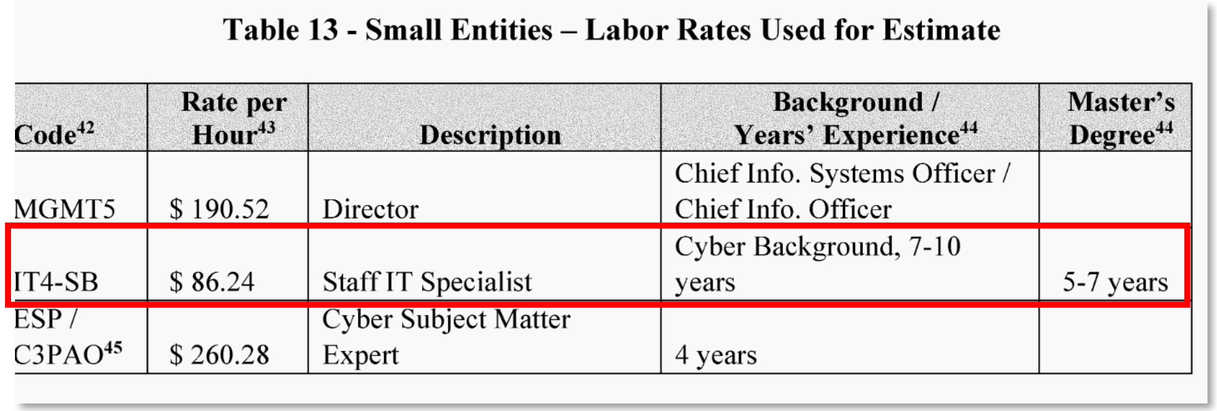


Table 13 - Small Entities – Labor Rates Used for Estimate

| Code[42] | Rate per Hour[43] | Description | Background / Years' Experience[44] | Master's Degree[44] |
|---|---|---|---|---|
| MGMT5 | $ 190.52 | Director | Chief Info. Systems Officer / Chief Info. Officer | |
| IT4-SB | $ 86.24 | Staff IT Specialist | Cyber Background, 7-10 years | 5-7 years |
| ESP / C3PAO[45] | $ 260.28 | Cyber Subject Matter Expert | 4 years | |

# $100k estimated cost does not equate to $100k price of C3PAO assessment

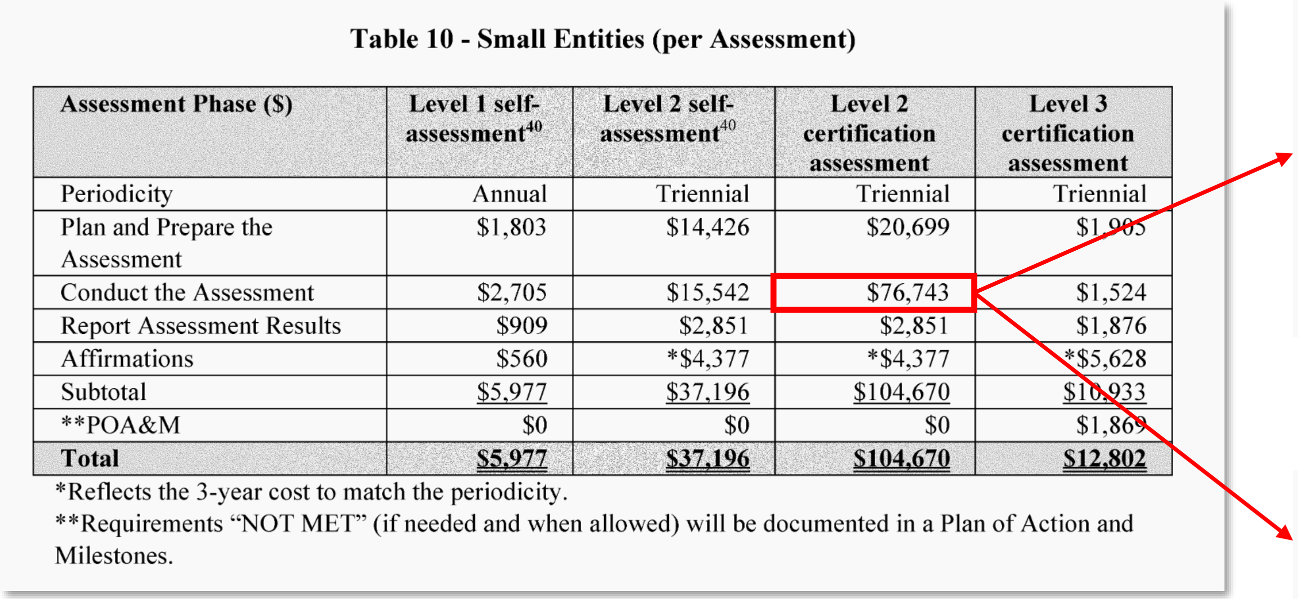


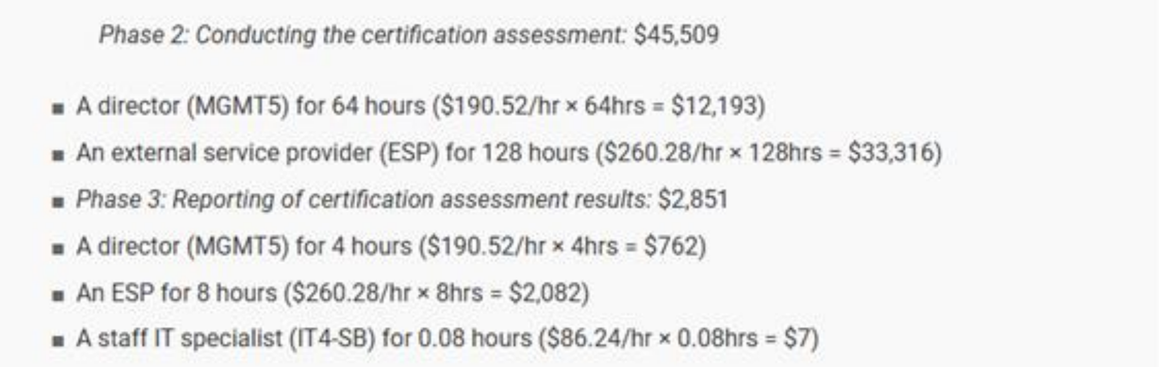
**Table 10 - Small Entities (per Assessment)**

| Assessment Phase ($) | Level 1 self-assessment[40] | Level 2 self-assessment[40] | Level 2 certification assessment | Level 3 certification assessment |
|---|---|---|---|---|
| Periodicity | Annual | Triennial | Triennial | Triennial |
| Plan and Prepare the Assessment | $1,803 | $14,426 | $20,699 | $1,905 |
| Conduct the Assessment | $2,705 | $15,542 | $76,743 | $1,524 |
| Report Assessment Results | $909 | $2,851 | $2,851 | $1,876 |
| Affirmations | $560 | *$4,377 | *$4,377 | *$5,628 |
| Subtotal | $5,977 | $37,196 | $104,670 | $10,933 |
| **POA&M | $0 | $0 | $0 | $1,869 |
| **Total** | **$5,977** | **$37,196** | **$104,670** | **$12,802** |

*Reflects the 3-year cost to match the periodicity.

**Requirements “NOT MET” (if needed and when allowed) will be documented in a Plan of Action and Milestones.

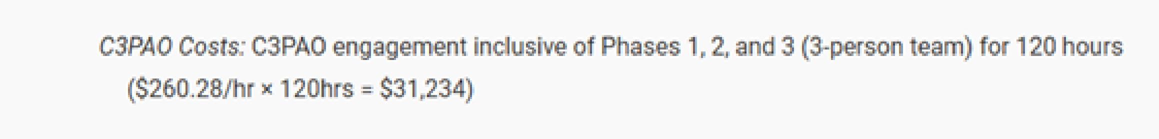
## Estimated Costs



*Phase 2: Conducting the certification assessment:* $45,509

- A director (MGMT5) for 64 hours ($190.52/hr × 64hrs = $12,193)
- An external service provider (ESP) for 128 hours ($260.28/hr × 128hrs = $33,316)
- *Phase 3: Reporting of certification assessment results:* $2,851
- A director (MGMT5) for 4 hours ($190.52/hr × 4hrs = $762)
- An ESP for 8 hours ($260.28/hr × 8hrs = $2,082)
- A staff IT specialist (IT4-SB) for 0.08 hours ($86.24/hr × 0.08hrs = $7)

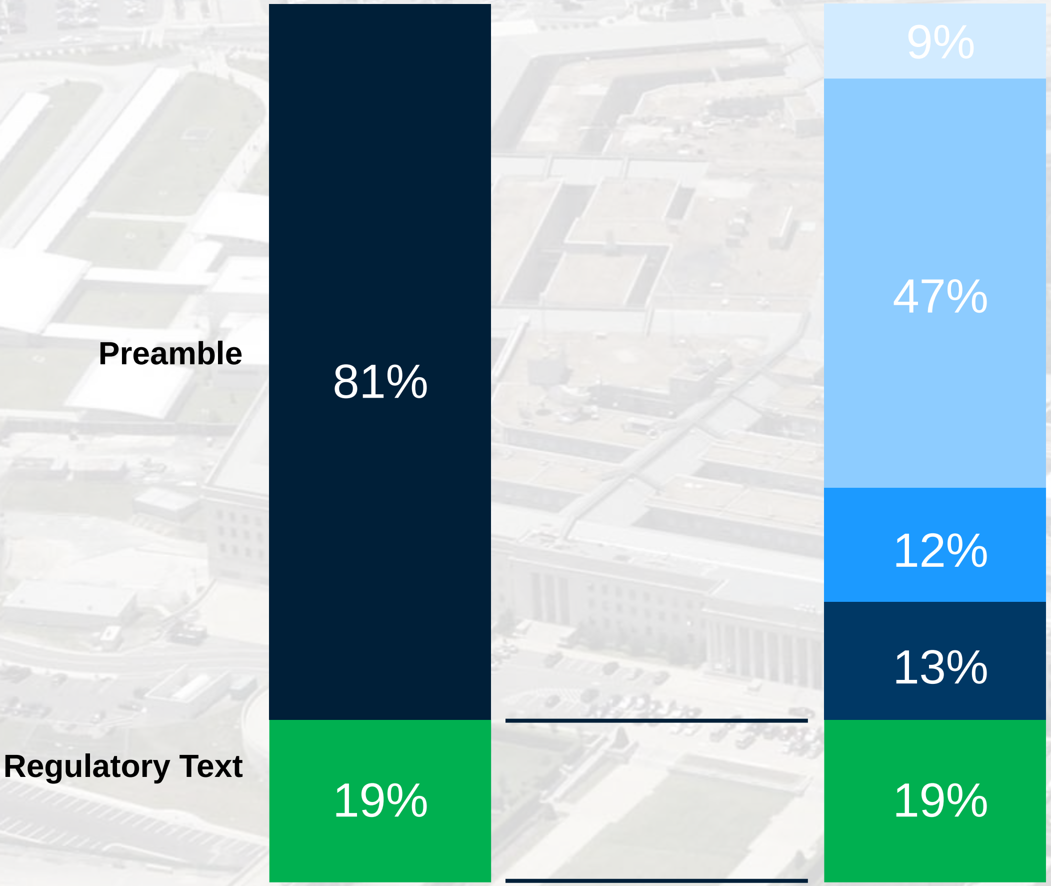
## Estimated C3PAO Price

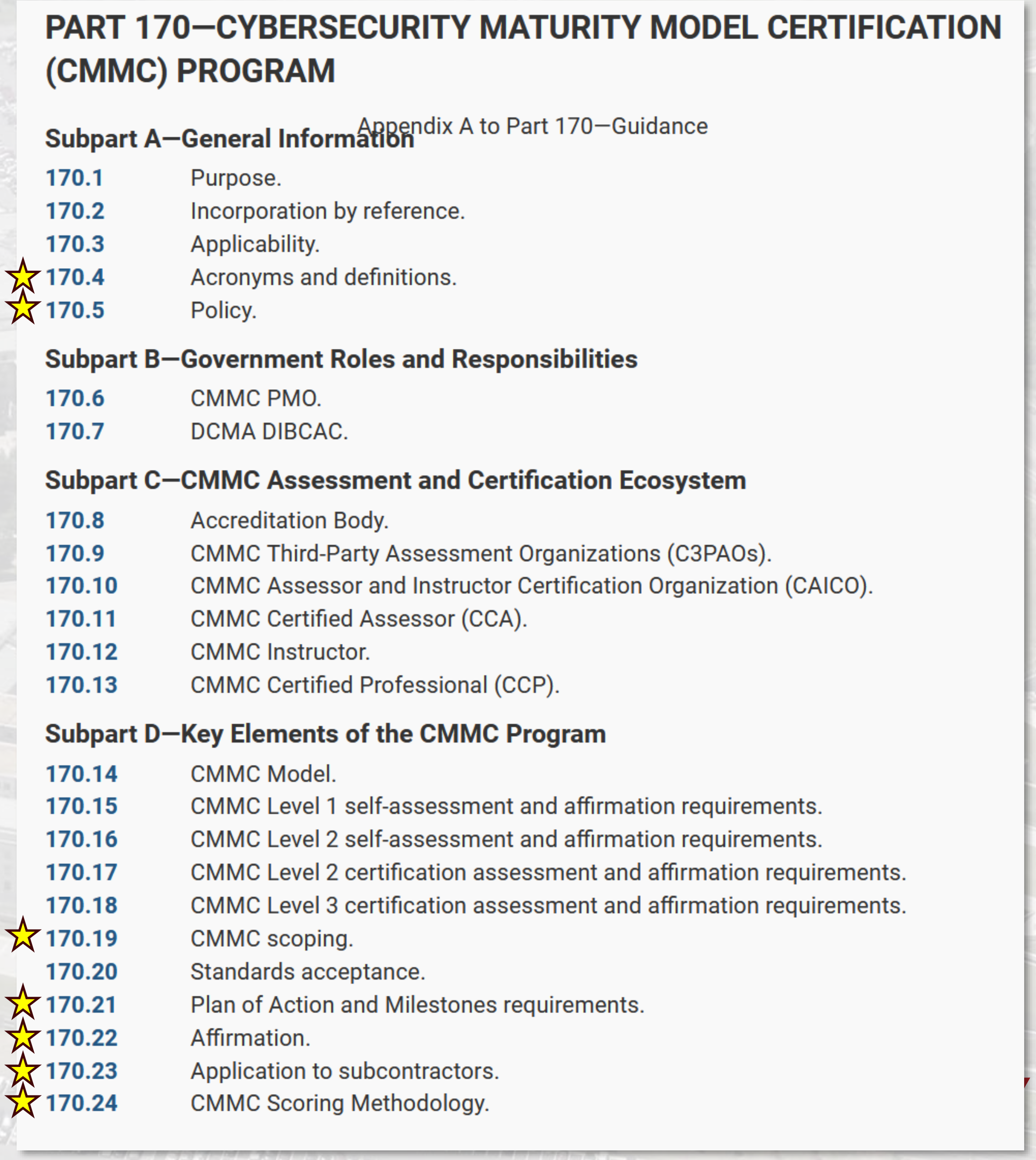


*C3PAO Costs:* C3PAO engagement inclusive of Phases 1, 2, and 3 (3-person team) for 120 hours ($260.28/hr × 120hrs = $31,234)

# The actual regulation

32 CFR Final Rule Composition by Page Count





## PART 170—CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) PROGRAM

Appendix A to Part 170—Guidance

### Subpart A—General Information

| | | |
|---|---|---|
| | 170.1 | Purpose. |
| | 170.2 | Incorporation by reference. |
| | 170.3 | Applicability. |
| ☆ | 170.4 | Acronyms and definitions. |
| ☆ | 170.5 | Policy. |

### Subpart B—Government Roles and Responsibilities

| | | |
|---|---|---|
| | 170.6 | CMMC PMO. |
| | 170.7 | DCMA DIBCAC. |

### Subpart C—CMMC Assessment and Certification Ecosystem

| | | |
|---|---|---|
| | 170.8 | Accreditation Body. |
| | 170.9 | CMMC Third-Party Assessment Organizations (C3PAOs). |
| | 170.10 | CMMC Assessor and Instructor Certification Organization (CAICO). |
| | 170.11 | CMMC Certified Assessor (CCA). |
| | 170.12 | CMMC Instructor. |
| | 170.13 | CMMC Certified Professional (CCP). |

### Subpart D—Key Elements of the CMMC Program

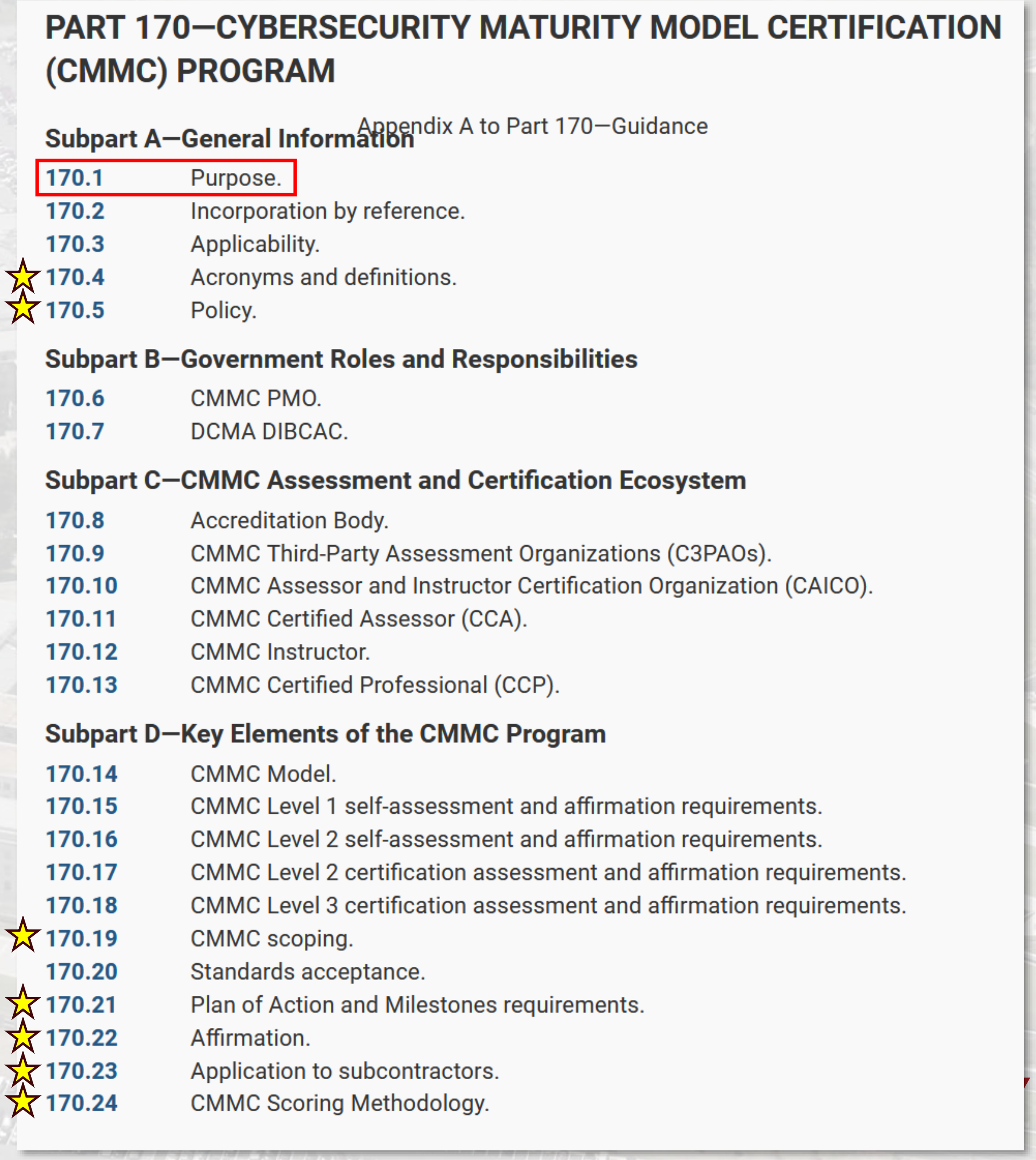
| | | |
|---|---|---|
| | 170.14 | CMMC Model. |
| | 170.15 | CMMC Level 1 self-assessment and affirmation requirements. |
| | 170.16 | CMMC Level 2 self-assessment and affirmation requirements. |
| | 170.17 | CMMC Level 2 certification assessment and affirmation requirements. |
| | 170.18 | CMMC Level 3 certification assessment and affirmation requirements. |
| ☆ | 170.19 | CMMC scoping. |
| | 170.20 | Standards acceptance. |
| ☆ | 170.21 | Plan of Action and Milestones requirements. |
| ☆ | 170.22 | Affirmation. |
| ☆ | 170.23 | Application to subcontractors. |
| ☆ | 170.24 | CMMC Scoring Methodology. |

# Rapid Fire Takeaways

# Contractor-relevant changes in specific sections of the regulatory text (Section Heatmap)

Key Takeaway:

*“The CMMC Program provides DoD with a viable means of conducting the volume of assessments necessary to verify contractor and subcontractor implementation of required cybersecurity requirements.”*



## PART 170—CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) PROGRAM

Appendix A to Part 170—Guidance

### Subpart A—General Information

| | | |
|---|---|---|
| | 170.1 | Purpose. |
| | 170.2 | Incorporation by reference. |
| | 170.3 | Applicability. |
| ★ | 170.4 | Acronyms and definitions. |
| ★ | 170.5 | Policy. |

### Subpart B—Government Roles and Responsibilities

| | | |
|---|---|---|
| | 170.6 | CMMC PMO. |
| | 170.7 | DCMA DIBCAC. |

### Subpart C—CMMC Assessment and Certification Ecosystem

| | | |
|---|---|---|
| | 170.8 | Accreditation Body. |
| | 170.9 | CMMC Third-Party Assessment Organizations (C3PAOs). |
| | 170.10 | CMMC Assessor and Instructor Certification Organization (CAICO). |
| | 170.11 | CMMC Certified Assessor (CCA). |
| | 170.12 | CMMC Instructor. |
| | 170.13 | CMMC Certified Professional (CCP). |

### Subpart D—Key Elements of the CMMC Program

| | | |
|---|---|---|
| | 170.14 | CMMC Model. |
| | 170.15 | CMMC Level 1 self-assessment and affirmation requirements. |
| | 170.16 | CMMC Level 2 self-assessment and affirmation requirements. |
| | 170.17 | CMMC Level 2 certification assessment and affirmation requirements. |
| | 170.18 | CMMC Level 3 certification assessment and affirmation requirements. |
| ★ | 170.19 | CMMC scoping. |
| | 170.20 | Standards acceptance. |
| ★ | 170.21 | Plan of Action and Milestones requirements. |
| ★ | 170.22 | Affirmation. |
| ★ | 170.23 | Application to subcontractors. |
| ★ | 170.24 | CMMC Scoring Methodology. |

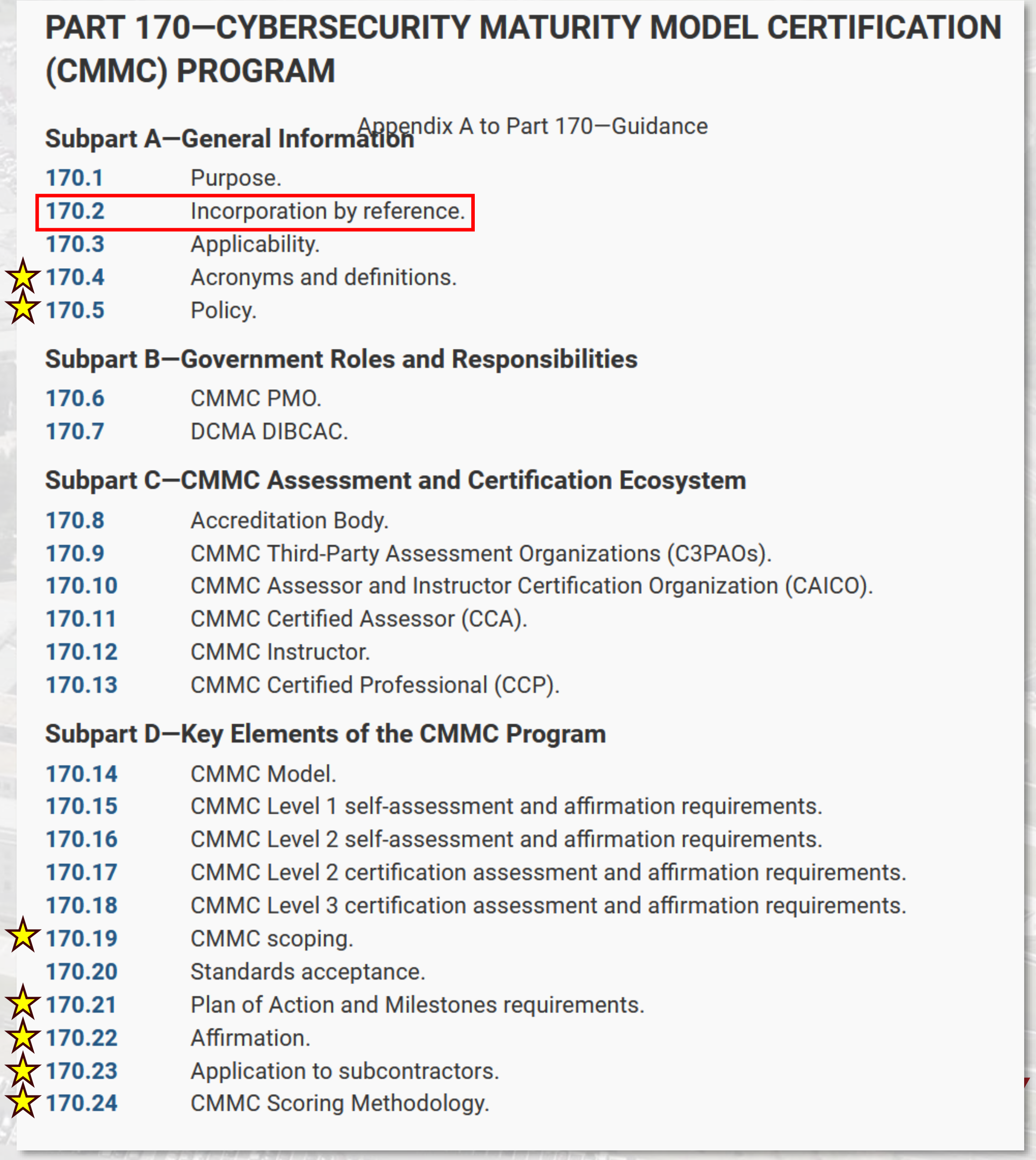
# Contractor-relevant changes in specific sections of the regulatory text (Section Heatmap)

Key Takeaway:

New rulemaking is triggered by updates to Incorporation by Reference (IBR) documents.

NIST SP 800-171 revision 2 is IBR.
NIST SP 800-171 revision 3 was published…

NIST SP 800-172 is IBR
NIST SP 800-172 revision 3 ETA: 2025



## PART 170—CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) PROGRAM

### Subpart A—General Information

Appendix A to Part 170—Guidance

| | | |
|---|---|---|
| | 170.1 | Purpose. |
| | 170.2 | Incorporation by reference. |
| | 170.3 | Applicability. |
| ★ | 170.4 | Acronyms and definitions. |
| ★ | 170.5 | Policy. |

### Subpart B—Government Roles and Responsibilities

| | | |
|---|---|---|
| | 170.6 | CMMC PMO. |
| | 170.7 | DCMA DIBCAC. |

### Subpart C—CMMC Assessment and Certification Ecosystem

| | | |
|---|---|---|
| | 170.8 | Accreditation Body. |
| | 170.9 | CMMC Third-Party Assessment Organizations (C3PAOs). |
| | 170.10 | CMMC Assessor and Instructor Certification Organization (CAICO). |
| | 170.11 | CMMC Certified Assessor (CCA). |
| | 170.12 | CMMC Instructor. |
| | 170.13 | CMMC Certified Professional (CCP). |

### Subpart D—Key Elements of the CMMC Program

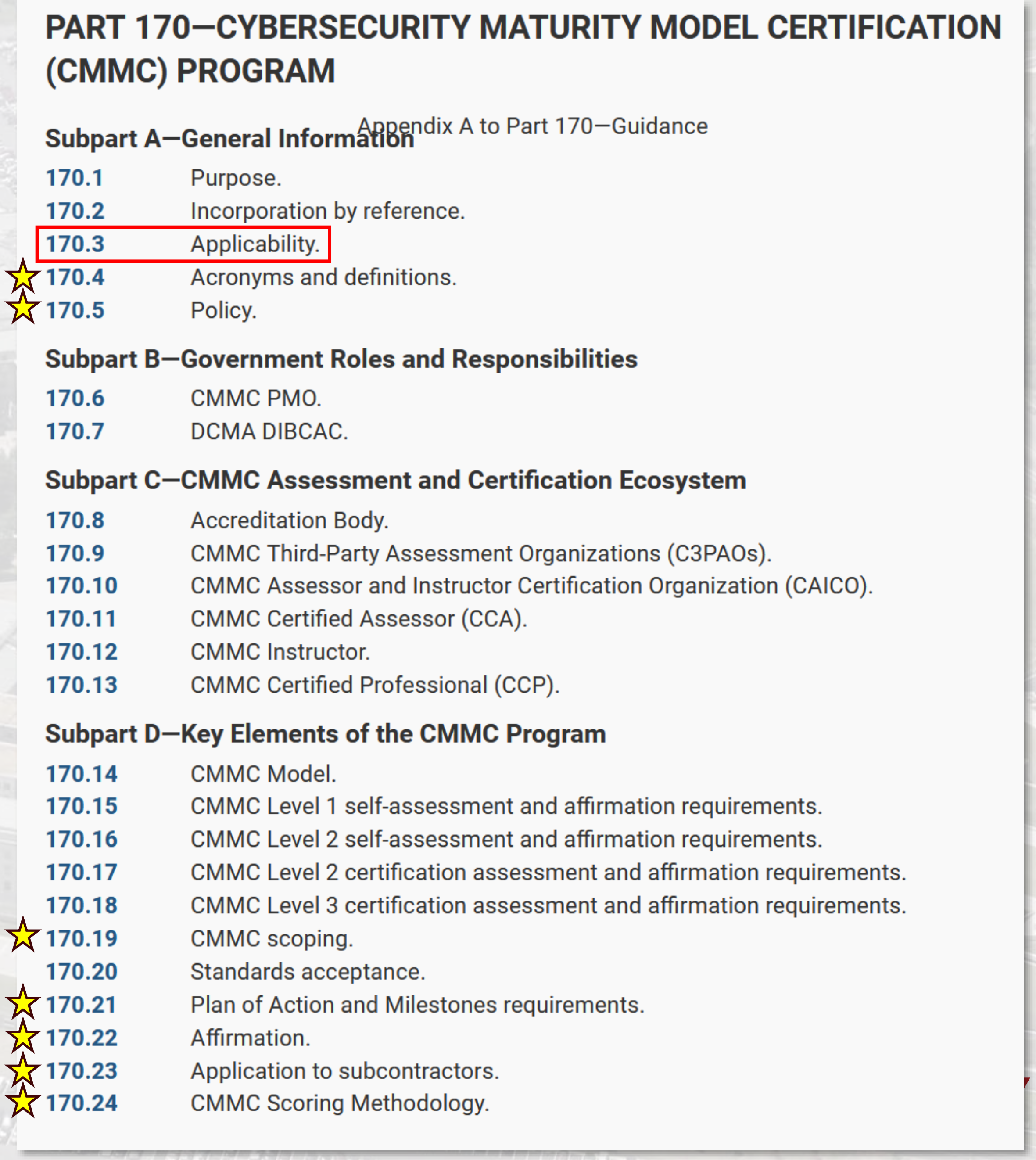
| | | |
|---|---|---|
| | 170.14 | CMMC Model. |
| | 170.15 | CMMC Level 1 self-assessment and affirmation requirements. |
| | 170.16 | CMMC Level 2 self-assessment and affirmation requirements. |
| | 170.17 | CMMC Level 2 certification assessment and affirmation requirements. |
| | 170.18 | CMMC Level 3 certification assessment and affirmation requirements. |
| ★ | 170.19 | CMMC scoping. |
| | 170.20 | Standards acceptance. |
| ★ | 170.21 | Plan of Action and Milestones requirements. |
| ★ | 170.22 | Affirmation. |
| ★ | 170.23 | Application to subcontractors. |
| ★ | 170.24 | CMMC Scoring Methodology. |

# Contractor-relevant changes in specific sections of the regulatory text (Section Heatmap)

Key Takeaway:

**Phased Roll-Out begins Q2 2025**

**Impossible to predict**



## PART 170—CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) PROGRAM

Appendix A to Part 170—Guidance

### Subpart A—General Information

| | | |
|---|---|---|
| | 170.1 | Purpose. |
| | 170.2 | Incorporation by reference. |
| | 170.3 | Applicability. |
| ☆ | 170.4 | Acronyms and definitions. |
| ☆ | 170.5 | Policy. |

### Subpart B—Government Roles and Responsibilities

| | | |
|---|---|---|
| | 170.6 | CMMC PMO. |
| | 170.7 | DCMA DIBCAC. |

### Subpart C—CMMC Assessment and Certification Ecosystem

| | | |
|---|---|---|
| | 170.8 | Accreditation Body. |
| | 170.9 | CMMC Third-Party Assessment Organizations (C3PAOs). |
| | 170.10 | CMMC Assessor and Instructor Certification Organization (CAICO). |
| | 170.11 | CMMC Certified Assessor (CCA). |
| | 170.12 | CMMC Instructor. |
| | 170.13 | CMMC Certified Professional (CCP). |

### Subpart D—Key Elements of the CMMC Program

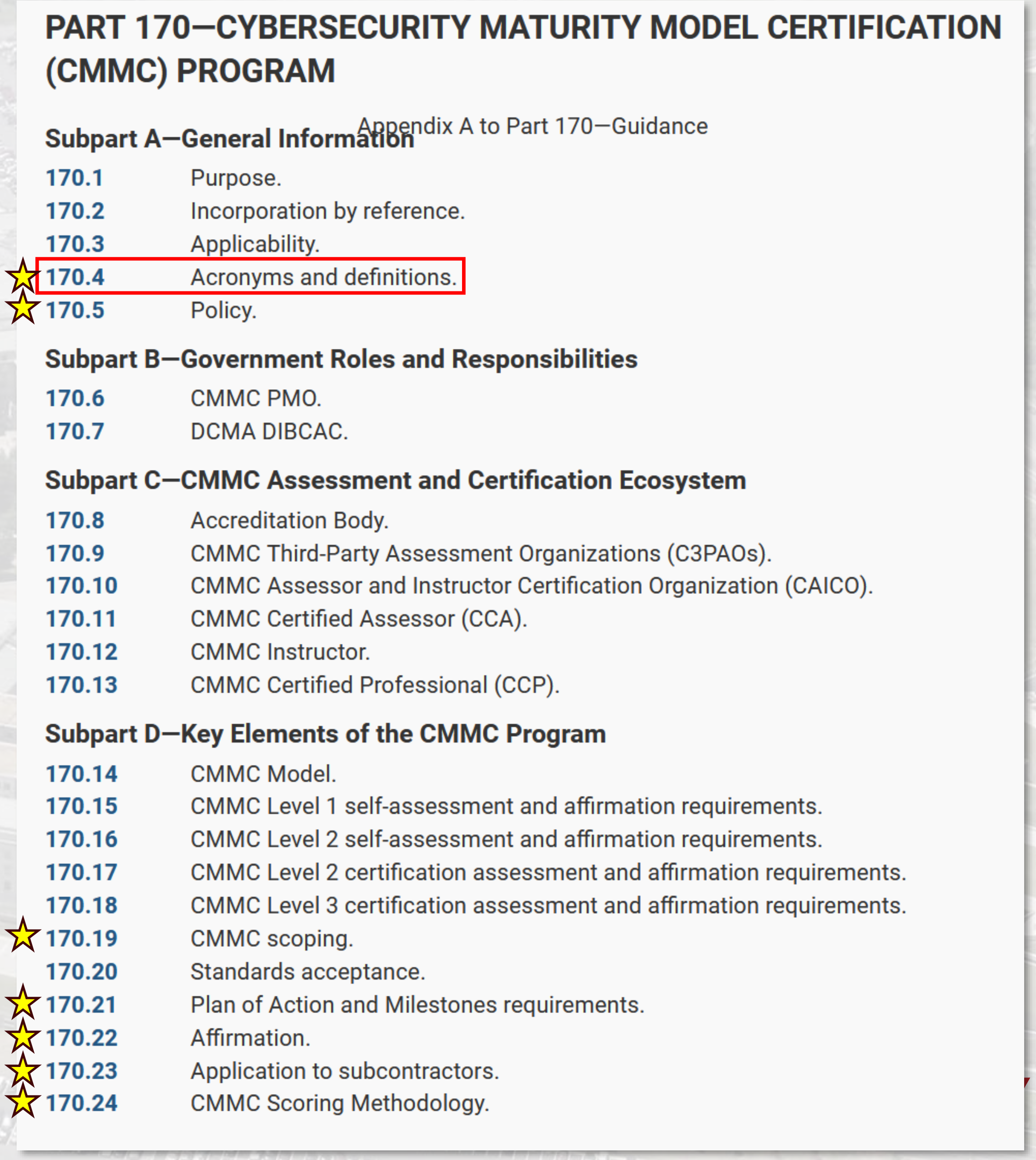
| | | |
|---|---|---|
| | 170.14 | CMMC Model. |
| | 170.15 | CMMC Level 1 self-assessment and affirmation requirements. |
| | 170.16 | CMMC Level 2 self-assessment and affirmation requirements. |
| | 170.17 | CMMC Level 2 certification assessment and affirmation requirements. |
| | 170.18 | CMMC Level 3 certification assessment and affirmation requirements. |
| ☆ | 170.19 | CMMC scoping. |
| | 170.20 | Standards acceptance. |
| ☆ | 170.21 | Plan of Action and Milestones requirements. |
| ☆ | 170.22 | Affirmation. |
| ☆ | 170.23 | Application to subcontractors. |
| ☆ | 170.24 | CMMC Scoring Methodology. |

# Contractor-relevant changes in specific sections of the regulatory text (Section Heatmap)

Key Takeaway:

Affirming Official:

The senior level representative from within each Organization Seeking Assessment (OSA) who is responsible for ensuring the OSA's compliance with the CMMC Program requirements and has the authority to affirm the OSA's continuing compliance with the specified security requirements for their respective organizations.



## PART 170—CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) PROGRAM

Appendix A to Part 170—Guidance

### Subpart A—General Information

### Subpart B—Government Roles and Responsibilities

### Subpart C—CMMC Assessment and Certification Ecosystem

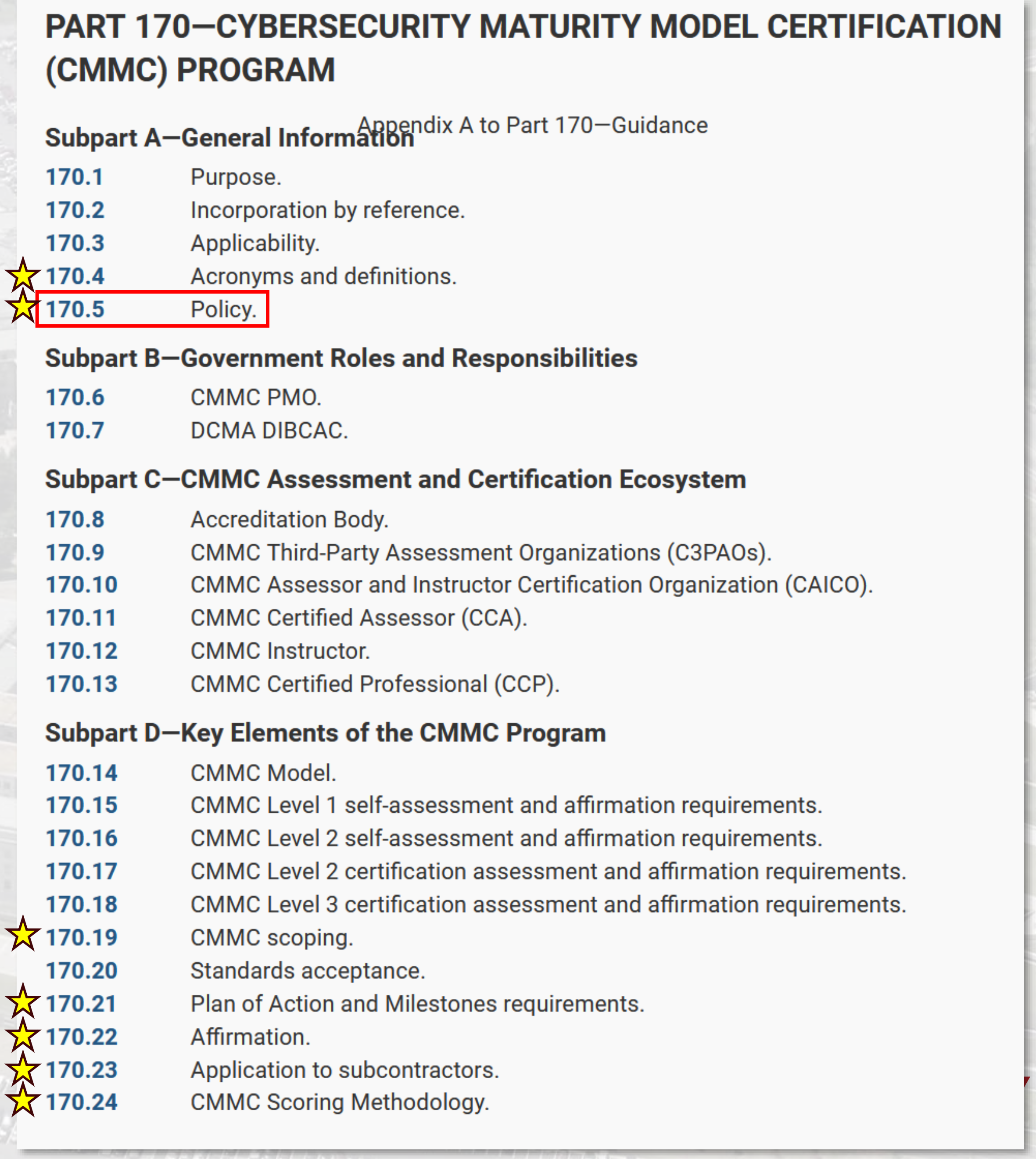
### Subpart D—Key Elements of the CMMC Program

# Contractor-relevant changes in specific sections of the regulatory text (Section Heatmap)

Key Takeaway:

How PMs will select CMMC level requirements

Waivers are for contracts, not contractors



## PART 170—CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) PROGRAM

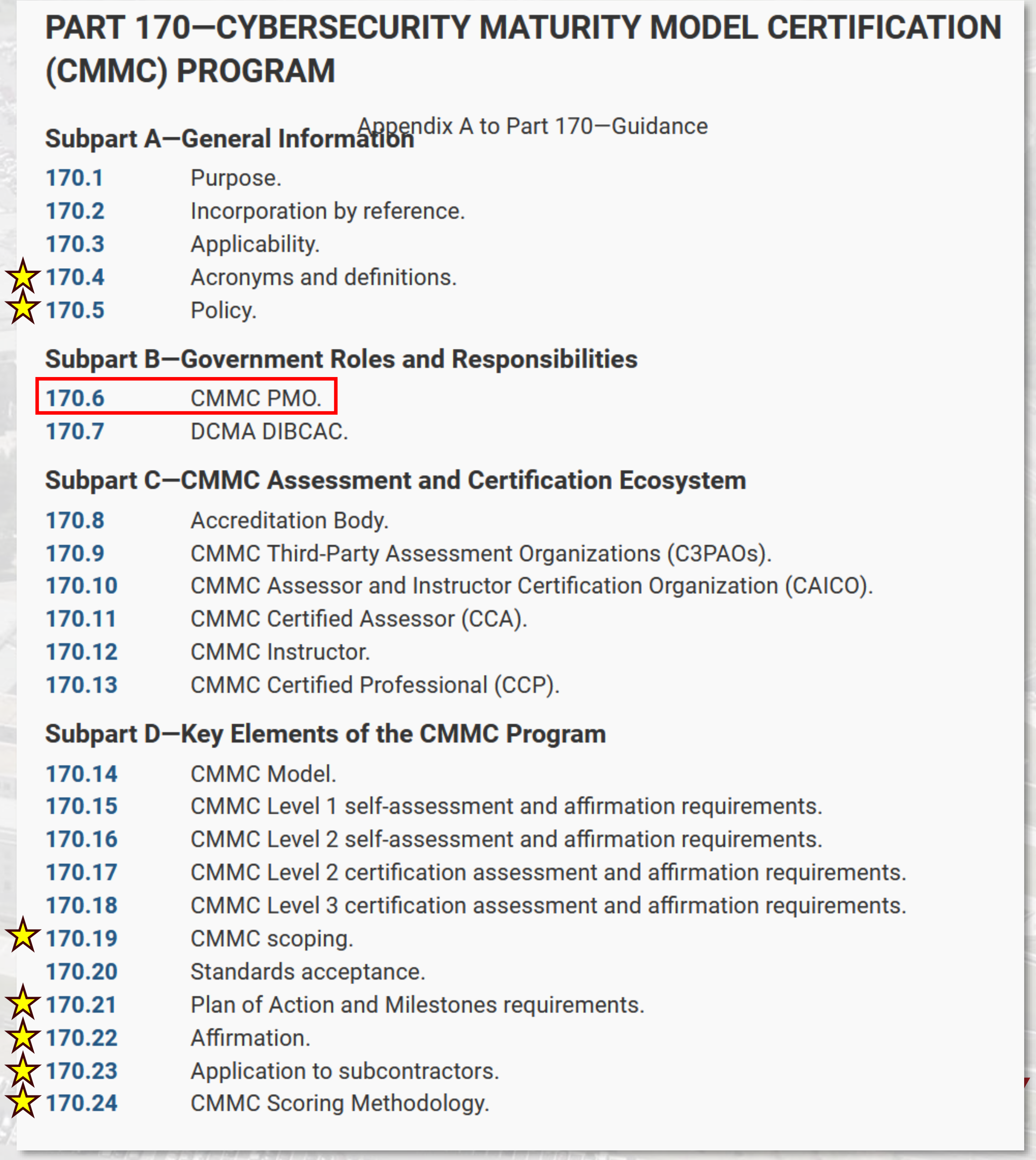
Appendix A to Part 170—Guidance

# Contractor-relevant changes in specific sections of the regulatory text (Section Heatmap)

Key Takeaway:

Oversight of the Accreditation Body

Investigates indications that an active CMMC status has been called into question.



## PART 170—CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) PROGRAM

Appendix A to Part 170—Guidance

### Subpart A—General Information

170.1 Purpose.
170.2 Incorporation by reference.
170.3 Applicability.
★ 170.4 Acronyms and definitions.
★ 170.5 Policy.

### Subpart B—Government Roles and Responsibilities

170.6 CMMC PMO.
170.7 DCMA DIBCAC.

### Subpart C—CMMC Assessment and Certification Ecosystem

170.8 Accreditation Body.
170.9 CMMC Third-Party Assessment Organizations (C3PAOs).
170.10 CMMC Assessor and Instructor Certification Organization (CAICO).
170.11 CMMC Certified Assessor (CCA).
170.12 CMMC Instructor.
170.13 CMMC Certified Professional (CCP).

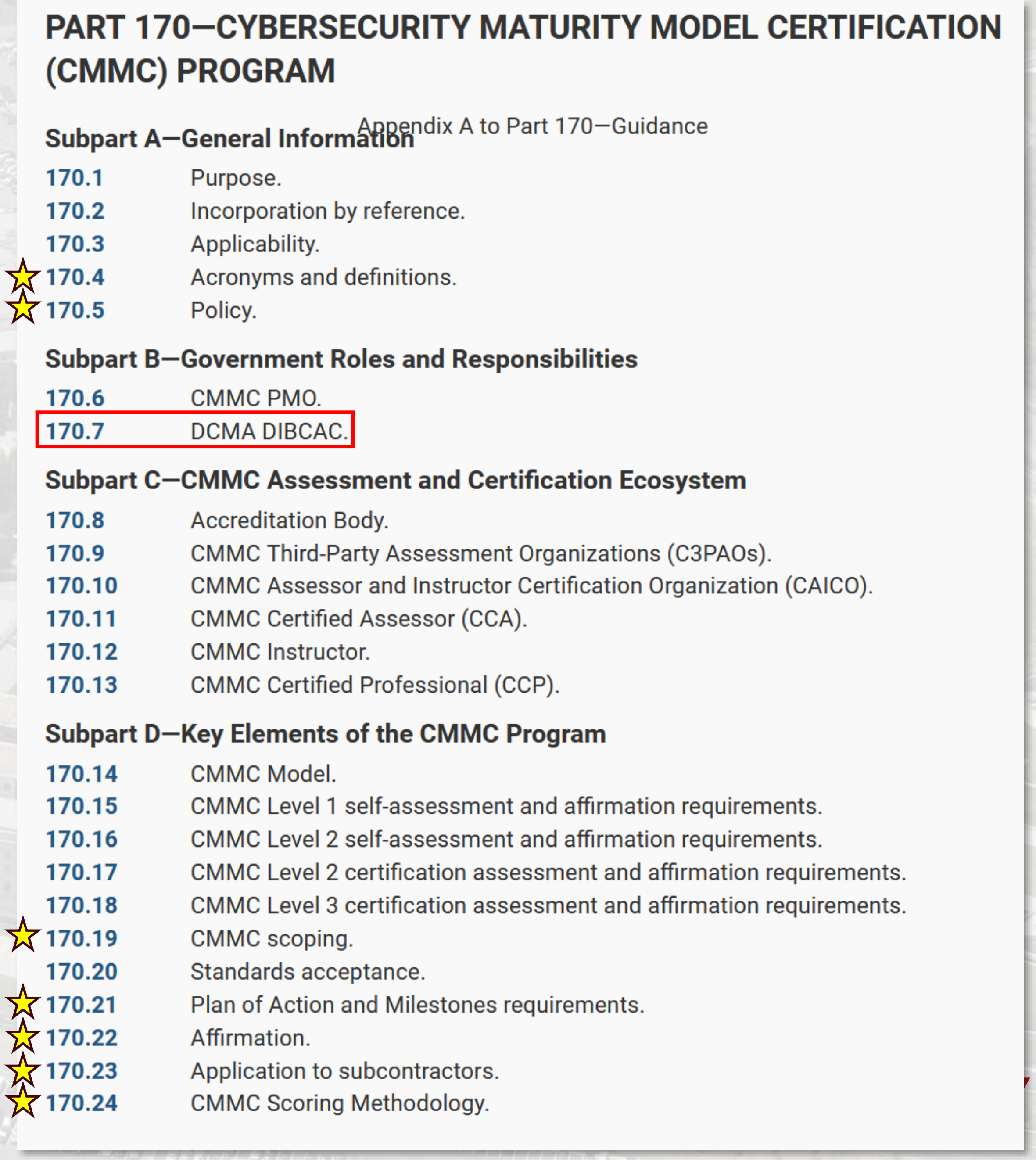
### Subpart D—Key Elements of the CMMC Program

170.14 CMMC Model.
170.15 CMMC Level 1 self-assessment and affirmation requirements.
170.16 CMMC Level 2 self-assessment and affirmation requirements.
170.17 CMMC Level 2 certification assessment and affirmation requirements.
170.18 CMMC Level 3 certification assessment and affirmation requirements.
★ 170.19 CMMC scoping.
170.20 Standards acceptance.
★ 170.21 Plan of Action and Milestones requirements.
★ 170.22 Affirmation.
★ 170.23 Application to subcontractors.
★ 170.24 CMMC Scoring Methodology.

# Contractor-relevant changes in specific sections of the regulatory text (Section Heatmap)

Key Takeaway:

An OSC, the CMMC AB, or a C3PAO may appeal the outcome of its DCMA DIBCAC conducted assessment within 21 days by submitting a written basis for appeal with the requirements in question for DCMA DIBCAC consideration.



## PART 170—CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) PROGRAM

Appendix A to Part 170—Guidance

### Subpart A—General Information

### Subpart B—Government Roles and Responsibilities

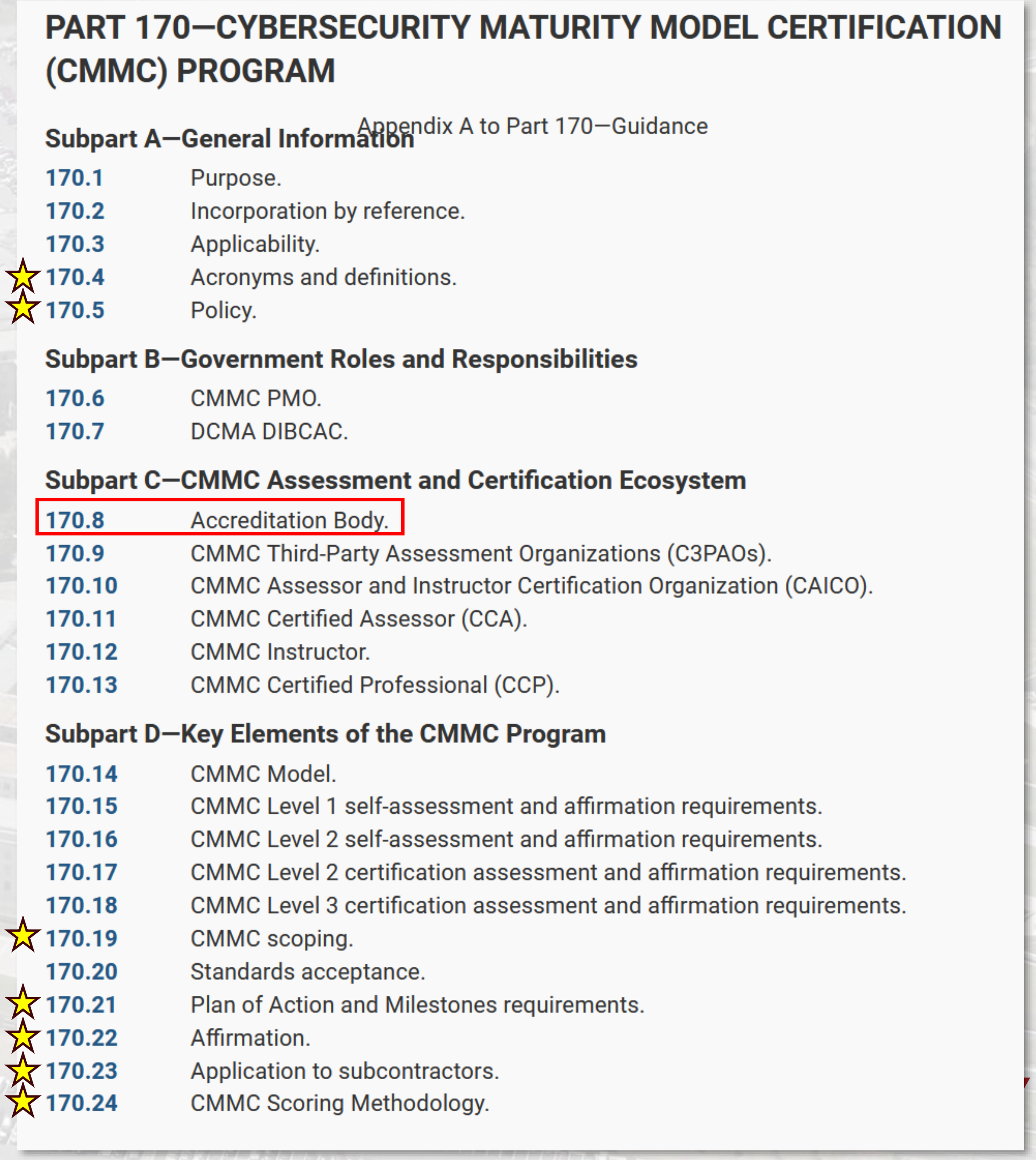
### Subpart C—CMMC Assessment and Certification Ecosystem

### Subpart D—Key Elements of the CMMC Program

# Contractor-relevant changes in specific sections of the regulatory text (Section Heatmap)

Key Takeaway:

- Conflict of Interest Policy
- Code of Professional Conduct Policy
- Ethics Policy



## PART 170—CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) PROGRAM

Appendix A to Part 170—Guidance

### Subpart A—General Information

**170.1** Purpose.
**170.2** Incorporation by reference.
**170.3** Applicability.
★ **170.4** Acronyms and definitions.
★ **170.5** Policy.

### Subpart B—Government Roles and Responsibilities

**170.6** CMMC PMO.
**170.7** DCMA DIBCAC.

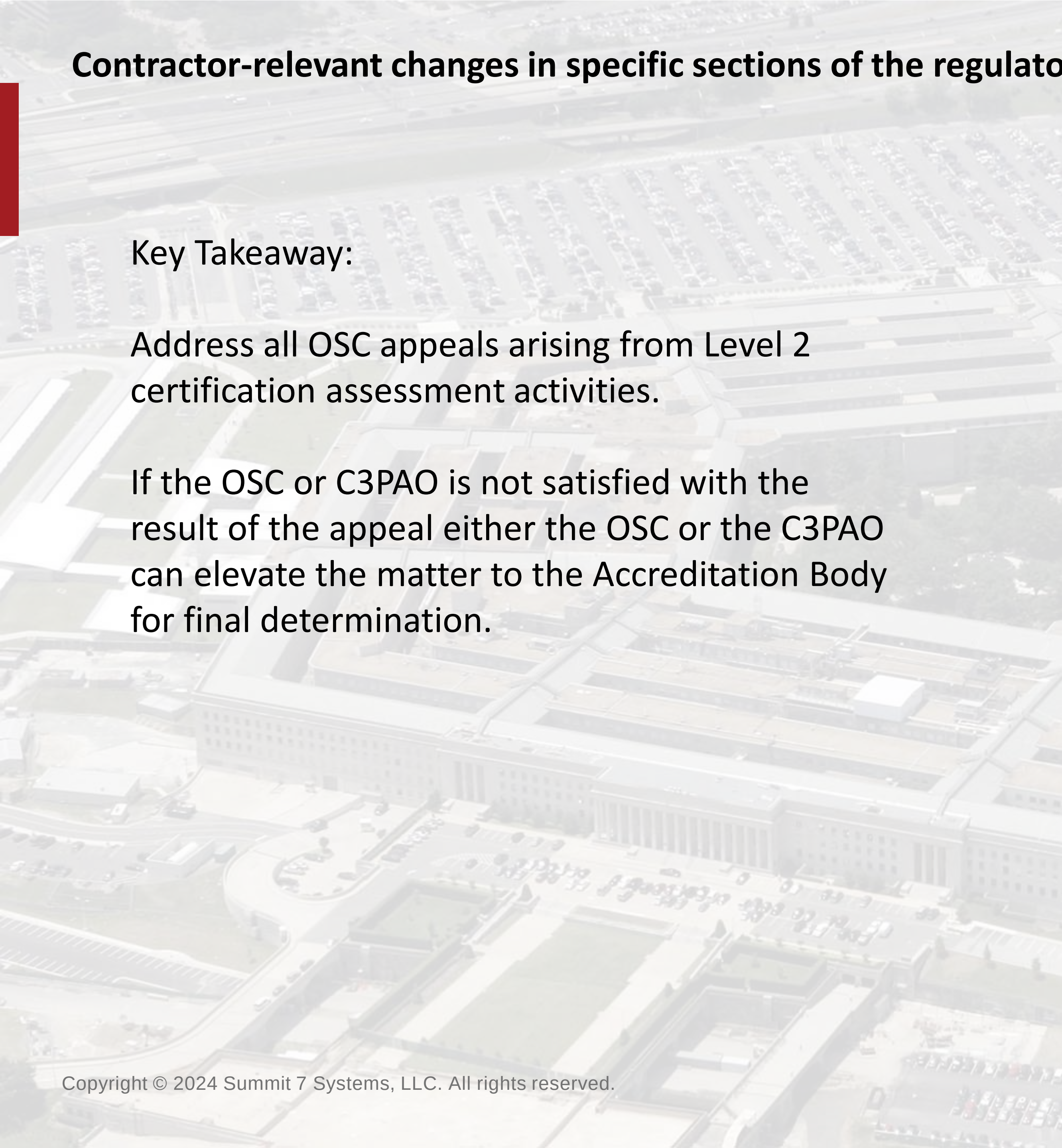
### Subpart C—CMMC Assessment and Certification Ecosystem

**170.8** Accreditation Body.
**170.9** CMMC Third-Party Assessment Organizations (C3PAOs).
**170.10** CMMC Assessor and Instructor Certification Organization (CAICO).
**170.11** CMMC Certified Assessor (CCA).
**170.12** CMMC Instructor.
**170.13** CMMC Certified Professional (CCP).

### Subpart D—Key Elements of the CMMC Program

**170.14** CMMC Model.
**170.15** CMMC Level 1 self-assessment and affirmation requirements.
**170.16** CMMC Level 2 self-assessment and affirmation requirements.
**170.17** CMMC Level 2 certification assessment and affirmation requirements.
**170.18** CMMC Level 3 certification assessment and affirmation requirements.
★ **170.19** CMMC scoping.
**170.20** Standards acceptance.
★ **170.21** Plan of Action and Milestones requirements.
★ **170.22** Affirmation.
★ **170.23** Application to subcontractors.
★ **170.24** CMMC Scoring Methodology.

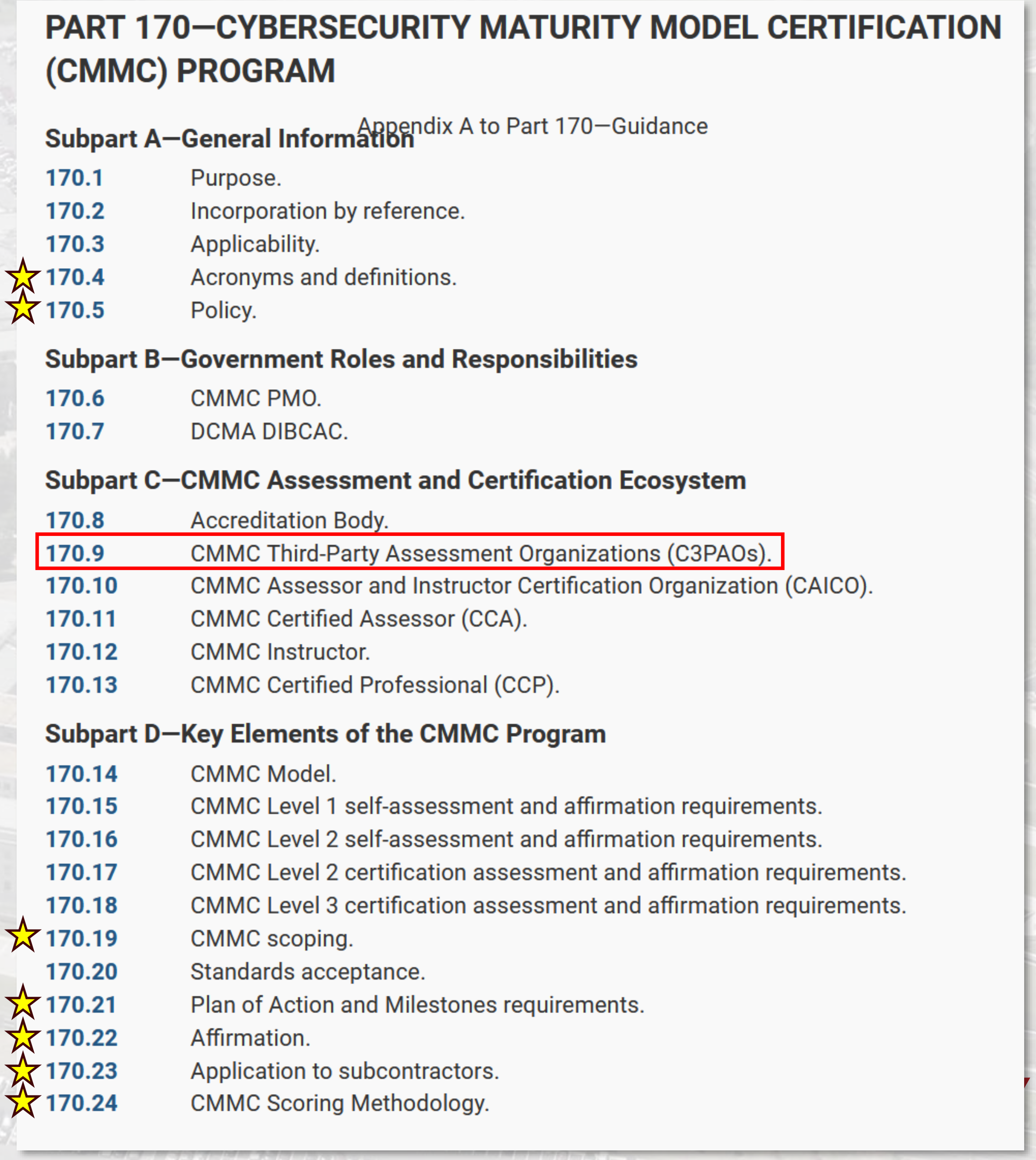
# Contractor-relevant changes in specific sections of the regulatory text (Section Heatmap)



Key Takeaway:

Address all OSC appeals arising from Level 2 certification assessment activities.

If the OSC or C3PAO is not satisfied with the result of the appeal either the OSC or the C3PAO can elevate the matter to the Accreditation Body for final determination.



## PART 170—CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) PROGRAM

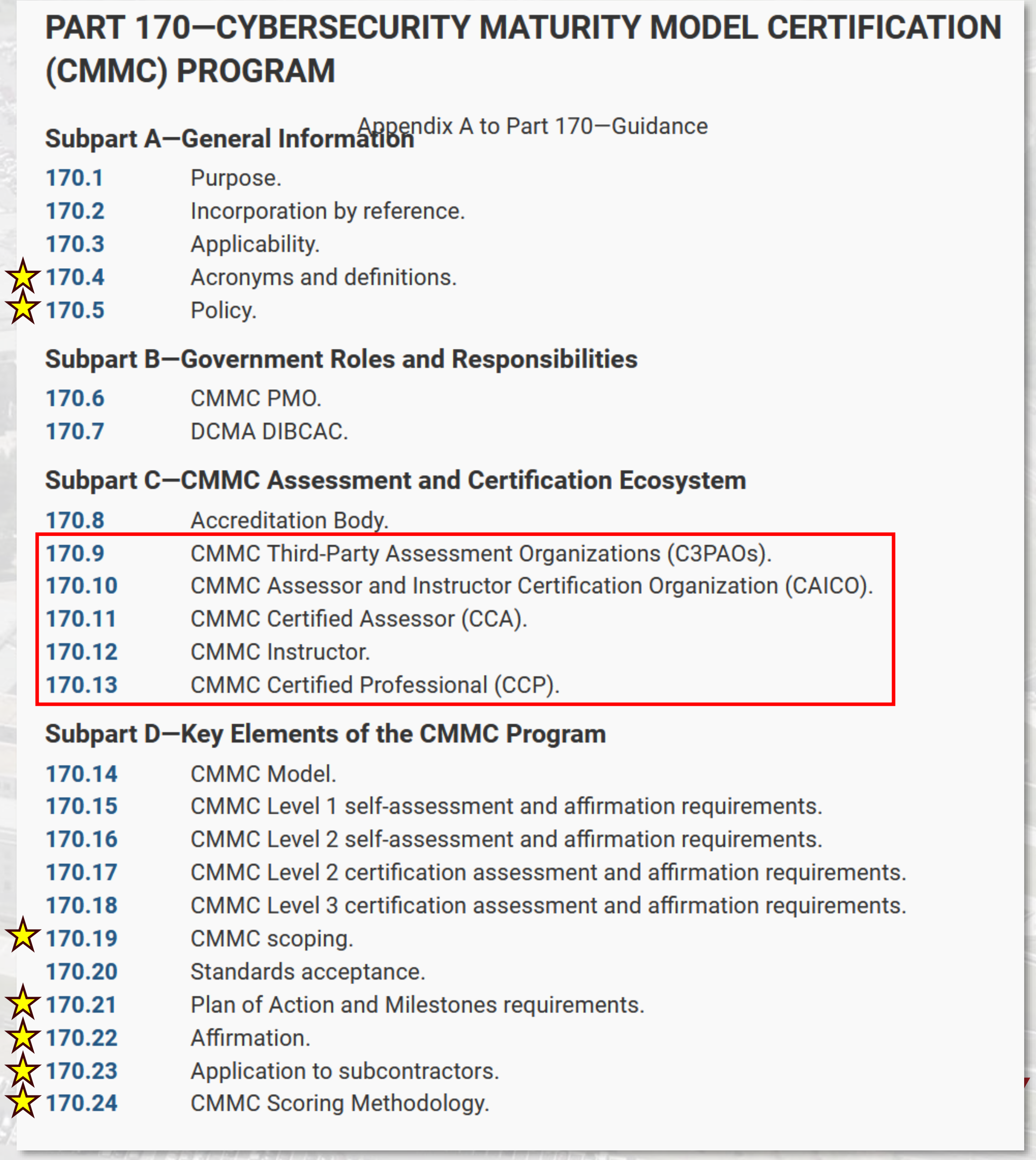
Appendix A to Part 170—Guidance

## Contractor-relevant changes in specific sections of the regulatory text (Section Heatmap)

Key Takeaway:

Assessor training and certification requirements are steep.

Your internal staff does not need to be CMMC certified.



### PART 170—CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) PROGRAM

**Subpart A—General Information**

Appendix A to Part 170—Guidance

|  |  |  |
|---|---|---|
|  | 170.1 | Purpose. |
|  | 170.2 | Incorporation by reference. |
|  | 170.3 | Applicability. |
| ★ | 170.4 | Acronyms and definitions. |
| ★ | 170.5 | Policy. |

**Subpart B—Government Roles and Responsibilities**

|  |  |  |
|---|---|---|
|  | 170.6 | CMMC PMO. |
|  | 170.7 | DCMA DIBCAC. |

**Subpart C—CMMC Assessment and Certification Ecosystem**

|  |  |  |
|---|---|---|
|  | 170.8 | Accreditation Body. |
|  | 170.9 | CMMC Third-Party Assessment Organizations (C3PAOs). |
|  | 170.10 | CMMC Assessor and Instructor Certification Organization (CAICO). |
|  | 170.11 | CMMC Certified Assessor (CCA). |
|  | 170.12 | CMMC Instructor. |
|  | 170.13 | CMMC Certified Professional (CCP). |

**Subpart D—Key Elements of the CMMC Program**

|  |  |  |
|---|---|---|
|  | 170.14 | CMMC Model. |
|  | 170.15 | CMMC Level 1 self-assessment and affirmation requirements. |
|  | 170.16 | CMMC Level 2 self-assessment and affirmation requirements. |
|  | 170.17 | CMMC Level 2 certification assessment and affirmation requirements. |
|  | 170.18 | CMMC Level 3 certification assessment and affirmation requirements. |
| ★ | 170.19 | CMMC scoping. |
|  | 170.20 | Standards acceptance. |
| ★ | 170.21 | Plan of Action and Milestones requirements. |
| ★ | 170.22 | Affirmation. |
| ★ | 170.23 | Application to subcontractors. |
| ★ | 170.24 | CMMC Scoring Methodology. |

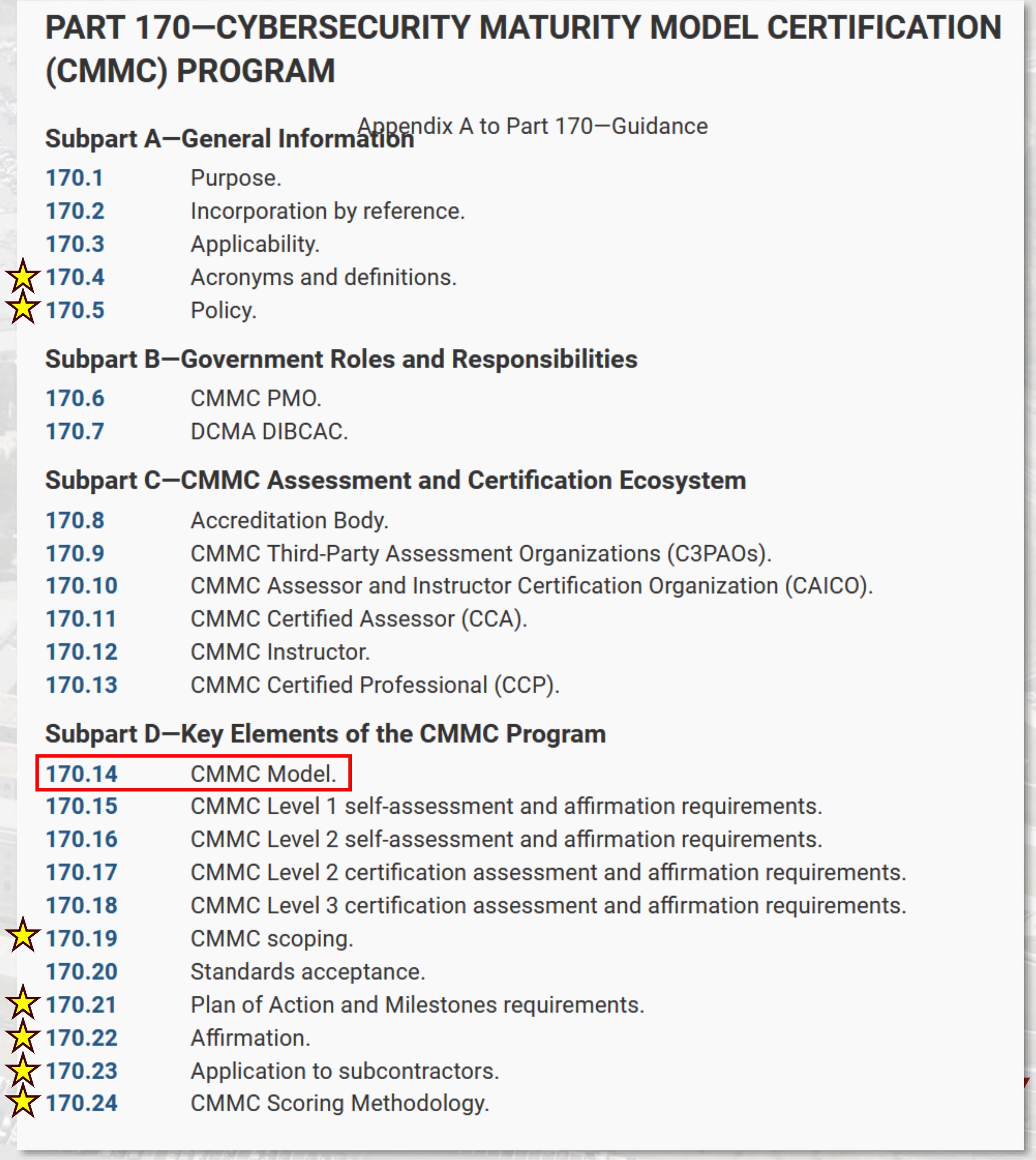
# Contractor-relevant changes in specific sections of the regulatory text (Section Heatmap)

Key Takeaway:

“Organization-defined” means as determined by the OSA.

“Periodically” means occurring at regular intervals, no less than annually.

NIST SP 800-172 Organizationally Defined Values



## PART 170—CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) PROGRAM

Appendix A to Part 170—Guidance

### Subpart A—General Information

170.1 Purpose.
170.2 Incorporation by reference.
170.3 Applicability.
☆ 170.4 Acronyms and definitions.
☆ 170.5 Policy.

### Subpart B—Government Roles and Responsibilities

170.6 CMMC PMO.
170.7 DCMA DIBCAC.

### Subpart C—CMMC Assessment and Certification Ecosystem

170.8 Accreditation Body.
170.9 CMMC Third-Party Assessment Organizations (C3PAOs).
170.10 CMMC Assessor and Instructor Certification Organization (CAICO).
170.11 CMMC Certified Assessor (CCA).
170.12 CMMC Instructor.
170.13 CMMC Certified Professional (CCP).

### Subpart D—Key Elements of the CMMC Program

170.14 CMMC Model.
170.15 CMMC Level 1 self-assessment and affirmation requirements.
170.16 CMMC Level 2 self-assessment and affirmation requirements.
170.17 CMMC Level 2 certification assessment and affirmation requirements.
170.18 CMMC Level 3 certification assessment and affirmation requirements.
☆ 170.19 CMMC scoping.
170.20 Standards acceptance.
☆ 170.21 Plan of Action and Milestones requirements.
☆ 170.22 Affirmation.
☆ 170.23 Application to subcontractors.
☆ 170.24 CMMC Scoring Methodology.

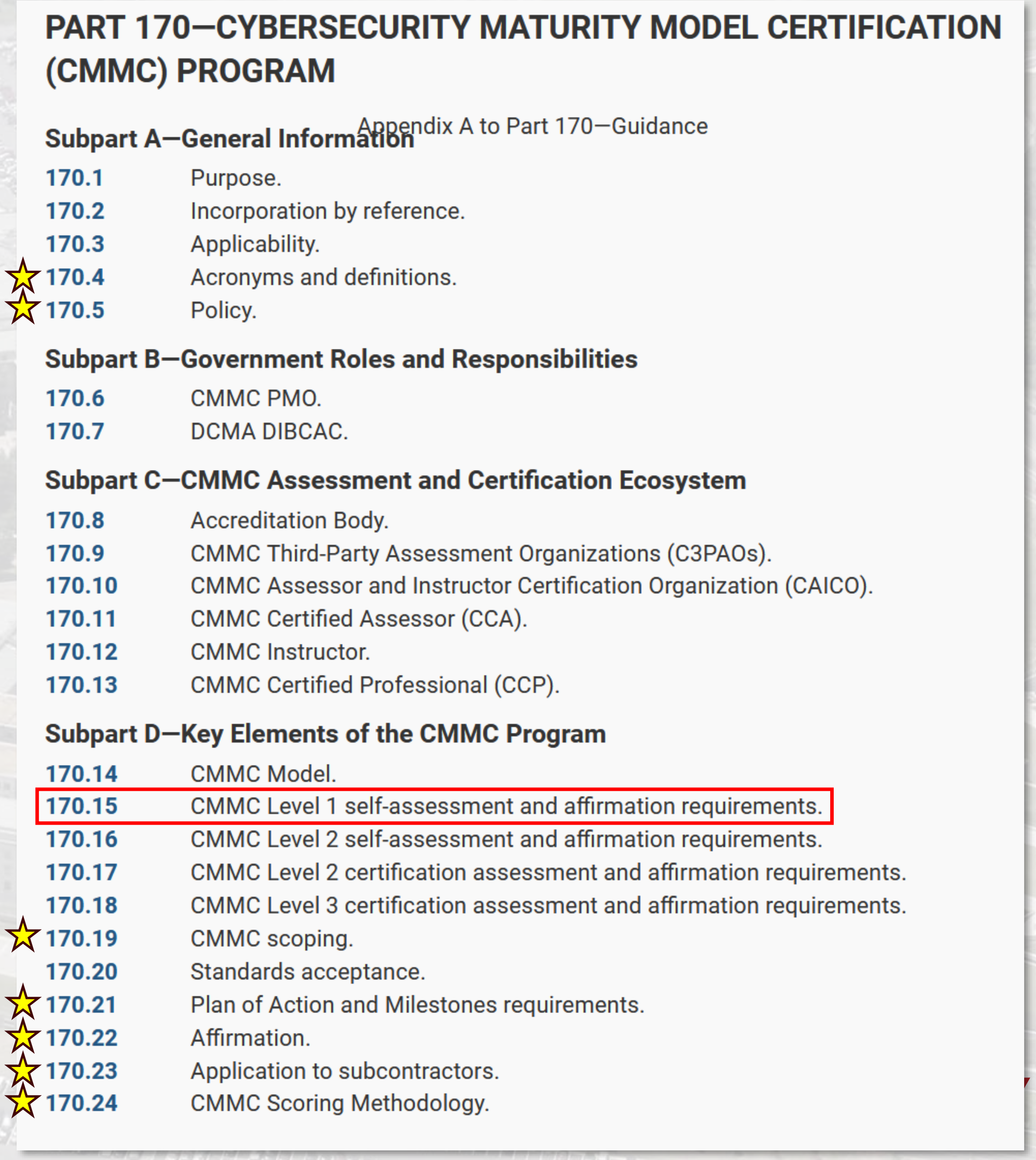
*Additional guidance can be found in appendix A

# Contractor-relevant changes in specific sections of the regulatory text (Section Heatmap)

Key Takeaway:

**Prior to award of any contract or subcontract** with a requirement for the CMMC Status of Level 1 (Self), OSAs must:

- Achieve a CMMC Status of Level 1 (Self) and
- Submit an affirmation of compliance into SPRS



## PART 170—CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) PROGRAM

Appendix A to Part 170—Guidance

### Subpart A—General Information

| | |
|---|---|
| 170.1 | Purpose. |
| 170.2 | Incorporation by reference. |
| 170.3 | Applicability. |
| ☆ 170.4 | Acronyms and definitions. |
| ☆ 170.5 | Policy. |

### Subpart B—Government Roles and Responsibilities

| | |
|---|---|
| 170.6 | CMMC PMO. |
| 170.7 | DCMA DIBCAC. |

### Subpart C—CMMC Assessment and Certification Ecosystem

| | |
|---|---|
| 170.8 | Accreditation Body. |
| 170.9 | CMMC Third-Party Assessment Organizations (C3PAOs). |
| 170.10 | CMMC Assessor and Instructor Certification Organization (CAICO). |
| 170.11 | CMMC Certified Assessor (CCA). |
| 170.12 | CMMC Instructor. |
| 170.13 | CMMC Certified Professional (CCP). |

### Subpart D—Key Elements of the CMMC Program

| | |
|---|---|
| 170.14 | CMMC Model. |
| 170.15 | CMMC Level 1 self-assessment and affirmation requirements. |
| 170.16 | CMMC Level 2 self-assessment and affirmation requirements. |
| 170.17 | CMMC Level 2 certification assessment and affirmation requirements. |
| 170.18 | CMMC Level 3 certification assessment and affirmation requirements. |
| ☆ 170.19 | CMMC scoping. |
| 170.20 | Standards acceptance. |
| ☆ 170.21 | Plan of Action and Milestones requirements. |
| ☆ 170.22 | Affirmation. |
| ☆ 170.23 | Application to subcontractors. |
| ☆ 170.24 | CMMC Scoring Methodology. |

*Additional guidance can be found in appendix A

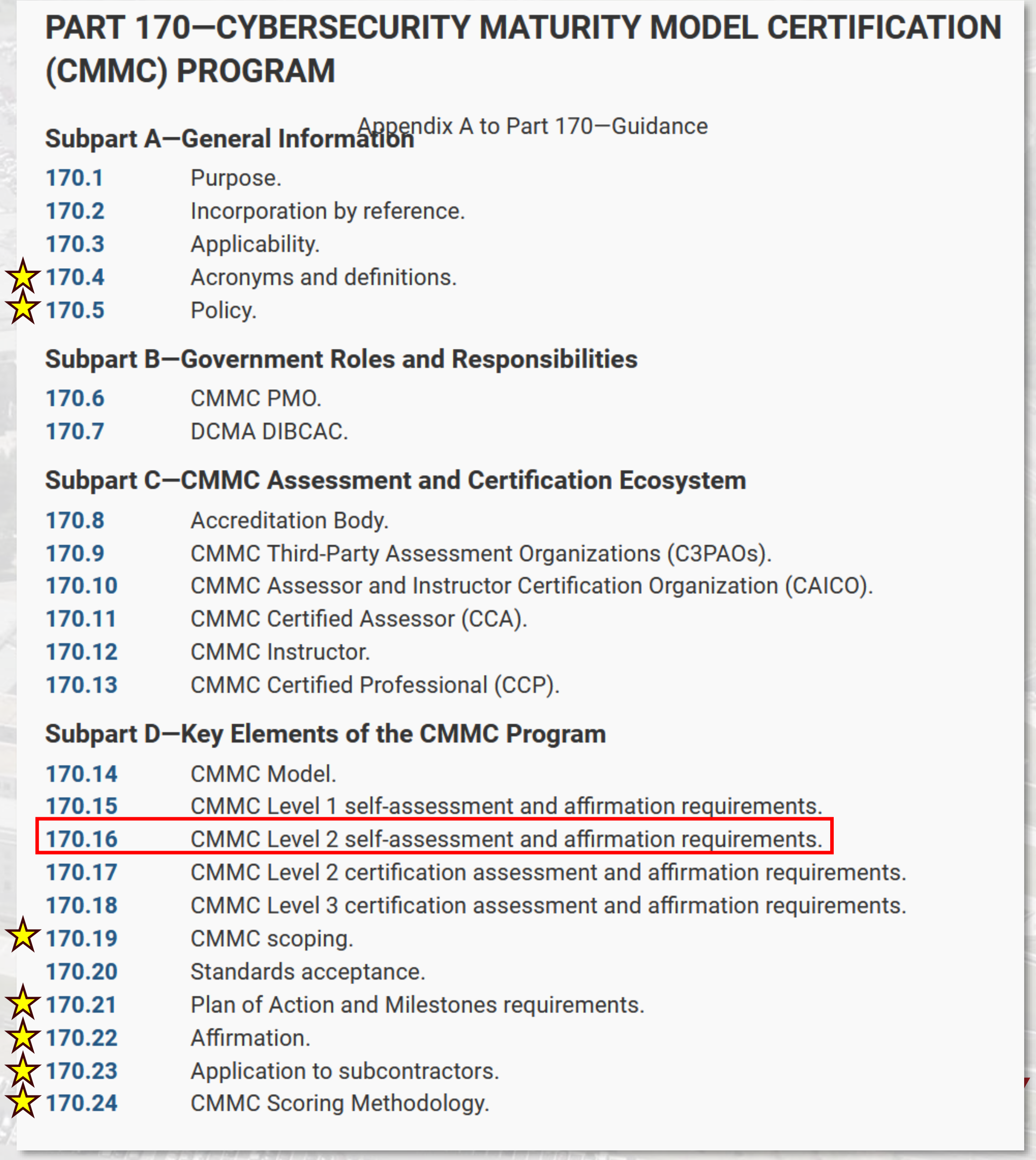
# Contractor-relevant changes in specific sections of the regulatory text (Section Heatmap)

Key Takeaway:

**Prior to award of any contract or subcontract** with requirement for CMMC Status of Level 2 (Self) the OSA must:

- Achieve a CMMC Status of either Conditional Level 2 (Self) or Final Level 2 (Self) (as a result of self-assessment)

- Submit an affirmation of compliance into SPRS



## PART 170—CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) PROGRAM

Appendix A to Part 170—Guidance

### Subpart A—General Information

| | | |
|---|---|---|
| | 170.1 | Purpose. |
| | 170.2 | Incorporation by reference. |
| | 170.3 | Applicability. |
| ★ | 170.4 | Acronyms and definitions. |
| ★ | 170.5 | Policy. |

### Subpart B—Government Roles and Responsibilities

| | | |
|---|---|---|
| | 170.6 | CMMC PMO. |
| | 170.7 | DCMA DIBCAC. |

### Subpart C—CMMC Assessment and Certification Ecosystem

| | | |
|---|---|---|
| | 170.8 | Accreditation Body. |
| | 170.9 | CMMC Third-Party Assessment Organizations (C3PAOs). |
| | 170.10 | CMMC Assessor and Instructor Certification Organization (CAICO). |
| | 170.11 | CMMC Certified Assessor (CCA). |
| | 170.12 | CMMC Instructor. |
| | 170.13 | CMMC Certified Professional (CCP). |

### Subpart D—Key Elements of the CMMC Program

| | | |
|---|---|---|
| | 170.14 | CMMC Model. |
| | 170.15 | CMMC Level 1 self-assessment and affirmation requirements. |
| | 170.16 | CMMC Level 2 self-assessment and affirmation requirements. |
| | 170.17 | CMMC Level 2 certification assessment and affirmation requirements. |
| | 170.18 | CMMC Level 3 certification assessment and affirmation requirements. |
| ★ | 170.19 | CMMC scoping. |
| | 170.20 | Standards acceptance. |
| ★ | 170.21 | Plan of Action and Milestones requirements. |
| ★ | 170.22 | Affirmation. |
| ★ | 170.23 | Application to subcontractors. |
| ★ | 170.24 | CMMC Scoring Methodology. |

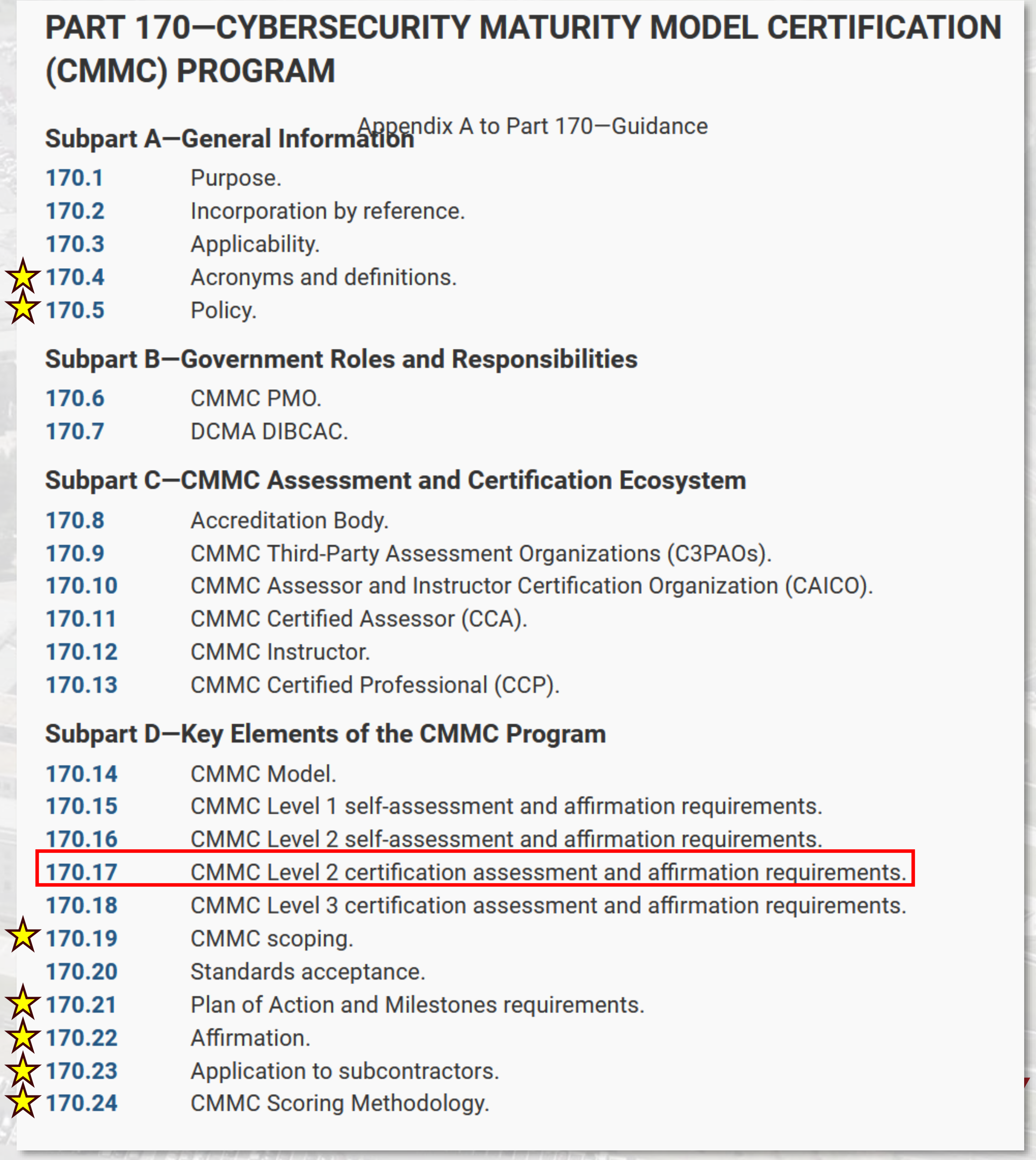
*Additional guidance can be found in appendix A

# Contractor-relevant changes in specific sections of the regulatory text (Section Heatmap)

Key Takeaway:

**Prior to award of any contract or subcontract** with a requirement for the CMMC Status of Level 2 (C3PAO) the OSA must:

- Achieve a CMMC Status of either Conditional Level 2 (C3PAO) or Final Level 2 (C3PAO) (as a result of 3rd-party assessment).
- Submit an affirmation of compliance into SPRS.



## PART 170—CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) PROGRAM

Appendix A to Part 170—Guidance

### Subpart A—General Information

| | | |
|---|---|---|
| | 170.1 | Purpose. |
| | 170.2 | Incorporation by reference. |
| | 170.3 | Applicability. |
| ★ | 170.4 | Acronyms and definitions. |
| ★ | 170.5 | Policy. |

### Subpart B—Government Roles and Responsibilities

| | |
|---|---|
| 170.6 | CMMC PMO. |
| 170.7 | DCMA DIBCAC. |

### Subpart C—CMMC Assessment and Certification Ecosystem

| | |
|---|---|
| 170.8 | Accreditation Body. |
| 170.9 | CMMC Third-Party Assessment Organizations (C3PAOs). |
| 170.10 | CMMC Assessor and Instructor Certification Organization (CAICO). |
| 170.11 | CMMC Certified Assessor (CCA). |
| 170.12 | CMMC Instructor. |
| 170.13 | CMMC Certified Professional (CCP). |

### Subpart D—Key Elements of the CMMC Program

| | | |
|---|---|---|
| | 170.14 | CMMC Model. |
| | 170.15 | CMMC Level 1 self-assessment and affirmation requirements. |
| | 170.16 | CMMC Level 2 self-assessment and affirmation requirements. |
| | 170.17 | CMMC Level 2 certification assessment and affirmation requirements. |
| | 170.18 | CMMC Level 3 certification assessment and affirmation requirements. |
| ★ | 170.19 | CMMC scoping. |
| | 170.20 | Standards acceptance. |
| ★ | 170.21 | Plan of Action and Milestones requirements. |
| ★ | 170.22 | Affirmation. |
| ★ | 170.23 | Application to subcontractors. |
| ★ | 170.24 | CMMC Scoring Methodology. |

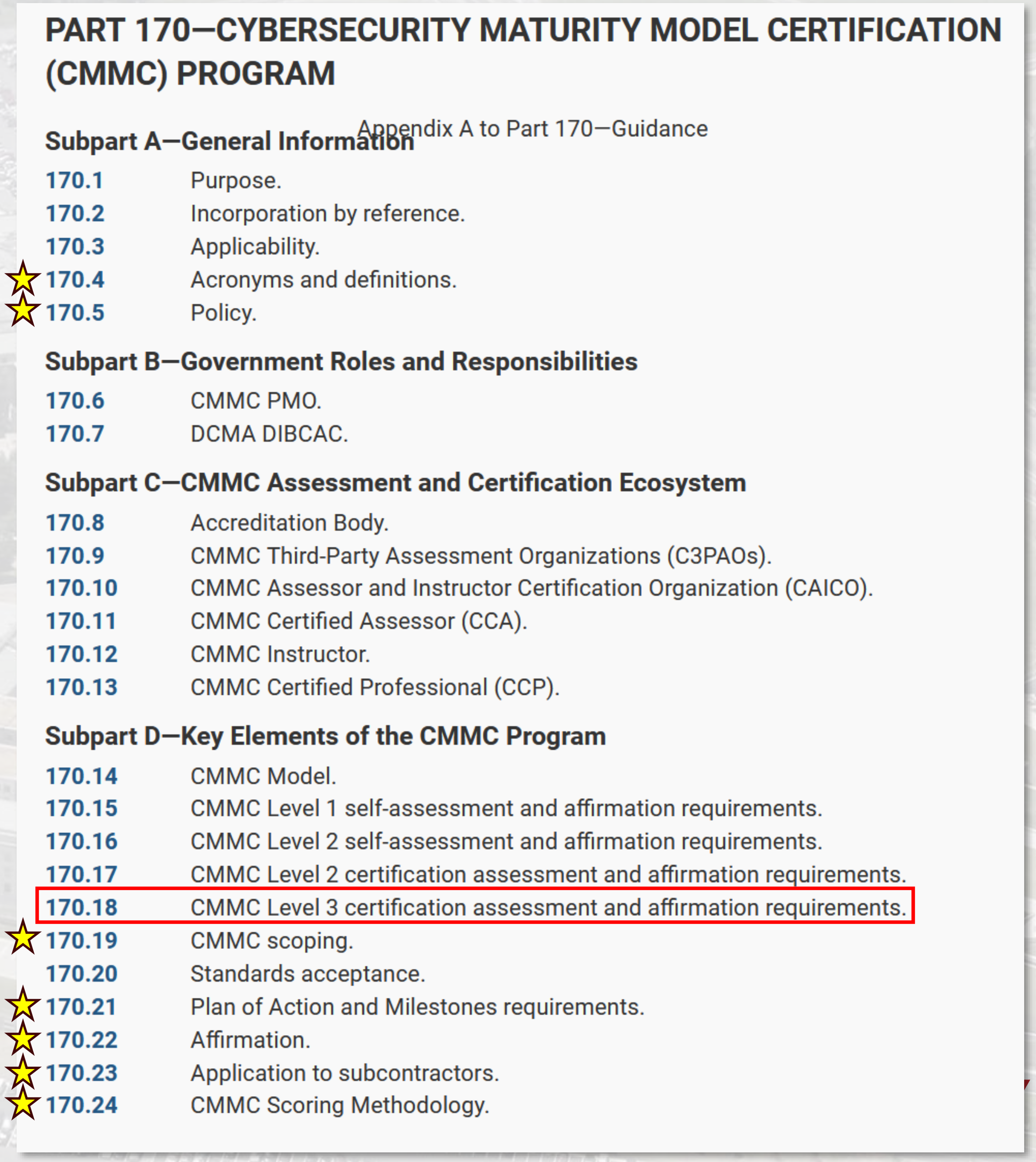
*Additional guidance can be found in appendix A

# Contractor-relevant changes in specific sections of the regulatory text (Section Heatmap)

Key Takeaway:

**Prior to award of any contract or subcontract** with requirement for CMMC Status of Level 3 (DIBCAC), the OSC must:

- Achieve a CMMC Status of either Conditional Level 3 (DIBCAC) or Final Level 3 (DIBCAC).
- Submit an affirmation of compliance into SPRS.



## PART 170—CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) PROGRAM

Appendix A to Part 170—Guidance

### Subpart A—General Information

| | |
|---|---|
| 170.1 | Purpose. |
| 170.2 | Incorporation by reference. |
| 170.3 | Applicability. |
| ★ 170.4 | Acronyms and definitions. |
| ★ 170.5 | Policy. |

### Subpart B—Government Roles and Responsibilities

| | |
|---|---|
| 170.6 | CMMC PMO. |
| 170.7 | DCMA DIBCAC. |

### Subpart C—CMMC Assessment and Certification Ecosystem

| | |
|---|---|
| 170.8 | Accreditation Body. |
| 170.9 | CMMC Third-Party Assessment Organizations (C3PAOs). |
| 170.10 | CMMC Assessor and Instructor Certification Organization (CAICO). |
| 170.11 | CMMC Certified Assessor (CCA). |
| 170.12 | CMMC Instructor. |
| 170.13 | CMMC Certified Professional (CCP). |

### Subpart D—Key Elements of the CMMC Program

| | |
|---|---|
| 170.14 | CMMC Model. |
| 170.15 | CMMC Level 1 self-assessment and affirmation requirements. |
| 170.16 | CMMC Level 2 self-assessment and affirmation requirements. |
| 170.17 | CMMC Level 2 certification assessment and affirmation requirements. |
| 170.18 | CMMC Level 3 certification assessment and affirmation requirements. |
| ★ 170.19 | CMMC scoping. |
| 170.20 | Standards acceptance. |
| ★ 170.21 | Plan of Action and Milestones requirements. |
| ★ 170.22 | Affirmation. |
| ★ 170.23 | Application to subcontractors. |
| ★ 170.24 | CMMC Scoring Methodology. |

*Additional guidance can be found in appendix A

# Contractor-relevant changes in specific sections of the regulatory text (Section Heatmap)

Key Takeaway:

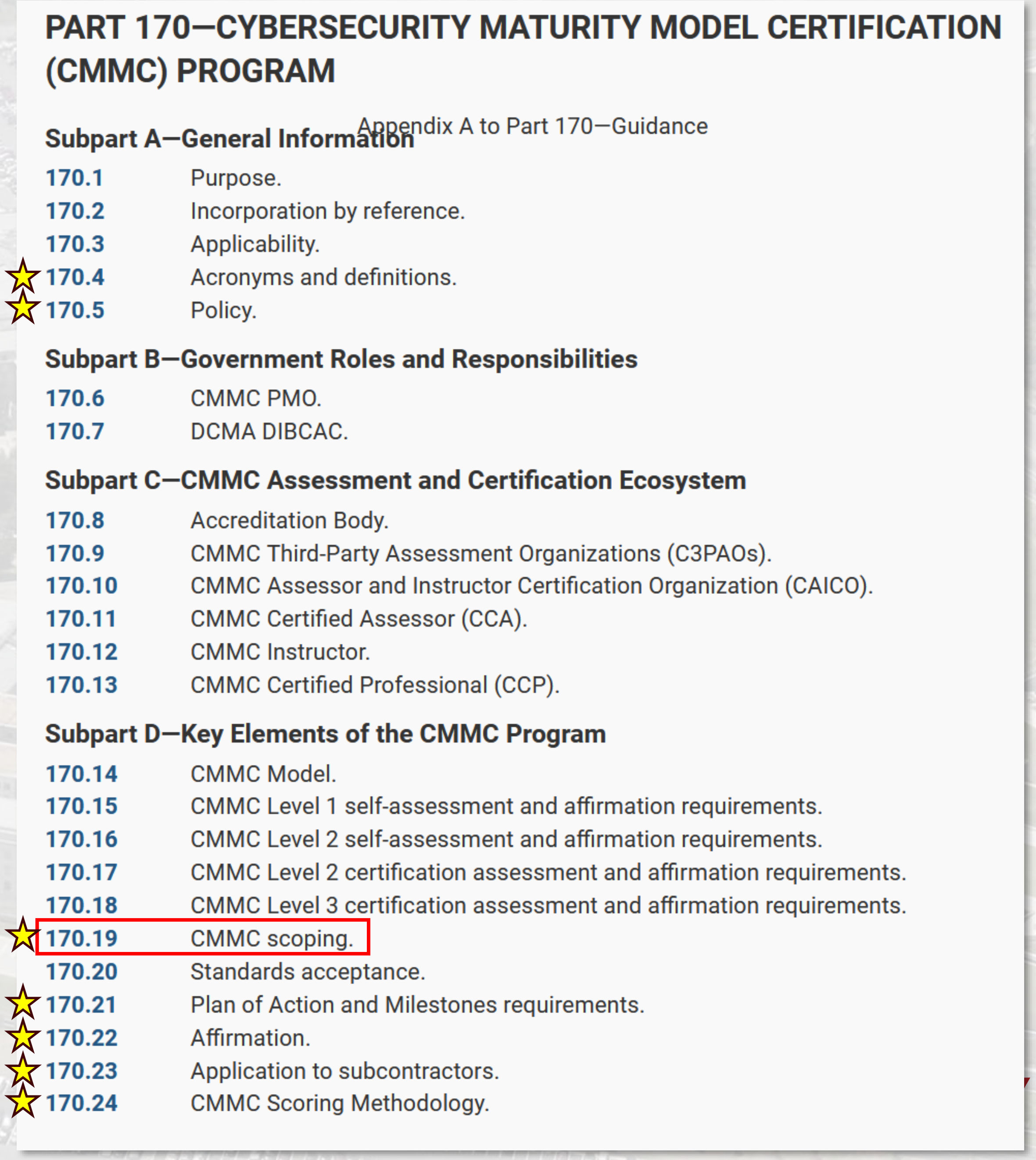
**Read the scoping guides**

**Your MSP is in-scope for your assessment**

**CUI in the cloud carries additional requirements**

**Things change between L2 and L3**

**VDI**



## PART 170—CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) PROGRAM

Appendix A to Part 170—Guidance

### Subpart A—General Information

| | | |
|---|---|---|
| | 170.1 | Purpose. |
| | 170.2 | Incorporation by reference. |
| | 170.3 | Applicability. |
| ★ | 170.4 | Acronyms and definitions. |
| ★ | 170.5 | Policy. |

### Subpart B—Government Roles and Responsibilities

| | | |
|---|---|---|
| | 170.6 | CMMC PMO. |
| | 170.7 | DCMA DIBCAC. |

### Subpart C—CMMC Assessment and Certification Ecosystem

| | | |
|---|---|---|
| | 170.8 | Accreditation Body. |
| | 170.9 | CMMC Third-Party Assessment Organizations (C3PAOs). |
| | 170.10 | CMMC Assessor and Instructor Certification Organization (CAICO). |
| | 170.11 | CMMC Certified Assessor (CCA). |
| | 170.12 | CMMC Instructor. |
| | 170.13 | CMMC Certified Professional (CCP). |

### Subpart D—Key Elements of the CMMC Program

| | | |
|---|---|---|
| | 170.14 | CMMC Model. |
| | 170.15 | CMMC Level 1 self-assessment and affirmation requirements. |
| | 170.16 | CMMC Level 2 self-assessment and affirmation requirements. |
| | 170.17 | CMMC Level 2 certification assessment and affirmation requirements. |
| | 170.18 | CMMC Level 3 certification assessment and affirmation requirements. |
| ★ | 170.19 | CMMC scoping. |
| | 170.20 | Standards acceptance. |
| ★ | 170.21 | Plan of Action and Milestones requirements. |
| ★ | 170.22 | Affirmation. |
| ★ | 170.23 | Application to subcontractors. |
| ★ | 170.24 | CMMC Scoring Methodology. |

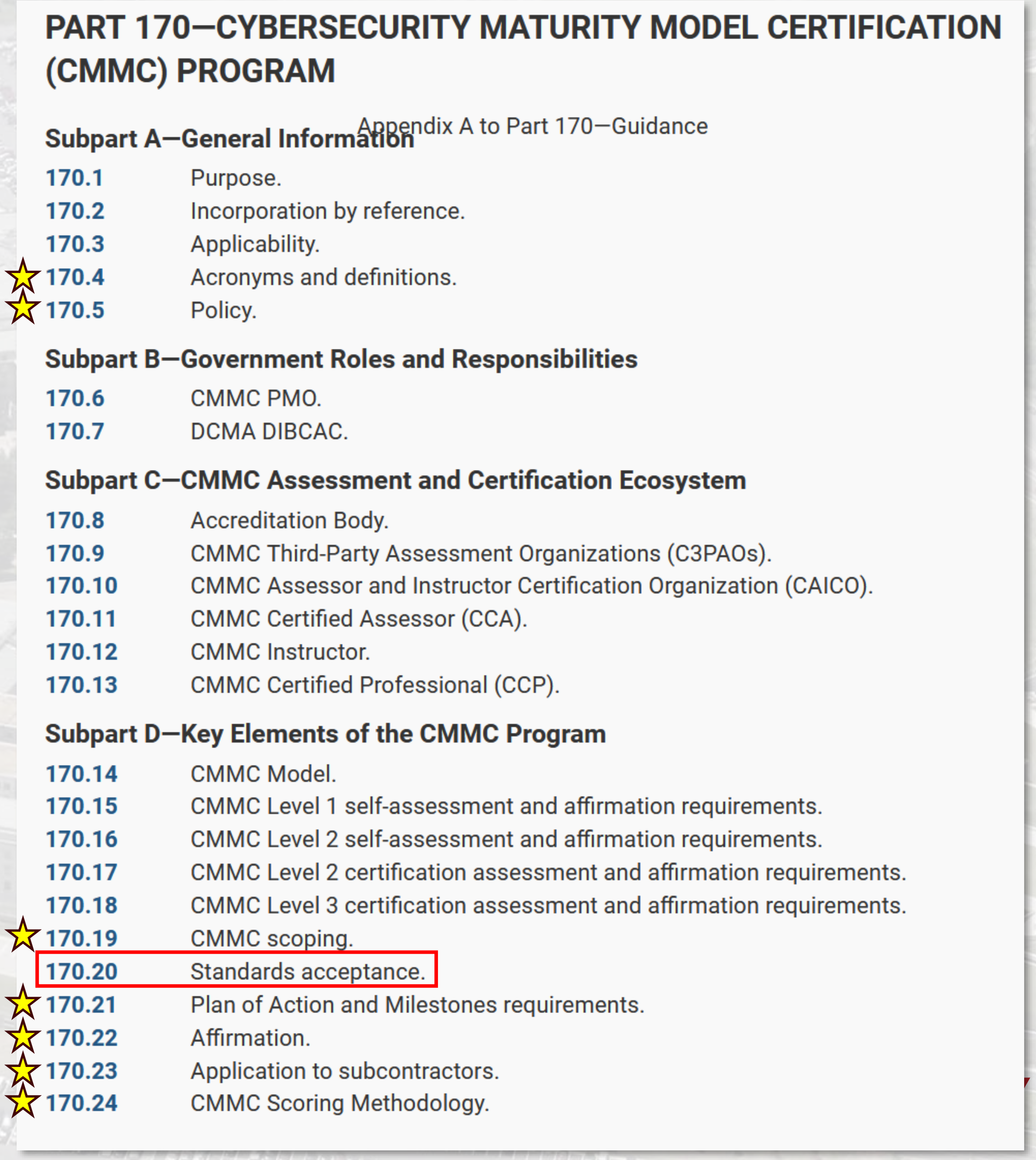
*Additional guidance can be found in appendix A

# Contractor-relevant changes in specific sections of the regulatory text (Section Heatmap)

Key Takeaway:

OSCs that have completed a DCMA DIBCAC High Assessment (including Joint Surveillance Assessments) aligned with CMMC Level 2 Scoping will be given the CMMC Status of Final Level 2 (C3PAO) if:

- Perfect score with no open POA&M items
- Assessment conducted prior to 12/16/2024



## PART 170—CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) PROGRAM

Appendix A to Part 170—Guidance

### Subpart A—General Information

| | | |
|---|---|---|
| | 170.1 | Purpose. |
| | 170.2 | Incorporation by reference. |
| | 170.3 | Applicability. |
| ★ | 170.4 | Acronyms and definitions. |
| ★ | 170.5 | Policy. |

### Subpart B—Government Roles and Responsibilities

| | | |
|---|---|---|
| | 170.6 | CMMC PMO. |
| | 170.7 | DCMA DIBCAC. |

### Subpart C—CMMC Assessment and Certification Ecosystem

| | | |
|---|---|---|
| | 170.8 | Accreditation Body. |
| | 170.9 | CMMC Third-Party Assessment Organizations (C3PAOs). |
| | 170.10 | CMMC Assessor and Instructor Certification Organization (CAICO). |
| | 170.11 | CMMC Certified Assessor (CCA). |
| | 170.12 | CMMC Instructor. |
| | 170.13 | CMMC Certified Professional (CCP). |

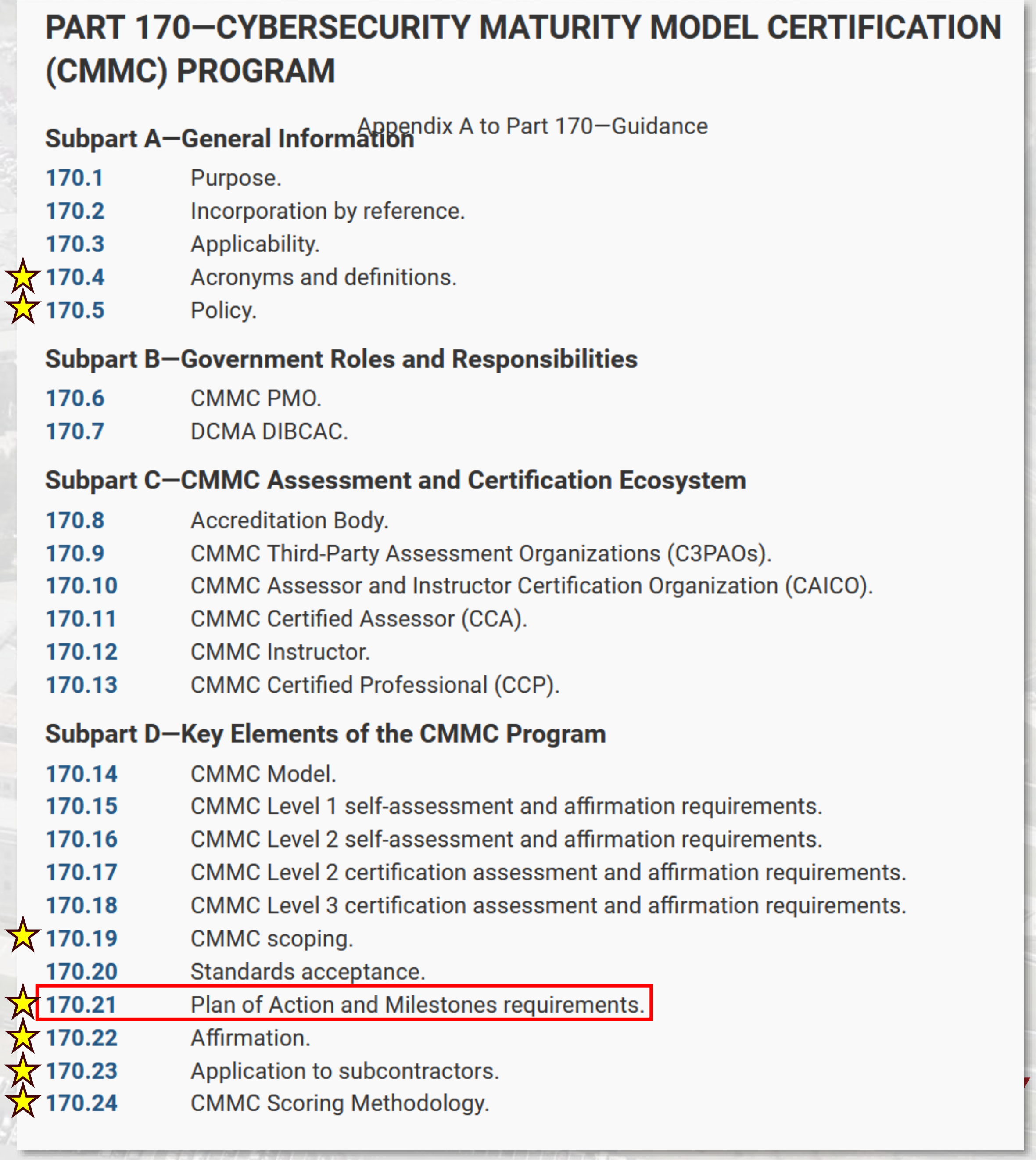
### Subpart D—Key Elements of the CMMC Program

| | | |
|---|---|---|
| | 170.14 | CMMC Model. |
| | 170.15 | CMMC Level 1 self-assessment and affirmation requirements. |
| | 170.16 | CMMC Level 2 self-assessment and affirmation requirements. |
| | 170.17 | CMMC Level 2 certification assessment and affirmation requirements. |
| | 170.18 | CMMC Level 3 certification assessment and affirmation requirements. |
| ★ | 170.19 | CMMC scoping. |
| | 170.20 | Standards acceptance. |
| ★ | 170.21 | Plan of Action and Milestones requirements. |
| ★ | 170.22 | Affirmation. |
| ★ | 170.23 | Application to subcontractors. |
| ★ | 170.24 | CMMC Scoring Methodology. |

# Contractor-relevant changes in specific sections of the regulatory text (Section Heatmap)

Key Takeaway:

POA&Ms are extremely limited – study carefully



## PART 170—CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) PROGRAM

### Subpart A—General Information

Appendix A to Part 170—Guidance

| | | |
|---|---|---|
| | 170.1 | Purpose. |
| | 170.2 | Incorporation by reference. |
| | 170.3 | Applicability. |
| ★ | 170.4 | Acronyms and definitions. |
| ★ | 170.5 | Policy. |

### Subpart B—Government Roles and Responsibilities

| | | |
|---|---|---|
| | 170.6 | CMMC PMO. |
| | 170.7 | DCMA DIBCAC. |

### Subpart C—CMMC Assessment and Certification Ecosystem

| | | |
|---|---|---|
| | 170.8 | Accreditation Body. |
| | 170.9 | CMMC Third-Party Assessment Organizations (C3PAOs). |
| | 170.10 | CMMC Assessor and Instructor Certification Organization (CAICO). |
| | 170.11 | CMMC Certified Assessor (CCA). |
| | 170.12 | CMMC Instructor. |
| | 170.13 | CMMC Certified Professional (CCP). |

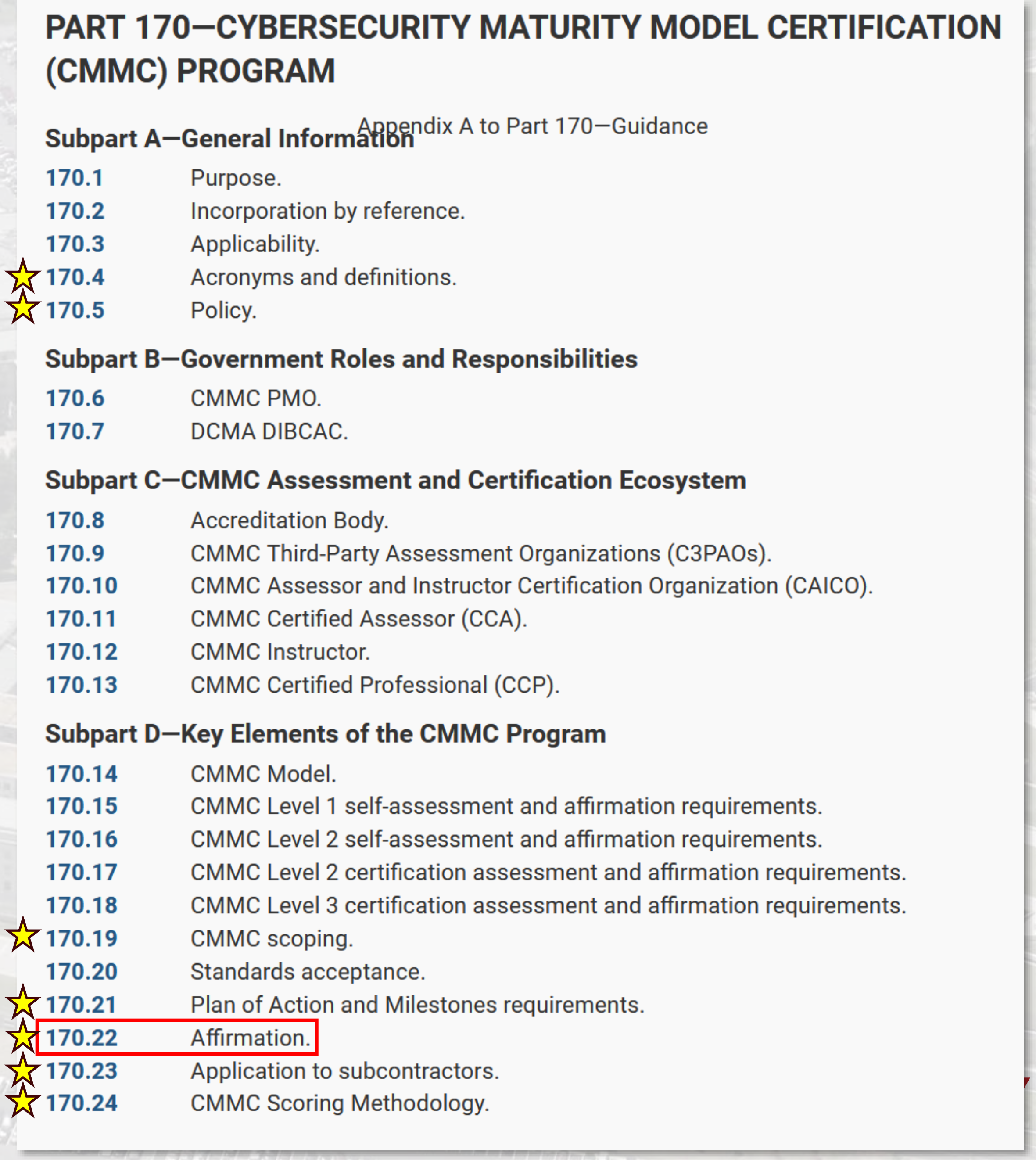
### Subpart D—Key Elements of the CMMC Program

| | | |
|---|---|---|
| | 170.14 | CMMC Model. |
| | 170.15 | CMMC Level 1 self-assessment and affirmation requirements. |
| | 170.16 | CMMC Level 2 self-assessment and affirmation requirements. |
| | 170.17 | CMMC Level 2 certification assessment and affirmation requirements. |
| | 170.18 | CMMC Level 3 certification assessment and affirmation requirements. |
| ★ | 170.19 | CMMC scoping. |
| | 170.20 | Standards acceptance. |
| ★ | 170.21 | Plan of Action and Milestones requirements. |
| ★ | 170.22 | Affirmation. |
| ★ | 170.23 | Application to subcontractors. |
| ★ | 170.24 | CMMC Scoring Methodology. |

# Contractor-relevant changes in specific sections of the regulatory text (Section Heatmap)

Key Takeaway:

The Affirming Official is the senior level representative from within each Organization Seeking Assessment (OSA) who is responsible for ensuring the OSA's compliance with the CMMC Program requirements and has the authority to affirm the OSA's continuing compliance with the specified security requirements for their respective organizations.



## PART 170—CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) PROGRAM

Appendix A to Part 170—Guidance

### Subpart A—General Information

| | | |
|---|---|---|
| | 170.1 | Purpose. |
| | 170.2 | Incorporation by reference. |
| | 170.3 | Applicability. |
| ★ | 170.4 | Acronyms and definitions. |
| ★ | 170.5 | Policy. |

### Subpart B—Government Roles and Responsibilities

| | | |
|---|---|---|
| | 170.6 | CMMC PMO. |
| | 170.7 | DCMA DIBCAC. |

### Subpart C—CMMC Assessment and Certification Ecosystem

| | | |
|---|---|---|
| | 170.8 | Accreditation Body. |
| | 170.9 | CMMC Third-Party Assessment Organizations (C3PAOs). |
| | 170.10 | CMMC Assessor and Instructor Certification Organization (CAICO). |
| | 170.11 | CMMC Certified Assessor (CCA). |
| | 170.12 | CMMC Instructor. |
| | 170.13 | CMMC Certified Professional (CCP). |

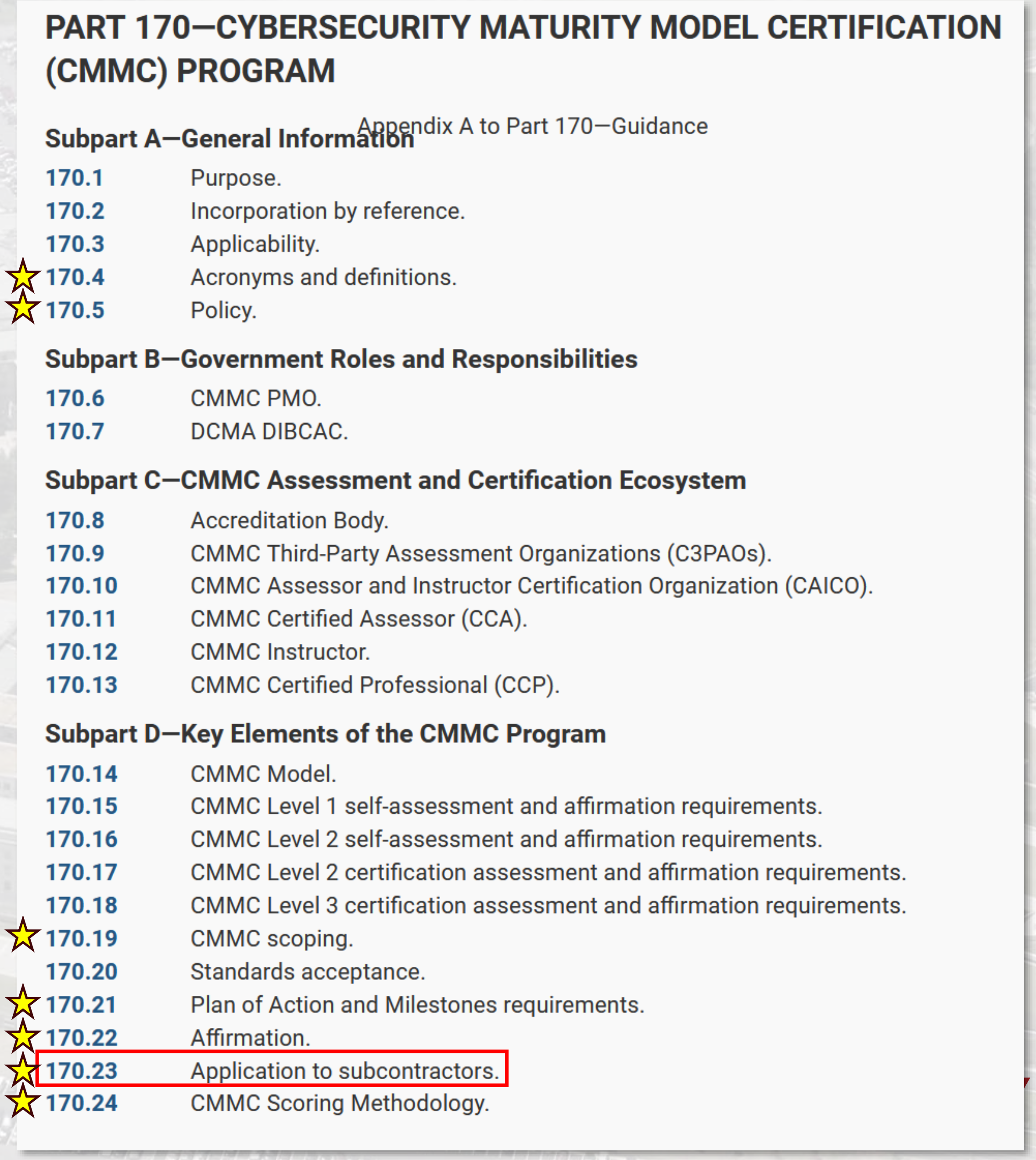
### Subpart D—Key Elements of the CMMC Program

| | | |
|---|---|---|
| | 170.14 | CMMC Model. |
| | 170.15 | CMMC Level 1 self-assessment and affirmation requirements. |
| | 170.16 | CMMC Level 2 self-assessment and affirmation requirements. |
| | 170.17 | CMMC Level 2 certification assessment and affirmation requirements. |
| | 170.18 | CMMC Level 3 certification assessment and affirmation requirements. |
| ★ | 170.19 | CMMC scoping. |
| | 170.20 | Standards acceptance. |
| ★ | 170.21 | Plan of Action and Milestones requirements. |
| ★ | 170.22 | Affirmation. |
| ★ | 170.23 | Application to subcontractors. |
| ★ | 170.24 | CMMC Scoring Methodology. |

# Contractor-relevant changes in specific sections of the regulatory text (Section Heatmap)

Key Takeaway:

If a subcontractor will process, store, or transmit CUI in performance of the subcontract and the associated prime contract has a requirement for a CMMC Status of Level 2 (C3PAO), then the CMMC Status of Level 2 (C3PAO) is the minimum requirement for the subcontractor.



## PART 170—CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) PROGRAM

**Subpart A—General Information**

Appendix A to Part 170—Guidance

170.1 Purpose.
170.2 Incorporation by reference.
170.3 Applicability.
☆ 170.4 Acronyms and definitions.
☆ 170.5 Policy.

**Subpart B—Government Roles and Responsibilities**

170.6 CMMC PMO.
170.7 DCMA DIBCAC.

**Subpart C—CMMC Assessment and Certification Ecosystem**

170.8 Accreditation Body.
170.9 CMMC Third-Party Assessment Organizations (C3PAOs).
170.10 CMMC Assessor and Instructor Certification Organization (CAICO).
170.11 CMMC Certified Assessor (CCA).
170.12 CMMC Instructor.
170.13 CMMC Certified Professional (CCP).

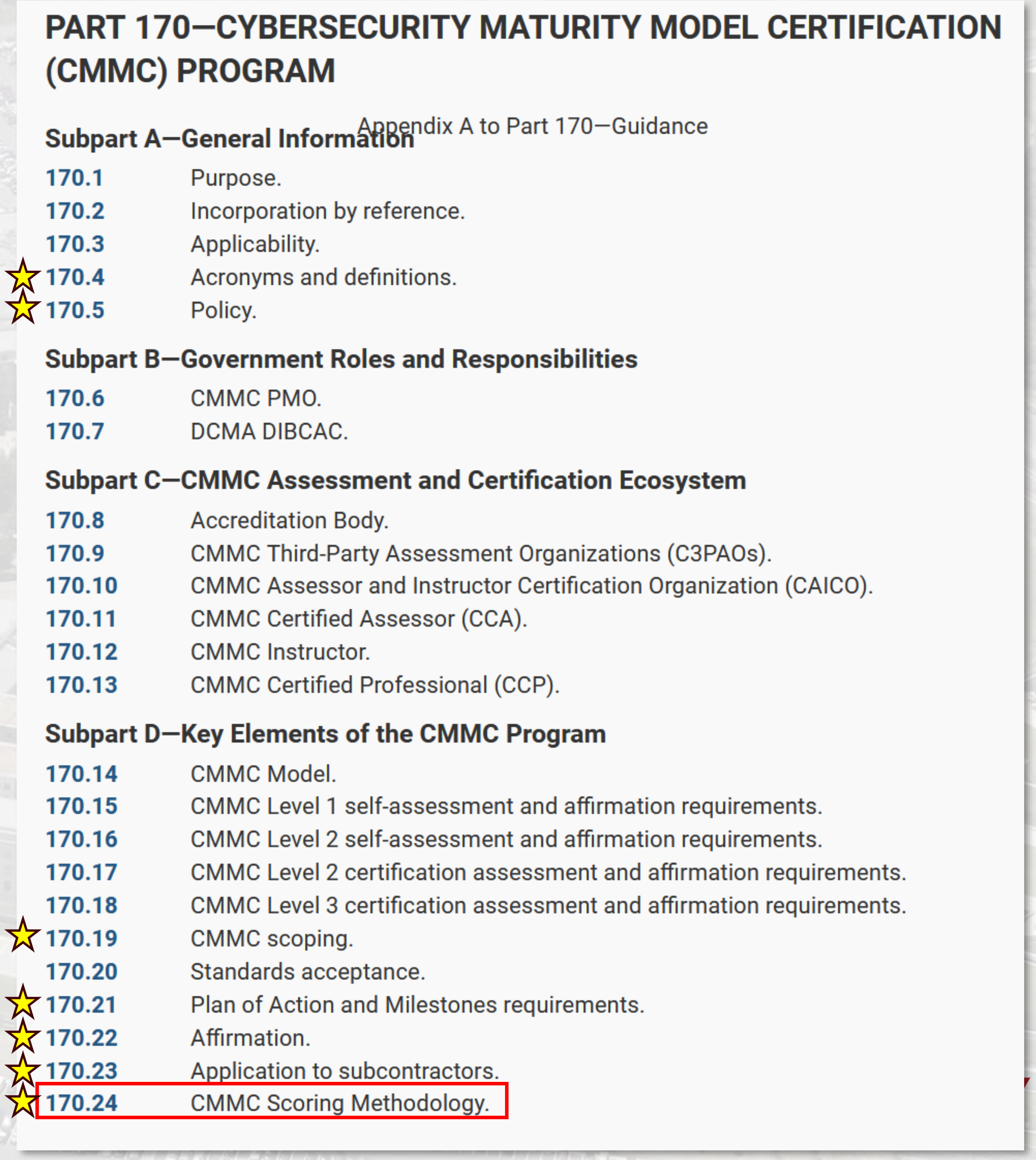
**Subpart D—Key Elements of the CMMC Program**

170.14 CMMC Model.
170.15 CMMC Level 1 self-assessment and affirmation requirements.
170.16 CMMC Level 2 self-assessment and affirmation requirements.
170.17 CMMC Level 2 certification assessment and affirmation requirements.
170.18 CMMC Level 3 certification assessment and affirmation requirements.
☆ 170.19 CMMC scoping.
170.20 Standards acceptance.
☆ 170.21 Plan of Action and Milestones requirements.
☆ 170.22 Affirmation.
☆ 170.23 Application to subcontractors.
☆ 170.24 CMMC Scoring Methodology.

## Contractor-relevant changes in specific sections of the regulatory text (Section Heatmap)

Key Takeaway:

POA&Ms are limited by total passing score – study carefully.



### PART 170—CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) PROGRAM

Appendix A to Part 170—Guidance

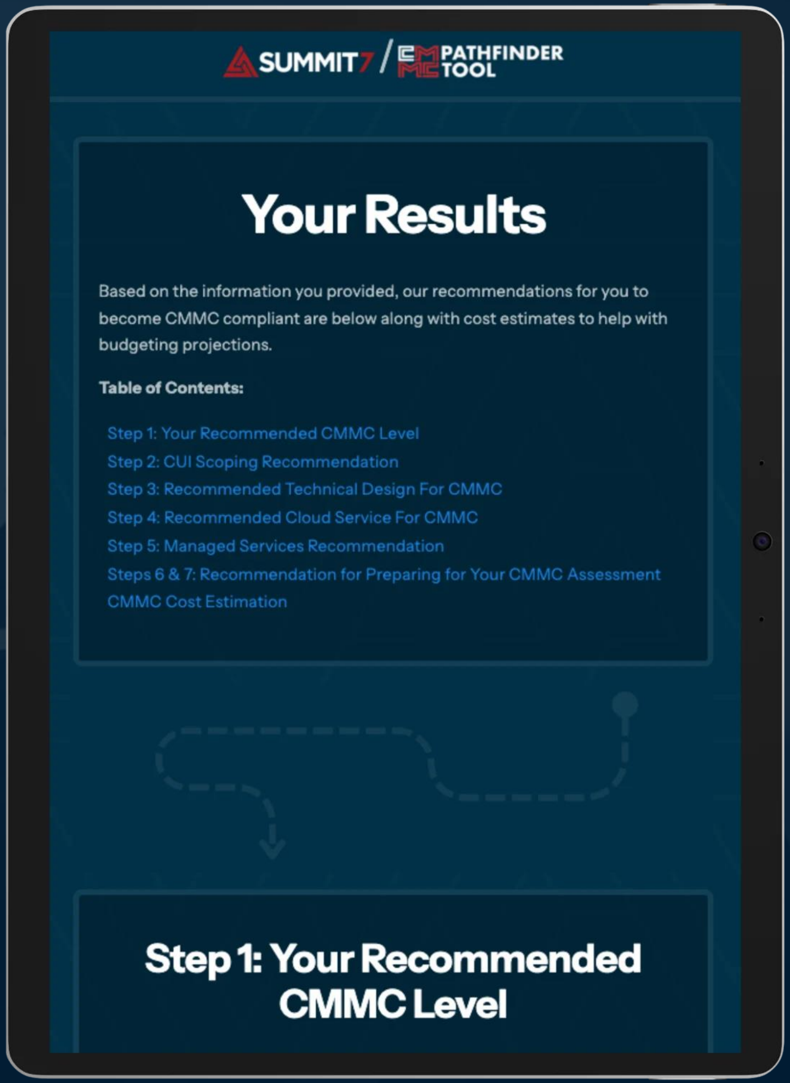
# Summary

# Achieving CMMC status and complying with CMMC program requirements will be a CONDITION OF CONTRACT AWARD

- DoD contractors have had cybersecurity requirements in their contracts since 2013.
- Since 2016 these cyber requirements have remained effectively unchanged.
- Since 2020 DoD contractors handling CUI have been required to calculate a self-assessment score and upload it to SPRS.
- Starting in Q2 2025, DoD contractors will need to prove that their cyber requirements have been implemented to take award of DoD contracts.
- It generally takes DoD contractors 6 – 18 months to get “assessment ready”.
- The overall program governing this process is known as the Cybersecurity Maturity Model Certification or “CMMC”.
- Once a CMMC level requirement is specified in a DoD solicitation, there are no waivers.
- There are no exceptions for small businesses.
- There is no reciprocity with other cybersecurity standards like ISO or SOC.
- CMMC makes no modifications to existing cyber requirements.
- The odds of you being allowed to self-assess for Level 2 are very small.

# CMMC PATHFINDER TOOL

summit7.us/pathfinder



## Your Results

Based on the information you provided, our recommendations for you to become CMMC compliant are below along with cost estimates to help with budgeting projections.

**Table of Contents:**

- Step 1: Your Recommended CMMC Level
- Step 2: CUI Scoping Recommendation
- Step 3: Recommended Technical Design For CMMC
- Step 4: Recommended Cloud Service For CMMC
- Step 5: Managed Services Recommendation
- Steps 6 & 7: Recommendation for Preparing for Your CMMC Assessment
- CMMC Cost Estimation

## Step 1: Your Recommended CMMC Level

SUMMIT7

Q & A

# Questions & Answers

✉ **Contact Us:** cmmc@summit7.us

SUMMIT7