CONNECTIONS
Knowledge Trust

BRIEFING

CMMC AND YOU

What the standard actually requires, where the program stands today, and what it means for contractors.

Rodd Ahrenstorff

AUGUST 2026

AGENDA · 60 MINUTES

WHAT WE'LL COVER

01

What CMMC is

FCI and CUI, the three levels, the two rules that make it binding

02

Where the program stands

Phase I live, Phase II suspended, a task force is formed but not active

03

The challenge

Where the work is, and the risk of sitting it out

04

What you have to do

You are in scope: tooling, matrix, scoring, packaging

PART 01

WHAT CMMC ACTUALLY IS

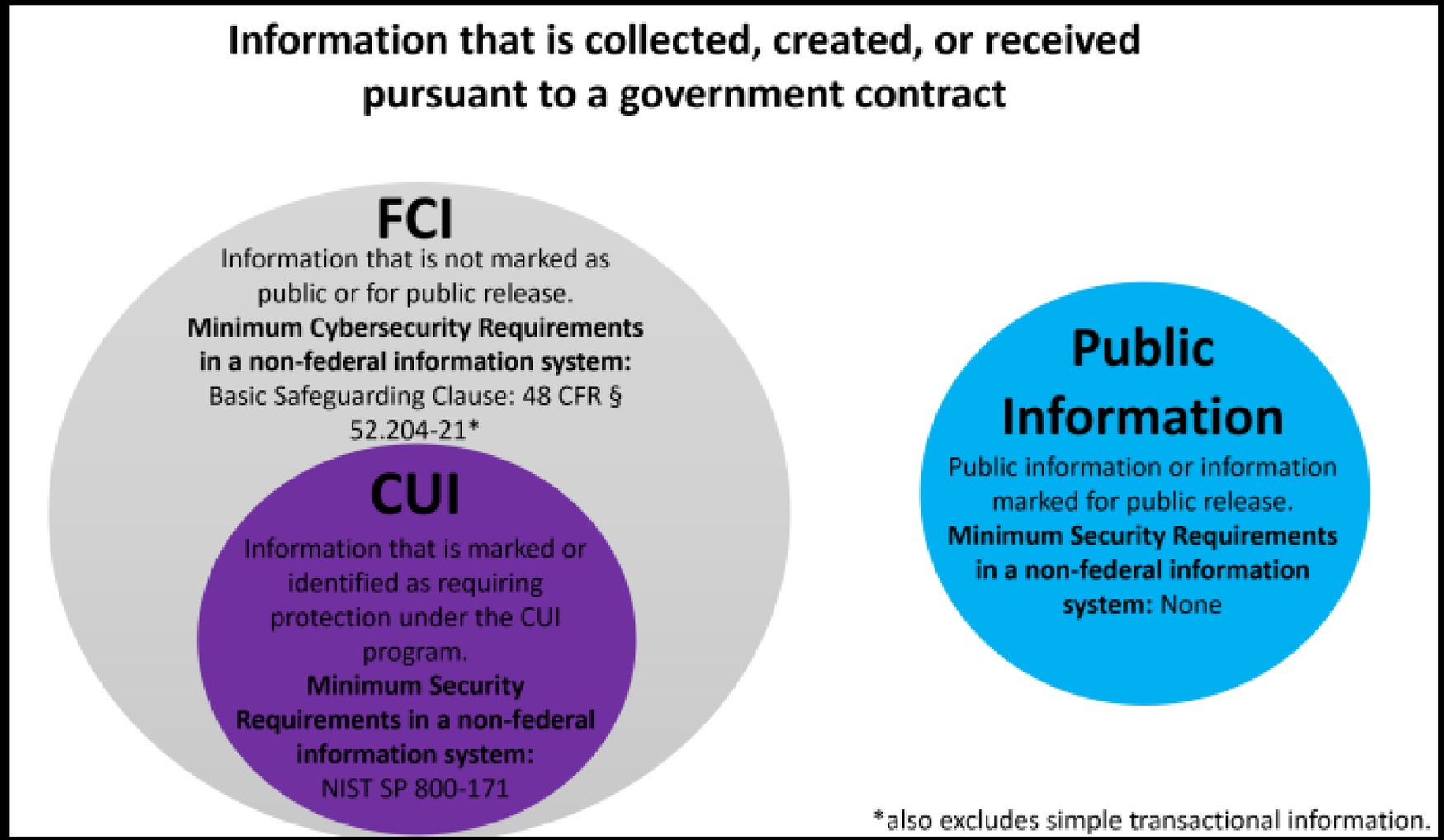
A verification program bolted onto a security standard the DoD has required since 2017.

Cybersecurity maturity model certification



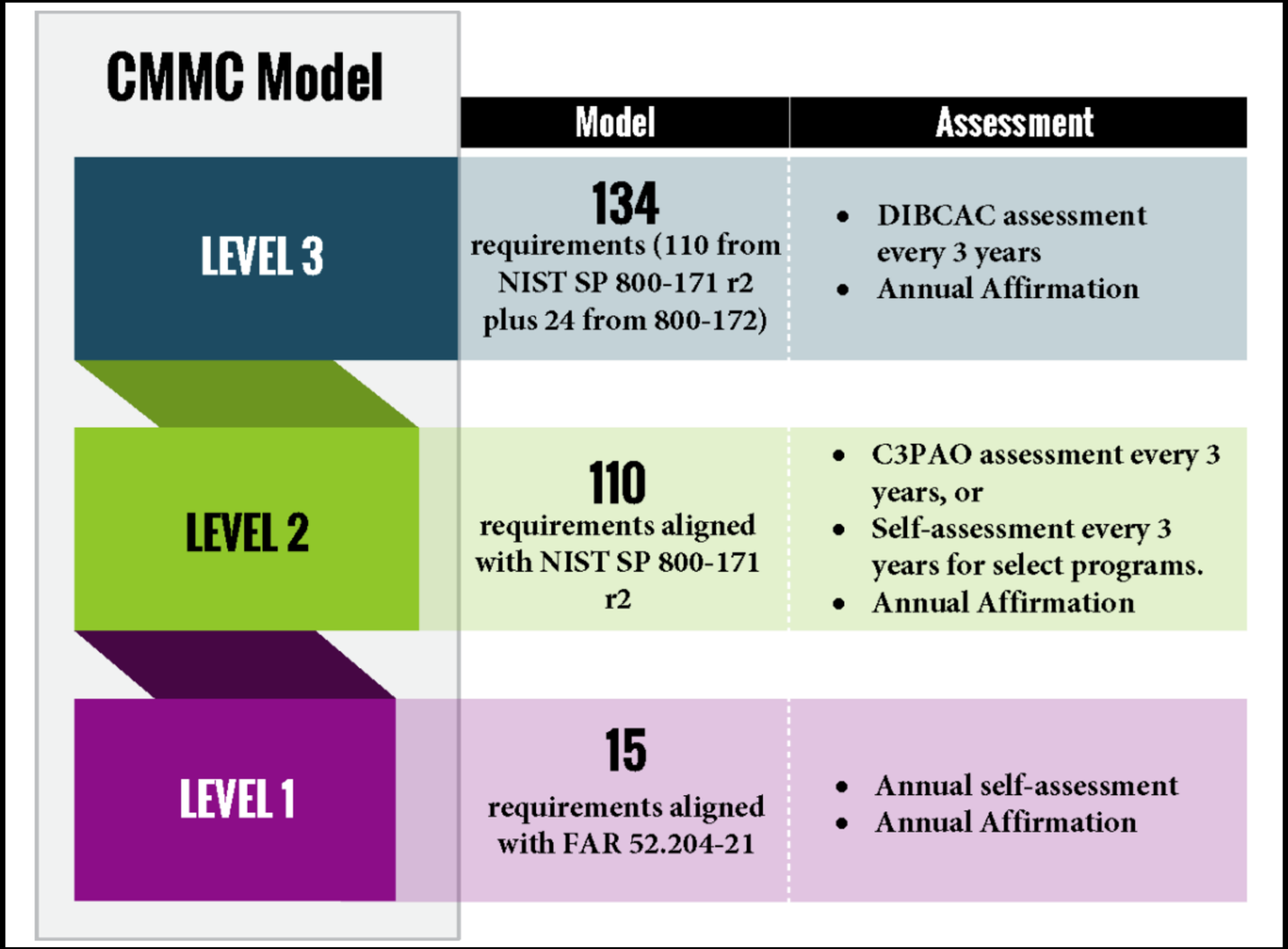
PART 01 — THE DATA

TWO KINDS OF DATA



PART 01 — THE MODEL

THREE LEVELS



PART 02 — ORIGIN

TWENTY - FIVE YEARS IN THE MAKING

DEFINING THE DATA

2001

An information-sharing problem

After 9/11 the government found terrorism information sitting in silos. Better sharing required agreeing on what the sensitive-but-unclassified data even was.

2009

CUI task force report

A federal task force recommended expanding the definition well past terrorism, to all categories of controlled unclassified data.

2010

Executive Order 13556

Created the CUI Program. One CUI program across 15 departments, 78 agencies, 173 bureaus. Requirements for non-federal systems, and a FAR rule to reach every contractor.

2015 → 2017

DFARS 252.204-7012

The contract requirement lands in 2015 with a grace period, fully in force from December 2017. Self-attested, largely unverified.

VERIFYING THE REQUIREMENT

2019 → 2020

CMMC announced, 1.0 published

Five maturity levels and third-party assessment, to close the verification gap DFARS left open.

2021

CMMC 2.0

Rebuilt to three levels, aligned to NIST SP 800-171, with self-assessment restored at the lower tier.

2024 → 2025

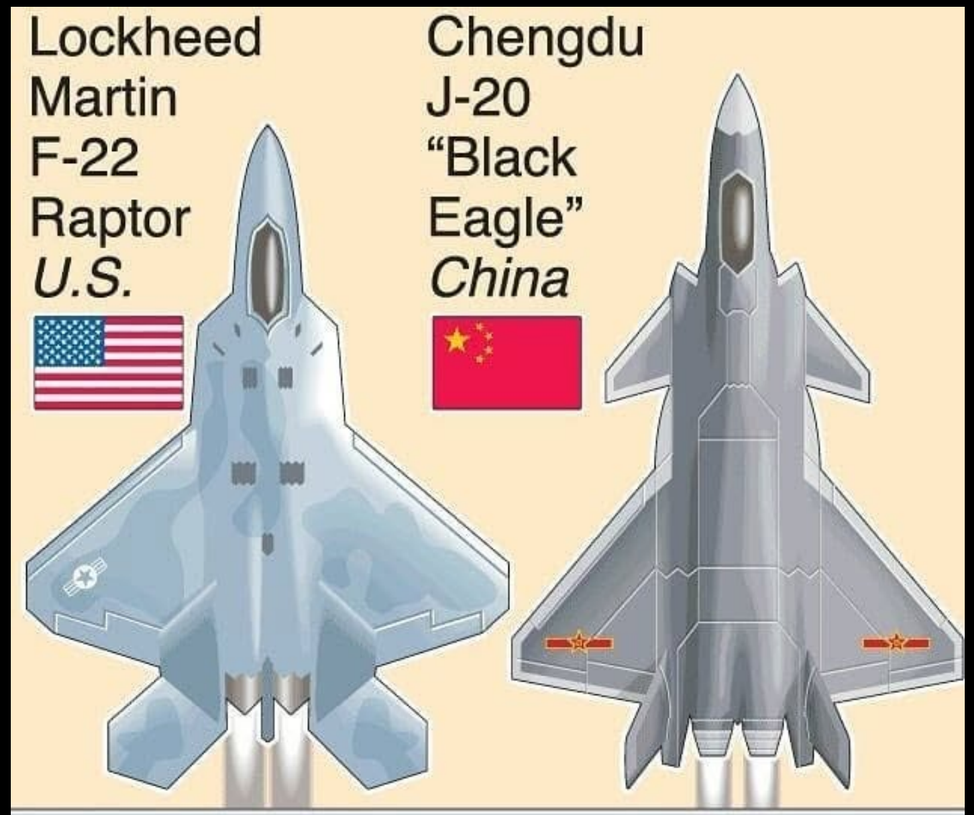
The two rules land

32 CFR Part 170 makes assessments possible in 2024. The 48 CFR rule makes CMMC a binding condition of award.

The plan — four phases

Nov 2025	Phase 1 — L1/L2 self-assessment
Nov 2026	Phase 2 — L2 certification
Nov 2027	Phase 3 — L3 certification
Nov 2028	Phase 4 — full implementation

CHINESE THEFT OF F -35 DATA



Length: **18.9m**	**20.3m**
Empty weight: **19,700kg**	**19,400kg**
Internal fuel: **8,200kg**	**11,340kg**
Max. speed: **Mach 2**	**Mach 1.7**
Introduction: **2005**	**2018**

China’s J-31 stealth fighter is built in part on plans taken from the US as part of a long-running espionage program. The breach occurred in 2007, and came through a subcontractor to Lockheed Martin, the principal maker of the F-35.

PART 02 — TIMELINE

HOW WE GOT TO September 2026

NOV 10, 2025

Phase I goes live

Level 1 and Level 2 self-assessments required at award on most new contracts.

JUL 13, 2026

Phase II suspended



DoW CIO Kirsten Davies, suspends the third-party assessment phase and all pending milestones, and stands up a CMMC Reform Task Force with a 60-day review.

~SEP 13, 2026

Task force report due

Recommendations to the DoW CIO. Industry RFI comments closed August 14.

Task force update

A Sept. 3 memo has directed contracting officers to strip out from contracts any and all of CMMC's requirements for third-party assessments. The department has since suspended that plan for a 60-day review.

DOW CIO MEMORANDUM, JULY 13, 2026

PART 02

WHERE THE PROGRAM STANDS

Phase I is live. Phase II is suspended. A reform task force still exists but is NOT currently in a review period.



PART 02 — THE SUSPENSION

WHAT MOVED, WHAT DIDN'T

STILL IN FORCE

DFARS 252.204-7012 and NIST SP 800-171 implementation, as your contracts already require

Phase I Level 1 and Level 2 self-assessment requirements

SPRS submission, senior-official affirmation, and annual refresh

False Claims Act exposure for an inaccurate score

Prime flow-down obligations already written into subcontracts

ON HOLD

Phase II mandatory C3PAO certification, which was set for November 10, 2026

Phases 3 and 4, including Level 3 milestones

All other pending and future CMMC milestones, “until further notice”

CONTRACTING OFFICES CONTINUE ACCEPTING SELF-ASSESSMENTS

PART 03

THE Advantages

The DIB cannot do this without strong IT support.



PART 03 — Advantages

THE ADVANTAGEs

Many defense contractors, especially in the SMB and mid-market range, do not have mature IT teams. They're looking to their MSPs to guide them through complex cybersecurity frameworks like NIST 800-171 and CMMC Level 1 & 2.

01

Increaseed cyber security posture

02

Differentiate in a competitive market

03

Remin eligible for DoD contracts

04

Improve overall supply chain security

05

Build stickier, longer-term relationships with DOD resources

PART 04

WHAT We All HAVE TO DO

Start with the uncomfortable part: you are inside the assessment, not next to it.



PART 04 — DELIVERY

APPOINT AN OWNER, THEN STANDARDIZE

STEP 01

Name a team member who owns the CMMC initiative, so everyone underneath them understands how the service is architected and why.

STEP 02
THE QUESTIONS THEY ANSWER

Cloud services handling CUI

Are the systems that process, store or transmit CUI FedRAMP Moderate or equivalent?

Responsibility split

Which controls belong wholly to the customer and which do you own outright?

Personnel screening

Background checks, training and authorization for every privileged technician.

STEP 03

Set one standard. The same configurations, the same tools, the same recurring processes…what holds across the board is what makes compliance repeatable.

APPROXIMATELY 80%

Delivered by the MSP

~20%

OSC retains

MSP DELIVERS

- Identity and directory
- Remote access
- Device management
- Multi-factor auth
- Application allowlisting
- Ticketing and logging
- Log collection
- Change management
- Endpoint protection
- Backup and recovery
- Network infrastructure
- Data loss prevention
- Voice communications
- Encryption at rest
- Physical access control
- Baseline configuration

OSC OWNS

- Policy distribution
- Policy adherence
- Risk assessment
- Personnel screening
- Physical security
- Training

SCAN

Get the customer responsibility matrix

PART 04

THE RESPONSIBILITY MATRIX

One row per requirement. One owner per row. This is the one document that protects both parties when the answer is “not us.”

CUSTOMER

Policy, training, personnel screening, physical security, incident decisions.

PROVIDER

Configuration, patching, logging, identity enforcement, backup integrity.

SHARED

Access approvals, incident response, media handling, change control. Name who does what, in what order.

INHERITED

Controls carried from an underlying cloud platform. Document the source and the limits of what carries.

PART 04 — PACKAGING

HOW IT PACKAGEs Managed IT services with CMMC

CMMC IS NOT AN MSP ADD ON

Different package tiers may depend on the level of inheritance/involvement of your service.

PRICE THE PROACTIVE MANAGEMENT

CMMC compliance will cost more to run than ordinary seats.

PUT THE MATRIX IN THE CONTRACT

Both parties need to agree with theh responsibility matrix. It defines what you owe, and just as importantly what you don't.

CANNOT MANAGED IT AND THE ASSESSMENT

Implementing controls and independently assessing them are different roles. They remain must separate.

CONNECTIONS
Knowledge Trust

QUESTIONS?



Rodd Ahrenstorff

AUGUST 2026