SAN FRANCISCO DISTRICT (SPN)
CYBER SECURITY MATURITY MODEL (CMMC) 2.0

BUSINESS OPPORTUNITIES OPEN HOUSE (BOOH)

Cyber Security Maturity Model (CMMC) 2.0

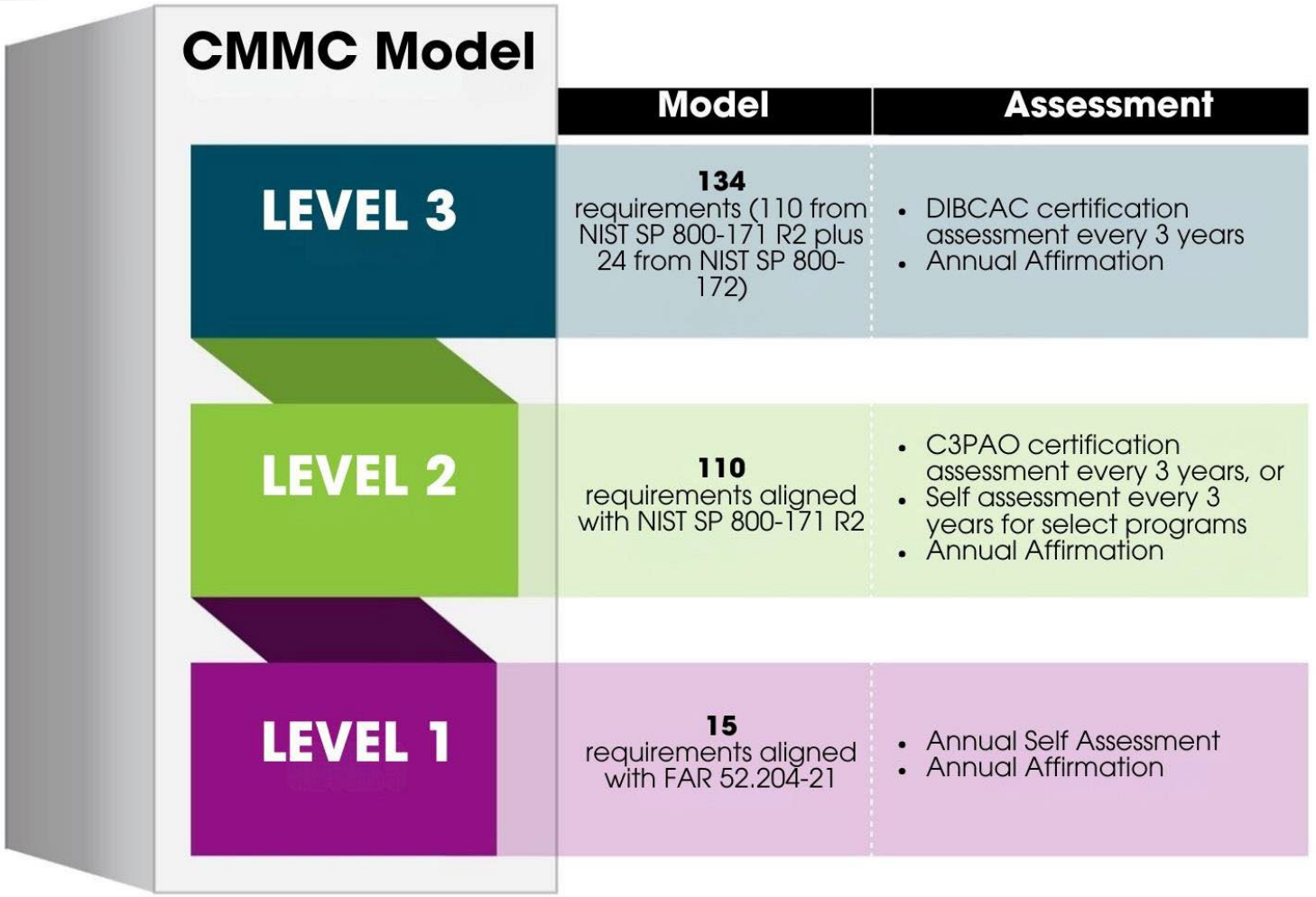
Stephanie Parra
Deputy, Office of Small Business Programs (OSBP)

U.S. ARMY

US Army Corps of Engineers®

U.S. ARMY

CYBER SECURITY MATURITY MODEL (CMMC) 2.0



Controlled Unclassified Information (CUI) / Secret
November 10, 2027

Controlled Unclassified Information (CUI)
November 10, 2025 self *
November 10, 2026 C3PAO

Federal Contract Information (FCI)
November 10, 2025

*Level 2 self certification can be required instead of C3PAO (November 10, 2026 – November 9, 2027) if market research indicates we would have inadequate competition

FCI VERSUS CUI

- **FCI** is information not intended for public release, that is provided by or generated for the Government under a contract.
- Defined in 48 CFR 4.1901
- Minimum safeguarding requirement : 48 CFR 52.204-21
- CMMC Level 1

- **CUI** is information marked or identified as requiring safeguarding in the DoD CUI Program, as defined in 32 CFR Part 2002.
- Minimum safeguarding requirement for DoD: NIST SP 800-171 Revision 2
- CMMC Level 2

LVL 2 CMMC - SELF CERTIFY VS C3PAO

Defense Organizational Index Grouping

- Defense is one Organizational Index Grouping for CUI that will mandate C3PAO certification for level 2 CMMC for certain CUI categories after 10 NOV 2026. However, if market research allows the government may award a CUI procurement base period as level 2 self certification and delay the C3PAO certification until option period 1.
- The cost of a C3PAO assessment for level 2 is estimated to be more than $75K.
- Level 2 self or C3PAO can be given a “Conditional” status, which means the company had a high cybersecurity score, but still has additional fixes needed before obtaining “Finalized” status.
- Conditional status is only valid for 180 days.

U.S. ARMY

CUI EXAMPLES REQUIRING CMMC L2

- Controlled Technical Information (CTI):
  - Engineering Drawings - Detailed plans for military facilities, including buildings, runways, and critical infrastructure.
  - Specifications - Documents outlining the specific materials, methods, and standards for a construction project on a federal site.
  - Technical Manuals - Instructions and guides related to the construction and maintenance of sensitive facilities.

- Physical Security & Critical Infrastructure Information:
  - Security System Layouts - Maps and diagrams detailing the placement of cameras, alarms, and other security devices.
  - Building Plans Revealing Sensitive Areas - Blueprints that show the design and construction of secure facilities like Sensitive Compartmented Information Facilities (SCIFs).
  - Vulnerability Assessments - Reports that identify potential weaknesses in the physical security of a facility.

- Project & Operational Security (OPSEC) Information:
  - Project Names and Details for Sensitive Sites - The name of a project supplying materials to. Example: a large order of a specific material for a known military project could reveal sensitive details about the project.
  - Geospatial Data (GIS) - Maps and topographical information of federal sites and military bases.
  - Construction Schedules - Timelines for construction on a military base revealing operational plans.