NAVAL UNDERSEA WARFARE CENTER
KEYPORT DIVISION

Cybersecurity Maturity Model Certification (CMMC)

Presented to:

CMMC – PNW 2026

Presented by:

Paul Stiglich and Monique Klose

Distribution Statement A: Cleared for Public Release

Cybersecurity Maturity Model Certification (CMMC)

DFARS **final rule** effective 10 Nov 2025: include CMMC requirements in contracts that require the handling of Controlled Unclassified Information (CUI) or Federal Contract Information (FCI). This update will sunset Class Deviation 2025-O0006 on the same date.

The first phase of CMMC implementation began on **November 10, 2025 and CMMC implementation is paused in Phase 1**. This action does not eliminate the requirement for companies to protect information in accordance with DFARS clause 252.204-7012.

Previously, CUI protections covered under DFARS clauses 252.204-7012, 252.204-7019, and 252.204-7020. FCI covered under FAR clause 52.204-21

CMMC builds upon those requirements with two DFARS clauses:

DFARS 252.204-7025, which will be included in solicitations as a notice provision, and an updated **DFARS 252.204-7021**, which contains the CMMC requirements that will be included in contracts.

On July 13, 2026 the DoW suspended the implementation of Phase II of the CMMC and established a CMMC reform task force. During this period the DoW will enforce cybersecurity compliance with NIST 800-171 Rev 2 through self-assessments and select government-led assessments.

https://dodcio.defense.gov/CMMC/about/

Cybersecurity Maturity Model Certification (CMMC)

Level 1: Basic Safeguarding of FCI

Requirements: Annual self-assessment and annual affirmation of compliance with the 15 security requirements in FAR clause 52.204-21.

Level 2: Broad Protection of CUI

Requirements: A self-assessment every three years, with annual affirmation of compliance with the 110 security requirements in NIST SP 800-171 Revision 2.

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 32 CFR § 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

CMMC Requirements Identification

- New Contracts/Orders:
  - Technical Department provide the required CMMC level for new requirements.
  - If a CMMC level is not identified, but the nature of the requirement suggests potential CMMC applicability (e.g., involves FCI or CUI), the Contracting Officer may request that the requiring office assess and provide the appropriate CMMC level, or confirm that the requirement is exempt from CMMC inclusion.
  - If a higher CMMC level is identified than what is permitted per the phased implementation, the higher CMMC level may be required at option exercise instead of award.

CMMC Requirements Identification

- Existing Contracts/Orders:
  - DoD does not currently plan to issue implementation direction applying CMMC requirements retroactively to existing contracts or active solicitations under FAR 1.108(d). The CMMC program is being implemented prospectively, in alignment with the DFARS rule (2019-D041) and the phase-in timelines outlined in 32 CFR §170.3.
  - FAR 1.108(d) permits new regulations to be applied to existing contracts when appropriate. Any decision to modify an existing contract to include CMMC requirements would be at the discretion of the requiring activity or program office, based on mission-specific needs.
  - HOWEVER, Phase 4 (10 Nov 2028) requires that CMMC requirements be included in option periods for contracts awarded prior to 10 Nov 2028.

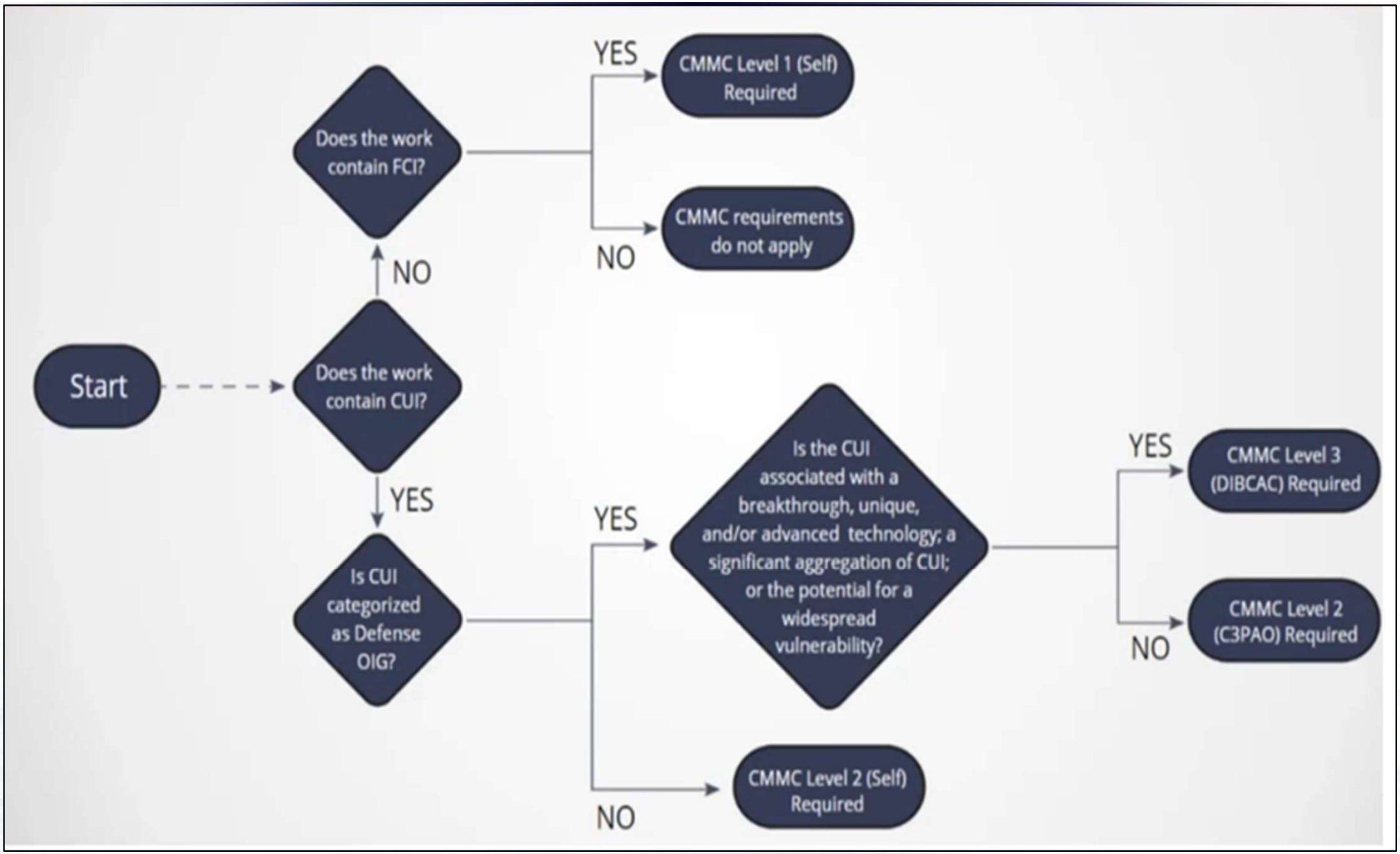
New Provision/Clause

- One new clause and one new provision that must be included when CMMC is applicable:
  - Provision: DFARS 252.204-7025 Notice of Cybersecurity Model Certification Level Requirements
    - Fill-ins required to identify required CMMC level
    - Requires the Offeror to provide, in the proposal, the CMMC unique identifier(s) (CMMC UIDs) issued by SPRS for each contractor information system that will process, store, or transmit FCI or CUI during performance of a contract, task order, or delivery order resulting from this solicitation.
  - Clause: DFARS 252.204-7021 Contractor compliance with the Cybersecurity Maturity Model Certification Level Requirements
    - Fill-ins required to identify required CMMC level
    - Requires the Contractor to submit to the Contracting Officer the CMMC UID(s) issued by SPRS for contractor information systems that will process, store, or transmit FCI or CUI during the performance of the contract and any changes in those UIDs during the life of the contract.

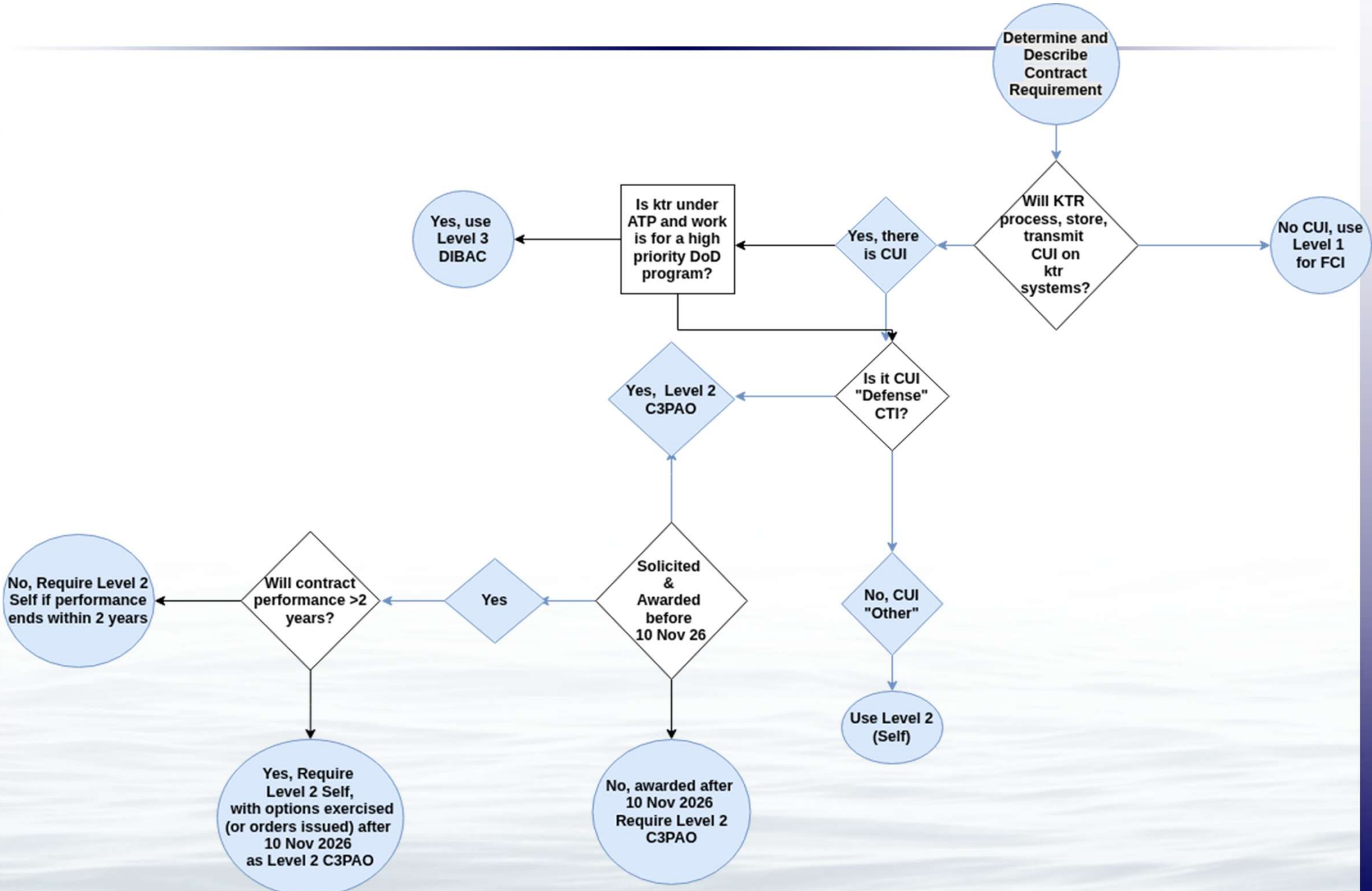
Validating the CMMC Certification

- Contract Specialists/Contracting Officers must validate that the required CMMC level is met prior to contract award, each option exercise, and period of performance extensions.
  - Address with other compliances (responsibility determination).
- Validation is performed in SPRS

CMMC Level Decision Tree



CMMC Level Decision Tree

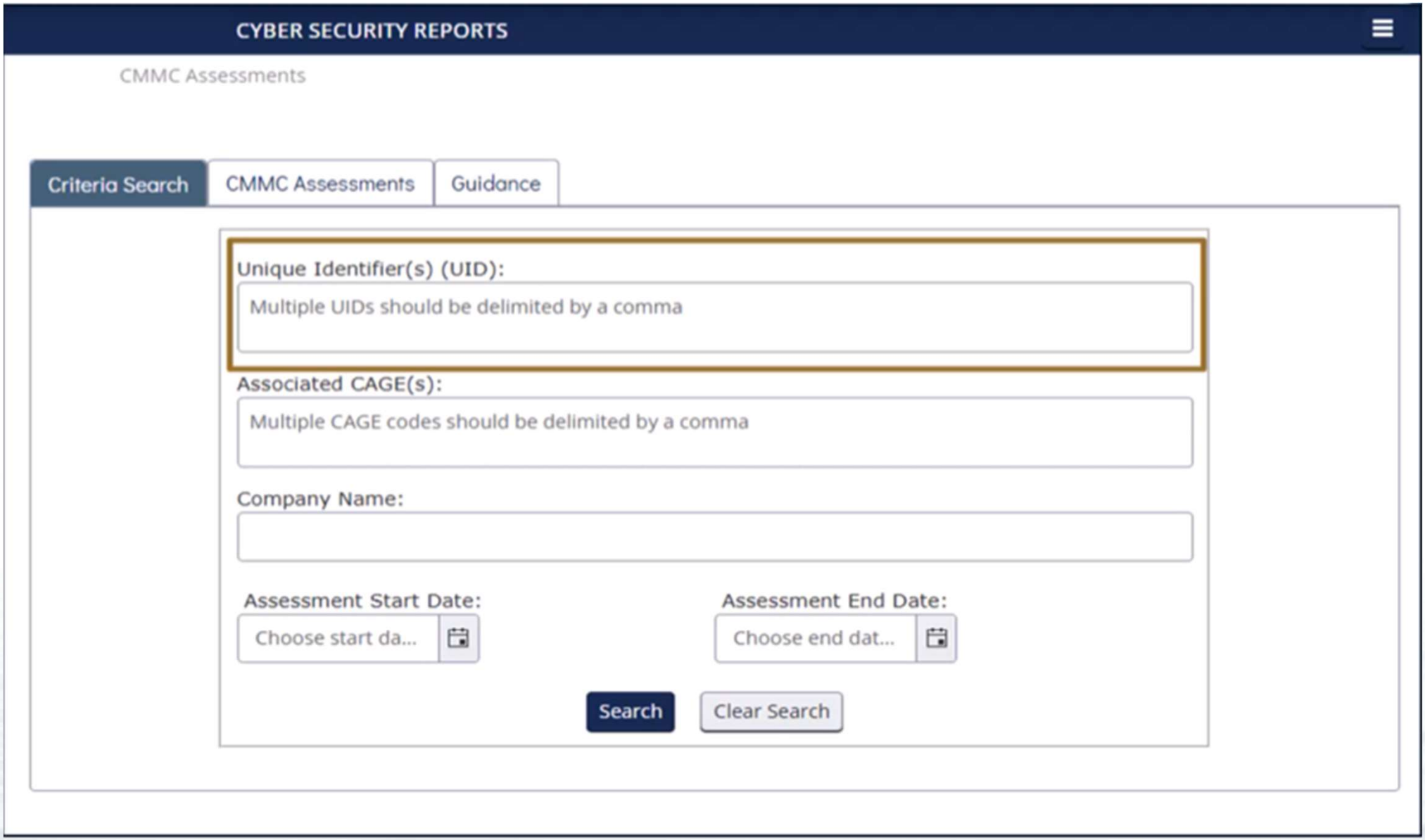


Cybersecurity Maturity Model Certification (CMMC)

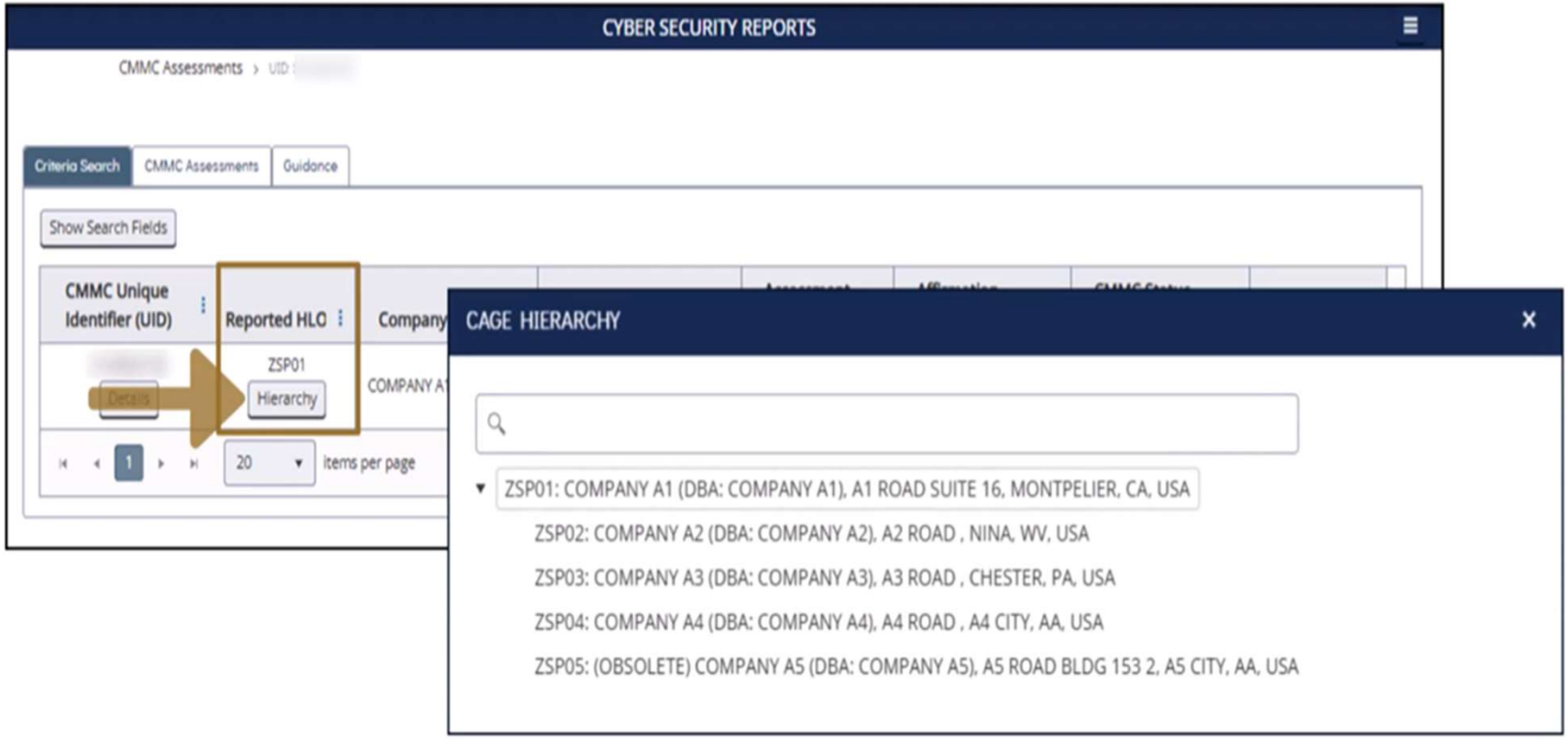
Cybersecurity Maturity Model Certification (CMMC)

Click CMMC Assessments from the left-hand menu to access the Criteria Search tab for CMMC Assessments.

Cybersecurity Maturity Model Certification (CMMC)

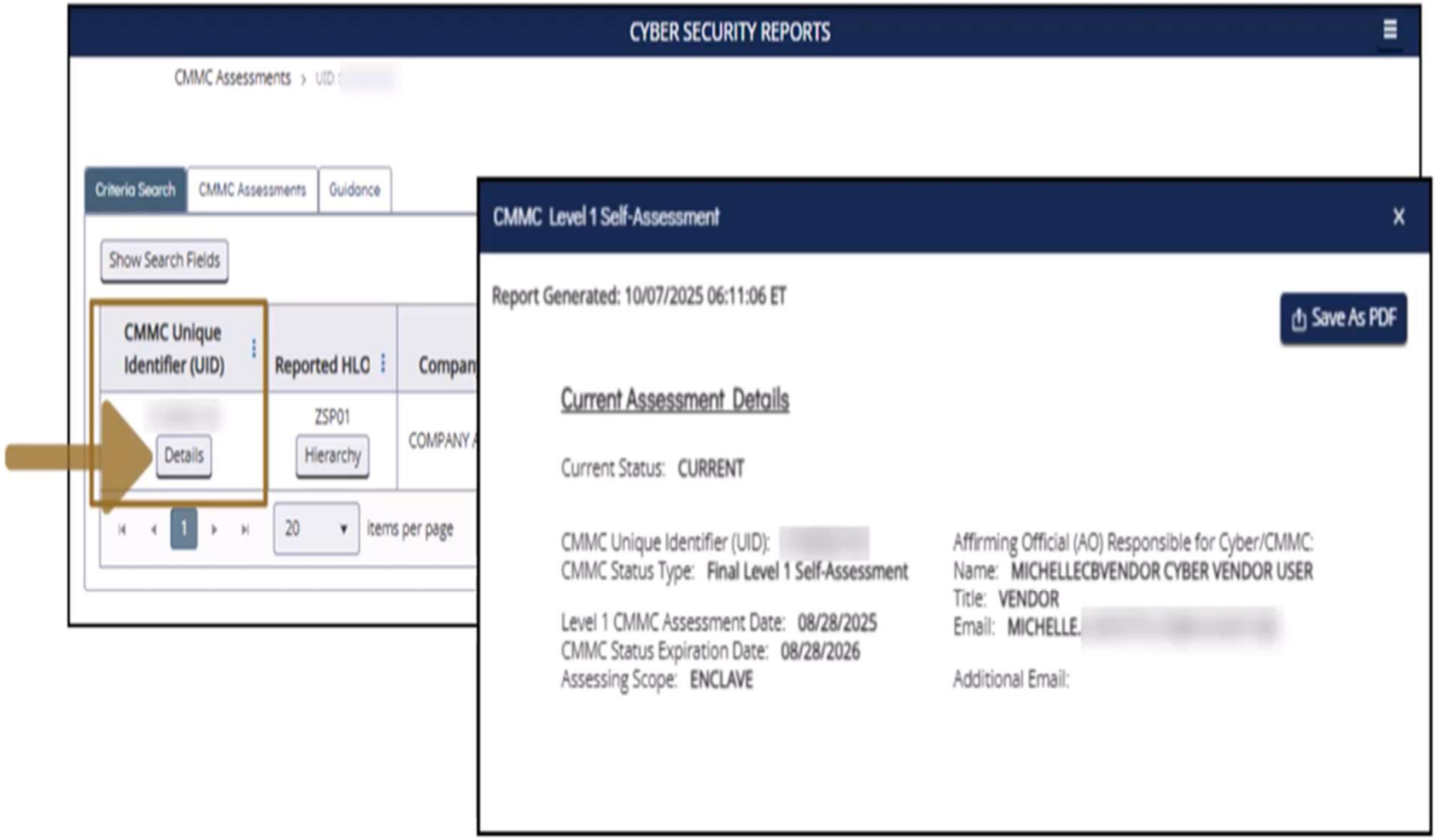


Cybersecurity Maturity Model Certification (CMMC)

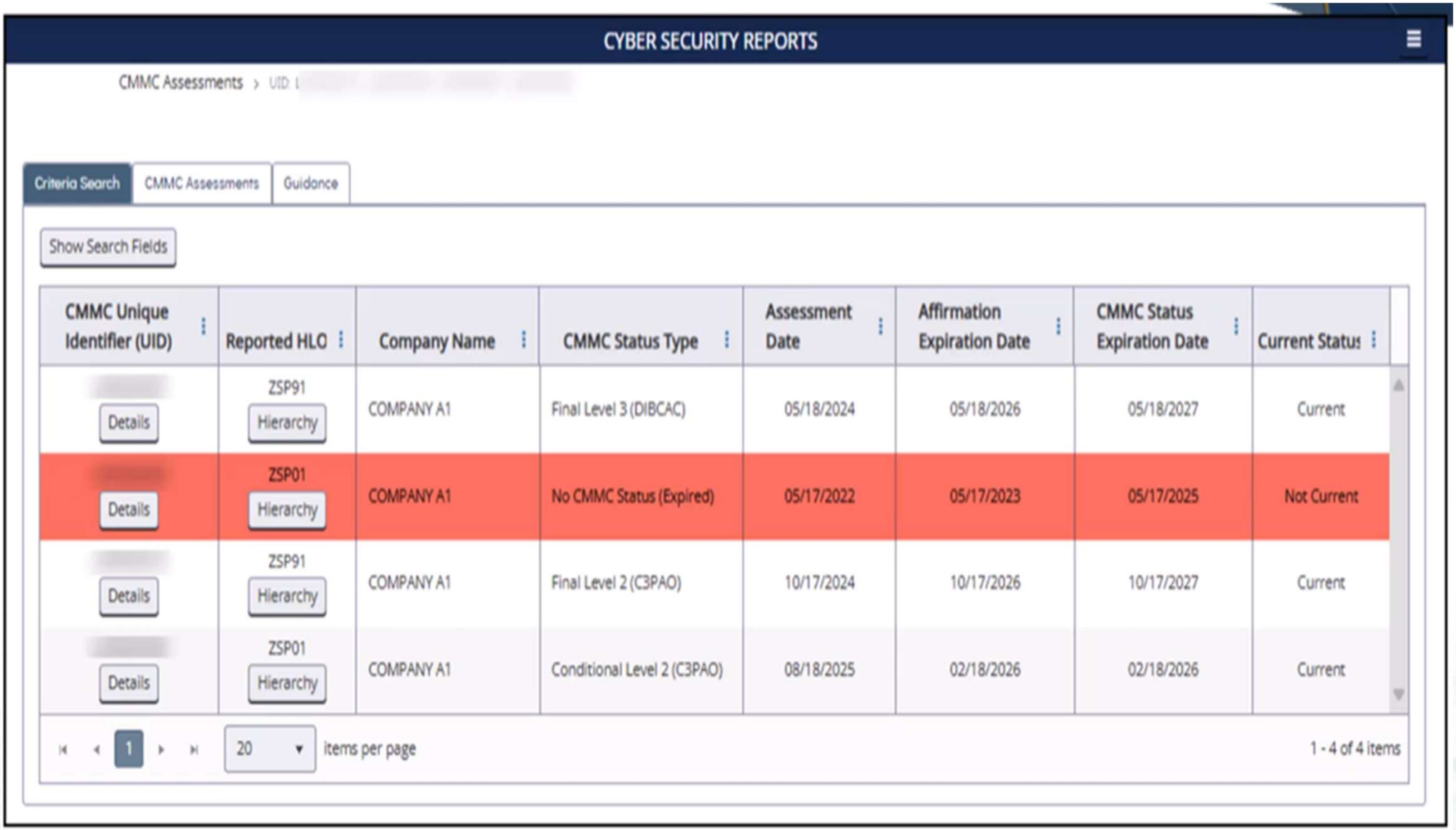


To find a specific CAGE within the Hierarchy select the Hierarchy button in the Reported HLO column.

Cybersecurity Maturity Model Certification (CMMC)



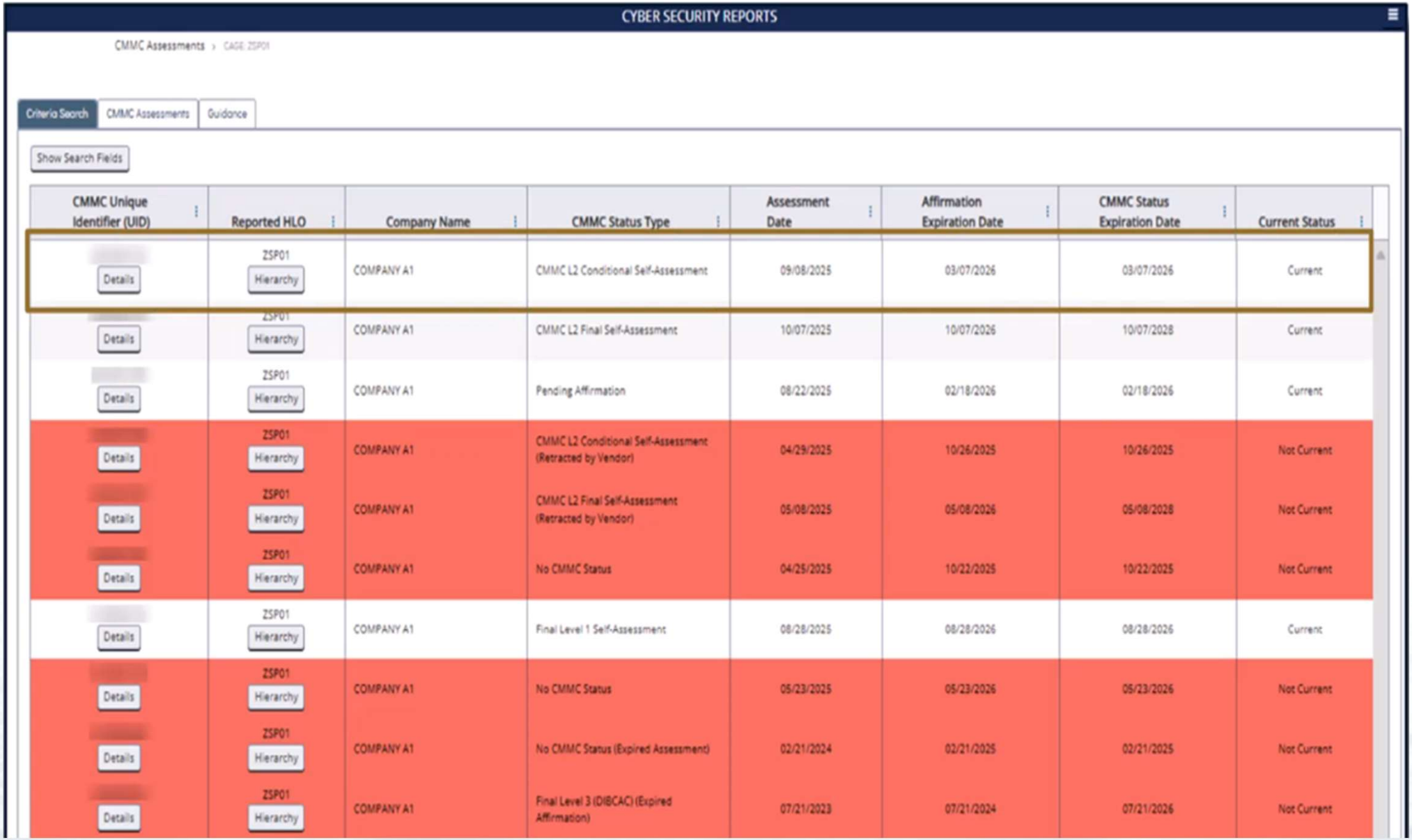
Cybersecurity Maturity Model Certification (CMMC)



CMMC Unique Identifier (UID)	Reported HLO	Company Name	CMMC Status Type	Assessment Date	Affirmation Expiration Date	CMMC Status Expiration Date	Current Status
Details	ZSP91 Hierarchy	COMPANY A1	Final Level 3 (DIBCAC)	05/18/2024	05/18/2026	05/18/2027	Current
Details	ZSP01 Hierarchy	COMPANY A1	No CMMC Status (Expired)	05/17/2022	05/17/2023	05/17/2025	Not Current
Details	ZSP91 Hierarchy	COMPANY A1	Final Level 2 (C3PAO)	10/17/2024	10/17/2026	10/17/2027	Current
Details	ZSP01 Hierarchy	COMPANY A1	Conditional Level 2 (C3PAO)	08/18/2025	02/18/2026	02/18/2026	Current

1 | 20 items per page | 1 - 4 of 4 items

Cybersecurity Maturity Model Certification (CMMC)



CYBER SECURITY REPORTS

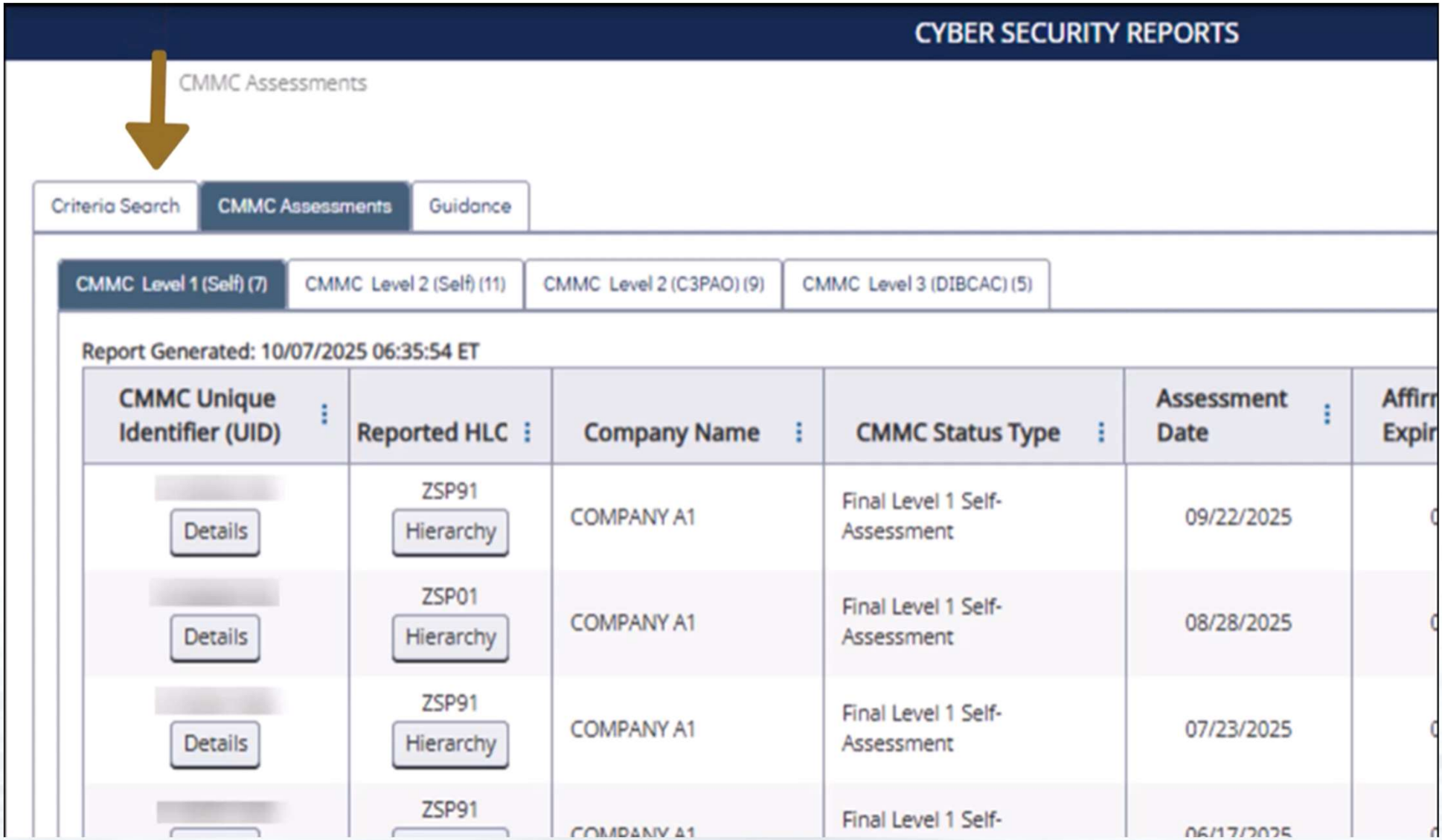
CMMC Assessments › CAGE: ZSP01

Criteria Search | CMMC Assessments | Guidance

Show Search Fields

CMMC Unique Identifier (UID)	Reported HLO	Company Name	CMMC Status Type	Assessment Date	Affirmation Expiration Date	CMMC Status Expiration Date	Current Status
Details	ZSP01 Hierarchy	COMPANY A1	CMMC L2 Conditional Self-Assessment	09/08/2025	03/07/2026	03/07/2026	Current
Details	ZSP01 Hierarchy	COMPANY A1	CMMC L2 Final Self-Assessment	10/07/2025	10/07/2026	10/07/2028	Current
Details	ZSP01 Hierarchy	COMPANY A1	Pending Affirmation	08/22/2025	02/18/2026	02/18/2026	Current
Details	ZSP01 Hierarchy	COMPANY A1	CMMC L2 Conditional Self-Assessment (Retracted by Vendor)	04/29/2025	10/26/2025	10/26/2025	Not Current
Details	ZSP01 Hierarchy	COMPANY A1	CMMC L2 Final Self-Assessment (Retracted by Vendor)	05/08/2025	05/08/2026	05/08/2028	Not Current
Details	ZSP01 Hierarchy	COMPANY A1	No CMMC Status	04/25/2025	10/22/2025	10/22/2025	Not Current
Details	ZSP01 Hierarchy	COMPANY A1	Final Level 1 Self-Assessment	08/28/2025	08/28/2026	08/28/2026	Current
Details	ZSP01 Hierarchy	COMPANY A1	No CMMC Status	05/23/2025	05/23/2026	05/23/2026	Not Current
Details	ZSP01 Hierarchy	COMPANY A1	No CMMC Status (Expired Assessment)	02/21/2024	02/21/2025	02/21/2025	Not Current
Details	ZSP01 Hierarchy	COMPANY A1	Final Level 3 (DIBCAC) (Expired Affirmation)	07/21/2023	07/21/2024	07/21/2026	Not Current

Cybersecurity Maturity Model Certification (CMMC)



Responsibilities

Role	Activities/Responsibilities
Program Office/Requiring Activity	• Determine and justify required CMMC level for solicitations • Prepare request for waiver package (as applicable) • Coordinate with Contracting/Agreements Officers to ensure requirements are applied • Include CMMC compliance in surveillance activities • Ensure CUI and FCI are properly identified and marked IAW DODI 5200.48
Contracting/Agreements Officer	• Insert required CMMC level in solicitations and contracts/agreements • Verify Contractor's CMMC status in SPRS and document the contract file before award, option exercise, or extension • Ensure Contractor maintains compliance throughout the life of the contract • Ensure all applicable clause(s) and provision(s) are in the solicitation
DoD Service Acquisition Executive or Component Acquisition Executive (or as delegated)	• In very limited circumstances, may elect to waive inclusion of CMMC program requirements in solicitation or contract • In such cases, Contractors and Sub-contractors remain obligated to comply with all applicable cybersecurity and information security requirements
Contractors	• Identify the Contractor Information Systems requiring compliance including Sub-Contractor/Vendor systems • Implement and maintain required cybersecurity practices, assessments, and certifications as required per assigned CMMC level • Submit assessments, affirmations and CMMC Unique identifiers (UIDs) in SPRS or eMASS • Flow down applicable CMMC requirements to Sub-Contractors handling FCI/CUI and verify Sub-Contractor CMMC level prior to award or performance start as appropriate • Report cyber incidents as required by DFARS 252.204-7012 or NMCARS Annex 16 language (if included)

Frequently Asked Questions

- **Are CMMC assessments required for organizations that only handle hard-copy CUI?**
  - No. Organizations that ONLY handle hard-copy CUI should not be required to complete a CMMC Assessment. CMMC assessment requirements address cybersecurity-related risk to CUI and apply only when the CUI is processed, stored or transmitted to a Contractor-owned information technology system.
- **Will CMMC apply to non-U.S. companies?**
  - Yes. When CMMC requirements are identified in DoW solicitations, they will apply to all companies performing under the resulting contract, whether domestic or international.

Frequently Asked Questions

- **What are the repercussions for the contractor NOT complying with or failing to obtain or maintain the required CMMC level during contract execution?**
  - Non-compliance or failing to obtain and maintain full compliance risk inability to award options in the contract or extend services, award of new orders under an IDIQ or BOA, termination, or suspension (stop work) under contract remedies.
  - Additionally, this would be documented in the CPARS record as a negative performance observation and possibly the assignment of a Marginal or Unsat under “Regulatory Compliance” which would hinder the ability to successfully compete for future opportunities.
  - Vendors may also find that failure to obtain and maintain certification may be viewed as a risk by a Prime Contractor when making Sub-contractor teaming decisions.