CMMC Level 1 Self-Attestation Checklist

Overview

This checklist walks your organization through **CMMC Level 2 self-attestation**, including required registrations, role setup, documentation, and submission to the DoD.

Company Registration & System Access

Register in SAM.gov

Purpose: Required to do business with the U.S. Government.

Actions:

- Register or verify your entity at **SAM.gov**
- Obtain a valid **CAGE Code**
- Confirm registration is **Active**

PIEE Registration & Role Assignment

Register in PIEE (Procurement Integrated Enterprise Environment)

Purpose: Provides access to systems required for CMMC compliance and SPRS submission.

Actions:

- Add Your CAGE Code to the PIEE Vendor Group Structure by Contacting the PIEE Help Desk by phone or email: 1-866-618-5988
- A company representative must request your CAGE Code to be added to a Vendor Group in the Procurement Integrated Enterprise Environment (PIEE).
- Provide your CAGE Code and desired Group Name. If you don't specify a Group Name, one will be assigned based on your CAGE Code or company name.
- Go to PIEE and click **Register**
- Select organization type:

- **Vendor** OR
- **Contractor** (either is acceptable)

Assign Contractor Administrator Manager (CAM) *(Done During Registration)*

Important:
The **CAM is designated during the PIEE registration process**

Requirements:

- Designate **one primary individual**
- This person should:
  - Be responsible for IT or cybersecurity
  - Serve as the main compliance point of contact

Responsibilities:

- Manage PIEE account and user roles
- Oversee SPRS submissions
- Maintain compliance documentation

Complete PIEE Registration

- Finish all required fields and organization setup
- Confirm account activation

Additional Role Configuration *(Done After Registration)*

Assign Cyber Vendor User Role

Purpose: Enables access to SPRS and cybersecurity modules.

Actions:

- Assign **Cyber Vendor User role** within PIEE
- Recommended: assign to the **same person as CAM**

Verify SPRS Access

Purpose: SPRS is where CMMC self-assessment scores are submitted.

Actions:

- Log into PIEE dashboard
- Confirm **SPRS (Supplier Performance Risk System)** appears
- If not:
    - Log out and back in
    - Verify correct role assignment

CMMC Level 1 – Security Self-Assessment

Complete DoD Self-Assessment

Purpose: Evaluate compliance with required security controls.

Actions:

- Use: **DoD Self-Assessment & SPRS Scoring Methodology (latest version available at CMMC | Intellicomm Group Inc)**
- Answer all applicable controls
- Calculate your **SPRS Score**

Note:
Level 1 focuses on **basic safeguarding of Federal Contract Information (FCI)**.

Required Security Documentation

Create System Security Plan (SSP)

Purpose: Documents your security controls and system environment.

Include:

- System scope and boundaries
- Hardware/software inventory
- Security controls in place
- Data handling processes (FCI)
- Access control methods

Create Incident Response Plan (IRP)

Purpose: Defines how your organization handles cybersecurity incidents.

Include:

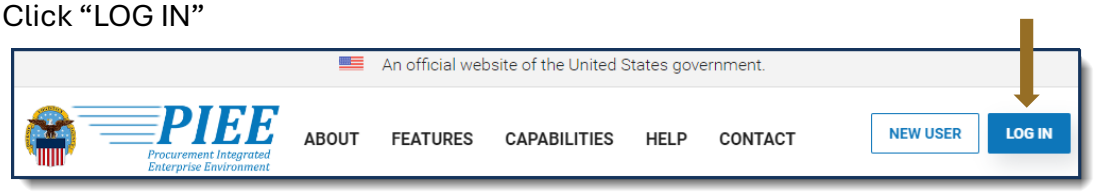
- Incident definitions
- Roles and responsibilities
- Response procedures
- Reporting requirements
- Key contacts

SPRS Submission & Attestation[1]

1. **PIEE Access:** A "SPRS Cyber Vendor User" role is required to enter CMMC Assessment information. PIEE Access Instructions: https://www.sprs.csd.disa.mil/access.htm

2. SPRS Application and Module Access:
   a. PIEE landing page: https://piee.eb.mil

   b. Click "LOG IN"



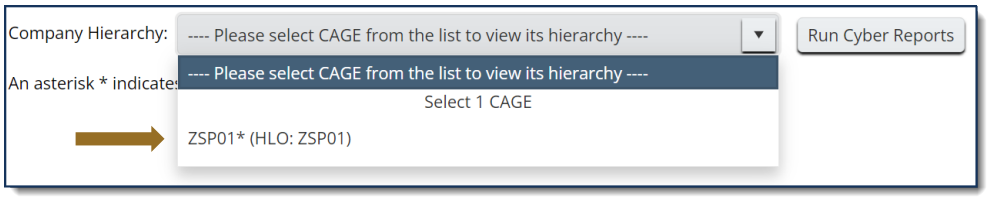
Screenshot Dtd 09 JAN 2024

   c. Select **SPRS**:

   d. Select **Cyber Reports**:

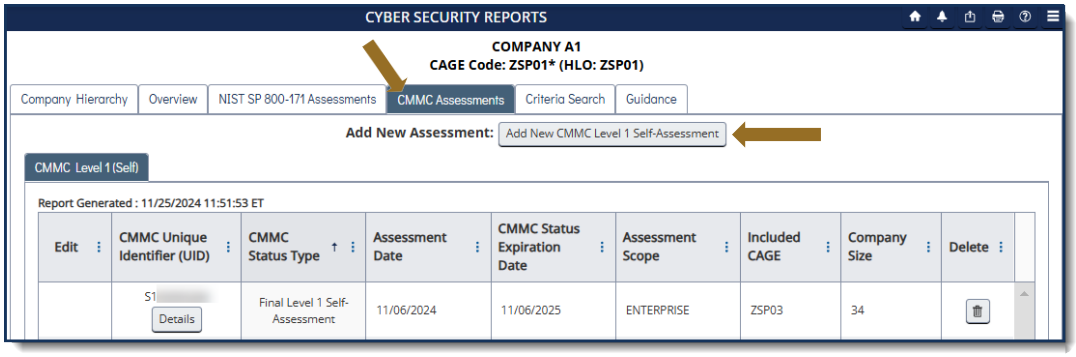
[1] CMMC LEVEL 1 SELF-ASSESSMENT QUICK ENTRY GUIDE VERSION 4.0

3. **Cyber Reports Module:** Select the desired Hierarchy, identified by the HLO, from the drop down.



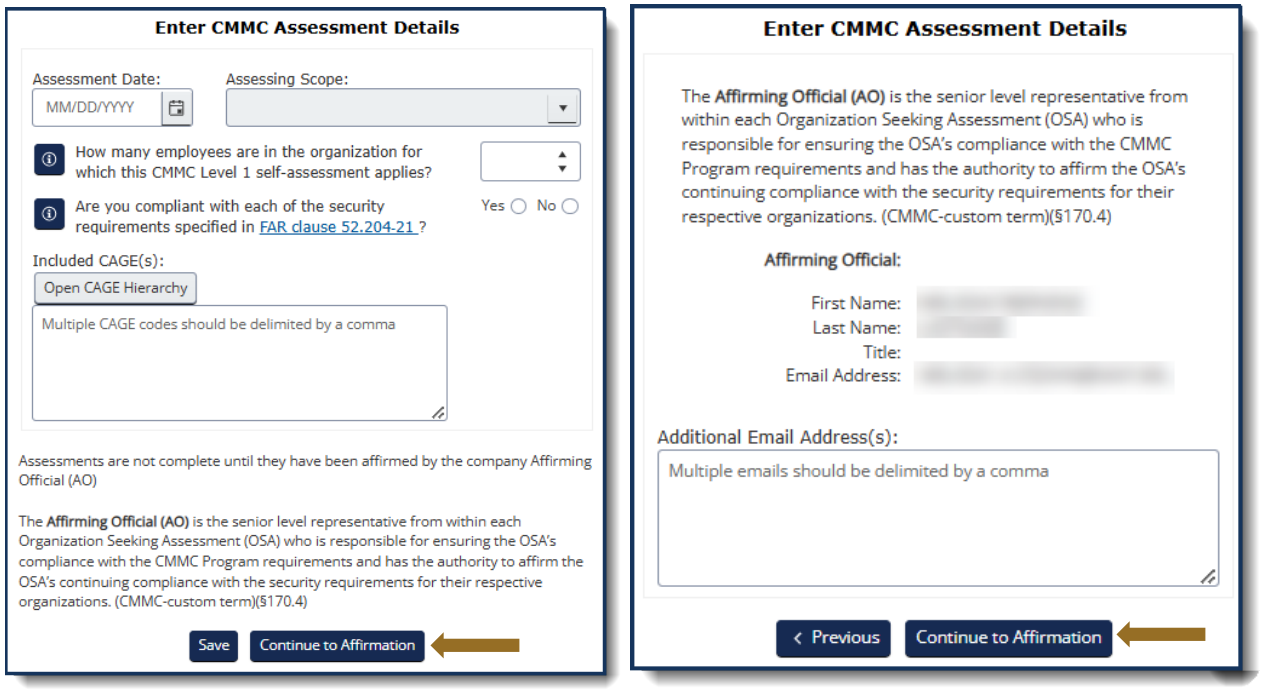
NOTE: An asterisk * indicates the user has the SPRS Cyber Vendor User role (access to add/edit/delete)

3.1 Add New Assessment: Within the CMMC Assessments tab, select "Add New Level 1 CMMC Self-Assessment".



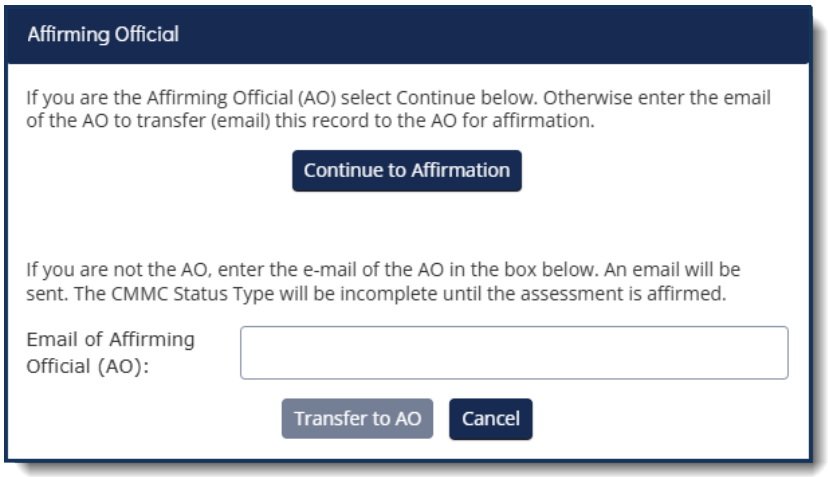
3.2 Enter Assessment Details: Enter assessment data and select "Continue to Affirmation".

NOTE: Compliance with the security requirements specified in FAR clause 52.204–21 is required to achieve a "Final Level 1 Self-Assessment".

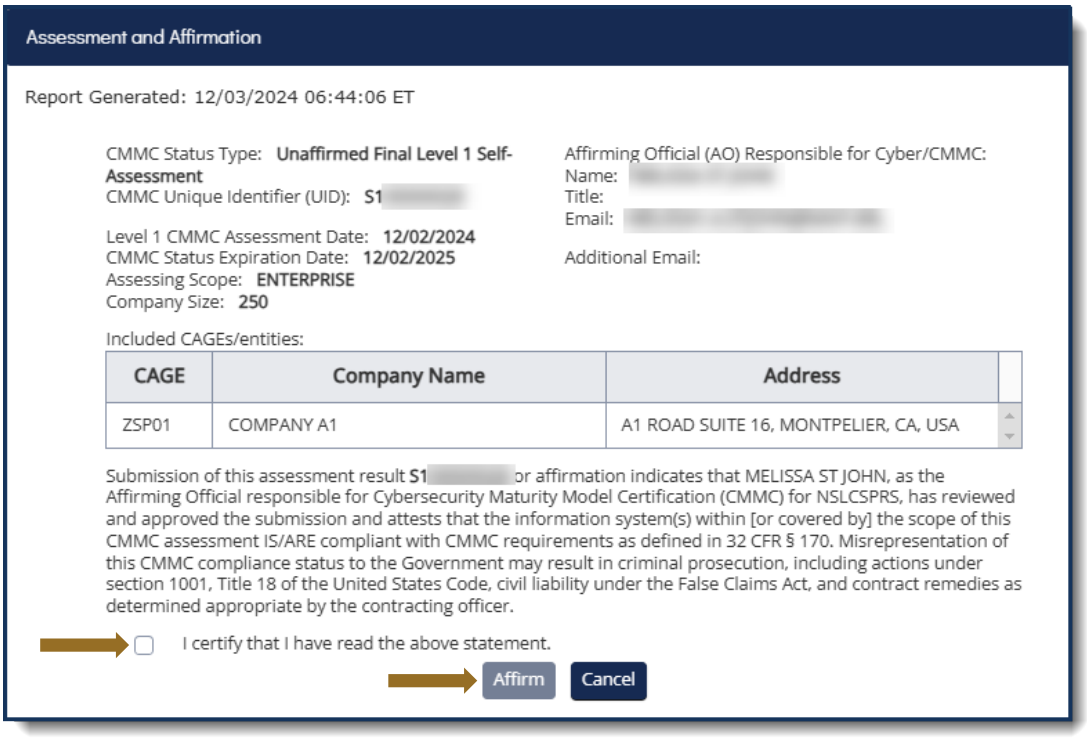


NOTE: CAGE Hierarchy is imported from the System for Award Management (SAM)

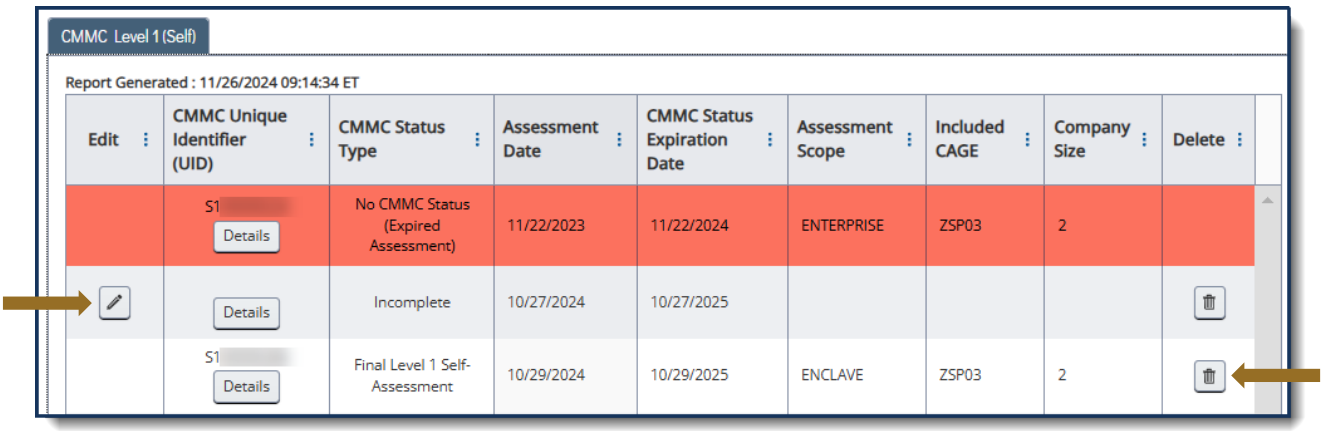
3.3 Transfer to Affirming Official (AO): If the user entering the assessment is not the AO, the assessment can be forwarded via email, to the AO by entering their email and selecting "Transfer to AO".



3.4 Affirm the Assessment: Review the assessment details, certify review of the affirmation statement, and select "Affirm".



3.5 Assessment Edit/Delete: A Cyber Vendor User may edit or delete certain CMMC Status Types.



NOTE: A "Final Level 1 Self-Assessment" will automatically become "No CMMC Status (Expired Assessment)" after 1 year.

NOTE: "Final Level 1 Self-Assessment" is the only CMMC Status Type that will be visible to Government Personnel.

Ongoing Compliance

Maintain Documentation

- Keep SSP, IRP, and assessment records updated
- Store documentation securely

Annual Review

- Review controls at least once per year
- Update documents as needed
- Reassess if systems or contracts change