

CMMC Level 2 Self-Attestation

Overview

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

This checklist can be used if you have not previously attested to Level 1. If you have attested for Level 1 – Please skip to [CMMC Level 2 – Security Self-Assessment](#)

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 & Attestation¹

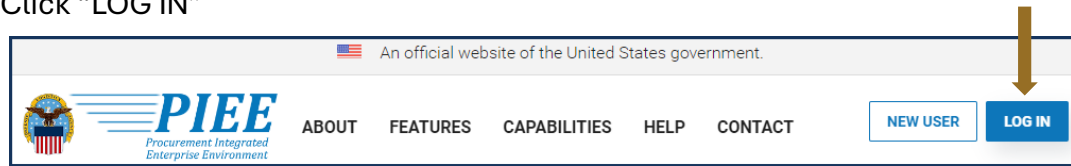
1. **PIEE Access:** A “SPRS Cyber Vendor User” role is required to enter CMMC Assessment information. PIEE Access Instructions:

<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

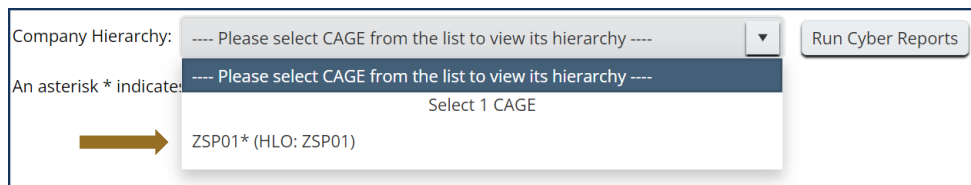
- c. Select **SPRS**:



- d. Select **Cyber Reports**:



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

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

(access to add/edit/delete)

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

The screenshot displays the 'CYBER SECURITY REPORTS' interface. At the top, there's a header bar with navigation icons. Below it, the 'COMPANY A1' section shows 'CAGE Code: ZSP01* (HLO: ZSP01)'. A navigation bar contains tabs: 'Company Hierarchy', 'Overview', 'NIST SP 800-171 Assessments', 'CMMC Assessments' (selected), 'Criteria Search', and 'Guidance'. An arrow points to the 'CMMC Assessments' tab. Below the tabs, the 'Add New Assessment:' section is visible, with an arrow pointing to the 'Add New CMMC Level 1 Self-Assessment' button. The 'CMMC Level 1 (Self)' section is expanded, showing a table of assessments. The table has columns: 'Edit', 'CMMC Unique Identifier (UID)', 'CMMC Status Type', 'Assessment Date', 'CMMC Status Expiration Date', 'Assessment Scope', 'Included CAGE', 'Company Size', and 'Delete'. A single row is visible with the following data: 'S1', 'Final Level 1 Self-Assessment', '11/06/2024', '11/06/2025', 'ENTERPRISE', 'ZSP03', '34'. A 'Details' button is located below the 'S1' UID. The 'Report Generated' timestamp is '11/25/2024 11:51:53 ET'.

Report Generated : 11/25/2024 11:51:53 ET

Edit	CMMC Unique Identifier (UID)	CMMC Status Type	Assessment Date	CMMC Status Expiration Date	Assessment Scope	Included CAGE	Company Size	Delete
	S1 Details	Final Level 1 Self-Assessment	11/06/2024	11/06/2025	ENTERPRISE	ZSP03	34	

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”.

Enter CMMC Assessment Details

Assessment Date: MM/DD/YYYY

Assessing Scope:

① How many employees are in the organization for which this CMMC Level 1 self-assessment applies?

① Are you compliant with each of the security requirements specified in [FAR clause 52.204-21](#)? Yes ☐ No ☐

Included CAGE(s):

Multiple CAGE codes should be delimited by a comma

Assessments are not complete until they have been affirmed by the company Affirming Official (AO)

The **Affirming Official (AO)** 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 security requirements for their respective organizations. (CMMC-custom term)(§170.4)

Enter CMMC Assessment Details

The **Affirming Official (AO)** 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 security requirements for their respective organizations. (CMMC-custom term)(§170.4)

Affirming Official:

First Name:

Last Name:

Title:

Email Address:

Additional Email Address(s):

Multiple emails should be delimited by a comma

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”.

Affirming Official

If you are the Affirming Official (AO) select Continue below. Otherwise enter the email of the AO to transfer (email) this record to the AO for affirmation.

If you are not the AO, enter the e-mail of the AO in the box below. An email will be sent. The CMMC Status Type will be incomplete until the assessment is affirmed.

Email of Affirming Official (AO):

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

Assessment and Affirmation

Report Generated: 12/03/2024 06:44:06 ET

CMMC Status Type: **Unaffirmed Final Level 1 Self-Assessment**
CMMC Unique Identifier (UID): S1
Level 1 CMMC Assessment Date: 12/02/2024
CMMC Status Expiration Date: 12/02/2025
Assessing Scope: **ENTERPRISE**
Company Size: **250**

Affirming Official (AO) Responsible for Cyber/CMMC:
Name:
Title:
Email:
Additional Email:

Included CAGEs/entities:

CAGE	Company Name	Address
ZSP01	COMPANY A1	A1 ROAD SUITE 16, MONTPELIER, CA, USA

Submission of this assessment result S1 or affirmation indicates that MELISSA ST JOHN, as the Affirming Official responsible for Cybersecurity Maturity Model Certification (CMMC) for NSLCSPRS, has reviewed and approved the submission and attests that the information system(s) within [or covered by] the scope of this CMMC assessment IS/ARE compliant with CMMC requirements as defined in 32 CFR § 170. Misrepresentation of this CMMC compliance status to the Government may result in criminal prosecution, including actions under section 1001, Title 18 of the United States Code, civil liability under the False Claims Act, and contract remedies as determined appropriate by the contracting officer.

☐ I certify that I have read the above statement.

Affirm
Cancel

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

CMMC Level 1 (Self)								
Report Generated : 11/26/2024 09:14:34 ET								
Edit	CMMC Unique Identifier (UID)	CMMC Status Type	Assessment Date	CMMC Status Expiration Date	Assessment Scope	Included CAGE	Company Size	Delete
	S1 Details	No CMMC Status (Expired Assessment)	11/22/2023	11/22/2024	ENTERPRISE	ZSP03	2	
	Details	Incomplete	10/27/2024	10/27/2025				
	S1 Details	Final Level 1 Self-Assessment	10/29/2024	10/29/2025	ENCLAVE	ZSP03	2	

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

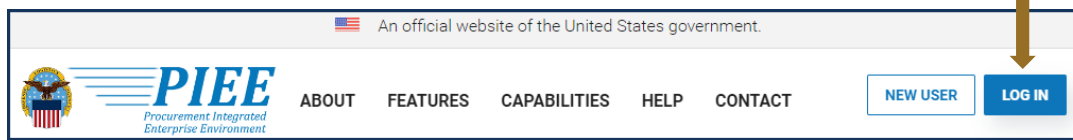
Annual Review

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

CMMC Level 2 – Security Self-Assessment

SPRS Submission & Attestation²

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](https://piee.eb.mil/piee-landing/) landing page: <https://piee.eb.mil/piee-landing/>
 - b. Click “LOG IN”

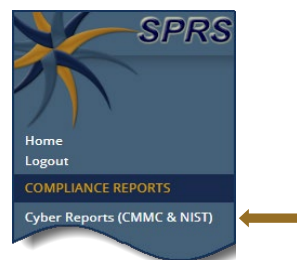


Screenshot Dtd 09 JAN 2024

- c. Select **SPRS**:



- d. Select **Cyber Reports (CMMC & NIST)**:



² CMMC LEVEL 2 SELF-ASSESSMENT QUICK ENTRY GUIDE
VERSION 4.0

3. **Cyber Reports (CMMC & NIST):** Select the desired Hierarchy, identified by the HLO, from the drop down and select Run Cyber Reports button.

Company Hierarchy: ---- Please select CAGE from the list to view its hierarchy ----

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

Run Cyber Reports

Select 1 CAGE

ZSP01* (HLO: ZSP01)

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

- 3.1 **Add New CMMC Level 2 Self-Assessment:** Within the CMMC Assessments and CMMC Level 2 (Self) tabs, select “Add New Level 2 CMMC Self-Assessment”.

CYBER SECURITY REPORTS

COMPANY A1
CAGE Code: * (HLO:)

Company Hierarchy Overview NIST SP 800-171 Assessments CMMC Assessments Criteria Search Guidance

Add New Assessment: Add New CMMC Level 2 Self-Assessment

CMMC Level 1 (Self) CMMC Level 2 (Self)

Report Generated : 02/21/2025 12:56:05 ET

Edit	CMMC Unique Identifier (UID)	CMMC Status Type	Assessment Date	CMMC Status Expiration Date	Assessment Scope	Included CAGE	Company Size	Cancel/ Delete
	S2	Affirm			ENCLAVE		1	
		Pending Affirmation						
	S2	Affirm			ENCLAVE		1	

- 3.2 **Enter Assessment Details:** Enter assessment data; review Requirement Objectives to each Requirement Number by selecting the Requirement Objectives button. Select the applicable Compliance Status. Select Save and Continue to navigate through each Requirement Family.

CYBER SECURITY REPORTS

COMPANY A1
CAGE Code: * (HLO:)
CMMC Status Type: Level 2 Self-Assessment
Assessment Standard: NIST SP 800-171 Rev 2

Back

Enter CMMC Assessment Details

AC AT AU CM IA IR MA MP PS PE RA CA SC SI Review CAGES Score Affirm

Requirement Family: Access Control (AC)

Save Save and Continue >

Requirement Number	Requirement Description	Compliance Status ⓘ		
		Met	Not Met	N/A
AC.L2-3.1.1 Requirement Objectives	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	☐ Met	☐ Not Met	☐ N/A
AC.L2-3.1.2 Requirement Objectives	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	☐ Met	☐ Not Met	☐ N/A
AC.L2-3.1.3 Requirement Objectives	Control the flow of CUI in accordance with approved authorizations.	☐ Met	☐ Not Met	☐ N/A

3.3 Review Assessment Details: Answers to Requirements must be complete prior to continuing.

COMPANY A1
CAGE Code: * (HLO:)
CMMC Status Type: Level 2 Self-Assessment
Assessment Standard: NIST SP 800-171 Rev 2

Back

Enter CMMC Assessment Details

AC AT AU CM IA IR MA MP PS PE RA CA SC SI **Review** CAGEs Score Affirm

< Previous Continue >

All Requirements must be answered before continuing to Affirmation.

Export all Data Fields: Export

Requirement Number	Compliance Status ⓘ		
	Met	Not Met	N/A or Partial
AC.L2-3.1.1	✓		
AC.L2-3.1.2			
AC.L2-3.1.3		✓	
AC.L2-3.1.4			N/A

3.4 Additional Assessment Details: Add Assessing Scope, Employee Count, and Included CAGE(s) as required. Select the “Open CAGE Hierarchy” button to add CAGEs or enter comma delimited CAGEs in the data field provided. Select “Save and Continue.”

CYBER SECURITY REPORTS

COMPANY A1
CAGE Code: * (HLO:)
CMMC Status Type: Level 2 Self-Assessment
Assessment Standard: NIST SP 800-171 Rev 2

Back

Enter CMMC Assessment Details

AC AT AU CM IA IR MA MP PS PE RA CA SC SI Review CAGEs Score Affirm

Assessing Scope:
ENCLAVE

How many employees are in the organization for which this CMMC Level 2 self-assessment applies? 42

Included CAGE(s):
Open CAGE Hierarchy

Multiple CAGE codes should be delimited by a comma

< Previous Save and Continue >

NOTE: CAGE Hierarchy data is imported from the System for Award Management (SAM). Users are unable to add CAGEs that are not part of their company hierarchy.

3.5 Score: Only CMMC L2 Conditional (score = 88 to 109) and Final Self-Assessments (score = 110) can be affirmed.

The screenshot displays the 'CYBER SECURITY REPORTS' interface. At the top, it identifies 'COMPANY A1' with a 'CAGE Code' and 'HLO'. The 'CMMC Status Type' is 'Level 2 Self-Assessment' and the 'Assessment Standard' is 'NIST SP 800-171 Rev 2'. A 'Back' button is visible. Below, a progress bar shows various assessment categories (AC, AT, AU, CM, IA, IR, MA, MP, PS, PE, RA, CA, SC, SI, Review, CAGEs, Score, Affirm) with 'Review' currently selected. The 'Final Score: 107' is prominently displayed. The 'CMMC Status Type' is 'Unaffirmed CMMC L2 Conditional Self-Assessment'. A message states: 'Your responses meet the requirements for a CMMC Level 2 Conditional Self-Assessment. Once affirmed, the assessment will be valid for 180 days.' A link for inquiries is provided: 'osd.pentagon.dod-cio.mbx.cmmc-inquiries@mail.mil'. At the bottom, there are buttons for '< Previous' and 'Continue To Affirmation >', with a yellow arrow pointing to the latter.

NOTE: If a requirement is not able to be subject to a Plan of Action and Milestones (POA&M), then the Status Type will be No CMMC Status regardless of score.

3.6 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".

The 'Affirming Official' dialog box provides instructions for users. It asks if the user is the Affirming Official (AO). If yes, they should select 'Continue to Affirmation', which is highlighted with a yellow arrow. If not, they should enter the AO's email in the provided box. An email will be sent, and the CMMC Status Type will be 'incomplete' until affirmed. Below the email input box, there are buttons for 'Transfer to AO' (highlighted with a yellow arrow) and 'Cancel'.

3.7 Affirm the Assessment: Review the assessment details, certify review of the affirmation statement, and select “Affirm”.

Assessment and Affirmation

Report Generated: 02/21/2025 13:09:57 ET

Assessment Standard: NIST SP 800-171 Rev 2
Assessment Type: CMMC Level 2 Self-Assessment

CMMC Status Type: Unaffirmed CMMC L2 Conditional Self-Assessment
CMMC Unique Identifier (UID): S2

Score: 91
Assessing Scope: ENCLAVE
Company Size: 42

Submission of this assessment result S2 or affirmation indicates that , as the Affirming Official responsible for Cybersecurity Maturity Model Certification (CMMC) for NSLCSPRS, has reviewed and approved the submission and attests that the information system(s) within [or covered by] the scope of this CMMC assessment IS/ARE compliant with CMMC requirements as defined in 32 CFR § 170. Misrepresentation of this CMMC compliance status to the Government may result in criminal prosecution, including actions under section 1001, Title 18 of the United States Code, civil liability under the False Claims Act, and contract remedies as determined appropriate by the contracting officer.

☐ I certify that I have read the above statement.

[Affirm](#) [Cancel](#)

VIEW/EXPAND ASSESSMENT RESULTS

VIEW/EXPAND INCLUDED CAGE(S)

VIEW/EXPAND AFFIRMATION CONTACT(S) AND HISTORY

3.8 Assessment Edit/Cancel/Delete: A Cyber Vendor User may Edit, Cancel, or Delete certain CMMC Status Types. Select the available icon to complete the action.

CMMC Level 1 (Self)		CMMC Level 2 (Self)		Report Generated : 02/21/2025 13:15:21 ET					
Edit	CMMC Unique Identifier (UID)	CMMC Status Type	Assessment Date	CMMC Status Expiration Date	Assessment Scope	Included CAGE	Company Size	Cancel/Delete	
	S2 Details	Incomplete	01/31/2025	07/30/2025	ENTERPRISE		42		
	S2 Details	CMMC L2 Final Self-Assessment	01/31/2025	01/31/2026	ENCLAVE		1		
	S2 Details	CMMC L2 Final Self-Assessment (Retracted by Vendor)	01/22/2025	01/22/2026	ENTERPRISE		12		



NOTE: A “CMMC L2 Conditional Level 2 Self-Assessment” is valid for 180 days. A “CMMC L2 Final Level 2 Self-Assessment”, with annual affirmations verifying compliance, is valid for 3 years.”