SPRS

Supplier Performance Risk System

Cybersecurity Maturity Model Certification (CMMC)

CMMC LEVEL 2 SELF-ASSESSMENT
QUICK ENTRY GUIDE

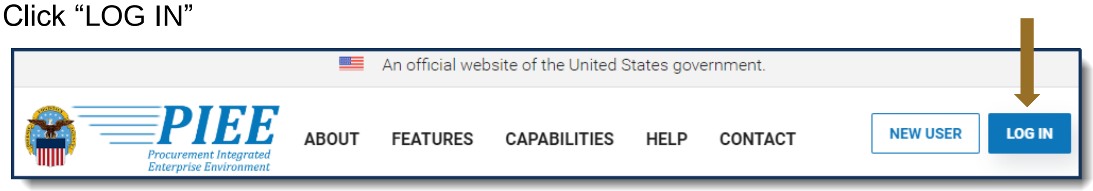
VERSION 4.0

NSLC PORTSMOUTH BLDG. 153-2 PORTSMOUTH NAVAL SHIPYARD, PORTSMOUTH, NH 03804-5000

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

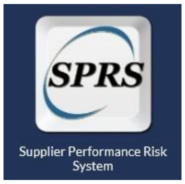
2. **SPRS Application and Module Access:**
   a. PIEE landing page: https://piee.eb.mil/piee-landing/

   b. Click “LOG IN”

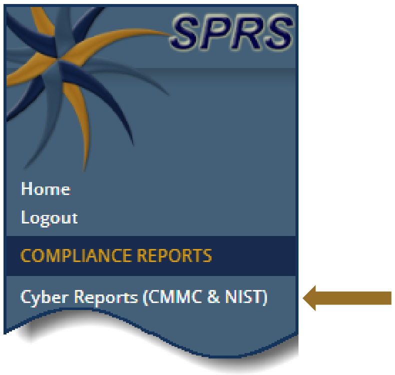

An official website of the United States government.
PIEE
Procurement Integrated Enterprise Environment
ABOUT
FEATURES
CAPABILITIES
HELP
CONTACT
NEW USER
LOG IN

Screenshot Dtd 09 JAN 2024

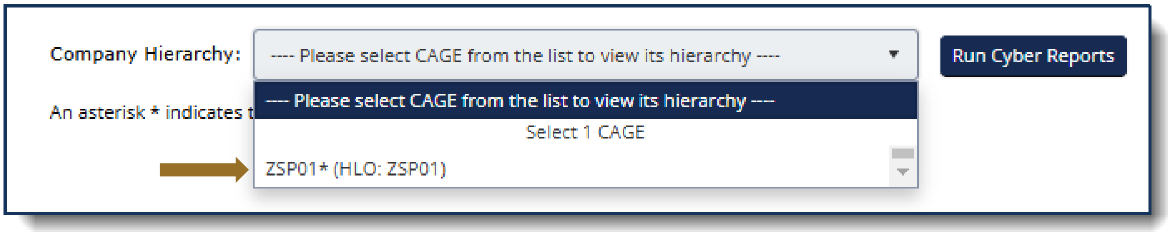
   c. Select **SPRS**:



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

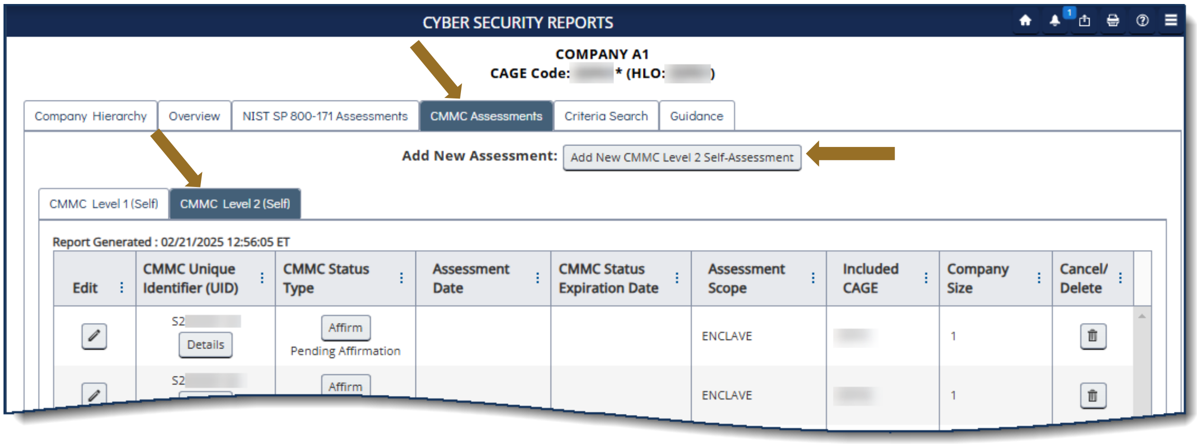


3. **Cyber Reports (CMMC & NIST):** Select the desired Hierarchy, identified by the HLO, from the drop down and select Run Cyber Reports button.


Company Hierarchy:
---- Please select CAGE from the list to view its hierarchy ----
Run Cyber Reports
An asterisk * indicates t
---- Please select CAGE from the list to view its hierarchy ----
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".



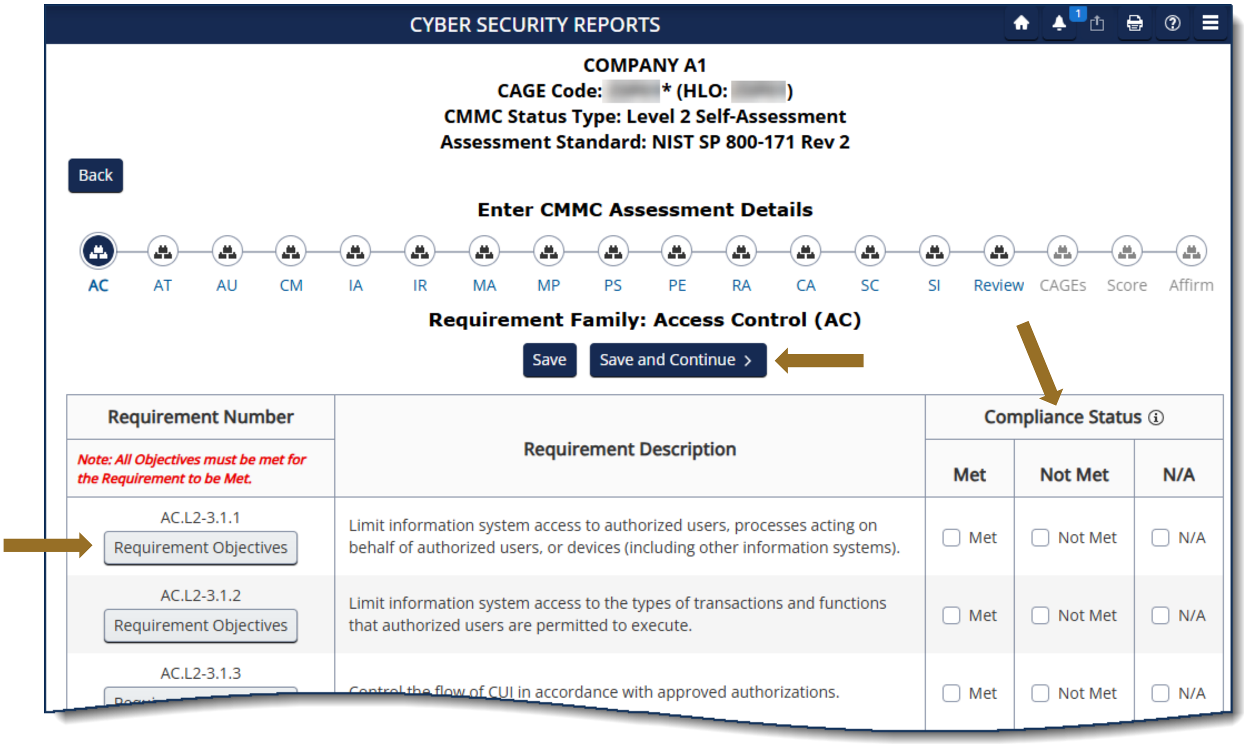
COMPANY A1
CAGE Code: [redacted] * (HLO: [redacted])

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

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[redacted] Details	Affirm Pending Affirmation			ENCLAVE	[redacted]	1	
	S2[redacted]	Affirm			ENCLAVE	[redacted]	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.



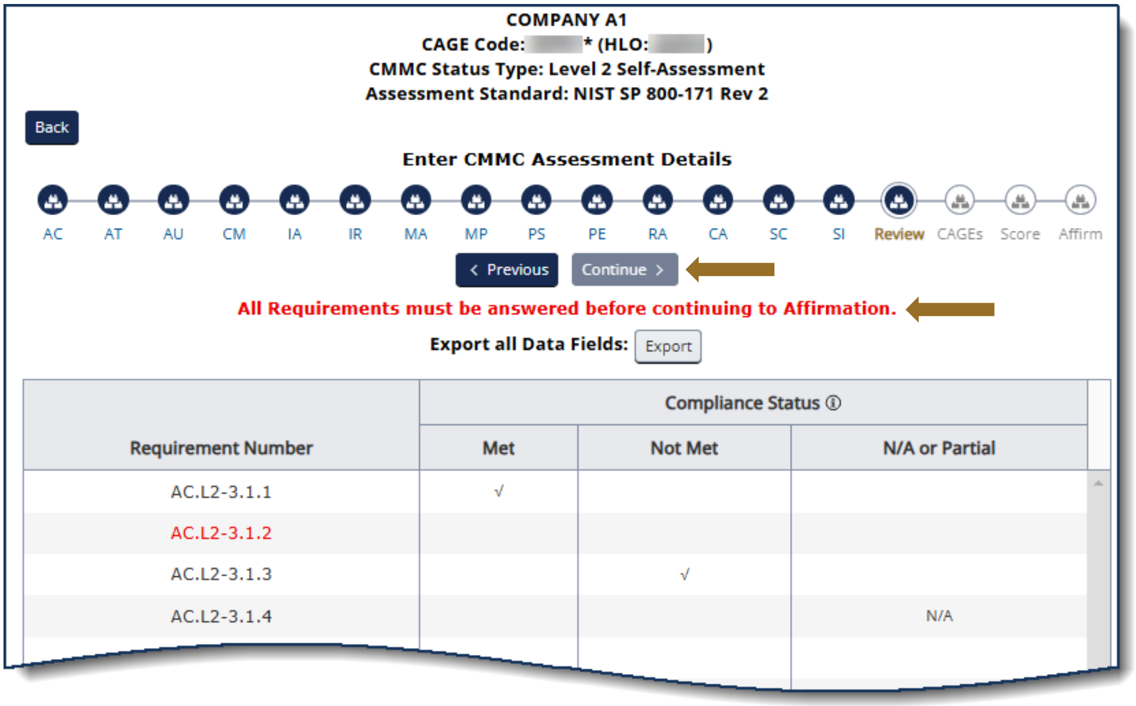
COMPANY A1
CAGE Code: [redacted] * (HLO: [redacted])
CMMC Status Type: Level 2 Self-Assessment
Assessment Standard: NIST SP 800-171 Rev 2

Enter CMMC Assessment Details

Requirement Family: Access Control (AC)

Requirement Number	Requirement Description	Compliance Status ⓘ		
Note: All Objectives must be met for the Requirement to be Met.		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	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.



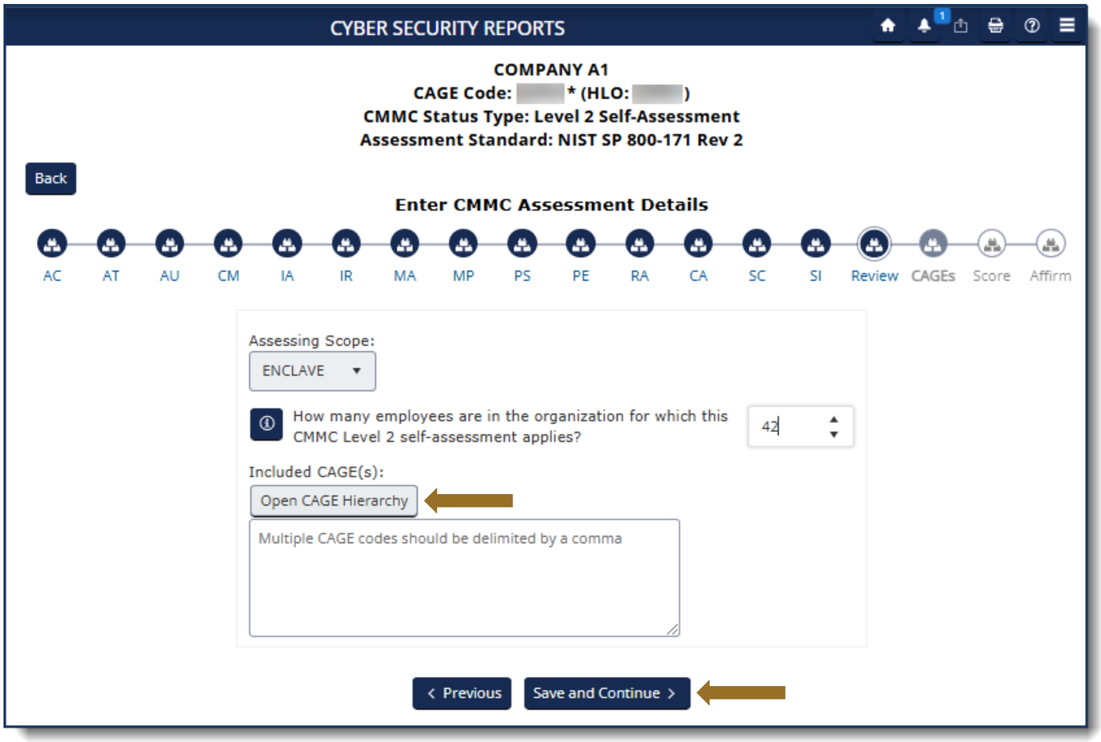
COMPANY A1
CAGE Code: [redacted] * (HLO: [redacted])
CMMC Status Type: Level 2 Self-Assessment
Assessment Standard: NIST SP 800-171 Rev 2

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.”



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

Assessing Scope: ENCLAVE ▾

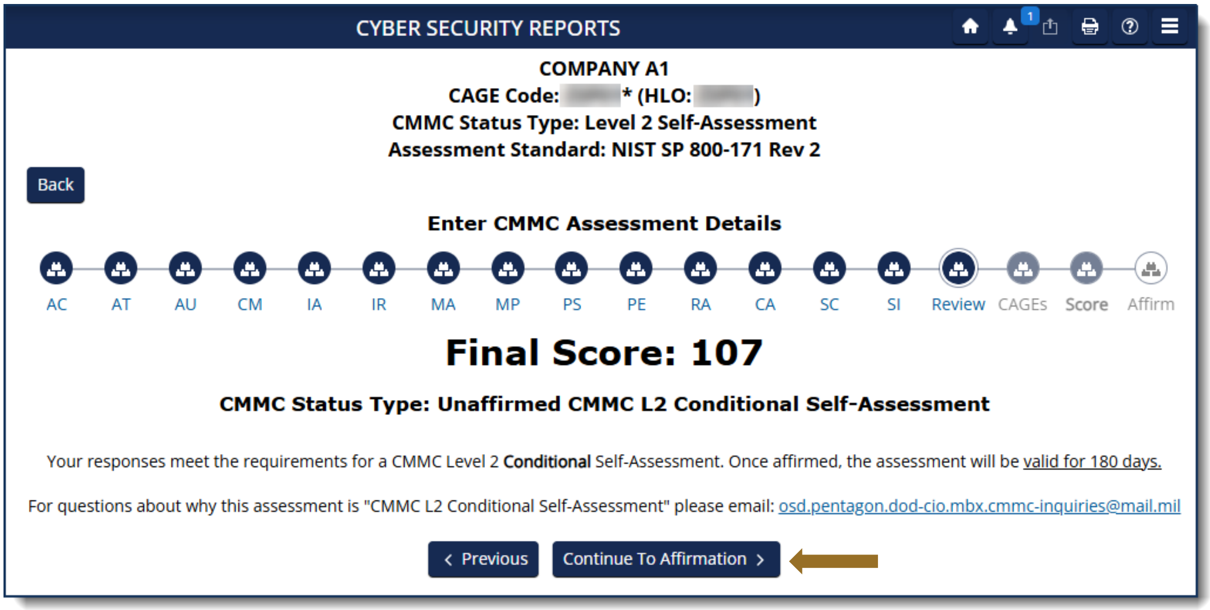
ⓘ How many employees are in the organization for which this CMMC Level 2 self-assessment applies? 42

Included CAGE(s):

Multiple CAGE codes should be delimited by a comma

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.



CYBER SECURITY REPORTS

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

Enter CMMC Assessment Details

Final Score: 107

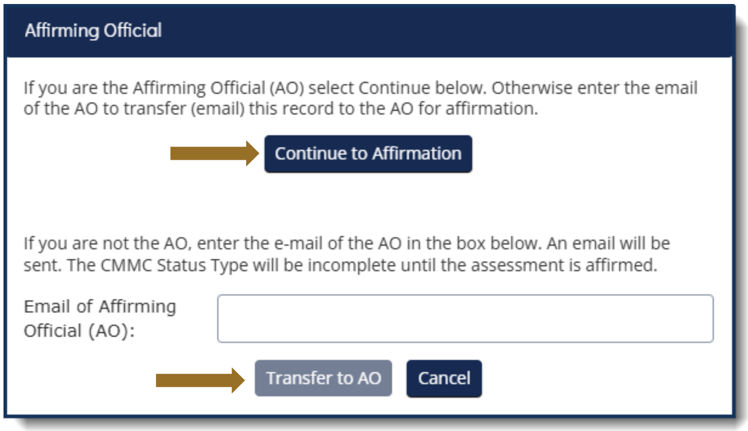
CMMC Status Type: Unaffirmed CMMC L2 Conditional Self-Assessment

Your responses meet the requirements for a CMMC Level 2 **Conditional** Self-Assessment. Once affirmed, the assessment will be valid for 180 days.

For questions about why this assessment is "CMMC L2 Conditional Self-Assessment" please email: osd.pentagon.dod-cio.mbx.cmmc-inquiries@mail.mil

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”.



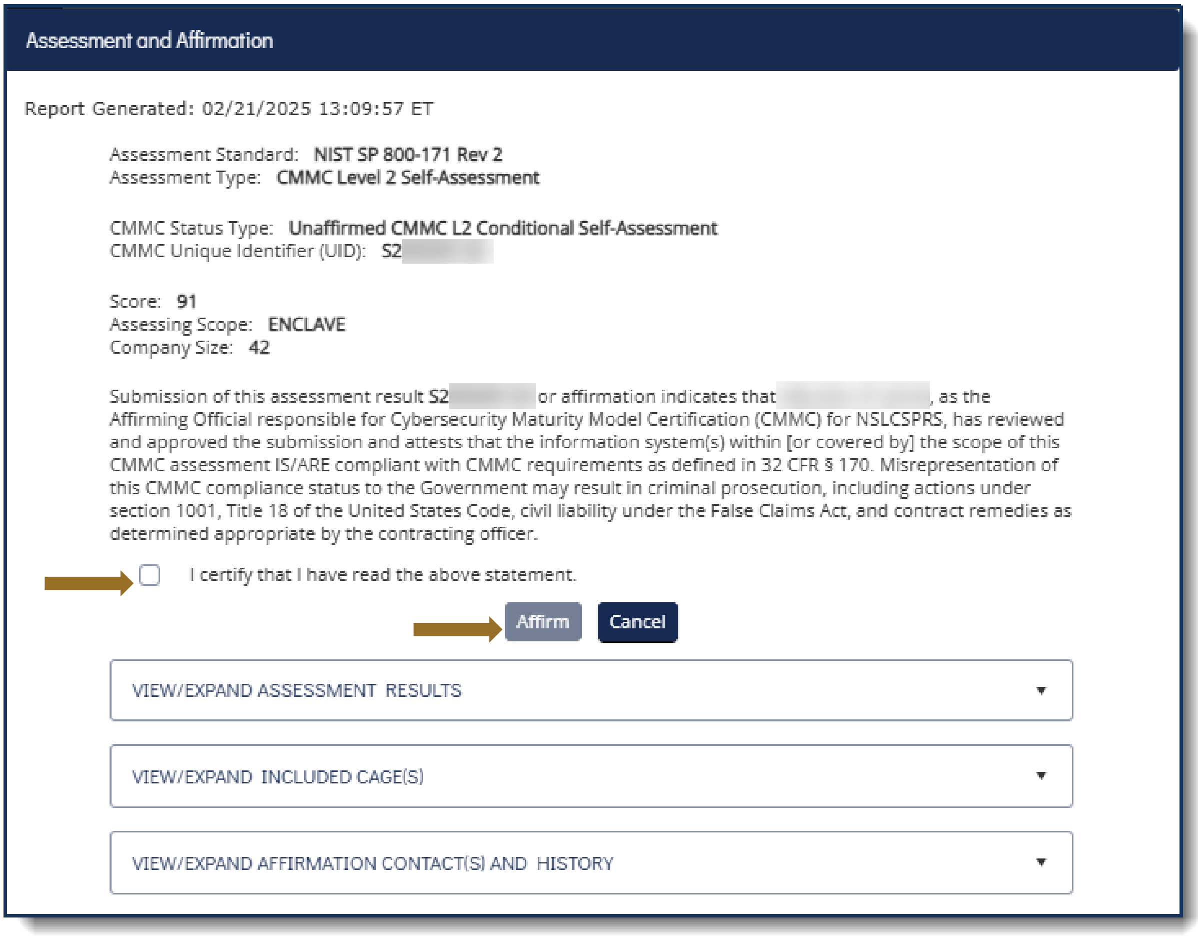
Affirming Official

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):

3.7 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[redacted]

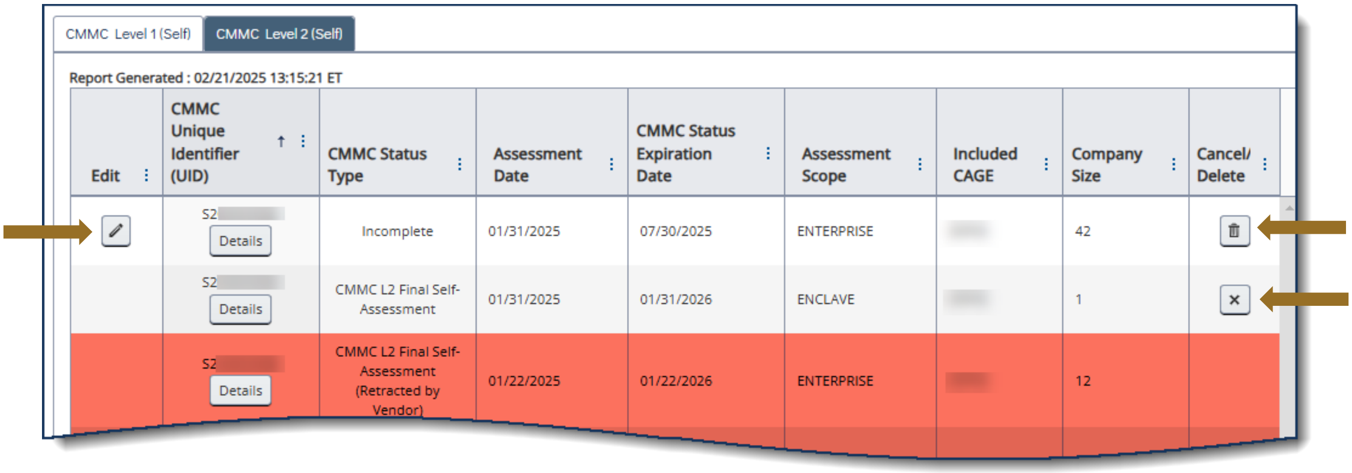
Score: 91
Assessing Scope: ENCLAVE
Company Size: 42

Submission of this assessment result S2[redacted]or affirmation indicates that [redacted], 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.



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[redacted] Details	Incomplete	01/31/2025	07/30/2025	ENTERPRISE	[redacted]	42	🗑
	S2[redacted] Details	CMMC L2 Final Self-Assessment	01/31/2025	01/31/2026	ENCLAVE	[redacted]	1	✕
	S2[redacted] Details	CMMC L2 Final Self-Assessment (Retracted by Vendor)	01/22/2025	01/22/2026	ENTERPRISE	[redacted]	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.”