## 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

FEB 2025

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

## 2. SPRS Application and Module Access:

- a. PIEE landing page: https://piee.eb.mil/piee-landing/
- b. Click "LOG IN"



**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	1	
	25P01*(HLO: 25P01)	*	

<u>NOTE:</u> 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			<b>.</b>	. <mark>1</mark> 1
			CAGE Co	COMPANY A1 de: * (HLO:	)			
Company Hierarchy	Overview NIS	ST SP 800-171 Assessments	CMMC Assessments	Criteria Search Gui	dance			
CMMC Level 1 (Si	elf) CMMC Level 2 d : 02/21/2025 12:56:	(Self) 05 ET	dd New Assessmen	t: Add New CMMC Level	2 Self-Assessment			
Edit :	CMMC Unique Identifier (UID)	CMMC Status Type	Assessment Date	CMMC Status Expiration Date	Assessment Scope	Included CAGE	Company Size	Cancel/ Delete
	S2 Details	Affirm Pending Affirmation			ENCLAVE		1	Î
	52	Affirm			ENCLAVE		1	Û

**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.



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

Back	COMPANY A1 CAGE Code: * (HLO: ) CMMC Status Type: Level 2 Self-Assessment Assessment Standard: NIST SP 800-171 Rev 2																
_						Ente	er CMN	1C Ass	essm	ent De	tails						
8-	-0-				-0-	-0-	-0-				-0-		-0	-3		-	-
AC	AT	AU	CM	IA	IR	MA	MP	PS	PE	RA	CA	SC	SI	Review	CAGEs	Score	Affirm
							< Pr	evious	Contir	iue > ]	<b>(</b>						
			All	Requi	rement	E	st be ai xport a	ISWERE	fields	Expor		g to Aff	irmat Is (i)	ion.		• 	
	R	equiren	nent Nu	umber			Me	et		Not	Met			N/A c	or Partia	ıl	
		AC.	L2-3.1.	1			V										*
		AC.	L2-3.1.	2													
		AC.	L2-3.1.	3						١	/						
		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 SECL	JRITY REPORTS		÷ *	≞ ⊕ ⊕ ≡
	CA CMMC S Assessm	COMPANY A AGE Code: * (H tatus Type: Level 2 S ent Standard: NIST	l LO: ) Self-Assessment SP 800-171 Rev 2		
Back	Ente	er CMMC Assessm	ent Details		
					All All All
	Assessing Scope: ENCLAVE  How many employed CMMC Level 2 self-a Included CAGE(s): Open CAGE Hierarchy Multiple CAGE codes shou	ees are in the organizat assessment applies? Id be delimited by a com	ion for which this 42	\$	

**<u>NOTE</u>**: 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: * (HLO: ) CMMC Status Type: Level 2 Self-Assessment Assessment Standard: NIST SP 800-171 Rev 2				
Enter CMMC Assessment Details				
<b> </b>	-	-0-	•	-
AC AT AU CM IA IR MA MP PS PE RA CA SC SI	Review	CAGEs	Score	Affirm
Final Score: 107				
CMMC Status Type: Unaffirmed CMMC L2 Conditional Self-Assess	sment	:		
Your responses meet the requirements for a CMMC Level 2 <b>Conditional</b> Self-Assessment. Once affirmed, the assess	ment wil	ll be <u>valid</u>	for 180	<u>) days.</u>
For questions about why this assessment is "CMMC L2 Conditional Self-Assessment" please email: osd.pentagon.dod-o	cio.mbx.	cmmc-ind	<u>uiries@</u>	mail.mil
< Previous Continue To Affirmation >				

<u>NOTE:</u> 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".



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

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: <b>91</b> Assessing Scope: <b>ENCLAVE</b> Company Size: <b>42</b>
Submission of this assessment result <b>S2</b> 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.

Report Gene	erated : 02/21/2025 13:15:2	1 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	1
	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	

**<u>NOTE</u>**: 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."