

CLEARED
For Open Publication

Jan 21, 2025

Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW



Overview for **DOD Cybersecurity & SAP IT Summit**

SPRS *Supplier Performance Risk System*

John Duncan
SPRS Program Manager
Portsmouth Naval Shipyard, Kittery, Maine
12 February 2025

Agenda

01

What is SPRS?

02

Path to Assessments

03

CMMC Level 1 Self-Assessments

04

CMMC Level 2 Self-Assessments

05

Online Resources and Points of Contact

What is SPRS? (1 of 2)

Supplier Performance Risk System

❖ “... the authoritative source to retrieve supplier and product PI [performance information]” (DoDI 5000.79)



❖ Vendor Performance

- ❖ Quality Classifications & On-time Delivery scores by FSC/PSC/NAICS
- ❖ Supplier Risk – Ranked risk of vendor performance – 79K+ CAGEs
- ❖ Price Risk – Average Price, Expected Range, over/underprice alerts – 1.6M+ items
- ❖ Item Risk – Suspected Counterfeit, CSI/CAI, DMSMS, etc. – 135K+ items

❖ Vendor Compliance

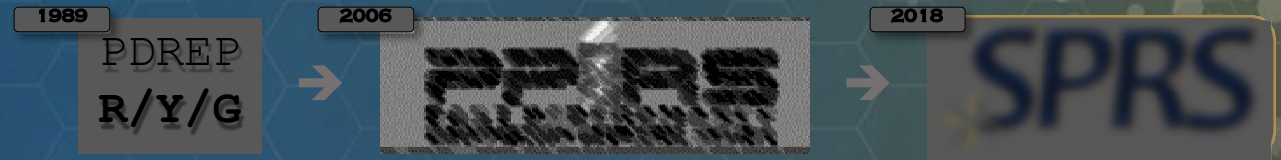
- ❖ Debarments/exclusions, § 889, FASCA, representations/certifications (from SAM)
- ❖ Cyber Security Assessments: NIST SP 800-171, CMMC
- ❖ NSS Restricted List (formerly § 806 “Do Not Buy List”)
- ❖ Vendor Threat Mitigation (§ 841 NCWtE)

❖ Supply Chain Illumination, contract history & analysis, corporate CAGE hierarchies

What is SPRS? (2 of 2)

Supplier Performance Risk System

❖ “... the authoritative source to retrieve supplier and product PI [performance information]” (DoDI 5000.79)



❖ Vendor Performance

- ❖ Quality Classifications & On-time Delivery scores by FSC/PSC/NAICS
- ❖ Supplier Risk – Ranked risk of vendor performance – 79K+ CAGEs
- ❖ Price Risk – Average Price, Expected Range, over/underprice alerts – 1.6M+ items
- ❖ Item Risk – Suspected Counterfeit, CSI/CAI, DMSMS, etc. – 135K+ items

❖ Vendor Compliance

- ❖ Debarments/exclusions, § 889, FASCA, representations/certifications (from SAM)
- ❖ Cyber Security Assessments: NIST SP 800-171, CMMC
- ❖ NSS Restricted List (formerly § 806 “Do Not Buy List”)
- ❖ Vendor Threat Mitigation (§ 841 NCWtE)

❖ **Supply Chain Illumination, contract history & analysis, corporate CAGE hierarchies**

Path to CS Self Assessments in SPRS

Create
System Security Plan (SSP)



NIST SP 800-171 Basic Assessment?
Use DPCAP Methodology
<https://www.acq.osd.mil/dpap/pdi/cyber/docs/NIST%20SP%20800-171%20Assessment%20Methodology%20Version%201.2.1%20%2006.24.2020.pdf>

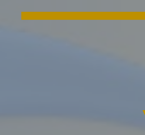
SAM – create
User account



SAM – register
Entities



SAM – receive
UEIs

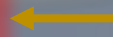


PIEE – establish
Vendor group

SAM – establish
CAGE hierarchy

CAGE.mil – validate
Company data

SAM - establish
EB POC



PIEE – assign
Contractor
Administrator (CAM)



PIEE – establish
User account(s)



PIEE – CAM approve
“SPRS Cyber
Vendor” role



SPRS – enter
Assessment results

Already using WAWF? You're in PIEE!

Create
System Security Plan (SSP)



NIST SP 800-171 Basic Assessment?
Use DPCAP Methodology
<https://www.acq.osd.mil/dpap/pdi/cyber/docs/NIST%20SP%20800-171%20Assessment%20Methodology%20Version%201.2.1%20%2006.24.2020.pdf>

SAM – create
User account



SAM – register
Entities

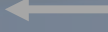


SAM – receive
UEIs



SAM - establish
EB POC

CAGE.mil – validate
Company data



SAM – establish
CAGE hierarchy



PIEE – establish
Vendor group



PIEE – assign
Contractor
Administrator (CAM)



PIEE – establish
User account(s)



**PIEE – CAM approve
“SPRS Cyber
Vendor” role**



**SPRS – enter
Assessment results**

CMMC Entry – Level 1 & 2



❖ Select CAGE from hierarchy

1

The screenshot shows the 'Supplier Performance Risk System' interface. On the left is a navigation menu with the following items: Home, Logout, COMPLIANCE REPORTS (with a sub-item 'Cyber Reports (CMMC & NIST)'), CAGE Hierarchy, RISK ANALYSIS REPORTS (with a sub-item 'Supplier Risk'), PERFORMANCE REPORTS (with sub-items 'Summary Report', 'Detail Pos/Neg Records', and 'Supply Code Relationship'), SERVICE (with a sub-item 'Feedback/Customer Support'), and Download. The main content area is titled 'CYBER SECURITY REPORTS' and contains a 'Company Hierarchy' dropdown menu with the text 'Please select CAGE from the list to view its hierarchy'. Below this is a list of CAGE codes, with 'ZSP01* (HLO: ZSP01)' highlighted. A 'Run Cyber Reports' button is located to the right of the dropdown. Red arrows indicate the steps: arrow 1 points to the 'Cyber Reports (CMMC & NIST)' menu item; arrow 2 points to the 'ZSP01* (HLO: ZSP01)' entry in the dropdown; and arrow 3 points to the 'Run Cyber Reports' button.

2

3

CMMC Entry – Level 1



CYBER SECURITY REPORTS

Back

COMPANY A1
CAGE Code: ZSP01* (HLO: ZSP01)

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

Add New Assessment: [Add New CMMC Level 1 Self-Assessment](#)

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

Report Generated : 01/14/2025 12:11:07 ET

Edit	CMMC Unique Identifier (UID)	CMMC Status Type	Assessment Date	CMMC Status Expiration Date	Assessment Scope	Included CAGE	Company Size	Delete
	S100000015 Details	Final Level 1 Self-Assessment	01/08/2025	01/08/2026	ENCLAVE	ZSP01	200	
	S100000034 Details	No CMMC Status	12/31/2024	12/31/2025	ENCLAVE	ZSP02	35	
	Details	Pending Affirmation	01/09/2025	01/09/2026	ENCLAVE	ZSP05	2	
	Details	Incomplete	01/09/2025	01/09/2026	ENCLAVE		0	

1 - 4 of 4 items

20 items per page

If you don't see this:

Add New CMMC Level 1 Self-Assessment

You don't have *SPRS Cyber Vendor User* role

CMMC Entry – Level 1 Entry



❖ Assessment Date

- ❖ Date assessment was conducted

❖ Assessing Scope

- ❖ Enterprise
- ❖ Enclave

❖ # Employees

❖ FAR 52.204-21 compliance

❖ Included CAGEs

- ❖ CAGEs accessing IT system subject to the SSP

CYBER SECURITY REPORTS

COMPANY A1
CAGE Code: ZSP01* (HLO: ZSP01)
CMMC Status Type: Level 1 Self-Assessment
Assessment Standard: NIST SP 800-171 Rev 2

Back

Enter CMMC Assessment Details

Assessment Date:

Assessing Scope:

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

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)

←

CMMC Entry – Send to Affirming Official



CYBER SECURITY REPORTS

COMPANY A1
CAGE Code: ZSP01* (HLO: ZSP01)
CMMC Status Type: Level 1 Self-Assessment
Assessment Standard: NIST SP 800-171 Rev 2

Back

Enter CMMC Assessment Details

Assessment Date:
1/7/2025

How many entries:
23

Are you complete:
Yes No

Included CAGE(s):
Open CAGE Hierarchy

ZSP05, ZSP01

Affirming Official

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

Continue to Affirmation

If you are not the AO, enter the e-mail of the AO in the box below and select "Transfer to AO". An email will be sent. The CMMC Status Type will be "Pending Affirmation" until the assessment is affirmed.

Email of Affirming Official (AO):

Transfer to AO **Cancel**

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

Save **Continue to Affirmation**

*Are you the AO?
Go to affirmation*

*Otherwise send email
w/ instructions to AO*

CMMC Affirmation Workflow



- ❖ AO logs into SPRS
- ❖ AO opens assessment “Pending Affirmation” (pencil to edit)

CYBER SECURITY REPORTS

COMPANY A1
CAGE Code: ZSP01* (HLO: ZSP01)

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

Add New Assessment: Add New CMMC Level 1 Self-Assessment

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

Report Generated : 01/14/2025 12:18:13 ET

Edit	CMMC Unique Identifier (UID)	CMMC Status Type	Assessment Date	CMMC Status Expiration Date	Assessment Scope	Included CAGE	Company Size	Delete
	Details	Final Level 1 Self-Assessment	01/07/2025	01/07/2026	ENCLAVE	ZSP01	23	
	Details	Final Level 1 Self-Assessment	01/07/2025	01/07/2026	ENCLAVE	ZSP05	23	
	Details	Incomplete	01/09/2025	01/09/2026	ENCLAVE		0	
	Details	No CMMC Status	12/31/2024	12/31/2025	ENCLAVE	ZSP02	35	
	Details	Pending Affirmation	01/09/2025	01/09/2026	ENCLAVE	ZSP05	2	

1 - 5 of 5 items



CMMC Affirmation Workflow (1 of 3)



- ❖ **AO verifies personal info and authority to affirm**
- ❖ **Optional: additional POCs for government KOs to contact regarding this assessment**

CYBER SECURITY REPORTS

COMPANY A1
CAGE Code: ZSP01* (HLO: ZSP01)
CMMC Status Type: Level 1 Self-Assessment
Assessment Standard: NIST SP 800-171 Rev 2

Back

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

< Previous Continue to Affirmation

CMMC Affirmation Workflow (2 of 3)



❖ AO reviews results and affirms

CYBER SECURITY REPORTS

Assessment and Affirmation

Report Generated: 01/14/2025 12:13:52 ET

Back

CMMC Status Type: **Unaffirmed Final Level 1 Self-Assessment**
CMMC Unique Identifier (UID): [REDACTED]

Level 1 CMMC Assessment Date: **01/07/2025**
CMMC Status Expiration Date: **01/07/2026**
Assessing Scope: **ENCLAVE**
Company Size: **23**

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

Included CAGEs/entities:

CAGE	Company Name	Address
ZSP01	COMPANY A1	A1 ROAD SUITE 16, MONTPELIER, CA, USA
ZSP05	COMPANY A5	A5 ROAD BLDG 153-2, A5 CITY, AA, USA

Submission of this assessment result [REDACTED] 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.

1 → I certify that I have read the above statement.

2 →

CMMC Affirmation Workflow (3 of 3)



- ❖ *Assessment record has UID, Final/No CMMC Status and Expiration Date*

Company Hierarchy	Overview	NIST SP 800-171 Assessments	CMMC Assessments	Criteria Search	Guidance
Add New Assessment: Add New CMMC Level 1 S...					
CMMC Level 1 (Self)		CMMC Level 2 (Self)			
Report Generated : 01/14/2025 12:11:07 ET					
Edit	CMMC Unique Identifier (UID)	CMMC Status Type	Assessment Date	CMMC Status Expiration Date	
	S100000015 Details	Final Level 1 Self-Assessment	01/08/2025	01/08/2026	

CMMC Entry – Level 2 (1 of 5)



CYBER SECURITY REPORTS

COMPANY A1
CAGE Code: ZSP01* (HLO: ZSP01)

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 : 01/14/2025 12:24:35 ET

Edit	CMMC Unique Identifier (UID)	CMMC Status Type	Assessment Date	CMMC Status Expiration Date	Assessment Scope	Included CAGE	Company Size	Cancel/Delete
	Details	Incomplete						
	Details	Incomplete			ENCLAVE	ZSP05	123	
	Details							
	Details	Incomplete			ENCLAVE	ZSP03	76	
	Details	No CMMC Status						

If you don't see this:
Add New CMMC Level 2 Self-Assessment
You don't have *SPRS Cyber Vendor User* role

DRAFT

CMMC Entry – Level 2 (2 of 5)



- ❖ *User steps through requirement “families” and checks appropriate responses*

CYBER SECURITY REPORTS

COMPANY A1
CAGE Code: ZSP01* (HLO: ZSP01)
CMMC Status Type: Level 2 Self-Assessment
Assessment Standard: NIST SP 800-171 Rev 2

Enter CMMC Assessment Details

Progress tracker

Back

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

Requirement Family 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).	<input type="checkbox"/> Met	<input type="checkbox"/> Not Met	<input type="checkbox"/> 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.	<input type="checkbox"/> Met	<input type="checkbox"/> Not Met	<input type="checkbox"/> N/A
AC.L2-3.1.3 Requirement Objectives	Control the flow of CUI in accordance with approved authorizations.	<input type="checkbox"/> Met	<input type="checkbox"/> Not Met	<input type="checkbox"/> N/A
AC.L2-3.1.4 Requirement Objectives	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	<input type="checkbox"/> Met	<input type="checkbox"/> Not Met	<input type="checkbox"/> N/A

CMMC Entry – Level 2 (3 of 5)



❖ *Objective details available in pop-up*

CYBER SECURITY REPORTS

COMPANY A1
CAGE Code: ZSP01* (HLO: ZSP01)
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 CAGEs Review Score Affirm

Requirement Family AC

Requirement Number	Requirement Description	Compliance Status ⓘ		
		Met	Not Met	N/A
AC.L2-3.1.1	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
AC.L2-3.1.2		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
AC.L2-3.1.3	Control the flow of CUI in accordance with approved authorizations.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
AC.L2-3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Requirement Objectives

Objective Number	Objective Description
AC.L2-3.1.2[a]	Determine if the types of transactions and functions that authorized users are permitted to execute are defined.
AC.L2-3.1.2[b]	Determine if system access is limited to the defined types of transactions and functions for authorized users.

CMMC Entry – Level 2 (4 of 5)



❖ *Certain requirements must be answered at the objective level*

CYBER SECURITY REPORTS

COMPANY A1
CAGE Code: ZSP01* (HLO: ZSP01)
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 CAGES Review Score Affirm

Requirement Family IA

< Previous Save Save and Continue >

Requirement Number	Requirement Description	Compliance Status ⓘ		
		Met	Not Met	N/A
IA.L2-3.5.1 Requirement Objectives	Identify information system users, processes acting on behalf of users, or devices.	<input type="checkbox"/> Met	<input type="checkbox"/> Not Met	<input type="checkbox"/> N/A
IA.L2-3.5.2 Requirement Objectives	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	<input type="checkbox"/> Met	<input type="checkbox"/> Not Met	<input type="checkbox"/> N/A
IA.L2-3.5.3 *Answer this requirement through the Open Objectives button Open Objectives	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	<input checked="" type="checkbox"/> Met *	<input checked="" type="checkbox"/> Not Met *	<input checked="" type="checkbox"/> Partial *
IA.L2-3.5.4 Requirement Objectives	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	<input type="checkbox"/> Met	<input type="checkbox"/> Not Met	<input type="checkbox"/> N/A

CMMC Entry – Level 2 (5 of 5)



❖ Individual objectives

CYBER SECURITY REPORTS

COMPANY A1
 CAGE Code: ZSP01* (HLO: ZSP01)
 CMMC Status Type: Level 2 Self-Assessment
 Assessment Standard: NIST SP 800-171 Rev 2

Back

Enter CMMC Assessment Details

AC AT AU SC SI CAGEs Review Score Affirm

Requirement Objectives

Objective Number	Objective Description	Compliance Status ⓘ		
		Met	Not Met	N/A
IA.L2-3.5.3[a]	Determine if privileged accounts are identified.	<input type="checkbox"/> Met	<input type="checkbox"/> Not Met	<input type="checkbox"/> N/A
IA.L2-3.5.3[b]	Determine if multifactor authentication is implemented for local access to privileged accounts.	<input type="checkbox"/> Met	<input type="checkbox"/> Not Met	<input type="checkbox"/> N/A
IA.L2-3.5.3[c]	Determine if multifactor authentication is implemented for network access to privileged accounts.	<input type="checkbox"/> Met	<input type="checkbox"/> Not Met	<input type="checkbox"/> N/A
IA.L2-3.5.3[d]	Determine if multifactor authentication is implemented for network access to non-privileged accounts.	<input type="checkbox"/> Met	<input type="checkbox"/> Not Met	<input type="checkbox"/> N/A

Save

Requirement Number		Compliance Status ⓘ		
		Met	Not Met	N/A
IA.L2-3.5.1	Requirement Objectives			
IA.L2-3.5.2	Requirement Objectives			
IA.L2-3.5.3	Open Objectives	<input type="checkbox"/> Met	<input type="checkbox"/> Not Met	<input type="checkbox"/> N/A
IA.L2-3.5.4	Requirement Objectives			
		Met *	Not Met *	Partial *

CMMC Affirmation – Level 2 (1 of 4)



❖ Affirmation process similar to Level 1

CYBER SECURITY REPORTS

COMPANY A1
CAGE Code: ZSP01* (HLO: ZSP01)
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 CAGES Review Score Affirm

< Previous Save Save and Continue >

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
ZSP04, ZSP05

< Previous Save Save and Continue >

CMMC Affirmation – Level 2 (2 of 4)



❖ *Assessment can't be sent to AO until all requirements have been answered*

CYBER SECURITY REPORTS

COMPANY A1
CAGE Code: ZSP01* (HLO: ZSP01)
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 CAGEs **Review** Score Affirm

< Previous Continue To Affirmation >

All Requirements must be answered before continuing to Affirmation.

Export all Data Fields:

Requirement Number	Compliance Status ①		
	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			
AC.L2-3.1.5			
AC.L2-3.1.6			
AC.L2-3.1.7			

CMMC Affirmation – Level 2 (3 of 4)



❖ *Score is calculated*

CYBER SECURITY REPORTS

COMPANY A1
CAGE Code: ZSP01* (HLO: ZSP01)
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 CAGEs Review Score Affirm

< Previous Continue To Affirmation >

Final Score: 90

CMMC Status Type: Unaffirmed CMMC L2 Conditional Self-Assessment

Your responses meet the requirements for a Level 2 Conditional Self-Assessment. This assessment will be valid for 180 days.

One or more responses did not meet the requirements for a Level 2 Self-Assessment. For more question about why this assessment is being logged as "CMMC L2 Conditional Self-Assessment" please email: osd.pentagon.dod-cio.mbx.cmmc-inquiries@mail.mil base email: osd.pentagon.dod-cio.mbx.cmmc-inquiries@mail.mil

< Previous Continue To Affirmation >

CMMC Affirmation – Level 2 (4 of 4)



- ❖ *AO verifies personal info, reviews results, and affirms*

CYBER SECURITY REPORTS

COMPANY A1
CAGE Code: ZSP01* (HLO: ZSP01)
CMMC Status Type: Level 2 Self-Assessment

Assessment and Affirmation

Report Generated: 01/14/2025 12:28:27 ET

Assessment Standard:
Assessment Type: CMMC Level 2 Self-Assessment

CMMC Status Type: [REDACTED]
CMMC Unique Identifier (UID): [REDACTED]

Score: No Score
Assessing Scope:
Company Size:

Submission of this assessment result S200000036 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.

1 I certify that I have read the above statement.

2 **Affirm** **Cancel**

VIEW/EXPAND ASSESSMENT RESULTS

VIEW/EXPAND INCLUDED CAGE(S)

< Previous Continue To Affirmation >

Expanded for details prior to affirming

SPRS User Roles – PIEE single sign-on



❖ *Government (KOs, PMs, LOGgies, etc.)*

❖ **SPRS ACQUISITION PROFESSIONAL**

- ❖ *Gives access to all scores/reports*

❖ *Contractor/Vendor*

❖ **SPRS CONTRACTOR/VENDOR (SUPPORT ROLE)**

- ❖ *View your company's scores/reports*
- ❖ *View-only access to CS assessments*
- ❖ *CAGE hierarchy*

❖ **SPRS CYBER VENDOR USER** ←

- ❖ *Add/edit/delete/affirm CS assessments*
- ❖ *CAGE hierarchy*

<https://piee.eb.mil>



Add New CMMC Level 2 Self-Assessment

Website and Help



<https://www.sprs.csd.disa.mil>

SPRS
Guiding the DoD in Responsible Acquisition Decisions

Menu X

- Home
- NSS Restricted List
- NIST SP 800-171 Assessments
- Enhanced Vendor Profile
- Access Instructions
- References
- FAQs
- Training
- Release
- Contacts

Login/Register (via PIEE) | SPRS FAQs | Cyber Reports (CMMC & NIST) | OSD Instructions GPC & Contracting | SPRS Reports

Welcome to SPRS

CMMC Level 1 Self-Assessment for Vendors now available online.
For assistance view our [CMMC Quick Entry Guide](#)

CMMC Entry Tutorial

SPRS
Supplier Performance Risk System
Training

References
User Guides
Quick Reference Guides
PIEE Access Help
Eval Criteria

Training
PPTs
Tutorial videos

CMMC Level 1
Quick Entry Guide

SPRS Contact Information

SPRS Website:

<https://www.sprs.csd.disa.mil>

NSLC Help Desk Email:

nslcports-helpdesk@us.navy.mil

Newly-improved **Feedback** (bottom of app menu)

Questions

