



Overview of Cybersecurity Assessments in SPRS

 **SPRS**
Supplier Performance Risk System

Disclaimer:

These slides are being posted by RTX for training and education purposes only, and permission was granted by the author to post the slides.

All the names, addresses, codes, scores, and other personal data information is fictitious and for training purposes only.

What is SPRS?

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?

Supplier Performance Risk System

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



- ❖ **Vendor Performance**

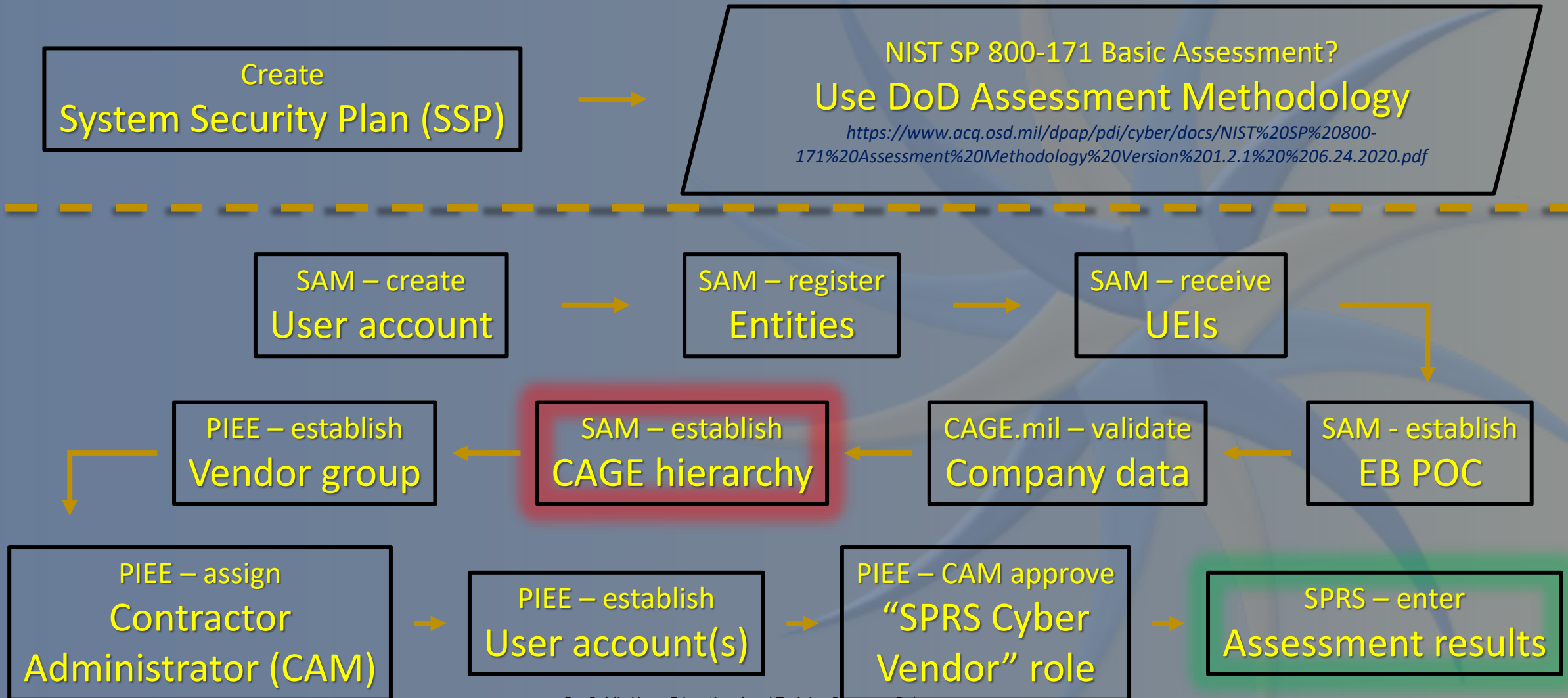
- ❖ Quality Classifications & On-time Delivery scores by FSC/PSC/NAICS
- ❖ Supplier Risk – Ranked risk of vendor performance – 79K+ CAGEs
- ❖ Price Risk – Average Price, Expected Range, over/underprice alerts – 1.6M+ items
- ❖ Item Risk – Suspected Counterfeit, CSI/CAI, DMSMS, etc. – 135K+ items

- ❖ **Vendor Compliance**

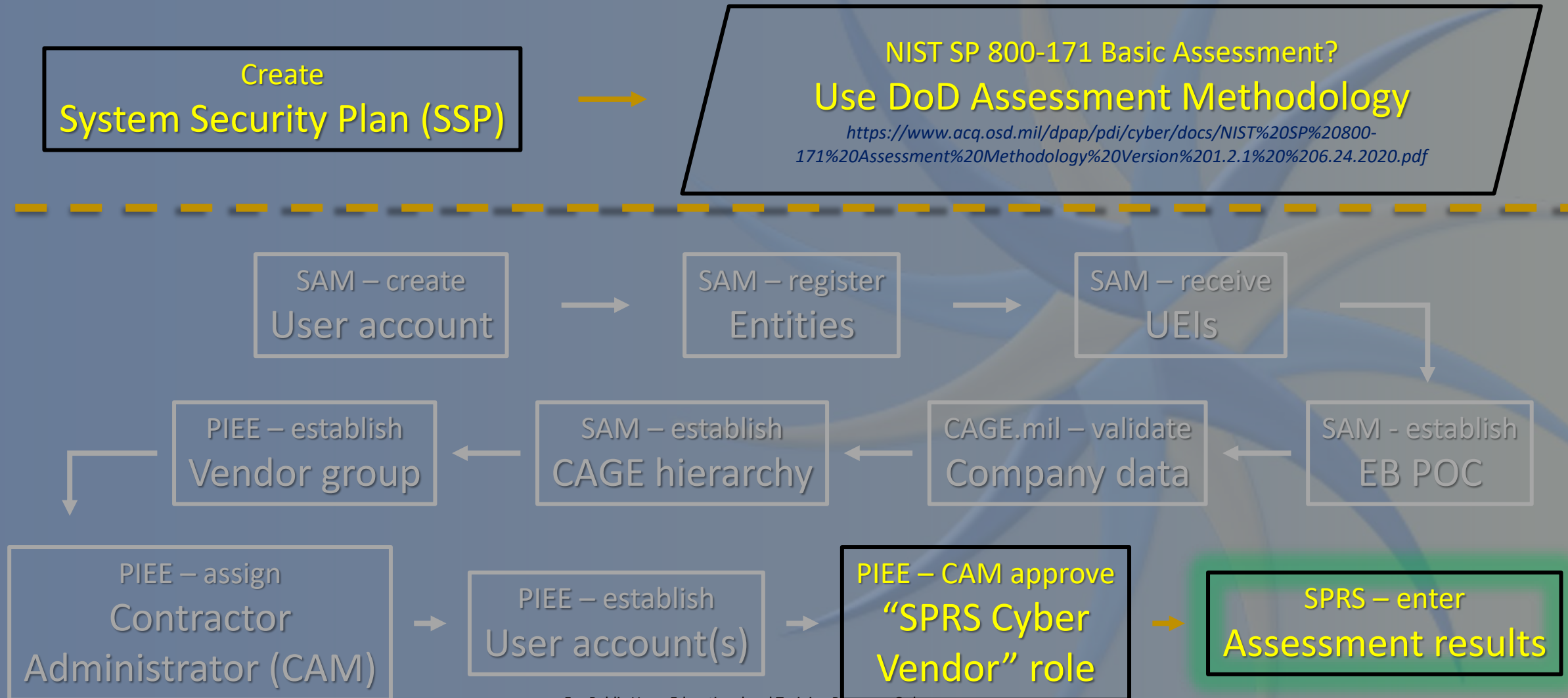
- ❖ Debarments/exclusions, § 889, FASCA, representations/certifications (from SAM)
- ❖ **Cyber Security Assessments: NIST SP 800-171, CMMC**
- ❖ NSS Restricted List (formerly § 806 “Do Not Buy List”)
- ❖ Vendor Threat Mitigation (§ 841 NCWtE)

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

Path to CS Self-Assessments in SPRS



Already using WAWF? You're in PIEE!



NIST SP 800-171 Assessments



❖ Select Highest Level Owner (HLO) CAGE from hierarchy

CYBER SECURITY REPORTS

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

An asterisk * indicates t

----- Please select CAGE from the list to view its hierarchy -----

Select 1 CAGE

ZSP01* (HLO: ZSP01)

Run Cyber Reports

If you don't see this: Add New NIST Assessment

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

❖ Add assessment result(s)

CYBER SECURITY REPORTS

Cyber Reports (CMMC & NIST) > CAGE: ZSP01* (HLO: ZSP01)

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 NIST Assessment

Basic Medium High Virtual High On-Site

Report Generated : 05/05/2025 10:05:12 ET

Edit/ Delete	DoD Unique Identifier (UID)	Included CAGE	Company Name	Assessment Date	Score	Assessment Scope	Plan Of Action Completion Date	System Security Plan (SSP) Assessed	SSP Version	Revision
		ZSP02	COMPANY A2	05/01/2025	108	ENTERPRISE	04/02/2026	MAW SSP Test		
		ZSP02	COMPANY A2	05/01/2025	108	ENTERPRISE	05/14/2025	Test 123	1	
		ZSP01	COMPANY A1	05/01/2025	108	ENTERPRISE	05/14/2025	Test 123	1	

NIST SP 800-171 Assessment - Entry



CYBER SECURITY REPORTS

COMPANY A1
CAGE Code: ZSP01* (HLO: ZSP01)
Confidence Level: BASIC
Assessment Standard: NIST SP 800-171

Back

Enter Assessment Details

Assessment Date:
MM/DD/YYYY

Assessment Score:
←

Assessing Scope:
--Select--

Plan of Action Completion Date:
MM/DD/YYYY

System Security Plan (SSP) Assessed:
Document Name

SSP Version/Revision:

SSP Date:
MM/DD/YYYY

Included CAGE(s):
Open CAGE Hierarchy
Multiple CAGE codes should be delimited by a comma

Save

Max = 110

*Enterprise,
Enclave,
Contract*

*Title of
document*

*Select CAGES
subject to the
assessed SSP*

CAGE Hierarchy

Search

- ☐ ZSP01: COMPANY A1 (DBA: COMPANY A1), A1 ROAD SUITE 16, MONTPELIER, CA, USA
- ☐ ZSP02: COMPANY A2 (DBA: COMPANY A2), A2 ROAD , NINA, WV, USA
- ☐ ZSP03: COMPANY A3 (DBA: COMPANY A3), A3 ROAD , CHESTER, PA, USA
- ☐ ZSP04: COMPANY A4 (DBA: COMPANY A4), A4 ROAD , A4 CITY, AA, USA
- ☐ ZSP05: (OBSOLETE) COMPANY A5 (DBA: COMPANY A5), A5 ROAD BLDG 153 2, A5 CITY, AA, USA

Cancel Ok

💡 If your hierarchy is wrong, you won't be able to select all your CAGES

CMMC Entry – Level 1 & 2



❖ *Select CAGE from hierarchy*

The screenshot displays the 'Supplier Performance Risk System' interface. On the left is a navigation menu with the following items: Home, Logout, COMPLIANCE REPORTS, Cyber Reports (CMMC & NIST), CAGE Hierarchy, RISK ANALYSIS REPORTS, Supplier Risk, PERFORMANCE REPORTS, Summary Report, Detail Pos/Neg Records, Supply Code Relationship, SERVICE, Feedback/Customer Support, and Download. A red arrow labeled '1' points to the 'Cyber Reports (CMMC & NIST)' menu item. The main content area is titled 'CYBER SECURITY REPORTS'. It contains a 'Company Hierarchy:' label, a text input field with the placeholder '--- Please select CAGE from the list to view its hierarchy ---', and a 'Run Cyber Reports' button. A red arrow labeled '2' points to the dropdown menu that appears below the input field, which contains the text '--- Please select CAGE from the list to view its hierarchy ---', 'Select 1 CAGE', and a list of options including 'ZSP01* (HLO: ZSP01)'. A red arrow labeled '3' points to the 'Run Cyber Reports' button.

CMMC Entry – Level 1



CYBER SECURITY REPORTS

Cyber Reports (CMMC & NIST) > CAGE: ZSP01* (HLO: ZSP01)

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)

CMMC Level 2 (C3PAO)

CMMC Level 3 (DIBCAC)

Report Generated : 05/05/2025 10:08:12 ET

Edit	CMMC Unique Identifier (UID)	CMMC Status Type	Assessment Date	CMMC Status Expiration Date	Assessment Scope	Included CAGE(s)	Company Size	Delete
	Details	Final Level 1 Self-Assessment	04/20/2025	04/20/2026	ENTERPRISE	ZSPA3	25	
	Details	Final Level 1 Self-Assessment	03/26/2025	03/26/2026	ENTERPRISE	ZSP01, ZSP02	25	
	Details	No CMMC Status	03/26/2025	03/26/2026	ENTERPRISE	ZSPA7	255	
		Final Level 1 Self-	02/06/2025			ZSP03	4	

!

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 with access to IT system subject to the assessment scope

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: MM/DD/YYYY

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)

Save Continue to Affirmation

! If your hierarchy is wrong, you won't be able to select all your CAGEs

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 employees:
23

Are you compliant:
Yes ☒ No ☐

Included CAGE(s):
Open CAGE Hierarchy

ZSP05, ZSP01

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)(5170.4)

Save Continue to Affirmation

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

*Are you the AO?
Go to affirmation*

*Otherwise send email
w/ instructions to AO*

CMMC Affirmation Workflow



- ❖ *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



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



CMMC Level 1 (Self) CMMC Level 2 (Self) CMMC Level 2 (C3PAO) CMMC Level 3 (DIBCAC)				
Report Generated : 10/22/2025 11:45:03 ET				
Edit	CMMC Unique Identifier (UID)	CMMC Status Type	Assessment Date	Affirmation Expiration
	S200002100 Details	CMMC L2 Final Self-Assessment	10/07/2025	10/07/2025
	S200001599 Details	Pending Affirmation Affirm	08/22/2025	02/18/2026
	S200002133 Details	CMMC L2 Conditional Self-Assessment	09/08/2025	03/07/2026

CMMC Affirmation Workflow



❖ 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 → **Affirm** **Cancel**

CMMC Affirmation Workflow



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

Company Hierarchy

Overview

NIST SP 800-171 Assessments

CMMC Assessments

Criteria Search

Add New Assessment:

Add New CMMC Level

CMMC Level 1 (Self)

CMMC Level 2 (Self)

CMMC Level 2 (C3PAO)

CMMC Level 3 (DIBCAC)

Report Generated : 05/05/2025 10:08:12 ET

Edit	CMMC Unique Identifier (UID)	CMMC Status Type	Assessment Date	CMMC Status Expiration Date
	S100001221 Details	Final Level 1 Self-Assessment	04/20/2025	04/20/2026

CMMC Entry – Level 2

CYBER SECURITY REPORTS

Cyber Reports (CMMC & NIST) > CAGE: ZSP01* (HLO: ZSP01)

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)

CMMC Level 2 (C3PAO)

CMMC Level 3 (DIBCAC)

Report Generated : 05/05/2025 10:11:22 ET

Edit	CMMC Unique Identifier (UID)	CMMC Status Type	Assessment Date	Affirmation Expiration Date	CMMC Status Expiration Date	Assessment Scope	Last Entered or Affirmed CAGE(s) in Scope	Current CAGE(s) Status	Company Size	Cancel/ Delete
	Details	Incomplete								
	Details	Affirm Pending Affirmation	04/18/2025	10/15/2025	10/15/2025	ENTERPRISE	ZSP05	ZSP05	25	
	Details	CMMC L2 Final Self-Assessment	04/30/2025	04/30/2026	04/30/2028	ENCLAVE	ZSPA4	ZSPA4	100	x
	Details	CMMC L2 Final Self-Assessment (Retracted by Vendor)	04/30/2025	04/30/2026	04/30/2028	ENCLAVE	ZSPA3		255	
		CMMC L2 Final Self-Assessment	04/30/2025	04/30/2026	04/30/2028				100	

If you don't see this:

Add New CMMC Level 2 Self-Assessment

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

CMMC Entry – Level 2



- ❖ *User steps through requirement “families” and checks appropriate responses*
- ❖ *Certain requirements must be answered at the objective level*

CYBER SECURITY REPORTS

Cyber Reports (CMMC & NIST) > CAGE: ZSP01* (HLO: ZSP01)

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

Progress tracker

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

Requirement Family: Identification and Authentication (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.	☐ Met	☐ Not Met	☐ 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.	☐ Met	☐ Not Met	☐ N/A
IA.L2-3.5.3 *Answer this requirement through the Open Objectives button	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	Met *	Not Met *	N/A *
IA.L2-3.5.4 Open Objectives	Use password-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	☐ Met	☐ Not Met	☐ N/A

CYBER SECURITY REPORTS

Cyber Reports (CMMC & NIST) > CAGE: ZSP01* (HLO: ZSP01)

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 Review CAGES Score Affirm

Requirement Number	Objective Description	Compliance Status
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.L2-3.1.2[a] Requirement Objectives	Determine if the types of transactions and functions that authorized users are permitted to execute are defined.	Met Not Met N/A
AC.L2-3.1.2[b] Requirement Objectives	Determine if system access is limited to the defined types of transactions and functions for authorized users.	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
AC.L2-3.1.4 Requirement Objectives	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	Met Not Met N/A
AC.L2-3.1.5 Requirement Objectives	Employ the principle of least privilege, including for specific security functions and privileged accounts.	Met Not Met N/A

CMMC Entry – Level 2



❖ Individual objectives

CYBER SECURITY REPORTS

Cyber Reports (CMMC & NIST) > CAGE: ZSP01* (HLO: ZSP01)

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

Back

ACATAU CM

Requirement Number

Note: All Objectives must be met for the Requirement to be Met.

IA.L2-3.5.1
Requirement Objectives

IA.L2-3.5.2
Requirement Objectives

IA.L2-3.5.3
*Answer this requirement though the Open Objectives button
Open Objectives

IA.L2-3.5.4

Identify information systems and organizational assets that contain or could be accessed by Federal agencies or other organizations for information that is excluded from public release.

Authenticate (or verify) the identity of users, devices, and systems that are accessing organizational information systems and organizational assets.

Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.

Use password-resistant authentication mechanisms for network access to privileged and non-privileged accounts.

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.	☐ Met	☐ Not Met	☐ N/A
IA.L2-3.5.3[b]	Determine if multifactor authentication is implemented for local access to privileged accounts.	☐ Met	☐ Not Met	☐ N/A
IA.L2-3.5.3[c]	Determine if multifactor authentication is implemented for network access to privileged accounts.	☐ Met	☐ Not Met	☐ N/A
IA.L2-3.5.3[d]	Determine if multifactor authentication is implemented for network access to non-privileged accounts.	☐ Met	☐ Not Met	☐ N/A

Save

ReviewCAGESScoreAffirm

Compliance Status ⓘ		
Met	Not Met	N/A
☐ Met	☐ Not Met	☐ N/A
☐ Met	☐ Not Met	☐ N/A
Met *	Not Met *	N/A *
☐ Met	☐ Not Met	☐ N/A

CMMC Affirmation – Level 2



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

CYBER SECURITY REPORTS

Cyber Reports (CMMC & NIST) > CAGE: ZSP01* (HLO: ZSP01)

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

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			
AC.L2-3.1.5			
AC.L2-3.1.6			
AC.L2-3.1.7			

For Public Use – Educational and Training Purposes Only

CMMC Affirmation – Level 2



❖ *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

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.

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

< Previous

Continue To Affirmation >

For Public Use – Educational and Training Purposes Only

22

CMMC Affirmation – Level 2



❖ *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 >

For Public Use – Educational and Training Purposes Only

CMMC Affirmation – Level 2



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

❖ *AO will NOT see the record if the HLO entered by the C3PAO is not yours (per SAM)*

💡 *If your C3PAO sends an incorrect HLO, your AO won't be able to affirm*

Assessment and Affirmation

Report Generated: 05/05/2025 10:22:05 ET

Current Assessment Details

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

CMMC Unique Identifier (UID): [REDACTED]
CMMC Status Type: Pending Affirmation
Score: 109
Assessment Date: 04/18/2025
Company Size: 25
Assessing Scope: ENTERPRISE
CAGE(s) in Scope: ZSP05

Initial Affirmation Expiration Date: 10/15/2025
Second Year Affirmation Expiration Date:
CMMC Status Expiration Date: 10/15/2025

Submission of this assessment result [REDACTED] or affirmation indicates that NICOLE SMITH, 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)

Historical Assessment Details

VIEW/EXPAND AFFIRMATION CONTACT(S) AND HISTORY

VIEW/EXPAND REMOVED CAGE(S) ASSOCIATED TO UID

Contact SPRS Customer Support: sprs-helpdesk@us.navy.mil

SUPPLIER PERFORMANCE RISK SYSTEM (SPRS) Monday, May 5, 2025
Version: 4.0.0, Build Date: 02/28/2025

CMMC Affirmation Schedule



❖ *After affirming, click on **Details** to see annual affirmation schedule for this UID*

Company Hierarchy

Overview

NIST SP 800-171 Assessment

CMMC Level 1 (Self)

CMMC Level 2 (Self)

CMMC Level 3 (Self)

Report Generated: 05/05/2025 10:25:38 ET

Edit	CMMC Unique Identifier (UID)	
		Details
		Details
		Details
		Details
		Details
		Details
		Details
		Details
		Details
		Details
		Details

CMMC Level 2 Self-Assessment

Report Generated: 05/05/2025 10:25:38 ET

Save As PDF

Current Assessment Details

Assessment Standard: NIST SP 800-171 Rev 2

Assessment Type: CMMC Level 2 Self-Assessment

CMMC Unique Identifier (UID):

CMMC Status Type: CMMC L2 Final Self-Assessment

Score: 110

Assessment Date: 04/30/2025

Company Size: 100

Assessing Scope: ENCLAVE

CAGE(s) in Scope: ZSPA4

Initial Affirmation Expiration Date: 04/30/2026

Second Year Affirmation Expiration Date: 04/30/2027

CMMC Status Expiration Date: 04/30/2028

VIEW/EXPAND ASSESSMENT RESULTS

VIEW/EXPAND CAGE(S) IN SCOPE DETAILS

Historical Assessment Details

VIEW/EXPAND AFFIRMATION CONTACT(S) AND HISTORY

Initial Affirmation:

Affirmation Date: 04/30/2025

Affirming Official: BELINDA

Title: NULL

Email: BELINDA

Additional Email(s): BELINDA.C.LAB

Second Year Affirmation:

Due Date: 04/30/2026

Affirmation Date:

Affirming Official:

Title:

Email:

Additional Email:

Third Year Affirmation:

Due Date: 04/30/2027

Affirmation Date:

Affirming Official:

Title:

Email:

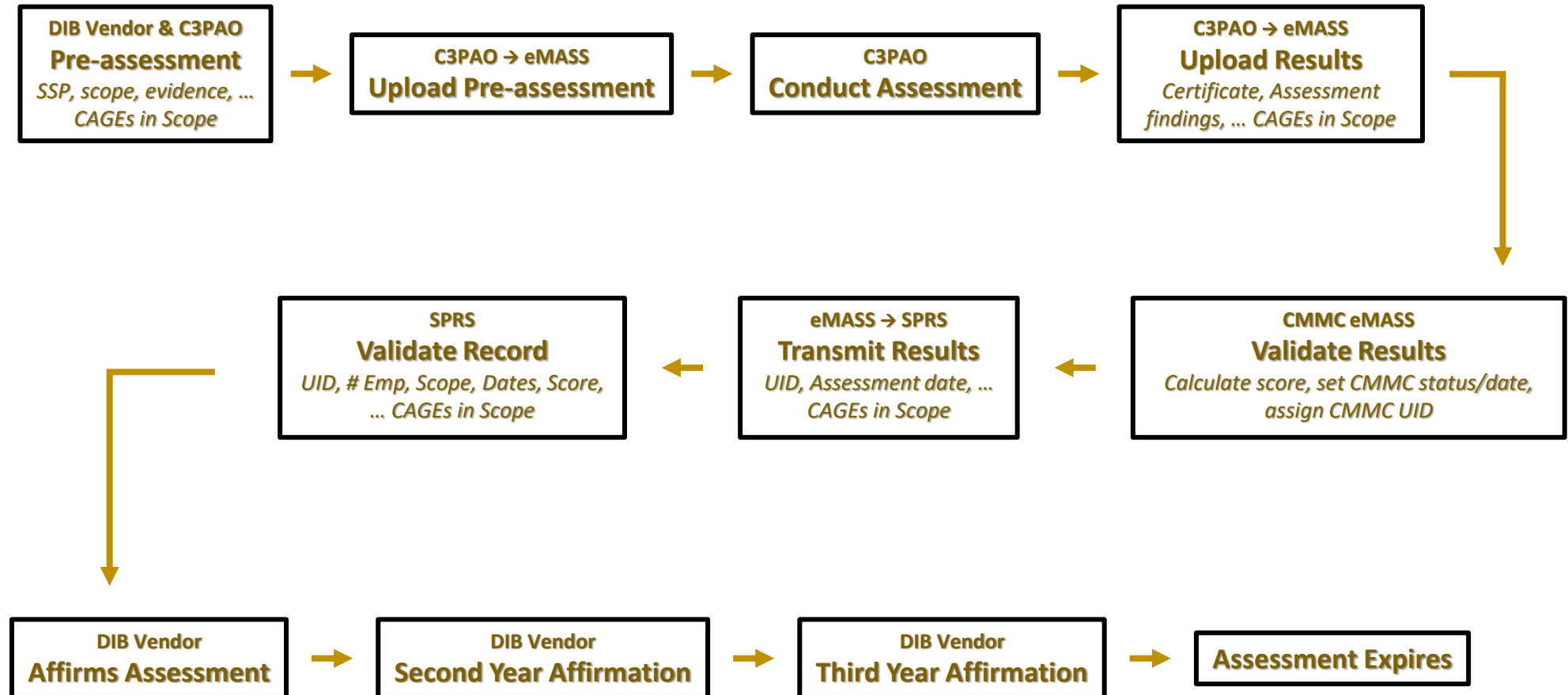
Additional Email:

VIEW/EXPAND REMOVED CAGE(S) ASSOCIATED TO UID

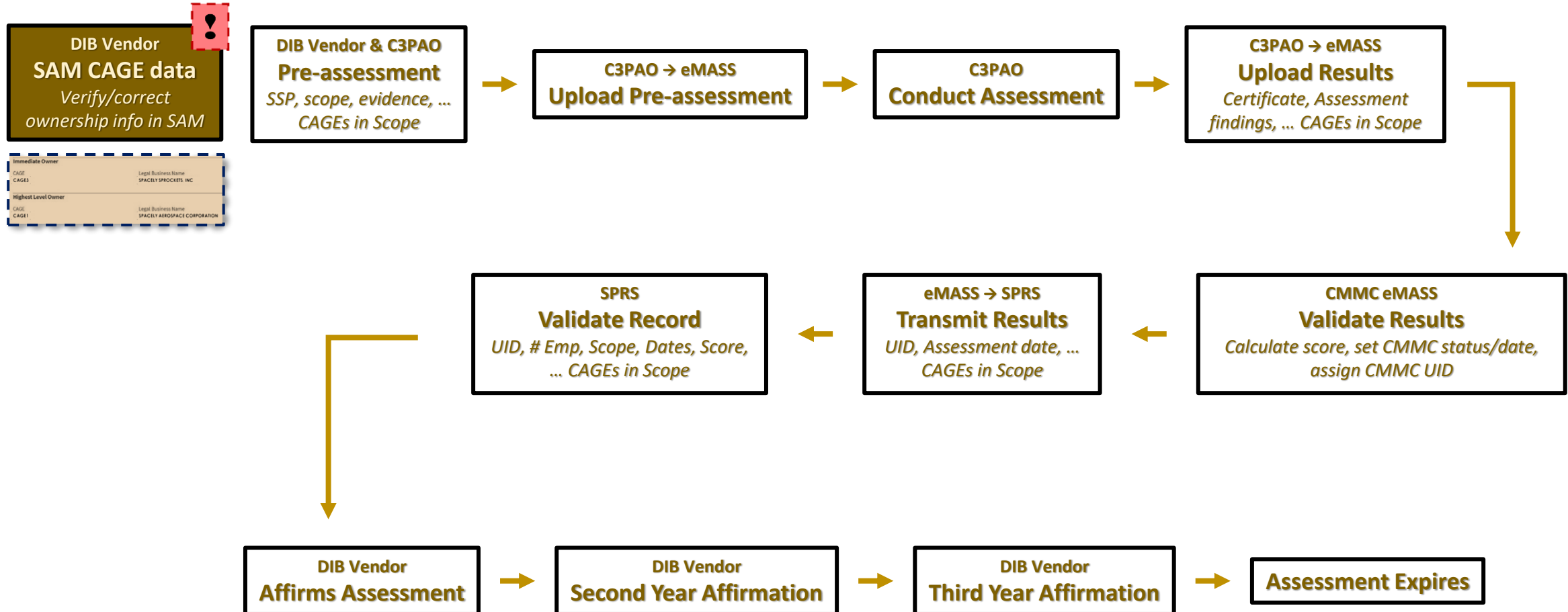
Affirmation history and milestones

Assessment Scope			Company Size	Cancel/Delete
ENTERPRISE	ZSP05	ZSP05	25	
ENCLAVE	ZSPA4	ZSPA4	100	X
ENCLAVE	ZSPA3		255	
ENCLAVE	ZSPA5, ZSPA6		100	
ENCLAVE	ZSP04	ZSP04	100	X
ENTERPRISE	ZSP01, ZSP02, ZSP03, ZSP04, ZSP05		6	
ENCLAVE	ZSP03	ZSP03	42	X
ENCLAVE	ZSPA2, ZSPA3, ZSPA5, ZSPA6	ZSPA2(ZSPA4), ZSPA3(ZSPA4), ZSPA5, ZSPA6	255	X
ENCLAVE	ZSP03		22	
ENCLAVE	ZSP03	ZSP03	255	X
ENTERPRISE	ZSP01	ZSP01	0	X

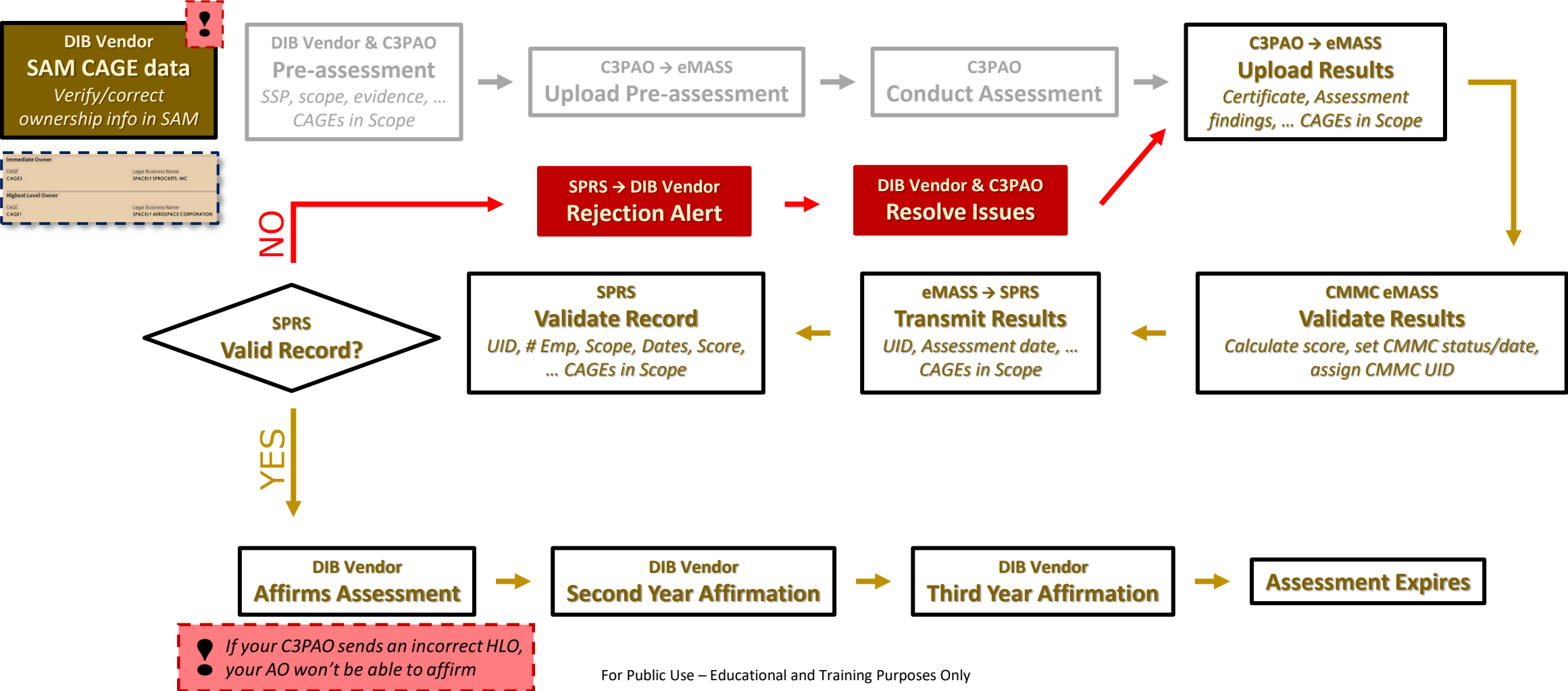
C3PAO CMMC Assessment Flow (notional)



CMMC Assessment Flow help



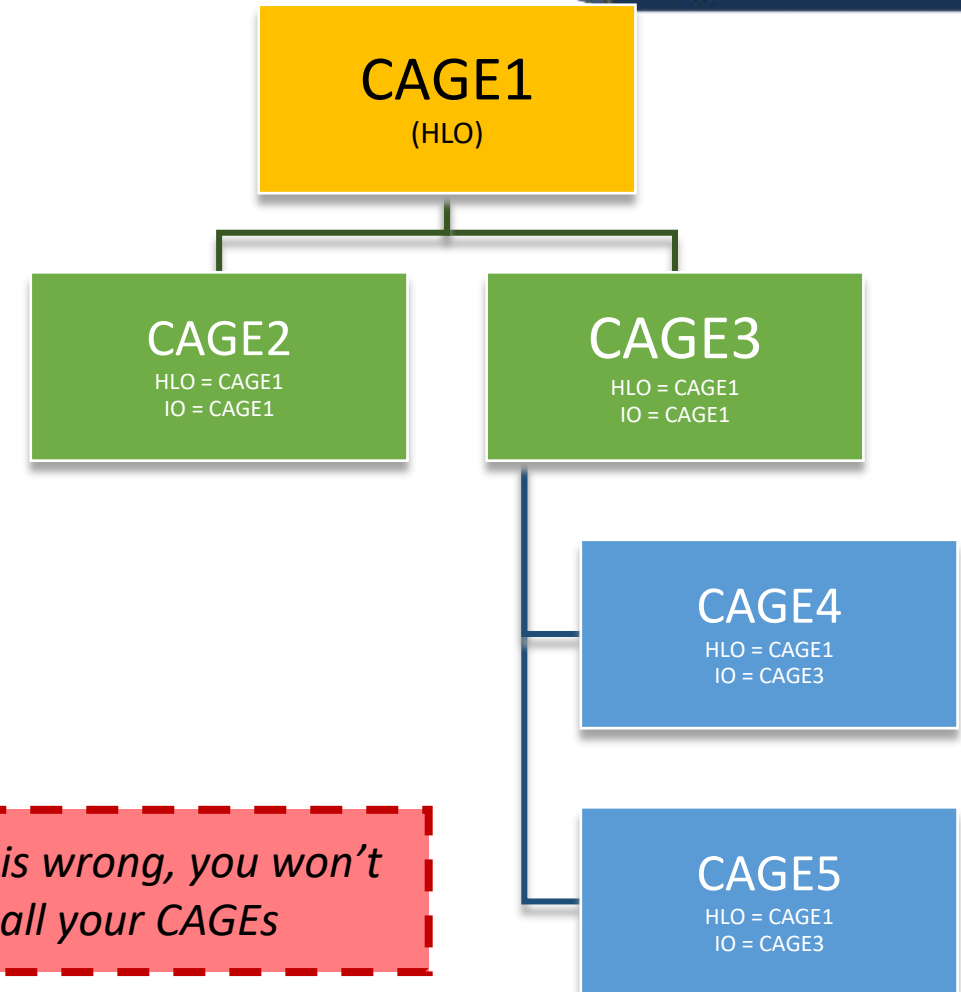
CMMC Assessment Flow (notional)



CMMC/NIST – CAGE Hierarchy



- ❖ **CAGE hierarchy data comes from SAM**
 - ❖ CAGE hierarchy must be correct in SAM
- ❖ **Top CAGE = Highest Level Owner (HLO)**
 - ❖ You should only have one
 - ❖ Every CAGE record should show the same HLO
- ❖ **Division CAGE = Immediate Owner (IO)**
 - ❖ Every lower CAGE must show HLO and IO
- ❖ **Each SAM entry should show a CAGE's HLO and IO**



💡 If your hierarchy is wrong, you won't be able to select all your CAGEs

CMMC/NIST – Fixing Hierarchy



Step 1: SAM
**Vendor fixes
HLO & IO(s)**



CAGE.dla.mil
[automatically updated]

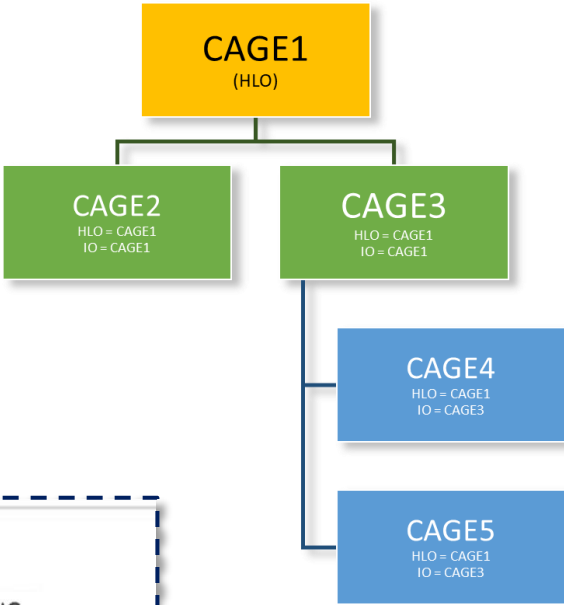


Step 2: SPRS
Vendor checks hierarchy

BUSINESS INFORMATION		(SAM record for CAGE5)
Doing Business As SPACELY GEARWORKS	Division Name SPACELY GEARS DIVISION	
URL http://www.spacelyengineers.com/	Division Number (blank)	
State / Country of Incorporation Delaware, United States	Congressional District Maryland 04	
Registration Dates		
Activation Date Jun 23, 2021	Initial Registration Date Jan 25, 2002	
Submission Date Jun 23, 2021		
Entity Dates		
Entity Start Date Dec 2, 1929	Fiscal Year End Close Date Dec 31	

Immediate Owner	
CAGE CAGE3	
Highest Level Owner	
CAGE CAGE1	

Immediate Owner	
CAGE CAGE3	Legal Business Name SPACELY SPROCKETS, INC
Highest Level Owner	
CAGE CAGE1	Legal Business Name SPACELY AEROSPACE CORPORATION



COMPLIANCE REPORTS
Cyber Reports (CMMC & NIST)
CAGE Hierarchy

💡 If your hierarchy is wrong, you won't be able to select all your CAGEs

Cybersecurity Assessment - Pointers



Q: Why can't I find one of my CAGEs?

A: HLO/IO data (hierarchy) not correct in SAM

Updates in SAM flow to SPRS within hours; vendors can verify hierarchy in SPRS

Q: Why don't I see this buttons? →

Add New CMMC Level 2 Self-Assessment

A: Verify **SPRS Cyber Vendor User** role (you probably don't have one)

Q: Why is my SPRS Cyber Vendor User role still "pending"?

A: Your Contractor Administrator (CAM) needs to approve it

CAMs cannot approve their own roles – may require PIEE help desk assist

Q: Why can't my AO see my UID in SPRS?

A: Your C3PAO sent the wrong HLO with your eMASS record; correct and resend

💡 If your C3PAO sends an incorrect HLO,
your AO won't be able to affirm

SPRS User Roles – PIEE single sign-on



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

❖ **SPRS ACQUISITION PROFESSIONAL**

❖ *Gives access to all scores/reports*

<https://piee.eb.mil>



❖ *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*



Add New CMMC Level 2 Self-Assessment

SPRS Downloads





UNCLASSIFIED

Supplier Performance Risk System



The Supplier Performance Risk System (SPRS) is the authoritative source to retrieve supplier and product PI [performance information] assessments for the DoD [Department of Defense] acquisition community to use in identifying, assessing, and monitoring unclassified performance. ([DoDI 5000.79](#))

Welcome to SPRS v4.1.2

CMMC Level 2 assessments by C3PAOs are now available for affirmation by SPRS Cyber Vendor users.

Home

Logout

COMPLIANCE REPORTS

Cyber Reports (CMMC & NIST)

CAGE Hierarchy

Website and Help

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

SPRS
Guiding the DoD in Responsible Acquisition Decisions

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

Welcome to SPRS

CMMC Level 2 assessments by C3PAOs are now available for affirmation

Latest SPRS News

- April 10, 2025
The SAM Reps and Certs Tab is now re-enabled in EVP for Government Users.
- April 8, 2025
NEW Live [Cyber Reports](#) (Including NIST & CMMC) training now available.
- March 31, 2025
For Vendors, CMMC Level 2 and Level 3 eMASS released into SPRS.
- February 28, 2025
[CMMC Level 2 Quick Entry Guide](#) released.
[CMMC Level 2 Training](#) released.
For Vendors, breadcrumbs released for easier navigation.
- December 20, 2024
CMMC Level 1 Self-Assessment for Vendors now available online. For assistance click here for the [CMMC Quick Entry Guide](#).
- December 3, 2024
New training [SPRS Overview for Contractors](#)

CMMC Level 2 Self-Assessment Tutorial

SPRS
Supplier Performance Risk System
Training

Watch Tutorial

This tutorial goes over entering, editing, and affirming the Cybersecurity Maturity Model Certification (CMMC) Level 2 Self-Assessment within SPRS.

Print PowerPoint | Transcript

Supplier Performance Risk System (SPRS) "...is the authoritative source to retrieve supplier and product PI [performance information] assessments for the DoD [Department of Defense] acquisition community to use in identifying, assessing, and monitoring unclassified performance." (DoDI 5000.79)

For Public Use - Educational and Training Purposes Only

Cyber help

References
User Guides
Quick Reference Guides
PIEE Access Help
Eval Criteria

Training
PPTs
Tutorial videos

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)