



SPRS

Supplier Performance Risk System

CMMC

Entry Tutorial



The purpose of the Cybersecurity Maturity Model Certificate (CMMC) “...is to enforce the protection of sensitive unclassified information shared by the Department with its contractors and subcontractors.

The program provides the DoD with increased assurance that contractors and subcontractors are meeting the cybersecurity requirements for nonfederal systems processing controlled unclassified information (CUI).” (DoD CIO).

SPRS Vendor User Roles

SPRS Cyber Vendor User



- Ensuring the CAGE Hierarchy is accurate
- Managing Cyber Reports Assessment data
- Provide customer feedback

SPRS Contractor/Vendor (Support Role)



- View company reports (including Cyber Reports)
- View CAGE Hierarchy Reports
- View vendor Performance Reports
- Execute Supplier Risk Reports
- Execute Supply Code Relationship Reports
- File data discrepancy Challenges and
- Provide customer feedback

SPRS Vendor User Roles

SPRS Cyber Vendor User



- Ensuring the CAGE Hierarchy is accurate
- Managing Cyber Reports Assessment data
- Provide customer feedback

SPRS Contractor/Vendor (Support Role)



- View company reports (including Cyber Reports)
- View CAGE Hierarchy Reports
- View vendor Performance Reports
- Execute Supplier Risk Reports
- Execute Supply Code Relationship Reports
- File data discrepancy Challenges and
- Provide customer feedback

Note to Viewers

To preserve
detail and
integrity
screenshots
have been
edited for
size & content



Cyber Reports



CYBER SECURITY REPORTS

Company Hierarchy:

An asterisk * indicates the user has the SPRS Cyber Vendor User role for this CAGE

Company Hierarchy:

An asterisk * indicates the user has the SPRS Cyber Vendor User role for this CAGE

Select 1 CAGE

ZSP01* (HLO: ZSP01)

Cyber Reports



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)

Report Generated : 12/02/2024 10:19:30 ET

Edit	CMMC Unique Identifier (UID)	CMMC Status Type	Assessment Date	CMMC Status Expiration Date	Assessment Scope	Included CAGE	Company Size	Delete
		Pending Affirmation	12/02/2024	12/02/2025	ENCLAVE	ZSP01	25	

Details

Cyber Reports



CYBER SECURITY REPORTS

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

Back

Enter CMMC Assessment Details

Assessment Date:

Assessing Scope:

December 2024 < Today >

SU	MO	TU	WE	TH	FR	SA
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	1	2	3	4
5	6	7	8	9	10	11

Confirming Official (AO)

Organization Seeking the CMMC Program with the security

Cyber Reports



CYBER SECURITY REPORTS

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

Back

Enter CMMC Assessment Details

Assessment Date:

Assessing Scope:

How many employees Level 1 self-assessment

Are you compliant with FAR clause 52.204-
 ENCLAVE
 ENTERPRISE

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)

Cyber Reports



CYBER SECURITY REPORTS

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

Back

Enter CMMC Assessment Details

Assessment Date: 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)

Cyber Reports



CYBER SECURITY REPORTS

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

<https://www.ecfr.gov/current/title-48/chapter-1/subchapter-H/part-52/section-52.204-21>

Cyber Reports



CYBER SECURITY REPORTS

COMPANY A1

CAGE Hierarchy

Back

Enter

Assessment Date: MM/DD/YYYY

How many employees are included in Level 1 self-assessment?

Are you compliant with FAR clause 52.201-21?

Included CAGE(s):

Open CAGE Hierarchy

Multiple CAGE codes should be entered.

Assessments are not complete until

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

osd.pentagon.dod-cio.mbx.cmmc-inquiries@mail.mil

Cyber Reports



CYBER SECURITY REPORTS

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

Cyber Reports



CYBER SECURITY REPORTS

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

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 Assessment (OSA) who is responsible for ensuring the OSA's compliance with the CMMC requirements and has the authority to affirm the OSA's continuing compliance with the requirements for their respective organizations. (CMMC-custom term){§170.4}

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):

Cyber Reports



SRNGTST : CMMC Level1 Assessment

Good day,

You have been identified as your company's Affirming Official (AO) by NICOLE SMITH, copied here. There is a CMMC Level 1 Self-Assessment that requires AO affirmation. **This is the only notification you will receive.**

- 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)

Action Required to affirm:

- Log into the DoD Procurement Integrated Enterprise Environment (PIEE): <https://piee.eb.mil/xhtml/unauth/home/login.xhtml> *
- Select SPRS tile*
- Click Cyber Reports in menu
- Click Edit button (pencil icon) for the record in "Pending Affirmation" status
- Review assessment information
- Affirm assessment

Access Information:

*If you do not have a PIEE account, or do not see the SPRS tile after logging into PIEE, refer to these SPRS access instructions, https://www.sprs.csd.disa.mil/pdf/SPRS_Access_NISTSP800-171.pdf

SPRS Resources:

- CMMC Resource: <https://dodcio.defense.gov/cmmc/Resources-Documentation/>
- FAQ's: <https://www.sprs.csd.disa.mil/faqs.htm>

Respectfully,
SPRS Team

Supplier Performance Risk System (SPRS)
<https://www.sprs.csd.disa.mil/>

Reply Reply all Forward

REPORTS

COMPANY A1
ID: ZSP01* (HLO: ZSP01)
Title: Level 1 Self-Assessment
Standard: NIST SP 800-171 Re

C Assessment Details

Scope:

organization for which this C

the security requirements spe

d by a comma

ve been affirmed by the company Affirming Official (AO)

representative from within each Organization Seeking
ensuring the OSA's compliance with the CMMC Program
in the OSA's continuing compliance with the security
ons. (CMMC-custom term)(§170.4)

Continue to Affirmation

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.

Continue to 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):

Transfer to AO

Cancel

Cyber Reports



CYBER SECURITY REPORTS

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

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.

[Continue to 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):

[Transfer to AO](#) [Cancel](#)

CYBER SECURITY REPORTS

COMPANY A1
CAGE Code: ZSP01* (HLO: ZSP01)
Confidence Level: 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: NICOLE
Last Name: SMITH
Title: NULL
Email Address:

Additional Email Address(s):
Multiple emails should be delimited by a comma

[← Previous](#) [Continue to Affirmation](#)

Affirming Official (AO)

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)

Cyber Reports



COMPANY A1
CAGE Code: ZSP01* (HLO: ZSP01)
Confidence Level: Level 1 Self-Assessment

Assessment and Affirmation

Report Generated: 12/10/2024 13:05:42 ET

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

Level 1 CMMC Assessment Date: **12/02/2024**
CMMC Status Expiration Date: **12/02/2025**
Assessing Scope: **ENTERPRISE**
Company Size: **4**

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

Included CAGES/entities:

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

Submission of this assessment result **S100000126** 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.

I certify that I have read the above statement.

Affirm **Cancel**

ponsible for
he security r

Cyber Reports



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:

CMMC Level 1 (Self)

Report Generated : 12/05/2024 10:53:29 ET

Edit	CMMC Unique Identifier (UID)	CMMC Status Type	Assessment Date	CMMC Status Expiration Date	Assessment Scope	Included CAGE	Company Size	Delete
	S <input type="button" value="Details"/>	No CMMC Status	12/05/2024	12/05/2025	ENCLAVE	ZSP01	45	<input type="button" value="Delete"/>
<input type="button" value="Edit"/>	<input type="button" value="Details"/>	Incomplete	12/01/2024	12/01/2025	ENCLAVE	ZSP01		<input type="button" value="Delete"/>
<input type="button" value="Edit"/>	<input type="button" value="Details"/>	Pending Affirmation	12/02/2024	12/02/2025	ENCLAVE	ZSP01	99	<input type="button" value="Delete"/>
	<input type="button" value="Details"/>	Final Level 1 Self-Assessment	12/02/2024	12/02/2025	ENTERPRISE	ZSP01	255	<input type="button" value="Delete"/>
	<input type="button" value="Details"/>	No CMMC Status (Expired Assessment)	12/04/2023	12/04/2024	ENCLAVE	ZSP02	99	<input type="button" value="Delete"/>
	<input type="button" value="Details"/>	Final Level 1 Self-Assessment	12/02/2024	12/02/2025	ENCLAVE	ZSP02	11	<input type="button" value="Delete"/>
	<input type="button" value="Details"/>	Final Level 1 Self-Assessment	12/01/2024	12/01/2025			999	<input type="button" value="Delete"/>

Cyber Reports



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:

CMMC Level 1 (Self)

Report Generated : 12/05/2024 10:53:29 ET

Edit	CMMC Unique Identifier (UID)	CMMC Status Type	Assessment Date	CMMC Status Expiration Date	Assessment Scope	Included CAGE	Company Size	Delete
	S	No CMMC Status	12/05/2024	12/05/2025	ENCLAVE	ZSP01	45	
	<input type="button" value="Details"/>	Incomplete	12/01/2024	12/01/2025	ENCLAVE	ZSP01		
	<input type="button" value="Details"/>	Pending Affirmation	12/02/2024	12/02/2025	ENCLAVE	ZSP01	99	
	<input type="button" value="Details"/>	Final Level 1 Self-Assessment	12/02/2024	12/02/2025	ENTERPRISE	ZSP01	255	
	<input type="button" value="Details"/>	No CMMC Status (Expired Assessment)	12/04/2023	12/04/2024	ENCLAVE	ZSP02	99	
	<input type="button" value="Details"/>	Final Level 1 Self-Assessment	12/02/2024	12/02/2025	ENCLAVE	ZSP02	11	
	<input type="button" value="Details"/>	Final Level 1 Self-Assessment	12/01/2024	12/01/2025			999	

Cyber Reports



CASE CODE: ZSP01 (REG: ZSP01)

Overview

CMMC Level 1 Self-Assessment

*** WARNING: Confirm Delete Of Below Assessment ***

Report Generated: 12/10/2024 13:09:10 ET

Save As PDF

CMMC Status Type: **Final Level 1 Self-Assessment**
CMMC Unique Identifier (UID): S100000126

Level 1 CMMC Assessment Date: 12/02/2024
CMMC Status Expiration Date: 12/02/2025
Assessing Scope: **ENTERPRISE**
Company Size: **4**

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

Included CAGES/entities:

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

Confirm Delete

Assessment Scope	Included CAGE	Company Size	Delete
No CMMC Status	ZSP01	45	
Incomplete	ZSP01	99	
Pending Affirmation	ZSP01	99	
Final Level 1 Self-Assessment	ZSP01	255	
No CMMC Status (Expired Assessment)	ZSP02	99	
Final Level 1 Self-Assessment	ZSP02	11	
Final Level 1 Self-Assessment	ZSP02	999	

Cyber Reports



Back

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

Report Generated: 12/10/2024 13:09:10 ET

Save As PDF

CMMC Level 1 Self-Assessment

Report Generated: 12/10/2024 13:09:10 ET

CMMC Status Type: **Final Level 1 Self-Assessment**
CMMC Unique Identifier (UID): S100000126

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

Level 1 CMMC Assessment Date: 12/02/2024
CMMC Status Expiration Date: 12/02/2025
Assessing Scope: ENTERPRISE
Company Size: 4

Included CAGES/entities:

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

Report Generated: 12/10/2024 13:09:10 ET

Edit	CMMC Unique Identifier (UID)	CMMC Status Type	Assessment Date	Assessment Expiration Date	Assessing Scope	Company Size	Assessment Date	Assessment Expiration Date	Assessing Scope	Company Size
	S100000126	No CMMC Status	12/05/2024							
		Incomplete	12/01/2024	12/01/2025	ENCLAVE	ZSP01				
		Pending Affirmation	12/02/2024	12/02/2025	ENCLAVE	ZSP01	99			
		Final Level 1 Self-Assessment	12/02/2024	12/02/2025	ENTERPRISE	ZSP01	255			
		No CMMC Status (Expired Assessment)	12/04/2023	12/04/2024	ENCLAVE	ZSP02	99			
		Final Level 1 Self-Assessment	12/02/2024	12/02/2025	ENCLAVE	ZSP02	11			
		Final Level 1 Self-Assessment	12/01/2024	12/01/2025			999			

Cyber Reports



CMMC Level 1 (Self)

Report Generated : 12/05/2024 10:53:29 ET

Edit	CMMC Unique Ident	CMMC Status Type	Assessment Date	CMMC Status Expiration	Assessment Scope	Included CAGE	Company Size	Delete
			2024	12/05/2025	ENCLAVE	ZSP01	45	
			2024	12/01/2025	ENCLAVE	ZSP01		

Sort Ascending
Sort Descending
Columns
Filter

The assessment expiration date; a Level 1 self-assessment is considered valid for one year.

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

Cyber Reports



CYBER SECURITY REPORTS

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

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

Hierarchy data is managed by the company Electronic Business Point of Contact (EBPOC) in [SAM.gov](#). CAGE Hierarchy information flows from SAM to SPRS.

Level 1	Level 2	Company Name	Company Location
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

Sam.gov/content/home

Cyber Reports



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

Basic | Medium | High Virtual | High On-Site

Report Generated : 11/12/2024 07:47:28 ET

Edit/ Delete	DoD Unique Identifier (UID)	Included CAGE	Company Name	Assessment Date	Score	Assessment Scope	Plan Of Action Completion Date	Syst Plan Ass
<input type="checkbox"/>	SB00026481 <input type="button" value="Details"/>	ZSP02	COMPANY A2	10/03/2024	89	ENTERPRISE	10/03/2025	BETA
<input type="checkbox"/>	SB00025940 <input type="button" value="Details"/>	ZSP01	COMPANY A1	12/03/2023	109	ENTERPRISE	12/30/2023	12/30
<input type="checkbox"/>	SB00025940 <input type="button" value="Details"/>	ZSP04	COMPANY A4	12/03/2023	109	ENTERPRISE	12/30/2023	12/30
<input type="checkbox"/>	SB00025940 <input type="button" value="Details"/>	ZSP03	COMPANY A3	12/03/2023	109	ENTERPRISE	12/30/2023	12/30
<input type="checkbox"/>	SB00025940 <input type="button" value="Details"/>	ZSP02	COMPANY A2	12/03/2023	109	ENTERPRISE	12/30/2023	12/30

1 2 3 items per page

CYBER SECURITY REPORTS

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

Enter Assessment Details

Assessment Date:

Assessment Score:

Assessing Scope:

Plan of Action Completion Date:

System Security Plan (SSP) Assessed:

SSP Version/Revision:

SSP Date:

Included CAGE(s):

Cyber Reports



CYBER SECURITY REPORTS

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

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

DoD Unique Identifier:

Included CAGE:

Multiple CAGE codes should be delimited by a comma

Company Name:

Assessment Score:
Min Max

Assessment Date:
Choose start date... Choose end date...

CYBER SECURITY REPORTS

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

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

Basic | Medium | High Virtual | High On-Site | **Level 1 Self Assessments**

Report Generated : 11/12/2024 07:36:44 ET

Edit/ Delete	CMMC Unique Identifier (UID)	CMMC Status Type	Assessment Date	CMMC Status Expiration Date	Assessment Scope	Included CAGE	Company Size
<input type="button" value="Details"/>		No CMMC Status (Expired)	10/01/2022	10/01/2023	ENTERPRISE	ZSP01	42

1 - 1 of 1 items

Cyber Reports



CYBER SECURITY REPORTS

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

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

GENERAL GUIDANCE

- Resource material, tutorials, and guidance are available on the [SPRS website](#). Click the SPRS icon at the top of the menu bar.
 - SPRS [Frequently Asked Questions](#)
- Highest-level owner (HLO) - The entity that owns or controls an immediate owner of the offeror, or that owns or controls one or more entities that control an immediate owner of the offeror. No entity owns or exercises control of the highest level owner. For additional information view [FAR 52.204-17](#) Ownership or Control of Offeror.
- Asterisk (*) - An Asterisk displayed next to the CAGE indicates that the user has a "SPRS Cyber Vendor User" role for that CAGE in the Procurement Integrated Enterprise Environment (PIEE). If there is no asterisk then the user role type is "Contractor/Vendor" (view-only access to the CAGE and associated subsidiaries).
- A "SPRS Cyber Vendor User" role is a privileged role that provides access to the entire company hierarchy and is required for entering and editing Cyber Assessment results in SPRS.

CMMC INFORMATION

- Security requirements specified in FAR clause 52.204-21 can be found at <https://www.ecfr.gov/current/title-48/chapter-1/subchapter-H/part-52/section-52.204-21>
- Supplemental guidance in the CMMC Level 1 Assessment Guide and CMMC Level 1 Scoping guide located at <https://dodcio.defense.gov/CMMC/Documentation/>
- Questions related to technical interpretation of these CMMC Level 1 supplemental guidance documents may be directed to osd.pentagon.dod-cio.mbx.cmmc-inquiries@mail.mil. Do not submit questions requesting interpretation or modification of NIST source documents, which are outside the CMMC Program's purview.

NIST SP 800-171 INFORMATION

- SPRS is the database that holds NIST SP 800-171 assessment summary information. SPRS resources:
 - [NIST SP 800-171 Information](#)
 - [NIST SP 800-171 Quick Entry Guide](#)
 - [SPRS Access for NIST SP 800-171 Assessment Entry](#)
- Preparation information including the NIST 800-171 Assessment Methodology can be found at the Defense Pricing and Contracting (DPC) Cyber page [here](#).

Cyber Reports



Print
Total: 2 sheets of paper

Printer: Adobe PDF

Copies: 1

Layout: Portrait

Pages: All

Color: Color

Print Cancel

UNCLASSIFIED

Welcome: NICCICYBERVEND_LASTNAME (NSLCSPRS)
Last Login: November 12, 2024 07:30:24 ET

Home
Logout

COMPLIANCE REPORTS

Cyber Reports (NIST)

CAGE Hierarchy

RISK ANALYSIS REPORTS

Supplier Risk

PERFORMANCE REPORTS

Summary Report

Detail Pos/Neg Records

Supply Code Relationship

SERVICE

Feedback/Customer Support

Download

Home Notification Upload Print Help Menu

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

Level 1 Self-Assessments

Report Generated : 11/12/2024 07:53:24 ET

Delete	CMMC Unique Identifier (UID)	CMMC Status Type	As De
	L100000102 Details	No CMMC Status (Expired)	10.
	L100000101 Details	Final L1 Self-Assessment	09.

Assessment Scope	Included CAGE	Company Size
ENTERPRISE	ZSP01	42
ENCLAVE	ZSP04	1
ENCLAVE	ZSP04	25
ENCLAVE	ZSP05	25
ENCLAVE	ZSP03	42

1 - 5 of 8 items

Cyber Reports



SPRS
Guiding the DoD in Responsible Acquisition Decisions

Menu

- Login/Register (via PIEE)
- NIST SP 800-171 Vendor Help posting Basic Assessments
- NIST SP 800-171 Information
- Vendor Threat Mitigation
- Enhanced Vendor Profile
- SPRS Reports

Reps & Certs information is temporarily unavailable, refer to SAM.gov for up to date information.

CONTRACTING OFFICIALS: ITEM/PRICE RISK FOR SERVICES

For help searching price risk for a service, view our new tutorial.
This tutorial shows how to run an Item/Price Risk Report for a Service PSC.

Automated Learning | Print Presentation | Transcript

WELCOME

Supplier Performance Risk System (SPRS) "...is the authoritative source to retrieve supplier and product PI (performance information) assessments for (Department of Defense) acquisition community to use in identifying...

Assessment Scope	Included CAGE	Company Size
ENTERPRISE	ZSP01	42
ENCLAVE	ZSP04	1
ENCLAVE	ZSP04	25
ENCLAVE	ZSP05	25
ENCLAVE	ZSP03	42

1 - 5 of 8 Items

SPRS Contact Information

SPRS Website:

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

NSLC Help Desk (Mon-Fri 6:30am- 6:00pm ET):

NSLC Help Desk Email:

sprs-helpdesk@us.navy.mil

SPRS Contact Information

SPRS Website:

Home

Logout

COMPLIANCE REPORTS

Cyber Reports

CAGE Hierarchy

SERVICE

Feedback/Customer Support

Download

FEEDBACK/CUSTOMER SUPPORT

New Feedback

ID	Date Modified	First Name	Last Name	Phone Number	Email	CAGE Code	Category
View Details - 609	01/25/2024	CYBER VENDOR USER	TRAINING	5555555555	TESTUSER@TESTING.COM	ZSP01	Cyber Repo

1 items per page 1 - 1 of 1 items

Thank you

for participating in the
CMMC
Entry Tutorial