SPRS

Supplier Performance Risk System

CMMC Level 2 Entry Tutorial

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

https://piee.eb.mil/

SPRS Vendor User Roles

SPRS Cyber Vendor User

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

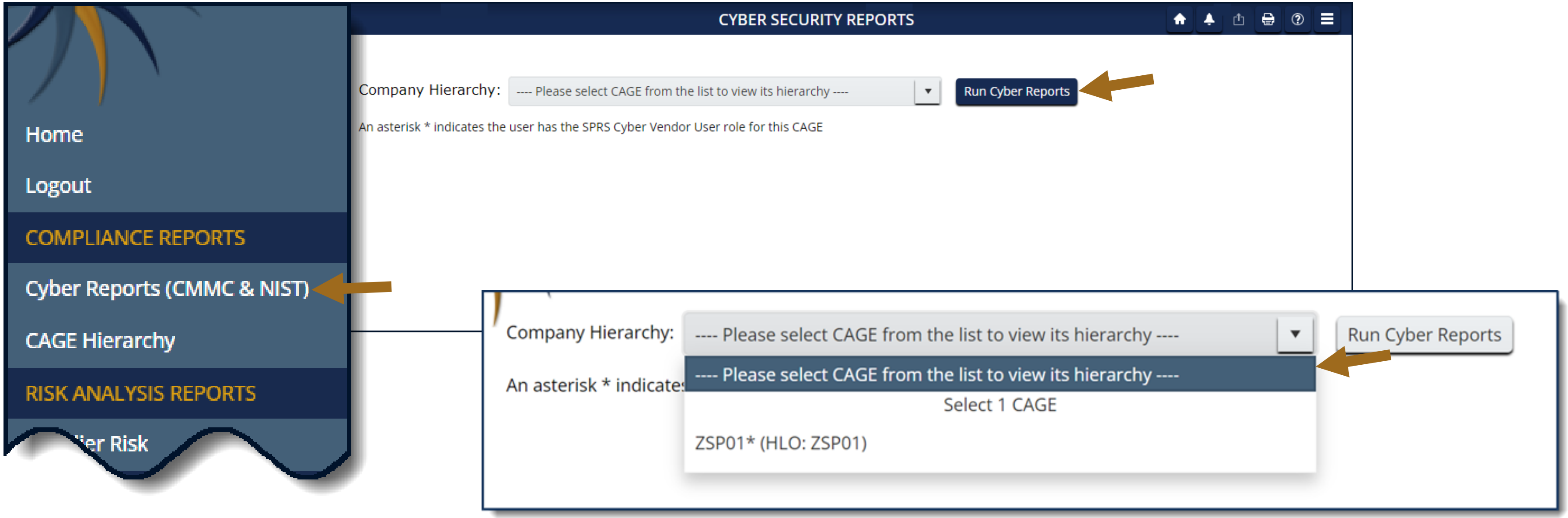
SPRS Contractor/Vendor (Support Role)

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



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

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

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

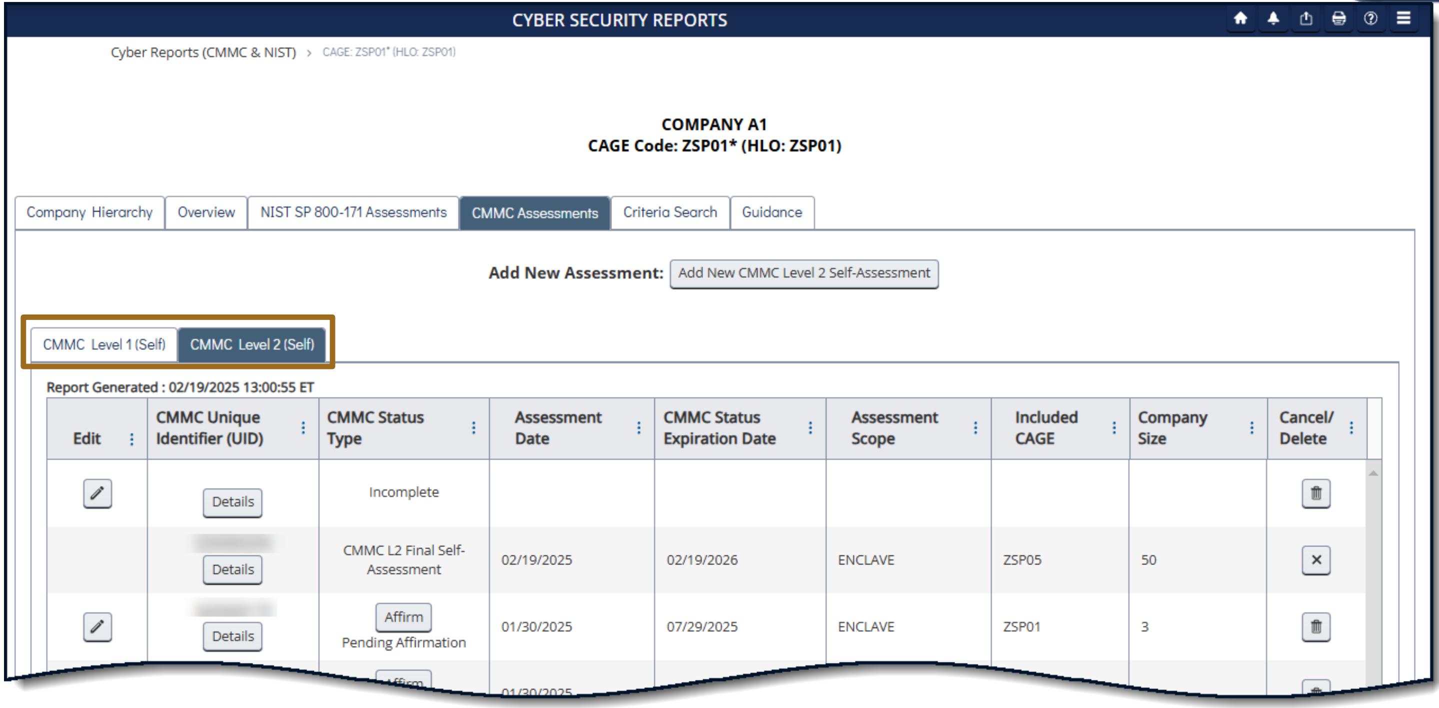
---- Please select CAGE from the list to view its hierarchy ----

Select 1 CAGE

ZSP01* (HLO: ZSP01)

An asterisk * indicates

Cyber Reports



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

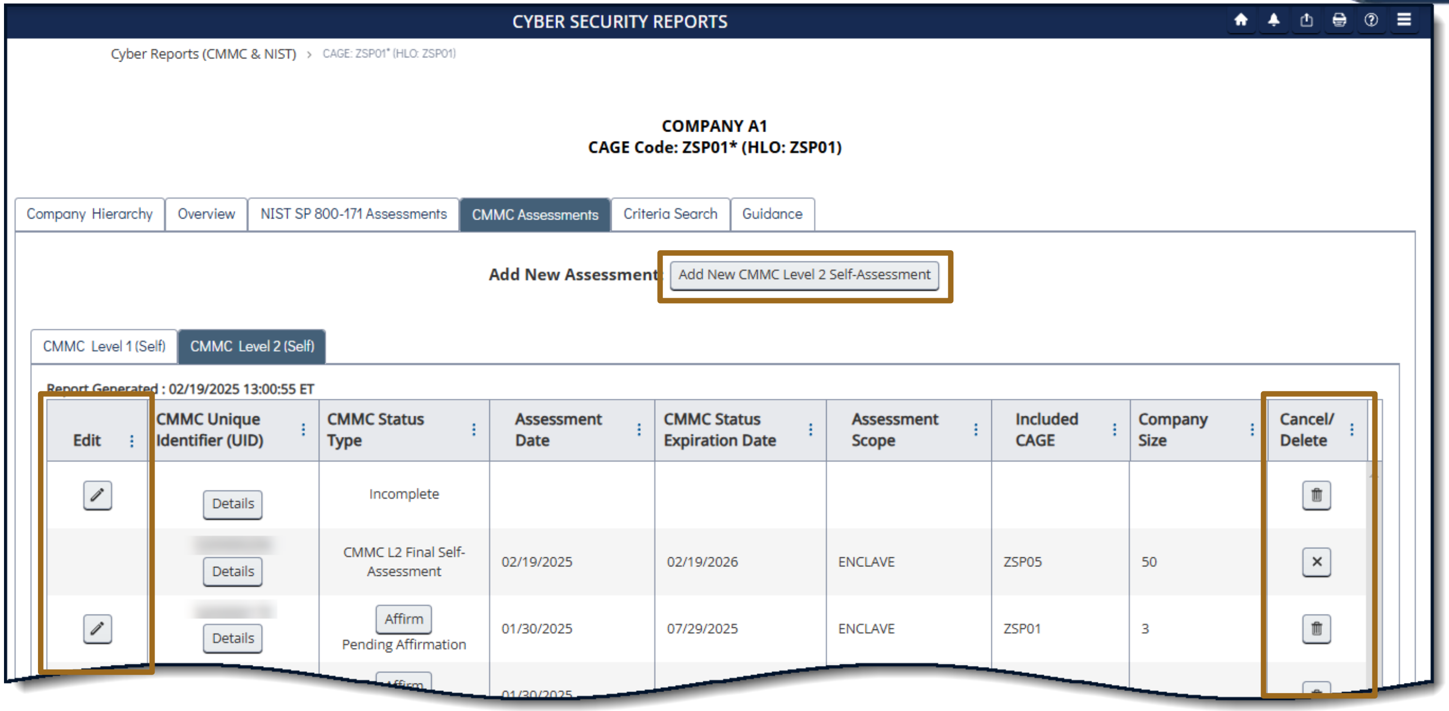
Add New Assessment: Add New CMMC Level 2 Self-Assessment

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

Report Generated : 02/19/2025 13:00:55 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						🗑
	[redacted] Details	CMMC L2 Final Self-Assessment	02/19/2025	02/19/2026	ENCLAVE	ZSP05	50	✕
✎	[redacted] Details	Affirm Pending Affirmation	01/30/2025	07/29/2025	ENCLAVE	ZSP01	3	🗑
		Affirm	01/30/2025					🗑

Cyber Reports



CYBER SECURITY REPORTS

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

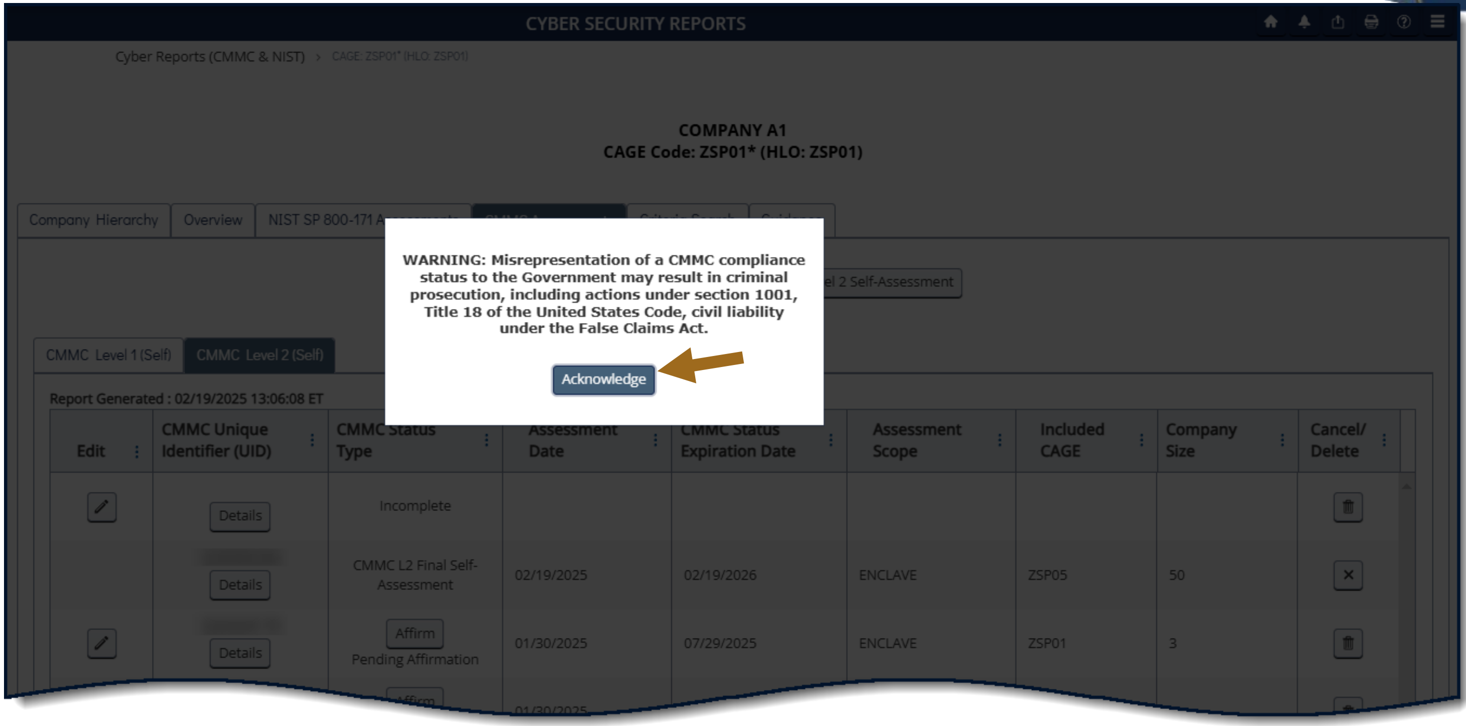
COMPANY A1
CAGE Code: ZSP01* (HLO: ZSP01)

Add New Assessment Add New CMMC Level 2 Self-Assessment

Report Generated : 02/19/2025 13:00:55 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						🗑
	[redacted] Details	CMMC L2 Final Self-Assessment	02/19/2025	02/19/2026	ENCLAVE	ZSP05	50	✕
✎	[redacted] Details	Affirm Pending Affirmation	01/30/2025	07/29/2025	ENCLAVE	ZSP01	3	🗑
		Affirm	01/30/2025					🗑

Cyber Reports



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

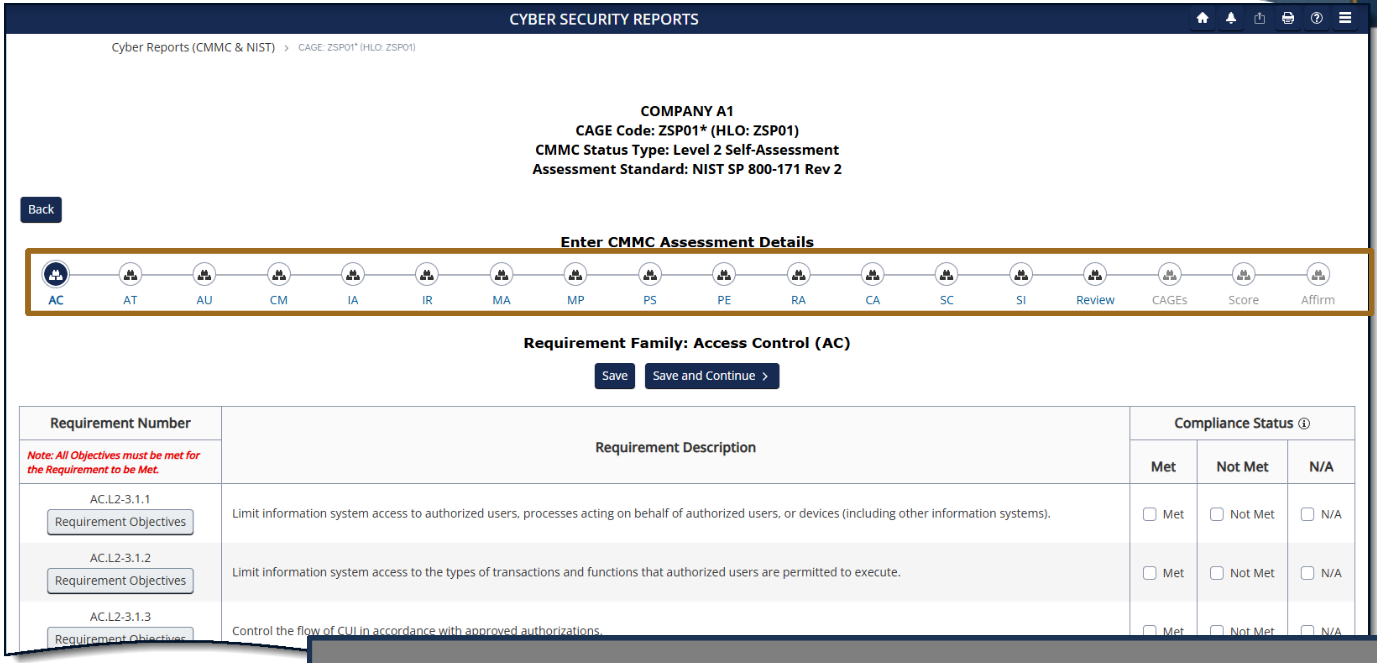
WARNING: Misrepresentation of a CMMC compliance status to the Government may result in criminal prosecution, including actions under section 1001, Title 18 of the United States Code, civil liability under the False Claims Act.

Acknowledge

Report Generated : 02/19/2025 13:06:08 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						🗑
	[redacted] Details	CMMC L2 Final Self-Assessment	02/19/2025	02/19/2026	ENCLAVE	ZSP05	50	✕
✎	[redacted] Details	Affirm Pending Affirmation	01/30/2025	07/29/2025	ENCLAVE	ZSP01	3	🗑

Cyber 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

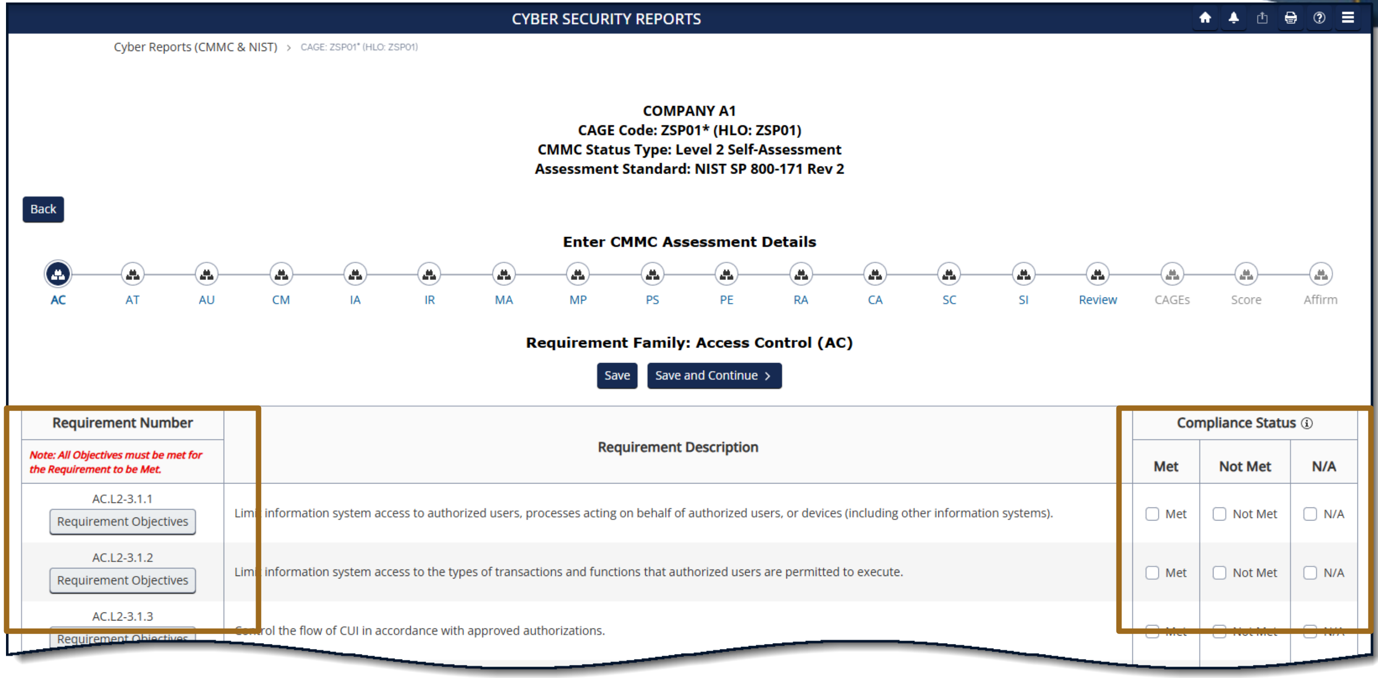
Enter CMMC Assessment Details

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 Requirement Objectives	Control the flow of CUI in accordance with approved authorizations.	☐ Met	☐ Not Met	☐ N/A

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

Cyber Reports



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

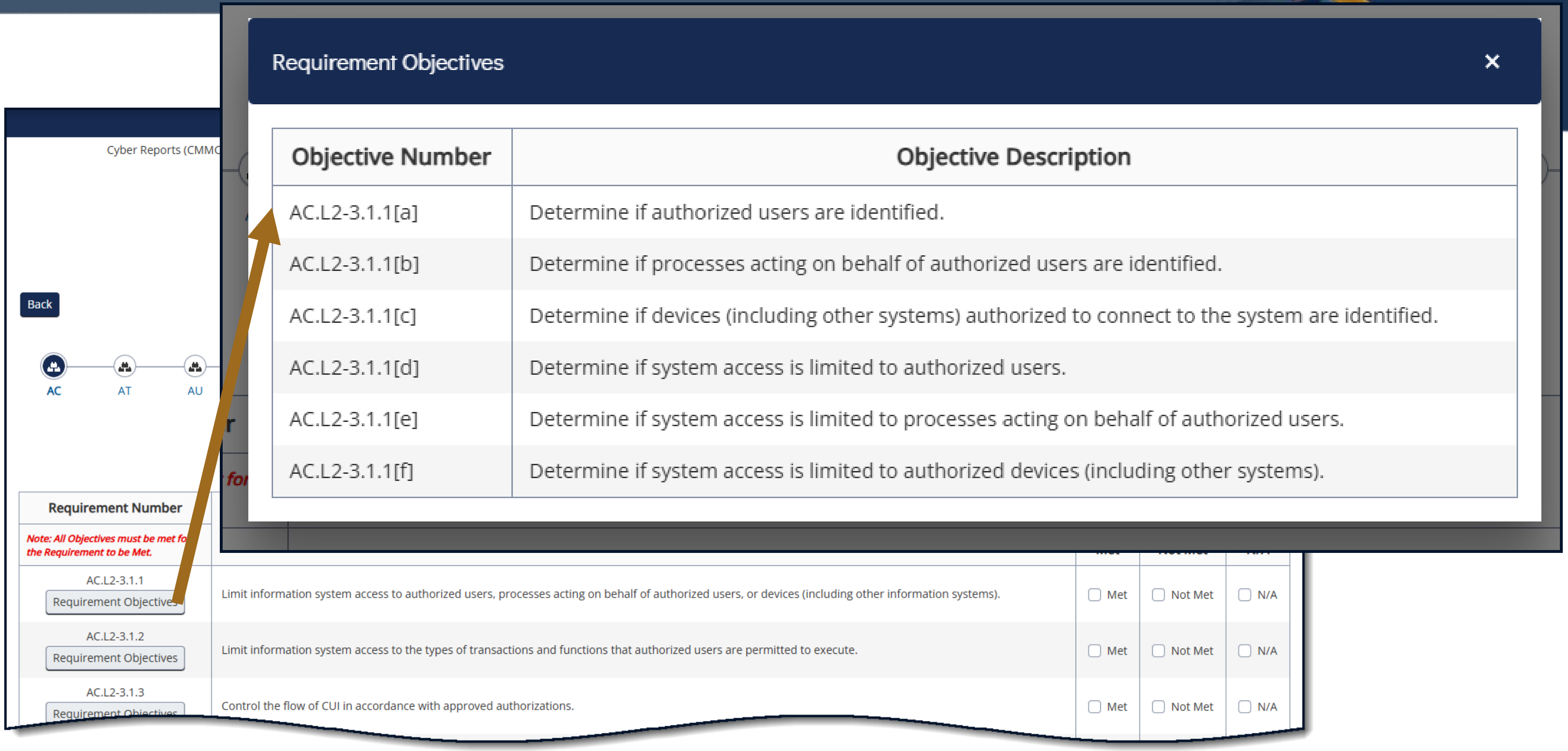
AC · AT · AU · CM · IA · IR · MA · MP · PS · PE · RA · CA · SC · SI · Review · CAGEs · Score · Affirm

Requirement Family: Access Control (AC)

Save | Save and Continue ›

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 Requirement Objectives	Control the flow of CUI in accordance with approved authorizations.	□ Met	□ Not Met	□ N/A

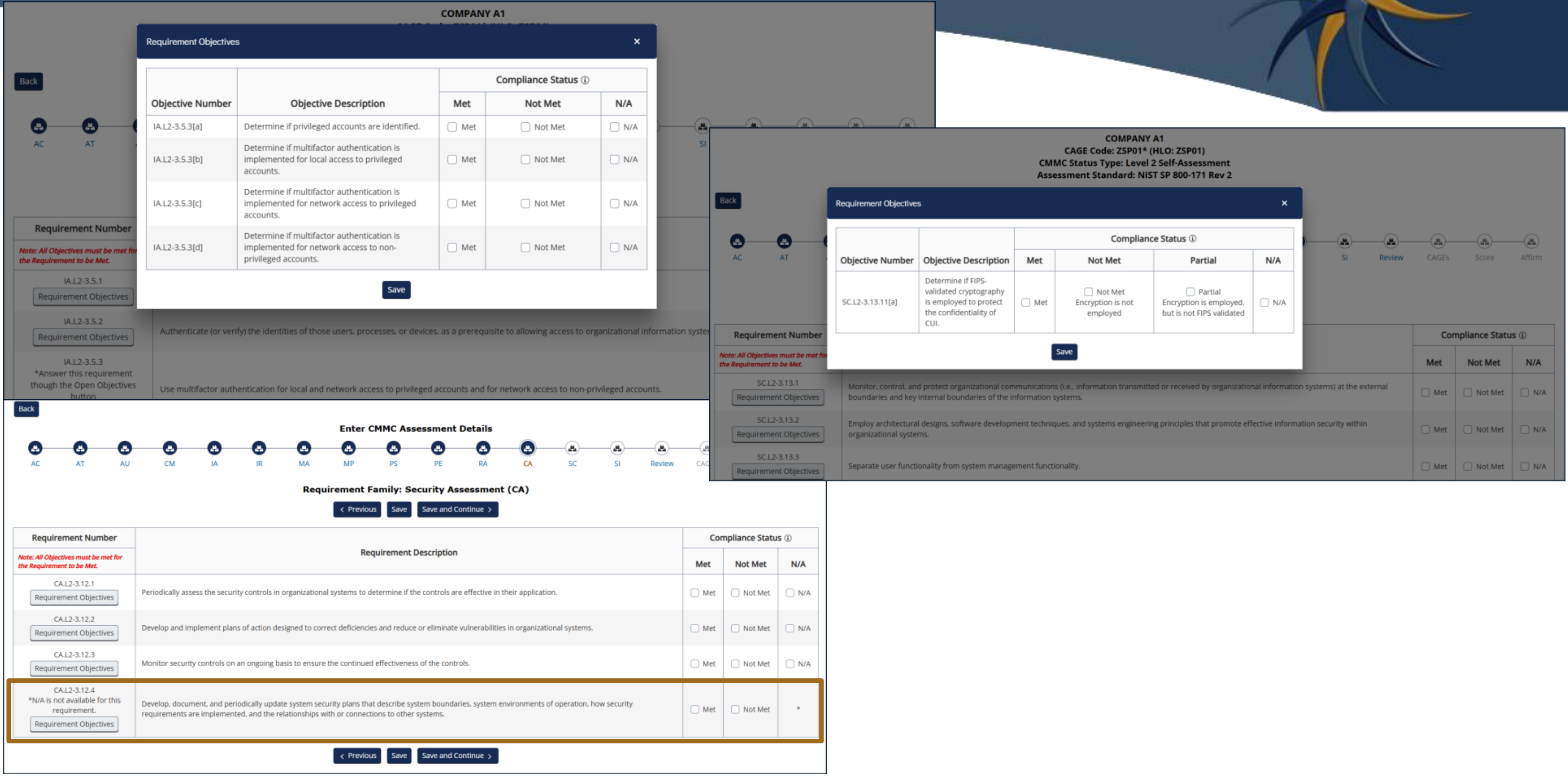
Cyber Reports



Objective Number	Objective Description
AC.L2-3.1.1[a]	Determine if authorized users are identified.
AC.L2-3.1.1[b]	Determine if processes acting on behalf of authorized users are identified.
AC.L2-3.1.1[c]	Determine if devices (including other systems) authorized to connect to the system are identified.
AC.L2-3.1.1[d]	Determine if system access is limited to authorized users.
AC.L2-3.1.1[e]	Determine if system access is limited to processes acting on behalf of authorized users.
AC.L2-3.1.1[f]	Determine if system access is limited to authorized devices (including other systems).

Requirement Number				
Note: All Objectives must be met fo the Requirement to be Met.				
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 Requirement Objectives	Control the flow of CUI in accordance with approved authorizations.	□ Met	□ Not Met	□ N/A

Cyber Reports



COMPANY A1

Back

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

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	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information syste
IA.L2-3.5.3 *Answer this requirement though the Open Objectives button	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.

COMPANY A1

CAGE Code: ZSP01* (HLO: ZSP01)

CMMC Status Type: Level 2 Self-Assessment

Assessment Standard: NIST SP 800-171 Rev 2

Back

Requirement Objectives ×

Objective Number	Objective Description	Compliance Status ⓘ			
		Met	Not Met	Partial	N/A
SC.L2-3.13.11[a]	Determine if FIPS-validated cryptography is employed to protect the confidentiality of CUI.	□ Met	□ Not Met Encryption is not employed	□ Partial Encryption is employed, but is not FIPS validated	□ N/A

Save

Requirement Number		Compliance Status ⓘ		
Note: All Objectives must be met for the Requirement to be Met.		Met	Not Met	N/A
SC.L2-3.13.1 Requirement Objectives	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	□ Met	□ Not Met	□ N/A
SC.L2-3.13.2 Requirement Objectives	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	□ Met	□ Not Met	□ N/A
SC.L2-3.13.3 Requirement Objectives	Separate user functionality from system management functionality.	□ Met	□ Not Met	□ N/A

Back

Enter CMMC Assessment Details

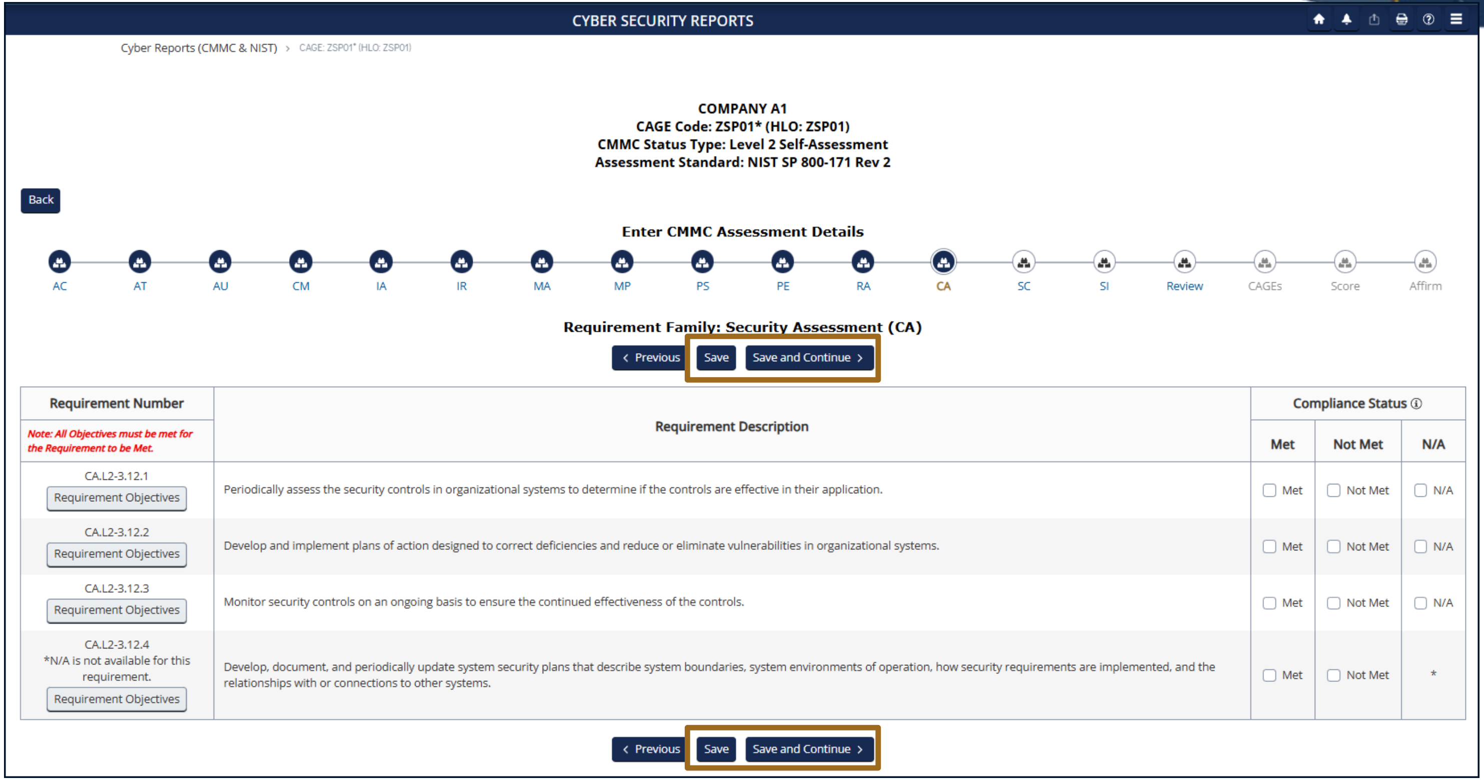
Requirement Family: Security Assessment (CA)

‹ Previous | Save | Save and Continue ›

Requirement Number	Requirement Description	Compliance Status ⓘ		
Note: All Objectives must be met for the Requirement to be Met.		Met	Not Met	N/A
CA.L2-3.12.1 Requirement Objectives	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.	□ Met	□ Not Met	□ N/A
CA.L2-3.12.2 Requirement Objectives	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	□ Met	□ Not Met	□ N/A
CA.L2-3.12.3 Requirement Objectives	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	□ Met	□ Not Met	□ N/A
CA.L2-3.12.4 *N/A is not available for this requirement. Requirement Objectives	Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.	□ Met	□ Not Met	*

‹ Previous | Save | Save and Continue ›

Cyber Reports



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

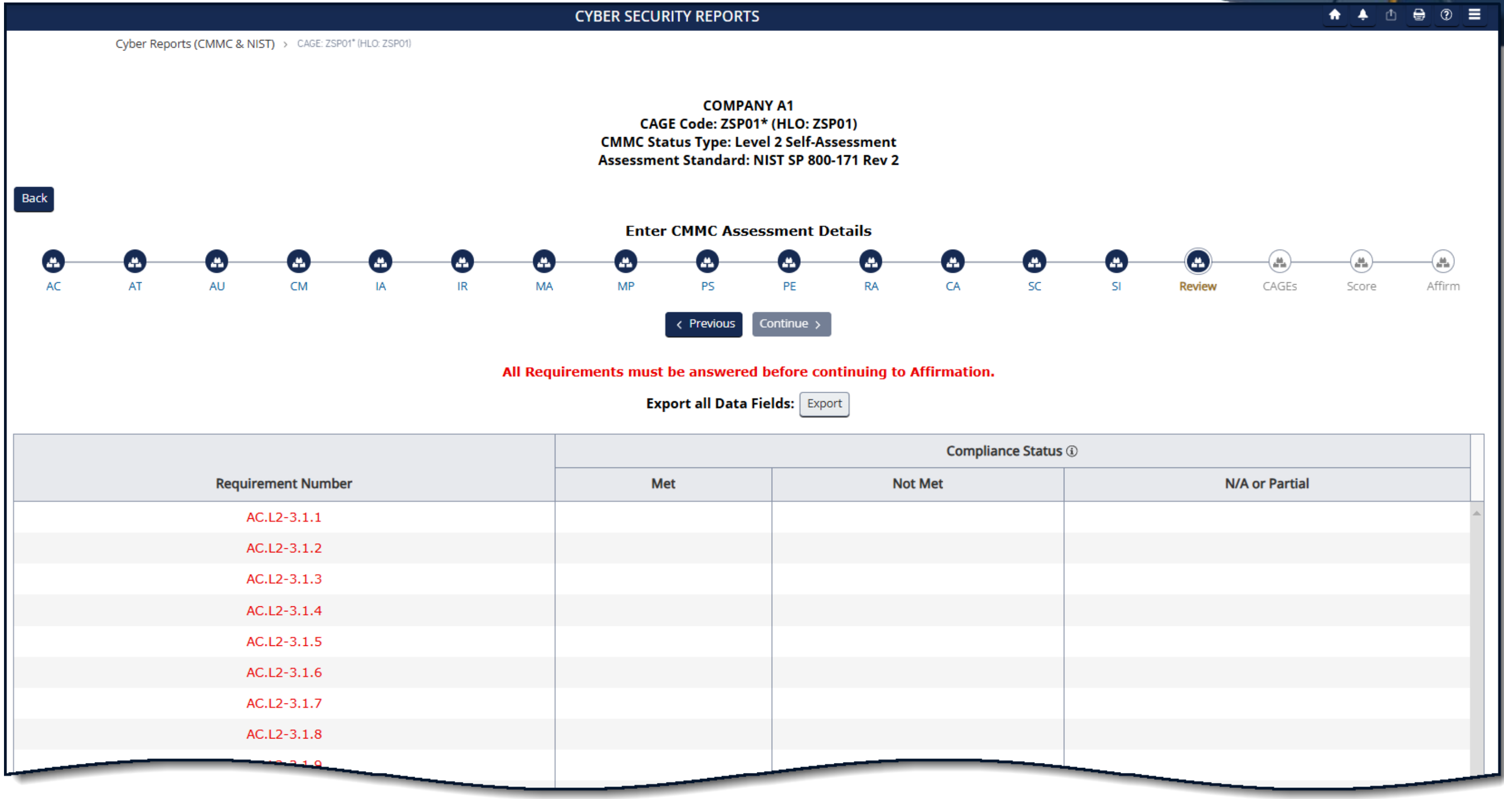
Back

Enter CMMC Assessment Details

Requirement Family: Security Assessment (CA)

Requirement Number	Requirement Description	Compliance Status ⓘ		
Note: All Objectives must be met for the Requirement to be Met.		Met	Not Met	N/A
CA.L2-3.12.1 Requirement Objectives	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.	☐ Met	☐ Not Met	☐ N/A
CA.L2-3.12.2 Requirement Objectives	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	☐ Met	☐ Not Met	☐ N/A
CA.L2-3.12.3 Requirement Objectives	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	☐ Met	☐ Not Met	☐ N/A
CA.L2-3.12.4 *N/A is not available for this requirement. Requirement Objectives	Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.	☐ Met	☐ Not Met	*

Cyber Reports



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

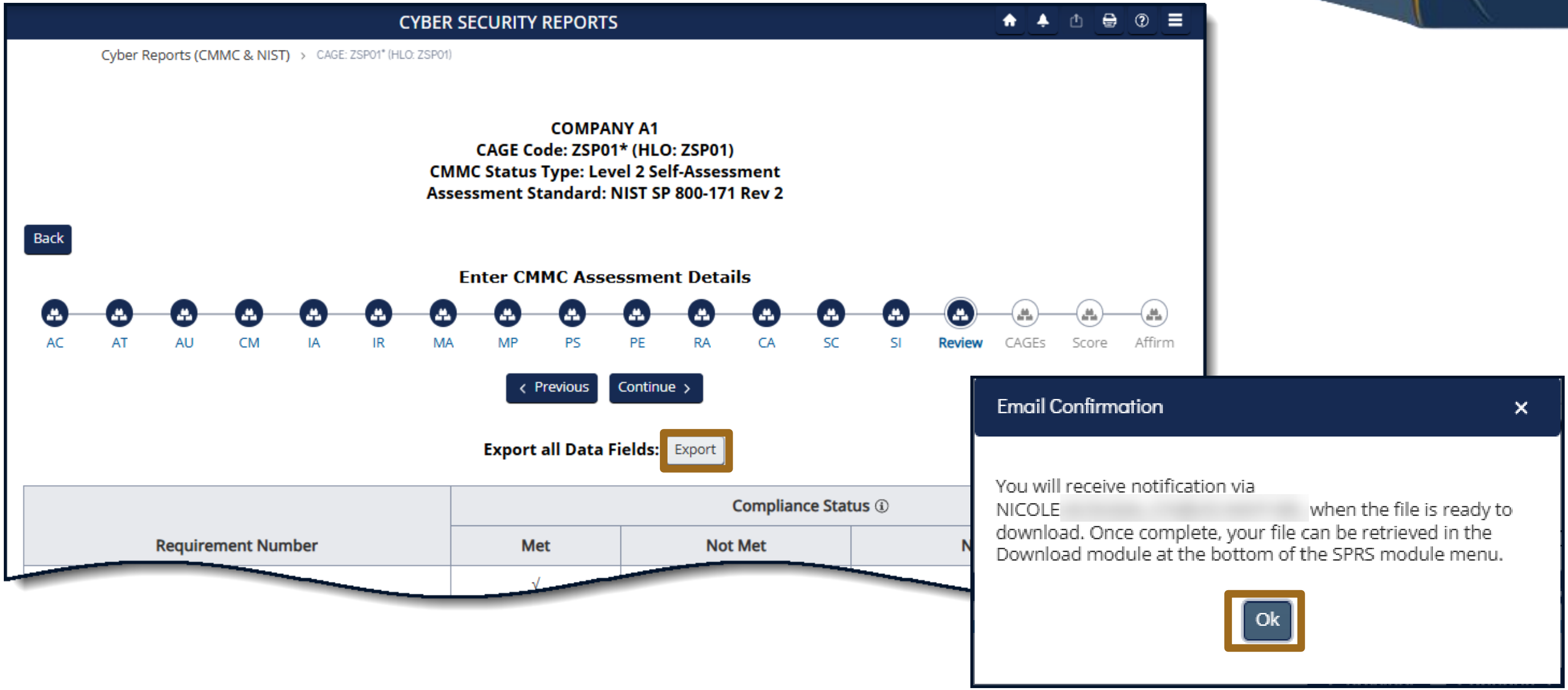
Enter CMMC Assessment Details

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			
AC.L2-3.1.8			

Cyber Reports



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

Export all Data Fields: Export

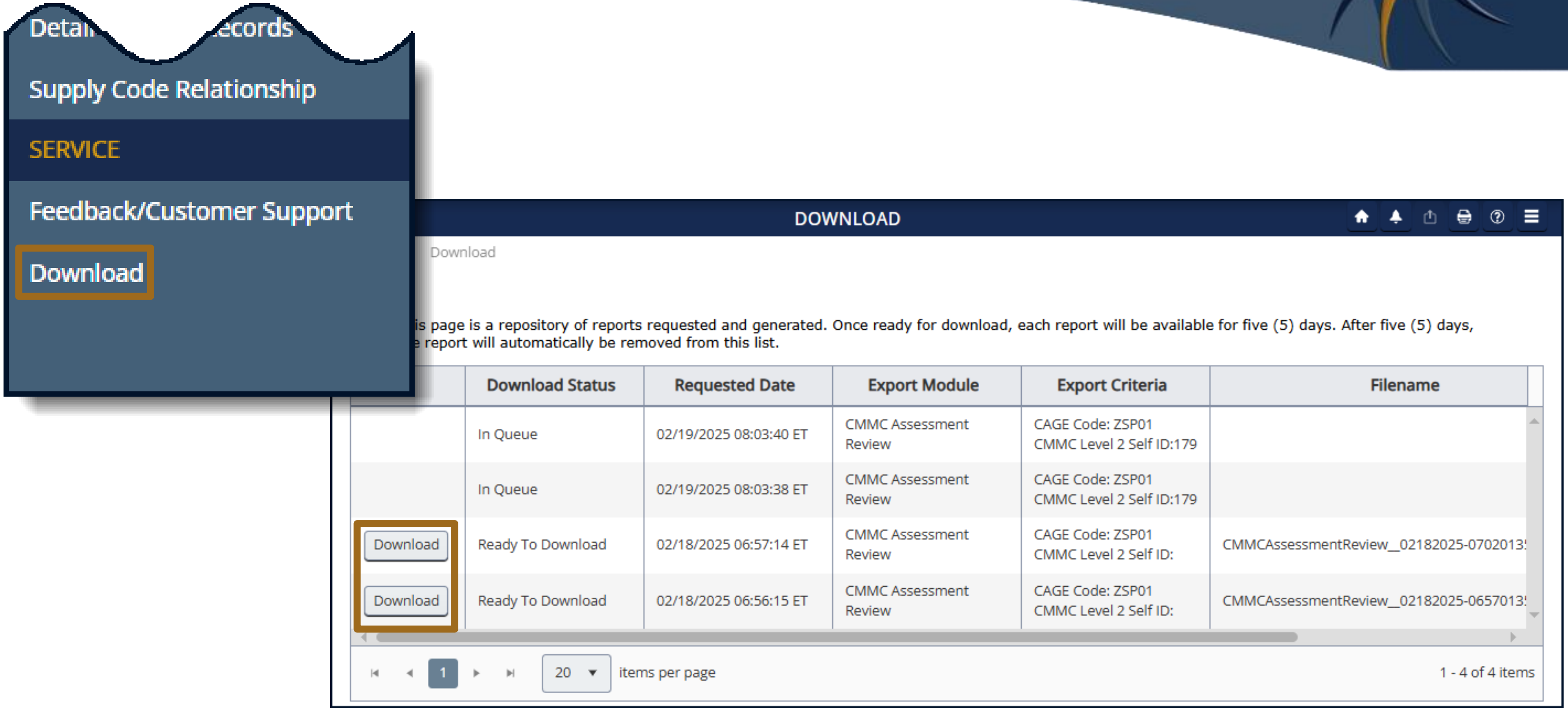
Requirement Number	Compliance Status ⓘ		
	Met	Not Met	N
	√		

Email Confirmation ×

You will receive notification via NICOLE[redacted] when the file is ready to download. Once complete, your file can be retrieved in the Download module at the bottom of the SPRS module menu.

Ok

Cyber Reports



DOWNLOAD

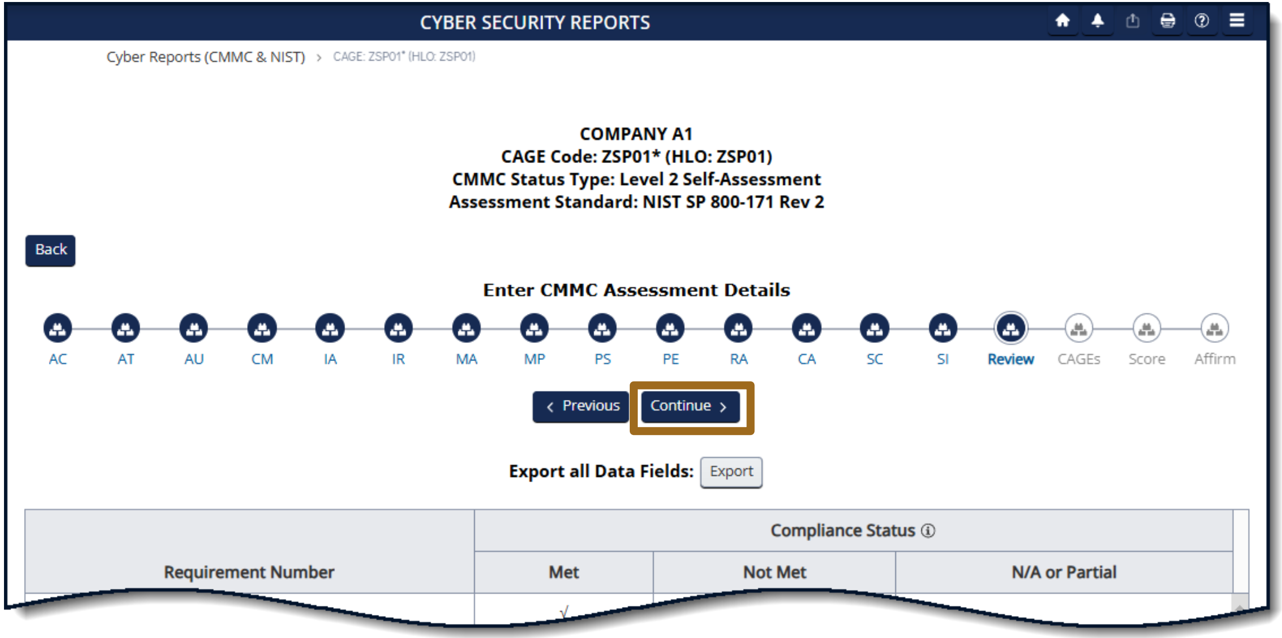
Download

is page is a repository of reports requested and generated. Once ready for download, each report will be available for five (5) days. After five (5) days, e report will automatically be removed from this list.

	Download Status	Requested Date	Export Module	Export Criteria	Filename
	In Queue	02/19/2025 08:03:40 ET	CMMC Assessment Review	CAGE Code: ZSP01 CMMC Level 2 Self ID:179	
	In Queue	02/19/2025 08:03:38 ET	CMMC Assessment Review	CAGE Code: ZSP01 CMMC Level 2 Self ID:179	
Download	Ready To Download	02/18/2025 06:57:14 ET	CMMC Assessment Review	CAGE Code: ZSP01 CMMC Level 2 Self ID:	CMMCAssessmentReview_02182025-0702013!
Download	Ready To Download	02/18/2025 06:56:15 ET	CMMC Assessment Review	CAGE Code: ZSP01 CMMC Level 2 Self ID:	CMMCAssessmentReview_02182025-0657013!

1   20 ▾ items per page   1 - 4 of 4 items

Cyber Reports



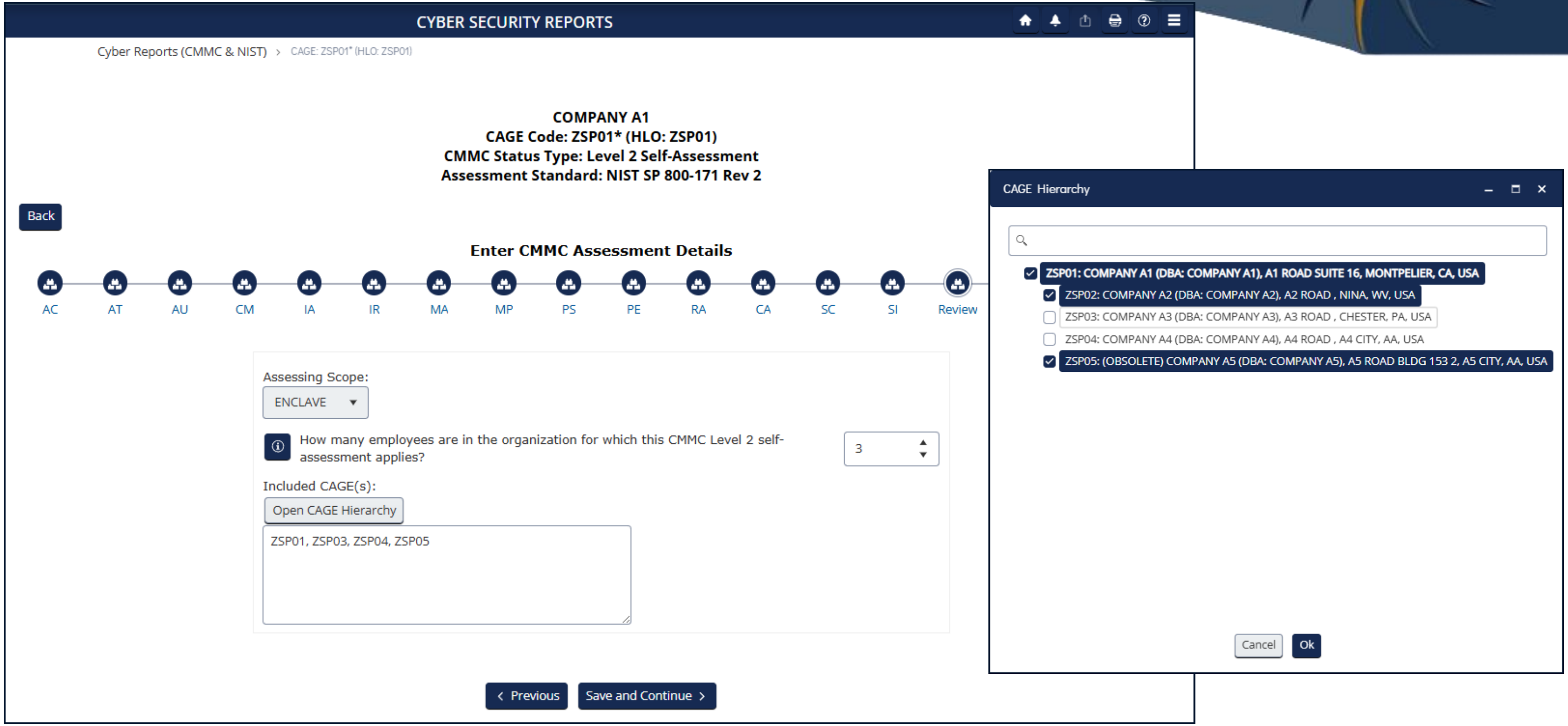
COMPANY A1
CAGE Code: ZSP01* (HLO: ZSP01)
CMMC Status Type: Level 2 Self-Assessment
Assessment Standard: NIST SP 800-171 Rev 2

Enter CMMC Assessment Details

Export all Data Fields: Export

Requirement Number	Compliance Status ⓘ		
	Met	Not Met	N/A or Partial
	√		

Cyber Reports



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

Assessing Scope: ENCLAVE ▾

ⓘ How many employees are in the organization for which this CMMC Level 2 self-assessment applies? 3

Included CAGE(s):

Open CAGE Hierarchy

ZSP01, ZSP03, ZSP04, ZSP05

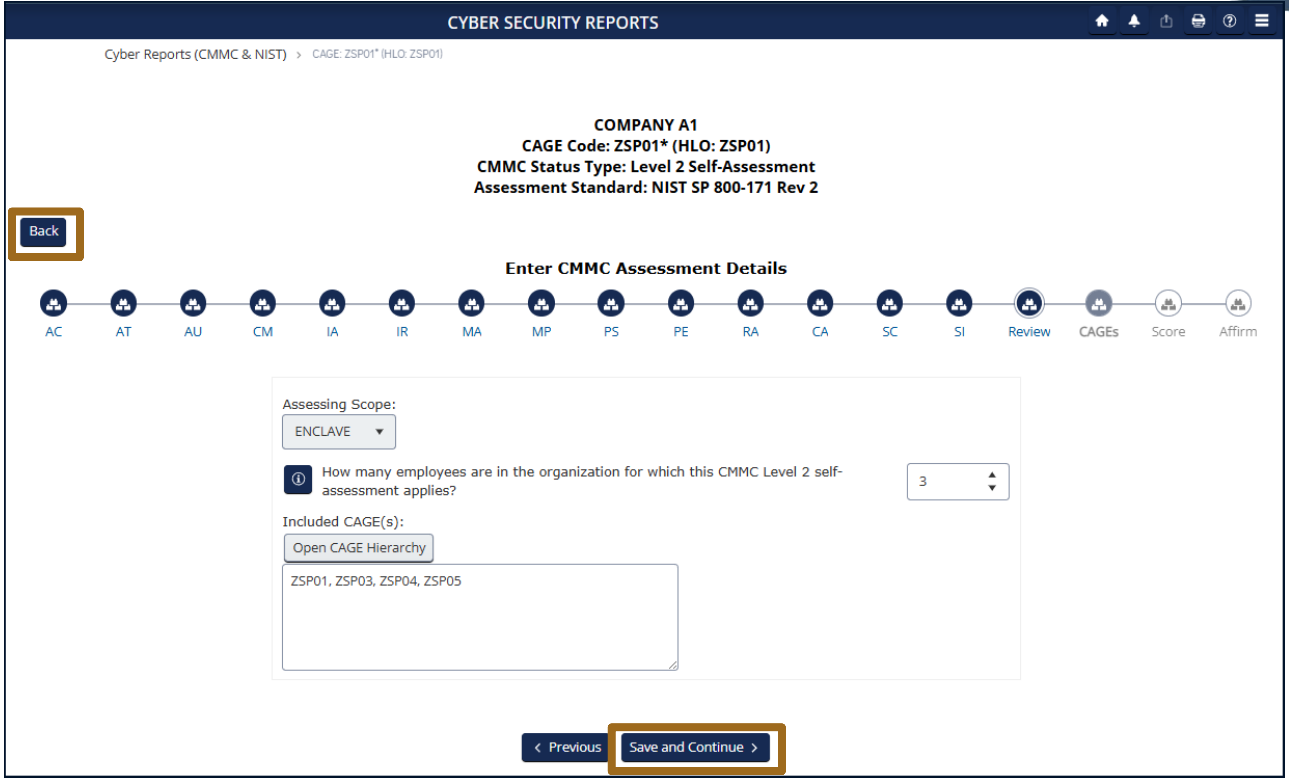
‹ Previous | Save and Continue ›

CAGE Hierarchy

- ☑ 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

Cyber 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

Enter CMMC Assessment Details

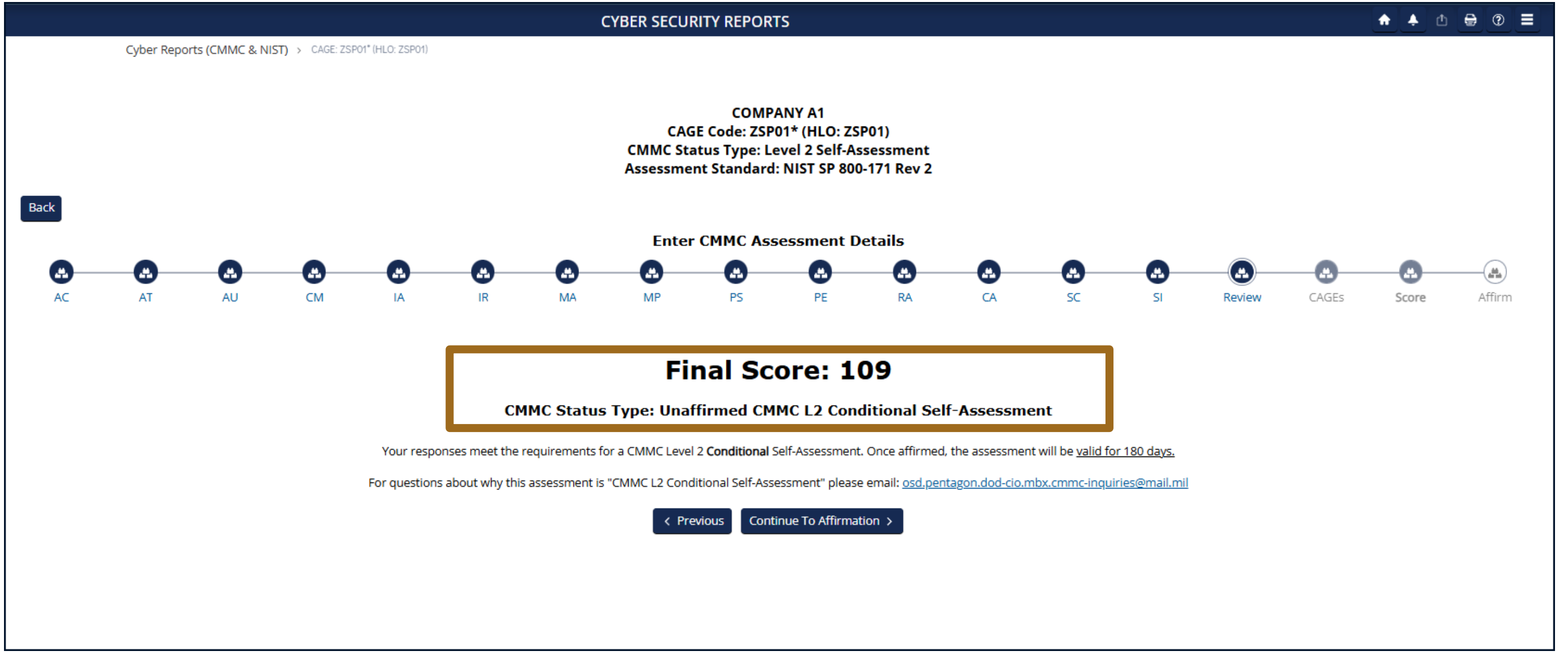
Assessing Scope: ENCLAVE

How many employees are in the organization for which this CMMC Level 2 self-assessment applies? 3

Included CAGE(s):

ZSP01, ZSP03, ZSP04, ZSP05

Cyber 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

Enter CMMC Assessment Details

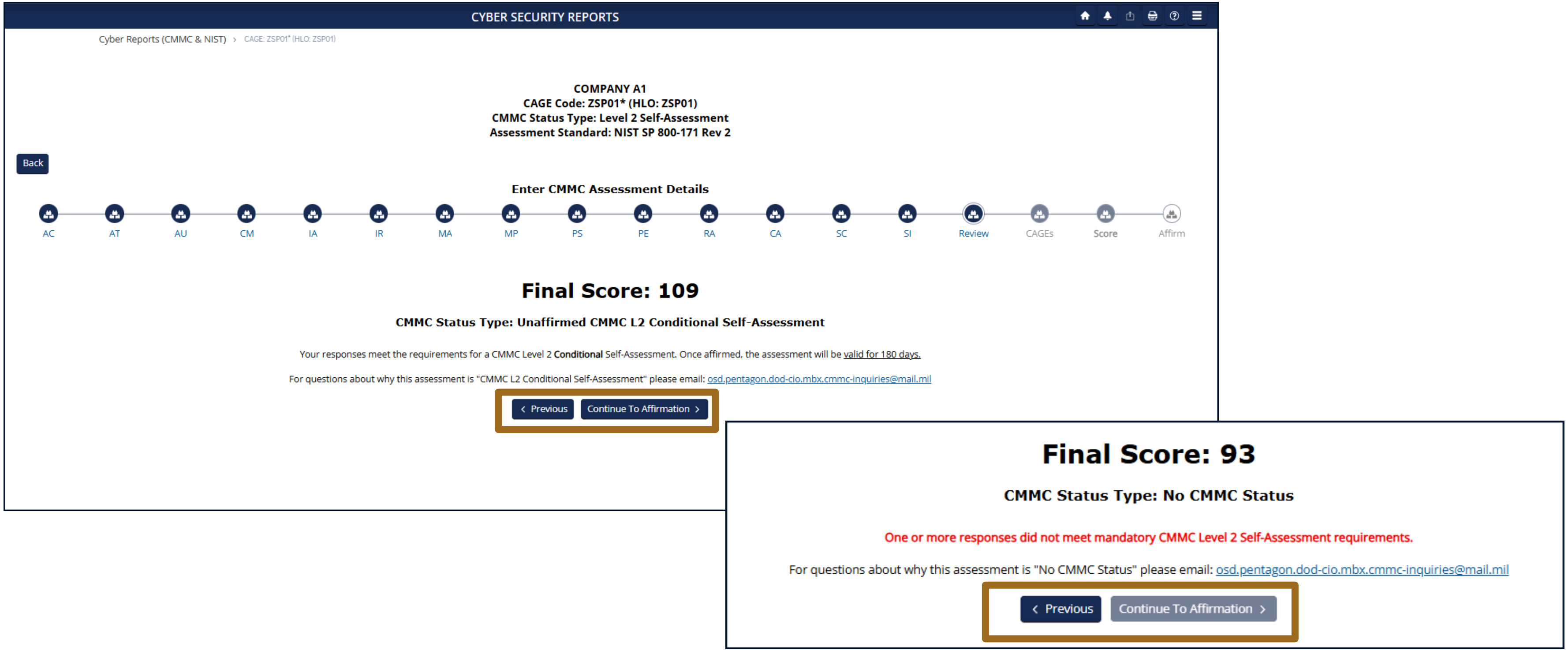
Final Score: 109

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

Cyber Reports



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

Enter CMMC Assessment Details

Final Score: 109

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

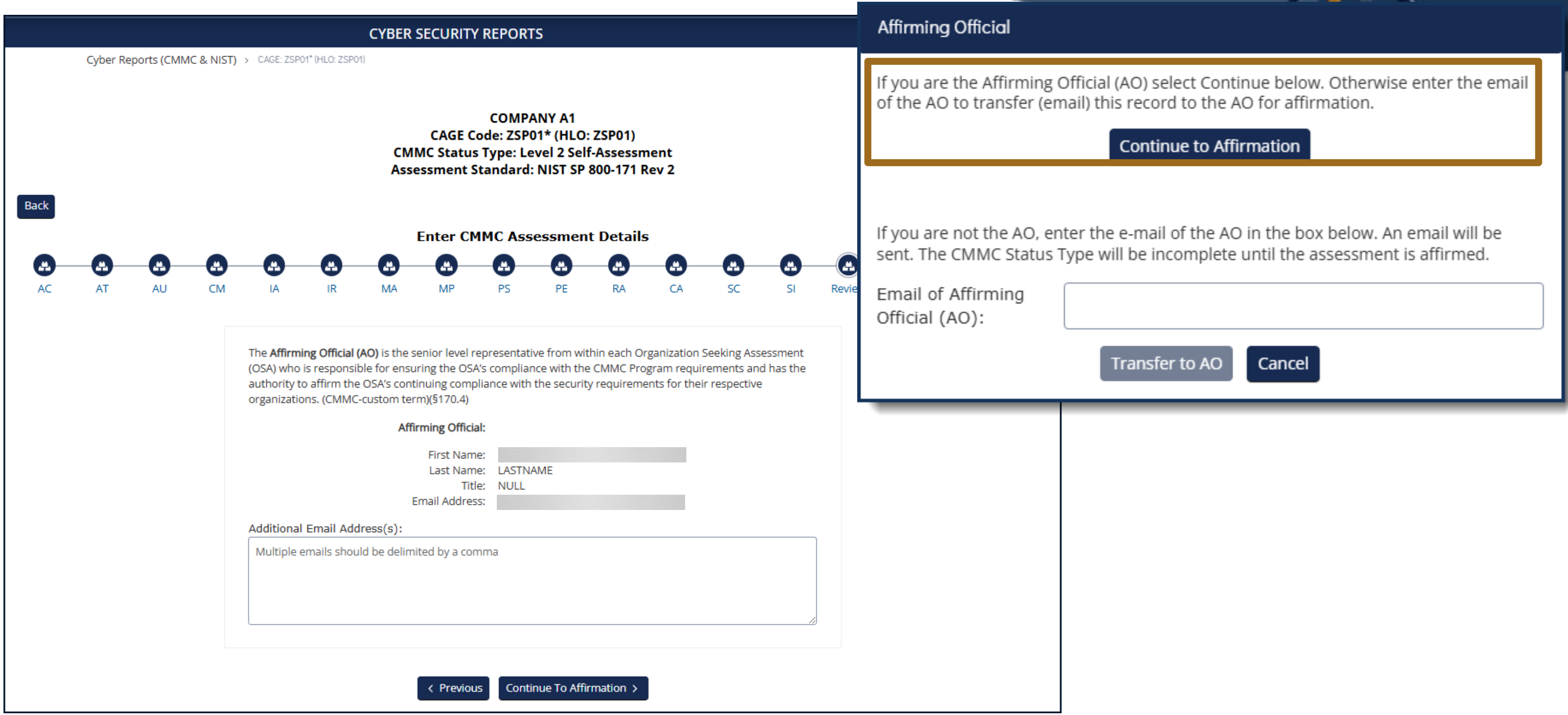
Final Score: 93

CMMC Status Type: No CMMC Status

One or more responses did not meet mandatory CMMC Level 2 Self-Assessment requirements.

For questions about why this assessment is "No CMMC Status" please email: osd.pentagon.dod-cio.mbx.cmmc-inquiries@mail.mil

Cyber Reports



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

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: [redacted]
Last Name: LASTNAME
Title: NULL
Email Address: [redacted]

Additional Email Address(s):

Multiple emails should be delimited by a comma

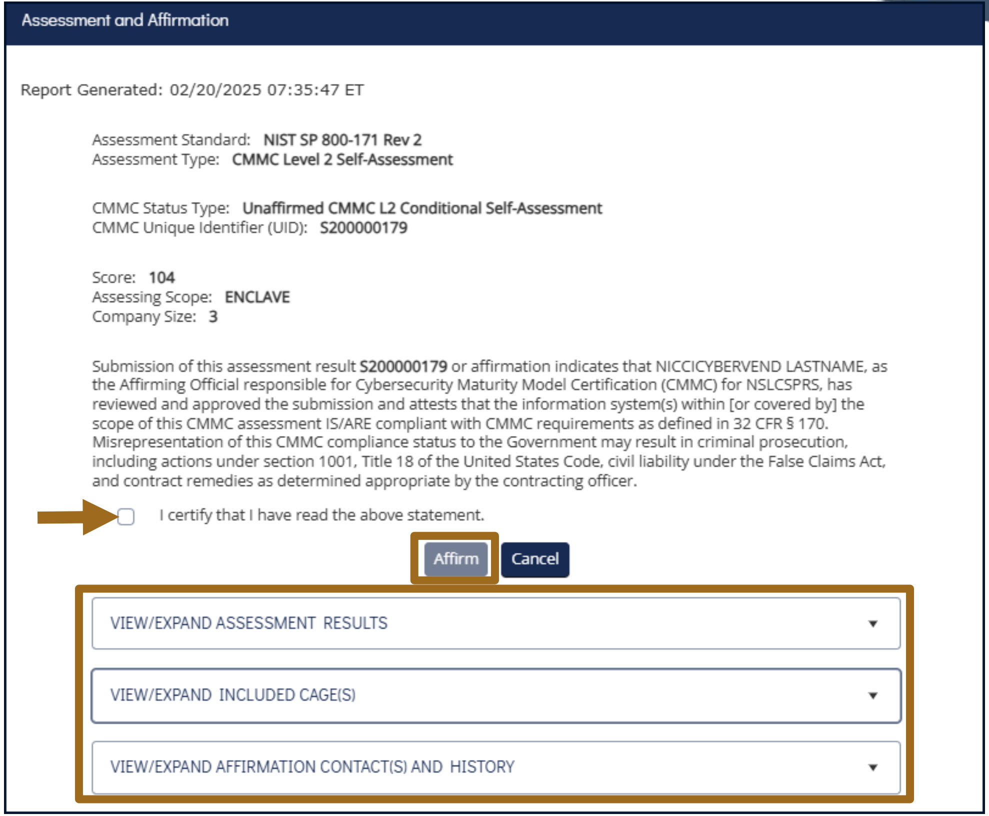
Affirming Official

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



Assessment and Affirmation

Report Generated: 02/20/2025 07:35:47 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): **S200000179**

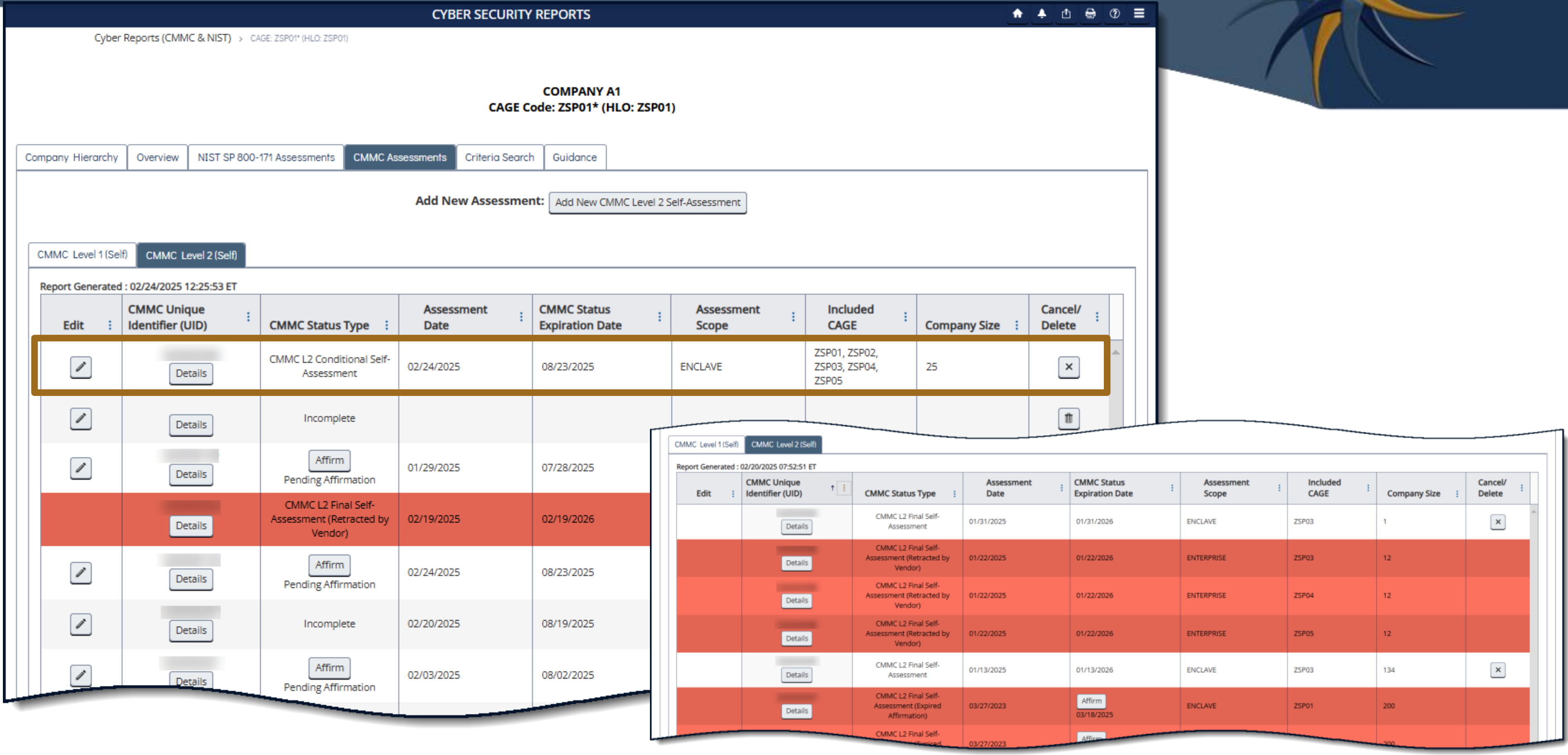
Score: **104**
Assessing Scope: **ENCLAVE**
Company Size: **3**

Submission of this assessment result **S200000179** or affirmation indicates that NICCICYBERVEND LASTNAME, 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 ▼

Cyber Reports



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)

Report Generated : 02/24/2025 12:25:53 ET

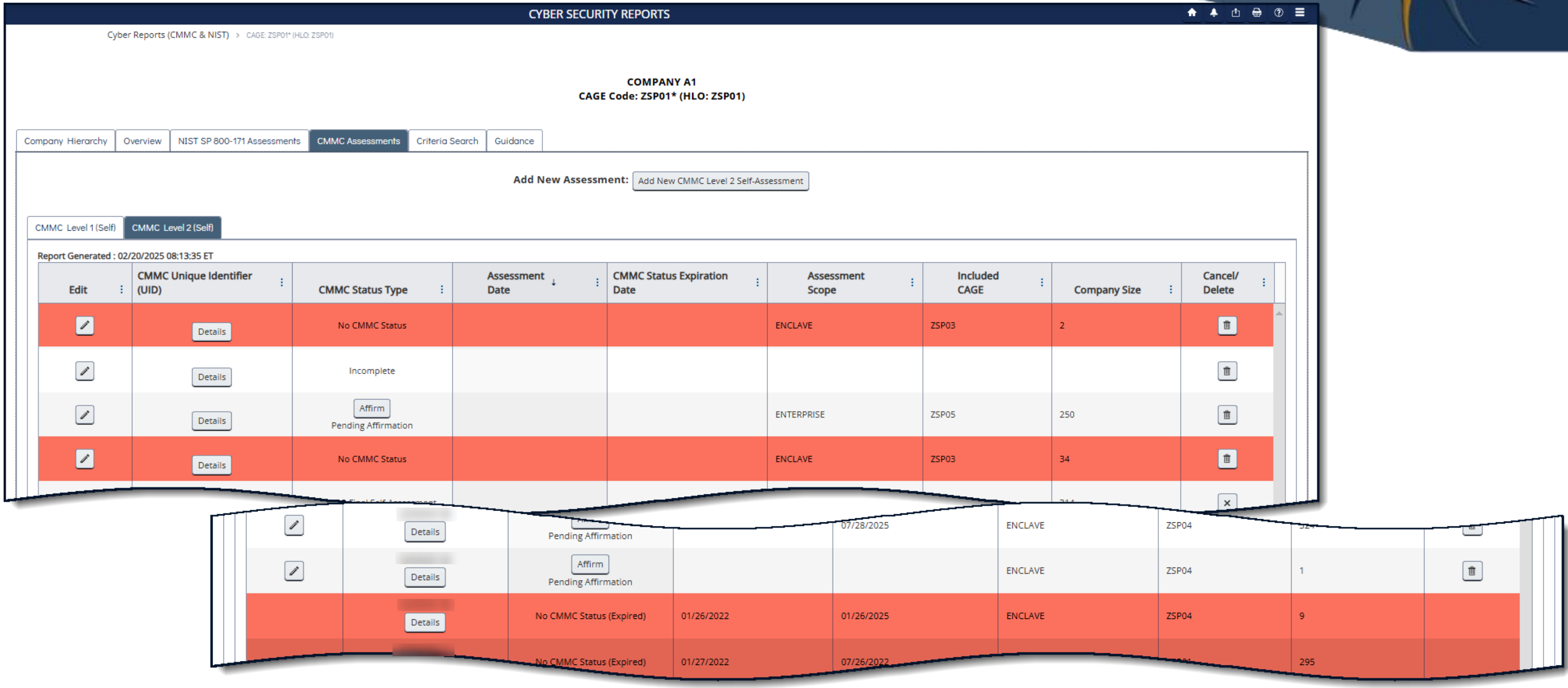
Edit	CMMC Unique Identifier (UID)	CMMC Status Type	Assessment Date	CMMC Status Expiration Date	Assessment Scope	Included CAGE	Company Size	Cancel/ Delete
✎	[redacted] Details	CMMC L2 Conditional Self-Assessment	02/24/2025	08/23/2025	ENCLAVE	ZSP01, ZSP02, ZSP03, ZSP04, ZSP05	25	✕
✎	Details	Incomplete						🗑
✎	[redacted] Details	Affirm Pending Affirmation	01/29/2025	07/28/2025				
	[redacted] Details	CMMC L2 Final Self-Assessment (Retracted by Vendor)	02/19/2025	02/19/2026				
✎	[redacted] Details	Affirm Pending Affirmation	02/24/2025	08/23/2025				
✎	[redacted] Details	Incomplete	02/20/2025	08/19/2025				
✎	[redacted] Details	Affirm Pending Affirmation	02/03/2025	08/02/2025				

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

Report Generated : 02/20/2025 07:52:51 ET

Edit	CMMC Unique Identifier (UID)	CMMC Status Type	Assessment Date	CMMC Status Expiration Date	Assessment Scope	Included CAGE	Company Size	Cancel/ Delete
	[redacted] Details	CMMC L2 Final Self-Assessment	01/31/2025	01/31/2026	ENCLAVE	ZSP03	1	✕
	[redacted] Details	CMMC L2 Final Self-Assessment (Retracted by Vendor)	01/22/2025	01/22/2026	ENTERPRISE	ZSP03	12	
	[redacted] Details	CMMC L2 Final Self-Assessment (Retracted by Vendor)	01/22/2025	01/22/2026	ENTERPRISE	ZSP04	12	
	[redacted] Details	CMMC L2 Final Self-Assessment (Retracted by Vendor)	01/22/2025	01/22/2026	ENTERPRISE	ZSP05	12	
	[redacted] Details	CMMC L2 Final Self-Assessment	01/13/2025	01/13/2026	ENCLAVE	ZSP03	134	✕
	[redacted] Details	CMMC L2 Final Self-Assessment (Expired Affirmation)	03/27/2023	Affirm 03/18/2025	ENCLAVE	ZSP01	200	
		CMMC L2 Final Self-	03/27/2023	Affirm			200	

Cyber Reports



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

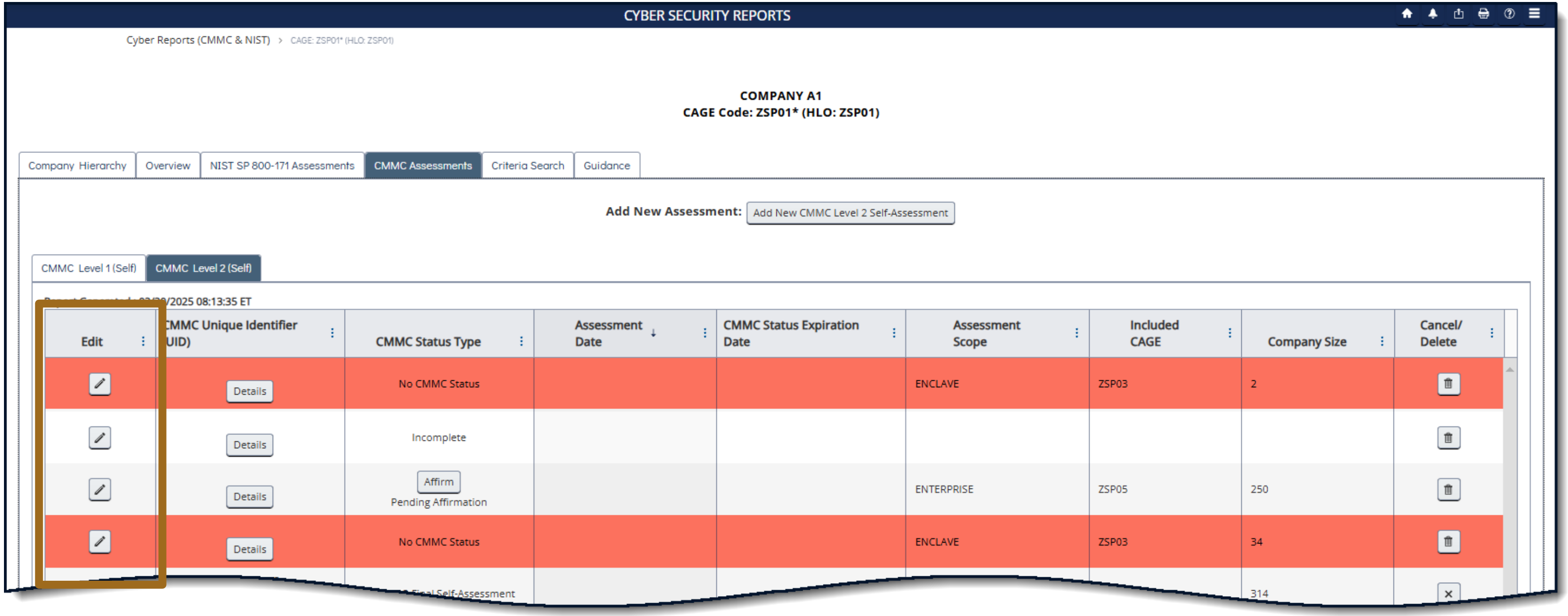
Add New Assessment: Add New CMMC Level 2 Self-Assessment

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

Report Generated : 02/20/2025 08:13:35 ET

Edit	CMMC Unique Identifier (UID)	CMMC Status Type	Assessment Date	CMMC Status Expiration Date	Assessment Scope	Included CAGE	Company Size	Cancel/ Delete
✎	Details	No CMMC Status			ENCLAVE	ZSP03	2	🗑
✎	Details	Incomplete						🗑
✎	Details	Affirm Pending Affirmation			ENTERPRISE	ZSP05	250	🗑
✎	Details	No CMMC Status			ENCLAVE	ZSP03	34	🗑
		Final Self-Assessment					314	×
✎	[redacted] Details	Pending Affirmation		07/28/2025	ENCLAVE	ZSP04	324	🗑
✎	[redacted] Details	Affirm Pending Affirmation			ENCLAVE	ZSP04	1	🗑
	[redacted] Details	No CMMC Status (Expired)	01/26/2022	01/26/2025	ENCLAVE	ZSP04	9	
	[redacted]	No CMMC Status (Expired)	01/27/2022	07/26/2022			295	

Cyber Reports



CYBER SECURITY REPORTS

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

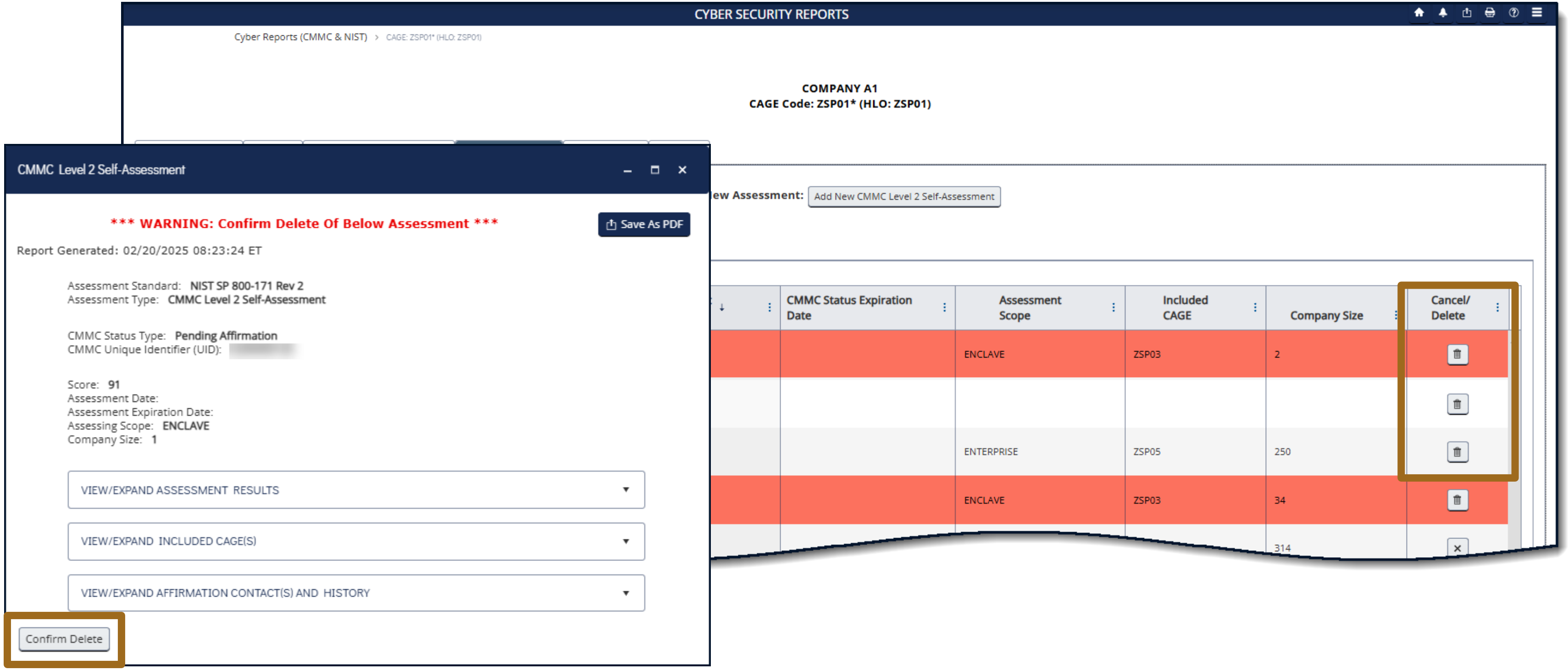
COMPANY A1
CAGE Code: ZSP01* (HLO: ZSP01)

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

Report Generated: [illegible]/2025 08:13:35 ET

Edit	CMMC Unique Identifier (UID)	CMMC Status Type	Assessment Date ↓	CMMC Status Expiration Date	Assessment Scope	Included CAGE	Company Size	Cancel/ Delete
✎	Details	No CMMC Status			ENCLAVE	ZSP03	2	🗑
✎	Details	Incomplete						🗑
✎	Details	Affirm Pending Affirmation			ENTERPRISE	ZSP05	250	🗑
✎	Details	No CMMC Status			ENCLAVE	ZSP03	34	🗑
		Final Self-Assessment					314	×

Cyber Reports



CYBER SECURITY REPORTS

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

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

ew Assessment: Add New CMMC Level 2 Self-Assessment

↓	CMMC Status Expiration Date	Assessment Scope	Included CAGE	Company Size	Cancel/ Delete
		ENCLAVE	ZSP03	2	🗑
					🗑
		ENTERPRISE	ZSP05	250	🗑
		ENCLAVE	ZSP03	34	🗑
				314	✕

CMMC Level 2 Self-Assessment

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

Save As PDF

Report Generated: 02/20/2025 08:23:24 ET

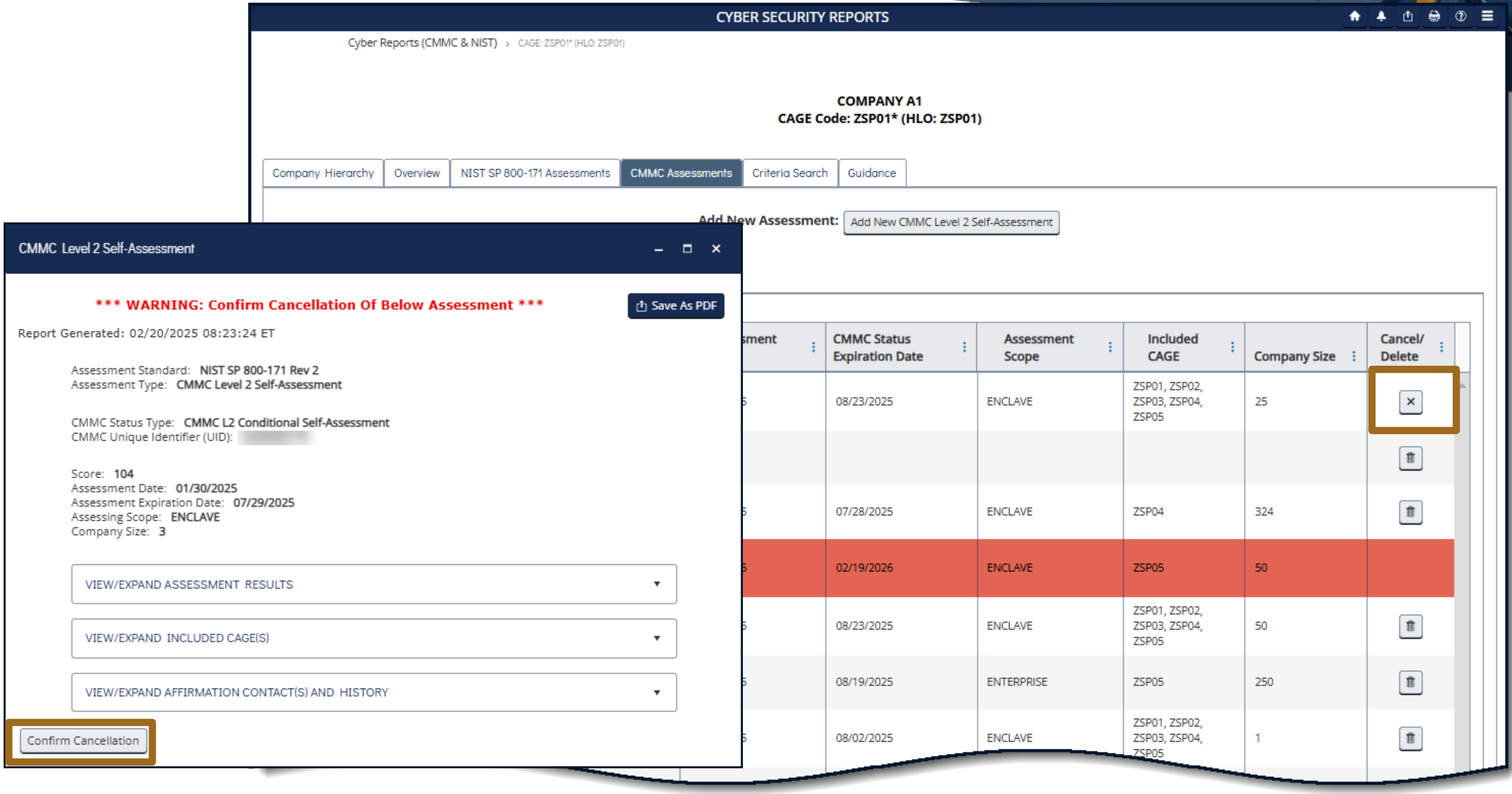
Assessment Standard: NIST SP 800-171 Rev 2
Assessment Type: CMMC Level 2 Self-Assessment

CMMC Status Type: Pending Affirmation
CMMC Unique Identifier (UID): [redacted]

Score: 91
Assessment Date:
Assessment Expiration Date:
Assessing Scope: ENCLAVE
Company Size: 1

VIEW/EXPAND ASSESSMENT RESULTS ▾
VIEW/EXPAND INCLUDED CAGE(S) ▾
VIEW/EXPAND AFFIRMATION CONTACT(S) AND HISTORY ▾
Confirm Delete

Cyber Reports



CYBER SECURITY REPORTS

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

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

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

sment	CMMC Status Expiration Date	Assessment Scope	Included CAGE	Company Size	Cancel/ Delete
5	08/23/2025	ENCLAVE	ZSP01, ZSP02, ZSP03, ZSP04, ZSP05	25	×
					🗑
5	07/28/2025	ENCLAVE	ZSP04	324	🗑
5	02/19/2026	ENCLAVE	ZSP05	50	
5	08/23/2025	ENCLAVE	ZSP01, ZSP02, ZSP03, ZSP04, ZSP05	50	🗑
5	08/19/2025	ENTERPRISE	ZSP05	250	🗑
5	08/02/2025	ENCLAVE	ZSP01, ZSP02, ZSP03, ZSP04, ZSP05	1	🗑

CMMC Level 2 Self-Assessment

*** WARNING: Confirm Cancellation Of Below Assessment ***

Save As PDF

Report Generated: 02/20/2025 08:23:24 ET

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

CMMC Status Type: CMMC L2 Conditional Self-Assessment
CMMC Unique Identifier (UID): [redacted]

Score: 104
Assessment Date: 01/30/2025
Assessment Expiration Date: 07/29/2025
Assessing Scope: ENCLAVE
Company Size: 3

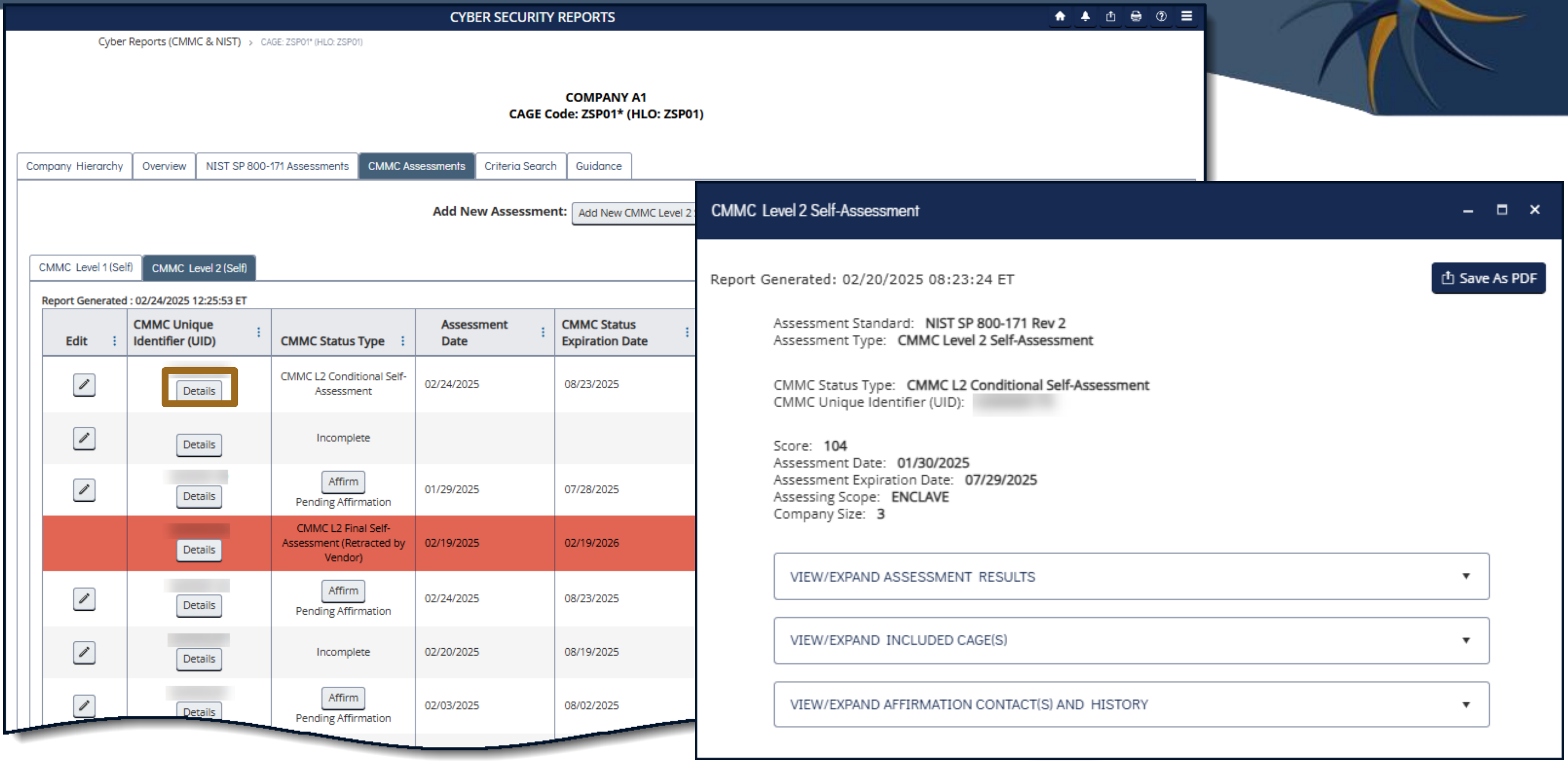
VIEW/EXPAND ASSESSMENT RESULTS ▾

VIEW/EXPAND INCLUDED CAGE(S) ▾

VIEW/EXPAND AFFIRMATION CONTACT(S) AND HISTORY ▾

Confirm Cancellation

Cyber Reports



CYBER SECURITY REPORTS

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

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

Add New Assessment: Add New CMMC Level 2

Report Generated : 02/24/2025 12:25:53 ET

Edit	CMMC Unique Identifier (UID)	CMMC Status Type	Assessment Date	CMMC Status Expiration Date
✎	Details	CMMC L2 Conditional Self-Assessment	02/24/2025	08/23/2025
✎	Details	Incomplete		
✎	[redacted] Details	Affirm Pending Affirmation	01/29/2025	07/28/2025
	[redacted] Details	CMMC L2 Final Self-Assessment (Retracted by Vendor)	02/19/2025	02/19/2026
✎	[redacted] Details	Affirm Pending Affirmation	02/24/2025	08/23/2025
✎	[redacted] Details	Incomplete	02/20/2025	08/19/2025
✎	[redacted] Details	Affirm Pending Affirmation	02/03/2025	08/02/2025

CMMC Level 2 Self-Assessment

Report Generated: 02/20/2025 08:23:24 ET

Save As PDF

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

CMMC Status Type: **CMMC L2 Conditional Self-Assessment**
CMMC Unique Identifier (UID): [redacted]

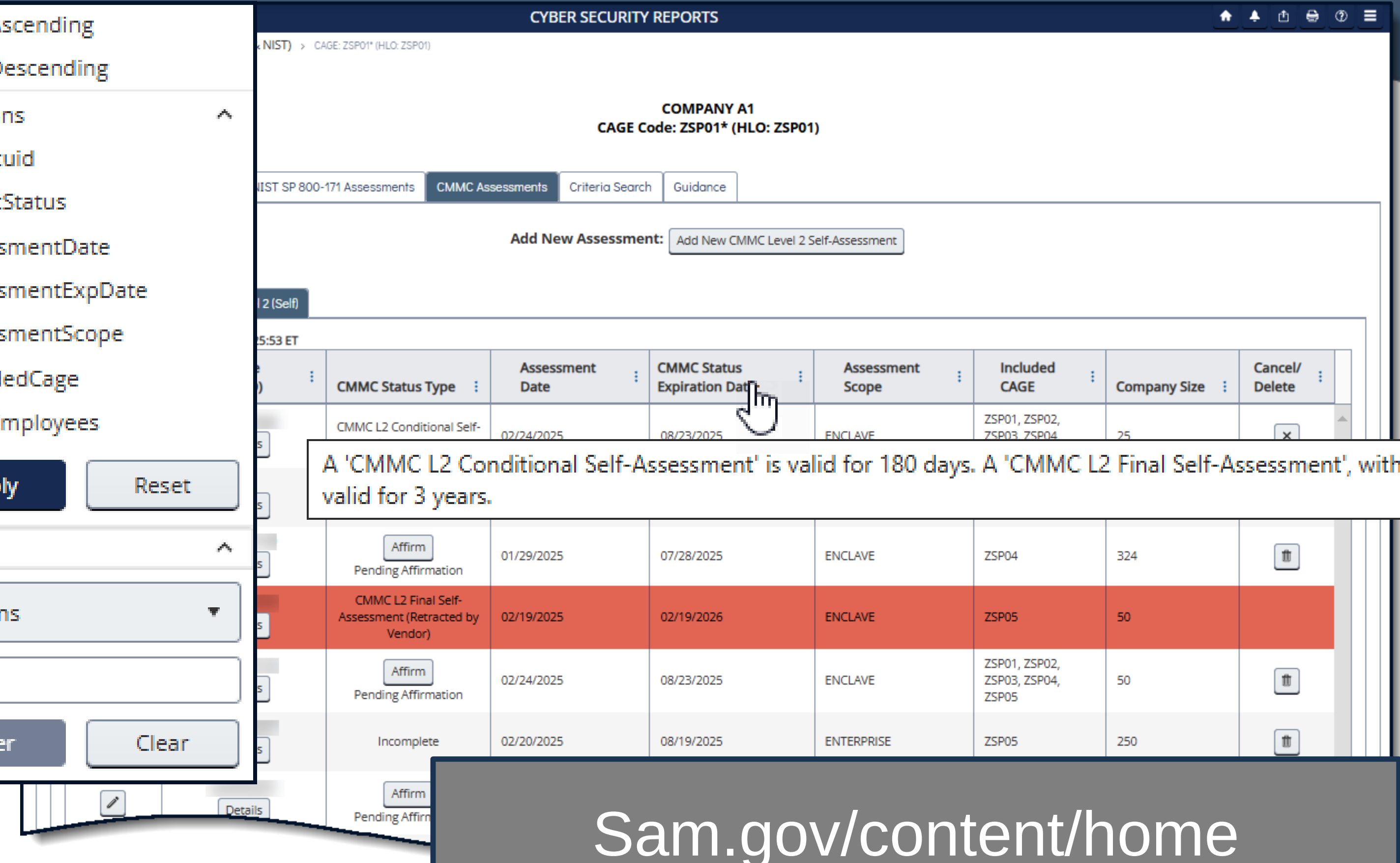
Score: **104**
Assessment Date: **01/30/2025**
Assessment Expiration Date: **07/29/2025**
Assessing Scope: **ENCLAVE**
Company Size: **3**

VIEW/EXPAND ASSESSMENT RESULTS ▼

VIEW/EXPAND INCLUDED CAGE(S) ▼

VIEW/EXPAND AFFIRMATION CONTACT(S) AND HISTORY ▼

Cyber Reports



CYBER SECURITY REPORTS

NIST) > CAGE: ZSP01* (HLO: ZSP01)

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

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

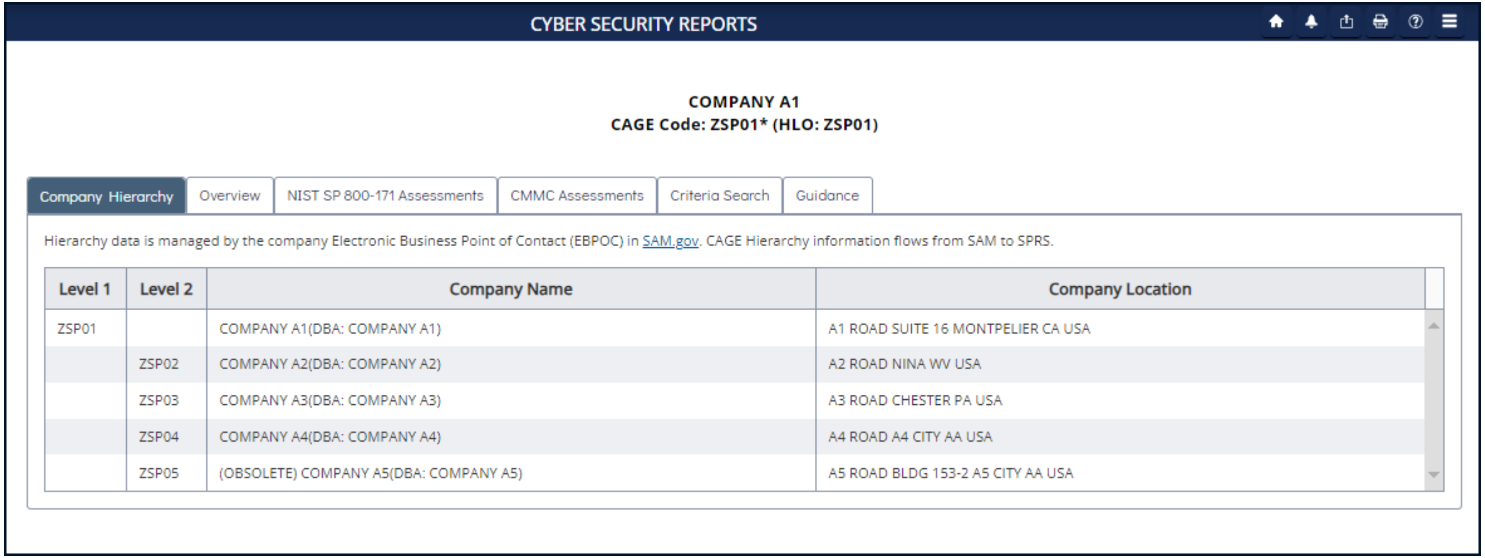
5:53 ET

e)	CMMC Status Type	Assessment Date	CMMC Status Expiration Date	Assessment Scope	Included CAGE	Company Size	Cancel/ Delete
s	CMMC L2 Conditional Self-	02/24/2025	08/23/2025	ENCLAVE	ZSP01, ZSP02, ZSP03, ZSP04	25	✕
s							
s	Affirm Pending Affirmation	01/29/2025	07/28/2025	ENCLAVE	ZSP04	324	🗑
s	CMMC L2 Final Self-Assessment (Retracted by Vendor)	02/19/2025	02/19/2026	ENCLAVE	ZSP05	50	
s	Affirm Pending Affirmation	02/24/2025	08/23/2025	ENCLAVE	ZSP01, ZSP02, ZSP03, ZSP04, ZSP05	50	🗑
s	Incomplete	02/20/2025	08/19/2025	ENTERPRISE	ZSP05	250	🗑
Details	Affirm Pending Affirm						

A 'CMMC L2 Conditional Self-Assessment' is valid for 180 days. A 'CMMC L2 Final Self-Assessment', with annual affirmations certifying compliance, is valid for 3 years.

Sam.gov/content/home

Cyber Reports



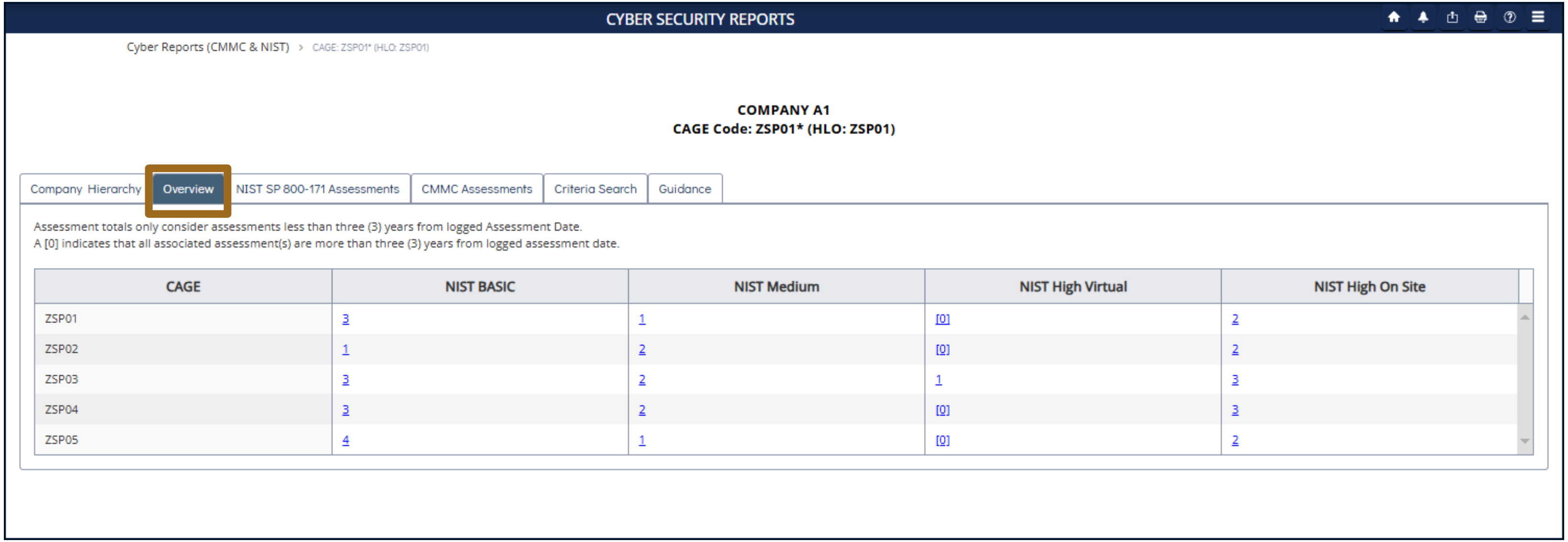
COMPANY A1
CAGE Code: ZSP01* (HLO: ZSP01)

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

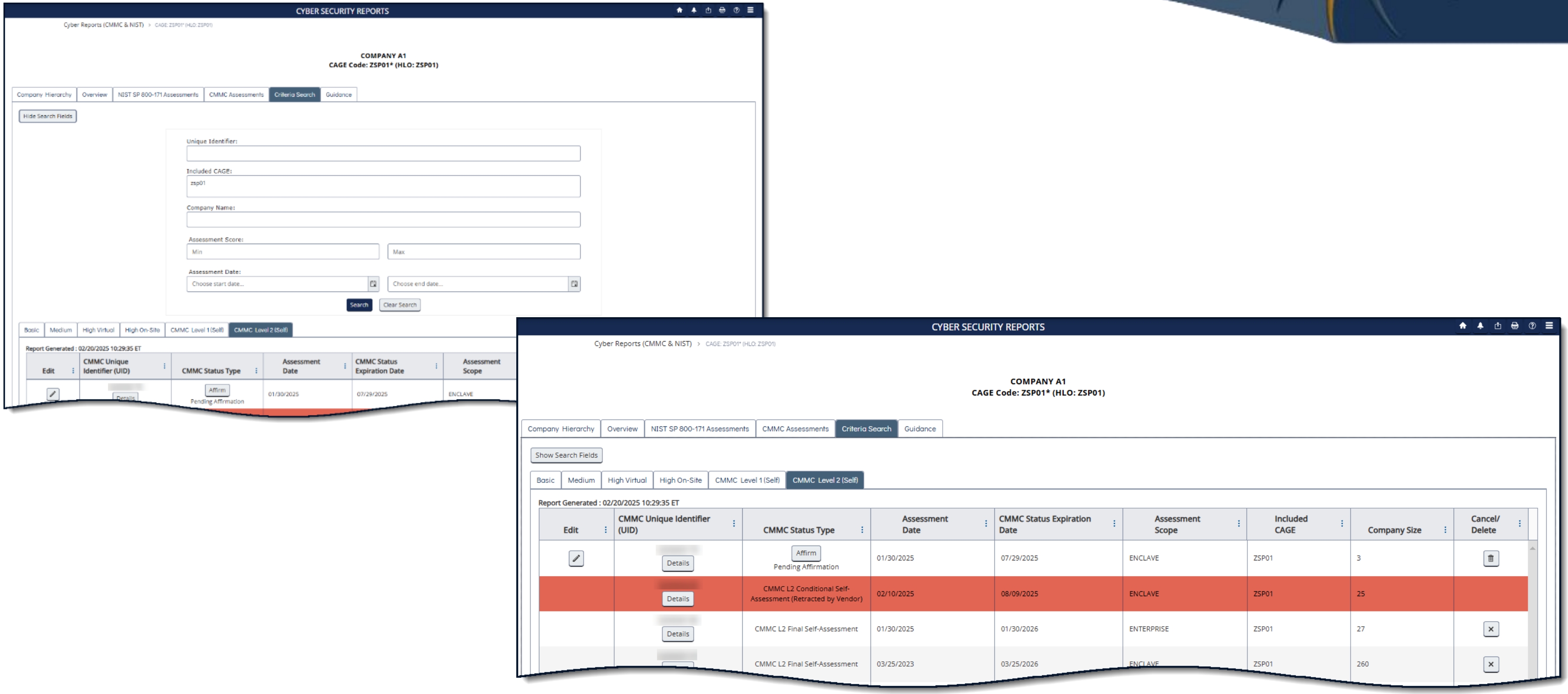


COMPANY A1
CAGE Code: ZSP01* (HLO: ZSP01)

Assessment totals only consider assessments less than three (3) years from logged Assessment Date.
A [0] indicates that all associated assessment(s) are more than three (3) years from logged assessment date.

CAGE	NIST BASIC	NIST Medium	NIST High Virtual	NIST High On Site
ZSP01	3	1	[0]	2
ZSP02	1	2	[0]	2
ZSP03	3	2	1	3
ZSP04	3	2	[0]	3
ZSP05	4	1	[0]	2

Cyber Reports



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

Unique Identifier:

Included CAGE: zsp01

Company Name:

Assessment Score: Min Max

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

Report Generated : 02/20/2025 10:29:35 ET

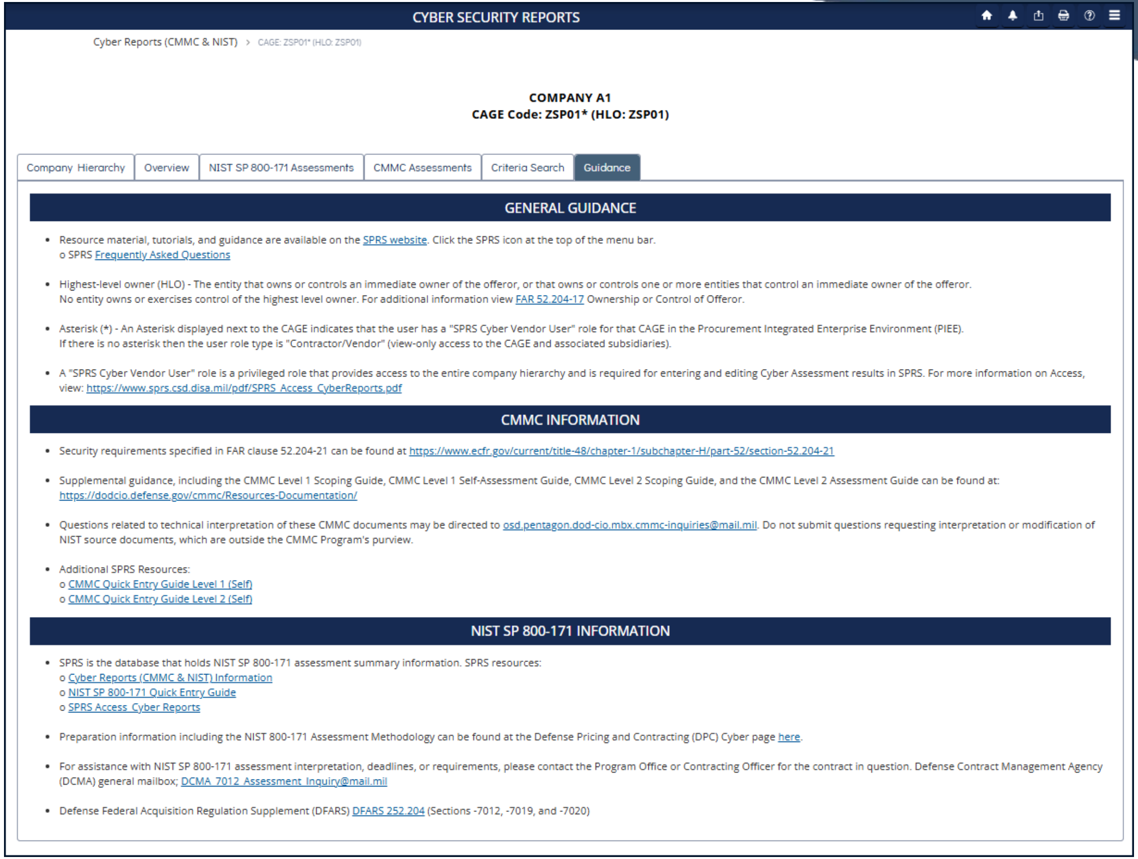
Edit	CMMC Unique Identifier (UID)	CMMC Status Type	Assessment Date	CMMC Status Expiration Date	Assessment Scope
	[redacted] Details	Affirm Pending Affirmation	01/30/2025	07/29/2025	ENCLAVE

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

Report Generated : 02/20/2025 10:29:35 ET

Edit	CMMC Unique Identifier (UID)	CMMC Status Type	Assessment Date	CMMC Status Expiration Date	Assessment Scope	Included CAGE	Company Size	Cancel/ Delete
	[redacted] Details	Affirm Pending Affirmation	01/30/2025	07/29/2025	ENCLAVE	ZSP01	3	
	[redacted] Details	CMMC L2 Conditional Self-Assessment (Retracted by Vendor)	02/10/2025	08/09/2025	ENCLAVE	ZSP01	25	
	[redacted] Details	CMMC L2 Final Self-Assessment	01/30/2025	01/30/2026	ENTERPRISE	ZSP01	27	✕
	[redacted]	CMMC L2 Final Self-Assessment	03/25/2023	03/25/2026	ENCLAVE	ZSP01	260	✕

Cyber Reports



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

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

GENERAL GUIDANCE

- Resource material, tutorials, and guidance are available on the SPRS website. Click the SPRS icon at the top of the menu bar.
  o 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. For more information on Access, view: https://www.sprs.csd.disa.mil/pdf/SPRS_Access_CyberReports.pdf

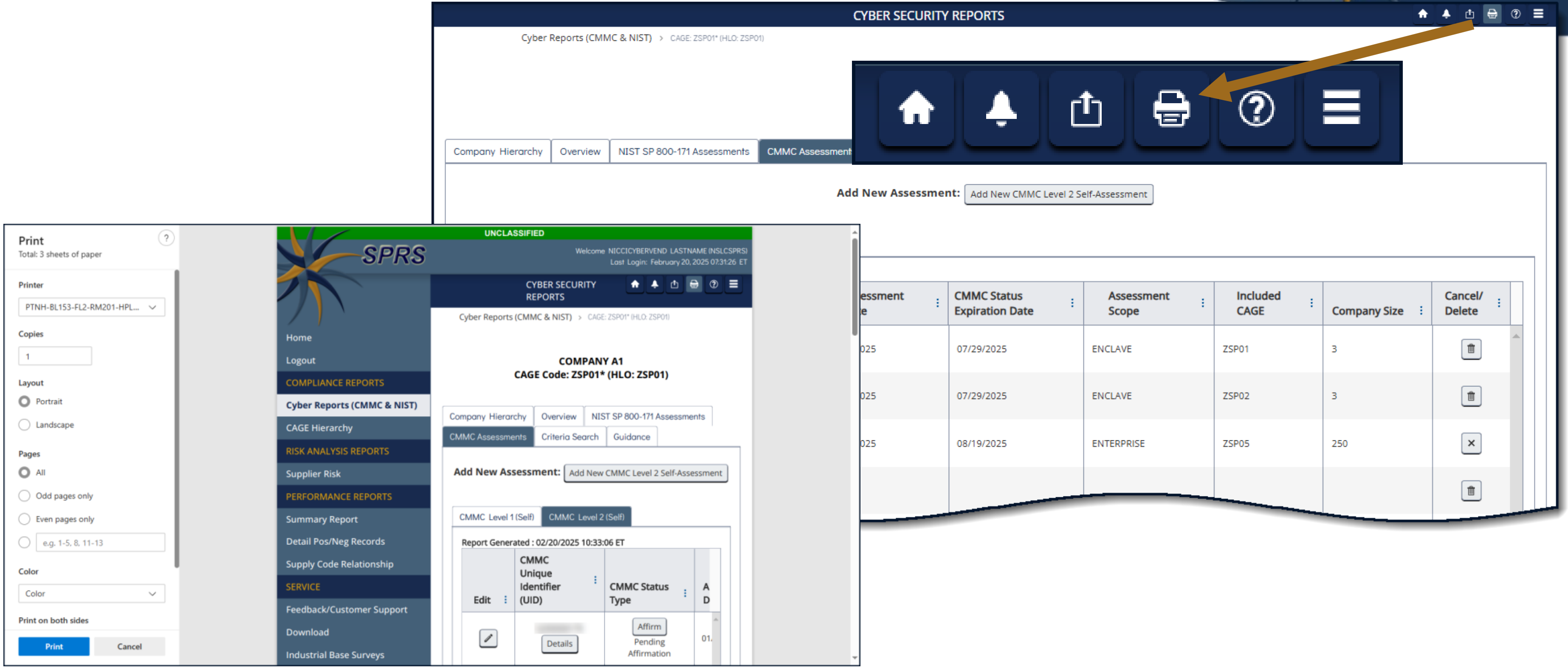
CMMC INFORMATION

- 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, including the CMMC Level 1 Scoping Guide, CMMC Level 1 Self-Assessment Guide, CMMC Level 2 Scoping Guide, and the CMMC Level 2 Assessment Guide can be found at: https://dodcio.defense.gov/cmmc/Resources-Documentation/
- Questions related to technical interpretation of these CMMC 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.
- Additional SPRS Resources:
  o CMMC Quick Entry Guide Level 1 (Self)
  o CMMC Quick Entry Guide Level 2 (Self)

NIST SP 800-171 INFORMATION

- SPRS is the database that holds NIST SP 800-171 assessment summary information. SPRS resources:
  o Cyber Reports (CMMC & NIST) Information
  o NIST SP 800-171 Quick Entry Guide
  o SPRS Access_Cyber Reports
- Preparation information including the NIST 800-171 Assessment Methodology can be found at the Defense Pricing and Contracting (DPC) Cyber page here.
- For assistance with NIST SP 800-171 assessment interpretation, deadlines, or requirements, please contact the Program Office or Contracting Officer for the contract in question. Defense Contract Management Agency (DCMA) general mailbox; DCMA_7012_Assessment_Inquiry@mail.mil
- Defense Federal Acquisition Regulation Supplement (DFARS) DFARS 252.204 (Sections -7012, -7019, and -7020)

Cyber Reports



CYBER SECURITY REPORTS

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

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

essment e	CMMC Status Expiration Date	Assessment Scope	Included CAGE	Company Size	Cancel/ Delete
025	07/29/2025	ENCLAVE	ZSP01	3	🗑
025	07/29/2025	ENCLAVE	ZSP02	3	🗑
025	08/19/2025	ENTERPRISE	ZSP05	250	✕
					🗑

Print
Total: 3 sheets of paper

Printer: PTNH-BL153-FL2-RM201-HPL...

Copies: 1

Layout
● Portrait
○ Landscape

Pages
● All
○ Odd pages only
○ Even pages only
○ e.g. 1-5, 8, 11-13

Color: Color

Print on both sides

UNCLASSIFIED

SPRS

Welcome NICCICYBERVEND LASTNAME (NSLCSPRS)
Last Login: February 20, 2025 07:31:26 ET

CYBER SECURITY REPORTS

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

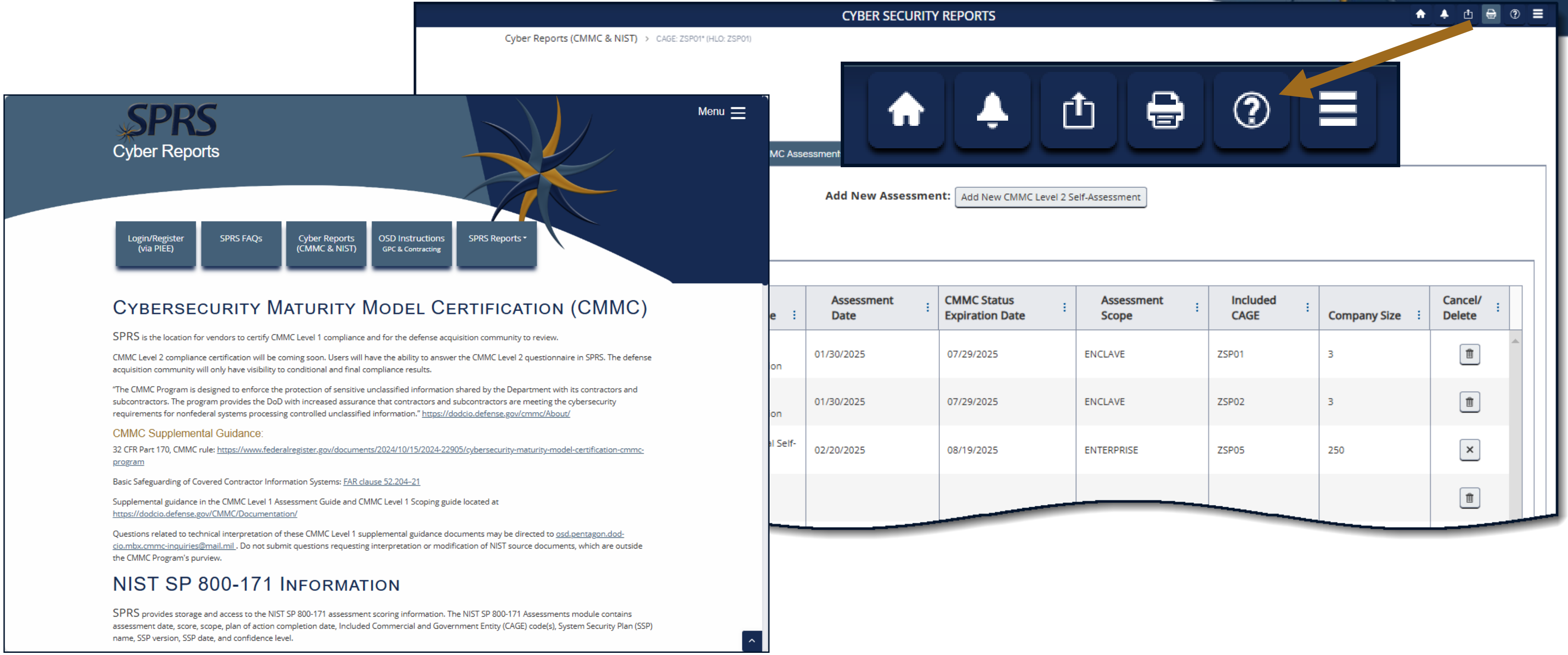
COMPANY A1
CAGE Code: ZSP01* (HLO: ZSP01)

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

Report Generated : 02/20/2025 10:33:06 ET

Edit	CMMC Unique Identifier (UID)	CMMC Status Type	A D
✎	[redacted] Details	Affirm Pending Affirmation	01.

Cyber Reports


CYBER SECURITY REPORTS
Cyber Reports (CMMC & NIST) › CAGE: ZSP01* (HLO: ZSP01)
MC Assessment
SPRS
Cyber Reports
Menu
Login/Register (via PIEE)
SPRS FAQs
Cyber Reports (CMMC & NIST)
OSD Instructions GPC & Contracting
SPRS Reports

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

e	Assessment Date	CMMC Status Expiration Date	Assessment Scope	Included CAGE	Company Size	Cancel/ Delete
on	01/30/2025	07/29/2025	ENCLAVE	ZSP01	3	🗑
on	01/30/2025	07/29/2025	ENCLAVE	ZSP02	3	🗑
l Self-	02/20/2025	08/19/2025	ENTERPRISE	ZSP05	250	✕
						🗑

Cybersecurity Maturity Model Certification (CMMC)

SPRS is the location for vendors to certify CMMC Level 1 compliance and for the defense acquisition community to review.

CMMC Level 2 compliance certification will be coming soon. Users will have the ability to answer the CMMC Level 2 questionnaire in SPRS. The defense acquisition community will only have visibility to conditional and final compliance results.

"The CMMC Program is designed 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." https://dodcio.defense.gov/cmmc/About/

CMMC Supplemental Guidance:

32 CFR Part 170, CMMC rule: https://www.federalregister.gov/documents/2024/10/15/2024-22905/cybersecurity-maturity-model-certification-cmmc-program

Basic Safeguarding of Covered Contractor Information Systems: FAR clause 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 provides storage and access to the NIST SP 800-171 assessment scoring information. The NIST SP 800-171 Assessments module contains assessment date, score, scope, plan of action completion date, Included Commercial and Government Entity (CAGE) code(s), System Security Plan (SSP) name, SSP version, SSP date, and confidence level.

SPRS Contact Information

SPRS Website:

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

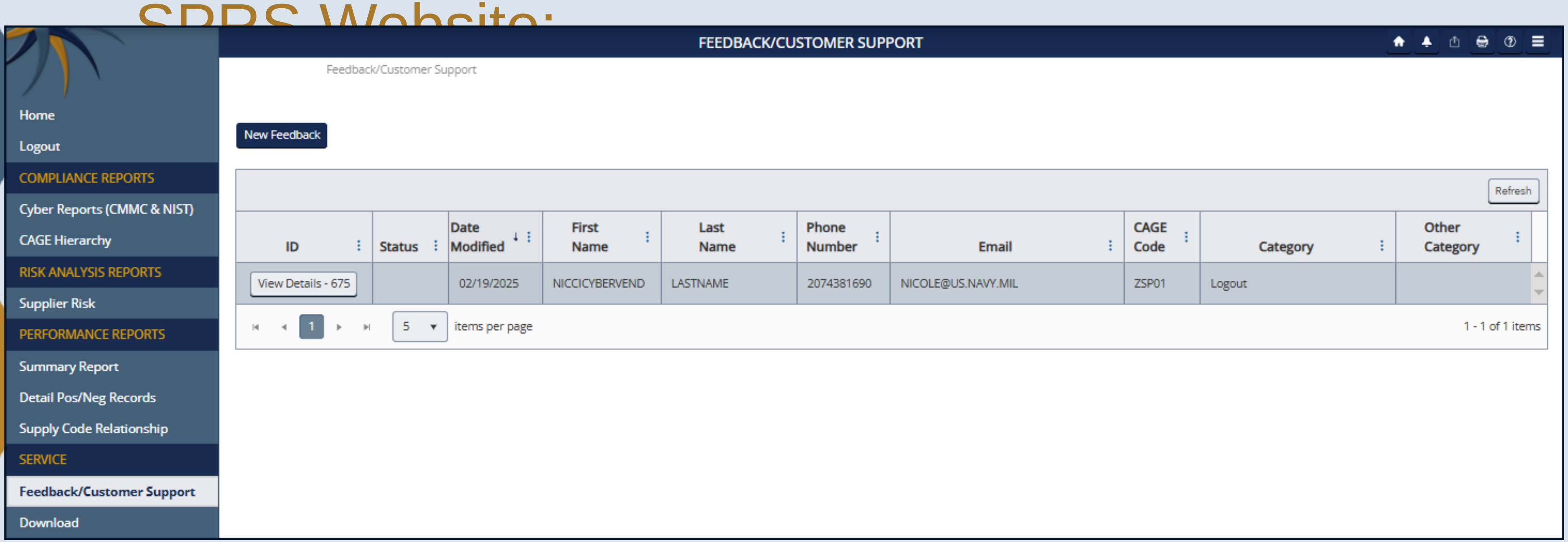
NSLC Help Desk (Mon-Fri 6:30am- 6:00pm ET):

NSLC Help Desk Email:

sprs-helpdesk@us.navy.mil

SPRS Contact Information

SPRS Website:



ID	Status	Date Modified	First Name	Last Name	Phone Number	Email	CAGE Code	Category	Other Category
View Details - 675		02/19/2025	NICCICYBERVEND	LASTNAME	2074381690	NICOLE@US.NAVY.MIL	ZSP01	Logout	

Thank you

for participating in the

CMMC Level 2

Entry Tutorial