

SPRS

Supplier Performance Risk System

SPRS Software User's Guide for
Awardees/Contractors

SPRS SOFTWARE USER'S GUIDE FOR
AWARDEES/CONTRACTORS



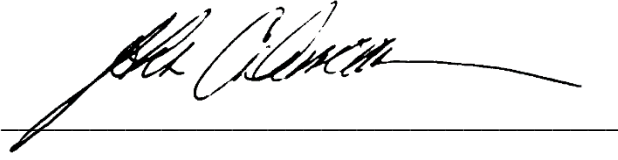
NSLC PORTSMOUTH BLDG. 153-2 PORTSMOUTH NAVAL SHIPYARD, PORTSMOUTH, NH 03804-5000

Approved for public release; distribution is unlimited

This page intentionally left blank.

SPRS 4 Document Acceptance

The undersigned agree this Supplier Performance Risk System (SPRS) Software User's Guide for Awardees/Contractors accurately describes the SPRS and the activities surrounding its development.

A handwritten signature in black ink, appearing to read "John C. Duncan", is written over a solid horizontal line.

John C. Duncan

Project Manager

Record of Versions and Changes

Document Version #	Version Date	Detailed Description of Change
1	MAR 2007	Baseline document
2	MAR 2009	Updates for V1.0.00134
3	SEP 2009	Updates for V2.0.0
4	SEP 2012	Updates for V2.2.13
5	MAY 2013	Updates for V2.2.17
6	JAN 2014	Updates for V2.2.18
7	MAR 2015	Updates for V2.2.25
8	NOV 2015	Updates for V3.0.0
9	JUN 2016	Updates for V3.2.002
10	DEC 2016	Updates for V3.2.3
11	JUL 2017	Updates for V3.2.5
12	OCT 2017	Updates for V3.2.6
13	JAN 2018	Updates for V3.2.7
14	OCT 2018	Updates for V3.2.8
15	MAY 2019	Updates for V3.2.9
16	AUG 2019	Updates for V3.2.10
17	MAR 2020	Updates for V3.2.11
18	SEP 2020	Updated Screenshots
19	OCT 2020	Updates for V3.2.12
20	MAR 2021	Updates for V3.2.14
21	SEP 2021	Updates for V3.3
22	JUL 2023	Updates for V3.3.10
23	JUL 2024	Updates for V4.0
24	DEC 2024	Updates for V4.0.2
25	FEB 2025	Updates for V4.0.3

Table of Contents

1.	WHAT IS SPRS?	6
1.1	Document Overview	6
1.2	SPRS Central Design Activity (CDA)	6
2.	ACCESSING SPRS	8
2.1	Minimum Software Requirements	8
2.2	Contractor/Vendor Access to SPRS	8
2.3	Accessing SPRS	9
3.	SPRS USER ROLES	11
3.1	Contractor/Vendor (Support Role):	11
3.2	SPRS Cyber Vendor User:	11
4.	WORKING IN SPRS	12
4.1	Navigating in SPRS.....	13
4.2	Toolbar in sprs	13
5.	COMPLIANCE REPORTS	14
5.1	CYBER REPORTS (CMMC & NIST)	14
5.2	CAGE Hierarchy.....	49
6.	RISK ANALYSIS REPORTS	50
6.1	Supplier Risk Report	50
7.	PERFORMANCE REPORTS	57
7.1	Summary Report	57
7.2	Detail Pos/Neg Records.....	64
7.3	Supply Code Relationship Report.....	68
8.	SERVICE	70
8.1	Feedback/Customer Support	70
8.2	Download	72
9.	TRAINING MATERIALS	74
	REFERENCED DOCUMENTS	76
	GLOSSARY	77
	SPRS USER ROLES	A
	TROUBLESHOOTING	B
	MENU ITEMS	C
	CHALLENGE PROCESS	D

Table of Figures

Figure 1: Finding Account Administrator in PIEE	8
Figure 2: PIEE LOG IN Header	10
Figure 3: SPRS Tile.....	10
Figure 4: Working Areas in SPRS (SPRS Application Landing Page) with Menu	12
Figure 5: Cyber Reports Landing Page.....	14
Figure 6: Cyber Reports Company Hierarchy Selection	15
Figure 7: Cyber Reports Company Hierarchy Tab	15
Figure 8: Cyber Reports Overview Tab.....	16
Figure 9: Cyber Reports Criteria Search Tab from Overview	16
Figure 10: Cyber Reports NIST SP 800-171 Assessments Tab.....	17
Figure 11: Cyber Reports NIST SP 800-171 Assessments Details Pop-up	18
Figure 12: Cyber Reports NIST SP 800-171 Red Assessment	19
Figure 13: Cyber Reports Column Sorting and Filtering.....	20
Figure 14: Cyber Reports NIST SP 800-171 Add New Assessment Button	20
Figure 15: Cyber Reports NIST SP 800-171 Enter Assessment Details.....	21
Figure 16: Cyber Reports NIST SP 800-171 Enter Assessment Details Open CAGE Hierarchy	22
Figure 17: Cyber Reports NIST SP 800-171 Enter Assessment Details Add Update Delete	23
Figure 18: Cyber Reports NIST SPT 800-171 Confirm Delete	24
Figure 19: Cyber Reports CMMC Assessment Tab	24
Figure 20: Cyber Reports CMMC Level 1 Self-Assessments Details Pop-up	26
Figure 21: Cyber Reports CMMC Level 1 Red Expire Assessment	26
Figure 22: Cyber Reports CMMC Column Sorting and Filtering	27
Figure 23: Cyber Reports Add New CMMC Level 1 Self-Assessment Button.....	27
Figure 24: Cyber Reports CMMC CAGE Hierarchy	28
Figure 25: Cyber Reports CMMC Save or Continue to Affirmation.....	29
Figure 26: Cyber Reports CMMC AO Email Sample	29
Figure 27: Cyber Reports CMMC Continue to Affirmation or Transfer to AO	30
Figure 28: Cyber Reports CMMC Assessment Details	30
Figure 29: Cyber Reports CMMC Certify and Affirm	31
Figure 30: Cyber Reports CMMC Edit an Assessment	32
Figure 31: Cyber Reports CMMC Delete an Assessment.....	32
Figure 32: Cyber Reports CMMC Level 2 Self-Assessments Details Pop-up	34
Figure 33: Cyber Reports CMMC Column Sorting and Filtering	35
Figure 34: Cyber Reports Add New CMMC Level 2 Self-Assessment Button.....	35
Figure 35: Cyber Reports Requirements in CMMC Level 2 Self-Assessment.....	36
Figure 36: Cyber Reports CMMC Level 2 Self Assessment Open Objectives	37
Figure 37: Cyber Reports Requirements in CMMC Level 2	38
Figure 38: Cyber Reports CMMC Level 2 Export	39
Figure 39: Cyber Reports CAGE(s) Stepper	39
Figure 40: Cyber Reports CMMC Level 2 CAGE Hierarchy.....	40
Figure 41: Cyber Reports CMMC Level 2 Score	41
Figure 42: Cyber Reports CMMC Level 2 Previous or Continue to Affirmation	42
Figure 43: Cyber Reports CMMC Level 2 Transfer to AO	42
Figure 44: Cyber Reports CMMC Level 2 Sample AO Email	43
Figure 45: Cyber Reports CMMC Continue to Affirmation.....	43
Figure 46: Cyber Reports CMMC Level 2 Assessment Details	44
Figure 47: Cyber Reports CMMC Level 2 Certify and Affirm	44
Figure 48: Cyber Reports CMMC Level 2 Edit an Assessment	45
Figure 49: Cyber Reports CMMC Level 2 Delete an Assessment	46
Figure 50: Cyber Reports CMMC Level 2 Cancel an Assessment.....	46

Figure 51: Cyber Reports CMMC Level 2 Annual Affirmation.....	47
Figure 52: Cyber Reports Criteria Search Tab	48
Figure 53: Cyber Reports Criteria Search tab Show Search fields	48
Figure 54: CAGE Hierarchy	49
Figure 55: Error on CAGE Hierarchy.....	49
Figure 56: Supplier Risk Report Request	50
Figure 57: Toggle Vendor Basic/Vendor Detail Supplier Risk	50
Figure 58: Supplier Risk Report	51
Figure 59: SPRS Color Legend	52
Figure 60: SPRS Color Legend Hover	52
Figure 61: Supplier Risk Color Tiles.....	53
Figure 62: Supplier Risk Factor Data	54
Figure 63: Quality Detail in Supplier Risk Tab	54
Figure 64: Supplier Risk Sort/Filter	55
Figure 65: Supplier Risk Contact for Information Link	55
Figure 66: Supplier Risk Contact for Information Pop-Up.....	56
Figure 67: Compliance Information	56
Figure 68: Contractor Summary Report Request.....	58
Figure 69: Summary Report	59
Figure 70: Summary Report Detail.....	60
Figure 71: Summary Report Detail.....	60
Figure 72: Summary Report Negative Detail	61
Figure 73: Summary Report Positive Detail	62
Figure 74: Contractor Detailed Report	63
Figure 75: Challenge Record Email.....	64
Figure 76: Detail Pos/Neg Records Report Request.....	65
Figure 77: Detail Negative Recordshi	66
Figure 78: Detail Report Positive Records	67
Figure 79: Supply Code Relationship Request	68
Figure 80: FSC/PSC to NAICS example.....	69
Figure 81: Feedback/Customer Support Window.....	70
Figure 82: Feedback/Customer Support Window.....	71
Figure 83: Feedback/Customer Support Submitted.....	71
Figure 84: Feedback/Customer Support Status.....	72
Figure 85: Export.....	72
Figure 86: Download module	73
Figure 87: SPRS Web Landing Page.....	74
Figure 88: SPRS Pop-Out Menu.....	75

1. WHAT IS SPRS?

Supplier Performance Risk System (SPRS) is a web-enabled enterprise application accessed through the Procurement Integrated Enterprise Environment (PIEE), <https://piee.eb.mil/>. SPRS (pronounced spurz) gathers, processes, and displays data about the performance of suppliers. SPRS is the Department of Defense's (DoD) single, authorized application to retrieve suppliers' performance information. (DoDI 5000.79)

SPRS alerts procurement specialists to Federal Supply Classification/Product Service Code (FSC/PSC) item-specific risks. SPRS's Supplier Risk Score provides procurement specialists with a composite score that considers each supplier's performance in the areas of product delivery and quality. The quality and delivery classifications identified for a supplier in SPRS may be used by the contracting officer to evaluate a supplier's performance. DFARS 204.76 "...provides policies and procedures for use of the Supplier Performance Risk System (SPRS) risk assessments in the evaluation of a quotation or offer."

SPRS provides storage and retrieval for the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 and the Cybersecurity Maturity Model Certification (CMMC) assessment results.

Suppliers/Vendors may view their own company information in SPRS.

1.1 DOCUMENT OVERVIEW

This software user's guide provides instructions and step-by-step procedures for SPRS functionality. It describes procedures for gaining access to SPRS, obtaining reports, providing feedback, and getting help. SPRS data is considered unclassified for contractors and vendors. Vendors can view, maintain, download and distribute their own data. The U.S. Government handles all SPRS data as Controlled Unclassified Information (CUI). A list of referenced links, glossary of acronyms, troubleshooting guide and other helpful appendices are available at the end of the document. Dissemination of this document is approved for public release with unlimited distribution. The content of all data files referenced within this are sensitive but unclassified; many are controlled by the Privacy Act of 1974.

For scoring information, refer to the SPRS Evaluation Criteria Manual located on the SPRS Reference Material page, <https://www.sprs.csd.disa.mil/reference.htm>.

For guidance on how SPRS risk analysis is used in the DoD acquisition process refer to the relevant agency, Contracting Officer or Contracting Specialist.

1.2 SPRS CENTRAL DESIGN ACTIVITY (CDA)

Naval Sea Logistics Center (NSLC) Portsmouth is the SPRS Central Design Activity that develops, designs, and maintains the SPRS application. The CDA will:

- Maintain SPRS software

- Maintain SPRS documentation
- Provide training and documentation to activity personnel
- Provide Customer Support Center to answer customer questions
- Respond to reported questions and/or problems in SPRS
- Provide technical expertise in SPRS application administration and processing
- Ensure SPRS databases contain up-to-date and accurate information

2. ACCESSING SPRS

This section discusses how to obtain access to the SPRS application and how to work within SPRS.

2.1 MINIMUM SOFTWARE REQUIREMENTS

SPRS fully supports the latest major desktop version of Chrome, Firefox, and Edge. Older browsers may still view SPRS, however users should expect mixed results. A "major version" refers to a full numeric release, like 9.0 and 10.0 (not minor releases like 9.2.x and 10.2.x). Accessing SPRS on an iOS device may also produce mixed results, desktop web browser is recommended to ensure no functionality impacts.

2.2 CONTRACTOR/VENDOR ACCESS TO SPRS

Detailed instructions are available at the [Supplier/Vendor Access](#) instructions link on the SPRS website Menu, located here:

<https://www.sprs.csd.disa.mil/access.htm>. Here is an overview with key points:

SPRS uses the Procurement Integrated Enterprise Environment (PIEE) platform for login verification and security. The user type when registering should always be 'Vendor'. PIEE requires each vendor/company to be registered in the System for Award Management (SAM) www.sam.gov, and have at least one PIEE Contractor Administrator (CAM) to control user access for the company.

The CAM is the Electronic Business point of contact (EBPOC) for the company listed in SAM or a designee. CAMs request the 'Administrator User' role in PIEE. Once the CAM has received access, they can then grant access to other company users and request additional roles for themselves. If there is only one CAM, the CAM will require PIEE to activate the CAM request and any additional roles.

To identify the CAM registered for the company, select the "Find my Account Administrator" button on the PIEE login page.

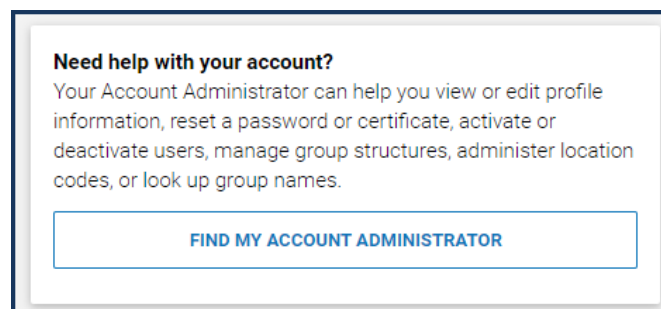


Figure 1: Finding Account Administrator in PIEE

PIEE will not allow the user requesting a role to proceed without a CAM beyond step (5), Roles. An error message will identify the eligible EBPOC(s) registered

in SAM if one exists.

For more information about creating an account for the first time in PIEE refer to their "Vendors - Getting Started Help" page.

<https://piee.eb.mil/xhtml/unauth/web/homepage/vendorGettingStartedHelp.xhtml>

Complete PIEE General Steps.

SPRS Access - PIEE Registration for SPRS:

1. Select SPRS from dropdown application list
2. Select the Role:
 - a. **Contractor/Vendor (Support Role)** - allows the user to monitor company performance data, CAGE Hierarchy, and view the CMMC and NIST SP 800-171 Assessment results data.
 - b. **SPRS Cyber Vendor User** - allows the user to add and edit their CMMC/NIST SP 800-171 Assessment results data and monitor CAGE hierarchy.
3. Click "+Add Roles" button
4. Enter Location Code/CAGE (Commercial and Government Entity code) for the company.

Repeat Steps 1-4 to select multiple Roles or multiple CAGEs before moving on to complete the registration. Access to one CAGE in a CAGE hierarchy will provide access to all CAGEs in that hierarchy with the SPRS Cyber Vendor User role.

User role requests must be activated by the CAM to allow access to SPRS.

NOTE: *If there is only one CAM, and that CAM is requesting a role, the CAM will require PIEE to activate any role request(s).*

2.3 ACCESSING SPRS

Once access has been granted via the single sign-on capability in PIEE, access to SPRS is available.

To Access SPRS:

- Open a browser session
- PIEE landing page: <https://piee.eb.mil>
- Click "log-in" and follow prompted log-in steps

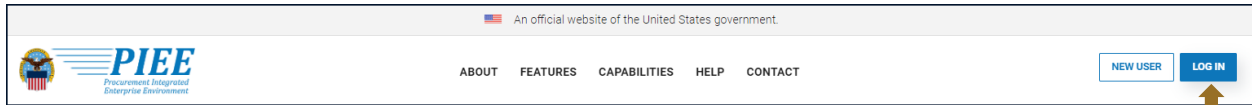


Figure 2: PEE LOG IN Header (As of FEB 2025)

Select the SPRS Tile:



Figure 3: SPRS Tile

3. SPRS USER ROLES

Two (2) basic user types may access SPRS, Vendor and Government. This section describes the Vendor User type roles. An overview of the roles and application access for each is contained in **Appendix A: SPRS USER ROLES**.

3.1 CONTRACTOR/VENDOR (SUPPORT ROLE):

- View company reports (including Cyber Reports)
- View CAGE Hierarchy Report
- Process Challenges

3.2 SPRS CYBER VENDOR USER:

- Add/Edit/View Cyber Reports Assessment results
- View CAGE Hierarchy Report

4. WORKING IN SPRS

SPRS Application Landing Page:

- SPRS uses two work areas: the menu, and the working window. Selecting a menu item will populate the working window. On the SPRS landing screen there is an additional area, user news, available at login and by clicking Home in the toolbar - this area is updated with each publish
- For security purposes, the system will log out users that have been inactive for longer than 15 minutes. A three (3) minute warning will appear to prompt user to continue working within SPRS/PIEE.



The screenshot displays the SPRS Application Landing Page. On the left is a dark blue sidebar menu with categories: HOME, LOGOUT, COMPLIANCE REPORTS (with sub-items: Cyber Reports (CMMC & NIST), CAGE Hierarchy), RISK ANALYSIS REPORTS (with sub-item: Supplier Risk), PERFORMANCE REPORTS (with sub-items: Summary Report, Detail Pos/Neg Records, Supply Code Relationship), and SERVICE (with sub-items: Feedback/Customer Support, Download, Industrial Base Surveys). The main content area features the SPRS logo, a welcome message, a list of recommended browsers, and sections for NIST SP 800-171/CMMC and HELP. A 'SPRS Session Expiration' dialog box is overlaid on the right, indicating a 2:58 timeout and offering 'Yes, Continue Session' and 'No, Sign Out' options. Three callout bubbles are present: '1' points to the menu, '2' points to the user news area, and '3' points to the HELP section.

Figure 4: Working Areas in SPRS (SPRS Application Landing Page) with Menu and Expiration window

NOTE: SPRS menu items, buttons, and controls within SPRS work areas are used to navigate the application. It is recommended not to use the Back or Forward in the browser toolbar.

4.1 NAVIGATING IN SPRS







The Menu, grouped in sections, allows the following actions:

-  – Click to open the SPRS web page for general information including training and reference materials
- **Home** – Click to return to the SPRS application landing screen
- **Logout** – Click to log out of the SPRS application (not PIEE)
- **Compliance Reports** – Click any link to review SPRS reports
- **Risk Analysis Reports** – Click any link to review SPRS reports
- **Performance Reports** – Click any link to review SPRS reports
- **Service** – Click Feedback/Customer Support to submit feedback
-  **Information button** – Click for additional definitions and information

NOTE: *Help Desk email is at the bottom of every page.*

4.2 TOOLBAR IN SPRS

The Toolbar is an icon-based list located in the upper right hand side of the header. It includes quick links, export, and print functions as described below:

-  **Home** – Click to return to the SPRS application landing screen
-  **Feedback** – Click to go to Feedback module, icon will reflect if there is a response waiting for review
-  **Export** – Click to Export to Excel the current report to the Download module on the Menu
-  **Print** – Click to print or save as PDF information on the current screen
-  **Information** – Click to open a tab to the SPRS main website
-  **Menu** – Click to hide the left-hand menu or to have it reappear

5. COMPLIANCE REPORTS

Compliance Reports allow users to review SPRS information. This module contains information required by the Defense Federal Acquisition Regulation Supplement, DFARS 252.204.

5.1 CYBER REPORTS (CMMC & NIST)

The Cyber Reports module allows Vendors access to their CMMC and NIST SP 800-171 Assessments. Depending on access level, the Cyber Reports module enables vendors to view and/or maintain implementation of CMMC Level 1, CMMC Level 2, and NIST SP 800-171.

There are two roles that provide access to this module:

- **Contractor Vendor (Support Role)** – view-only CMMC and NIST SP 800-171 Assessments for the CAGE authorized in PIEE and any CAGE(s) below (subsidiaries).
- **SPRS Cyber Vendor User** – a privileged role required to enter and edit Basic NIST SP 800-171 and CMMC assessment records for the CAGE authorized in PIEE, and any that share the same hierarchy (HLO).

Guidance for obtaining Contractor Vendor or SPRS Cyber Vendor User role Access, found here: <https://www.sprs.csd.disa.mil/access.htm>

To access CMMC and NIST SP 800-171 Assessments:
Select the [Cyber Reports \(CMMC & NIST\)](#) from the menu.

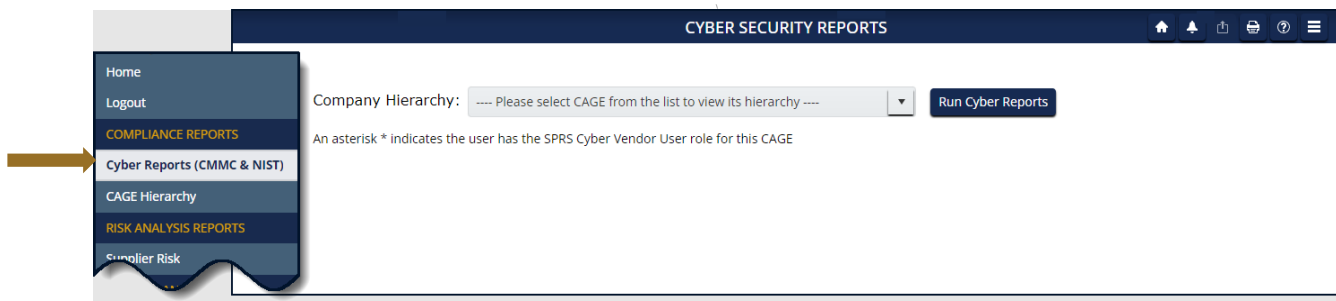


Figure 5: Cyber Reports Landing Page

Select the desired CAGE and hierarchy combination from the dropdown and click the **Run Cyber Reports** button. The first CAGE displayed is the CAGE that is associated with the user's PIEE profile. The CAGE in parenthesis is the Highest Level Owner (HLO), the hierarchy, reported to SPRS for that CAGE.

An asterisk * indicates the user has the SPRS Cyber Vendor User role (access to add/edit) for this CAGE/Hierarchy.

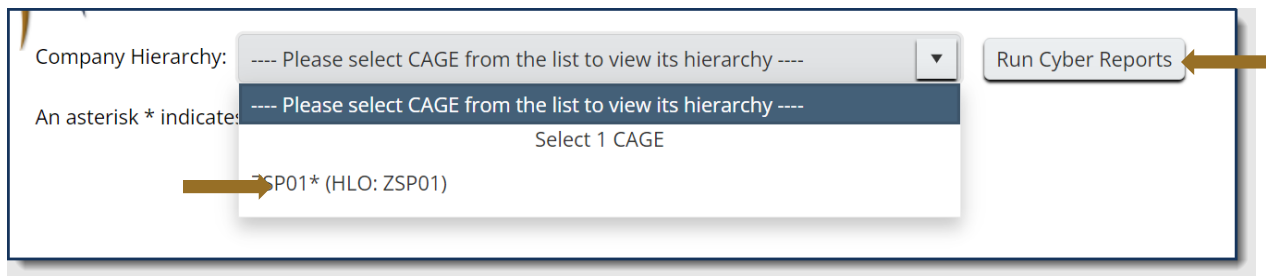


Figure 6: Cyber Reports Company Hierarchy Selection

The Company name and CAGE code selected from the dropdown will be listed at the top of the report page.

The report is divided by tabs: Company Hierarchy, Overview, NIST SP 800-171 Assessments, CMMC Assessments, Criteria Search, and Guidance.

The **Company Hierarchy** tab displays the company's complete hierarchy. SPRS imports CAGE hierarchy data from SAM via CAGE DLA. If the Corporate CAGE hierarchy is not accurate, contact the Electric Business Point of Contact (EBPOC) for the CAGE listed at <https://sam.gov> to request correction. CAGE hierarchy information flows from SAM to SPRS.

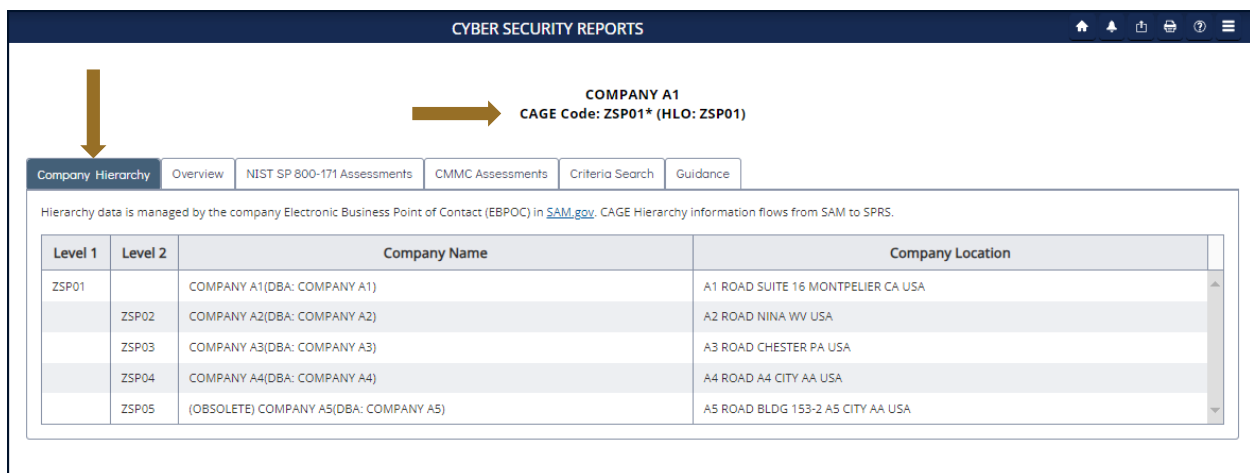


Figure 7: Cyber Reports Company Hierarchy Tab

The **Overview** tab displays the CAGE(s), within the hierarchy, that have NIST assessments. Only CAGE(s) that have assessments, and that the user has access to view, will show within this tab. The linked number indicates how many assessments for that CAGE and confidence level combination exist that are less than three (3) years old from the logged assessment date. A bracketed zero [0] indicates that all associated assessment(s) are more than three (3) years from logged assessment date.

NOTE: If a CAGE is missing from the hierarchy, contact the Electric Business Point of Contact (EBPOC) listed in the SAM registration for the CAGE at the website listed here: <https://sam.gov/content/home>.

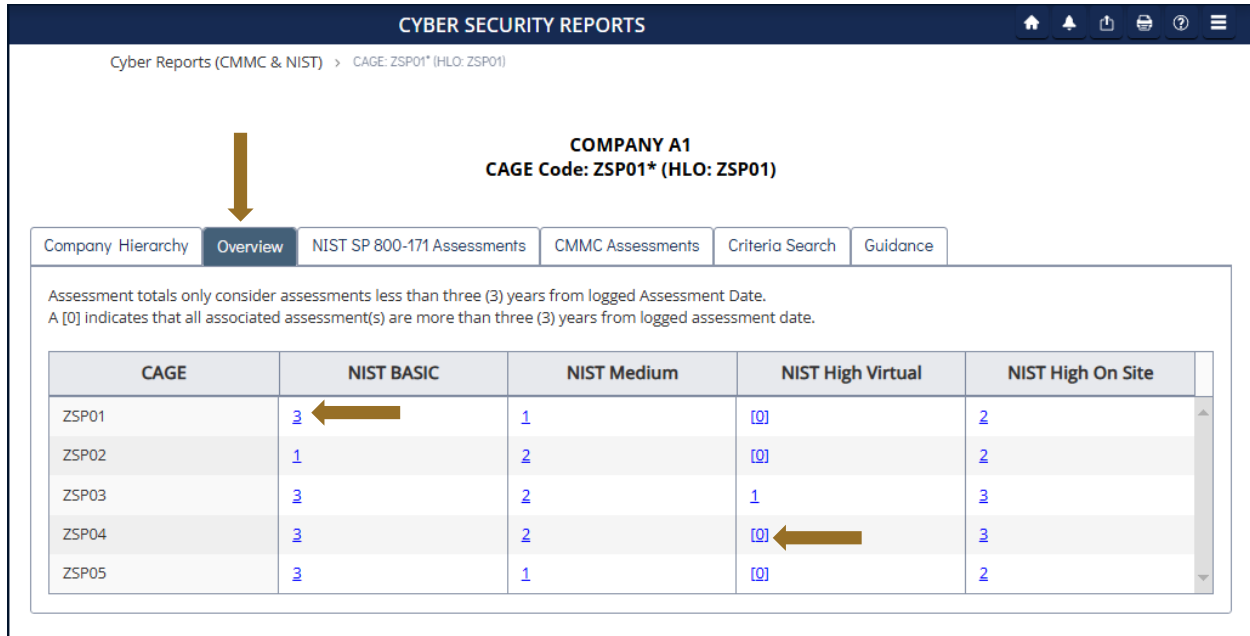


Figure 8: Cyber Reports Overview Tab

Clicking on the linked number/bracketed zero will bring the user to the **Criteria Search** tab with that CAGE pre-populated in the search criteria, the related confidence level tab opened, the search executed, and results listed below.

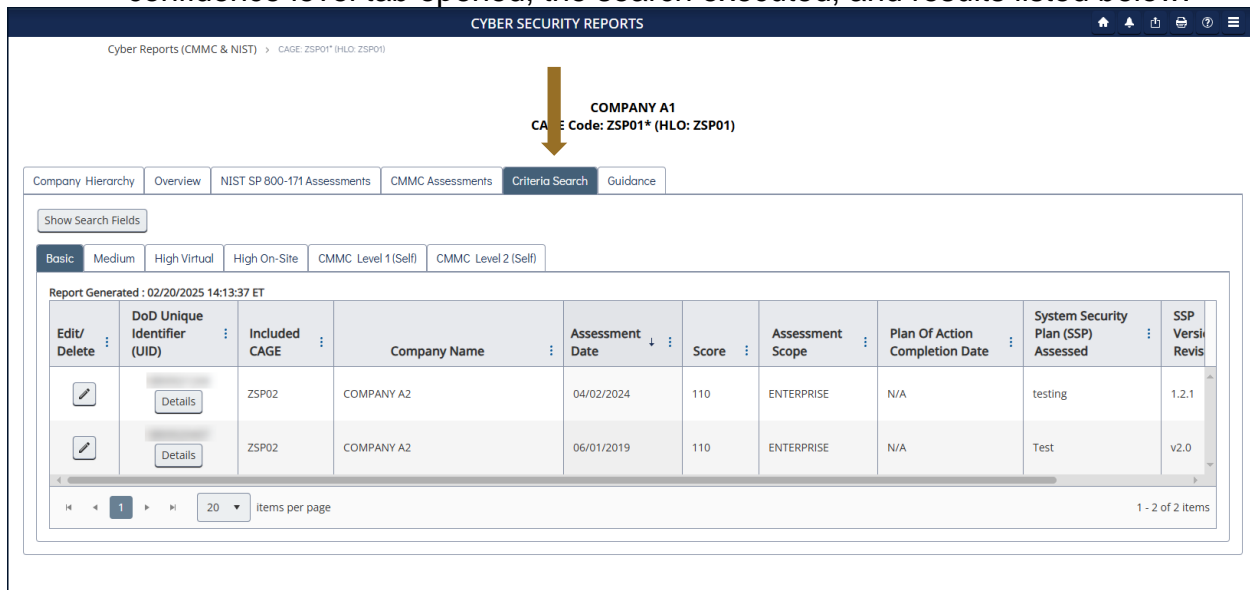


Figure 9: Cyber Reports Criteria Search Tab from Overview

The **NIST SP 800-171 Assessments** tab displays logged assessment summary results. If the user has a SPRS Cyber Vendor User role, they will have an **Add New NIST Assessment** button as well as an **Edit/Delete** column with pencil icons. Users with Contractor Vendor (view-only) will not see those items.

There are 4 tabs within the **NIST SP 800-171 Assessments** tab. These are the assessment confidence levels. NIST SP 800-171 assessment results fall into four (4) confidence level categories. Select each tab to view the logged assessments for the related confidence level:

- High On-site (conducted by DoD)
- High Virtual (conducted by DoD)
- Medium (reviewed by DoD)
- Basic (Contractor self-assessments)

The Basic Confidence Level is the only assessment that can be maintained (add/edit/delete) by vendors.

Report Generated : 02/20/2025 14:33:59 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	SSP Date
	Details	ZSP02	COMPANY A2	06/01/2019	110	ENTERPRISE	N/A	Test	v2.0	06/01/2018
	Details	ZSP01	COMPANY A1	08/01/2020	102	ENCLAVE	02/02/2022	Company A		08/01/2020
	Details	ZSP03	COMPANY A3	12/26/2023	99	CONTRACTS	12/31/1969			
	Details	ZSP05	COMPANY A5	12/26/2023	99	CONTRACTS	12/31/1969			
	Details	ZSP04	COMPANY A4	12/26/2023	99	CONTRACTS	12/31/1969			

1 - 5 of 12 items

Figure 10: Cyber Reports NIST SP 800-171 Assessments Tab

NIST SP 800-171 Assessment Summary results include the following information:

- **DoD Unique Identifier (UID)** – a 10-digit alphanumeric identifier automatically assigned to each newly saved assessment. The first two letters delineate the confidence level of the assessment. Basic, Medium, and High confidence levels start with SB, SM, SH respectively.
- **Included CAGE** – Indicates that CAGE is included in the assessment and considered assessed.
- **Company Name** – Company Name as defined by CAGE DLA.

- **Assessment Date** – The date of the most recent assessment conducted.
- **Score** – The Score of the assessment conducted.
- **Assessment Scope** – There are three selections for scope:
 - Enterprise – Entire Company’s network under the CAGEs listed
 - Enclave – Standalone under Enterprise CAGE as business unit (test enclave, hosted resources, etc.)
 - Contract – Contract specific SSP review
- **Plan of Action Completion Date** – Estimated date that all identified deficiencies will be resolved.
- **System Security Plan (SSP) Assessed** – The name of the System Security Plan that was assessed.
- **SSP Version/Revision** – The version of the System Security Plan that was assessed.
- **SSP Date** – The Date of the System Security Plan assessed.
- **Assessing CAGE or DoDAAC** – Exclusive to Medium and High Confidence Level assessments. The CAGE or DoDAAC of the assessor.
- **DFARS 252.204-7012 Compliance** – Exclusive to High On-Site Confidence Level assessment. If “Yes”, it indicates that the DFARS 252.204-7012 clause requirements are met. If “No”, contact the assessing DoDAAC for details.

Selecting the **Details** button opens a pop-up that contains a print friendly display of all information associated with that Unique Identifier (UID). To download select **Save As PDF**.

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

Hierarchy

Medium

Generated :

Do Ide (UI

Of Actio completion D

2025

2024

SB00021244

Details

ZSP05

COMPANY A5

04/02/2024

110

ENTERPRISE

N/A

NIST SP 800-171 Assessment Details

Report Generated: 02/20/2025 14:12:51 ET

Assessment Standard: NIST SP 800-171
Confidence Level: BASIC

Assessment Score: 110
Plan of Action Completion Date: N/A

DoD Unique Identifier (UID): [REDACTED]
Assessment Date: 04/02/2024
Assessing Scope: ENTERPRISE

System Security Plan Assessed: testing
System Security Plan Version/Revision: 1.2.1
System Security Plan Date: 04/02/2024

Included CAGEs/entities:

CAGE	Company Name	Address
ZSP01	COMPANY A1	A1 ROAD SUITE 16, MONTPELIER, CA, USA
ZSP02	COMPANY A2	A2 ROAD, NINA, WV, USA
ZSP03	COMPANY A3	A3 ROAD, CHESTER, PA, USA
ZSP04	COMPANY A4	A4 ROAD, A4 CITY, AA, USA
ZSP05	COMPANY A5	A5 ROAD BLDG 153-2, A5 CITY, AA, USA

Figure 11: Cyber Reports NIST SP 800-171 Assessments Details Pop-up

Assessments results turn red when the assessment date expands beyond three (3) years.

The screenshot shows the 'CYBER SECURITY REPORTS' interface. At the top, it displays 'COMPANY A1' and 'CAGE Code: ZSP01* (HLO: ZSP01)'. Below this are navigation tabs: 'Company Hierarchy', 'Overview', 'NIST SP 800-171 Assessments', 'CMMC Assessments', 'Criteria Search', and 'Guidance'. A button 'Add New Assessment: Add New NIST Assessment' is visible. The main content area shows a table of assessments with the following data:

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	SSP Date
		ZSP02	COMPANY A2	06/01/2019	110	ENTERPRISE	N/A	Test	v2.0	06/01/2018
		ZSP01	COMPANY A1	08/01/2020	102	ENCLAVE	02/02/2022	Company A		08/01/2020
		ZSP03	COMPANY A3	12/26/2023	99	CONTRACTS	12/31/1969			
		ZSP05	COMPANY A5	12/26/2023	99	CONTRACTS	12/31/1969			
		ZSP04	COMPANY A4	12/26/2023	99	CONTRACTS	12/31/1969			

At the bottom of the table, there is a pagination control showing '1' of 5 items per page and '1 - 5 of 12 items'.

Figure 12: Cyber Reports NIST SP 800-171 Red Assessment

Sort and filter columns to search for specific data by using the three-vertical dots and selecting various methods of sorting. The **Clear** button will reset all selected filters.

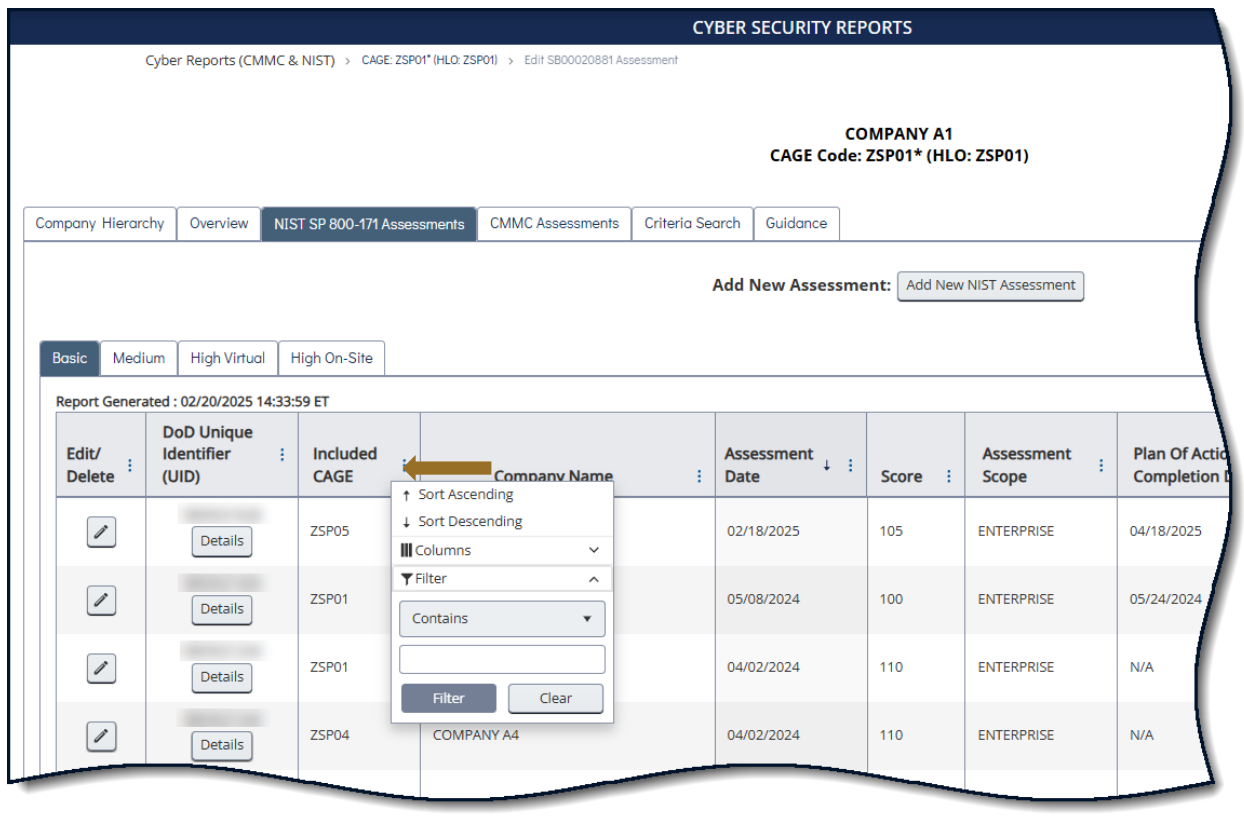


Figure 13: Cyber Reports Column Sorting and Filtering

To add an assessment, users must have the SPRS Cyber Vendor User role.

Select the **Add New NIST Assessment** button, enter the required information, and select **Save**.



Figure 14: Cyber Reports NIST SP 800-171 Add New Assessment Button

CYBER SECURITY REPORTS

COMPANY A1
CAGE Code: ZSP01* (HLO: 8V615)
Confidence Level: BASIC
Assessment Standard: NIST SP 800-171

Back

Enter Assessment Details

Assessment Date:
MM/DD/YYYY

Assessment Score:
[Text Input]

Assessing Scope:
--Select--

Plan of Action Completion Date:
MM/DD/YYYY

System Security Plan (SSP) Assessed:
Document Name

SSP Version/Revision:
[Text Input]

SSP Date:
MM/DD/YYYY

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

Save

Figure 15: Cyber Reports NIST SP 800-171 Enter Assessment Details

The **Open CAGE Hierarchy** button opens the CAGE tree, allowing users to select which CAGEs are included/assessed CAGEs. Users can also copy and paste a comma-delimited list of CAGEs into the CAGE text box provided.

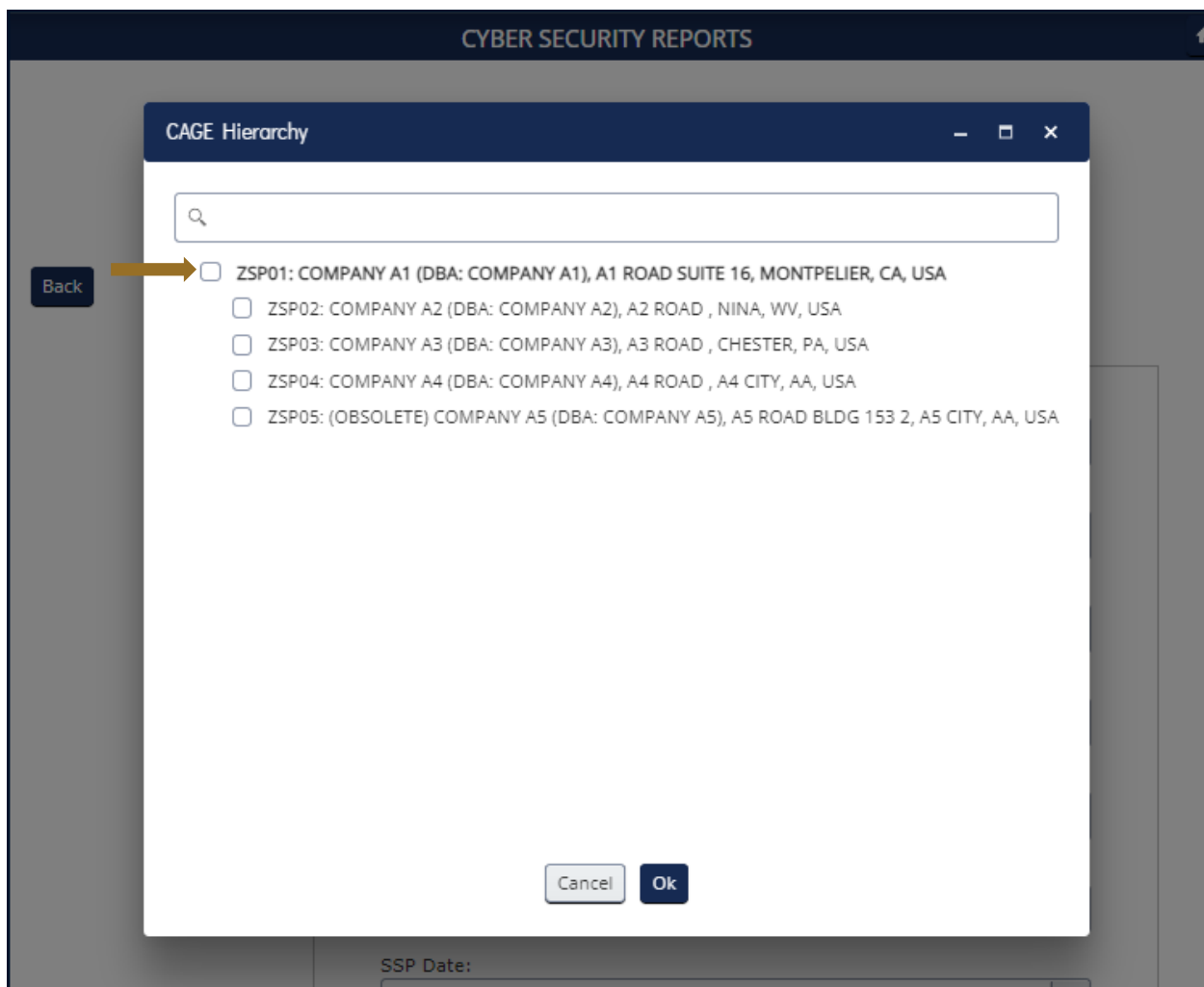


Figure 16: Cyber Reports NIST SP 800-171 Enter Assessment Details Open CAGE Hierarchy

Assessment results entered will populate the entry fields. To revise or update the assessment information, update the information within the fields and select the **Update** button. Select the **Back** button to go back.

The **Edit/Delete** pencil icon will also bring the user to the Enter Assessment Details screen with the details populated. To edit, update the information within the fields and select the **Update** button.

To add additional assessments, select the **Clear and Add Additional Assessment(s)** button. This will clear the fields and allow users to enter additional assessments. Clearing the fields does not delete the previously entered assessment.

CYBER SECURITY REPORTS

Cyber Reports (CMMC & NIST) > CAGE: ZSP01* (HLO: ZSP01) > Edit SB00021626 Assessment

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):

➔

DoD Unique Identifier (UID)	Included CAGE	Company Name	Assessment Date	Score	Assessment Scope	Plan Of Action Completion Date	Sys. Plat. Ass.
<input type="button" value="Details"/>	ZSP05	COMPANY AS	02/18/2025	105	ENTERPRISE	04/18/2025	Alp

Figure 17: Cyber Reports NIST SP 800-171 Enter Assessment Details Add Update Delete

To delete an assessment, select the **Delete** button. This will open a pop-up of the complete assessment details with a warning to confirm deletion. Deleting the assessment will delete it for all Included CAGEs. Select **Confirm Delete** to delete.

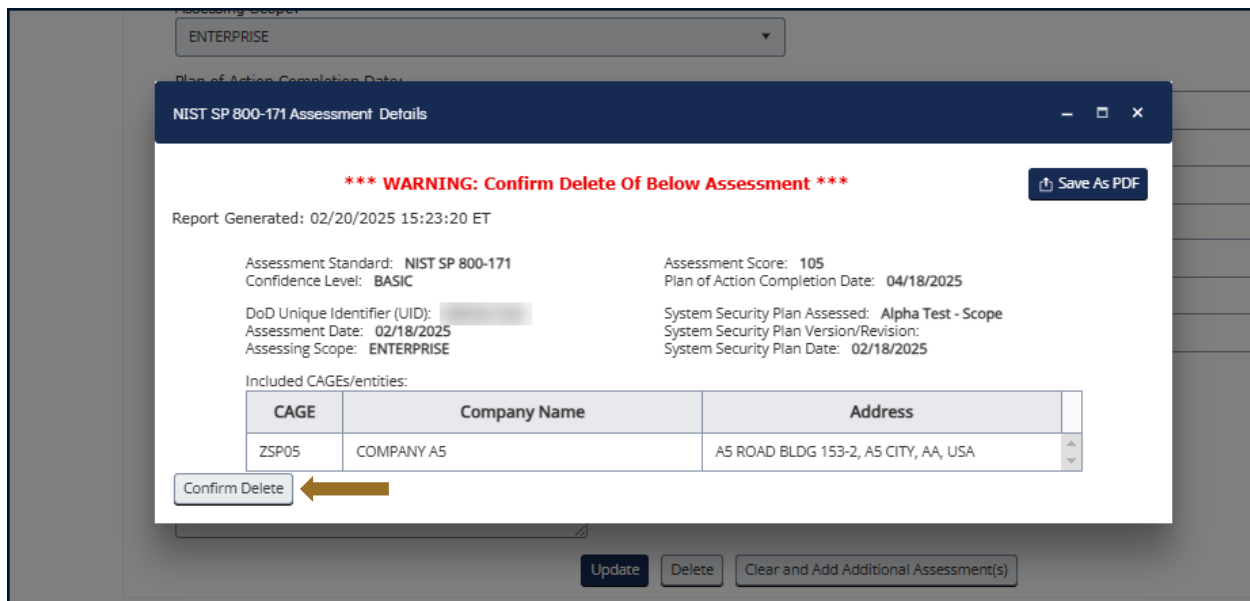


Figure 18: Cyber Reports NIST SPT 800-171 Confirm Delete

The **NIST SP 800-171 Quick Entry Guide** provides summary level instructions on entering and editing summary assessment results. These instructions are located on the SPRS web page:

<https://www.sprs.csd.disa.mil/pdf/NISTSP800-171QuickEntryGuide.pdf>

The **CMMC Assessments** tab displays logged assessments. Tabs in the summary area identify the CMMC Levels for viewing. If the user has a SPRS Cyber Vendor User role, they will have visibility of an **Add New CMMC Level 1/Level 2 Self-Assessment** button. As well as Edit (pencil icon) and Cancel/Delete (“x”/trashcan icon) functions for specific CMMC Status Types.

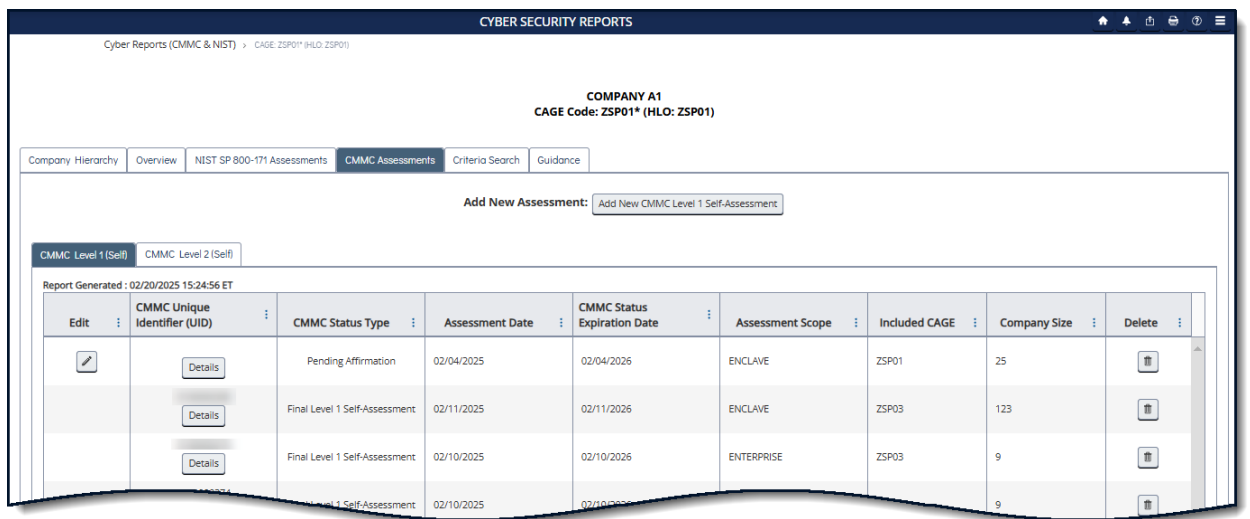


Figure 19: Cyber Reports CMMC Assessment Tab

CMMC Level 1 (Self) Summary results include the following information:

- **CMMC Unique Identifier (UID)** – a 10-digit alphanumeric identifier automatically assigned to each newly saved assessment. The first two letters delineate the CMMC Status Type. Level 1 and Level 2 Self-Assessments have prefix S1 and S2 respectively. Level 2 and Level 3 Assessments will observe prefix L2 and L3.
- **CMMC Status Type** – The status of the Assessment
 - Incomplete
 - Pending Affirmation – Indicates that a record has been completed but is waiting for the AO to affirm
 - Final Level 1 Self-Assessment – Indicates the assessment met requirements and is visible to government personnel
 - No CMMC Status – Indicates the assessment was completed but “No” was identified under the question “Are you compliant with each of the security requirements specified in FAR clause 52.204-21?”
 - No CMMC Status (Expired Assessment) – Indicates an expired “Final Level 1 Self-Assessment”
- **Assessment Date** – The date the Assessment was conducted
- **CMMC Status Expiration Date** – The assessment expiration date; a Level 1 self-assessment is considered valid for one year from Assessment Date
- **Assessment Scope** – There are two selections for scope:
 - Enterprise – an organization with a defined mission/goal and a defined boundary, using information systems to execute that mission, and with responsibility for managing its own risks and performance
 - Enclave – a set of system resources that operate in the same security domain and that share the protection of a single common continuous security perimeter (NIST)
- **Included CAGE** – List of all CAGE Codes included in the assessment scope
- **Company Size** – Total of employees at all locations of the organization

Selecting the **Details** button opens a pop-up that contains a print friendly display of all information associated with that Unique Identifier (UID). To download select **Save As PDF**.

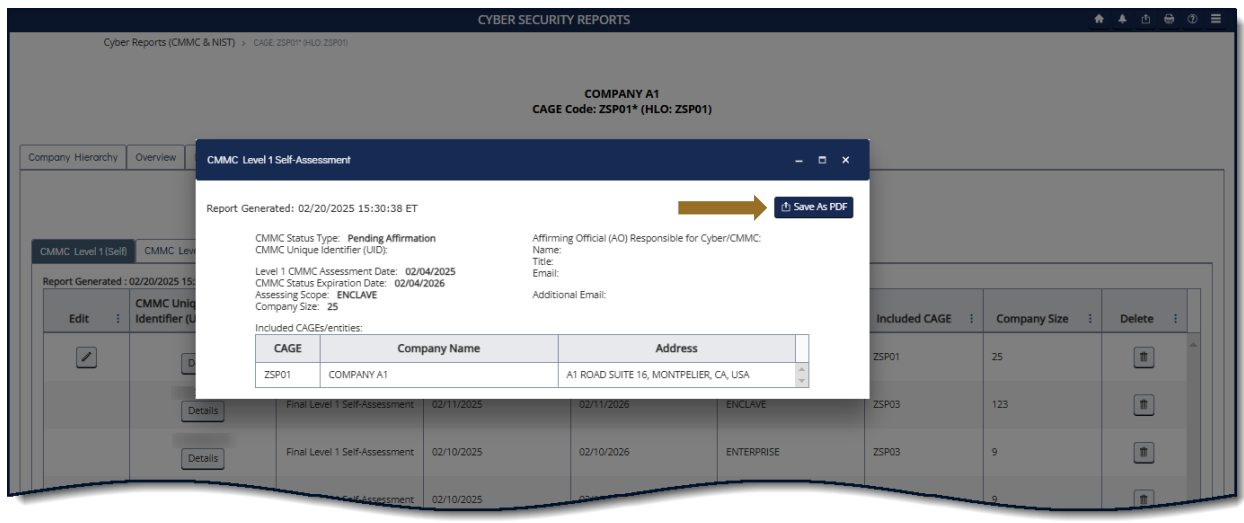


Figure 20: Cyber Reports CMMC Level 1 Self-Assessments Details Pop-up

A Level 1 Self-Assessment will automatically become “No CMMC Status (Expired Assessment)” after one year, turn red, and will no longer be visible to Government personnel.

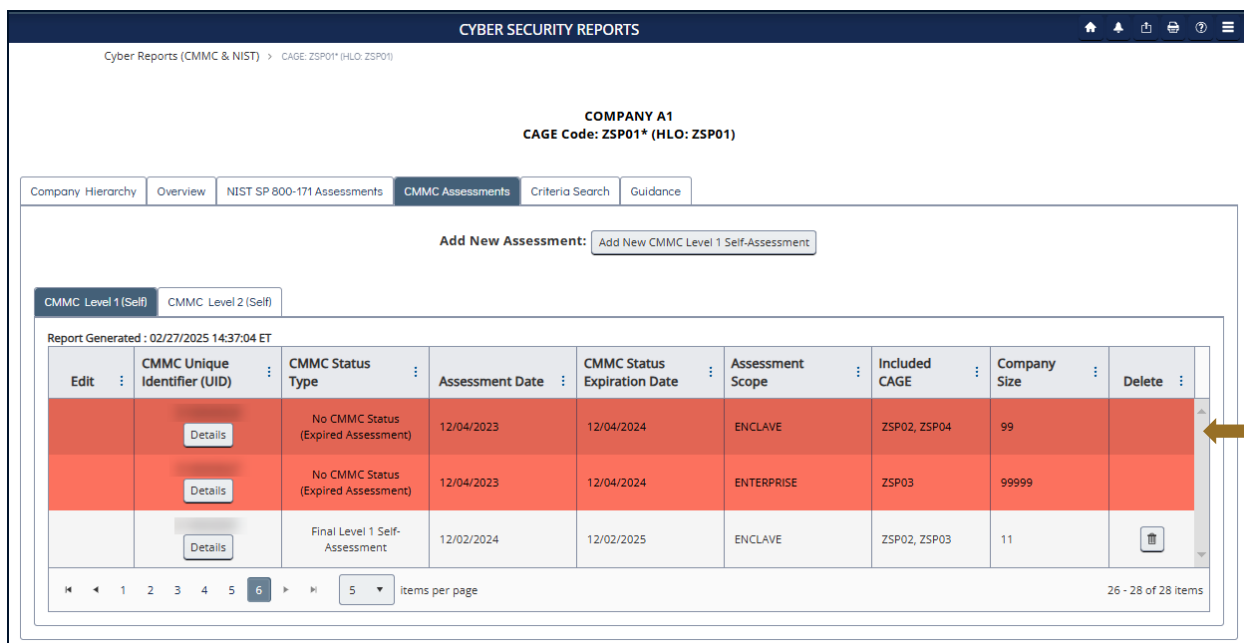


Figure 21: Cyber Reports CMMC Level 1 Red Expired Assessment

Sort and filter columns to search for specific data by using the three-vertical dots and selecting various methods of sorting.

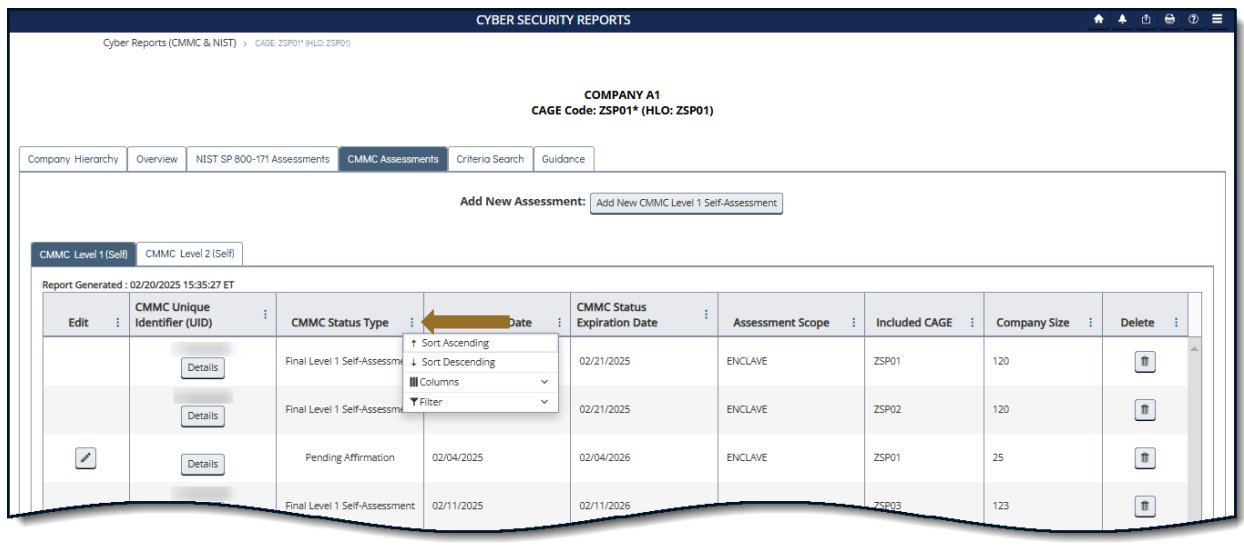


Figure 22: Cyber Reports CMMC Column Sorting and Filtering

To add an assessment, users must have the SPRS Cyber Vendor User role.

Select the **Add New CMMC Level 1 Self-Assessment** button, enter the required information, and select **Save**.

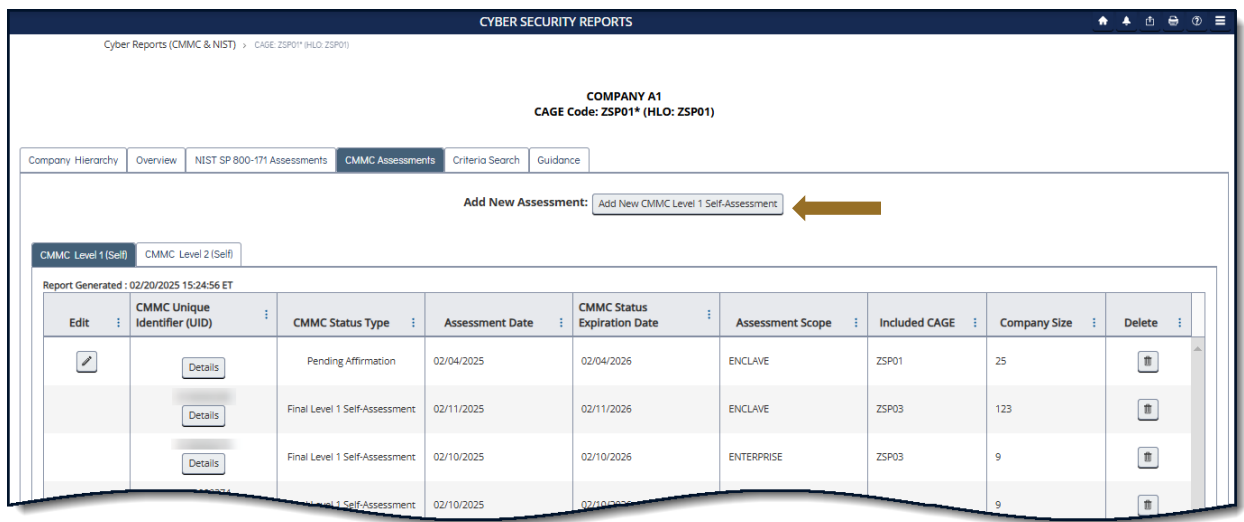


Figure 23: Cyber Reports Add New CMMC Level 1 Self-Assessment Button

The **Open CAGE Hierarchy** button opens the CAGE tree, allowing users to select which CAGEs are included/assessed CAGEs. Users can also copy and paste a comma-delimited list of CAGEs into the CAGE text box provided.

The screenshot displays the 'CYBER SECURITY REPORTS' interface. At the top, it identifies 'COMPANY A1' with 'CAGE Code: ZSP01* (HLO: ZSP01)', 'Confidence Level: Level 1 Self-Assessment', and 'Assessment Standard: NIST SP 800-171 Rev 2'. A 'Back' button is visible on the left. The main form is titled 'Enter CMMC Assessment Details'. It contains an 'Assessment Date' field (MM/DD/YYYY), an 'Assessment' field, and a question: 'How many employees are in the Level 1 self-assessment applicable to this assessment?'. Below this is another question: 'Are you compliant with each of the requirements in FAR clause 52.204-21?'. An 'Included CAGE(s)' field is present, with a blue arrow pointing to an 'Open CAGE Hierarchy' button. The 'CAGE Hierarchy' dialog box is open, showing a search bar and a list of CAGE codes with checkboxes: 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; and ZSP05: (OBSOLETE) COMPANY A5 (DBA: COMPANY A5), A5 ROAD BLDG 153 2, A5 CITY, AA, USA. The dialog box has 'Cancel' and 'Ok' buttons. At the bottom of the main form, there are 'Save' and 'Continue to Affirmation' buttons.

Figure 24: Cyber Reports CMMC CAGE Hierarchy

Questions related to technical interpretation of these CMMC Level 1 supplemental guidance documents may be directed to the email listed here: . Do not submit questions requesting interpretation or modification of NIST source documents, which are outside the CMMC Program's purview.

Each assessment requires affirmation by a company's Affirming Official (AO). As defined in 32 CFR 170.4, the 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 organization. (CMMC-custom term 170.4)

Assessments can be saved without completing and edited or affirmed at a later date. Click the Save button to return to the report grid. These assessments will be identified as Incomplete in the CMMC Status Type column and will not be assigned a CMMC UID.

Once the assessment detail information is completed, select **Continue to Affirmation**.

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)

Figure 25: Cyber Reports CMMC Save or Continue to Affirmation

If the user entering the CMMC Self-Assessment is not the AO, enter the AO's email address and select Transfer to AO. The AO will be sent an email, with the user on copy, that an assessment is waiting for their affirmation. This email is only sent once. It includes helpful information but it is not required and may be prevented from being delivered depending on a company's email server settings.

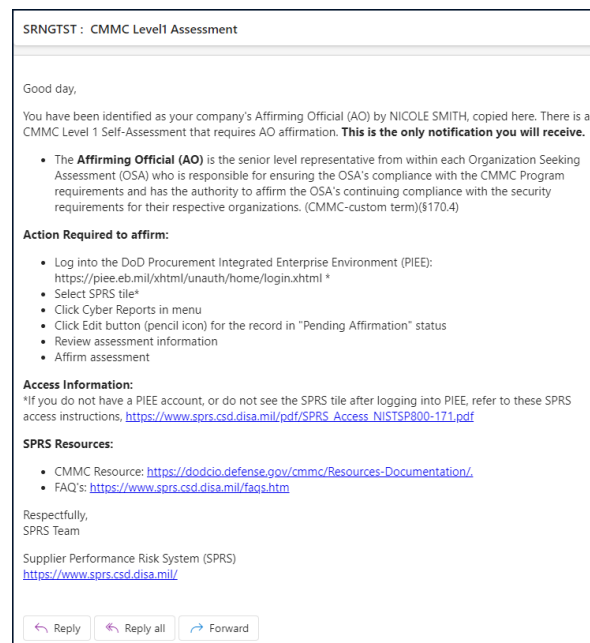


Figure 26: Cyber Reports CMMC AO Email Sample

If the user is the AO, select **Continue to Affirmation**.

Figure 27: Cyber Reports CMMC Continue to Affirmation or Transfer to AO

This information for the Affirming Official is transferred from the user's PIEE profile. Any changes must be made in PIEE and cannot be changed on this screen. Enter any additional emails to be associated with the record and click **Continue to Affirmation**.

Figure 28: Cyber Reports CMMC Assessment Details

Review the information and statement, and click the check box to certify. Select **Affirm** to complete or **Cancel** if information on the form needs to be updated or if the user is not the AO.

Assessment and Affirmation

Report Generated: 02/20/2025 15:45:20 ET

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

Level 1 CMMC Assessment Date: **02/04/2025**
 CMMC Status Expiration Date: **02/04/2026**
 Assessing Scope: **ENCLAVE**
 Company Size: **25**

Affirming Official (AO) Responsible for Cyber/CMMC:
 Name: **NICCICYBERVEND LASTNAME**
 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: [REDACTED] 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

Figure 29: Cyber Reports CMMC Certify and Affirm

To **Edit** a CMMC Assessment, select the **pencil** icon within the Edit column.

- CMMC Status Types **“Incomplete”** and **“Pending Affirmation”** are the only status types that can be edited.
- If the data within a **“Final Level 1 Self-Assessment”** or a **“No CMMC Status”**, needs to change, this assessment type will need to be deleted and recreated.
- CMMC Status Type **“No CMMC Status (Expired Assessment)”** cannot be edited nor deleted.

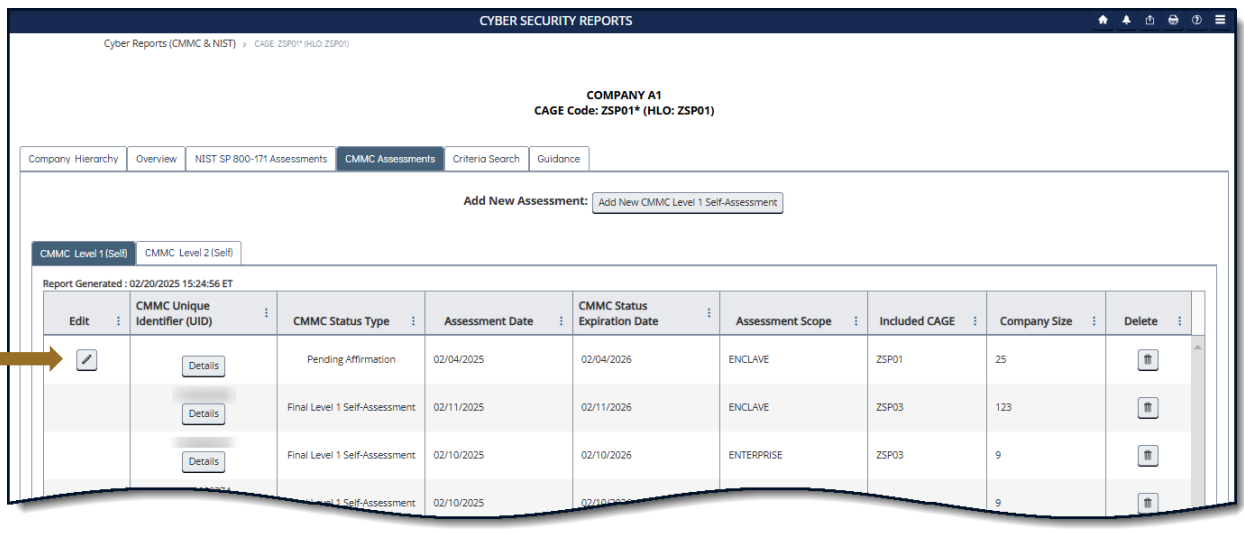


Figure 30: Cyber Reports CMMC Edit an Assessment

To **Delete** an Assessment, select the **trashcan** button from the Delete column. This will open a pop-up of the assessment details with a warning to confirm deletion. Deleting the assessment will delete it for all Included CAGEs. Select **Confirm Delete** to delete.

All CMMC Status Types can be deleted with the exception of the **“No CMMC Status (Expired Assessment).”**

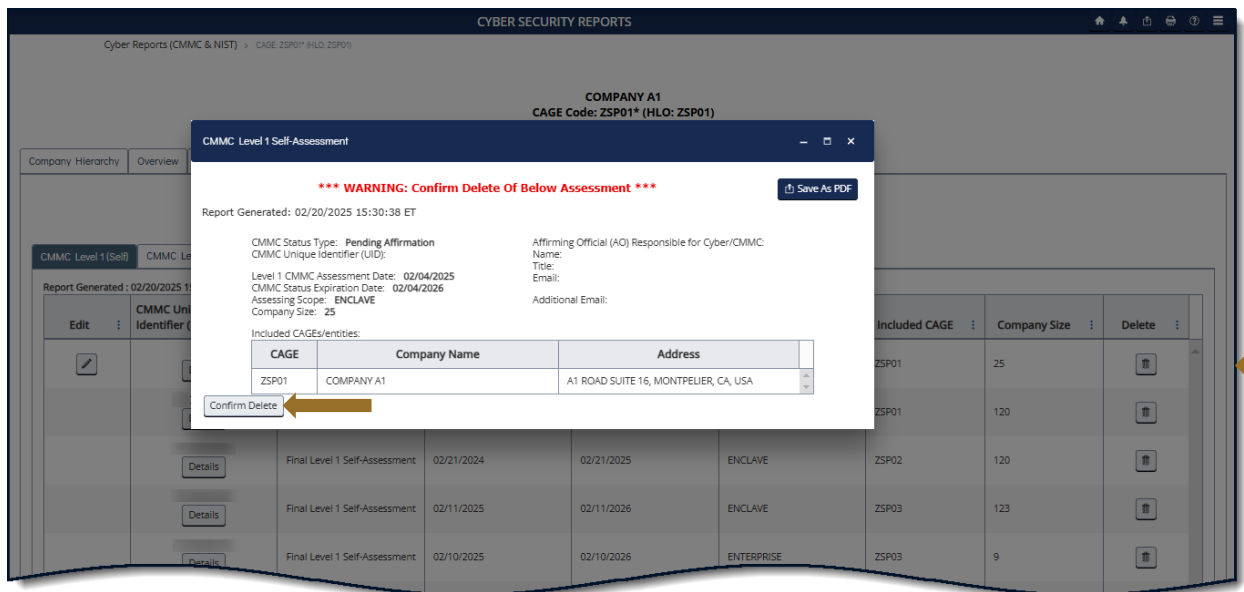


Figure 31: Cyber Reports CMMC Delete an Assessment

The **CMMC Quick Entry Guide** provides summary level instructions on entering and editing summary assessment results. These instructions are located on the SPRS web page:

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

The **CMMC Assessments** tab includes **CMMC Level 2 (Self)** tab. This tab displays logged CMMC Level 2 Self-Assessments.

Report Generated : 02/27/2025 14:56:22 ET	Edit	CMMC Unique Identifier (UID)	CMMC Status Type	Assessment Date	CMMC Status Expiration Date	Assessment Scope	Included CAGE	Company Size	Cancel/Delete
		Details	Affirm Pending Affirmation			ENCLAVE	ZSP01, ZSP02, ZSP03, ZSP04	1	
		Details	Affirm Pending Affirmation	08/30/2024	02/26/2025	ENTERPRISE	ZSP02, ZSP04, ZSP05	6	
			Incomplete						

Figure 32: Cyber Reports CMMC Level 2 (Self) Tab

CMMC Level 2 (Self) Summary results include the following information:

- **CMMC Unique Identifier (UID)** – a 10-digit alphanumeric identifier automatically assigned to each newly saved assessment. The first two letters delineate the CMMC Status Type. Level 1 and Level 2 Self-Assessments have prefix S1 and S2 respectively. Level 2 and Level 3 Assessments will observe prefix L2 and L3.
- **CMMC Status Type** – The status of the Assessment
 - Incomplete
 - Pending Affirmation
 - CMMC L2 Conditional Self-Assessment
 - CMMC L2 Conditional Self-Assessment (Retracted by Vendor)
 - CMMC L2 Final Self-Assessment
 - CMMC L2 Final Self-Assessment (Expired Affirmation)
 - CMMC L2 Final Self-Assessment (Retracted by Vendor)
 - No CMMC Status – One or more responses did not meet mandatory CMMC assessment requirements.
 - No CMMC Status (Expired) – Indicates an expired Assessment

NOTE: *If an assessment qualifies to be a CMMC L2 Conditional or Final Self-Assessment once affirmed, then on the Score stepper and Affirmation pop-up, it will show “Unconfirmed” in the title.*

- **Assessment Date** – The date of the most recent assessment was conducted
- **CMMC Status Expiration Date** – The assessment expiration date; a Level 2 self-assessment is considered valid for a year
- **Assessment Scope** – There are two selections for scope:
 - Enterprise – an organization with a defined mission/goal and a defined boundary, using information systems to execute that mission, and with responsibility for managing its own risks and performance
 - Enclave – a set of system resources that operate in the same security domain and that share the protection of a single common continuous security perimeter (NIST)
- **Included CAGE** – List of all CAGE Codes included in the assessment scope.
- **Company Size** – Total of employees at all locations of the organization

Selecting the Detail button in the CMMC Unique Identifier (UID) column, opens a pop-up that contains a print friendly display of all information associated with that record. There is also a View/Expand option to see additional assessment information. Click Save As PDF to save a copy.

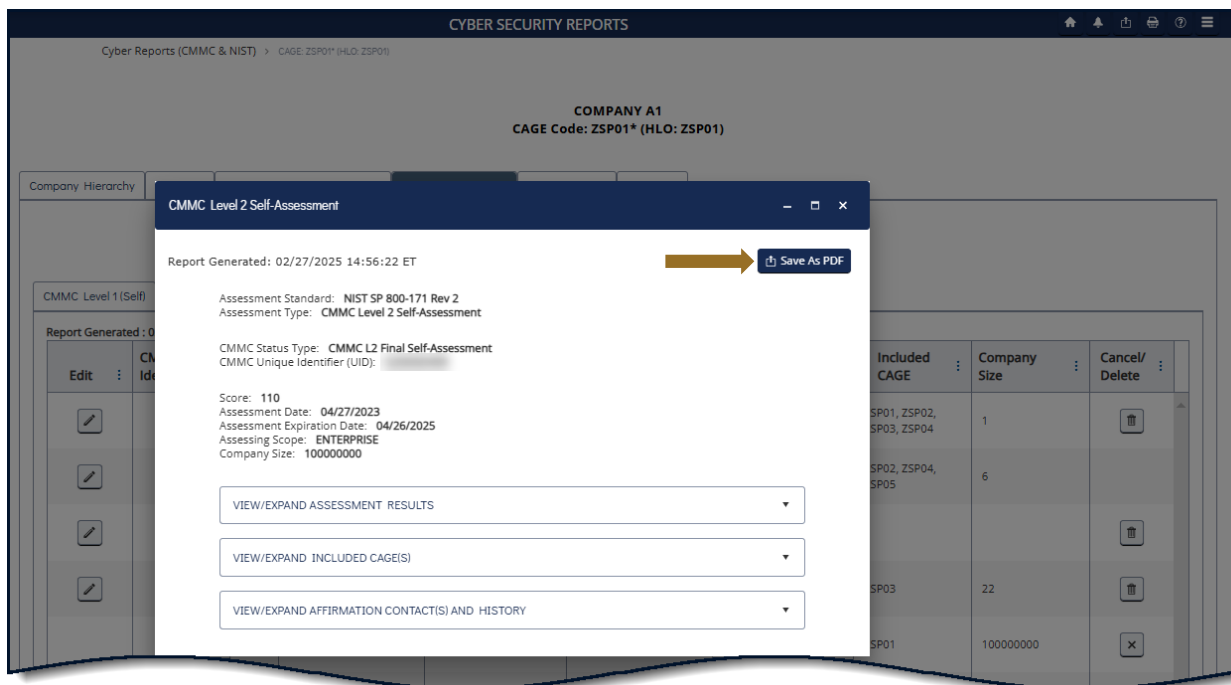


Figure 32: Cyber Reports CMMC Level 2 Self-Assessments Details Pop-up

Sort and filter columns to search for specific data by using the three-vertical dots and selecting various methods of sorting.

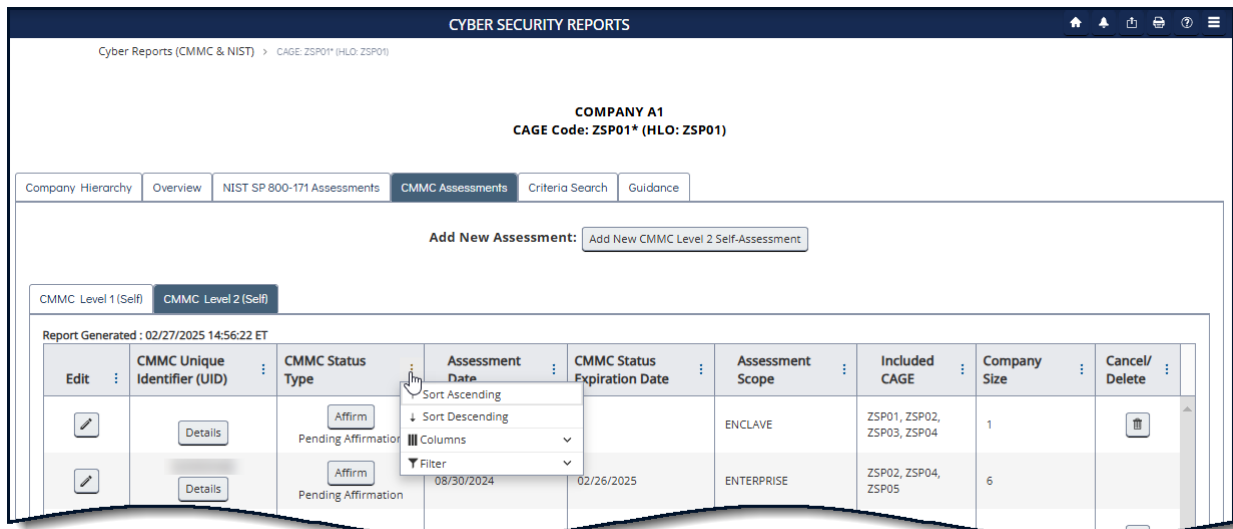


Figure 33: Cyber Reports CMMC Column Sorting and Filtering

To add an assessment, users must have the SPRS Cyber Vendor User role.

Select the **Add New CMMC Level 2 Self-Assessment** button.

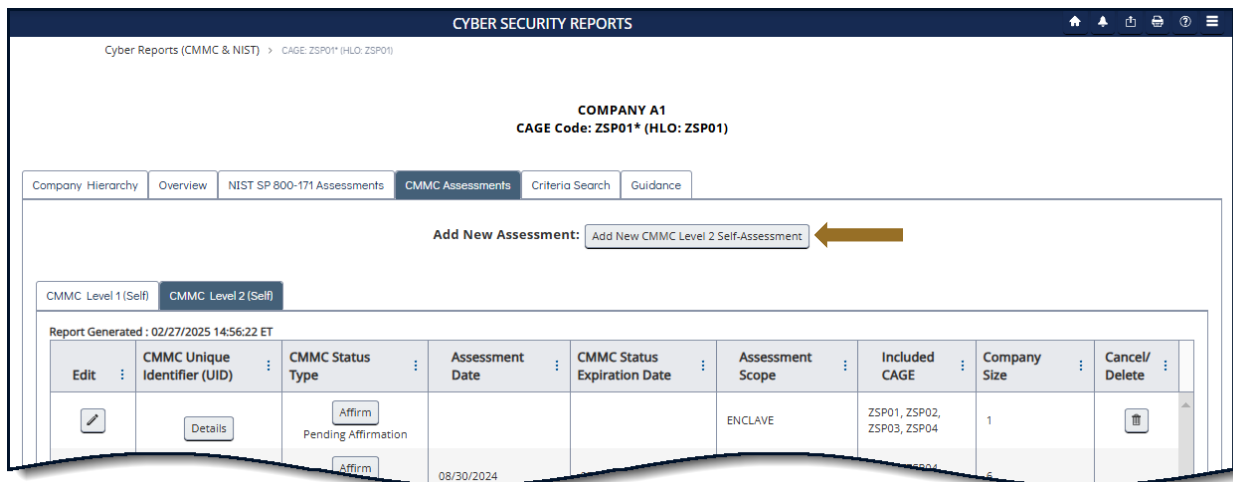


Figure 34: Cyber Reports Add New CMMC Level 2 Self-Assessment Button

Complete the Compliance Status for each Requirement Number; choosing Met, Not Met, or N/A for each question. All Objectives must be met for the Requirements to be Met. Use the Requirement Objectives button to view a list of the objectives required.

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 ⓘ		
		Met	Not Met	N/A
<i>Note: All Objectives must be met for the Requirement to be Met.</i>				
ACL2-3.1.1 Requirement Objectives	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<input type="checkbox"/> Met	<input type="checkbox"/> Not Met	<input type="checkbox"/> N/A
ACL2-3.1.2 Requirement Objectives	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	<input type="checkbox"/> Met	<input type="checkbox"/> Not Met	<input type="checkbox"/> N/A
ACL2-3.1.3 Requirement Objectives	Control the flow of CUI in accordance with approved authorizations.	<input type="checkbox"/> Met	<input type="checkbox"/> Not Met	<input type="checkbox"/> N/A
ACL2-3.1.4 Requirement Objectives	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	<input type="checkbox"/> Met	<input type="checkbox"/> Not Met	<input type="checkbox"/> N/A
ACL2-3.1.5 Requirement Objectives	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<input type="checkbox"/> Met	<input type="checkbox"/> Not Met	<input type="checkbox"/> N/A
ACL2-3.1.6 Requirement Objectives	Use non-privileged accounts or roles when accessing nonsecurity functions.	<input type="checkbox"/> Met	<input type="checkbox"/> Not Met	<input type="checkbox"/> N/A
ACL2-3.1.7 Requirement Objectives	Prevent non-privileged users from executing privileged functions and capture the execution of such functions and errors.	<input type="checkbox"/> Met	<input type="checkbox"/> Not Met	<input type="checkbox"/> N/A

Figure 35: Cyber Reports Requirements in CMMC Level 2 Self-Assessment

For requirements IA.L2-3.533 and SC.L2-3.13.11, use the Open Objectives button to complete the answers, the answer may result in partial credit for these requirements.

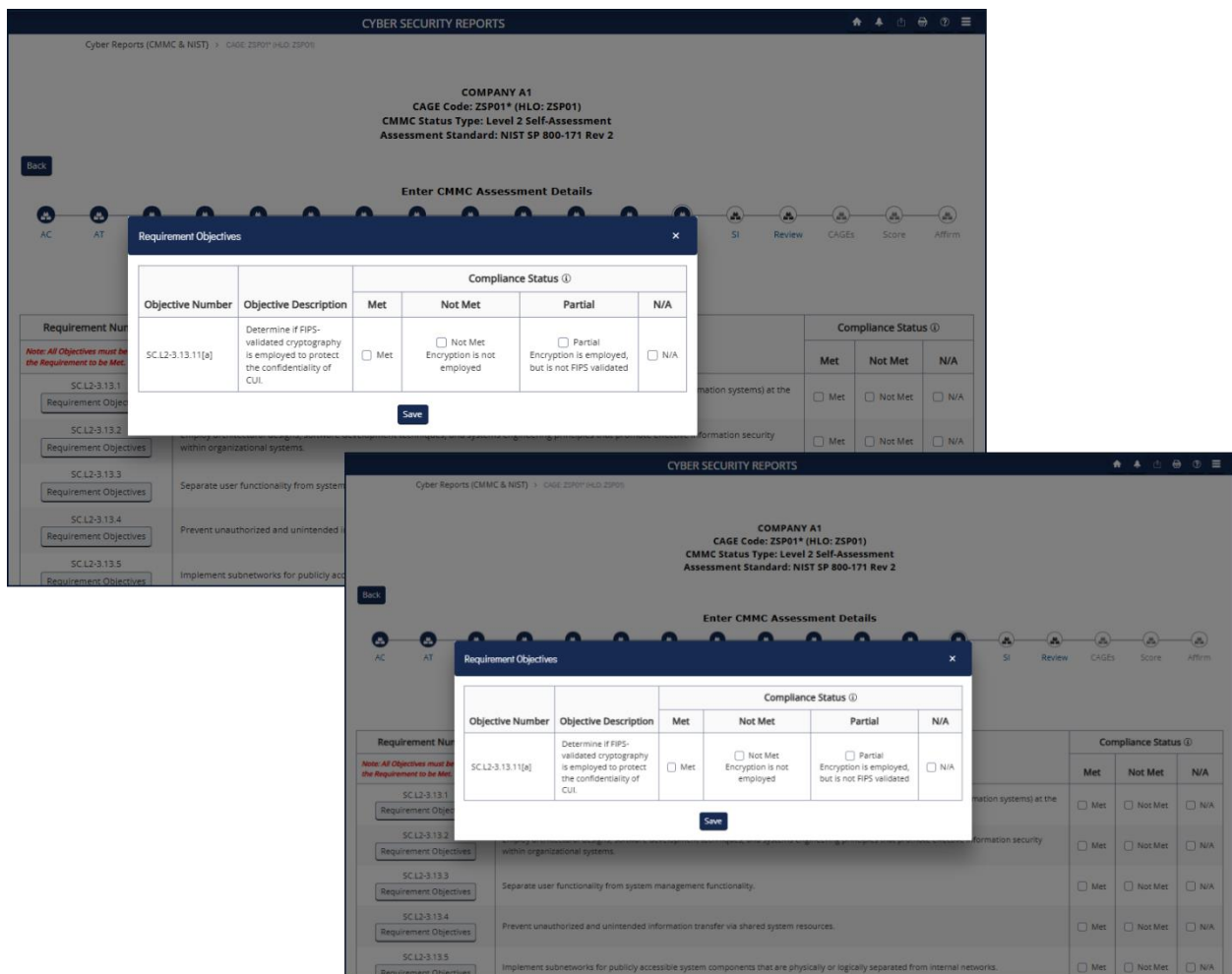


Figure 36: Cyber Reports CMMC Level 2 Self Assessment Open Objectives

For the requirement CA.L2-3.13.4, a user must answer Met or Not Met, N/A is not an option. Select **Save**.

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

ACATAUCMIAIRMAMPPSPERACASCSI

Review

CAGEsScoreAffirm

Requirement Family: Security Assessment (CA)

< Previous
Save
Save and Continue >

Requirement Number	Requirement Description	Compliance Status ⓘ		
<i>Note: All Objectives must be met for the Requirement to be Met.</i>		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.	<input type="checkbox"/> Met	<input type="checkbox"/> Not Met	<input type="checkbox"/> 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.	<input type="checkbox"/> Met	<input type="checkbox"/> Not Met	<input type="checkbox"/> N/A
CA.L2-3.12.3 Requirement Objectives	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	<input type="checkbox"/> Met	<input type="checkbox"/> Not Met	<input type="checkbox"/> 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.	<input type="checkbox"/> Met	<input type="checkbox"/> Not Met	*

< Previous
Save
Save and Continue >

Figure 37: Cyber Reports Requirements in CMMC Level 2

To export the report list, click the Export button on the Review step to send the requirements list data to the Download module. The user will receive a pop-up, select "Ok". The system will send an email when the Export is available, select the Download option from the left-hand menu and select Download when ready. See the SERVICE section in this guidance for more information.

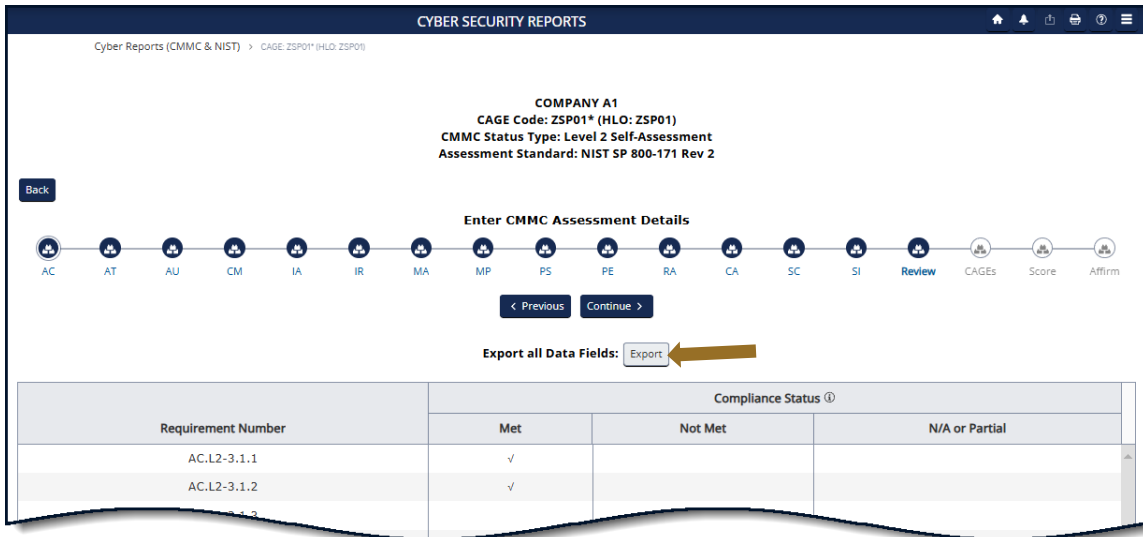


Figure 38: Cyber Reports CMMC Level 2 Export

Add Assessment Scope, Employee Count, and included CAGE(s) as required.

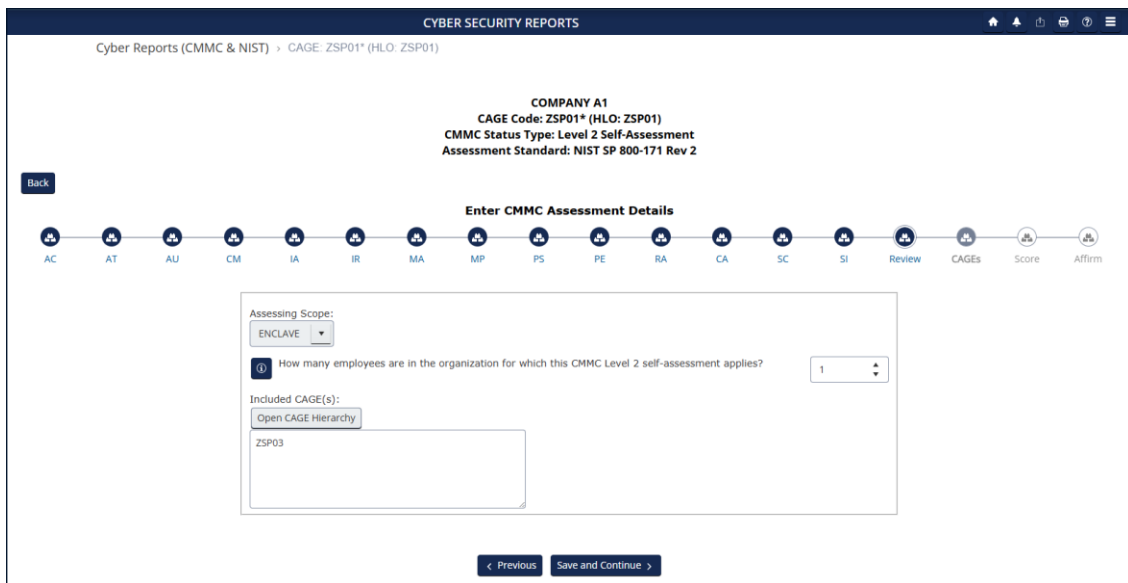


Figure 39: Cyber Reports CAGE(s) Stepper

The **Open CAGE Hierarchy** button opens the CAGE tree, allowing users to select which CAGEs are included/assessed CAGEs. Users can also copy and paste a comma-delimited list of CAGEs into the CAGE text box provided.

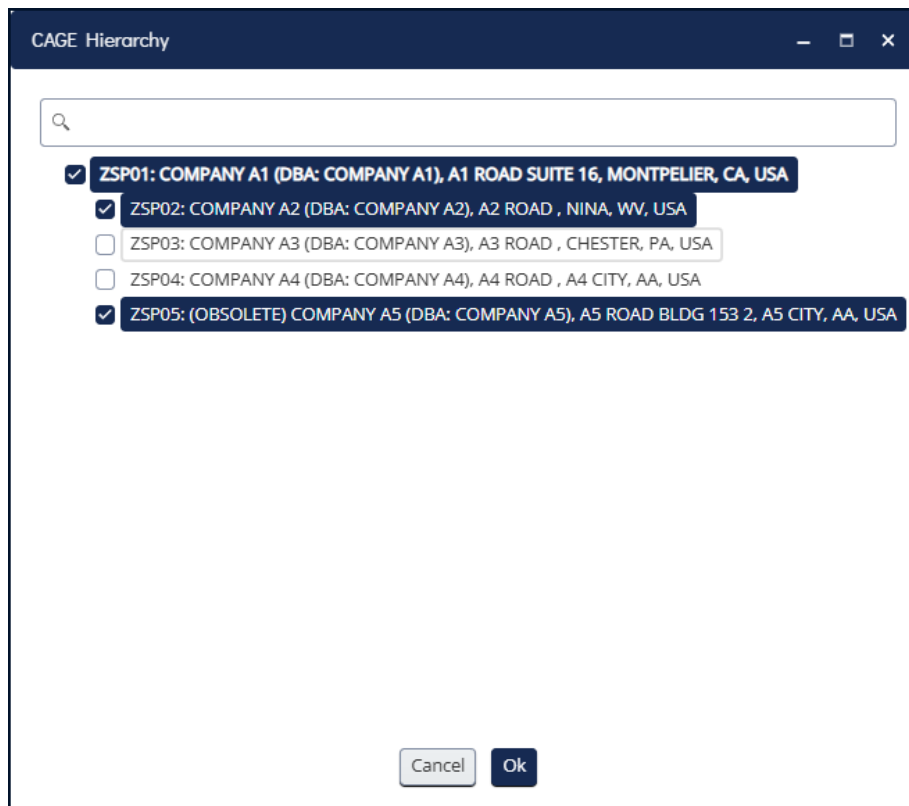


Figure 40: Cyber Reports CMMC Level 2 CAGE Hierarchy

NOTE: *CAGE Hierarchy is imported from the System for Award Management (SAM). Users are unable to add CAGEs that are not part of their company hierarchy.*

SPRS will calculate the score and status. The Score is listed in bold at the top.

Score: Only status types Conditional (score = 88 to 109) and Final (score = 110) can be affirmed.

The screenshot displays the 'CYBER SECURITY REPORTS' interface. At the top, it shows the breadcrumb 'Cyber Reports (CMMC & NIST) > CAGE: ZSP01* (HLO: ZSP01)'. The main content area is titled 'COMPANY A1' and lists 'CAGE Code: ZSP01* (HLO: ZSP01)', 'CMMC Status Type: Level 2 Self-Assessment', and 'Assessment Standard: NIST SP 800-171 Rev 2'. A progress bar below the title shows 16 steps: AC, AT, AU, CM, IA, IR, MA, MP, PS, PE, RA, CA, SC, SI, Review, CAGEs, Score, and Affirm. The 'Review' step is currently active. Below the progress bar, the 'Final Score: 108' is prominently displayed. Underneath, the 'CMMC Status Type: Unaffirmed CMMC L2 Conditional Self-Assessment' is shown. A note states: 'Your responses meet the requirements for a CMMC Level 2 Conditional Self-Assessment. Once affirmed, the assessment will be valid for 180 days.' A link for inquiries is provided: 'For questions about why this assessment is "CMMC L2 Conditional Self-Assessment" please email: osd.pentagon.dod-cio.mbx.cmmc-inquiries@mail.mil'. At the bottom, there are two buttons: '< Previous' and 'Continue To Affirmation >'.

Figure 41: Cyber Reports CMMC Level 2 Score

NOTE: *If a requirement is not able to be subject to a Plan of Action and Milestones (POA&M), then the Status Type will be No CMMC Status regardless of score.*

Questions related to technical interpretation of these CMMC Level 2 supplemental guidance documents may be directed to the email listed here: 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.

Each assessment requires affirmation by a company's Affirming Official (AO). As defined in 32 CFR 170.4, the 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 organization. (CMMC-custom term 170.4)

Assessments can be saved without completing and edited or affirmed at a later date. Click the Save button to return to the report grid. These assessments will be identified as Incomplete in the CMMC Status Type column and will not be assigned a CMMC UID.

Once the assessment detail information is complete, select **Continue to Affirmation**.

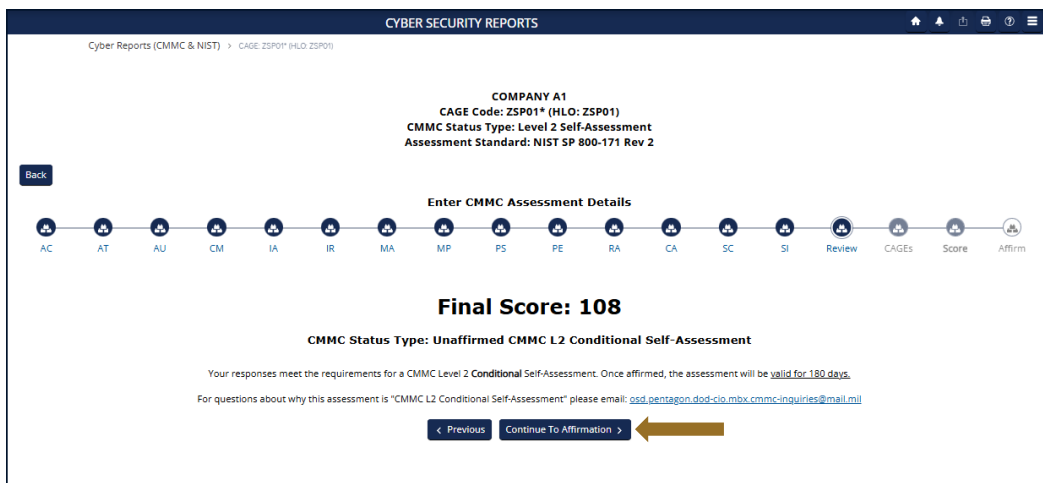


Figure 42: Cyber Reports CMMC Level 2 Previous or Continue to Affirmation

If the user entering the CMMC Self-Assessment is not the Affirming Official (AO), enter the AO's email address and select **Transfer to AO**.

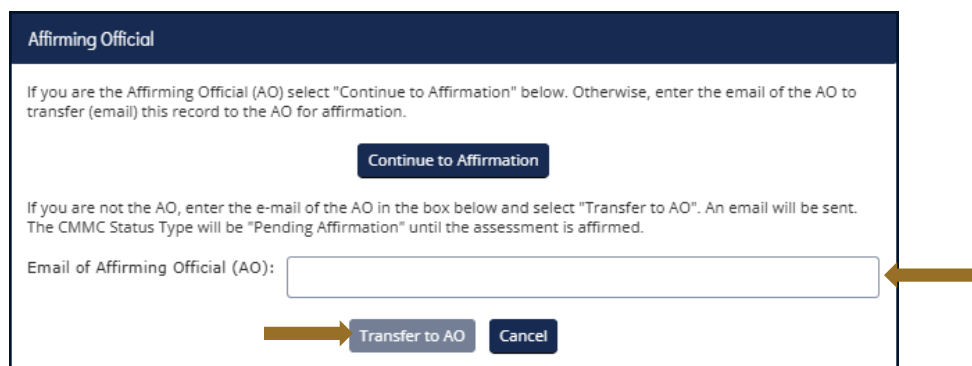


Figure 43: Cyber Reports CMMC Level 2 Transfer to AO

The AO will be sent an email, with the user on copy, that an assessment is waiting for their affirmation. This email is only sent once. It includes helpful information but it is not required and may be prevented from being delivered depending on a company's email server settings.

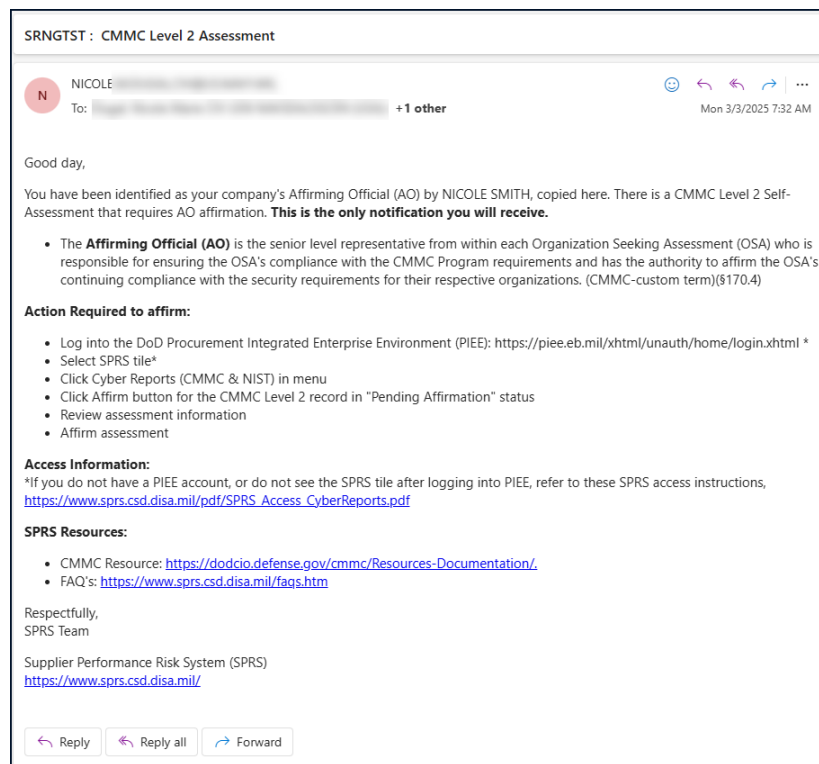


Figure 44: Cyber Reports CMMC Level 2 Sample AO Email

If the user is the AO, select **Continue to Affirmation**.

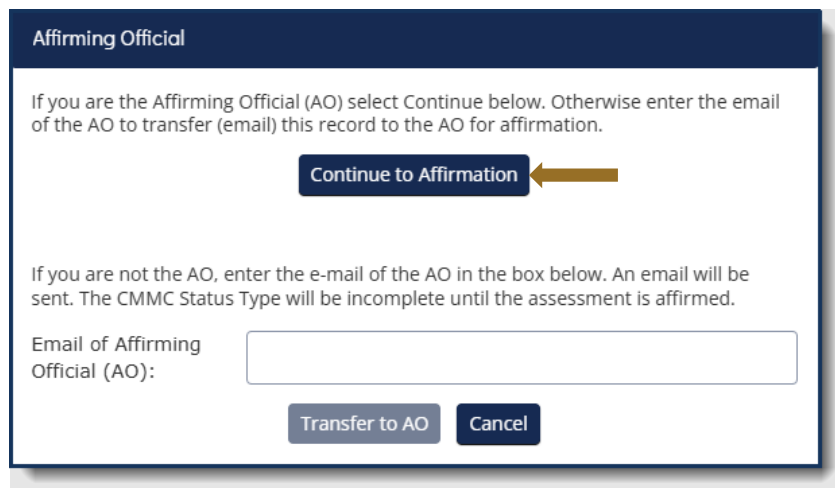


Figure 45: Cyber Reports CMMC Level 2 Continue to Affirmation

This information for the Affirming Official is transferred from the user's PIEE profile. Any changes must be made in PIEE and cannot be changed on this screen. Enter any additional emails to be associated with this record and click **Continue to Affirmation**.

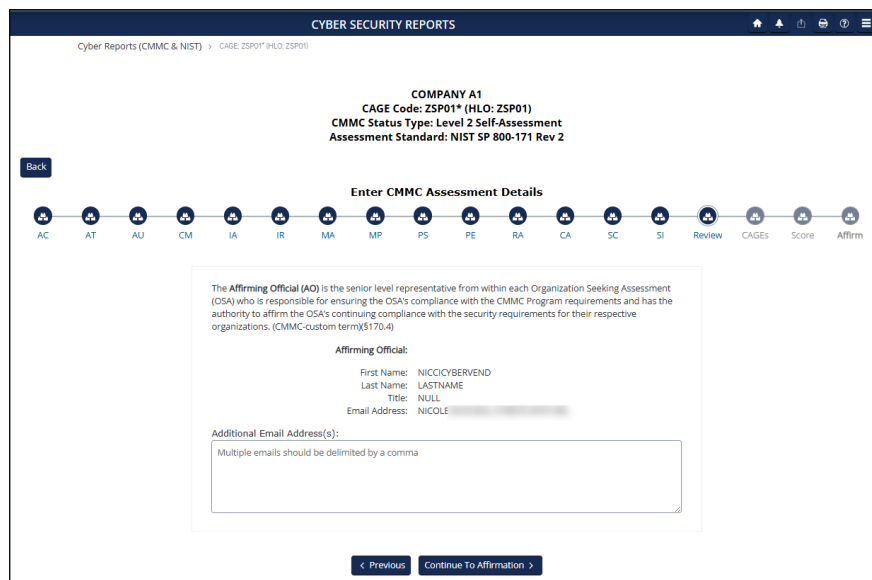


Figure 46: Cyber Reports CMMC Level 2 Assessment Details

Review the information and statement and click the check box to certify. An **Assessment and Affirmation** pop-up will appear. Assessment results and CAGE information are in expandable sections at the bottom. Click the check box to certify, and select the **Affirm** button. Or select **Cancel** to return to the assessment for any updates or if the user is not the AO.

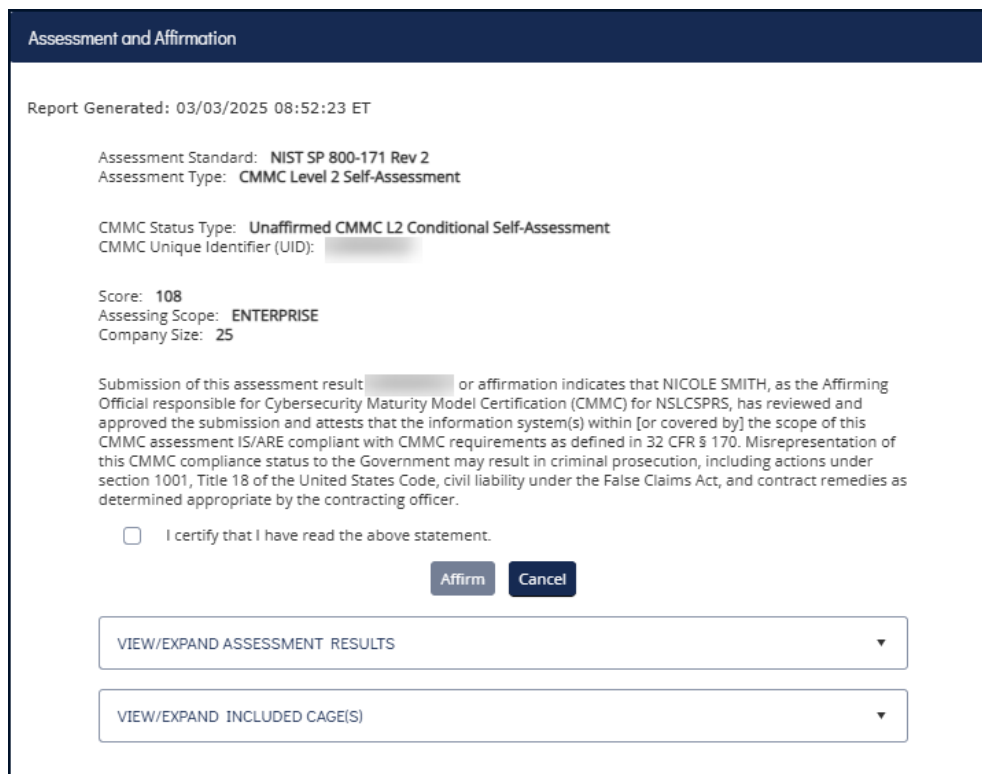


Figure 47: Cyber Reports CMMC Level 2 Certify and Affirm

The assessment will appear at the top of the report. A **“CMMC L2 Conditional Self-Assessment”** is valid for 180 days. A **“CMMC L2 Final Self-Assessment”**, with annual affirmations, is valid for 3 years.

To **Edit** a CMMC Assessment, select the **pencil** icon within the Edit column.

- CMMC Status Types that can be edited include:
 - **“Incomplete”**
 - **“Pending Affirmation”**
 - **“No CMMC Status”**
 - **“CMMC L2 Conditional Self-Assessment”**

The screenshot shows the 'CYBER SECURITY REPORTS' interface for 'COMPANY A1' (CAGE Code: ZSP01* (HLO: ZSP01)). The 'CMMC Assessments' tab is active. A table displays assessment data with columns: Edit, CMMC Unique Identifier (UID), CMMC Status Type, Assessment Date, CMMC Status Expiration Date, Assessment Scope, Included CAGE, Company Size, and Cancel/Delete. Three rows are visible: 'No CMMC Status', 'Pending Affirmation', and 'Incomplete'. A red arrow points to the pencil icon in the 'Edit' column of the 'No CMMC Status' row.

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			ENTERPRISE	ZSP05	0	
	Details	Pending Affirmation			ENTERPRISE	ZSP01	25	
	Details	Incomplete	08/30/2024	02/26/2025	ENTERPRISE	ZSP02, ZSP04, ZSP05	6	

Figure 48: Cyber Reports CMMC Level 2 Edit an Assessment

If an assessment has delete capability, there will be a trashcan icon within the **Cancel/Delete** column located on the far right. To Delete an Assessment, select the **Trash Can** button from the **Delete** column. This will open a pop-up of the assessment details with a warning to confirm deletion. Deleting the assessment will delete it for all Included CAGEs. Select **Confirm Delete** to delete.

- CMMC Status Types that can be deleted include:
 - **“Incomplete”**
 - **“Pending Affirmation”**
 - **“No CMMC Status”**

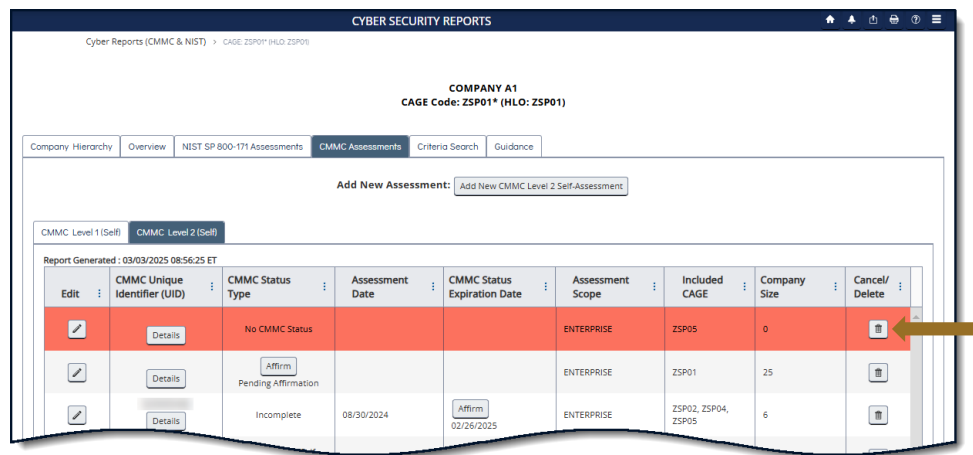


Figure 49: Cyber Reports CMMC Level 2 Delete an Assessment

If an assessment can be canceled, an “X” button in the **Cancel/Delete** column is available. When a record is canceled, it will turn red, and the status type will be appended with “(Retracted by Vendor)”. Canceled records will remain visible to authorized government users.

- CMMC Status Types that can be canceled include:
 - “CMMC L2 Conditional Self-Assessment”
 - “CMMC L2 Final Self-Assessment”



Figure 50: Cyber Reports CMMC Level 2 Cancel an Assessment

- CMMC Status Types that cannot be edited, deleted, or canceled include:
 - “CMMC L2 Conditional Self-Assessment (Retracted by Vendor)”
 - “CMMC L2 Final Self-Assessment (Retracted by Vendor)”
 - “No CMMC Status (Expired)”

Canceled and expired records will remain visible to authorized government users.

Annual affirmations are required for “CMMC L2 Final Self-Assessments”. An **Affirm** button will appear in the **CMMC Status Expiration Date** column 60 Days prior to the CMMC Status Expiration Date and will persist until the assessment is affirmed. If the assessment is not affirmed before expiration, the CMMC Status Type will change to “CMMC L2 Final Self-Assessment (Expired Affirmation)” and turn red until affirmed. Regardless of affirmation, once the assessment is three (3) years beyond the Assessment Date, the CMMC Status Type will change to “No CMMC Status (Expired)”.

To complete an annual affirmation, the AO will elect the Affirm button from within the CMMC Status Expiration Date column. Review the AO information, add any Additional Email Address(s) associated with the assessment, and select Continue To Affirmation. Review the information and statement within the pop-up, and click the check box to certify. Select Affirm to complete.

Note: The second-year annual affirmation and third-year expiration is based on the Assessment Date regardless of the date the assessment was previously annually affirmed.

The screenshot displays the 'CYBER SECURITY REPORTS' interface for 'COMPANY A1' with CAGE Code: ZSP01* (HLO: ZSP01). The 'CMMC Assessments' tab is active, showing a table of assessments. The table has columns for Edit, CMMC Unique Identifier (UID), CMMC Status Type, Assessment Date, CMMC Status Expiration Date, Assessment Scope, Included CAGE, Company Size, and Cancel/Delete. Two assessments are listed, both with 'Affirm' buttons in the expiration date column.

Edit	CMMC Unique Identifier (UID)	CMMC Status Type	Assessment Date	CMMC Status Expiration Date	Assessment Scope	Included CAGE	Company Size	Cancel/Delete
	[Details]	CMMC L2 Final Self-Assessment	04/29/2023	Affirm 04/28/2025	ENCLAVE	ZSP02, ZSP04, ZSP05	999999999	[X]
	[Details]	CMMC L2 Final Self-Assessment	04/29/2024	Affirm 04/29/2025	ENTERPRISE	ZSP01	0	[X]

Figure 51: Cyber Reports CMMC Level 2 Annual Affirmation

The **CMMC Level 2 Quick Entry Guide** provides summary level instructions on entering and editing summary assessment results. These instructions are located on the SPRS web page:

<https://www.sprs.csd.disa.mil/pdf/CMMCL2SelfQuickEntryGuide.pdf>

The **Criteria Search** tab allows the user to enter various data points and search all Cyber assessments within their selected hierarchy based on the entered criteria. Enter desired search criteria and select the **Search** button. Applicable information will load below.

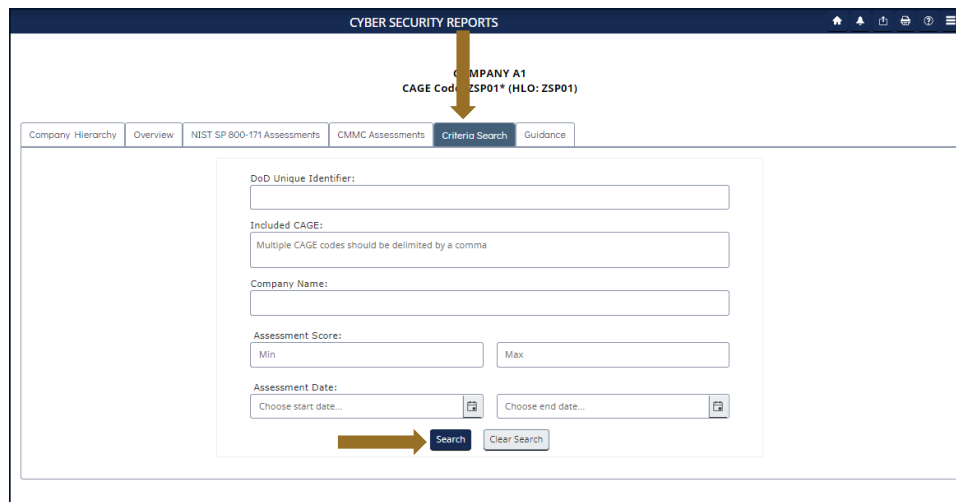


Figure 52: Cyber Reports Criteria Search Tab

The **Show/Hide Search Fields** button will collapse or expand the criteria search fields for space saving considerations.

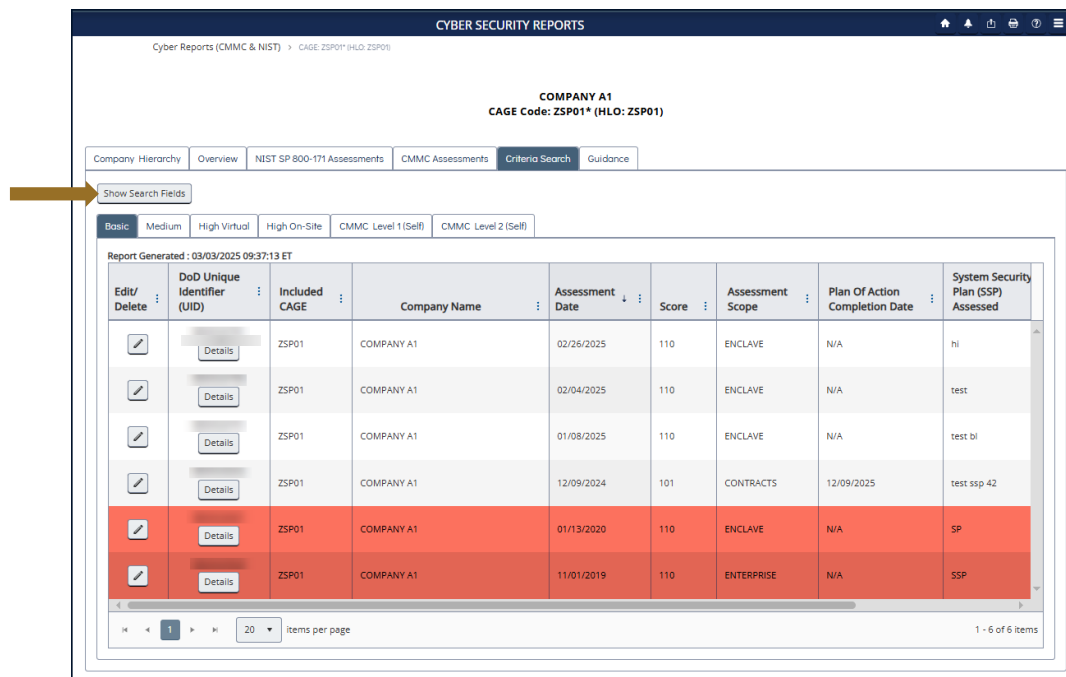


Figure 53: Cyber Reports Criteria Search tab Show Search fields

Contractor Vendor User roles may only view details associated with their CAGE(s) or the subordinate CAGE(s). For questions about the company CAGE hierarchy, refer to the Electric Business Point of Contact (EBPOC) listed in the SAM registration for the CAGE at the website listed here: <https://sam.gov/content/home>.

Users may request access to additional CAGEs by updating their PIEE profile.

The **Guidance** tab provides General Guidance as well as CMMC and NIST SP 800-171 specific information and contains links to Assessment Methodology, Quick Entry Guides, DFARS 252.204, FAR Clause 52.204-21, and more.

5.2 CAGE HIERARCHY

The CAGE Hierarchy report identifies the CAGE(s) specified in the user's profile in PIEE (bold font), the associated CAGE(s), and ownership. SPRS imports CAGE hierarchy data from SAM via CAGE DLA. This information is identical to the Company Hierarchy tab in the Cyber Report, displayed in a different format.

To access CAGE Hierarchy:

Select **CAGE Hierarchy** from the Menu.

Use the dropdown menu to select CAGE to see the associated hierarchy.



Figure 54: CAGE Hierarchy

A Warning message will appear if one or more CAGEs within the hierarchy profile appears to have missing or inaccurate information. Review the SAM registrations of all CAGEs to confirm the correct ILO and HLO information is listed. Contact the Electric Business Point of Contact, (EBPOC) listed at <https://sam.gov> for correction.

SPRS imports CAGE information from the Defense Logistics Agency (DLA) and the System for Award Management (SAM). Corrections to company hierarchy profiles are completed in SAM.

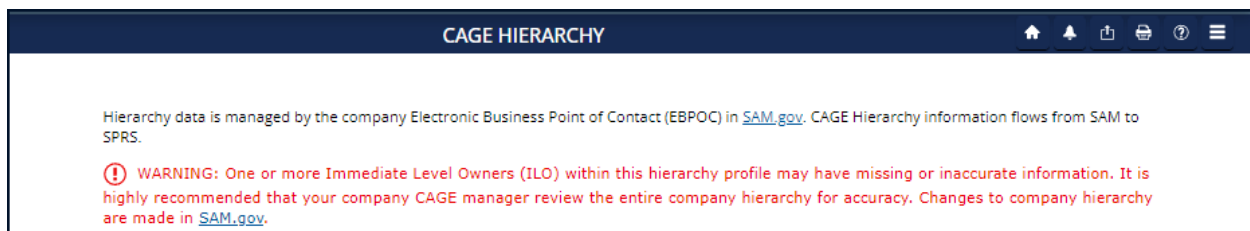


Figure 55: Error on CAGE Hierarchy

6. RISK ANALYSIS REPORTS

SPRS Risk Analysis Reports use business intelligence to reflect the risk associated with vendors & items.

6.1 SUPPLIER RISK REPORT

The Supplier Risk Report is a standalone way to view detailed Supplier Risk for a specific company. The Supplier Risk Score is an overall score using 3-years of supplier performance information (PI) data designed to calculate and identify supplier risk by calculating a single overall numerical score. The Supplier Risk Score is derived by using ten identified risk factors and adjusting based on age, number of contracts, and record weight. The final scores are ranked against one another to provide a color ranking based on a 5-color rating system.

For detailed information on how the Supplier Risk score is calculated, see SPRS Evaluation Criteria Manual:

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

To access Supplier Risk Report:

Select [Supplier Risk](#) from the Menu.

- If only one CAGE is available on the user's PIEE account, report will run automatically upon menu click.
- For multiple CAGEs, select CAGE from the dropdown.
- Click **Run Supplier Risk Report** button.



Figure 56: Supplier Risk Report Request

- Page display defaults to Vendor Detail Information. User can toggle between Vendor Basic and Vendor Detail for space considerations.

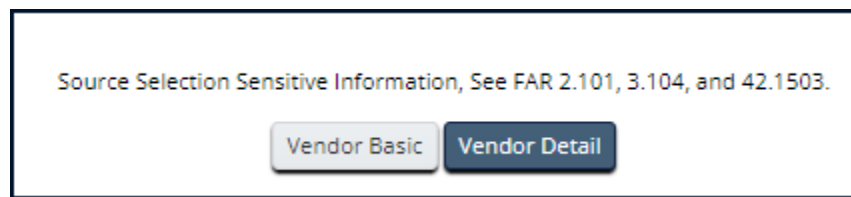


Figure 57: Toggle Vendor Basic/Vendor Detail Supplier Risk

- Contractor Information:** This includes Basic Company Information and Commercial and Government Entity (CAGE) Code Status. This information is received from the DLA CAGE Program and System for Award Management (SAM) at the URLs listed here: Commercial and Government Entity Program (CAGE) <https://cage.dla.mil/Home/> and <https://sam.gov>.



Figure 58: Supplier Risk Report

- Supplier Color:** The SPRS Color Legend represents the percentage breakdown of a normal statistical distribution, commonly referred to as a bell curve. Color assignment is based on a comparative assessment among suppliers. Supplier rankings are re-calculated whenever new data is introduced to the system or records age out. The top percentage group is Blue, and the lowest percentage group is Red.

Color is also used to communicate information unrelated to ranking. Black identifies a supplier with no Supplier Risk Score and Grey identifies supplier that have been excluded from selling to the government. Suppliers who have no scored factor data but have at least one contract reported in Federal Procurement Data System (FPDS) will not receive a numerical score but have a Green color score. The system will display an asterisk (*) in place of a numerical score. This is a neutral rating.

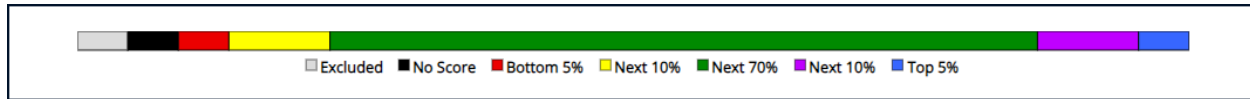


Figure 59: SPRS Color Legend

Hover over the question mark next to the color in the Supplier Risk Color Ranking column to see the SPRS Color Legend.



Figure 60: SPRS Color Legend Hover

- **Color Tiles:** There are three Supplier Risk Color tiles.
 - **Supplier Risk Score:** Displays the SPRS Supplier Risk Numerical Score and corresponding Color Score.
 - **Suspected Counterfeit:** Suspected Counterfeit (SC) information uses Agency Action Notices (AAN) from the Government Industry Data Exchange Program (GIDEP). If there are government issued AANs reporting suspected counterfeit material, the tile will be red and will indicate the number of alerts.

- **Level III/IV CAR(s):** Corrective Action Requests (CARs) are issued to the supplier to identify and correct instances of noncompliance with established methods for processing product, controlling quality systems or violation of contract/purchase order requirements. Level III/IV CARs are the most severe types of CAR. If a vendor has either a level three (3) or four (4) CAR, this tile will turn red to indicate a higher level of risk potential.

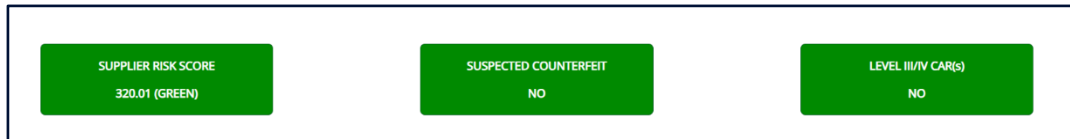


Figure 61: Supplier Risk Color Tiles

- Factor Data is the data the Supplier Risk Score uses to calculate an overall score using 3-years of supplier performance information (PI) data designed to identify supplier risk by calculating a single overall numerical score.

NOTE: For detailed information on how each of the 10 factors are calculated and summed to produce the Supplier Risk Score, with examples, see *SPRS Evaluation Criteria Manual*:
https://www.sprs.csd.disa.mil/pdf/SPRS_DataEvaluationCriteria.pdf

If records are greater than zero, the Factor becomes a link to display additional detail. Click on the hyperlinked Factor to find the Factor Detail Data tab.

Factor	Records	Score
Suspected Counterfeit (SC)	5	0
Quality Score Rankings ←	254	0
Overall Delivery Score	80	39
Contractor Performance Assessment Reporting System (CPARS)	0	0
Corrective Action Requests (CAR)	8	0
Corrective Action Plans (CAP)	0	0
Surveys	44	-28.98
Program Assessment Reports (PAR)	43	55.84
Government-Industry Data Exchange Program (GIDEP) (non-counterfeit)	11	0.07
Integrity Records	4	0
Scaling	0	N/A

Figure 62: Supplier Risk Factor Data

- Factor Detail Data:** Selecting the hyperlinked factors will bring the user to the associated data tab for the factor detail. To switch tabs user may click on the tabs directly or select from the hyperlinked list.

SC (5)	Quality (254)	Delivery (80)	CPARS (0)	CAR (8)	CAP (0)	Survey (44)	PAR (43)	GIDEP (11)	Integrity Record (4)
Quality Performance Ranking(s) - (8)									
Contact for Information									
Supply Code ↑	⋮	Quality Records	⋮	Received Delivery w/No As...	⋮	Ranking	⋮		
1630		1		0		Bottom			
2910		1		0		Bottom			
3130		1		0		Bottom			
4730		1		0		Bottom			
4820		247		53		Bottom			
5342		1		0		Bottom			
5365		1		0		Bottom			
5998		1		0		Bottom			
<div style="display: flex; justify-content: space-between; align-items: center;"> 1 20 items per page 1 - 8 of 8 items </div>									

Figure 63: Quality Detail in Supplier Risk Tab

Sort and filter columns to search for specific data by using the three-vertical dots and selecting various methods of sorting. The **Clear** button will reset all selected filters.

Supply Code ↑	Quality Records	Received Delivery w/No As...	Ranking
1630		0	Bottom
2910		0	Bottom
3130		0	Bottom
4730		0	Bottom
4820		53	Bottom
5342		0	Bottom
5365		0	Bottom
5998		0	Bottom

Figure 64: Supplier Risk Sort/Filter

- Contact for Information:** The Contact for Information link directs users to the Summary Report for Quality or Delivery record details. If there are questions about other record types, record review needs to occur at the record source, however, with proper OQE some records can be reviewed and challenged within the Summary Report module. Refer to the Summary Report section for more information on that process.

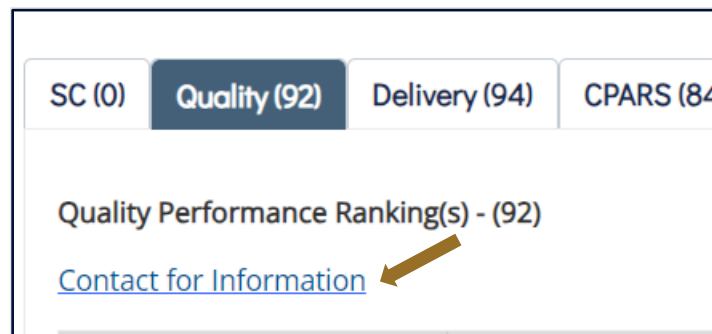


Figure 65: Supplier Risk Contact for Information Link

Clicking the link will display a pop-up with information on disputing any data inaccuracies for each specific record type.

Click “Ok” to close pop-up window.

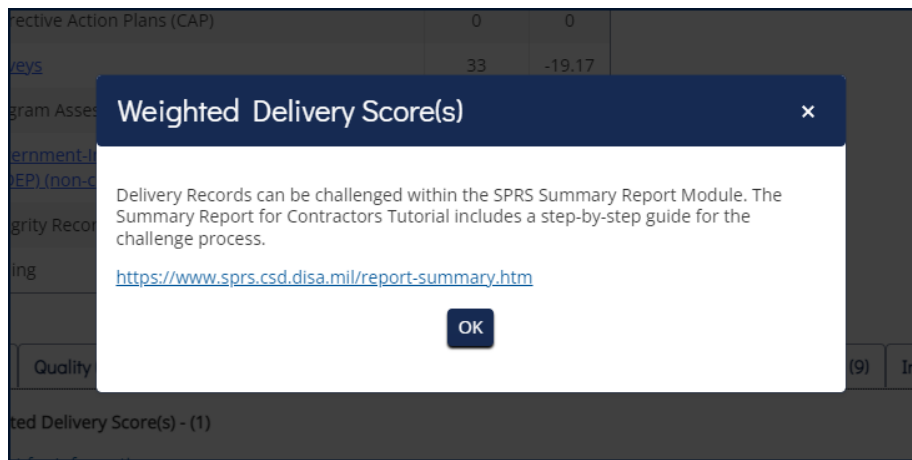


Figure 66: Supplier Risk Contact for Information Pop-Up

- **Compliance Information:** Displays additional compliance information for CAGE Code searched. This data is not used in scoring but for an all-in-one display purpose.
 - **NIST SP 800- 171 Assessment:** “YES” indicates there is a NIST SP 800-171 Assessment, for any confidence level, logged in SPRS. “NO” indicates there are no NIST assessments present for the CAGE.
- **Section 889 FAR 52.204-26 Representation:** SPRS utilizes the Reqs & Certs Information from SAM.gov. If a vendor has self-certified in SAM to the FAR 52.204-26 Representation, then SPRS will display “YES” Active Records. If a company has not answered the questions, not registered in SAM, or SPRS API connection to SAM was unsuccessful then SPRS will display “NO”.

Compliance Information ⓘ	Active Records
National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 Assessment	YES
Section 889 FAR 52.204-26 (c) (1) Representation	Data Not Available
Section 889 FAR 52.204-26 (c) (2) Representation	Data Not Available

Figure 67: Compliance Information

7. PERFORMANCE REPORTS

SPRS gathers, processes, and displays data about the performance of suppliers.

7.1 SUMMARY REPORT

The Summary Report displays the Supply Code Classifications associated with the CAGE data received by SPRS within the last three (3) years. The landing page allows the user to define the report based on their PIEE profile. Users with access to more than one CAGE may select up to five CAGEs. The default report will return all data organized by the FSC/PSC Supply Code type. Users may select the NAICS Supply Code type to refine the report by entering specific Supply Code data.

Preview period records, negative records not used in scoring for a period of fourteen (14) days from added date are visible in the Summary Report and Detail Pos/Neg Records. Preview period records are not visible to acquisition professionals.

Data discrepancies may be addressed through the Challenge process initiated in this report.

To access Summary Report:

Select [Summary Report](#) from the Menu.

- Click into the **CAGE Code(s)** box to open dropdown
- Select up to five (5) CAGE Codes
- Click **Run Summary Report**
- Or, further refine the search
 - Click **NAICS** to change the Supply Code type
 - Type or paste one or many comma delimited Supply Codes into **Supply Code** box

Figure 68: Contractor Summary Report Request

The Summary Report opens to an overview page. The top portion of the report displays the search fields prepopulated with the searched criteria, and the SPRS Color Legend. The bottom portion allows a quick glance of the CAGE(s) and Supply Codes selected that includes:

- Classification date
- CAGE, Company name and address
- Report timestamp
- Supply Code(s) for the selected Supply Code type
- Weighted Delivery Score
- Weighted Quality Performance color
- Scored record counts in parenthesis ()
 - 'Preview records only' will display when only unscored data is available
 - 'No Data Available' will display when searched data combination does not exist

Navigation:

- Edit the search fields and click **Run Summary Report** to rerun report
- Click the **Supply Code** to view Detail Report
- Click the relevant Service in the Point(s) of Contact list to send email

SPRS Color Legend

Top 5%:	BLUE
Next 10%:	PURPLE
Next 70%:	GREEN
Next 10%:	YELLOW
Lowest 5%:	RED
No Scorable Data:	WHITE (*)
Scorable Data Pending:	GREEN (**)
Vendor Excluded:	GREY
No Score:	BLACK

Supply Code	Weighted Delivery Score	Weighted Quality Performance
1630	0 (0 Records)	Color YELLOW (1 Records)
2910	0 (0 Records)	Color RED (1 Records)
3130	0 (0 Records)	Color RED (1 Records)
4730	0 (0 Records)	Color RED (1 Records)

Point(s) of Contact:

Services - Click on the link to send email

- AIR FORCE,ALC HILL,ALC ROBINS,ALC TINKER
- ARMY
- DAPS,DCSO,DDC,DESC,DNSC,DRMS,DSC RICHMOND
- DLA,DLA DELIVERY,GENERAL PROGRAM,MARINE,USMC/NAVY
- DSC COLUMBUS
- DSC PHILADELPHIA

Figure 69: Summary Report

Summary Report Detail

The Detail Report retrieves the positive and negative records for the particular CAGE/Supply Code selected. The top section includes the searched criteria, challenge legend, vendor information: basic (default selection) or detailed buttons, and the negative (default selection) and positive records display buttons.

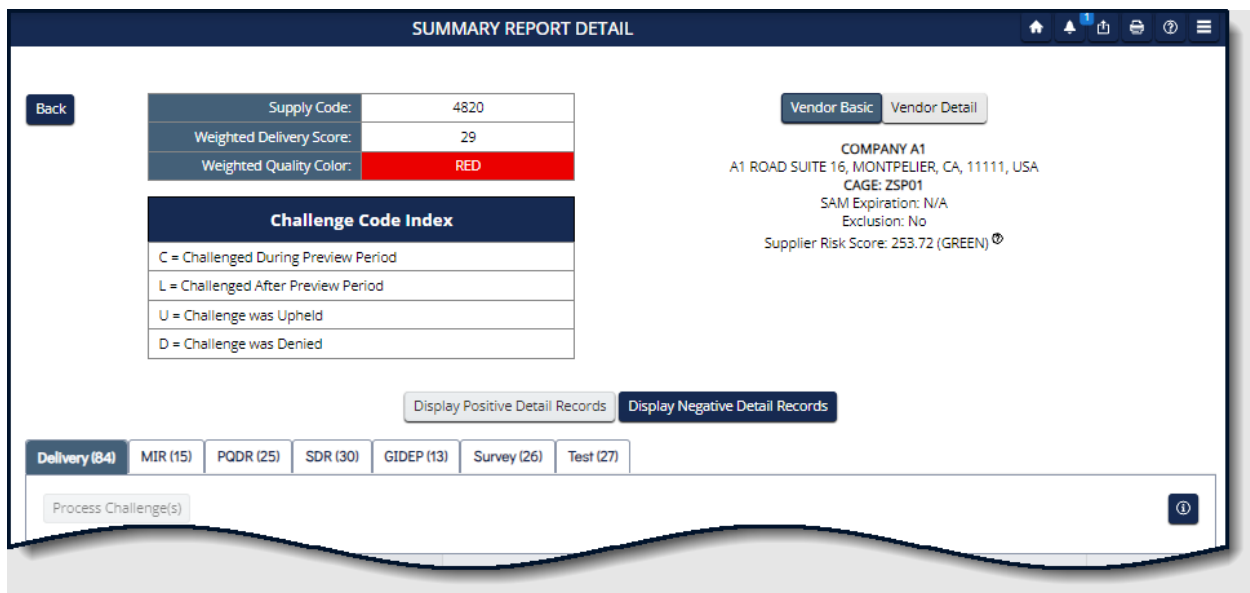


Figure 70: Summary Report Detail

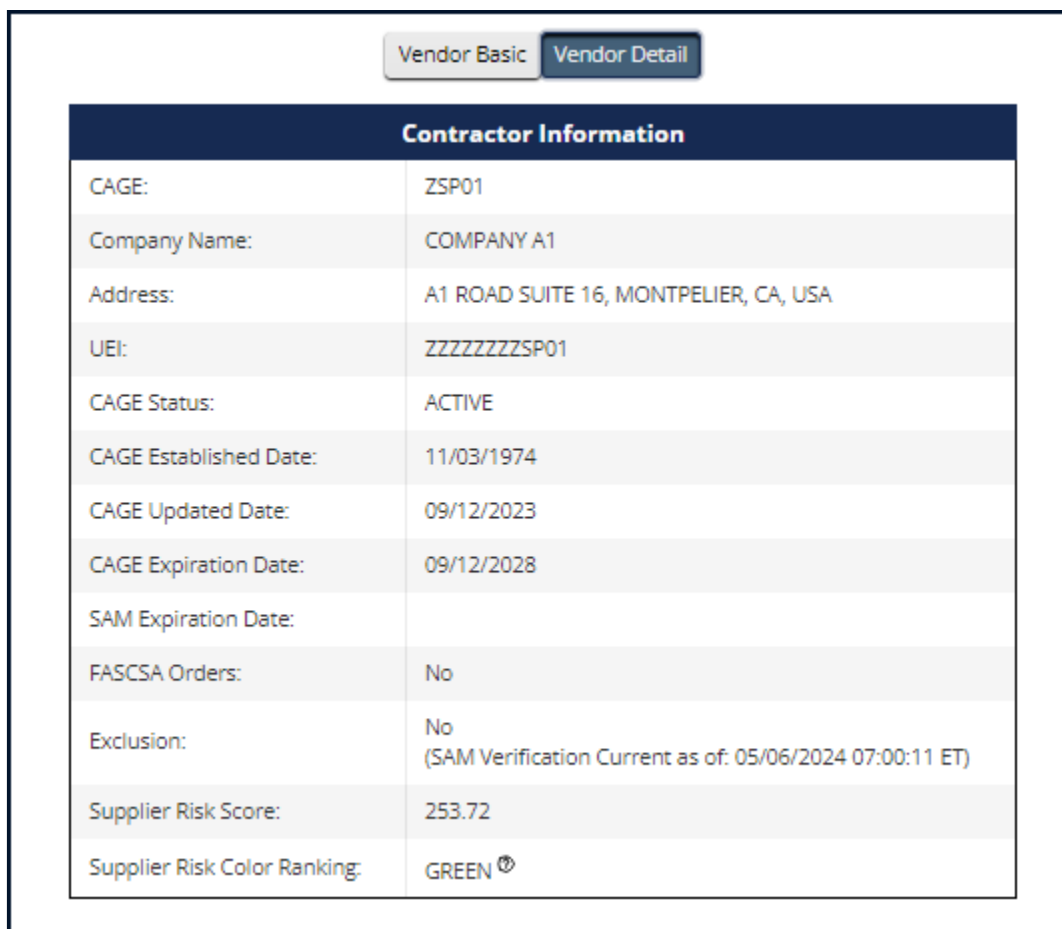


Figure 71: Summary Report Detail

The bottom section displays the negative or positive record types listed below, each on a separate tab. Record counts in parenthesis reflect the total of scored and unscored records available for that record type. In the **Scored** column, a **Y** indicates a scored record and **N** indicates an unscored. Records can be unscored during the 14-day preview period, while adjudication after being challenged during the preview period, or awaiting new data after a challenge is upheld. The system lists unscored records first sorted by Contract Reference for Delivery records, and Serial or Report Control number for quality records. The system lists scored records next, sorted the same way.

Negative Record Types:

- **Delivery** – Delivery Records
- **MIR** – Material Inspection Record(s)
- **PQDR** – Product Quality Deficiency Report(s)
- **SDR** – Supply Discrepancy Report(s)
- **GIDEP** – Government-Industry Data Exchange Program Alert(s)
- **Survey** – Survey Report(s)
- **Test** – Test Report(s)

Challenge	Scored	Contract Reference	Supply Code/NSN	Due Date	Ship/Rec Date	Termination Date	Termination Code	Associated Quality Record	Department/Agency	Added Date
<input type="checkbox"/>	N	SPRSXXZSP01003CTRNUM	4820014850042	10/17/2023	01/22/2024			Y	USMC/NAVY	01/24/2024
<input type="checkbox"/>	N	SPRSXXZSP010020CTRNUM	4820014700480	10/17/2023	01/22/2024			Y	USMC/NAVY	01/24/2024
N/A	N	SPRSXXZSP01001CTRNUM	4820014700480	10/17/2023	01/22/2024			Y	USMC/NAVY	01/24/2024
N/A	N	SPRSXXZSP010019CTRNUM	4820014850042	10/17/2023	01/22/2024			Y	USMC/NAVY	01/24/2024
<input type="checkbox"/>	Y	WARMYXZSP01000003	4820	10/19/2023	11/06/2023			N	GENERAL PROGRAM	11/16/2023

Figure 72: Summary Report Negative Detail

Positive Record Types:

- **Delivery** – Delivery Records
- **MIR** – Material Inspection Record(s)
- **Survey** – Survey Report(s)
- **Test** – Test Report(s)

Display Positive Detail Records Display Negative Detail Records									
Delivery (8) MIR (8) Survey (6) Test (6)									
Positive Delivery Record(s) - (8)									
Scored	Contract Reference ↓	Supply Code/ NSN	Due Date	Ship/Rec Date	Reason For Delay Code	Associated Quality Record	Department/Agency	Added Date	
Y	SPRSXZSP01PO59	4820014700480	11/26/2023	11/16/2023		N	DLA DELIVERY	11/21/2023	
Y	SPRSXZSP01PO58	4820014700480	11/26/2023	11/16/2023		N	DLA DELIVERY	11/21/2023	
Y	SPRSXZSP01PO57	4820014700480	11/26/2023	11/16/2023		N	DLA DELIVERY	11/21/2023	
Y	SPRSXZSP01PO56	4820015068050	11/26/2023	11/16/2023		N	DLA DELIVERY	11/21/2023	
Y	ARMYXXZSP01PO55	4820100000076	11/26/2023	11/16/2023		N	DLA DELIVERY	11/21/2023	
Y	ARMYXXZSP01PO5	4820100000076	11/26/2023	11/16/2023		N	DLA DELIVERY	01/24/2024	
Y	AFXXXZSP01PO54	4820014700480	11/26/2023	11/16/2023		N	DLA DELIVERY	11/21/2023	
Y	AFXXXZSP01PO4	4820014700480	11/26/2023	11/16/2023		N	DLA DELIVERY	01/24/2024	

1 20 Items per page 1 - 8 of 8 Items

Figure 73: Summary Report Positive Detail

Navigation by single click:

- **Back** button to return to the overview page
- Record tab to review that record type
- **Display Positive Detail Records** to view positive data
- **Display Negative Detail Records** to view negative data
- **Process Challenge** after checking the record **Challenge** box
- Three vertical dots in the column title access a sort and filter menu
- Items per page selected from the dropdown
- Scroll bars to view information out of the page view

Users may challenge records they believe are inaccurate. Challenging a record requires objective quality evidence (OQE). Some examples of OQE include PDFs of government receiving reports (ex. WAWF), contract terms, and modifications. Correspondence with the Contracting Officer or Contracting Specialist, and Bill of Lading documents that show receiving date and signature.

Records may be challenged twice (2x). An N/A in the Challenge column identifies that the record is not available to challenge. There are two possible reasons: either the record has been challenged and is under review, or the record has been challenged twice.

Challenged preview period or unscored (N) records are not visible to the government or used in scoring while they are waiting for adjudication. **C** in the **Challenge Code** column identifies these records.

Challenged scored (Y) records are visible to government personnel and used in scoring. **L** in the **Challenge Code** column identifies these records.

The **Challenge Code** column shows **U** (Upheld) or **D** (Denied) after adjudication. The system uses Denied records in scoring but waits for revised data before scoring Upheld records.

NOTE: Instructions for challenging a record are available in Appendix D: CHALLENGE PROCESS.

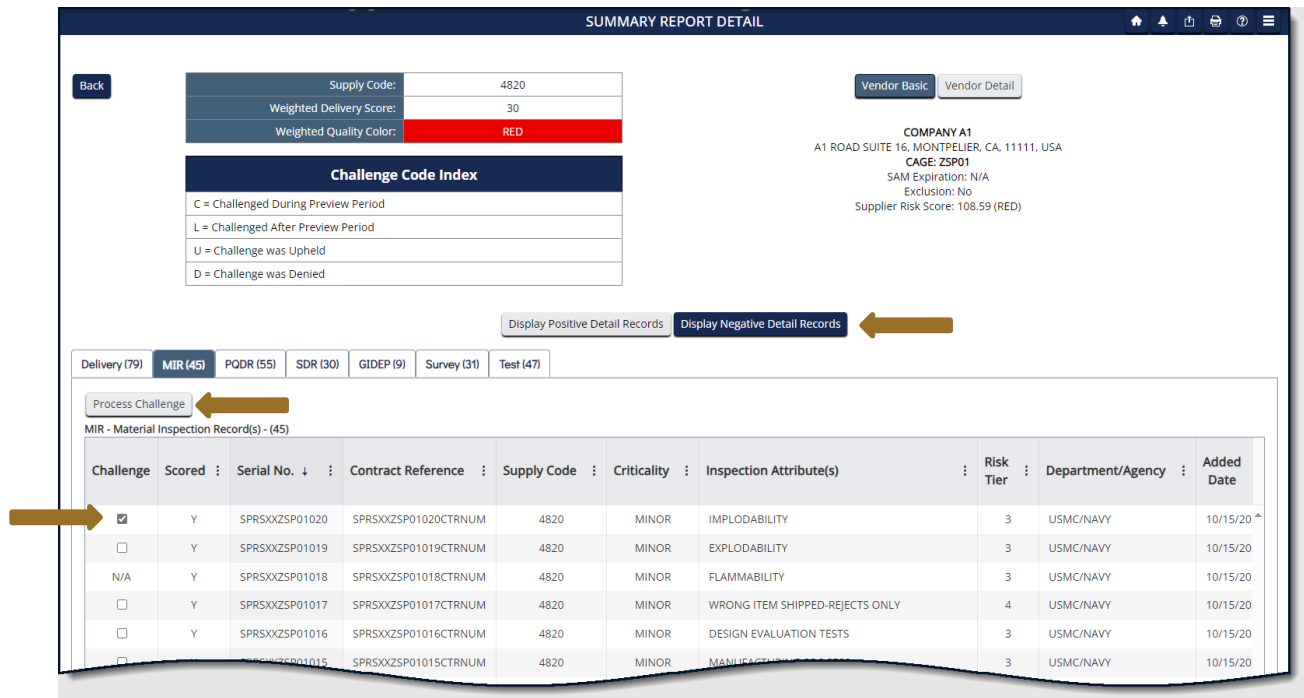


Figure 74: Contractor Detailed Report

After selecting one or many records, click the **Process Challenge** button to open the dated Challenge Submission pop-up with the destination email address, selected record(s), and record details. Provided for the user is a mandatory **Enter Message** box to explain why they believe the record is inaccurate. The **Select files** button, allows the user to attach supporting documentation. Users will not receive a copy of the email but may click the **Save As PDF** button to save a copy before clicking **Submit** to email the adjudicator(s).

Navigation by single click (Challenge submission):

- Type a short, detailed message in **Enter Message** box
- **Select Files** to attach files, OQE, supporting the challenge message
- **Save As PDF** to save a PDF copy of the challenge
- **Submit** to email the POC identified for the record
- **Cancel** to clear submission & return to Summary Report Detail

Quality Challenge

Challenge Type: MIR
Challenge Date: 01/22/2024

Email Sent To	CAGE Code	Contract Reference	Serial No.	Supply Code
SPRSINFO.fct@navy.mil	ZSP01	SPRSXXZSP01020CTRNUM	SPRSXXZSP01020	4820

Enter Message:

Attach documentation supporting above challenge statements. (Suggest PDF. Max 2 MB file)

Select files... Drop files here to select

Cancel Submit

Figure 75: Challenge Record Email

NOTE: Users will not receive a copy of the original email. They will receive an email once the challenge has been adjudicated, explaining the decision to uphold or deny.

7.2 DETAIL POS/NEG RECORDS

The Detail Pos/Neg Records report, similar to the Summary Report, displays the Supply Code classifications associated with the users CAGE data received by SPRS within the last three (3) years. However, this simplified report does not include scoring, or segregate data by Supply Code. The report segregates by data type all positive or negative records associated with the selected CAGE from the users PIEE profile. The user may refine the report by entering specific Supply Codes of either Supply Code type: FSC/PSC or NAICS.

Delivery records are negative for the following reasons: terminated by default, no Ship/Receiving date received, or Ship/Receiving date received is past Due Date. Quality records are negative as identified by the data source.

The report includes scored and unscored, preview period, records. The preview period for a record is fourteen (14) days from the added date and applies only to negative records. Preview period records are visible here and in the Summary Report to the vendor only. They are not included in reporting provided to acquisition professionals.

Use the Challenge process to address any data inaccuracy identified in this report. See Summary Report or **Appendix D: CHALLENGE PROCESS** for instructions.

To access the Detail Pos/Neg Records:

Select [Detail Pos/Neg Records](#) from the Menu.

- Select a CAGE from the dropdown
- Click either Display button (Positive or Negative Detail Records)
- Or, further refine the search
 - Click NAICS to change the Supply Code type
 - Type or paste one or many comma delimited Supply Codes into Supply Code box

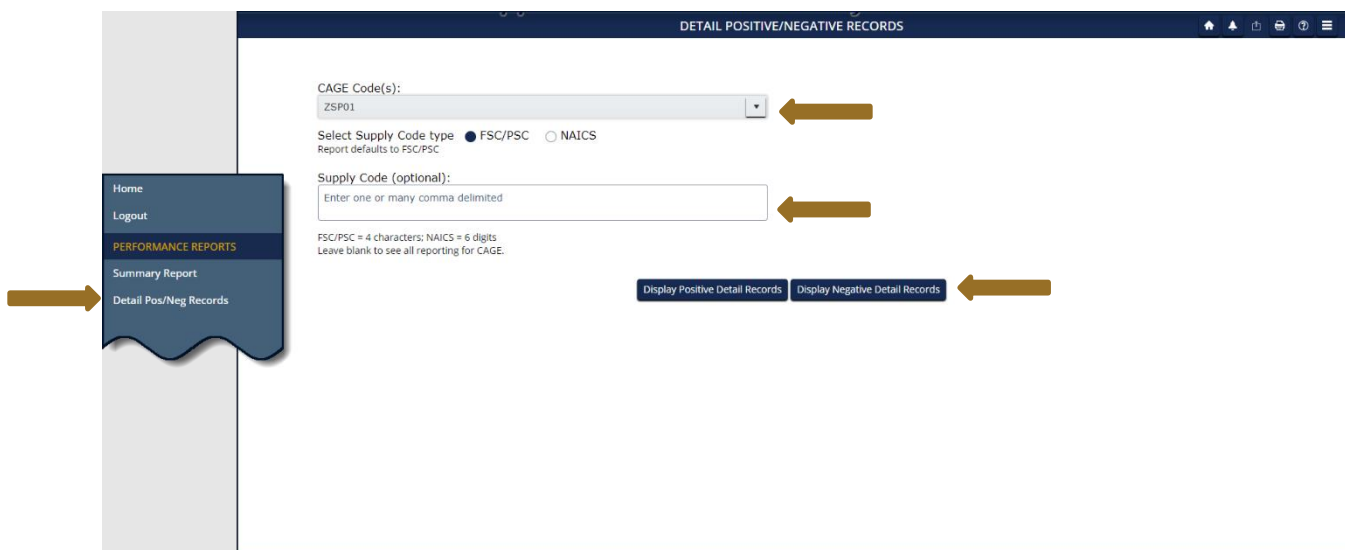


Figure 76: Detail Pos/Neg Records Report Request

The top section includes the search fields with the searched criteria, vendor information: basic (default) or detailed, and Toolbar.

The bottom section displays the selected negative or positive records. Record types listed on tabs display the record count in parenthesis (). The count is the total of negative scored and unscored or positive records available for that record type. In the **Scored** column, a **Y** indicates a scored record and **N** indicates an unscored, preview period, record.

Negative Record Types:

- **Delivery** – Delivery Records
- **MIR** – Material Inspection Record(s)
- **PQDR** – Product Quality Deficiency Report(s)
- **SDR** – Supply Discrepancy Report(s)
- **GIDEP** – Government-Industry Data Exchange Program Alert(s)
- **Survey** – Survey Report(s)
- **Test** – Test Report(s)

The screenshot shows the 'DETAIL POSITIVE/NEGATIVE RECORDS' interface. At the top, there are navigation icons and a title bar. Below the title bar, there are search and filter options: 'CAGE Code(s): ZSP01', 'Vendor Basic' and 'Vendor Detail' buttons, 'Select Supply Code type' with radio buttons for 'FSC/PSC' (selected) and 'NAICS', and a 'Supply Code (optional):' input field. A company profile for 'COMPANY A1' is displayed on the right, including address, CAGE code, SAM expiration, exclusion status, and supplier risk score. Below these are buttons for 'Display Positive Detail Records' and 'Display Negative Detail Records'. A tabbed interface shows 'Delivery (79)' as the active tab, with other tabs for MIR (48), PQDR (48), SDR (65), GIDEP (16), Survey (37), and Test (38). The main content area displays a table of 'Negative Delivery Record(s) - (79)' with columns: Scored, Contract Reference, Supply Code/NSN, Due Date, Ship/Rec Date, Termination Date, Termination Code, Associated Quality Record, Department/Agency, Added Date, and Challenge Code. The table contains several rows of data, including records for contract references TIMXXZSP01N4, SPRSXXZSP01003CTRNUM, SPRSXXZSP010020CTRNUM, SPRSXXZSP01001CTRNUM, SPRSXXZSP010019CTRNUM, and KEVINXZSP01N5.

Scored	Contract Reference	Supply Code/NSN	Due Date	Ship/Rec Date	Termination Date	Termination Code	Associated Quality Record	Department/Agency	Added Date	Challenge Code
N	TIMXXZSP01N4	AJ94100000076	10/17/2023	01/22/2024			N	DLA DELIVERY	01/24/2024	
N	SPRSXXZSP01003CTRNUM	4820014850042	10/17/2023	01/22/2024			Y	USMC/NAVY	01/24/2024	
N	SPRSXXZSP010020CTRNUM	4820014700480	10/17/2023	01/22/2024			Y	USMC/NAVY	01/24/2024	
N	SPRSXXZSP01001CTRNUM	4820014700480	10/17/2023	01/22/2024			Y	USMC/NAVY	01/24/2024	C
N	SPRSXXZSP010019CTRNUM	4820014850042	10/17/2023	01/22/2024			Y	USMC/NAVY	01/24/2024	C
N	KEVINXZSP01N5	AJ94100000076	10/17/2023	01/22/2024			N	DLA DELIVERY	01/24/2024	
N		AJ94100000076	10/17/2023	01/22/2024			N	DLA DELIVERY	01/24/2024	

Figure 77: Detail Negative Recordshi

Positive Record Types:

- **Delivery** – Delivery Records
- **MIR** – Material Inspection Record(s)
- **Survey** – Survey Report(s)
- **Test** – Test Report(s)

The screenshot displays the 'DETAIL POSITIVE/NEGATIVE RECORDS' interface. At the top, there are navigation tabs for 'Vendor Basic' and 'Vendor Detail'. The 'Vendor Basic' tab is active, showing company information for 'COMPANY A1' located at 'A1 ROAD SUITE 16, MONTPELIER, CA, 11111, USA'. The CAGE Code is 'ZSP01', SAM Expiration is 'N/A', Exclusion is 'No', and Supplier Risk Score is '65.93 (RED)'. Below this, there are buttons for 'Display Positive Detail Records' and 'Display Negative Detail Records'. The 'Display Positive Detail Records' button is active, and the 'Delivery (8)' tab is selected. The main content area shows a table of 'Positive Delivery Record(s) - (8)' for CAGE Code: ZSP01. The table has columns for 'Scored', 'Contract Reference', 'Supply Code/NSN', 'Due Date', 'Ship/Rec Date', 'Reason For Delay Code', 'Associated Quality Record', 'Department/Agency', and 'Added Date'. The table contains 8 rows of data, all with a 'Scored' value of 'Y' and an 'Associated Quality Record' value of 'N'. The 'Department/Agency' for all records is 'DLA DELIVERY'. The 'Added Date' for most records is '11/21/2023', with one record dated '01/24/2024'.

Scored	Contract Reference	Supply Code/NSN	Due Date	Ship/Rec Date	Reason For Delay Code	Associated Quality Record	Department/Agency	Added Date
Y	SPRSXXZSP01POS9	4820014700480	11/26/2023	11/16/2023		N	DLA DELIVERY	11/21/2023
Y	SPRSXXZSP01POS8	4820014700480	11/26/2023	11/16/2023		N	DLA DELIVERY	11/21/2023
Y	SPRSXXZSP01POS7	4820014700480	11/26/2023	11/16/2023		N	DLA DELIVERY	11/21/2023
Y	SPRSXXZSP01POS6	4820015068050	11/26/2023	11/16/2023		N	DLA DELIVERY	11/21/2023
Y	ARMYXXZSP01POS5	4820100000076	11/26/2023	11/16/2023		N	DLA DELIVERY	11/21/2023
Y	ARMYXXZSP01POP5	4820100000076	11/26/2023	11/16/2023		N	DLA DELIVERY	01/24/2024
		4820014700480	11/26/2023	11/16/2023			DLA DELIVERY	11/21/2023

Figure 78: Detail Report Positive Records

Navigation by single click:

- Record tab to review that record type
- **Display Positive Detail Records** to view positive data
- **Display Negative Detail Records** to view negative data
- Three vertical dots in the column title access a sort and filter menu
- Column title to sort by ascending/descending (excluding **Scored**)
- Items per page selected from the dropdown
- Scroll bars to view information out of the page view

NOTE: Identify the FSC/PSC for any records believed to be inaccurate to make it easier to challenge the record in the Summary Report (See Appendix D: CHALLENGE PROCESS). The FSC/PSC is the first four (4) characters of the NSN.

7.3 SUPPLY CODE RELATIONSHIP REPORT

The Supply Code Relationship report displays the current relationships between Federal Supply Code/Product Service Code (FSC/PSC) and North American Industry Classification System (NAICS) supply types. Government buying offices use FSC/PSC codes to categorize the various government products, supplies, and services. NAICS codes identify products and services by industry or business sector.

SPRS collects source data in either supply type, FSC/PSC or NAICS. This report identifies the translation SPRS uses to convert one supply type to the other.

SPRS uses relationship data from the PSCTool, <https://psctool.us/home>, maintained by the Defense Pricing and Contracting (DPC) office and the Federal Procurement Data System Product Codes Manual for these translations.

Users may search for specific supply codes or run the report to see all relationships organized by the supply type selected.

To access Supply Code Relationship:

Select [Supply Code Relationship](#) from the Menu.

- Select the **Search/Sort by** Supply Type for the search, default FSC/PSC
- Enter up to five (5) different Supply Codes in the Code List
- Click **Search**
- Or
- Click **Show All**

SUPPLY CODE RELATIONSHIP REPORT

This report is an administrative helper tool to enable the user to verify the current data integrity relationships between FSC/PSC to NAICS and NAICS to FSC/PSC supply codes. You can use the report to search for specific supply codes, or by selecting the 'Display All Relationships' button see the entire matrix.

This data and its relationships are updated whenever new codes are added.

General Search Instructions:
Select one of the following radio buttons in order to search or to sort by either FSC/PSC or NAICS Supply Code:

Search/Sort by: FSC/PSC NAICS

Code List:

Search

Display All Relationship Instructions
Selecting this link will provide a complete listing of all FSC/PSC to NAICS code relationships and their descriptions sorted by the Supply Code selected in the 'Search/Sort' radio buttons, and then sub-sorted by the other code.

Show All

Figure 79: Supply Code Relationship Request

The top section includes the search fields with the searched criteria, if applicable.

The bottom section displays the Supply Type, Supply Code, and Description for both the searched and result data.

SUPPLY CODE RELATIONSHIP REPORT

This report is an administrative helper tool to enable the user to verify the current data integrity relationships between FSC/PSC to NAICS and NAICS to FSC/PSC supply codes. You can use the report to search for specific supply codes, or by selecting the 'Display All Relationships' button see the entire matrix.

This data and its relationships are updated whenever new codes are added.

General Search Instructions:
Select one of the following radio buttons in order to search or to sort by either FSC/PSC or NAICS Supply Code:

Search/Sort by: FSC/PSC NAICS

Code List:

Search

Display All Relationship Instructions
Selecting this link will provide a complete listing of all FSC/PSC to NAICS code relationships and their descriptions sorted by the Supply Code selected in the 'Search/Sort' radio buttons, and then sub-sorted by the other code.

Show All

Search Type	Search Code	Search Description	Result Type	Result Code	Result Description
FSC/PSC-NAICS	4730	HOSE PIPE TUBE LUBRICATION AND RAILING FITTINGS	FSC/PSC-NAICS	326122	PLASTICS PIPE AND PIPE FITTING MANUFACTURING
FSC/PSC-NAICS	4730	HOSE PIPE TUBE LUBRICATION AND RAILING FITTINGS	FSC/PSC-NAICS	332919	OTHER METAL VALVE AND PIPE FITTING MANUFACTURING
FSC/PSC-NAICS	4730	HOSE PIPE TUBE LUBRICATION AND RAILING FITTINGS	FSC/PSC-NAICS	332996	FABRICATED PIPE AND PIPE FITTING MANUFACTURING

1 - 3 of 3 items

Figure 80: FSC/PSC to NAICS example

Navigation by single click:

- **Search** to view specific Supply Codes
- **Show All** to view all Supply Code Relationship data
- Three vertical dots in the column title access a sort and filter menu
- Items per page selected from the dropdown

8. SERVICE

8.1 FEEDBACK/CUSTOMER SUPPORT

Feedback/Customer Support allows the user to submit feedback, suggestions and questions about the application to the SPRS Program Management Office (PMO). Responses to these communications will be visible in the same Feedback/Customer Support module within 48 business hours. Additional comments or questions on the topic may be added to this numbered conversation until it is closed.

To access Feedback/Customer Support:

Select [Feedback/Customer Support](#) from the Menu or the Feedback button at the top of the page.

NOTE: This section is not for 'challenge' or disputed data information.

- Click **New Feedback** to begin

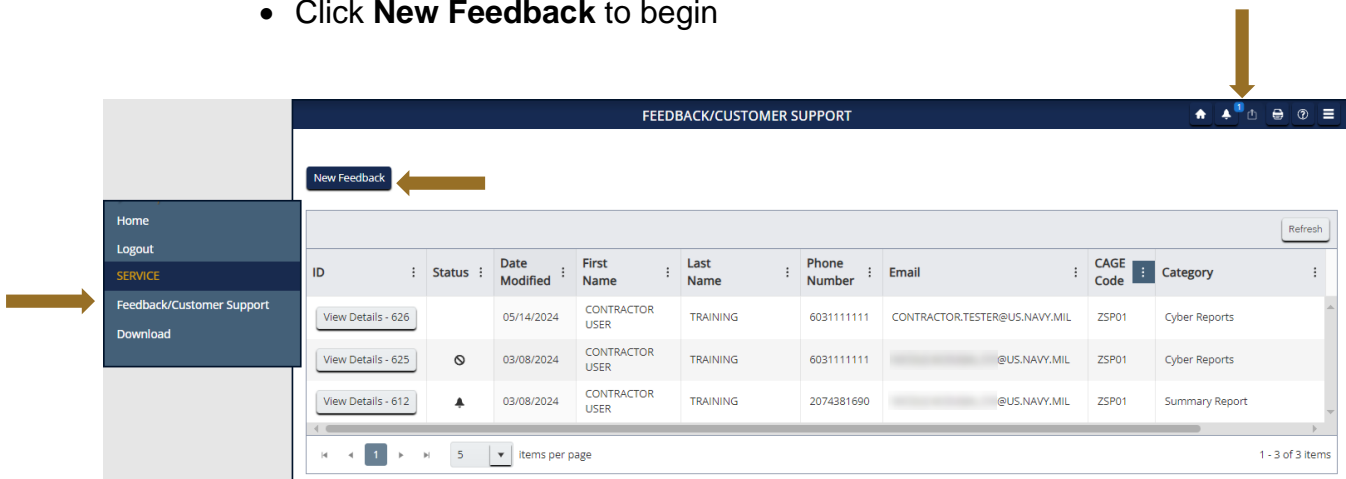



Figure 81: Feedback/Customer Support Window

- Select **CAGE code** from the dropdown
- POC name and email are prepopulated
- Select appropriate **Category** from the dropdown list
- Enter POC **Phone**
- Enter **Other Category** title if category selected is "Other Category"
- Add comments to the **Comment** section
- Click **Select files** button to attach files (If troubleshooting an issue, it may be helpful to attach a screenshot)
- Click the **Submit** button
- Or click **Cancel**, entries will not be saved

Figure 82: Feedback/Customer Support Window

The submission will appear in the grid below with a conversation identification number (**ID**) and basic details, including the date that the conversation was last modified. The **Date Modified** column is the default sort for conversations with most recent listed first.

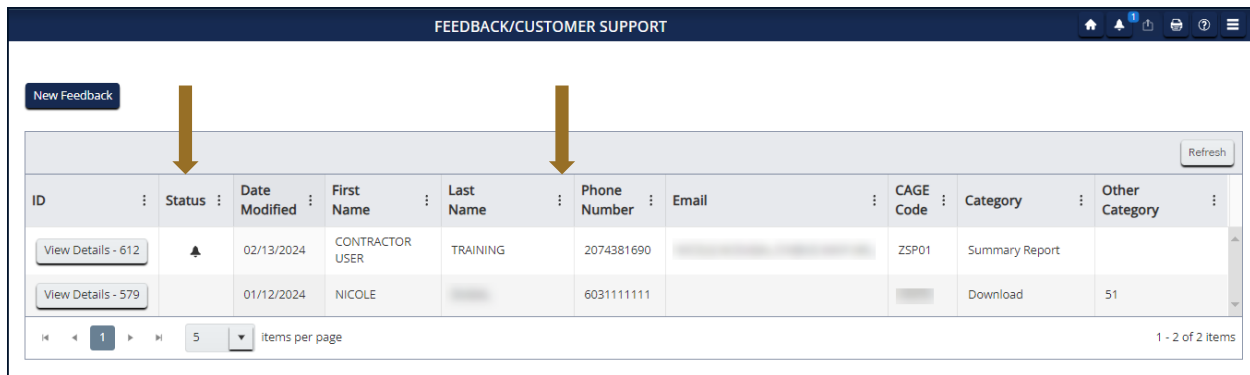
A number will appear near the Feedback toolbar button () in the header when a response is available.

- Click the **Feedback** bell icon or **Feedback/Customer Support** from the left-hand menu
- Click the **View Details** button to view response(s) or add comments

ID	Status	Date Modified	First Name	Last Name	Phone Number	Email	CAGE Code	Category	Other Category
View Details - 612		02/13/2024	CONTRACTOR USER	TRAINING	2074381690		ZSP01	Summary Report	
View Details - 579		01/12/2024	NICOLE		6031111111			Download	51

Figure 83: Feedback/Customer Support Submitted

- Click the three vertical dots in a column title to sort or filter.
- A bell icon in the **Status** column indicates a response has been sent
- A circle with a line in the **Status** column indicates the conversation is closed
 - Conversations are closed the Friday of the week following the last comment response.



ID	Status	Date Modified	First Name	Last Name	Phone Number	Email	CAGE Code	Category	Other Category
View Details - 612	🔔	02/13/2024	CONTRACTOR USER	TRAINING	2074381690		ZSP01	Summary Report	
View Details - 579	🚫	01/12/2024	NICOLE		6031111111			Download	51

Figure 84: Feedback/Customer Support Status

8.2 DOWNLOAD

The Download module serves as a repository for all downloaded reports requested within the last five (5) days. Download ready files are listed after being requested in other SPRS modules.

To receive a download, select the Export button in the Toolbar. SPRS will export into excel the report of the module where the Downloads button was selected.

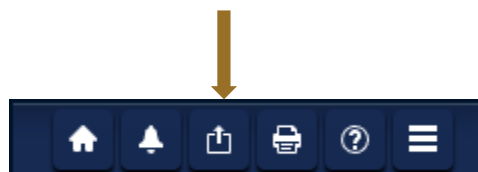


Figure 85: Export

SPRS will send an emailed message indicating that a requested file is ready for download.

NOTE: Users should check their Spam or Junk folders for the email notification.

To access Download:

Select [Download](#) from the Menu.

The table displayed contains the following information:

- **Requested Date** – is the day and time the user requested the file from a specific module
- **Export Module** – is the specific module that generates the file upon request
- **Export Criteria** – represents the values filtered by the user to generate the report
- **Filename** – is the module_CAGE_and date/time from which the file is generated
- **Download Status** – will read either in Queue or Ready to Download
- **Downloaded Date** – is the date and time the file was last retrieved by the user.

NOTE: The file will only be available for five (5) days from the time of its generation. After that period, a new report will need to be requested through the originating module

This 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, the report will automatically be removed from this list.

	Download Status	Requested Date	Export Module	Export Criteria	Filename	Download
	In Queue	06/10/2024 12:41:24 ET	Supply Code Relationship	Supply Code: Relationship Type: PSC-NAICS		
Download	Ready To Download	06/10/2024 12:33:41 ET	Cyber Reports	CAGE Code: ZSP01	Cyber_ZSP01_06102024-123703.xlsx	
Download	Ready To Download	06/10/2024 12:32:52 ET	Summary Report	Supply Type: FSC/PSC CAGE Code: ZSP01 Supply Code: 4820	SummaryNegativeRecordsList_ZSP01_06102024-123701.xlsx	
Download	Ready To Download	06/10/2024 12:32:38 ET	Supplier Risk	CAGE Code: ZSP01	SupplierRisk_ZSP01_06102024-123700.xlsx	

1 - 4 of 4 items

Figure 86: Download module

9. TRAINING MATERIALS

The SPRS web page provides a variety of public resources accessible by selecting from the pop-out menu and buttons.

To access the SPRS web page:



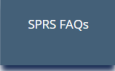
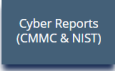

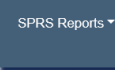

Select the  icon from the Menu in the SPRS application, or <https://www.sprs.csd.disa.mil/>.



Figure 87: SPRS Web Landing Page

Navigation:

-  - Login/Register (via P1EE) button for redirection to the Procurement Integrated Enterprise Environment (P1EE)
-  - Frequently Asked Questions for using the SPRS Application
-  - Cyber Reports (CMMC & NIST) for CMMC and NIST SP 800-171 to display related training and information
-  - OSD Instructions GPC & Contracting button to display a PDF of Recommended SPRS Reports for MPT Card holder Review
-  - SPRS Reports button to display information for select SPRS reports

 Click the Menu icon to display a pop-out menu

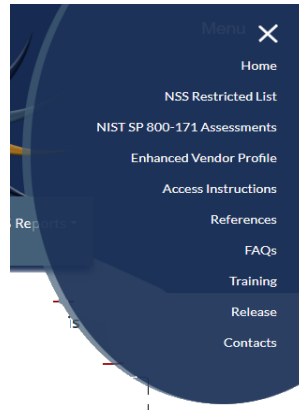


Figure 88: SPRS Pop-Out Menu

Home - Return to the SPRS web-landing page

NSS Restricted List - Restricted Government-only

NIST SP 800-171 Assessments - Restricted Government-only

Enhanced Vendor Profile - Restricted Government-only

Access Instructions - Access Instructions for Government and Supplier/Vendor

References - User Guides and relevant policy guidance

FAQs - SPRS Frequently Asked Questions (FAQs)

Training - SPRS on-line and instructor-led Training Opportunities

Release - SPRS application changes

Contacts - SPRS program office contact information

REFERENCED DOCUMENTS

The following documents of the exact issue shown form a part of this document to the extent specified herein.

DOCUMENTS REFERENCED IN THIS USER'S GUIDE	
DOCUMENT	LOCATION
Privacy Act of 1974	<u>https://www.justice.gov/oip/foia-resources</u>
SPRS Evaluation Criteria	<u>https://www.sprs.csd.disa.mil/pdf/SPRS_DataEvaluationCriteria.pdf</u>
SPRS CMMC Quick Entry Guide Level 1	<u>https://www.sprs.csd.disa.mil/pdf/CMMCQuickEntryGuide.pdf</u>
SPRS CMMC Quick Entry Guide Level 2	<u>https://www.sprs.csd.disa.mil/pdf/CMMCL2SelfQuickEntryGuide.pdf</u>
SPRS NIST Quick Entry Guide	<u>https://www.sprs.csd.disa.mil/pdf/NISTSP800-171QuickEntryGuide.pdf</u>
DFARS 204.7603	<u>https://www.acquisition.gov/dfars/204.7603-procedures</u>
DoDI 5000.79	<u>https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500079p.PDF?ver=2019-10-15-115609-957</u>

GLOSSARY

This section provides definitions for acronyms, abbreviations and terms used in SPRS.

ACRONYM/ ABBREVIATION	DEFINITION
AO	Affirming Official
CAGE Code	Commercial and Government Entity Code
CAM	Contractor Account Administrator
CAP	Corrective Action Plan
CAR	Corrective Action Request
CDA	Central Design Activity
CMMC	Cybersecurity Maturity Model Certification
DLA	Defense Logistics Agency
DoD	Department of Defense
EBPOC	Electronic Business Point of Contact
FLIS	Federal Logistics Information System
FPDS	Federal Procurement Data System
FSC/PSC	Federal Supply Classification/Product Service Code
JDRS	Joint Deficiency Reporting System
HLO	Highest Level Owner
NAICS	North American Industry Classification System
NIST SP	National Institute of Standards and Technology Special Publication
NSLC	Naval Sea Logistics Center
NSN	National Stock Number
NSS	National Security Systems
OQE	Objective Quality Evidence
OSA	Organization Seeking Assessment
PDF	Portable Document Format
PDREP	Product Data Reporting and Evaluation Program
PIEE	Procurement Integrated Enterprise Environment
PMO	Program Management Office
POC	Point of Contact
POD	Proof of Delivery
PQDR	Product Quality Deficiency Report
SAM	System for Award Management
SPRS	Supplier Performance Risk System
UEI	Unique Entity Identifier

ACRONYM/ ABBREVIATION	DEFINITION
UID	Unique Identifier
WAWF	Wide Area Workflow

SPRS USER ROLES

TERM	DESCRIPTION
Contractor/Vendor (Support Role) Access	View company information View Vendor Summary Reports View company CMMC and NIST SP 800-171 Assessments View CAGE Hierarchy Execute Supply Code Relationship Reports Execute Supplier Risk Report View Vendor Detailed Reports File a Challenge, if necessary Provide customer feedback
SPRS Cyber Vendor User Access	Add/Edit/View company CMMC and NIST SP 800-171 assessment results View CAGE Hierarchy

TROUBLESHOOTING


Should assistance with SPRS be required, read the following troubleshooting hints and tips to help determine the point of contact (POC) for assistance.

Common SPRS Issues		
PROBLEM	DIAGNOSIS	POC
SPRS doesn't execute	Confirm using recommended browser. List available on the application main page.	Once browser is confirmed, email <u>sprs-helpdesk@us.navy.mil</u> for additional assistance
SPRS is not running efficiently. Isolated or widespread?	If widespread, possible local PC issue or local network issues. Try refreshing the page.	Local IT personnel (a trace route and/or a set of pings would be helpful) If Local IT cannot resolve, email <u>sprs-helpdesk@us.navy.mil</u>
SPRS is unavailable	SPRS may be running a batch job which typically run between 2300 and 0200 GMT	If outside batch job timeframe, email <u>sprs-helpdesk@us.navy.mil</u>
* When local network engineers are involved, a trace route or a set of pings or both would be very helpful to have when calling.		

For any problems or questions while using the system, contact the Help Desk at: [**sprs-helpdesk@us.navy.mil**](mailto:sprs-helpdesk@us.navy.mil) for assistance.

NOTE: When emailing it is helpful to include the web browser, P1EE user id, the URL, and screenshots of the issue.

MENU ITEMS

ITEM	DESCRIPTION
	Opens SPRS web landing page for resource tools
Home	Returns the user to the SPRS application landing page
Logout	Used to log out of SPRS
COMPLIANCE REPORTS	
Cyber Reports	Enables authorized users to enter results and DoD to assess a contractor's implementation of NIST SP 800-171 and CMMC
CAGE Hierarchy	Identifies the CAGEs associated with the user's profile in PIEE and their relationship to each other
RISK ANALYSIS REPORTS	
Supplier Risk Report	Supplier Risk Score and the data that it comprises
PERFORMANCE REPORTS	
Summary Report	Allows users to monitor the records used to calculate the Quality, Delivery, and Supplier Risk scores for specified CAGE or CAGE/Supply Code and challenge inaccurate data
Detail Pos/Neg Records	Displays the same records found in the Summary Report organized into simple Positive or Negative reports with Preview Period Records (Negative reports only) sectioned for quick review
Supply Code Relationship Report	Identifies the current data integrity relationships between FSC/PSC to NAICS and NAICS to FSC/PSC supply codes
SERVICE	
Feedback/Customer Support	Allows users to ask questions and provide suggestions to improve the application
Download	Allows users to have an Excel Spreadsheet of a report. Once the Export button is pressed on the report, when ready it will appear in the Download module.

CHALLENGE PROCESS

Delivery Scores and Quality Performance are calculated on a daily basis. Fluctuation in scoring may be the result of other vendors' scoring and not the result of a change in the CAGE data. It is the responsibility of the user to monitor their SPRS data and 'challenge' when they believe data is inaccurate. Users must have objective quality evidence (OQE) to support their claim.

Steps to Challenge a Record in the SPRS application:

1. Identify the FSC/PSC associated with the inaccurate record
 - a. The FSC/PSC is the first four (4) characters of the NSN
2. Note the record type (Delivery, MIR, PQDR, etc.)
3. Click the Summary Report in the Menu bar
4. Select the CAGE and click the **Run Summary Report** button
5. Click the relevant FSC/PSC to open the Detail Report
6. Click the relevant record type tab (Delivery, MIR, PQDR, etc)
7. Locate the inaccurate data record
8. Click the box in the Challenge column of the record
9. Click the **Process Challenge(s)** button just below the record type tabs
10. A window will open labeled **Delivery Challenge** or **Quality Challenge**
11. Write brief comments detailing reason for challenge in the message area
12. Click the **Select file(s)** button to attach the OQE
13. Optional* Click the **Save As PDF** button to save a copy of the submission
 - a. Users do not receive a copy of the email
14. Click the **Submit** button
15. A **System update in progress** pop-up will appear and remain until process completion
16. Click the **Ok** button when the **Email sent** pop-up appears

Click the **Cancel** button to close Challenge without sending, records will be cleared, and no draft will be saved

The government POC adjudicator may request more information or simply uphold or deny the challenge. Users will receive a SPRS system email indicating the decision when the action has been completed.

A record may be challenged consecutively a maximum of two times.

Challenge status is identified in the 'Challenge Code' column of the record. Codes and descriptions are available in the Challenge Code Index above the data record tabs.

NOTE: For additional Challenge information please see Section 7.1 Summary Report

This page intentionally left blank.