SPRS

Supplier Performance Risk System

Vendor User Guide

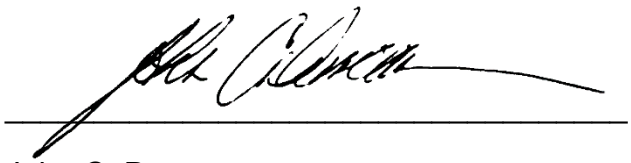
SPRS SOFTWARE USER'S GUIDE FOR AWARDEES/CONTRACTORS

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

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.



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
26	APR 2025	Updates for V4.0.4
27	SEP 2025	Updates for V4.1.1
28	DEC 2025	Updates for V4.1.2

This document is intended to be read online. To navigate quickly select the Content button at the far left of the PDF Tool Bar to Keep the Table of Contents open.

Table of Contents

Figure Table

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.

This document is intended to be read electronically. Each section begins on a new page to meet accessibility standards. Select the **Content** button at the far left of the PDF Tool Bar to keep the Table of Contents open as a menu on the left. Select topics from the menu to navigate throughout the document.

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 USER REGISTRATION

SPRS users must have an account with the Procurement Integrated Enterprise Environment (PIEE) application. Detailed instructions to create a PIEE account are available on the PIEE Getting Started web page, ***https://cac.piee.eb.mil/xhtml/unauth/web/homepage/vendorGettingStartedHelp.xhtml*** .

SPRS uses the 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 Contractor Account 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 grant access to other company users and request additional roles for themselves. If there is only one CAM, SPRS role requests for the CAM will be automatically activated.

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

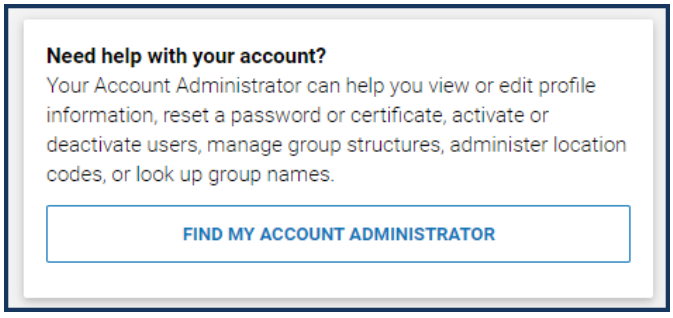


Figure 1: Finding Account Administrator in PIEE

Selecting SPRS Roles after logging into PIEE:

1. Select **My Account** at the top left of the landing page
2. Select **Add Additional Roles** in the center of the page
3. Select **SPRS** from dropdown application list
4. Select the Role:
    a. **Contractor/Vendor (Support Role)** –
        - CAGE-specific reporting
        - View risk, and performance data
        - View Cyber Reports (CMMC & NIST)
        - View CAGE Hierarchy Report
        - Process Challenges

    b. **SPRS Cyber Vendor User** –
        - Add/Edit/View Cyber Reports (CMMC & NIST)
        - View CAGE Hierarchy Report
        - Affirm CMMC Assessments
5. Select **+Add Roles** button
6. 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. For the SPRS Cyber Vendor User role only: access to one CAGE in a CAGE hierarchy will provide access to all CAGEs in that hierarchy.

User role requests must be activated by the CAM to allow access to SPRS. Users that are the only CAM for their CAGE will have their role automatically activated by PIEE.

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

These instructions to add SPRS roles are also available on the SPRS Access web page, ***https://www.sprs.csd.disa.mil/access.htm***.

2.3 ACCESSING SPRS

Once SPRS role requests have been activated in PIEE the application will be added to the users PIEE landing page.

To Access SPRS:

- Open a browser session
- PIEE landing page: https://piee.eb.mil
- Select **LOG IN** and follow prompted log-in steps

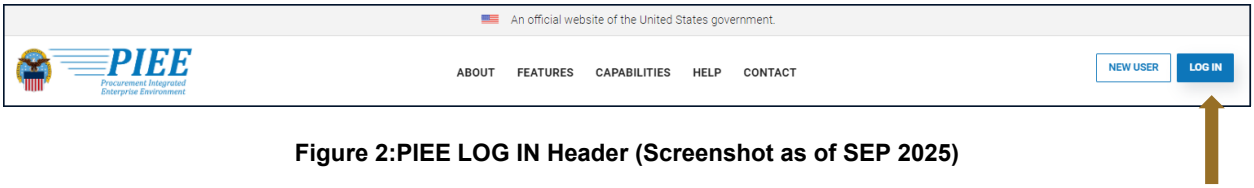


Figure 2:PIEE LOG IN Header (Screenshot as of SEP 2025)

- Select the **SPRS** Tile:

Figure 3: SPRS Tile

Maintain your PIEE account by logging in every 45 days.

PIEE activity:

- 45 days without accessing, users receive an email reminder
- 60 days without accessing, the account will become inactive
  - Contact the Company Account Administrator (CAM) or PIEE Helpdesk
- 90 days without accessing, the account will be archived
  - Contact the PIEE Helpdesk, **disa.global.servicedesk.mbx.eb-ticket-requests@mail.mil**

3. SPRS USER ROLES

Two (2) basic user types may access SPRS: Vendor and Government. Awardee/Contractors select Vendor user type. Section 2.2, User Registration, provides instructions for requesting roles. An overview of the roles and application access for each is listed below and contained in **Appendix A: SPRS USER ROLES**.

3.1 CONTRACTOR/VENDOR (SUPPORT ROLE):

- CAGE-specific reporting
- View risk, and performance data
- View Cyber Reports (CMMC & NIST)
- View CAGE Hierarchy Report
- Process Challenges
- Provide customer feedback
- Add/Edit/View company Industrial Base Surveys

Allows access to company performance and risk reports for the CAGE authorized in PIEE and cyber reports for any CAGE(s) below (subsidiaries).

3.2 SPRS CYBER VENDOR USER:

- Add/Edit/View Cyber Reports Assessment results
- View CAGE Hierarchy Report
- Affirm CMMC Assessments
- Provide customer feedback
- Add/Edit/View company Industrial Base Surveys

Allows privileged access to the CAGE authorized in PIEE and any additional CAGE(s) that share the same Highest Level Owner (HLO) hierarchy.

4. WORKING IN SPRS

4.1 SPRS APPLICATION LANDING PAGE:

SPRS uses two work areas: 1. the menu, and 2. 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.

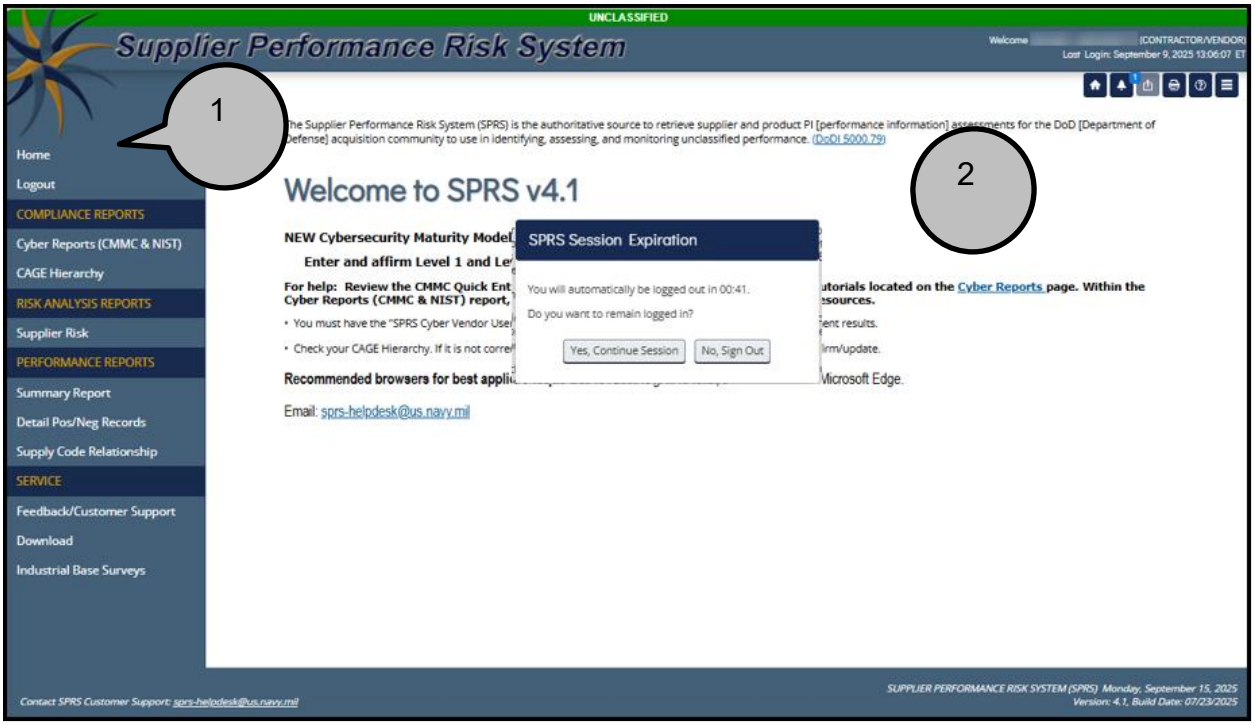


Figure 4: SPRS Application Landing Page

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.*

4.2 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

Breadcrumbs are located at the top of the screen and show the path a user has taken to arrive at the current page. Click on the links in the Breadcrumb to return to the previous screen or respective landing screen.

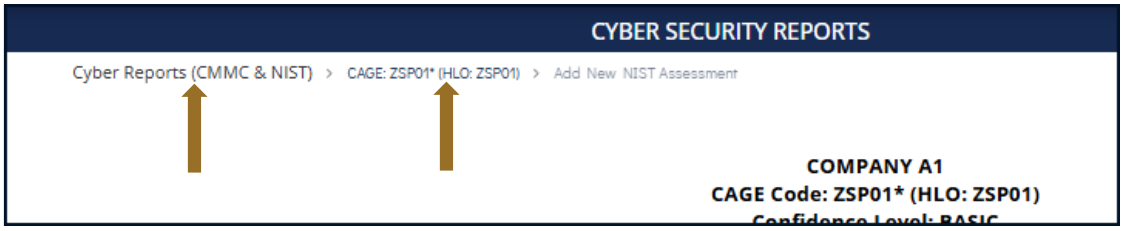


Figure 5: Breadcrumbs example

The **SPRS Help Desk email** is at the bottom of every page.

4.3 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 from the SPRS team
- **Export** – Click to Export to Excel the current report to the Download module on the Menu (icon will be greyed out if page cannot be exported)

-  **Print** – Click to print or save as PDF information on the current screen
-  **Information** – Click to open a tab to the SPRS website
-  **Menu** – Click to hide the left-hand menu or to have it reappear

5. COMPLIANCE REPORTS

Compliance Reports include 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 view, create, edit, and affirm, their CMMC and NIST SP 800-171 assessments.

5.1.1 Accessing Cyber Reports

There are two roles that provide access to this module:

- **SPRS Cyber Vendor User** – the role required to add, edit, and affirm NIST SP 800-171 Basic and CMMC assessment records. This privileged role allows access to the CAGE authorized in PIEE, and any additional CAGE(s) that share the same Highest Level Owner (HLO) hierarchy.
- **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).

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.

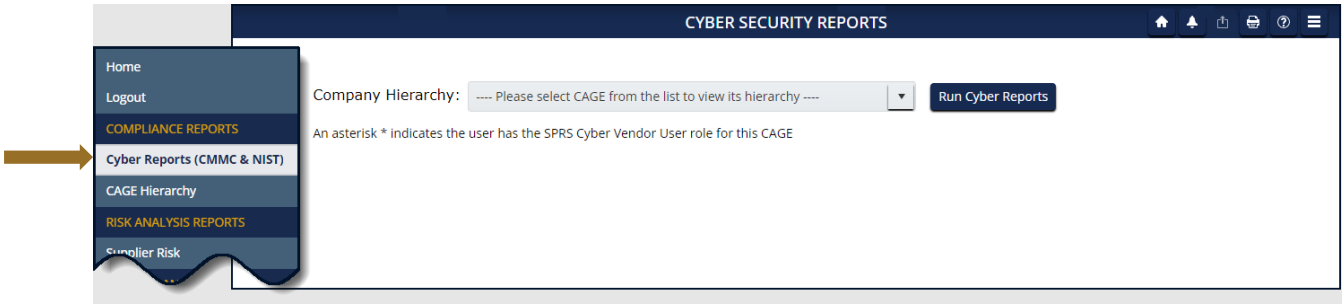


Figure 6: Cyber Reports Landing Page

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, listed in SPRS for that CAGE.

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

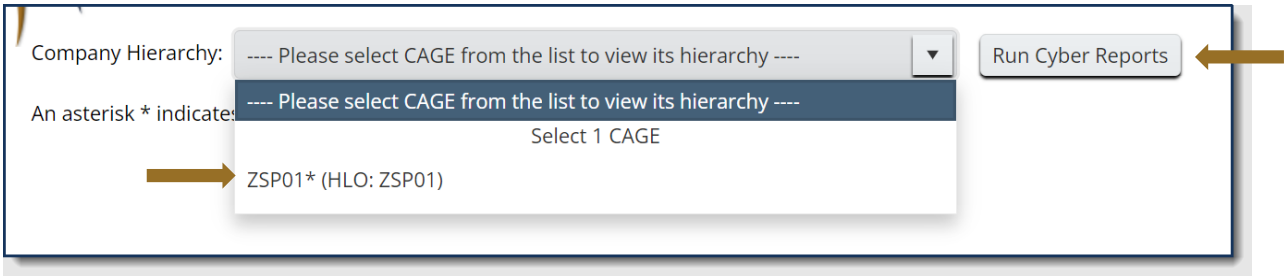


Figure 7: Cyber Reports Company Hierarchy Selection

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.

5.1.2 The Company Hierarchy Tab

Select the **Company Hierarchy** tab to display 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) listed in the SAM registration for the CAGE at ***https://sam.gov*** to request an update.

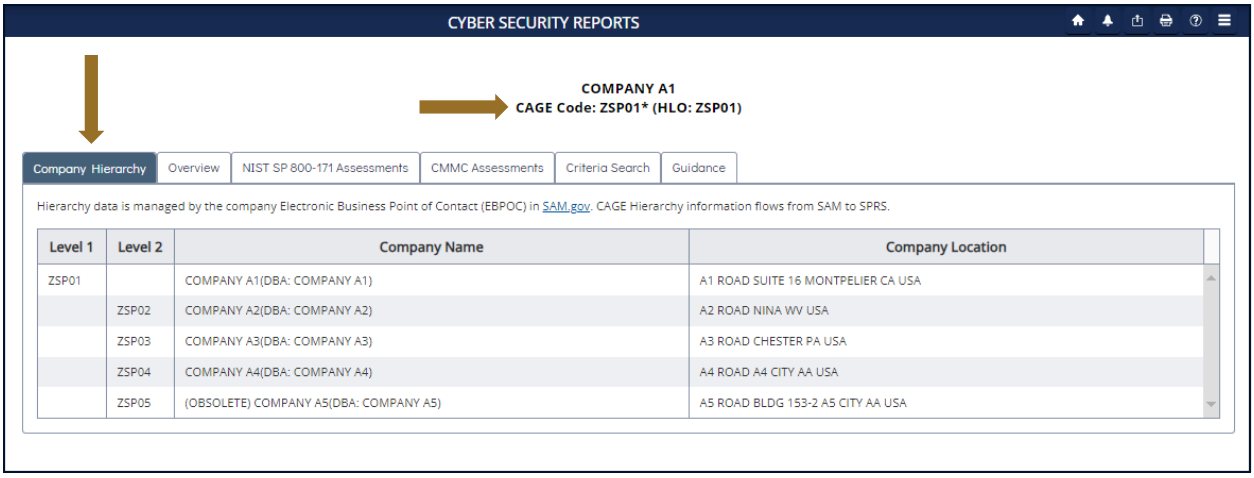


Figure 8: Cyber Reports Company Hierarchy Tab

5.1.3 The Overview Tab

Select the **Overview** tab to display the CAGE(s) that have assessments. Only CAGE(s) that have assessments 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 Current. A bracketed zero [0] indicates that all associated assessment(s) were but are not now Current.

- **NIST:** Assessment totals only consider assessments less than three (3) years from the Assessment Date. A [0] indicates that all associated assessment(s) are more than three (3) years from the logged Assessment Date.
- **CMMC:** Assessment totals identify affirmed assessments that have achieved CMMC Conditional or Final status, are not expired or retracted. A [0] indicates that all assessment(s), have an assigned UID, but are either expired, retracted, pending annual affirmation, or did not achieve CMMC status.

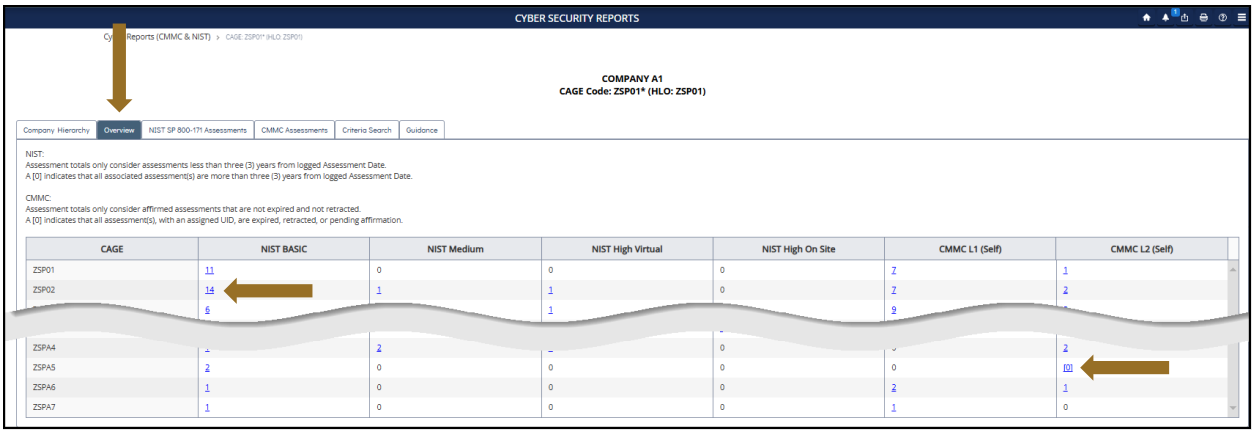


Figure 9: Cyber Reports Overview Tab

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, and results listed below.

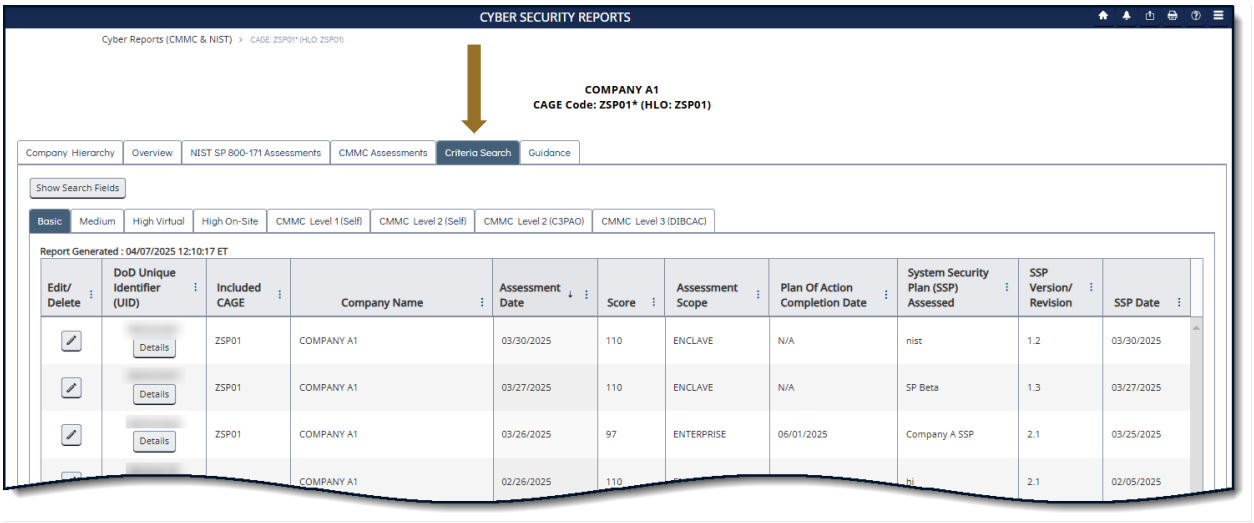


Figure 10: Cyber Reports Criteria Search Tab from Overview

5.1.4 The NIST SP 800-171 Assessments Tab

This tab displays logged assessment summary results supporting DFARS 252.204–7019/7020 requirements. 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. (See section 5.1.1)

There are 4 tabs within the **NIST SP 800-171 Assessments** tab. 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.

Users will only have access to view assessment records associated with their current hierarchy (HLO). Assessments entered under a previous HLO will not be visible but remain available to the government.

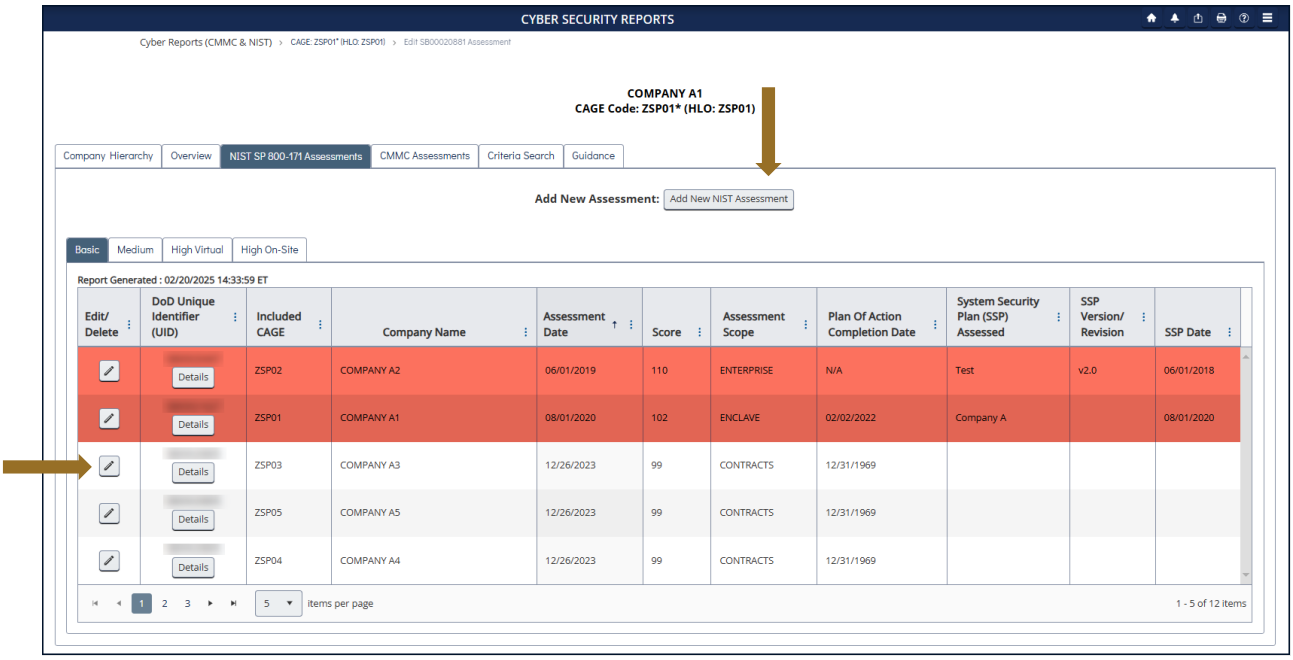


Figure 11: Cyber Reports NIST SP 800-171 Assessments Tab

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. (excluding High Virtual)
- **Assessment Scope** – One of three selections:
    - 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. Required for any scores less than 110.
- **System Security Plan (SSP) Assessed** – The name of the System Security Plan that was created for the assessment.
- **SSP Version/Revision** – Optional field available for identification.

- **SSP Date** – The date the company System Security Plan was created.
- **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.**

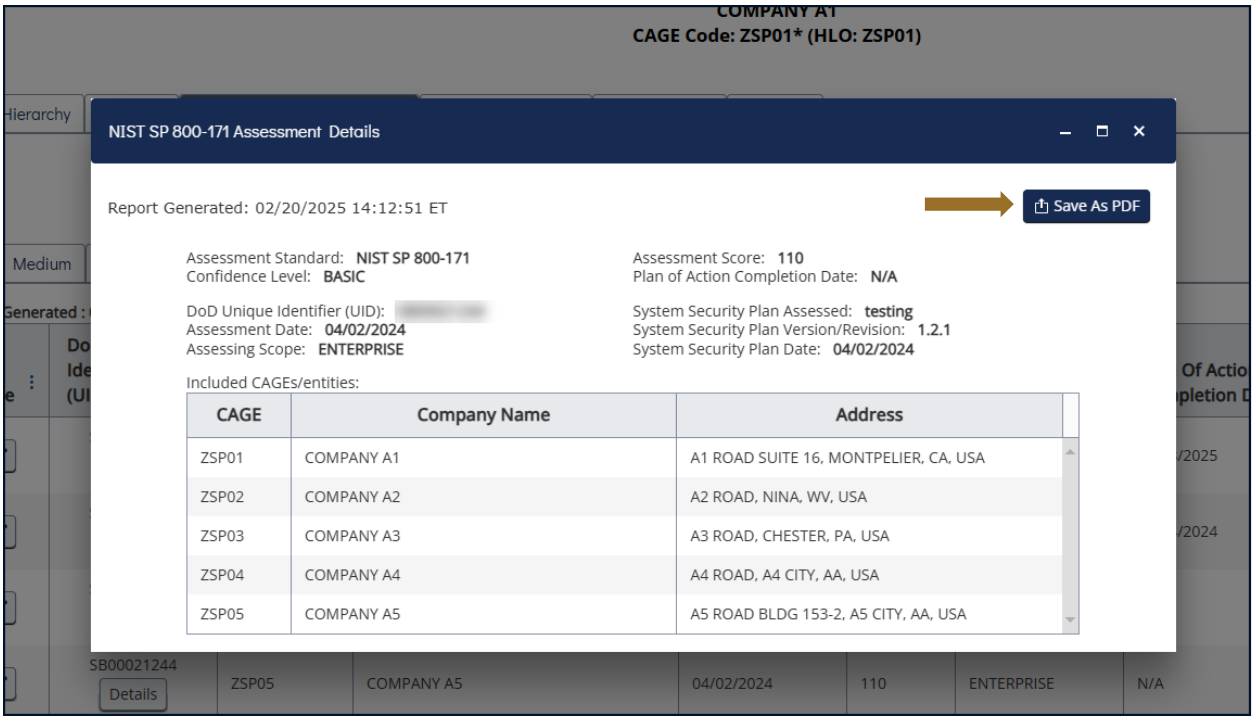


Figure 12: Cyber Reports NIST SP 800-171 Assessments Details Pop-up

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

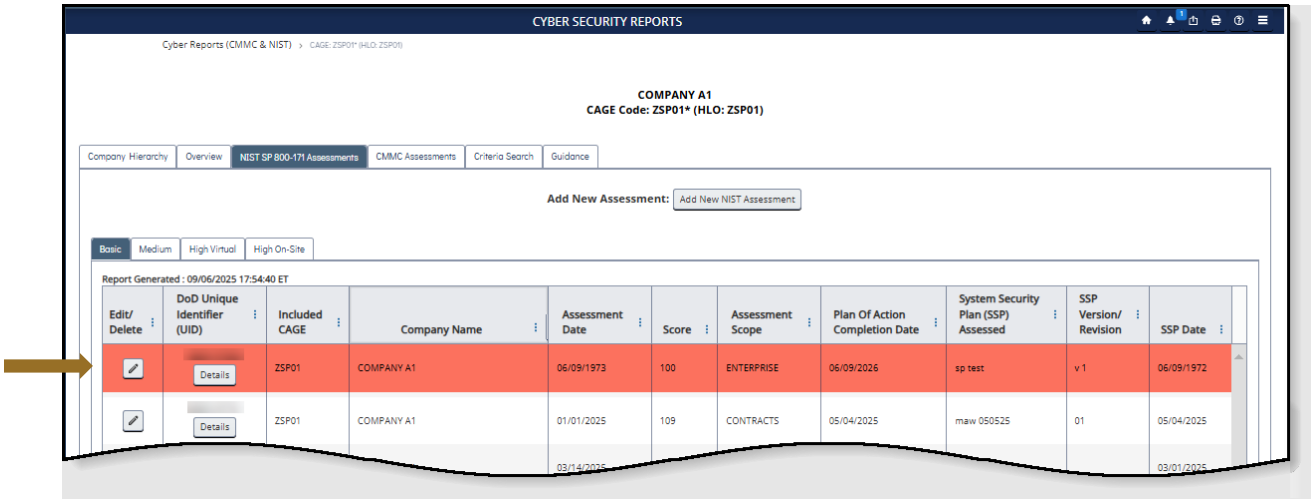


Figure 13: Cyber Reports NIST SP 800-171 Red Assessment

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.

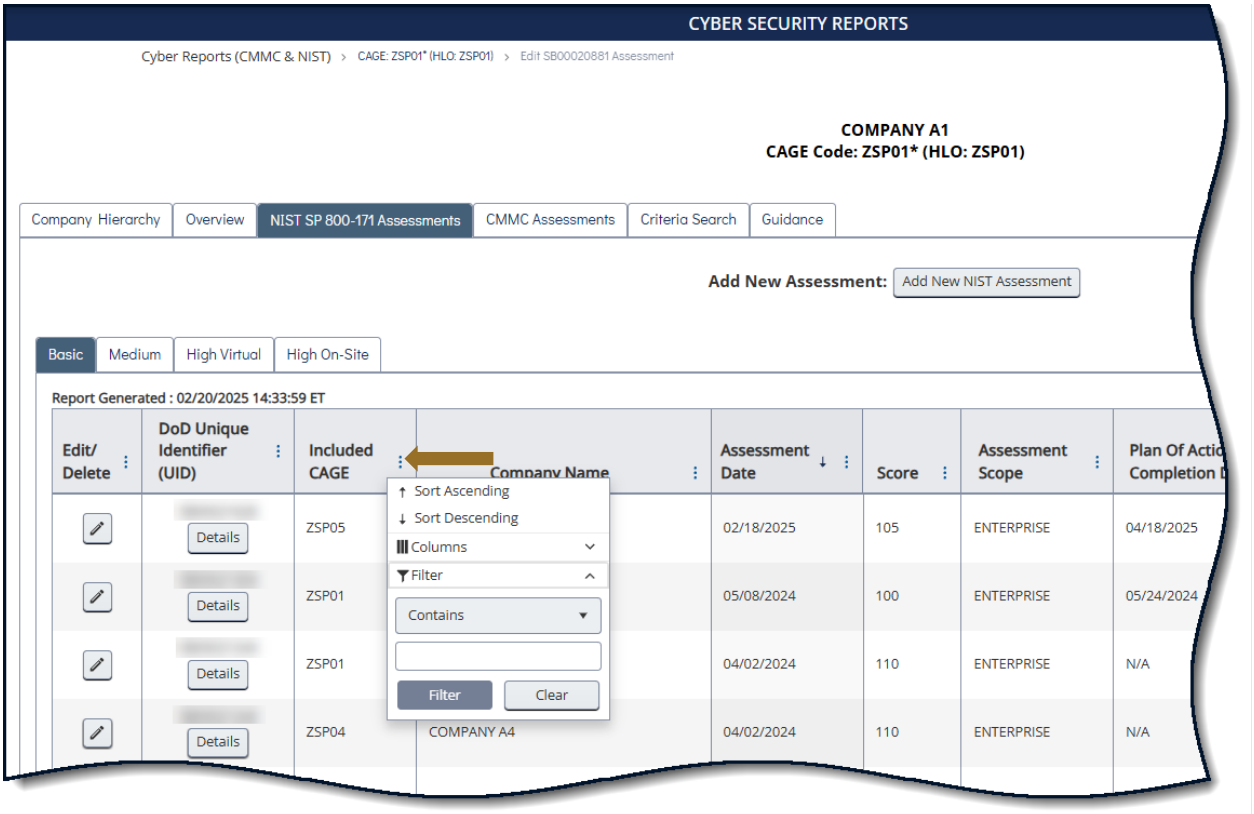


Figure 14: Cyber Reports Column Sorting and Filtering

(i) NIST SP 800-171 Basic Self-Assessment

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**.

The NIST SP 800-171 DoD Assessment Methodology can be found on the ASD(A) – DPC – Contract Policy page, ***https://www.acq.osd.mil/asda/dpc/cp/cyber/safeguarding.html#nistSP800171***

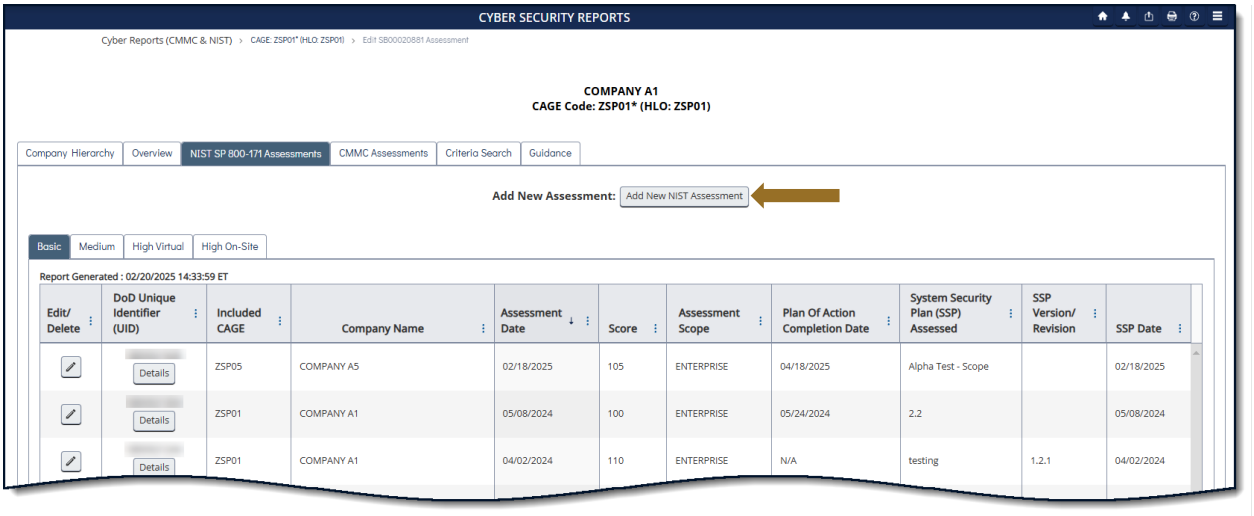


Figure 15: Cyber Reports NIST SP 800-171 Add New Assessment Button

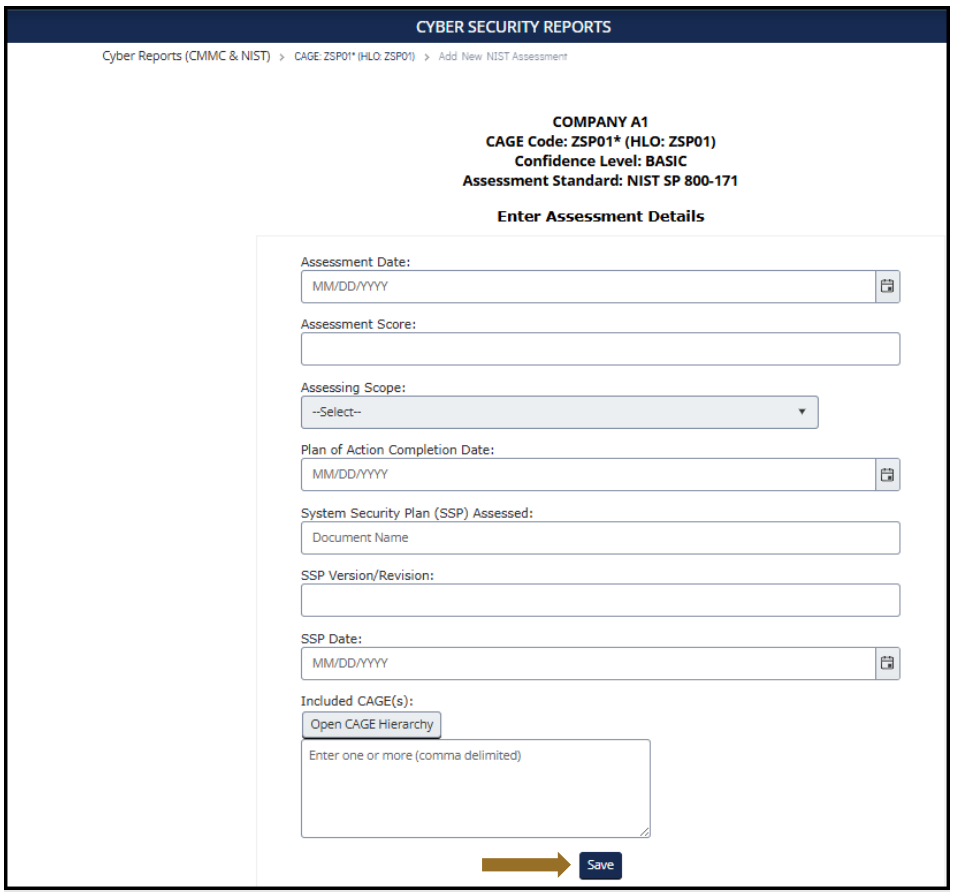


Figure 16: Cyber Reports NIST SP 800-171 Enter Assessment Details

The **Open CAGE Hierarchy** button opens the CAGE tree, allowing users to select which CAGEs are included in the assessment.

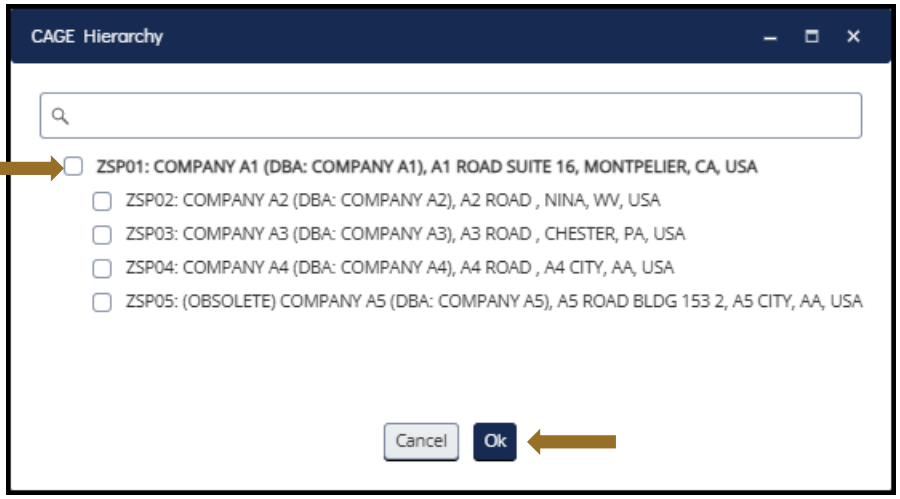


Figure 17: Cyber Reports NIST SP 800-171 CAGE Hierarchy Pop-up

Users can also copy and paste a comma-delimited list of CAGEs into the CAGE text box provided. CAGEs must be included in the current CAGE Hierarchy.

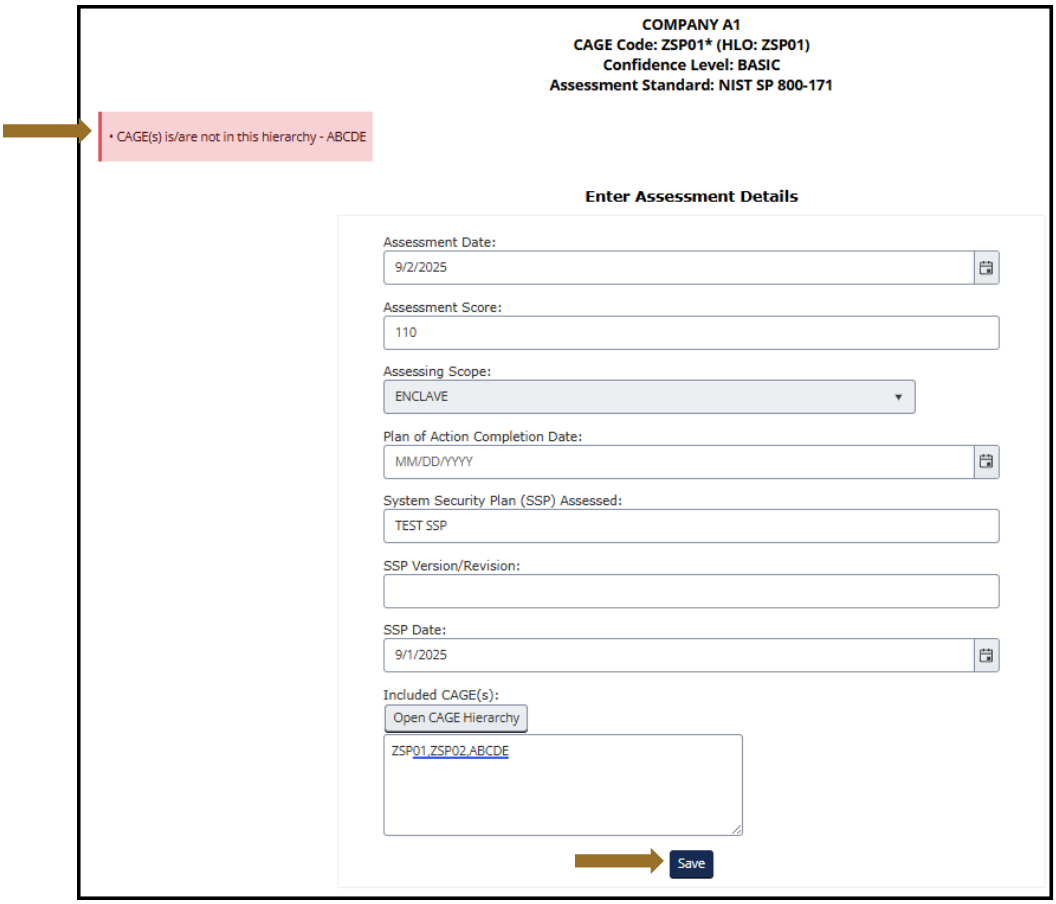


Figure 18: Cyber Reports NIST SP 800-171 Enter Included CAGE(s)

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.

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.

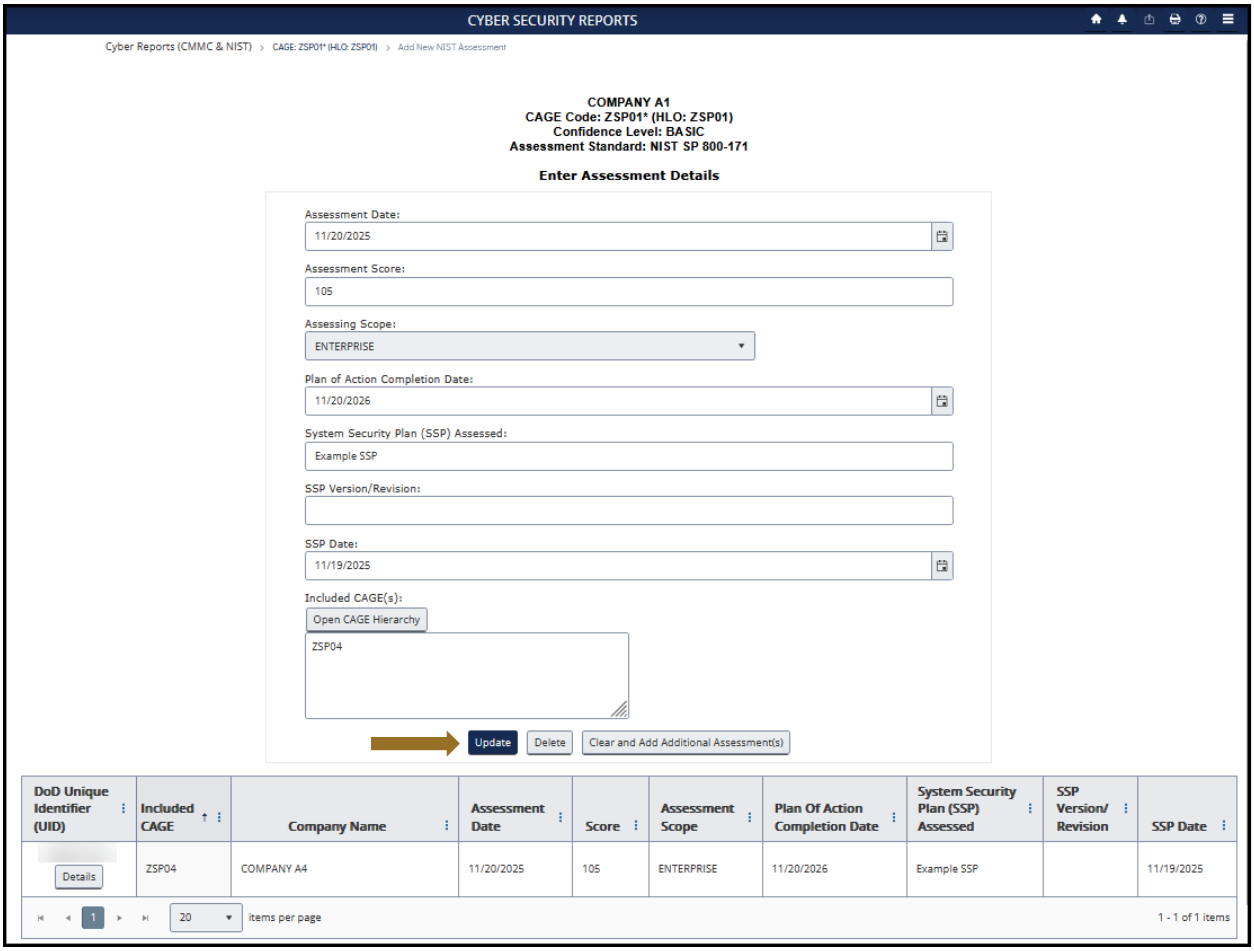


Figure 19: Cyber Reports NIST SP 800-171 Enter Assessment Details

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.

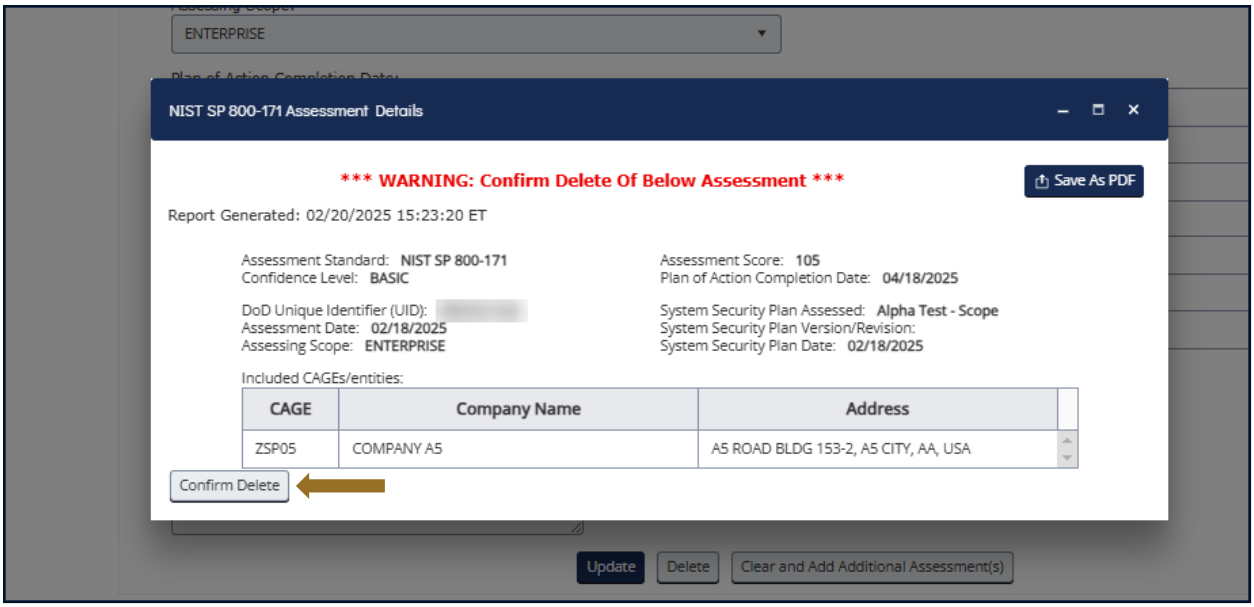


Figure 20: Cyber Reports NIST SPT 800-171 Confirm Delete

Use the breadcrumb navigation to return to the NIST SP 800-171 assessment record grid.

Figure 21: Cyber Reports NIST SP 800-171 Navigate from Enter Assessment Details

To Edit/Delete assessment records from the Basic assessment tab click the pencil icon at the far left of the record. The Enter Assessment Details screen will open with the record details populated. To edit, enter new data and select the Update button. To delete, select the delete button and follow the prompts.

The **NIST SP 800-171 Quick Entry Guide** provides summary instructions on entering and editing assessment results. The guide is located on the SPRS web

page: ***https://www.sprs.csd.disa.mil/pdf/NISTSP800-171QuickEntryGuide.pdf***

5.1.5 The CMMC Assessments Tab

Select the **Acknowledge** button after reviewing the statement in the pop-up.

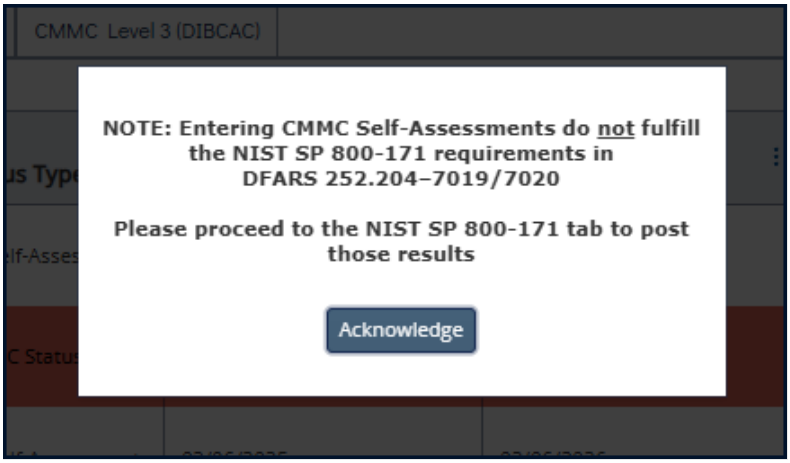


Figure 22: CMMC Acknowledge Screen

This tab displays logged CMMC assessment summary results. If the user has a SPRS Cyber Vendor User role, an **Add New CMMC Level 1** button as well as **Edit** and **Delete** columns will be visible. Users with Contractor Vendor (view-only) will not see those items.

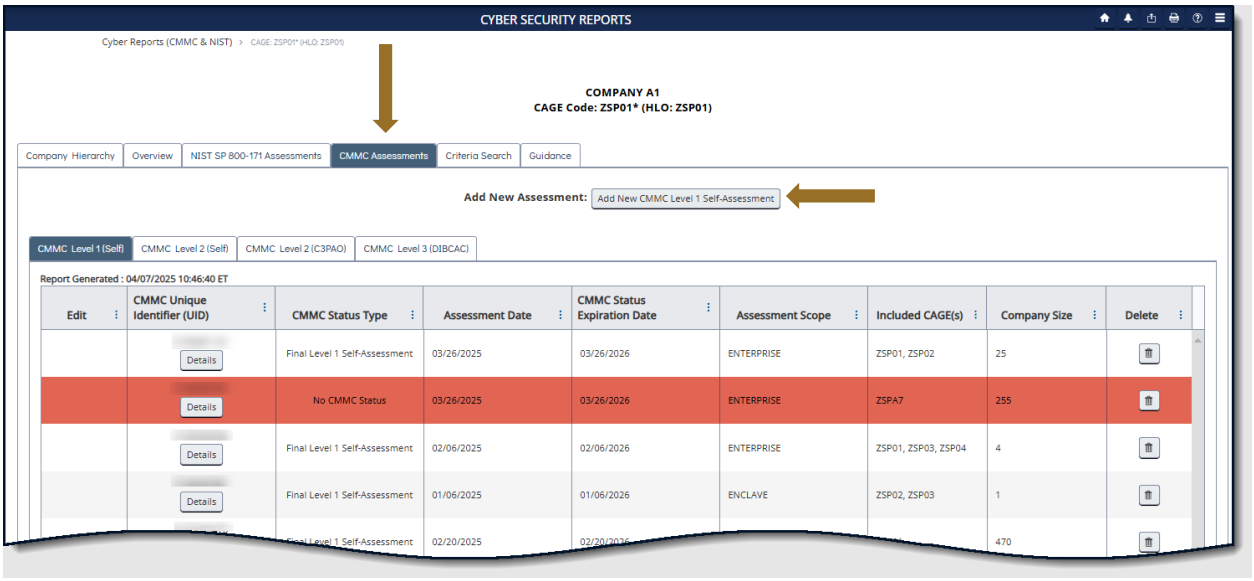


Figure 23: Cyber Reports CMMC Assessment Tab

There are 4 tabs within the **CMMC Assessments** tab. Select each tab to view the logged assessments for the related confidence level:

- CMMC Level 1 (Self) (Contractor self-assessments)
- CMMC Level 2 (Self) (Contractor self-assessments)
- CMMC Level 2 (C3PAO) (conducted by CMMC Third-Party Assessor Organization)
- CMMC Level 3 (DIBCAC) (conducted by DoD)

All CMMC confidence levels require some vendor action. CMMC Level 1 and CMMC Level 2 assessments are created and affirmed by the vendor. CMMC Level 2 (C3PAO) and CMMC Level 3 (DIBCAC) must be affirmed by the vendor.

(i) CMMC Level 1 (Self)

Summary results include the following information:

- **CMMC Unique Identifier (UID) –** The 10-digit alphanumeric assessment identifier. The first two letters delineate the CMMC confidence level. Level 1 and Level 2 Self-Assessments, assigned after initial affirmation, have prefix S1 and S2 respectively. Level 2 and Level 3 Assessments, assigned by eMASS, have prefix L2 and L3.
- **CMMC Status Type** – The status of the assessment record. Incomplete and Pending Affirmation status types will not be visible to government users. Refer to Appendix E for list of Status Types and descriptions.
- **Assessment Date** – The date the assessment was completed.
- **CMMC Status Expiration Date** – The assessment expiration date; a Level 1 self-assessment is considered valid for one year from Assessment Date.
- **Assessment Scope** – One of two selections:
    - 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(s)** – List of all CAGE Codes included in the assessment scope.
- **Company Size** – Total of employees at all locations of the organization.

The CMMC tab opens to the CMMC Level 1 (Self) subtab. Select the **Details** button to open a print friendly display of all information associated with that assessment record. To download select **Save As PDF.**

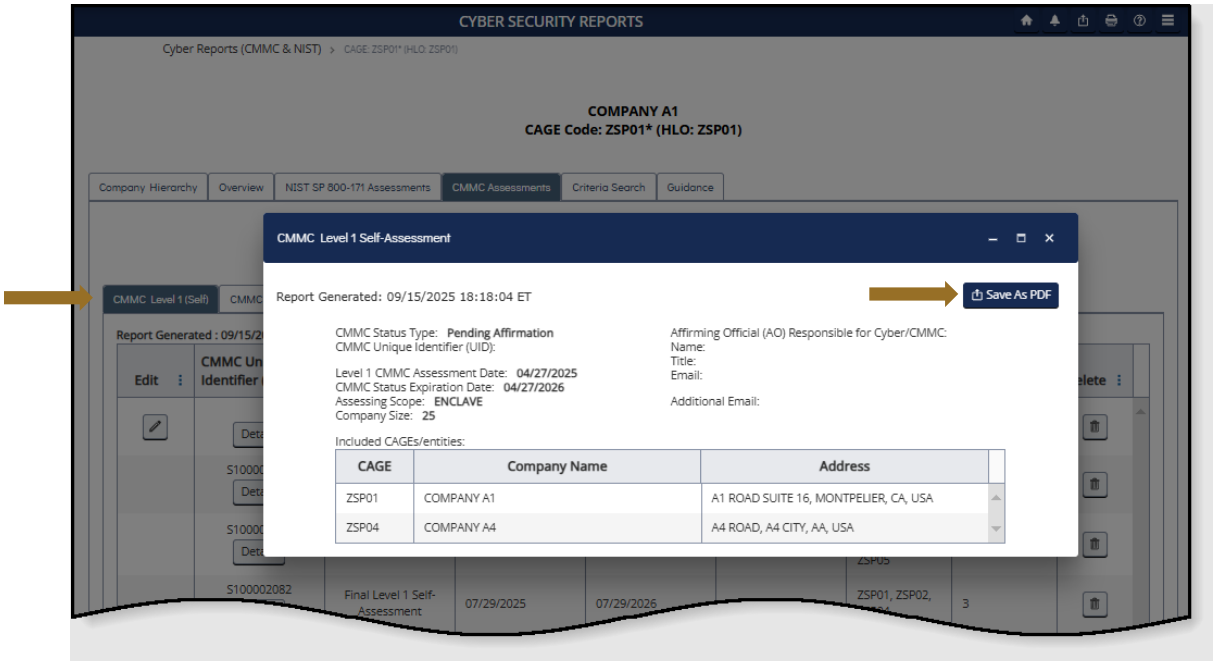


Figure 24: Cyber Reports CMMC Level 1 Self-Assessments Details Pop-up

A Level 1 Self-Assessment will automatically become "**No CMMC Status (Expired Assessment)**" after one year, and turn red. Once affirmed, assessments continue to be visible to Government personnel.

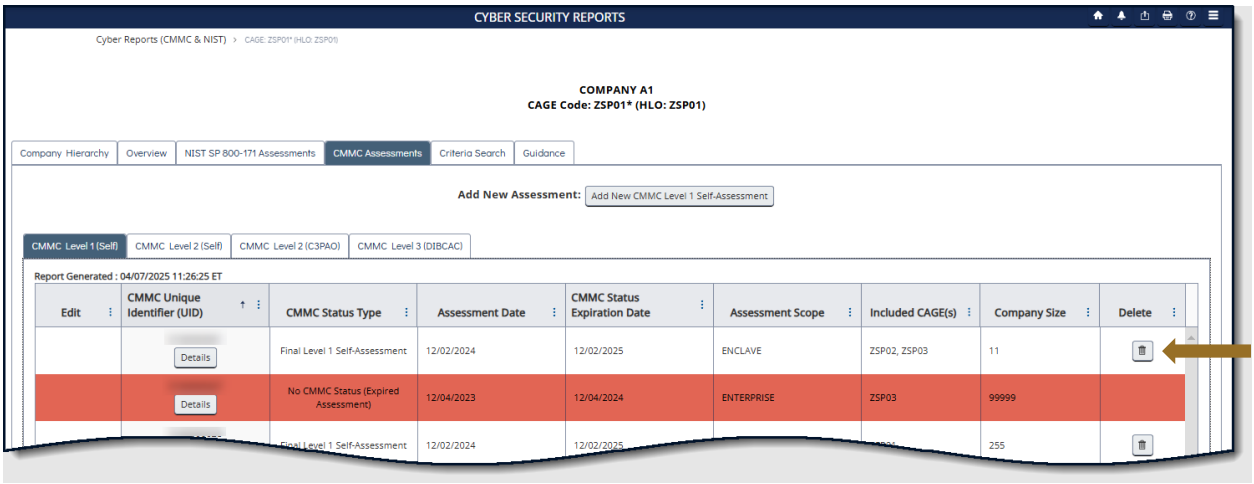


Figure 25: Cyber Reports CMMC Level 1 Red Expired Assessment

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

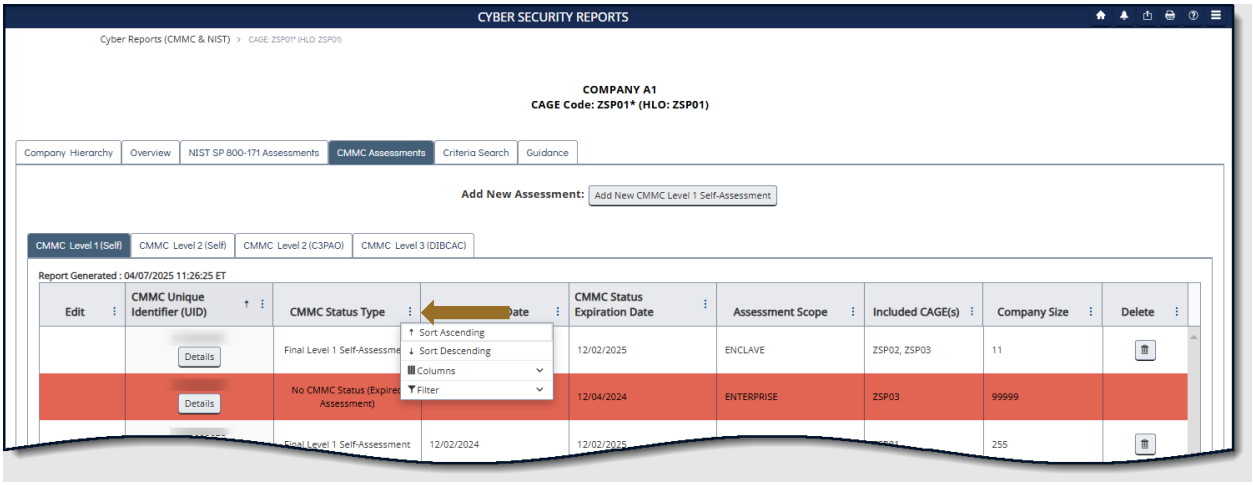


Figure 26: Cyber Reports CMMC Column Sorting and Filtering

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

Select the **Add New CMMC Level 1 Self-Assessment** button.

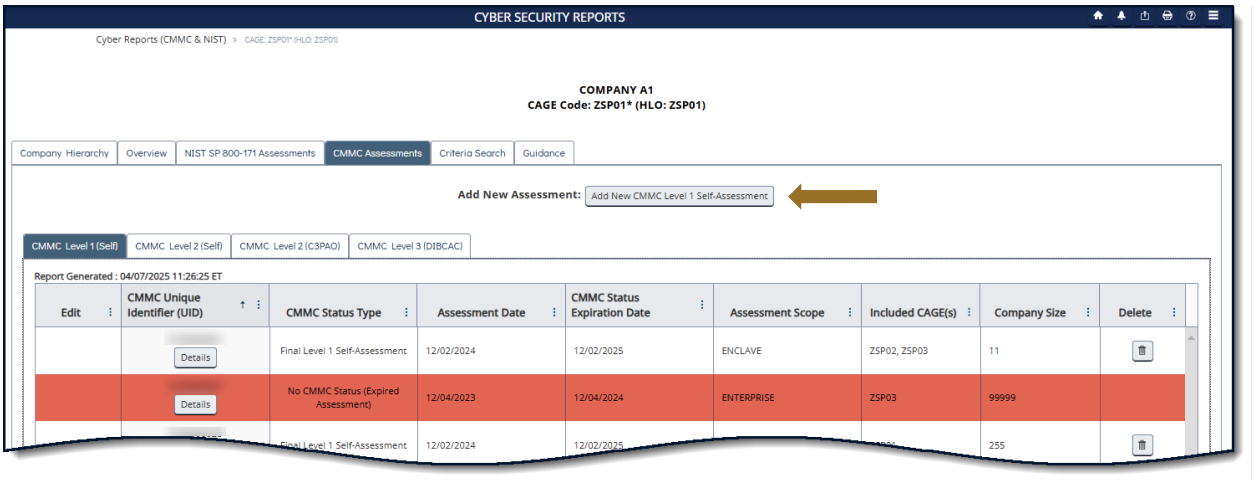


Figure 27: Cyber Reports Add New CMMC Level 1 Self-Assessment Button

Review the warning message and select **Acknowledge**.

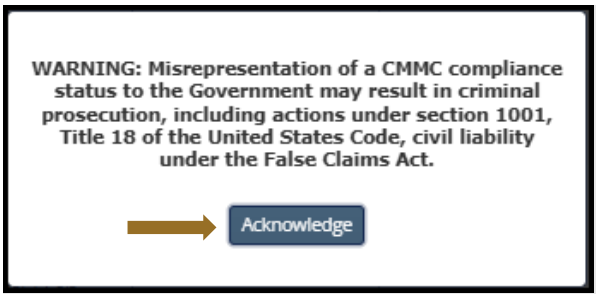


Figure 28: Cyber Reports Warning CMMC Levels 1 and 2

Enter the assessment information. The **Open CAGE Hierarchy** button opens the CAGE tree, allowing users to select which CAGEs are included/assessed. Users can also copy and paste a comma-delimited list of CAGEs into the CAGE text box provided. CAGEs must be in the current CAGE Hierarchy. (See Sec. 5.1.2)

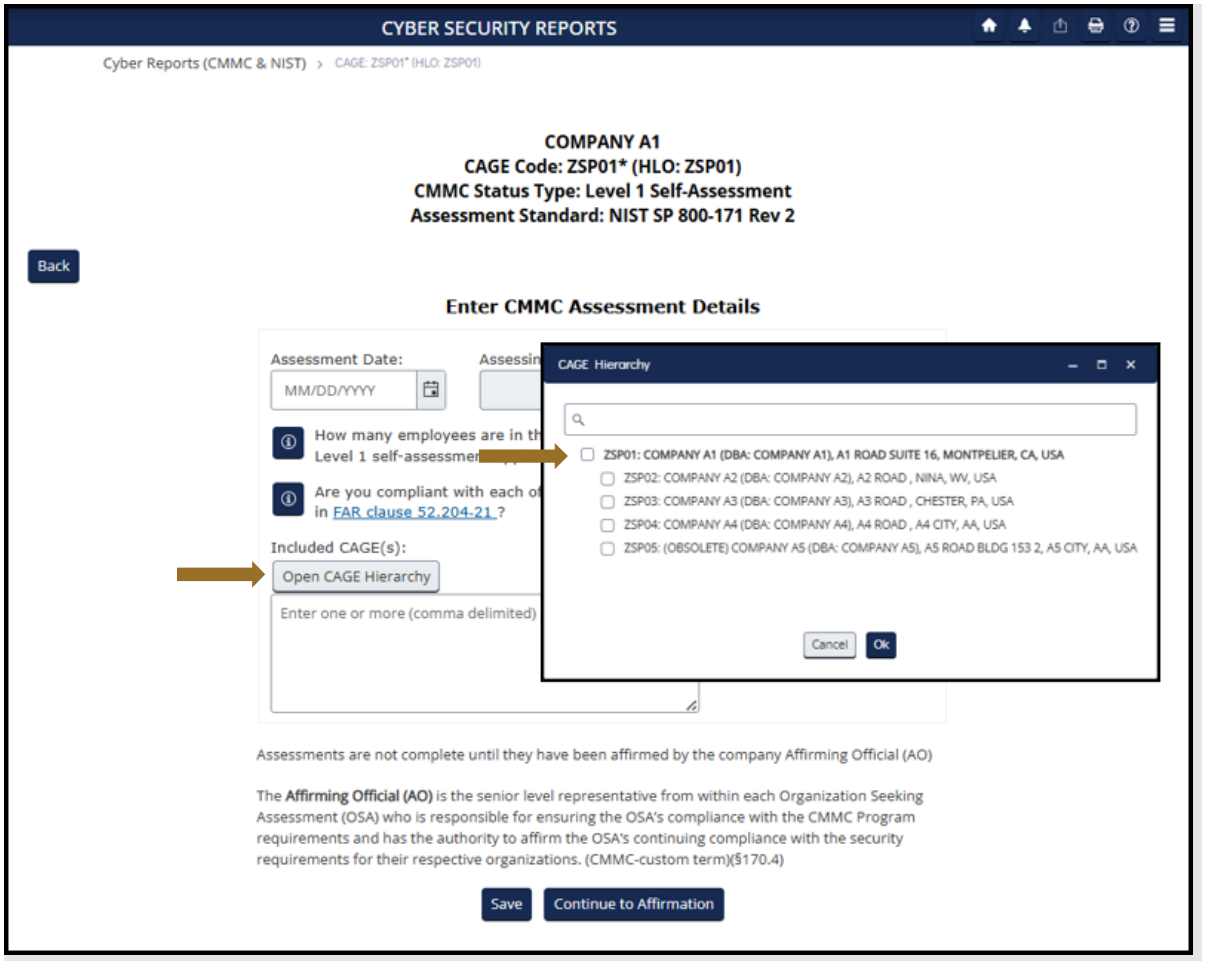


Figure 29: Cyber Reports CMMC Level 1 CAGE Hierarchy Pop-up

Questions related to technical interpretation of these CMMC Level 1

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 in progress and edited or affirmed later. Select 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**.

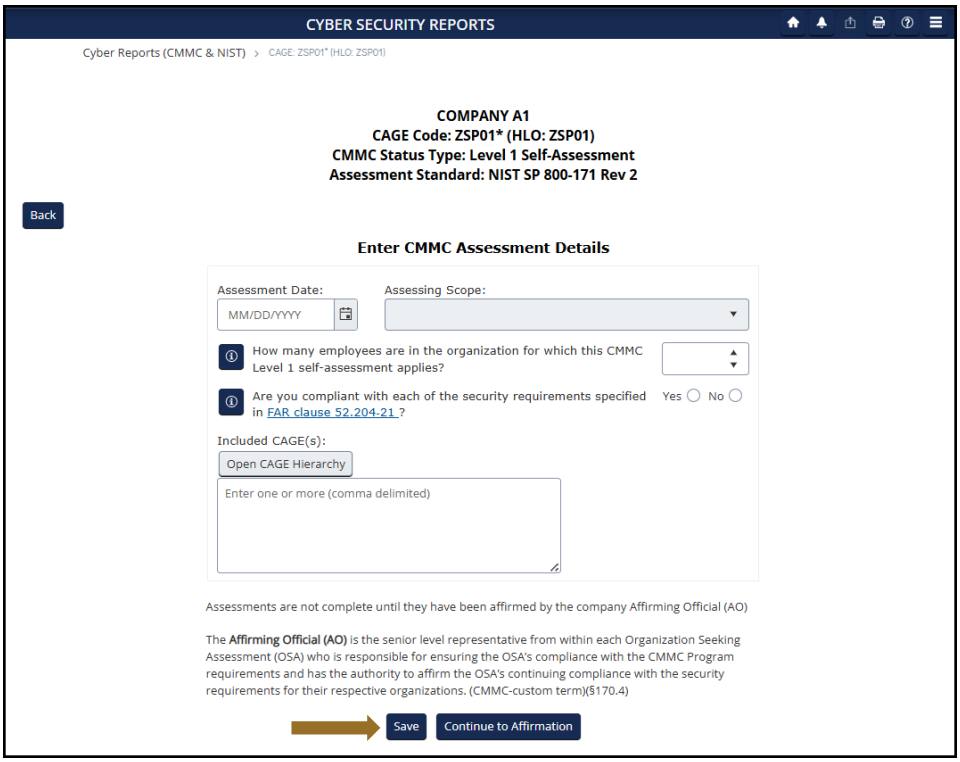


Figure 30: Cyber Reports CMMC Level 1 Entry Screen

If the user entering the CMMC Self-Assessment is not the AO, enter the AO's

email address and select **Transfer to AO**.

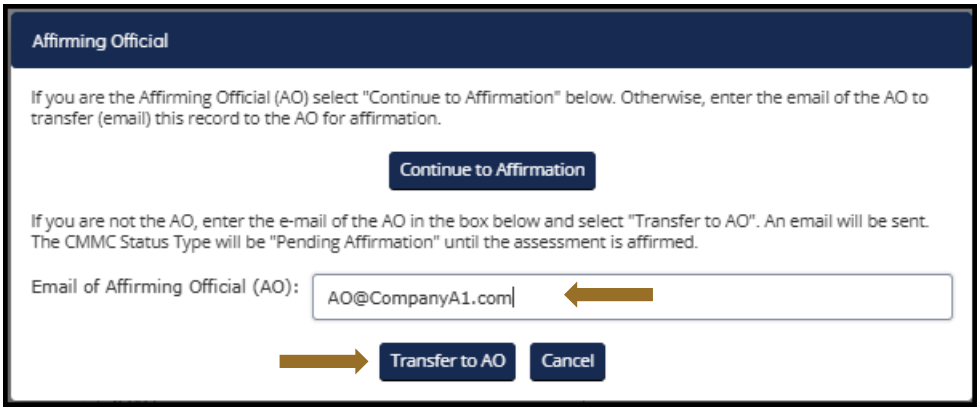


Figure 31: Cyber Reports CMMC Transfer to AO

The AO will be sent an email notification, with the user on copy, that an assessment is waiting for their affirmation. This email is only sent once and may be prevented from being delivered by a company's email server settings.

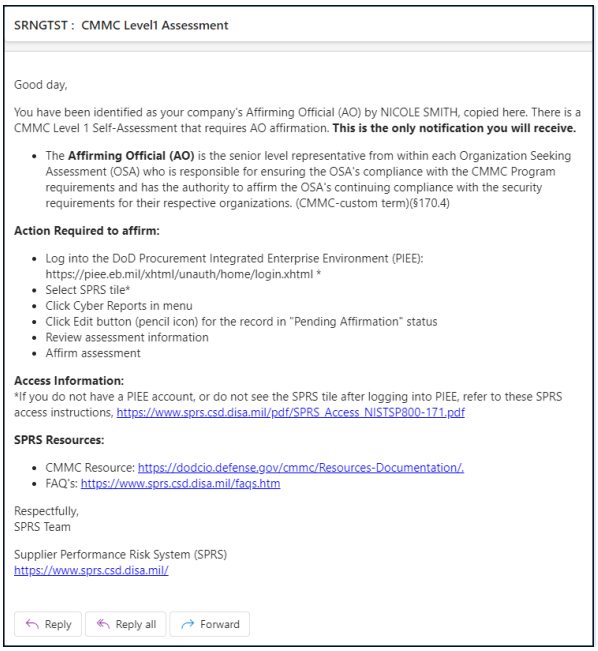


Figure 32: Cyber Reports CMMC AO Email Sample

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

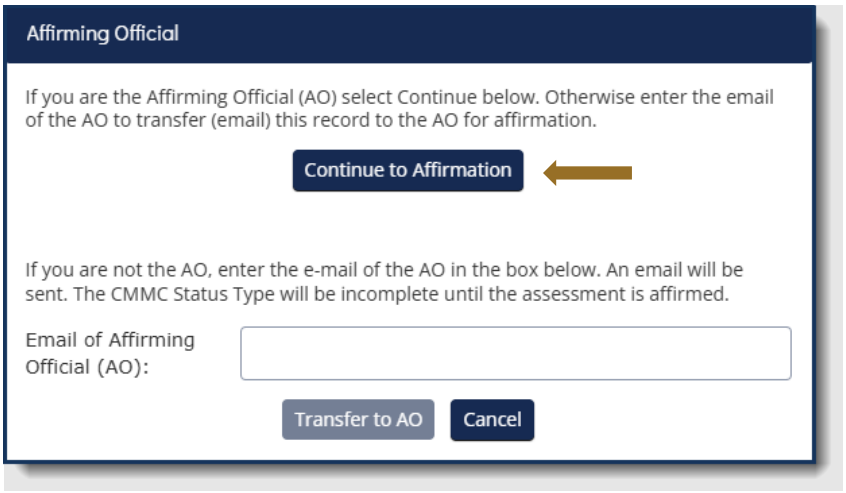


Figure 33: Cyber Reports CMMC Continue to Affirmation or Transfer to AO

The Affirming Official information is pulled from the user's PIEE profile. Any changes must be made in PIEE and cannot be changed on this screen. Select **Back** or **Previous** to exit without affirming. Or enter any additional emails to be associated with the record and select **Continue to Affirmation.** No notification will be sent to the additional emails.

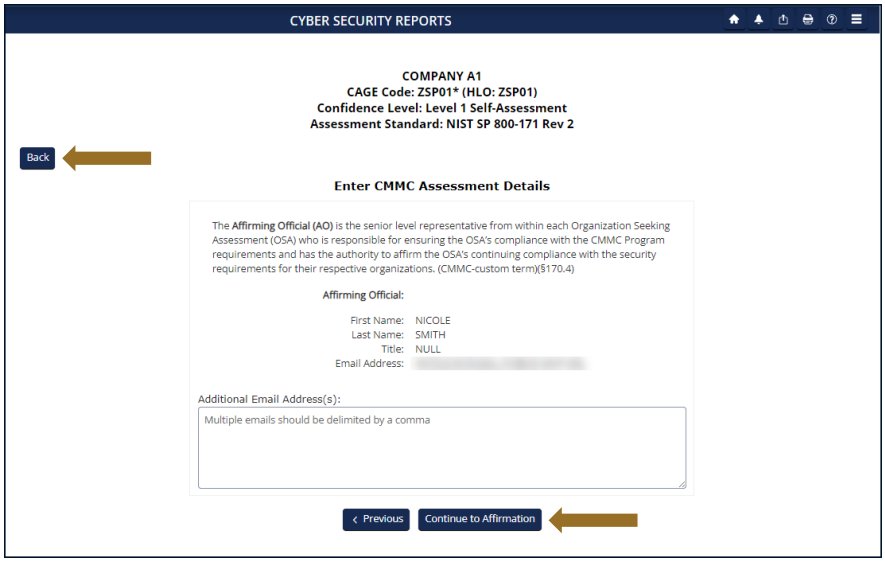


Figure 34: Cyber Reports CMMC Assessment Details

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.

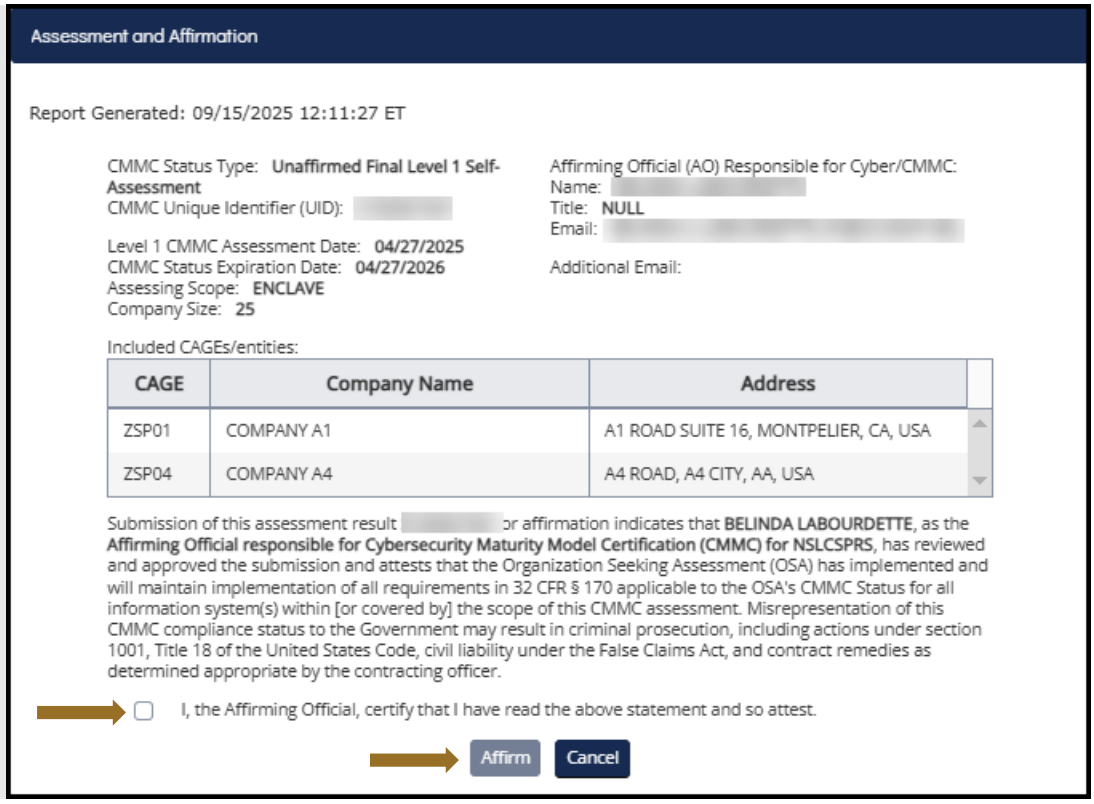


Figure 35: Cyber Reports CMMC Certify and Affirm

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.

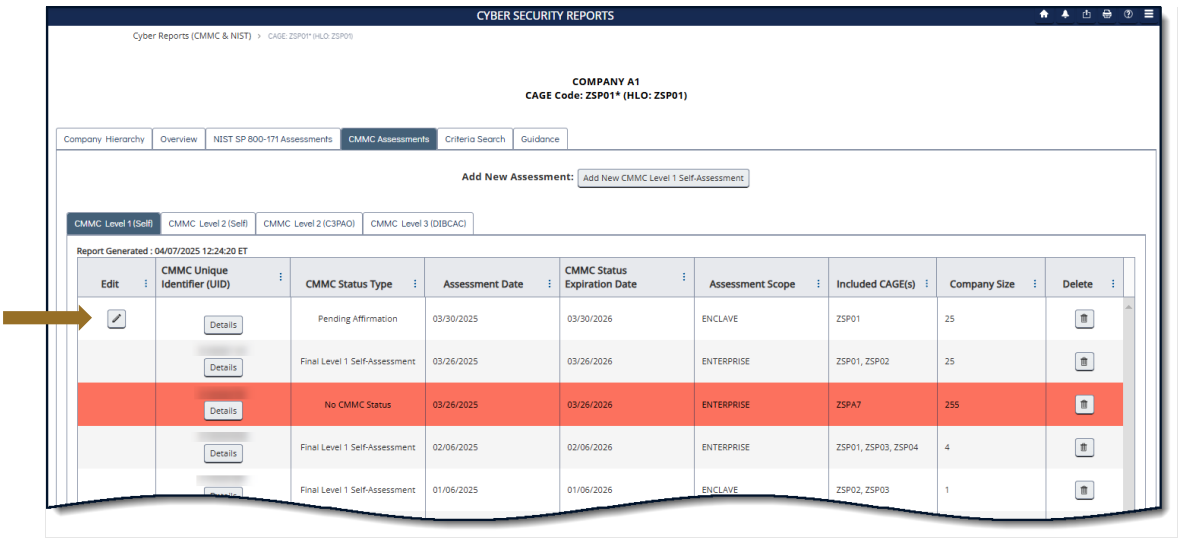


Figure 36: Cyber Reports CMMC Edit an Assessment

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 except for the **"No CMMC Status (Expired Assessment)."**

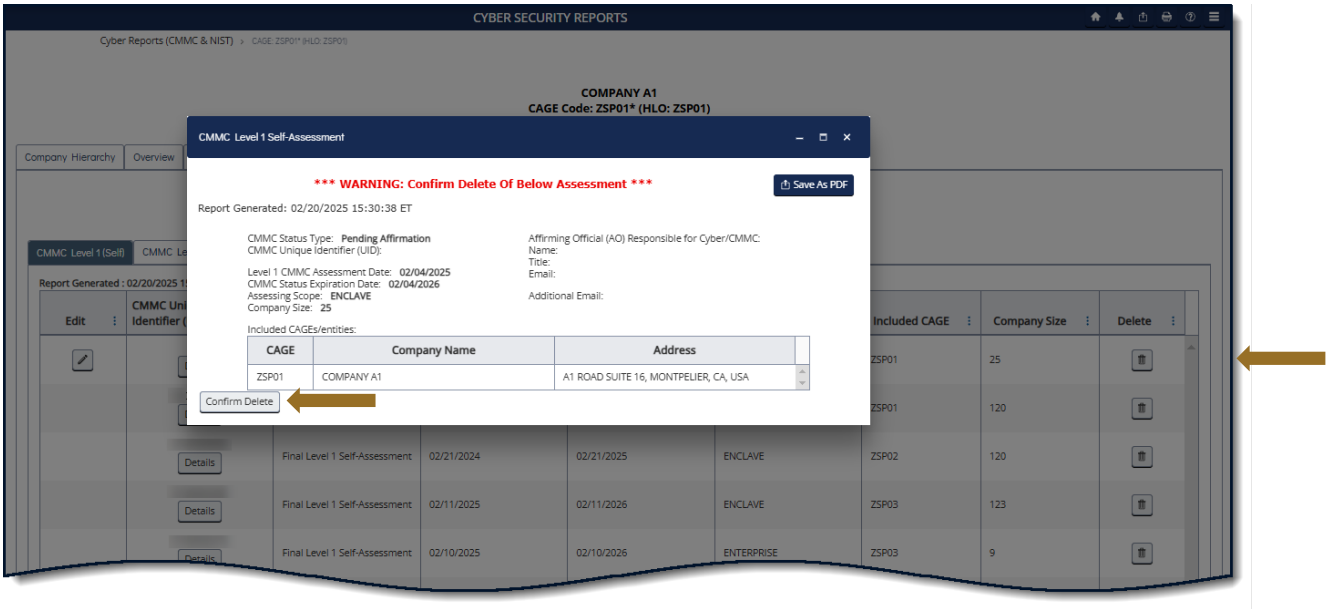


Figure 37: Cyber Reports CMMC Delete an Assessment

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

(ii) CMMC Level 2 (Self)

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

- **CMMC Unique Identifier (UID) –** The 10-digit alphanumeric assessment identifier. The first two letters delineate the CMMC confidence level. Level 1 and Level 2 Self-Assessments, assigned after initial affirmation, have prefix S1 and S2 respectively. Level 2 and Level 3 Assessments, assigned by eMASS, have prefix L2 and L3.
- **CMMC Status Type** – The status of the assessment record. Incomplete and Pending Affirmation (no CMMC UID) Status Types will not be visible to government users. Refer to Appendix E for list of Status Types and descriptions.

***NOTE*:** *Prior to affirmation, assessments that qualify as CMMC L2 Conditional or Final Self-Assessment will show "Unaffirmed" in the title on both the Score step and the Affirmation pop-up.*

- **Assessment Date** – The date the assessment was completed.
- **Affirmation Expiration Date** – System calculated date based on assessment date and status type: 180 days for conditional status, and one (1) year intervals for final status records.
- **CMMC Status Expiration Date** – System calculated date based on assessment date and status type: 180 days for conditional status, and three (3) years for final status records.
- **Assessment Scope** – One of two selections:
    - 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)

- **Last Entered or Affirmed CAGE(s) in Scope** – CAGE(s) in scope when the assessment was initially entered or last affirmed.
- **Current CAGE(s) Status** – CAGE(s) in scope in the current assessment.
- **Company Size** – Total of employees at all locations of the organization.

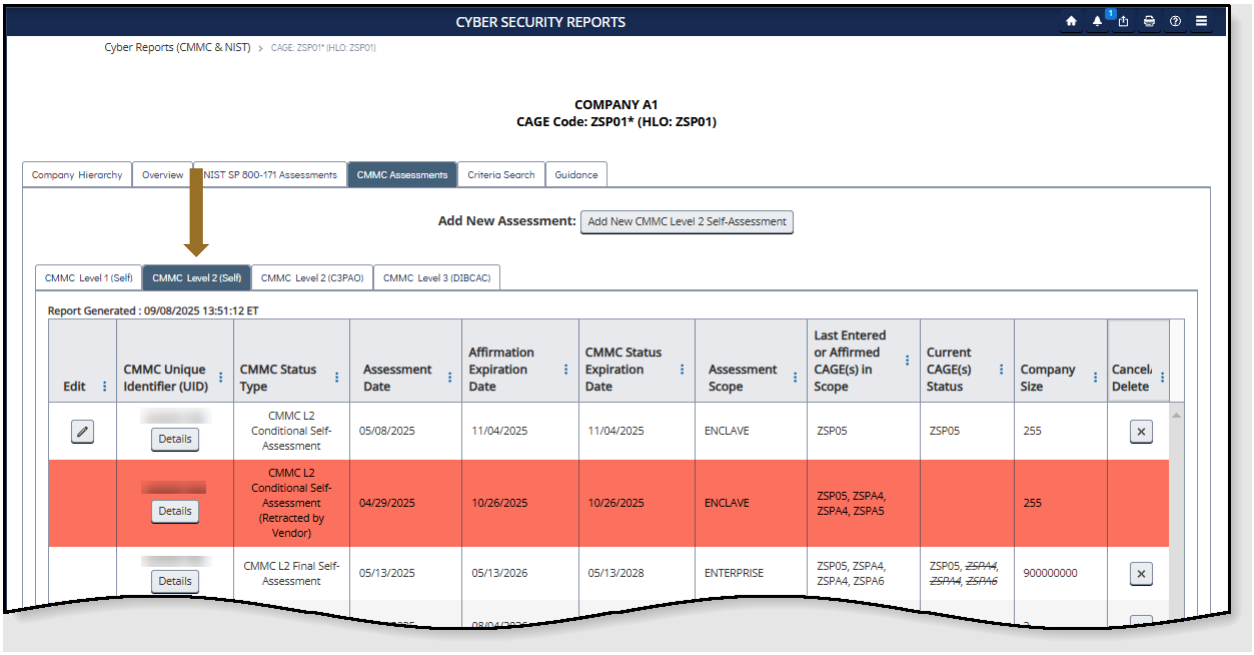


Figure 38: Cyber Reports CMMC Level 2 (Self) Subtab

Select the **Details** button in the CMMC Unique Identifier (UID) column to open a print friendly display of all information associated with that record. Select the **View/Expand** options to see additional assessment information. Select **Save As PDF** to save a copy.

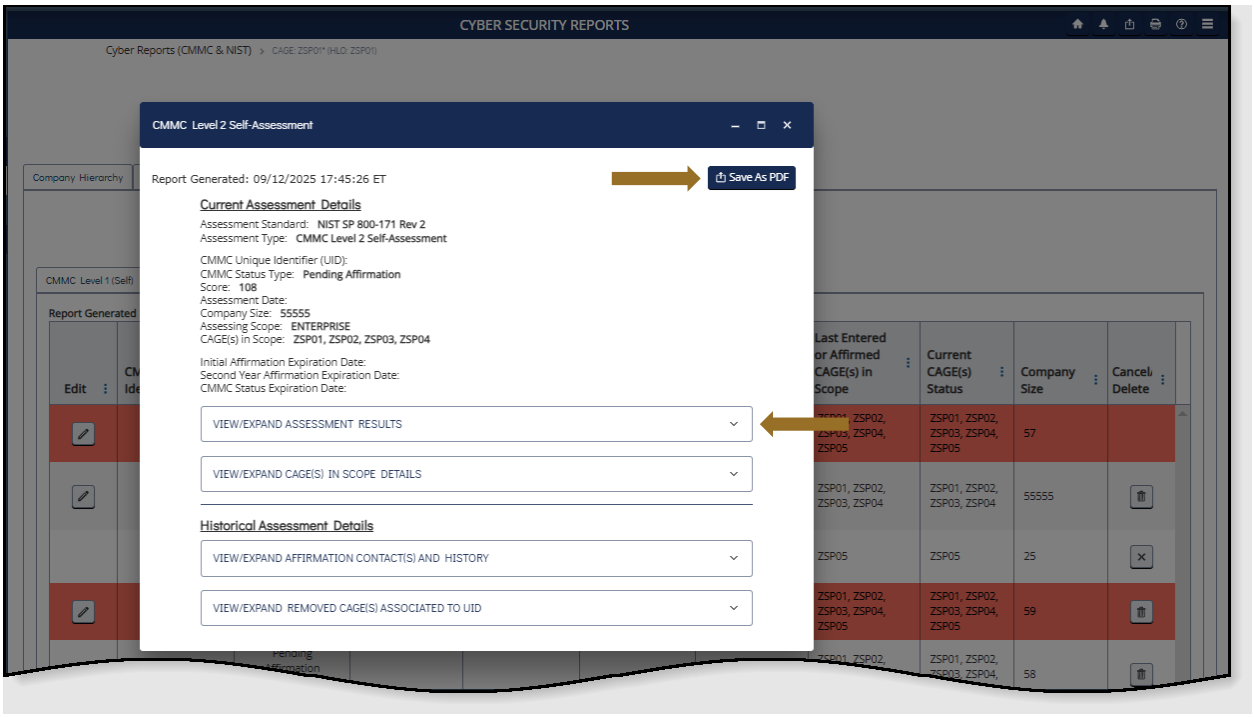


Figure 39: Cyber Reports CMMC Level 2 Self-Assessments Details Pop-up

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

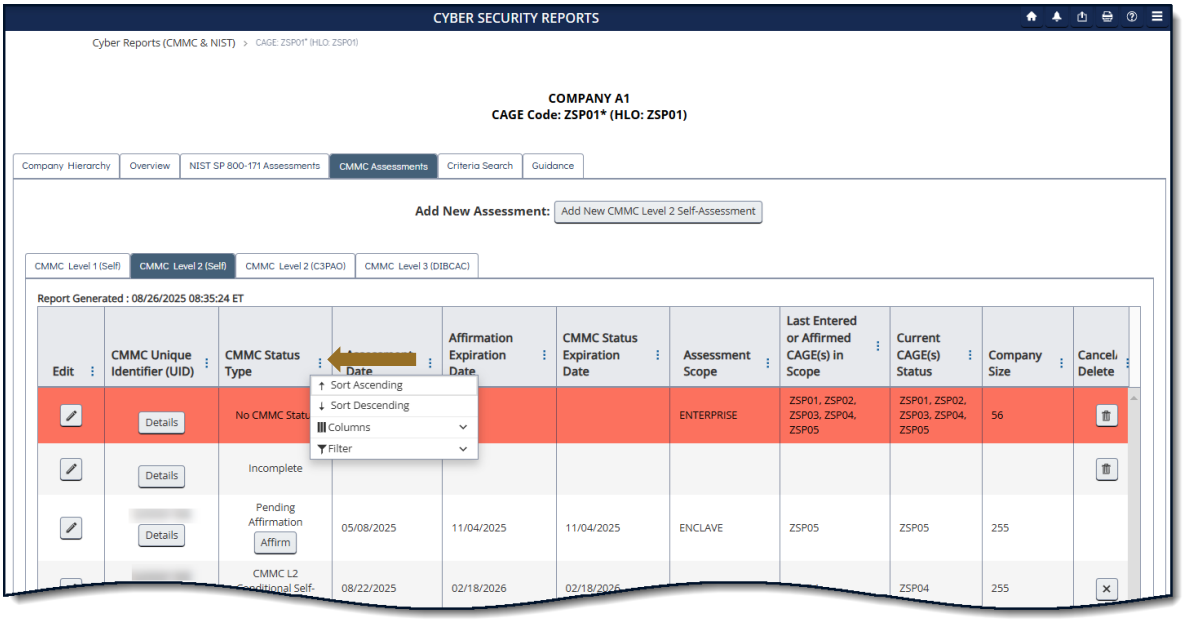


Figure 40: Cyber Reports CMMC Column Sorting and Filtering

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

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

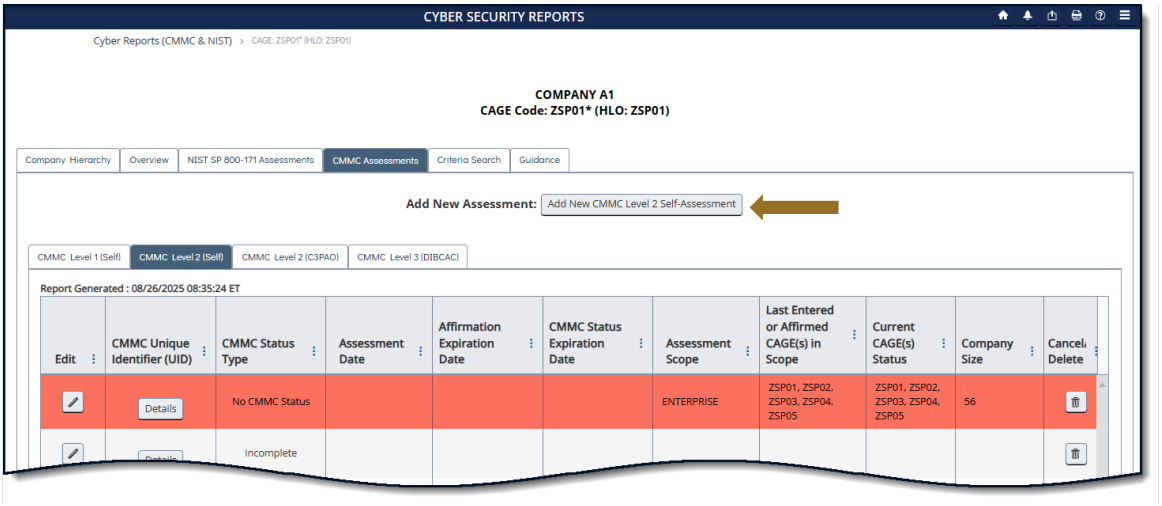


Figure 41: Cyber Reports CMMC Level 2 (Self) Add New

Review the warning message and select **Acknowledge**.

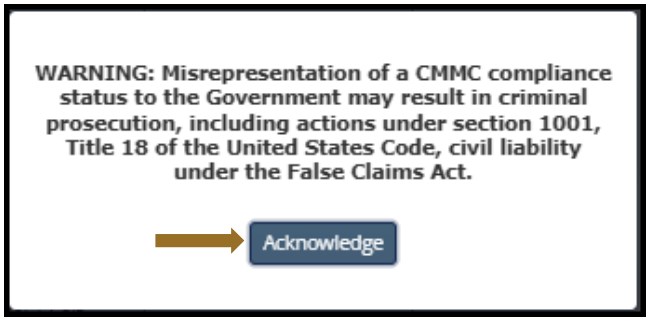


Figure 42: Cyber Reports Warning CMMC Levels 1 and 2

The requirements entry screen opens with the company name, CAGE/HLO combination, confidence level, and assessment standard in the header. A stepper identifies the Requirement Families and assessment progress. Select a step to open the associated requirements or proceed using the **Save and Continue** button.

Complete the Compliance Status for each Requirement Number; choose **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.

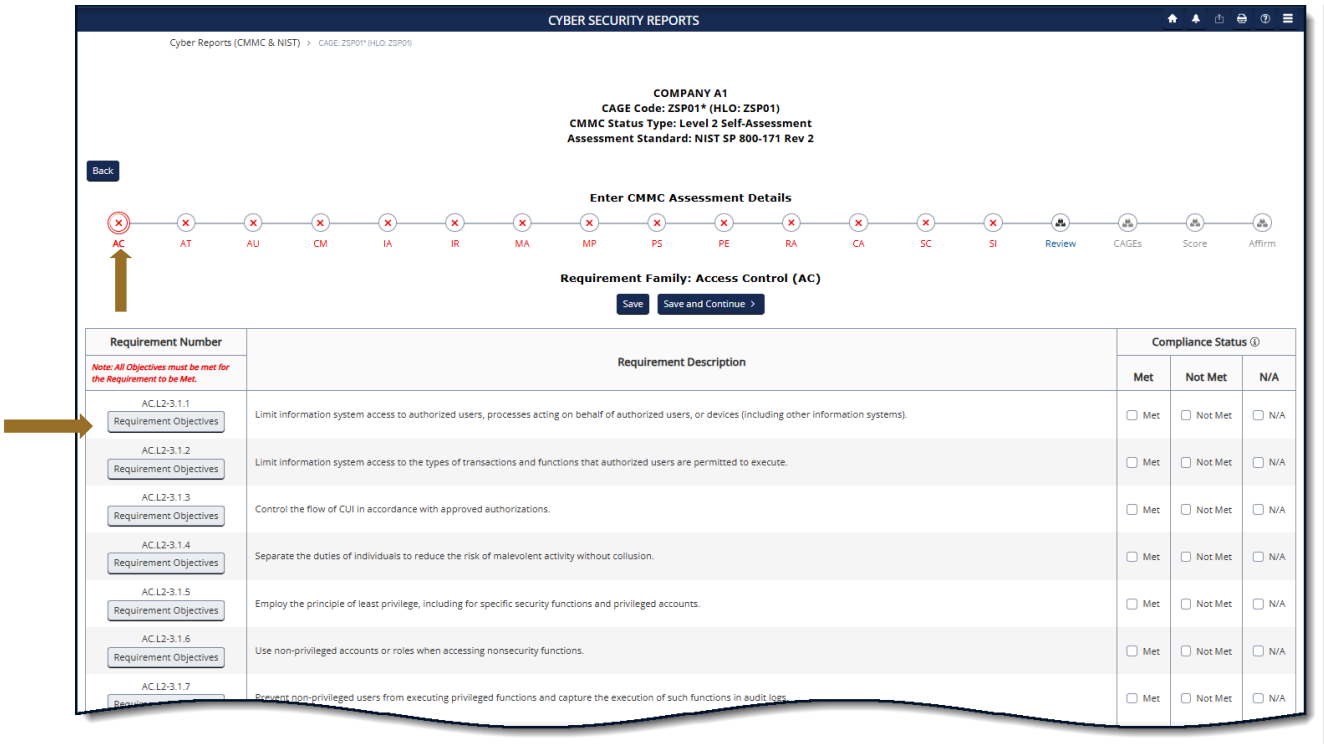


Figure 43: Cyber Reports Requirements in CMMC L2 Self-Assessment

For requirements IA.L2-3.533 and SC.L2-3.13.11, use the **Open Objectives** button in the Requirement Number column to complete the answers. The answer may result in partial credit for these requirements. Select **Save**.

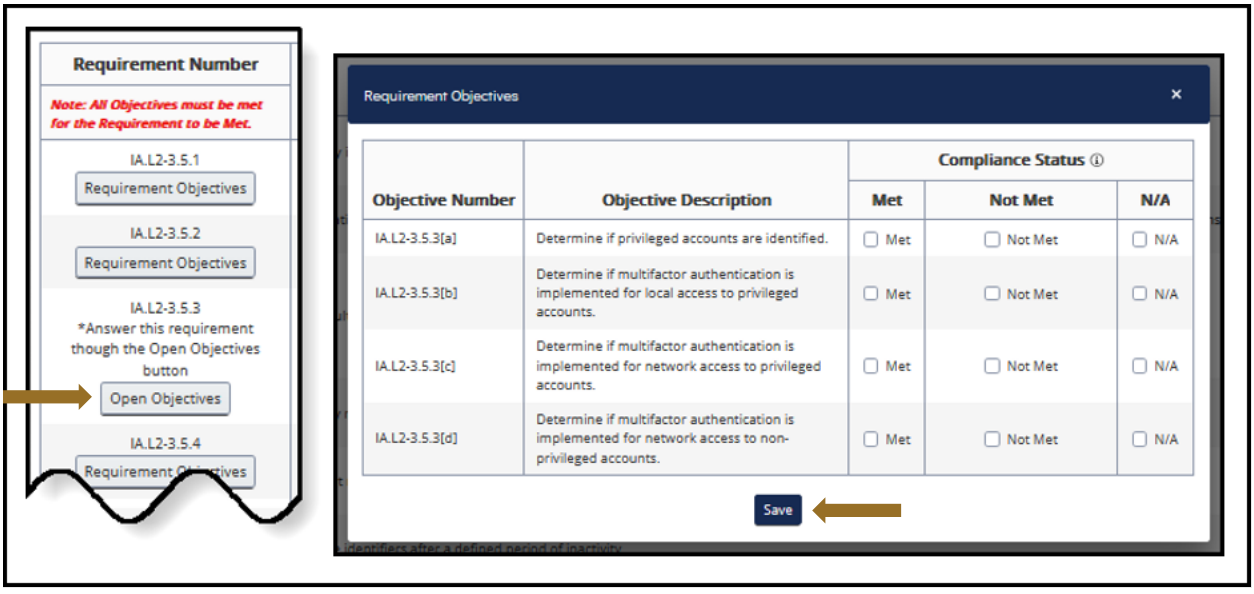


Figure 44: Cyber Reports CMMC L2 Self Assessment - Open Objectives Button

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

Steps in the stepper change from a red X to a blue ✓ when all requirements have been answered. Select the **Previous** button to navigate back within the page. Select the **Back** button to return to the CMMC summary report page.

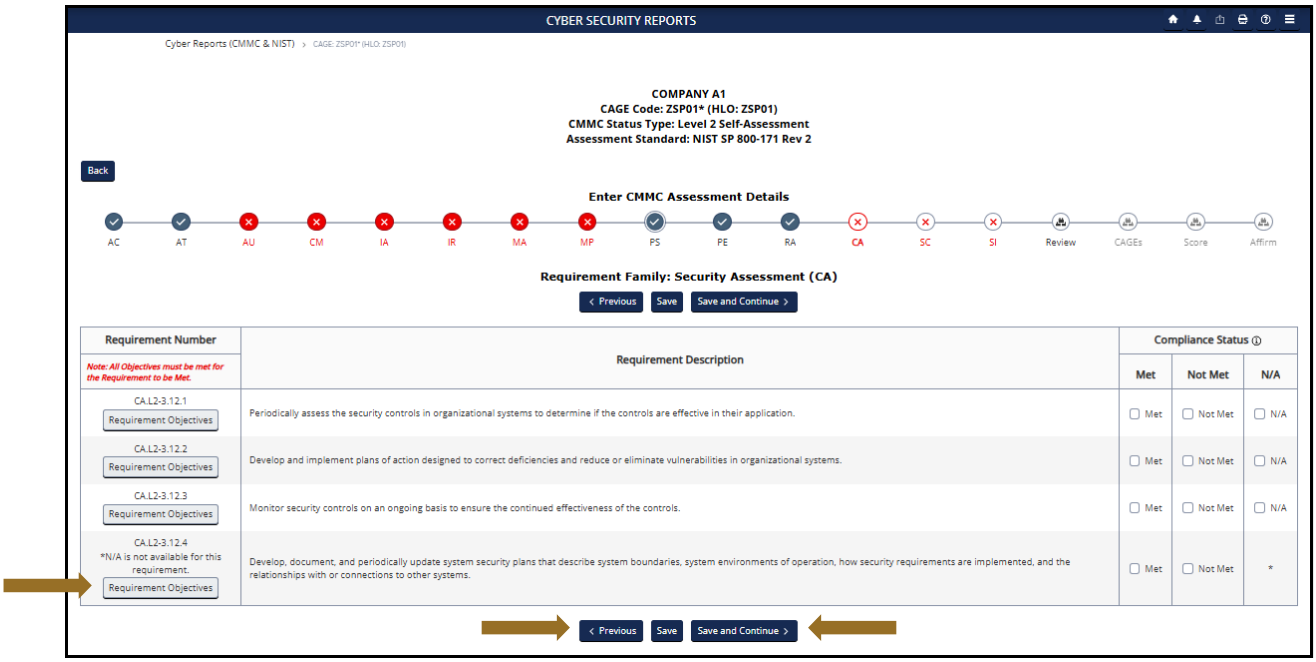


Figure 45: Cyber Reports Requirements in CMMC L2

The **Review** step shows the complete list of requirements and the selected compliance status. All requirements must be answered before continuing. To download an excel copy of the requirement number, description, and compliance status, select the **Export** button.

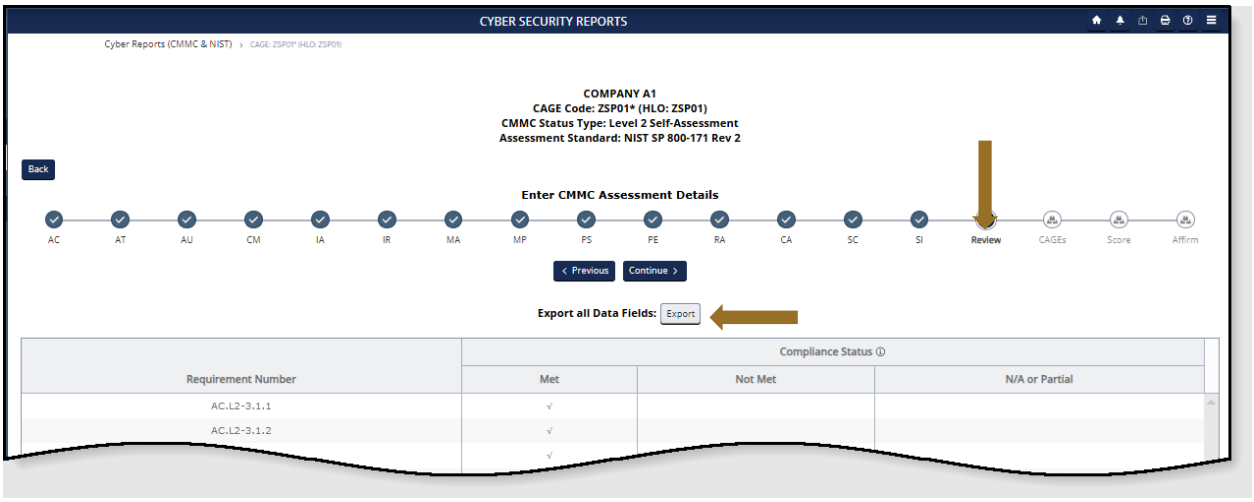


Figure 46: Cyber Reports CMMC L2 Export

The user will receive an Email Confirmation pop-up, select "**Ok**". The system will send an email when the Export is available. Select Download from the report menu and select the **Download** button when ready. (See Sec. 8.2)

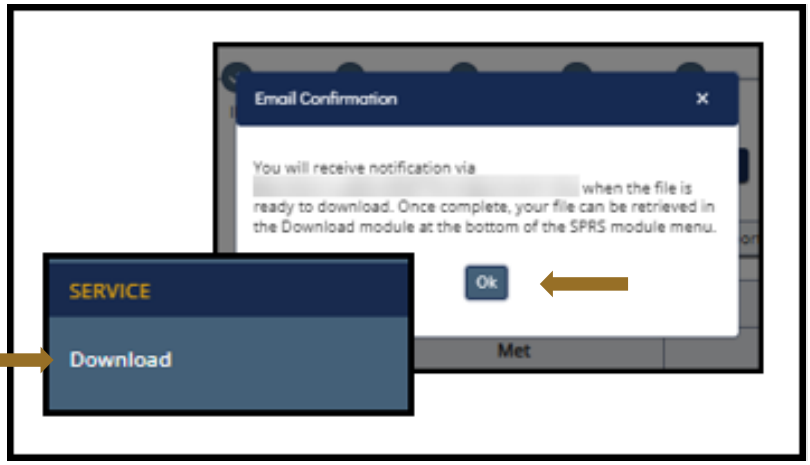


Figure 47: Cyber Reports CMMC L2 Export Notification and Retrieval

The CAGEs step requires the user to add the Assessment Scope, Employee Count, and included CAGE(s) information.

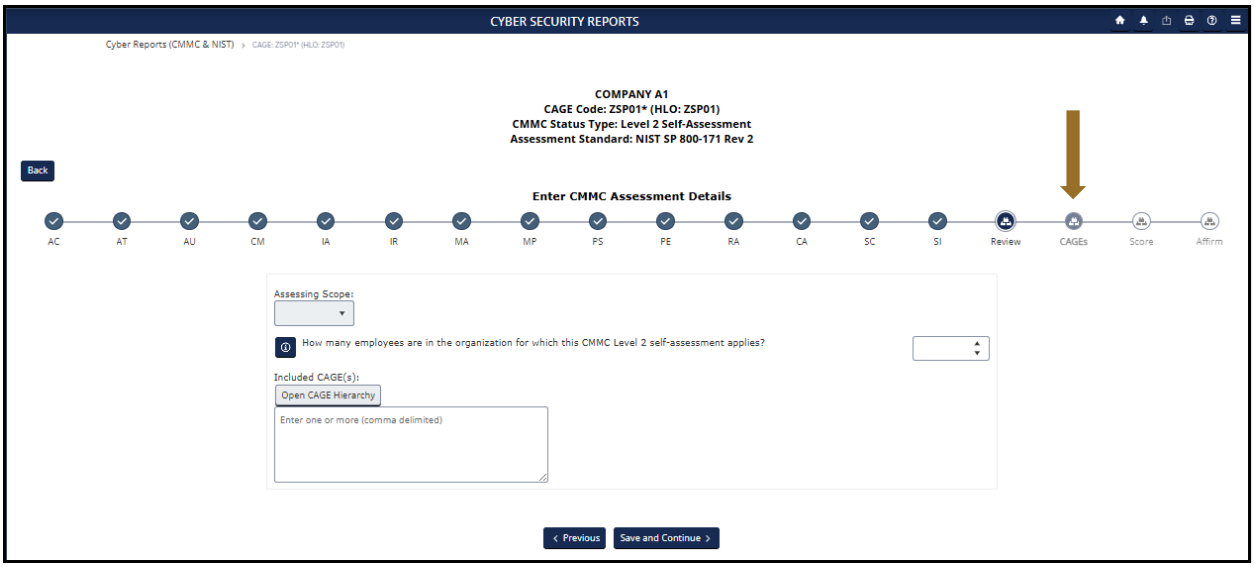


Figure 48: Cyber Reports CAGE(s) Stepper

The **Open CAGE Hierarchy** button opens the CAGE tree, allowing users to select which CAGEs are included/assessed. Users can also copy and paste a comma-delimited list of CAGEs into the CAGE text box provided. CAGEs must be in the current CAGE Hierarchy to be included in the assessment. (See Sec. 5.1.2)

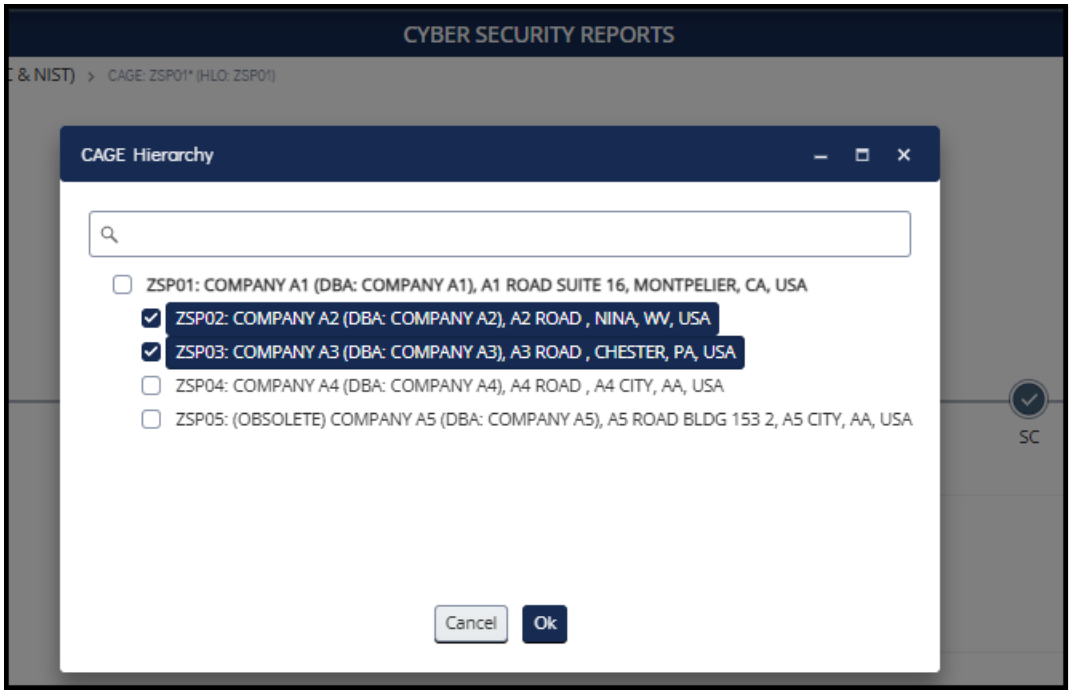


Figure 49: Cyber Reports CMMC L2 CAGE Hierarchy

After selecting **Save and Continue** on the CAGEs step, SPRS will calculate the score and status. The Score is listed in bold at the top.

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

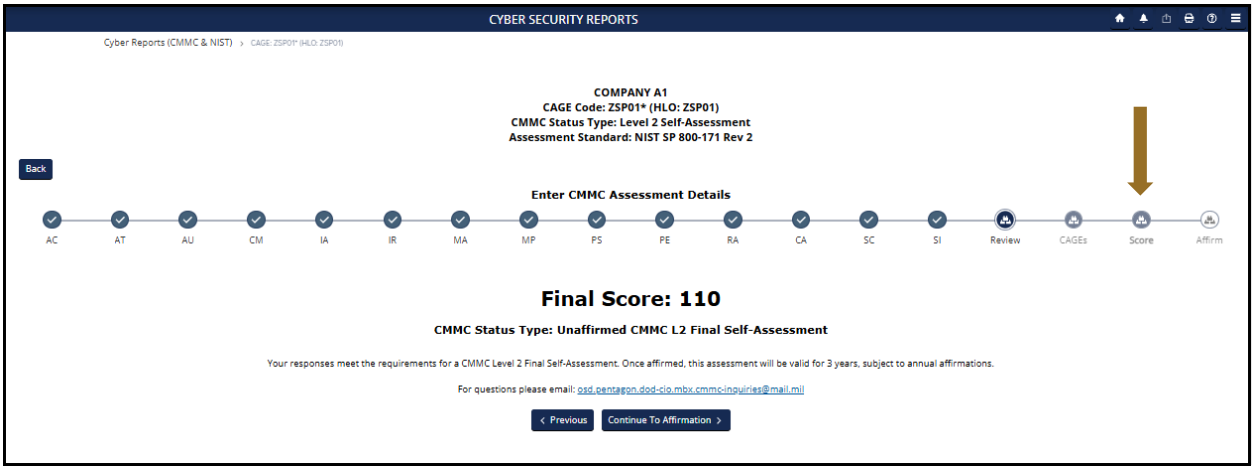


Figure 50: Cyber Reports CMMC L2 Score

***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 in progress and edited or affirmed later. Select the **Back** button to return to the report grid. These assessments will be identified as "Incomplete" in the CMMC Status Type column, will not be assigned a CMMC UID, and will not be visible to authorized government users.

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

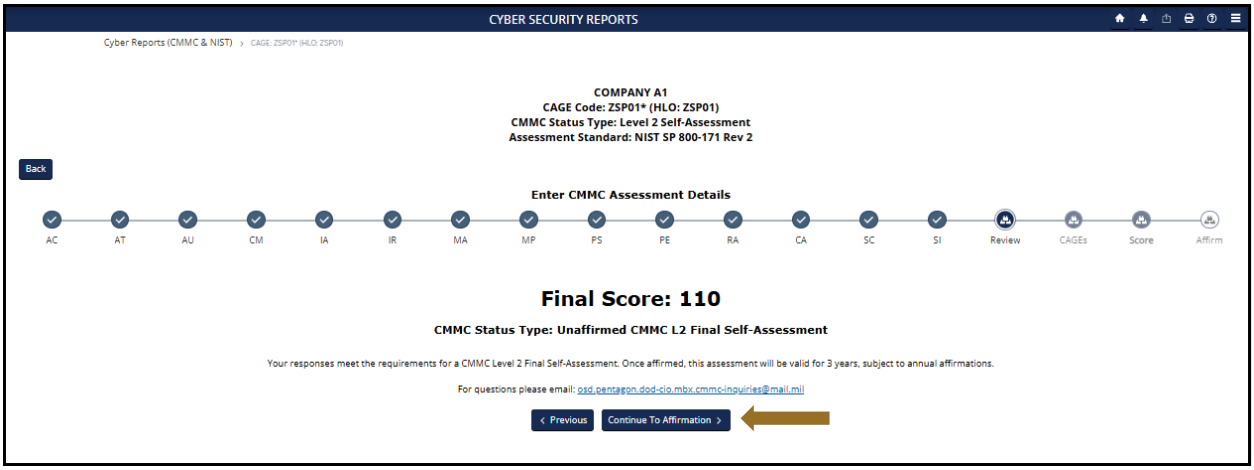


Figure 51: Cyber Reports CMMC L2 Previous or Continue to Affirmation

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**.

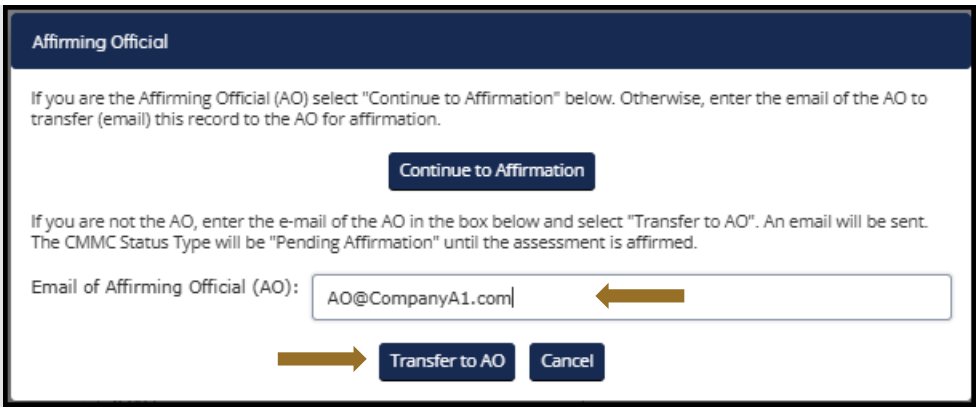


Figure 52: Cyber Reports CMMC L2 Transfer to AO

The AO will be sent an email notification, with the user on copy, that an assessment is waiting for their affirmation. This email is only sent once and may be prevented from being delivered by a company's email server settings.

For users that will only be entering SPRS to affirm assessments the *Affirming Official for CMMC Tutorial* is available on the SPRS Cyber Reports page here, ***https://www.sprs.csd.disa.mil/nistsp.htm***

To affirm an assessment, the AO must have the SPRS Cyber Vendor User role.

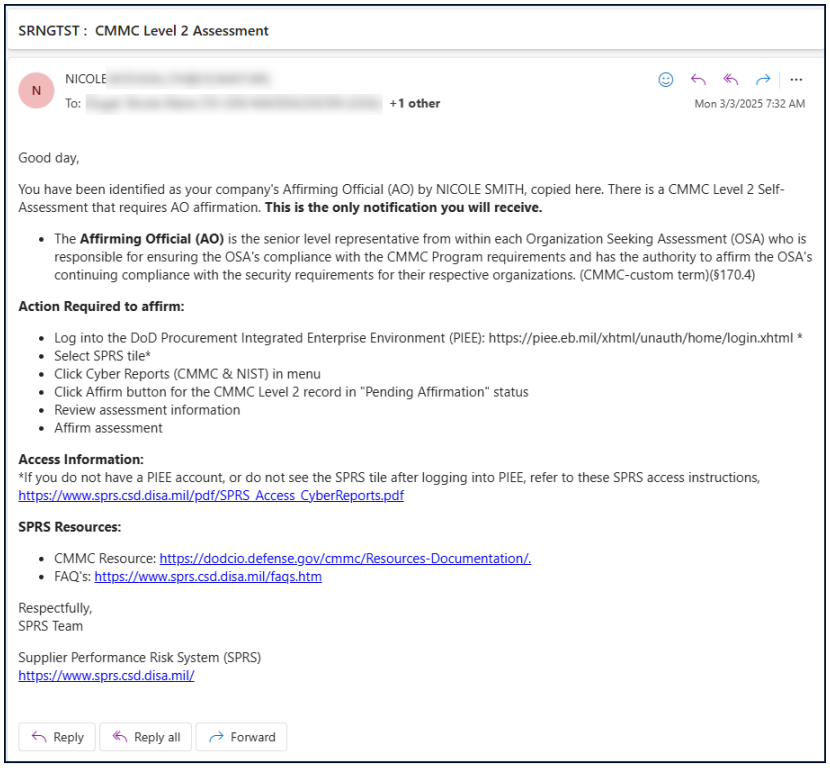


Figure 53: Cyber Reports CMMC L2 Sample AO Email

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

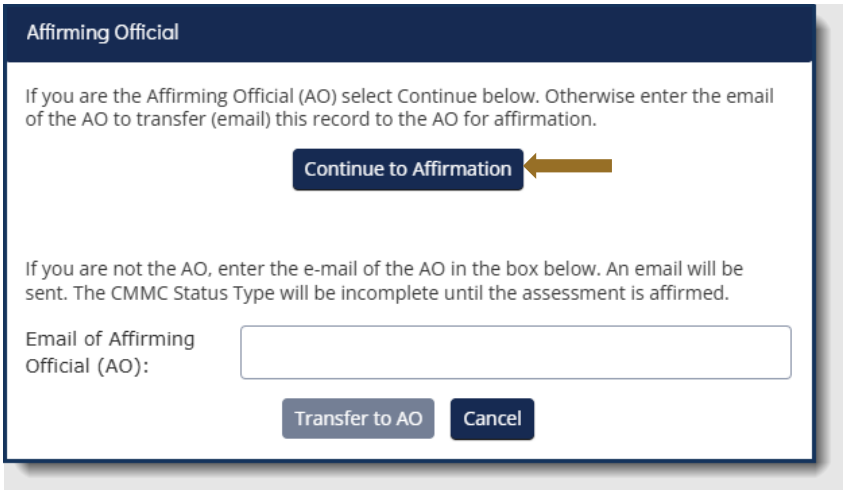


Figure 54: Cyber Reports CMMC L2 Continue to Affirmation

The Affirming Official information is pulled from the user's PIEE profile. Any changes must be made in PIEE and cannot be changed on this screen. Select **Back** or **Previous** to exit without affirming. Or enter any additional emails to be

associated with the record and click **Continue to Affirmation.** No notification will be sent to the additional emails.

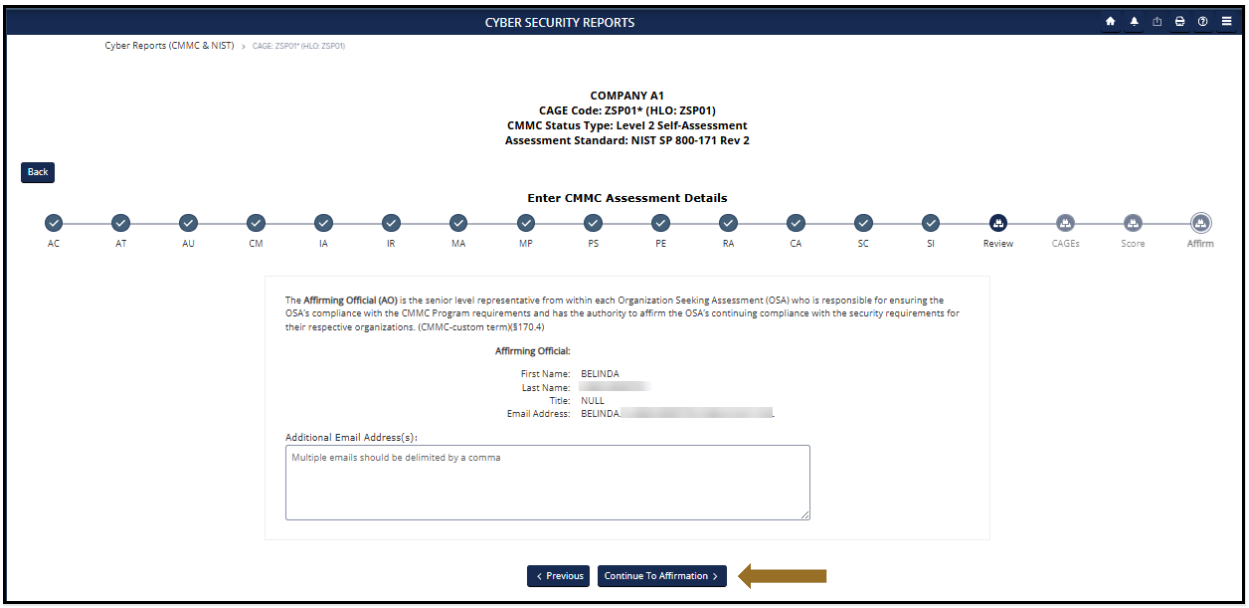


Figure 55: Cyber Reports CMMC L2 Affirming Official Identification

Review the information and statement in the Assessment and Affirmation pop-up. Select **Cancel** if information on the form needs to be updated or if the user is not the AO. To affirm, click the check box to certify and select the **Affirm** button.

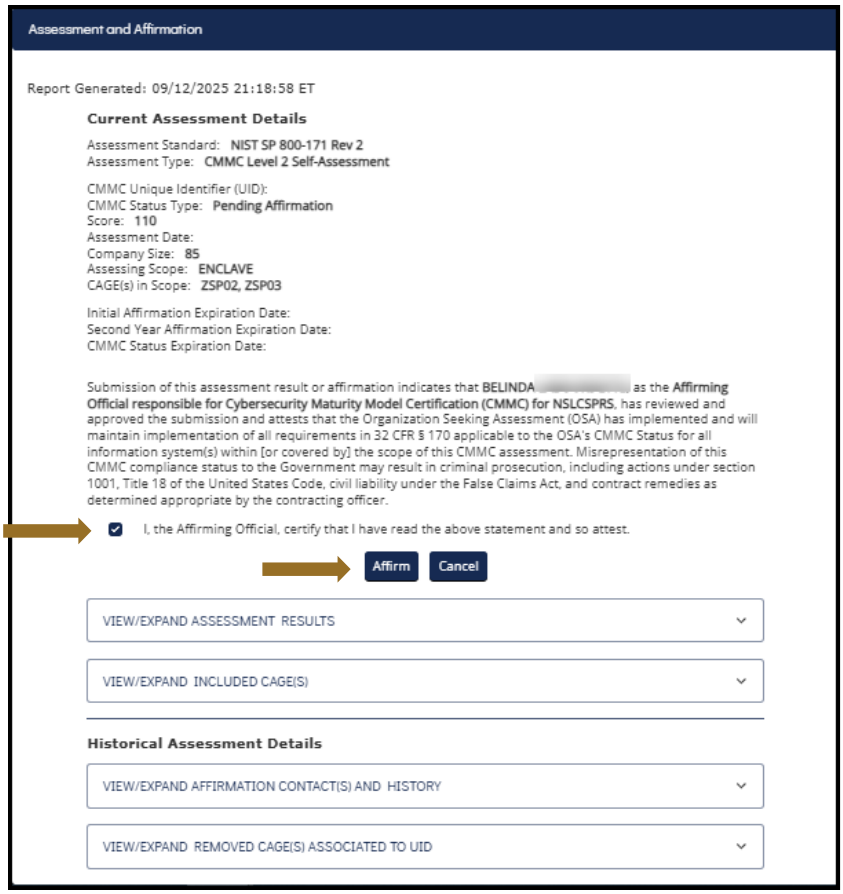


Figure 56: Cyber Reports CMMC L2 Certify and Affirm

The assessment will appear at the top of the report with a CMMC Unique Identifier (UID) assigned.

All CMMC assessment records must have a current affirmation to be considered Current. For a **"CMMC L2 Conditional Self-Assessment"** the CMMC Status and Affirmation Expiration dates are 180 days from the Assessment Date. For a **"CMMC L2 Final Self-Assessment"** the CMMC Status Expiration Date is three (3) years from the Assessment Date. The record requires annual affirmations to remain current. The initial Affirmation Expiration Date is one (1) year from the Assessment Date. The second year Affirmation Expiration Date is two (2) years from the Assessment Date.

The affirmation expiration dates are calculated based on the assessment date, not the date the record is affirmed. The record will be available for annual affirmation sixty (60) days prior to the affirmation expiration date. Users will not be notified when an affirmation has expired. The record will turn red and (Expired Affirmation) will be appended to the CMMC Status Type.

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**

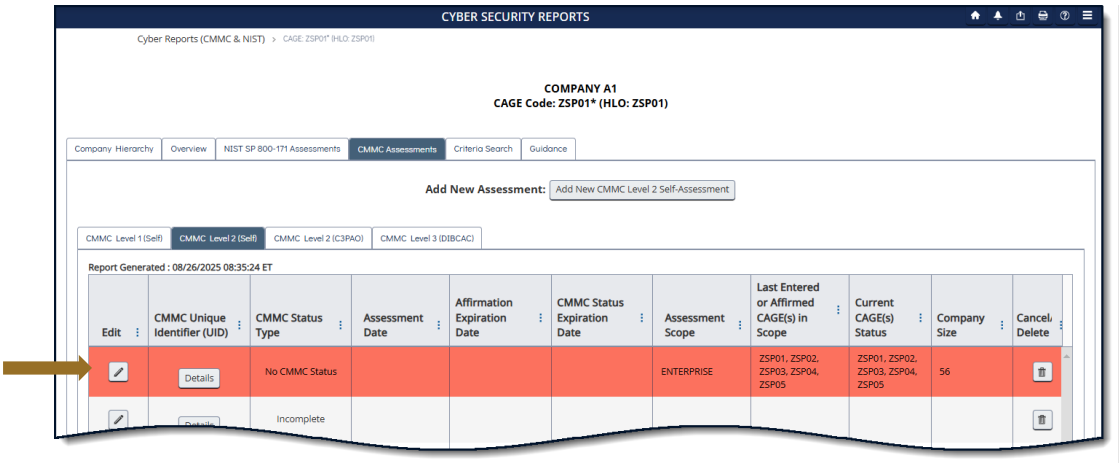


Figure 57: Cyber Reports CMMC L2 Edit an Assessment

If an assessment can be deleted, a trashcan icon will be within the far right **Cancel/Delete** column. Select the **Trashcan** button to delete. Review the assessment details and warning message. Deleting the assessment will delete it for all Included CAGEs. Select **Confirm Delete** or close the window without deleting.

- CMMC Status Types that can be deleted include:
    - **Incomplete**
    - **Pending Affirmation**
    - **No CMMC Status (Unaffirmed)**

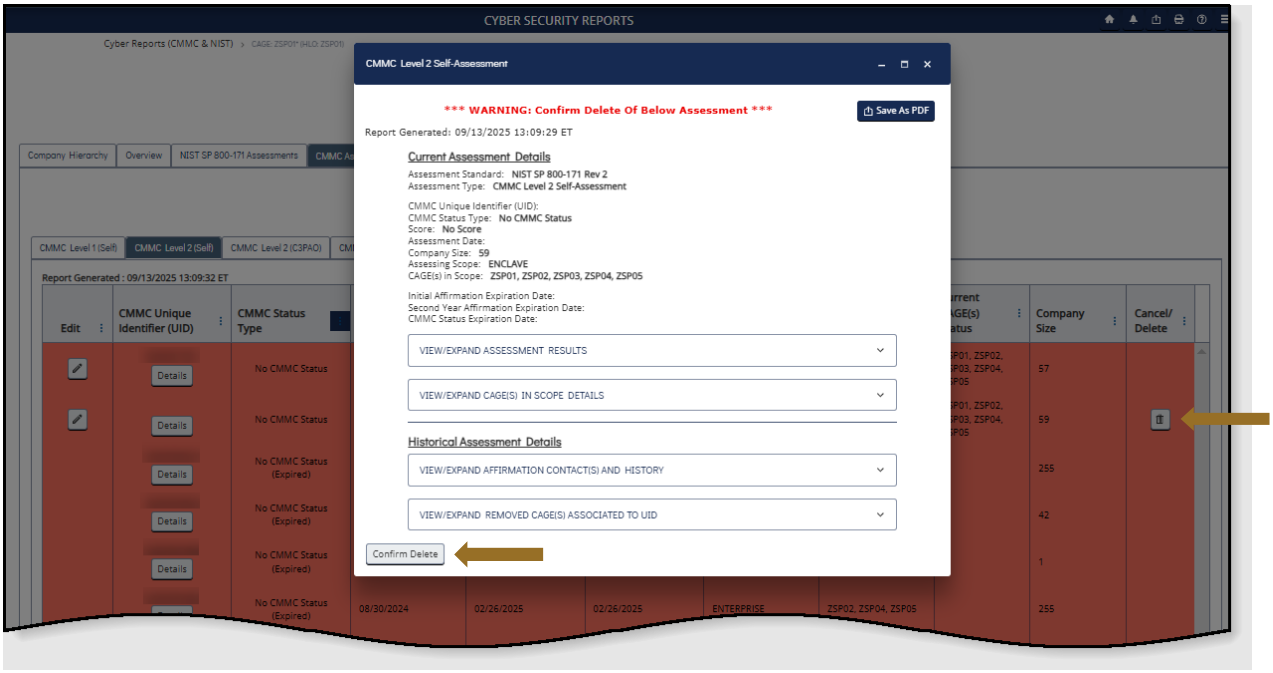


Figure 58: Cyber Reports CMMC L2 Delete an Assessment

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**

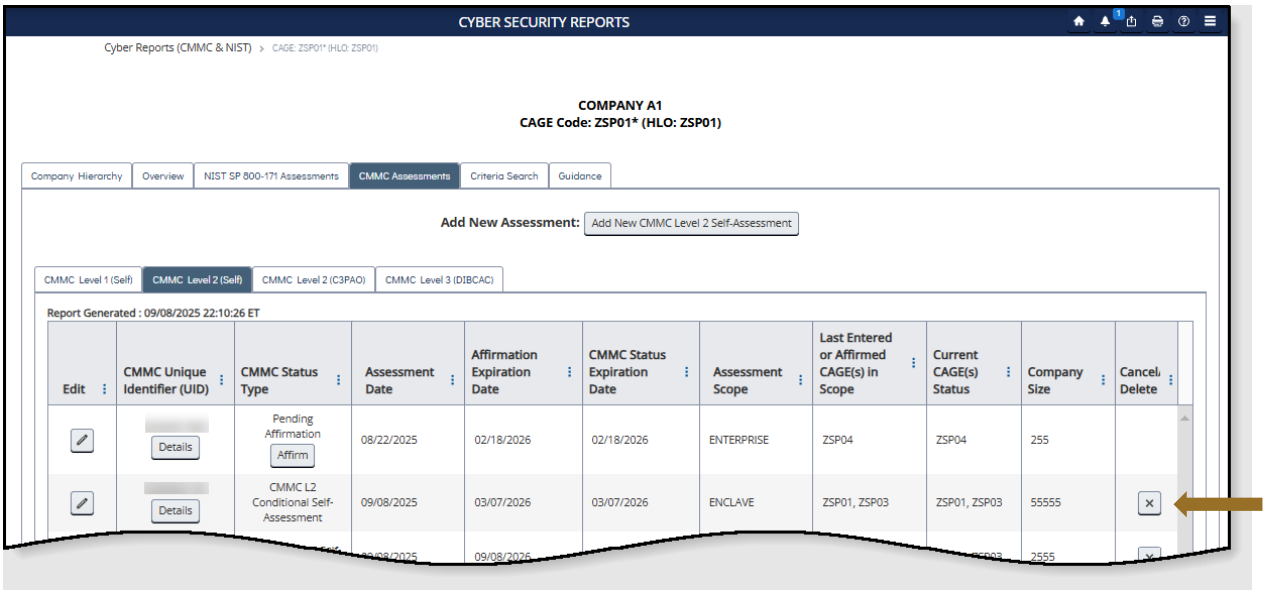


Figure 59: Cyber Reports CMMC L2 Cancel an Assessment

- 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 remain visible to authorized government users.

Annual affirmations are required for "CMMC L2 Final Self-Assessments". An Affirm button will appear in the Affirmation Expiration Date column 60 Days prior to the date listed and will persist until the assessment is affirmed. If the assessment is not affirmed before the 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 goes beyond the CMMC Status Expiration Date, the CMMC Status Type will change to "No CMMC Status (Expired)".

To complete an annual affirmation, select the **Affirm** button from within the Affirmation Expiration Date column. The report will open to the Affirming Official (AO) description. Review the AO information, any changes must be made in the users PIEE profile. 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. (Refer to Figures 55 & 56) If assessment information has changed a new assessment must be completed.

***NOTE*:** *The Affirmation Expiration and CMMC Status Expiration dates are based on the Assessment Date.*

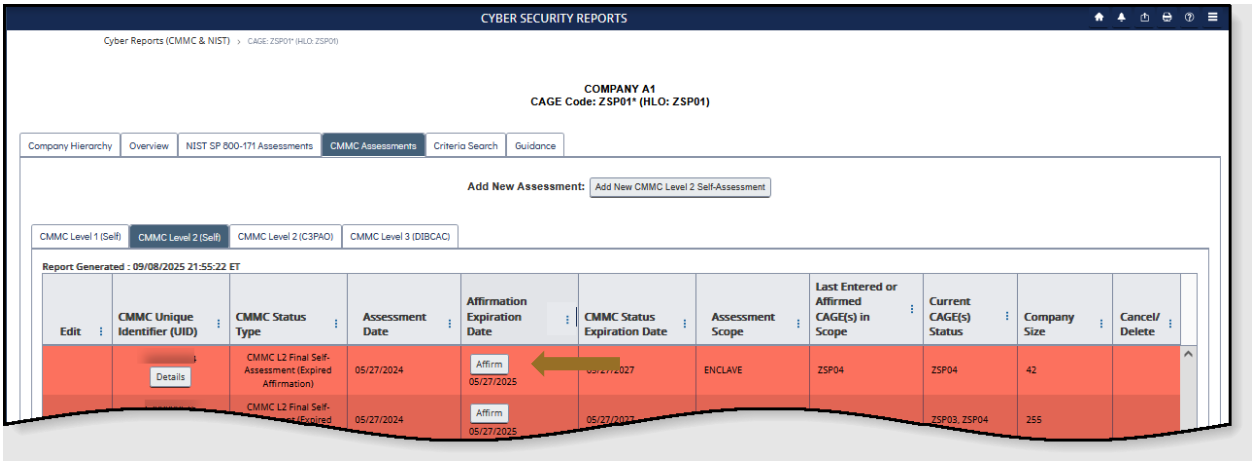


Figure 60: Cyber Reports CMMC L2 Annual Affirmation

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

For users that will only be entering SPRS to affirm assessments the *Affirming Official for CMMC Tutorial* is available on the SPRS Cyber Reports page here, ***https://www.sprs.csd.disa.mil/nistsp.htm***

(iii) CMMC Level 2 (C3PAO)

Summary results located on the CMMC Level 2 (C3PAO) subtab include the following information:

- **CMMC Unique Identifier (UID) –** The 10-digit alphanumeric assessment identifier. The first two letters delineate the CMMC confidence level. Level 1 and Level 2 Self-Assessments, assigned after initial affirmation, have prefix S1 and S2 respectively. Level 2 and Level 3 Assessments, assigned by eMASS, have prefix L2 and L3.
- **CMMC Status Type** – The status of the assessment record. Pending Affirmation (no CMMC UID) Status Types will not be visible to government users. Refer to Appendix E for list of Status Types and descriptions.
- **Assessment Date** – Date the assessment certificate was awarded.

- **Affirmation Expiration Date** – The date the current affirmation expires.
- **CMMC Status Expiration Date** – System calculated date based on assessment date and status type: 180 days for conditional status, and three (3) years for final status records.
- **Assessment Scope** – One of two selections:
    - 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)
- **Original CAGE(s) in Scope** – CAGE(s) in scope when the assessment was initially affirmed.
- **Current CAGE(s) in Scope** – CAGE(s) in scope in the current assessment.
- **Current Company Size** – Total of employees at all locations of the organization. Counts with strike-through are totals from previous record affirmations.
- **Score** – Score of the Assessment.

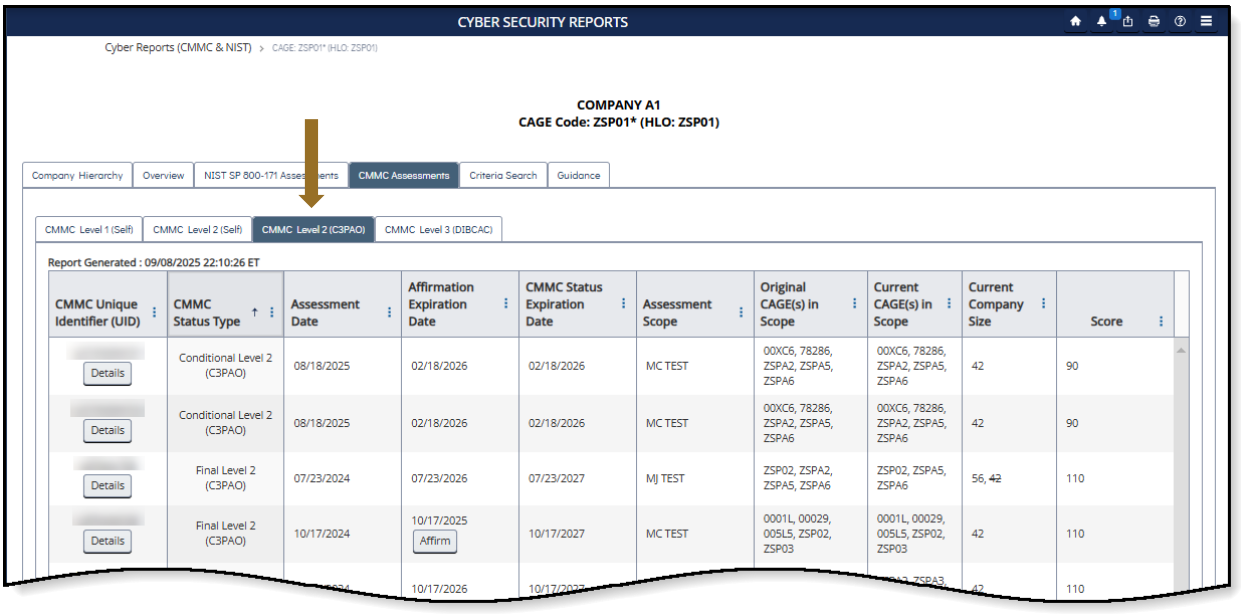


Figure 61: Cyber Reports CMMC L2 (C3PAO) Subtab

Select the **Details** button in the CMMC Unique Identifier (UID) column to open a print friendly display of all information associated with that record. Select the **View/Expand** options to see additional assessment information. Select **Save As**

PDF to save a copy.

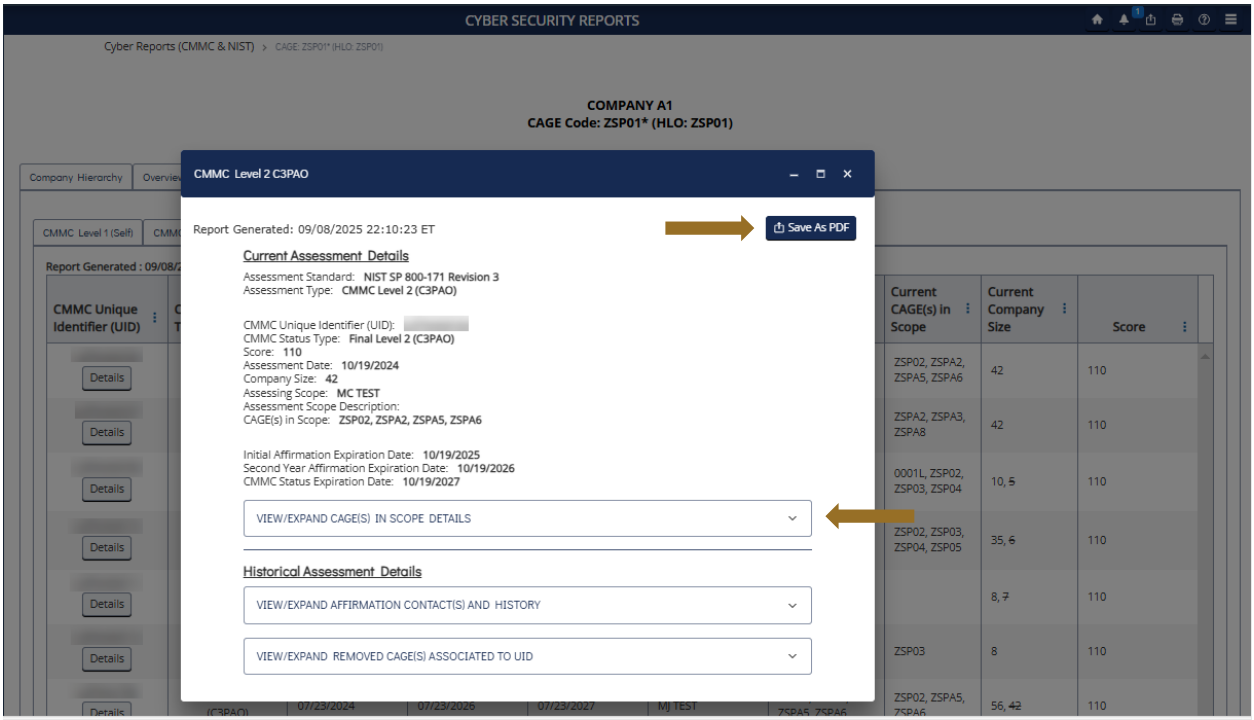


Figure 62: Cyber Reports CMMC L2 (C3PAO) Details Pop-up

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

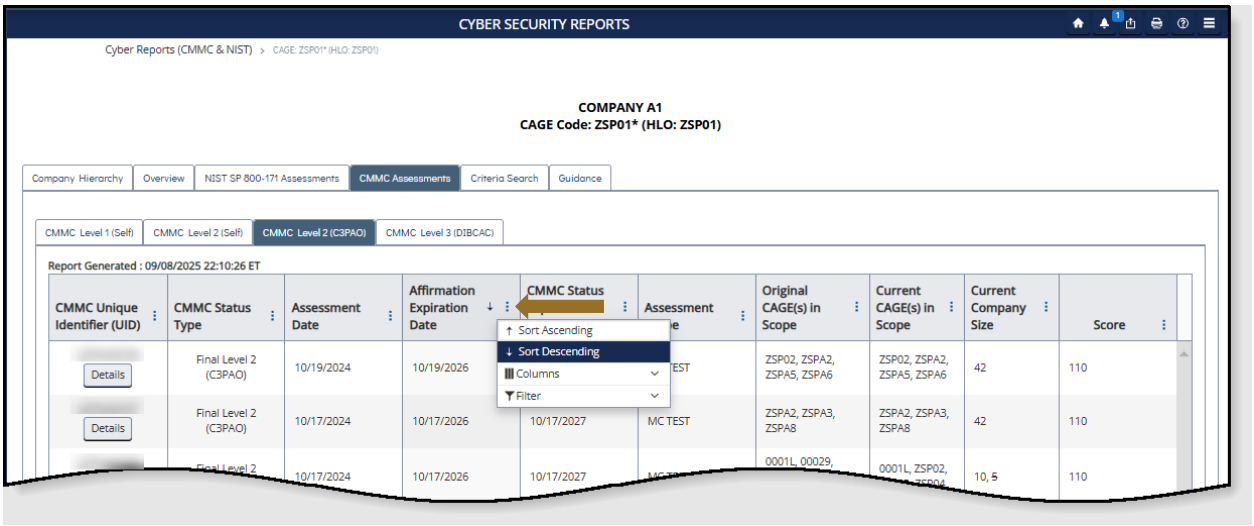


Figure 63: Cyber Reports CMMC Column Sorting and Filtering

All CMMC assessment records must have a current affirmation to be considered current. For a **"Conditional Level 2 (C3PAO)"** the CMMC Status and Affirmation Expiration dates are 180 days from the Assessment Date. For a **"Final Level 2 (C3PAO)"** the CMMC Status Expiration Date is three (3) years from the Assessment Date. The record requires annual affirmations to remain current. The initial Affirmation Expiration Date is one (1) year from the Assessment Date. The second year Affirmation Expiration Date is two (2) years from the Assessment Date.

The Affirmation Expiration Date column will remain blank until the initial affirmation. Affirmation dates can be seen by selecting either the **Details** or **Affirm** button. The affirmation expiration dates are calculated based on the assessment date, not the date the record is affirmed. After the initial affirmation the record will be available for annual affirmation sixty (60) days prior to the affirmation expiration date. Users will not be notified when an affirmation has expired. The record will turn red and (Expired Affirmation) will be appended to the CMMC Status Type.

Assessments must be affirmed by the 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)

To affirm an assessment, the AO must have the SPRS Cyber Vendor User role. For users that will only be entering SPRS to affirm assessments the *Affirming Official for CMMC Tutorial* is available on the SPRS Cyber Reports page here, ***https://www.sprs.csd.disa.mil/nistsp.htm***

To complete the initial affirmation, select the **Affirm** button located in the CMMC Status Type column.

Figure 64: Cyber Reports CMMC L2 (C3PAO) Initial Affirmation Button

The **Assessment and Affirmation** pop-up will open with the assessment record details and affirmation certification for the AO. View/Expand sections for CAGE(s) in scope, affirmation history, and CAGE(s) previously removed are at the bottom.

Click the check box to certify and select the **Affirm** button. Or select **Cancel** to return to the summary results if information is incorrect or if the user is not the AO. If information is incorrect, contact the submitting C3PAO.

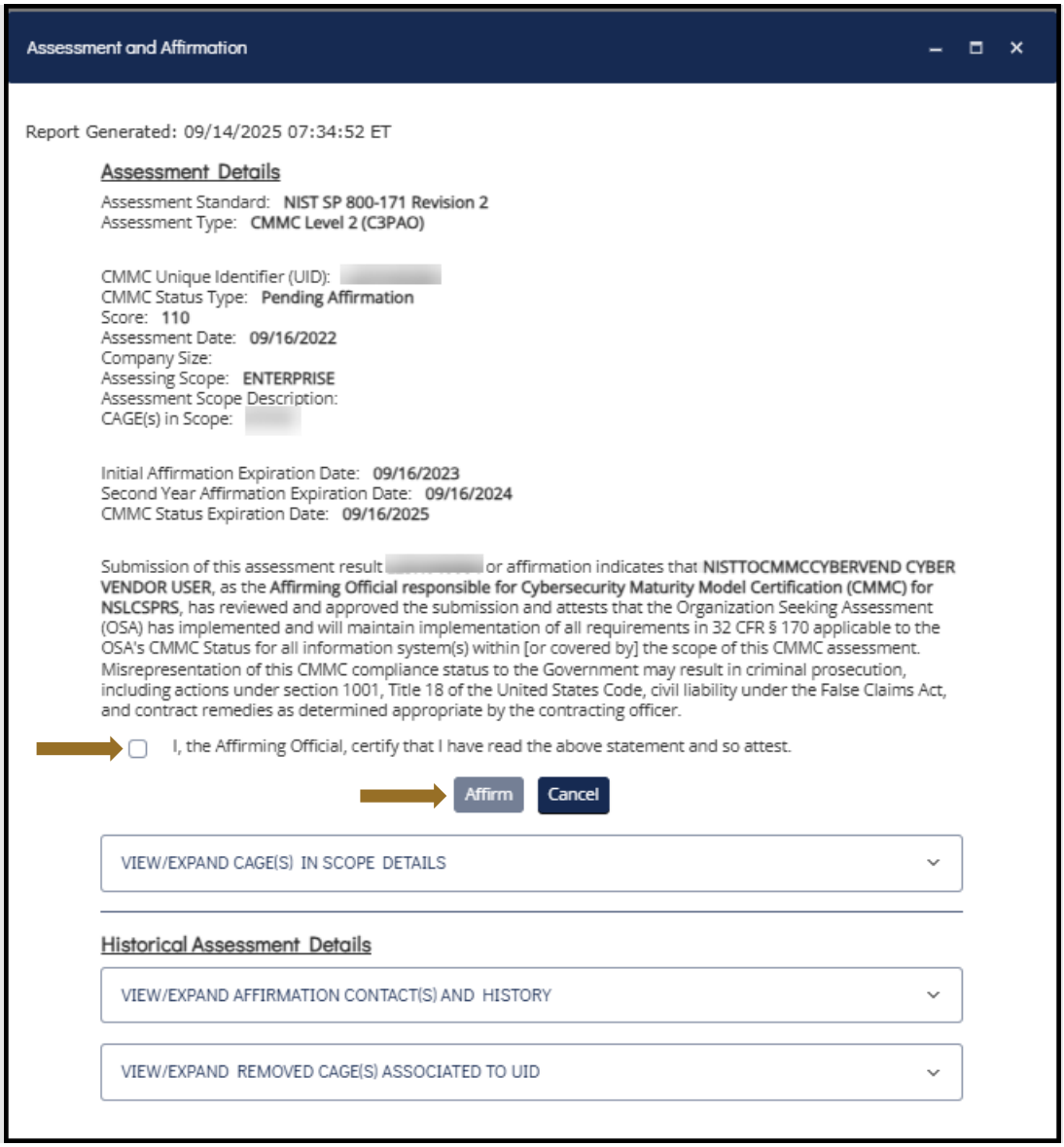


Figure 65: Cyber Reports CMMC L2 (C3PAO) Initial Affirmation

The affirmed assessment will appear at the top of the summary results as either a "**Conditional Level 2 (C3PAO)**" or "**Final Level 2 (C3PAO)**" status type.

To complete an annual affirmation for a **"Final Level 2 (C3PAO)"** assessment select the **Affirm** button in the Affirmation Expiration Date column.

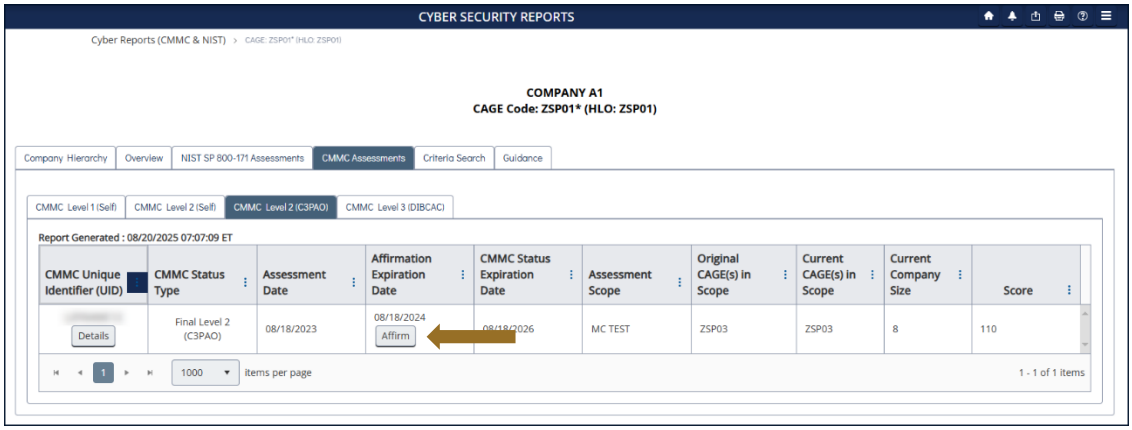


Figure 66: Cyber Reports CMMC L2 (C3PAO) Annual Affirmation Button

The **Assessment and Affirmation** pop-up will open with the assessment record details and affirmation certification for the AO. Two fields may be edited at this time.

Select the **pencil icon** button next to Company Size and update. Select the **check box** to confirm.

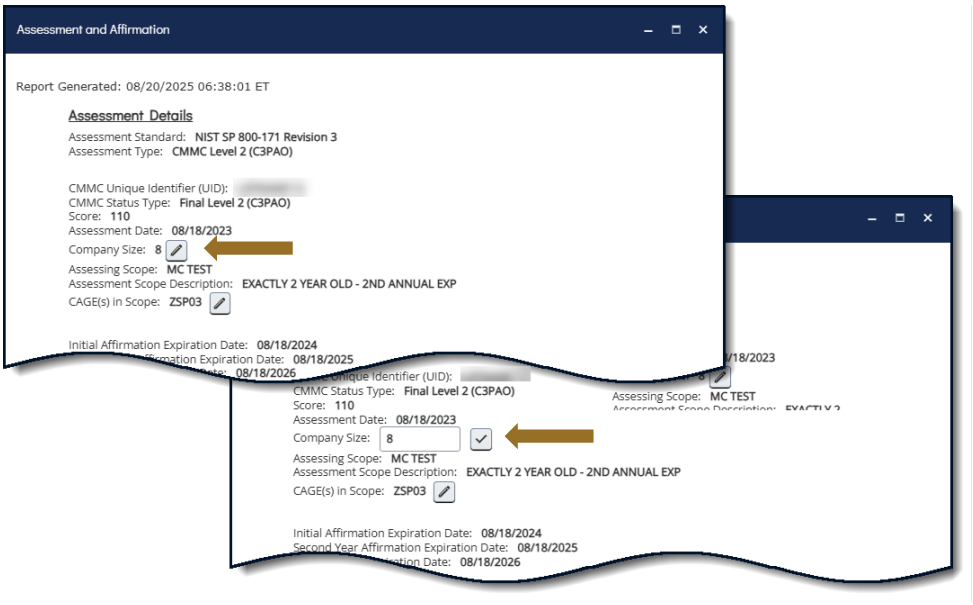


Figure 67: Cyber Reports CMMC L2 (C3PAO) Annual Affirmation - Company Size

Select the **pencil icon** button next to CAGE(s) in Scope to remove any CAGE(s) no longer associated with the assessment. The CAGE Hierarchy opens with a list of the CAGE(s) in scope pre-selected and a warning message. If a CAGE is removed, it cannot be re-added in SPRS. Click the check box of the CAGE to remove and select the **Ok** button to confirm.

Figure 68: Cyber Reports CMMC L2 (C3PAO) Annual Affirmation – CAGE(s) in Scope

Review the View/Expand sections for CAGE(s) in scope, affirmation history, and CAGE(s) previously removed at the bottom. Click the check box to certify and select the **Affirm** button. Or select **Cancel** to return to the summary results screen.

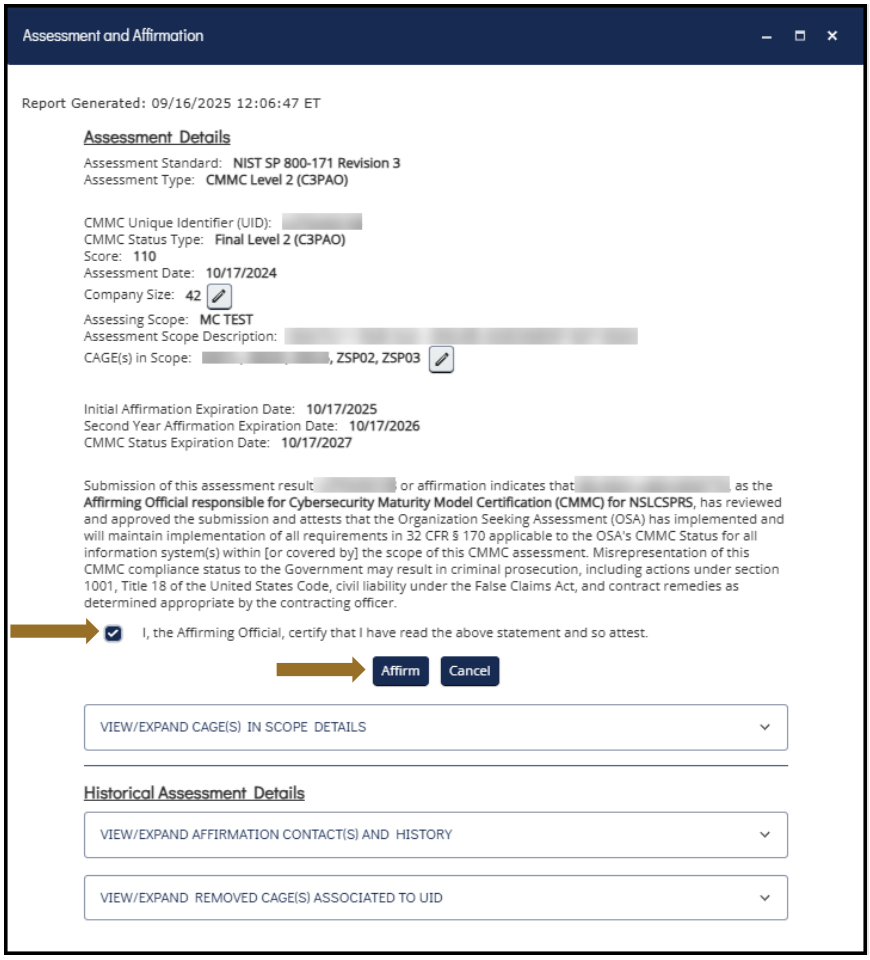


Figure 69: Cyber Reports CMMC L2 (C3PAO) Annual Affirmation Screen

The affirmed assessment will appear at the top of the summary results page with the updated Affirmation Expiration Date.

(iv) CMMC Level 3 (DIBCAC)

Summary results located on the CMMC Level 3 (DIBCAC) subtab include the following information:

- **CMMC Unique Identifier (UID) –** The 10-digit alphanumeric assessment identifier. The first two letters delineate the CMMC confidence level. Level 1 and Level 2 Self-Assessments, assigned after initial affirmation, have prefix S1 and S2 respectively. Level 2 and Level 3 Assessments, assigned by eMASS, have prefix L2 and L3.
- **CMMC Status Type** – The status of the assessment record. Pending

Affirmation (no CMMC UID) Status Types will not be visible to government users. Refer to Appendix E for list of Status Types and descriptions.

- **Assessment Date** – Date the assessment certificate was awarded.
- **Affirmation Expiration Date** – The date the current affirmation expires.
- **CMMC Status Expiration Date** – System calculated date based on assessment date and status type: 180 days for conditional status, and three (3) years for final status records.
- **Assessment Scope** – One of two selections:
    - 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)
- **Original CAGE(s) in Scope** – CAGE(s) in scope when the assessment was initially affirmed.
- **Current CAGE(s) in Scope** – CAGE(s) in scope in the current assessment.
- **Score** – Score of the Assessment.

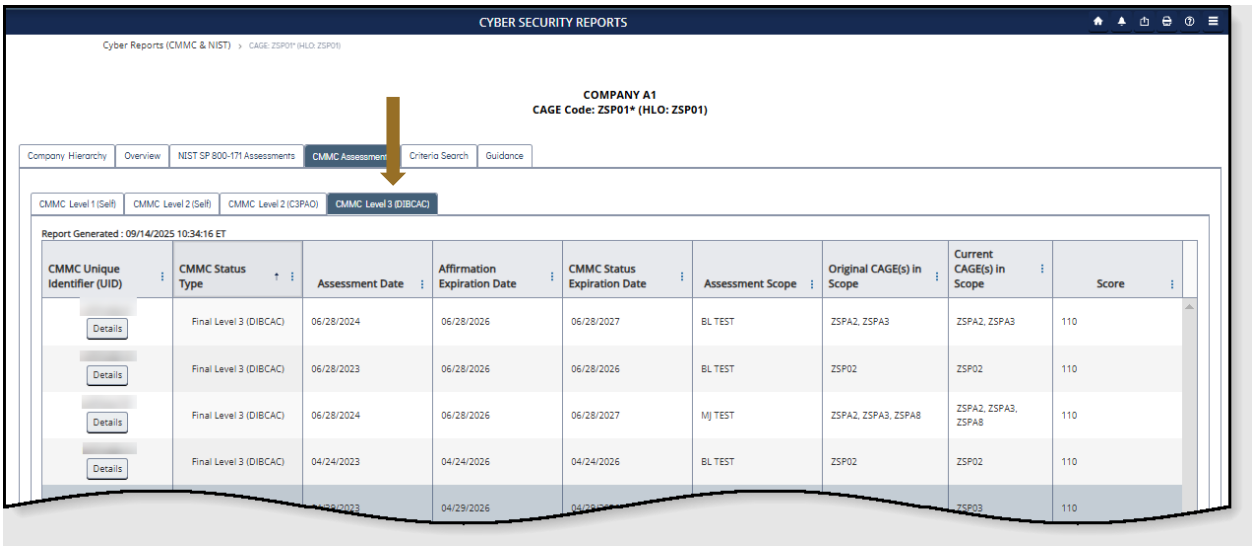


Figure 70: Cyber Reports CMMC L3 (DIBCAC) Subtab

Select the **Details** button in the CMMC Unique Identifier (UID) column to open a print friendly display of all information associated with that record. Select the **View/Expand** options to see additional assessment information. Select **Save As PDF** to save a copy.

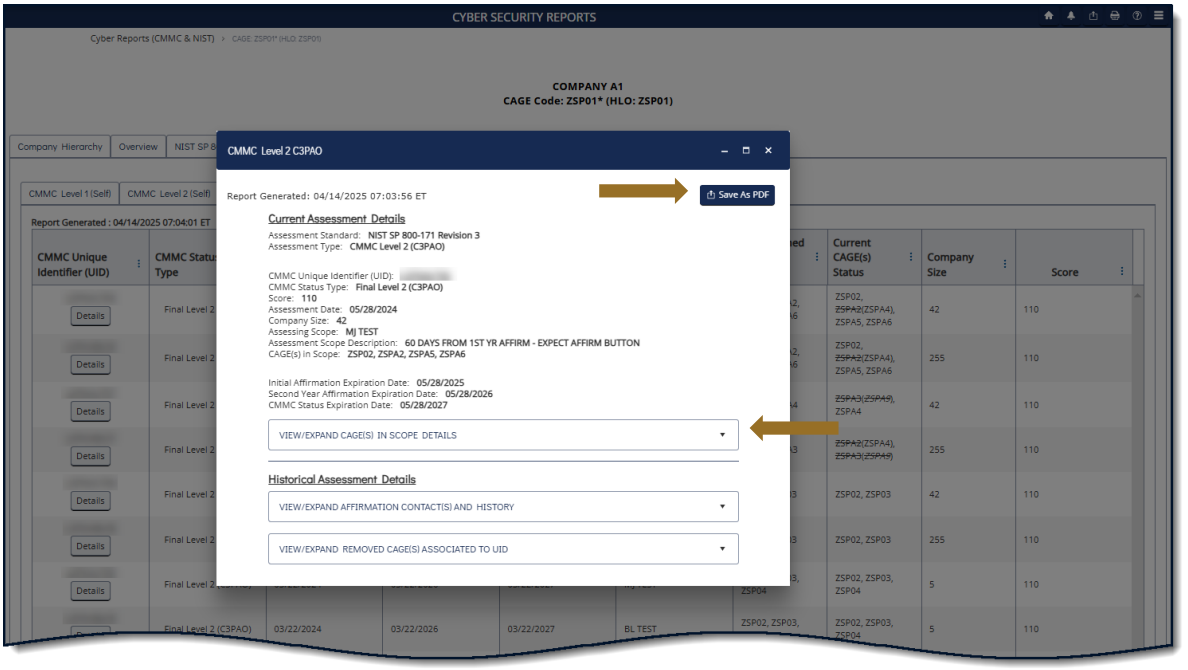


Figure 71: Cyber Reports CMMC L3 (DIBCAC) Details Pop-up

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

Figure 72: Cyber Reports CMMC Column Sorting and Filtering

All CMMC assessment records must have a current affirmation to be considered

current. For a **"Conditional Level 3 (DIBAC)"** the CMMC Status and Affirmation Expiration dates are 180 days from the Assessment Date. For a **"Final Level 3 (DIBCAC)"** the CMMC Status Expiration Date is three (3) years from the Assessment Date. The record requires annual affirmations to remain current. The initial Affirmation Expiration Date is one (1) year from the Assessment Date. The second year Affirmation Expiration Date is two (2) years from the Assessment Date.

The Affirmation Expiration Date column will remain blank until the initial affirmation. Affirmation dates can be seen by selecting either the **Details** or **Affirm** button. The affirmation expiration dates are calculated based on the assessment date, not the date the record is affirmed. After the initial affirmation the record will be available for annual affirmation sixty (60) days prior to the affirmation expiration date. Users will not be notified when an affirmation has expired. The record will turn red and "**(Expired Affirmation)**" will be appended to the CMMC Status Type.

Assessments must be affirmed by the 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)

To affirm an assessment, the AO must have the SPRS Cyber Vendor User role. For users that will only be entering SPRS to affirm assessments the *Affirming Official for CMMC Tutorial* is available on the SPRS Cyber Reports page here, ***https://www.sprs.csd.disa.mil/nistsp.htm***.

To complete the initial affirmation, select the **Affirm** button located in the CMMC Status Type column.

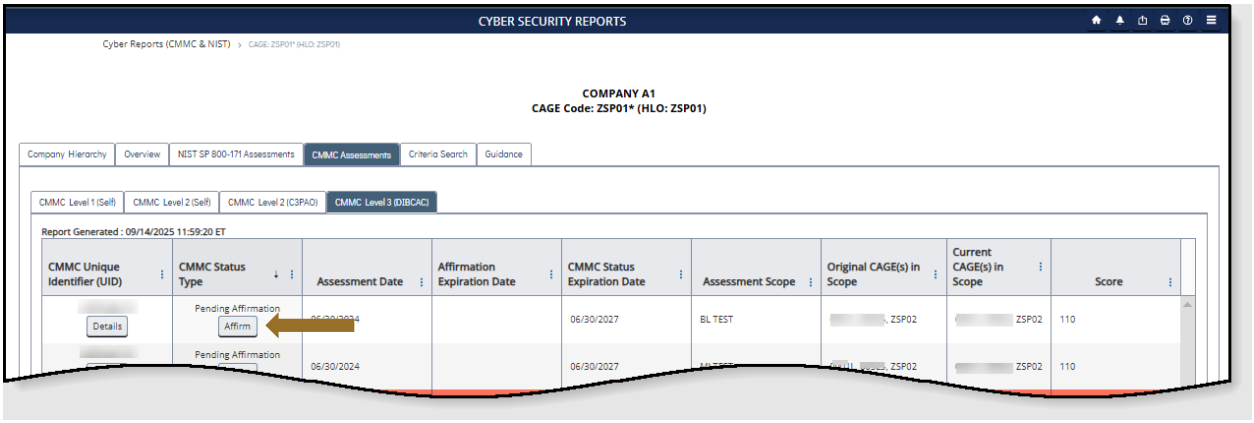


Figure 73: Cyber Reports CMMC L3 (DIBCAC) Initial Affirmation Button

The **Assessment and Affirmation** pop-up will open with the assessment record details and affirmation certification for the AO. View/Expand sections for CAGE(s) in scope, affirmation history, and CAGE(s) previously removed are at the bottom.

Click the check box to certify and select the **Affirm** button. Or select **Cancel** to return to the summary report screen if information is incorrect or if the user is not the AO. If information is incorrect, contact DIBCAC.

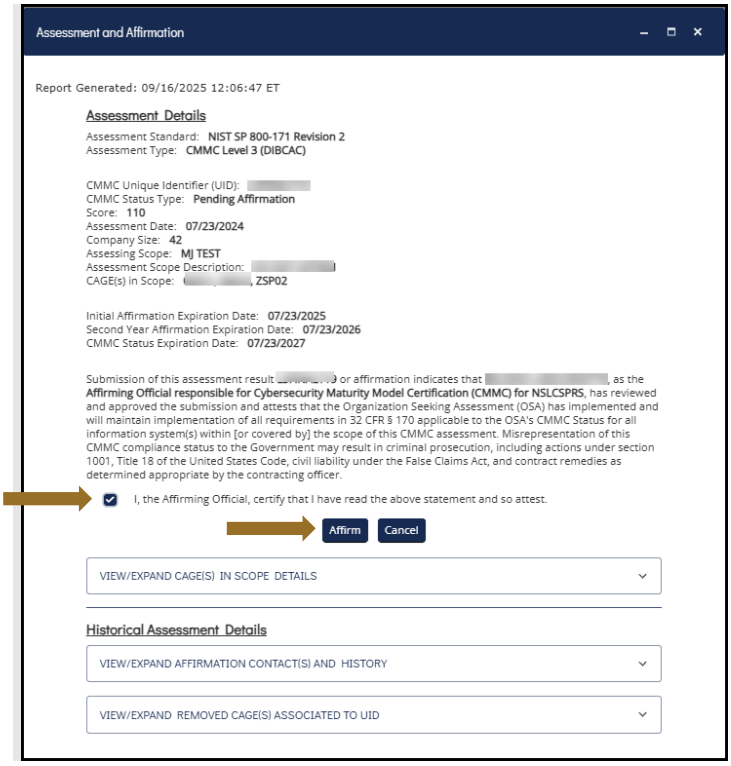


Figure 74: Cyber Reports CMMC L3 (DIBCAC) Initial Affirmation

The affirmed assessment will appear at the top of the summary report as either a "**Conditional Level 3 (DIBCAC)**" or "**Final Level 3 (DIBCAC)**" status type.

To complete an annual affirmation for a **"Final Level 3 (DIBCAC)"** assessment select the **Affirm** button in the Affirmation Expiration Date column.

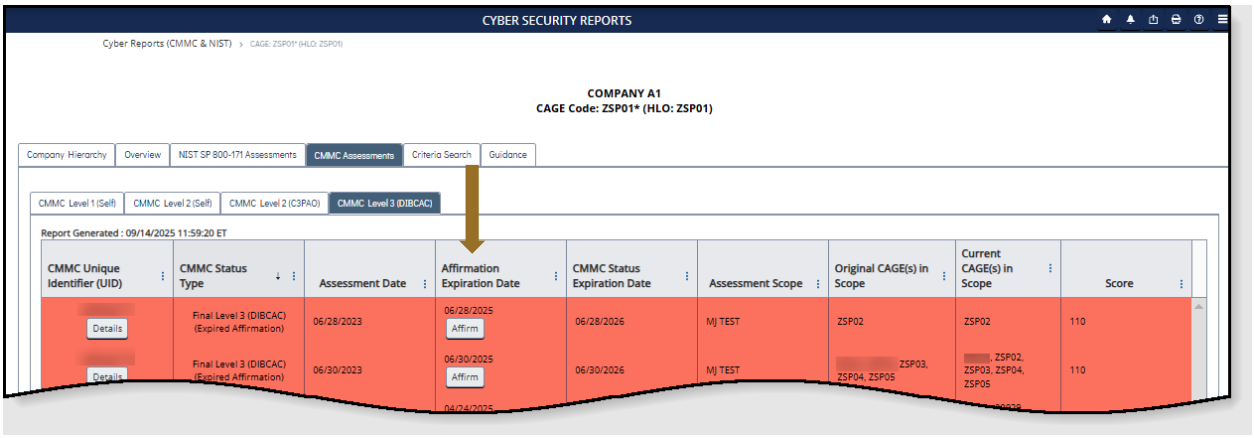


Figure 75: Cyber Reports CMMC L3 (DIBCAC) Annual Affirmation Button

The **Assessment and Affirmation** pop-up will open with the assessment record details and affirmation certification for the AO. Two fields may be edited at this time.

Select the **pencil icon** button next to Company Size and update. Select the **check box** to confirm.

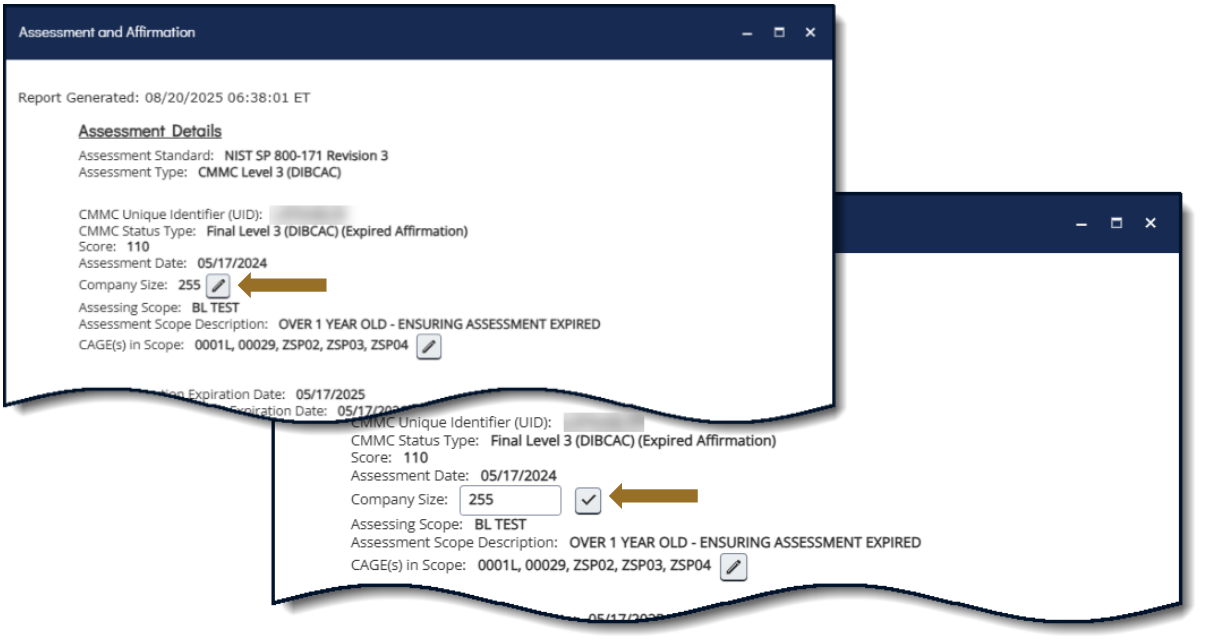


Figure 76: Cyber reports CMMC L3 (DIBCAC) Annual Affirmation - Company Size

Select the **pencil icon** button next to CAGE(s) in Scope to remove any CAGE(s) no longer associated with the assessment. The CAGE Hierarchy opens with a list of the CAGE(s) in scope pre-selected and a warning message. If a CAGE is removed, it cannot be re-added in SPRS. Click the check box of the CAGE to remove and select the **Ok** button to confirm.

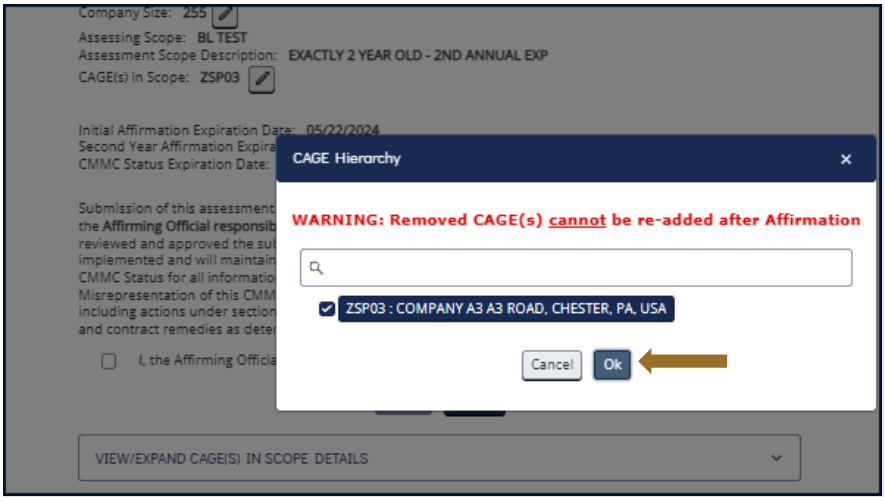


Figure 77: Cyber Reports CMMC L3 (DIBCAC) Annual Affirmation - CAGE(s) in Scope

Review assessment details and the View/Expand sections for CAGE(s) in scope, affirmation history, and CAGE(s) removed at the bottom. Click the check box to certify and select the **Affirm** button. Or select **Cancel** to return to the summary report screen.

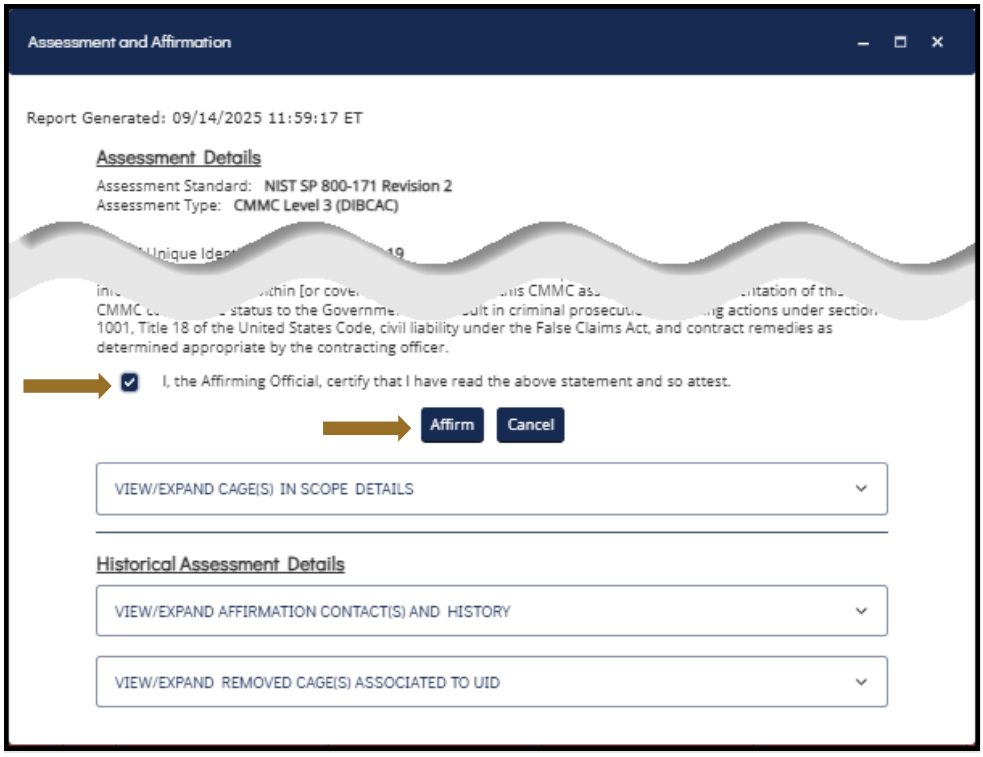


Figure 78: Cyber Reports CMMC Level 3 (DIBCAC) Annual Affirmation

The affirmed assessment will appear at the top of the summary results with the updated Affirmation Expiration Date.

5.1.6 Criteria Search Tab

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. Users will also have access to any CMMC C3PAO and DIBCAC prepared assessment that includes their authorized CAGE in the assessed scope. Enter the desired search criteria and select the **Search** button.

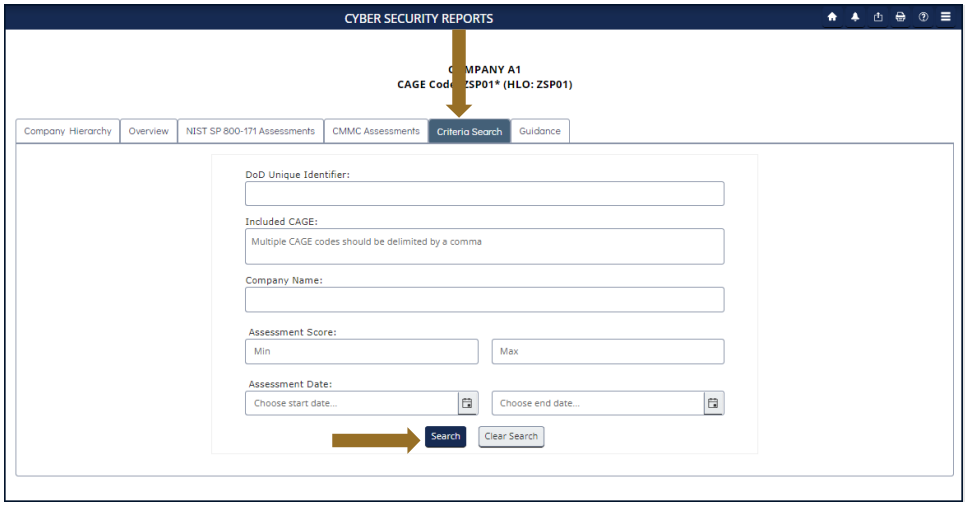


Figure 79: Cyber Reports Criteria Search Tab

The search returns all applicable records organized by confidence level in subtabs beginning with the Basic subtab.

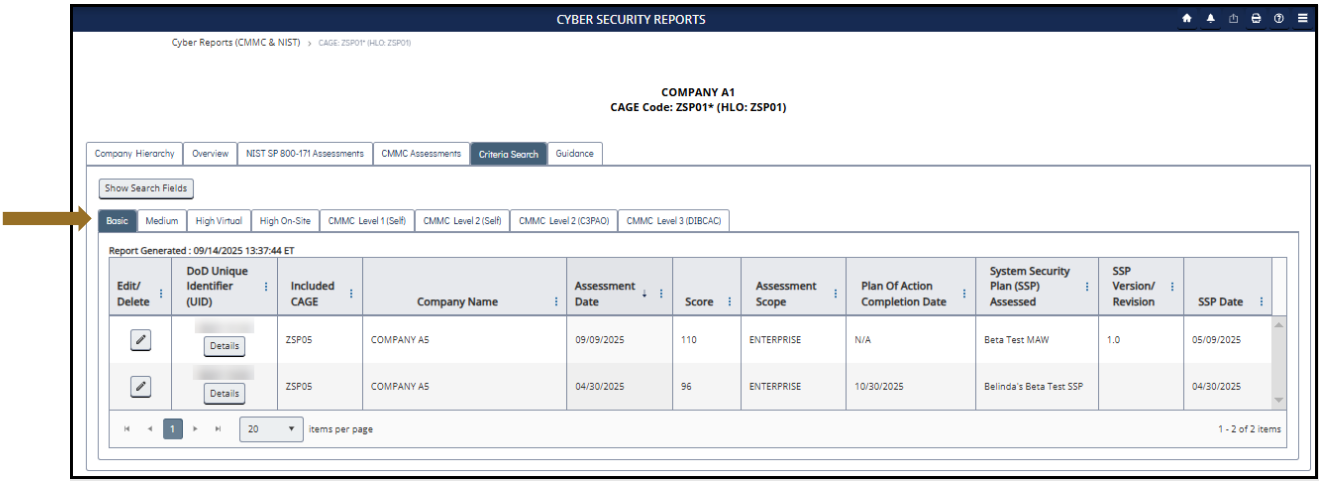


Figure 80: Cyber Reports Criteria Search Results

Select the **Show Search Fields** button to open the search fields to review the searched criteria or create a new search. Select the **Hide Search Fields** button to collapse the search fields to conserve space.

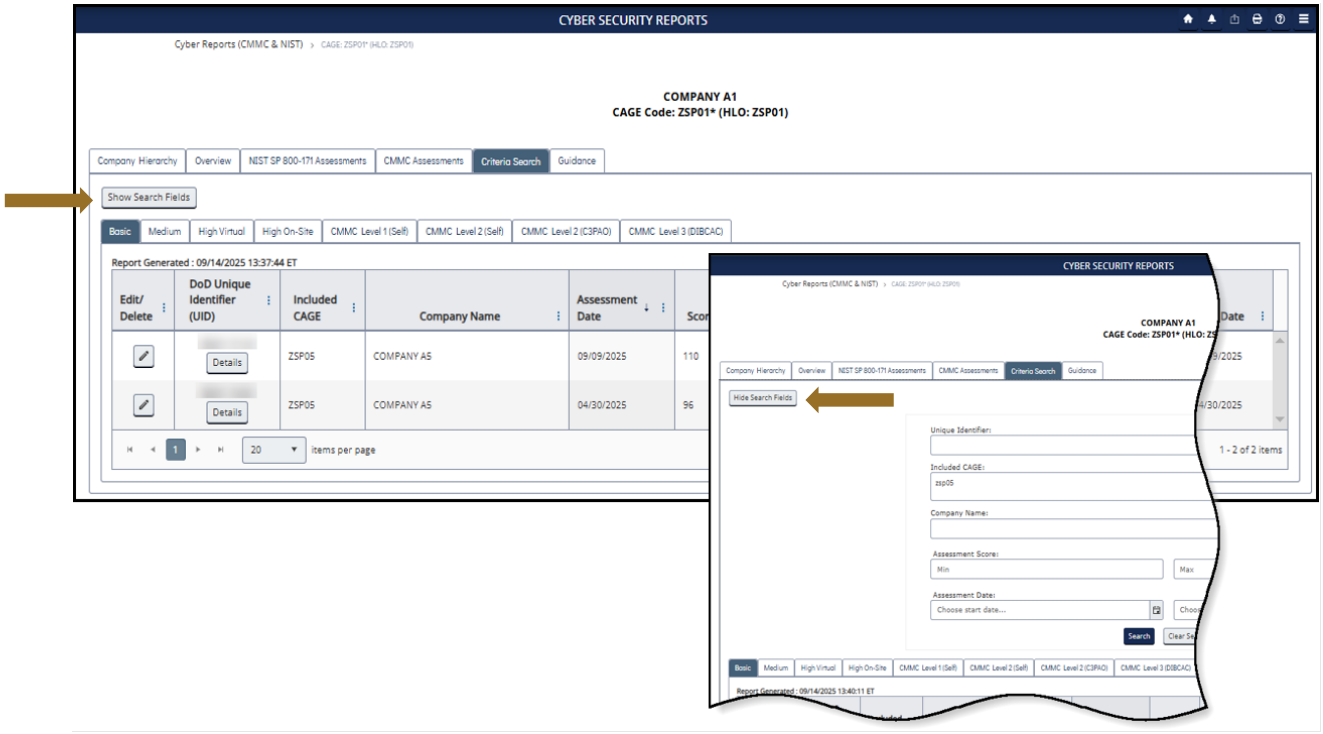


Figure 81: Cyber Reports Criteria Search Report – Show/Hide Search Fields

Users with the Contractor Vendor (Support Role) can only view details for the CAGE authorized in PIEE and any CAGE(s) below (subsidiaries). Users will have view-only access to any CMMC C3PAO and DIBCAC-prepared assessment that includes their authorized CAGE in the assessed scope. To review the hierarchy, select the Company Hierarchy tab. (See Sec. 5.1.2)

5.1.7 The Guidance Tab

Select the **Guidance** tab to review General Guidance, CMMC, and NIST SP 800-171 information organized by sections. Links throughout provide access to additional guidance, policy help desk emails, regulations, CMMC security requirements, and the NIST SP 800-171 Assessment Methodology.

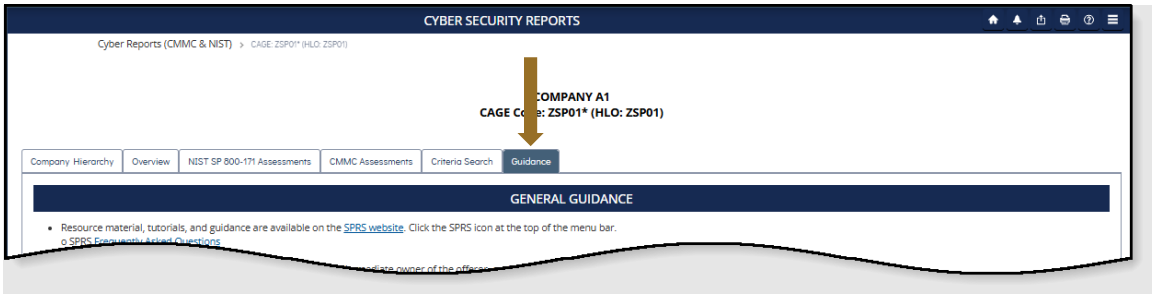


Figure 82: Cyber Reports Guidance Tab

5.2 CAGE HIERARCHY

The CAGE Hierarchy report identifies the CAGE(s) specified in the user's PIEE profile (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.

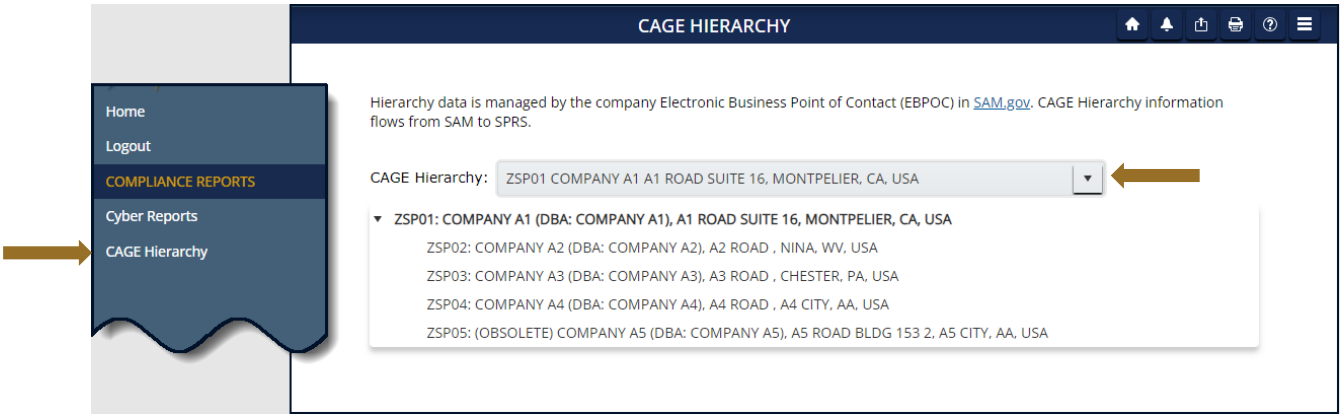


Figure 83: CAGE Hierarchy

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 immediate level owner and highest level owner (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.

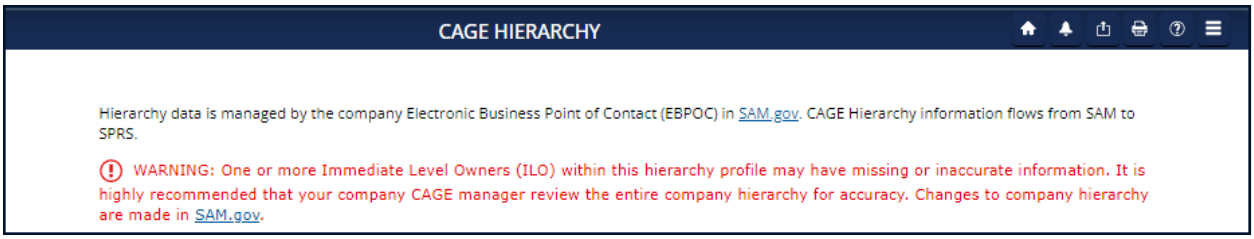


Figure 84: Error in CAGE Hierarchy

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.
- Select **Run Supplier Risk Report** button.

Figure 85: Supplier Risk Report Request

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

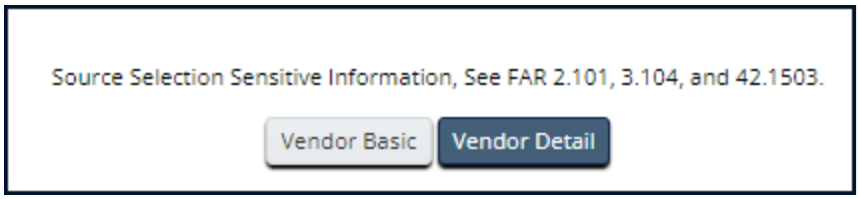


Figure 86: Toggle Vendor Basic/Vendor Detail Supplier Risk

- **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***.

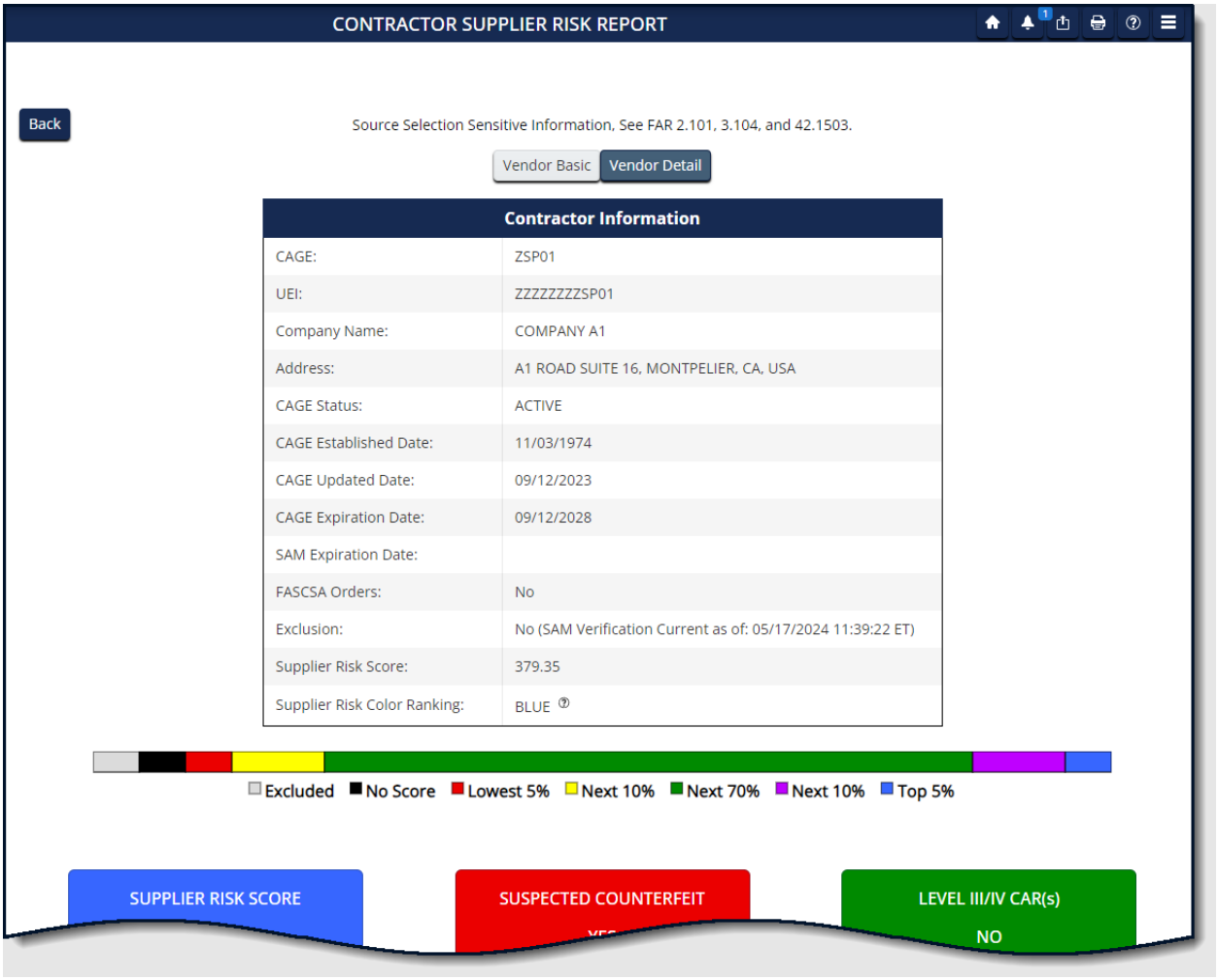


Figure 87: Supplier Risk Report

Supplier Color: The SPRS Color Legend represents the percentage breakdown of a normal statistical distribution, commonly referred to as a bell curve. Color assignments are 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 has 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.

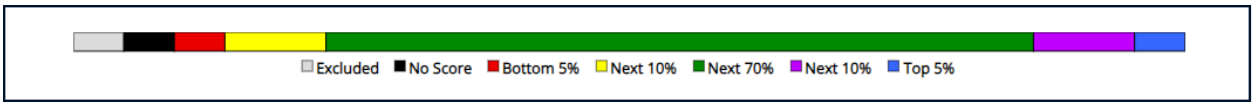


Figure 88: SPRS Color Legend

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

Figure 89: 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.

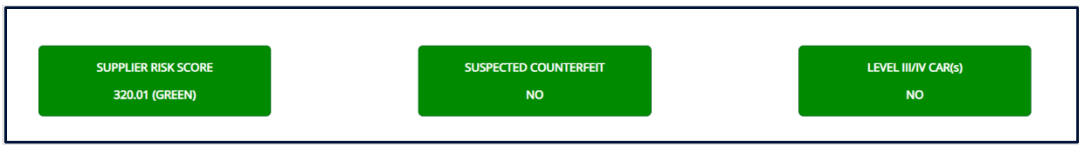


Figure 90: Supplier Risk Color Tiles

- 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 91: 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.

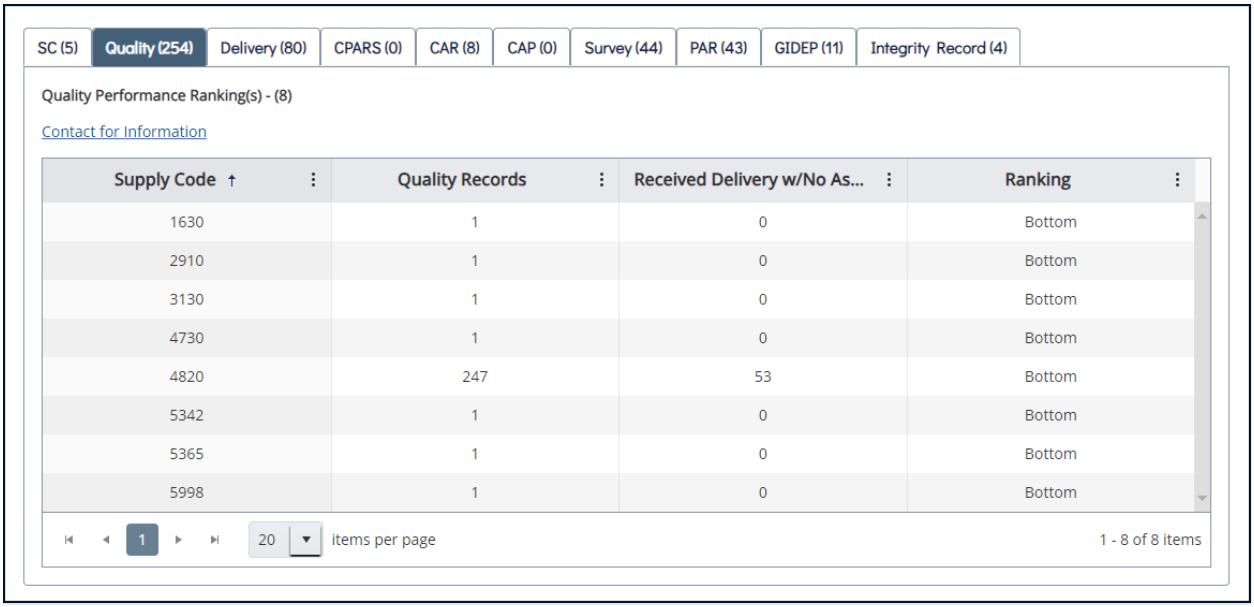


Figure 92: Quality Detail in Supplier Risk Tab

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.

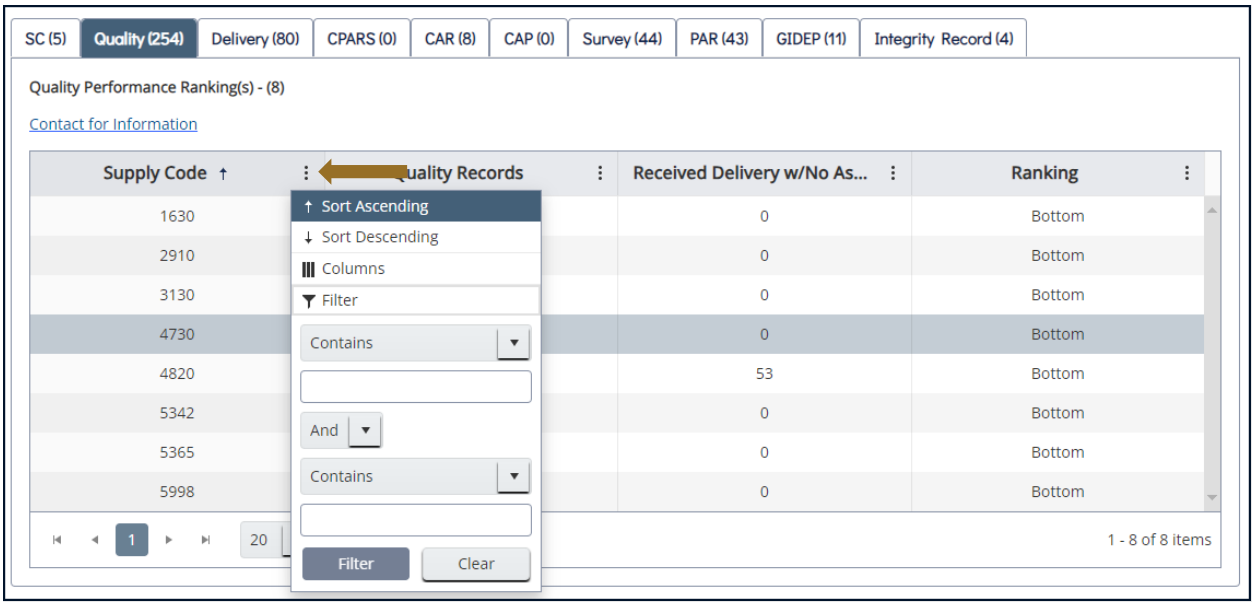


Figure 93: Supplier Risk Sort/Filter

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 Objective Quality Evidence (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.

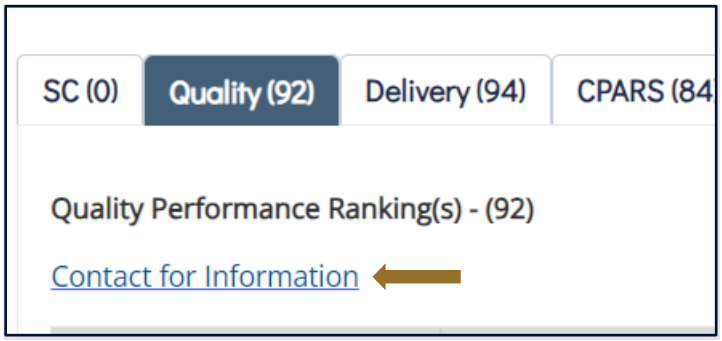


Figure 94: Supplier Risk Contact for Information Link

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

Select **Ok** button to close pop-up window.

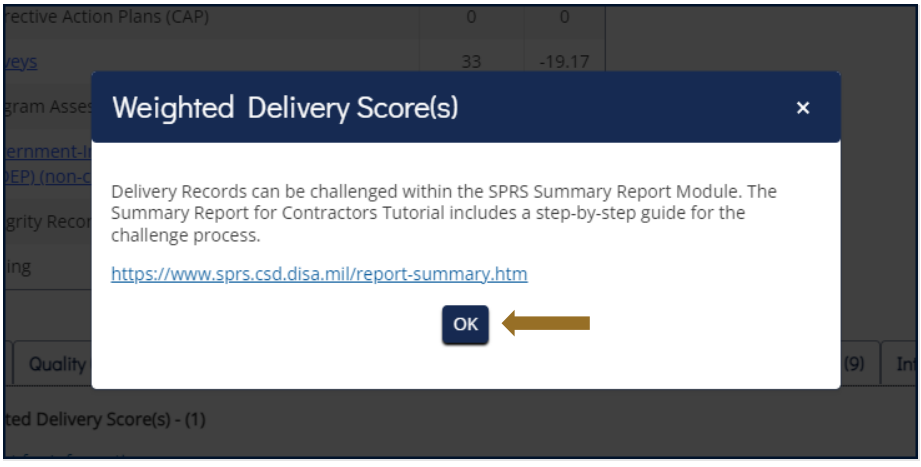


Figure 95: Supplier Risk Contact for Information Pop-Up

- **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.
  - **Cybersecurity Maturity Model Certification:** "YES" indicates

there is an affirmed CMMC Assessment, for any level, logged in SPRS. "NO" indicates there are no affirmed CMMC assessments present for the CAGE, or all assessments are considered expired or retracted.

- **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, or all assessments are considered expired.

- **Section 889 FAR 52.204-26 Representation:** SPRS utilizes the Reps & 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
Cybersecurity Maturity Model Certification (CMMC) Assessment	NO
National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 Assessment	YES
Section 889 FAR 52.204-26 (c) (1) Representation	YES
Section 889 FAR 52.204-26 (c) (2) Representation	YES

Figure 96: Supplier Risk 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. Challenge instructions are available in Appendix D.

To access Summary Report:

Select **Summary Report** from the Menu.

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

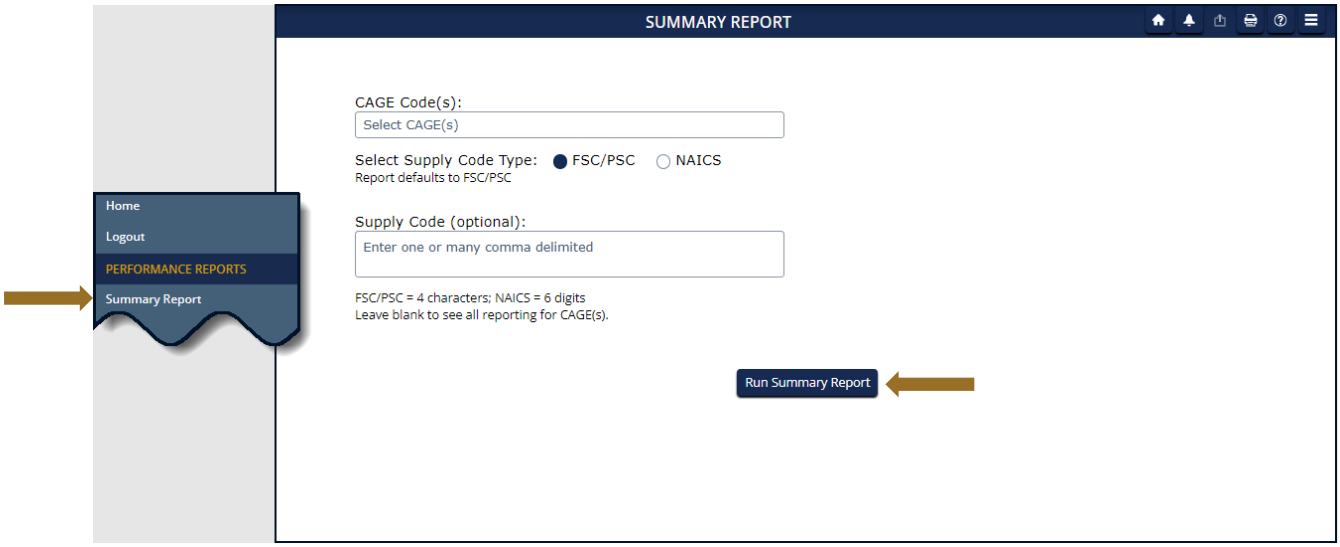


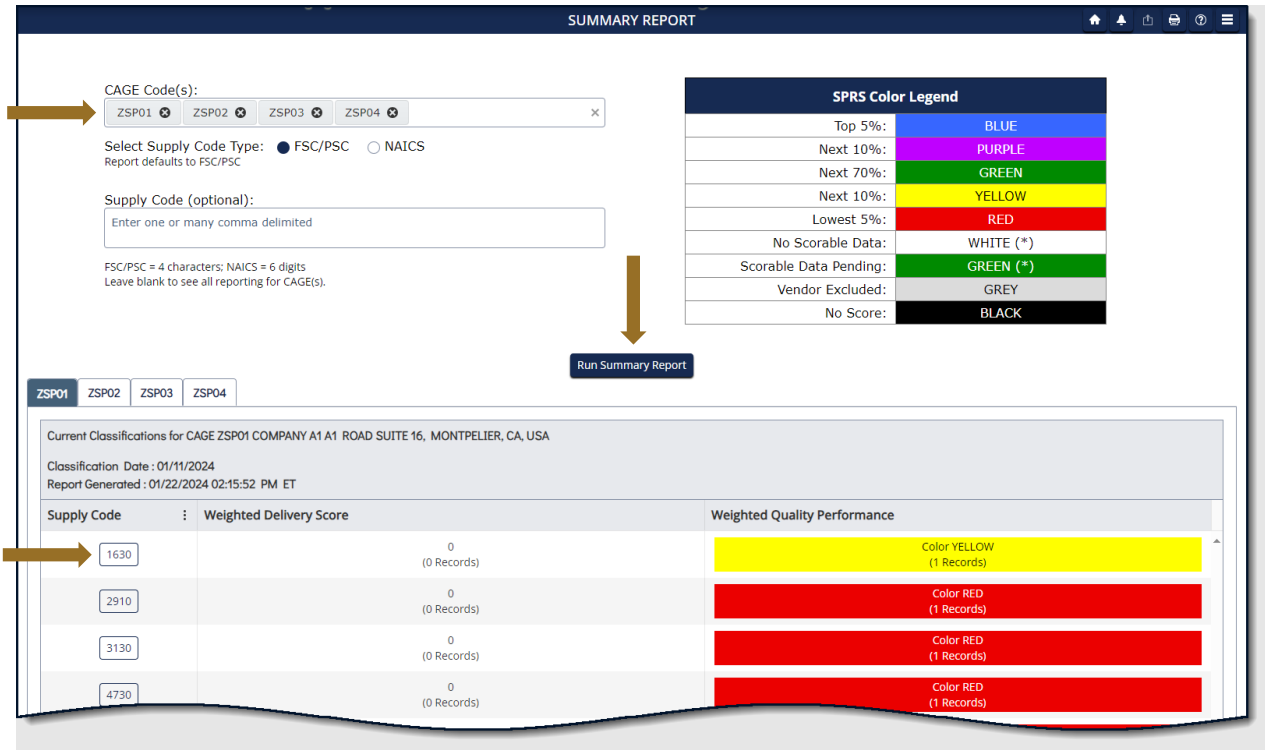
Figure 97: Contractor Summary Report Request

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



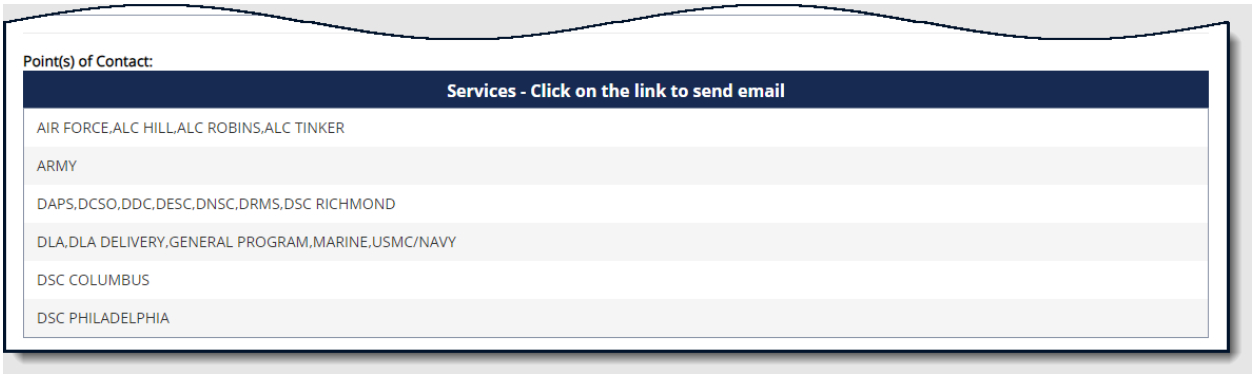


Figure 98: Summary Report

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.

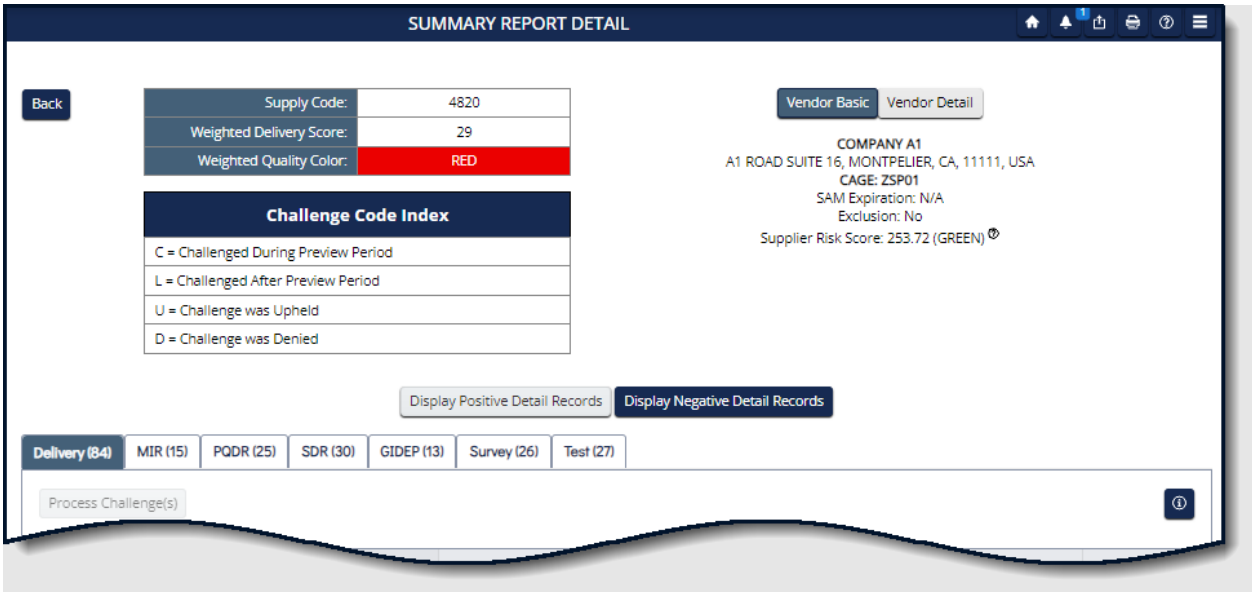


Figure 99: Summary Report Detail

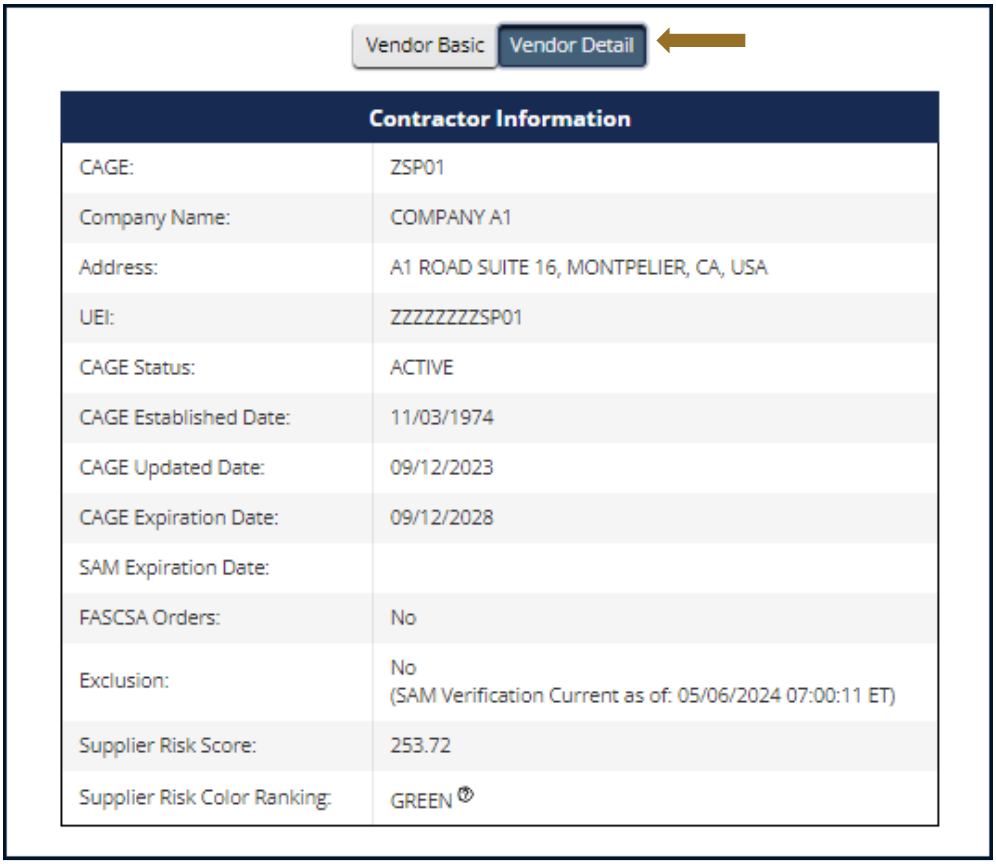


Figure 100: Summary Report Detail

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)

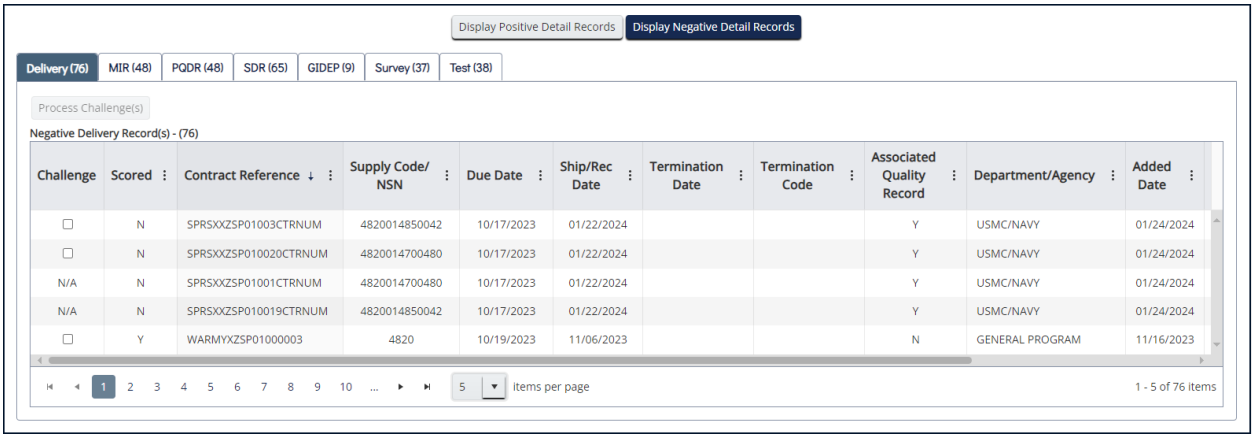


Figure 101: Summary Report Negative Detail

Positive Record Types:

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

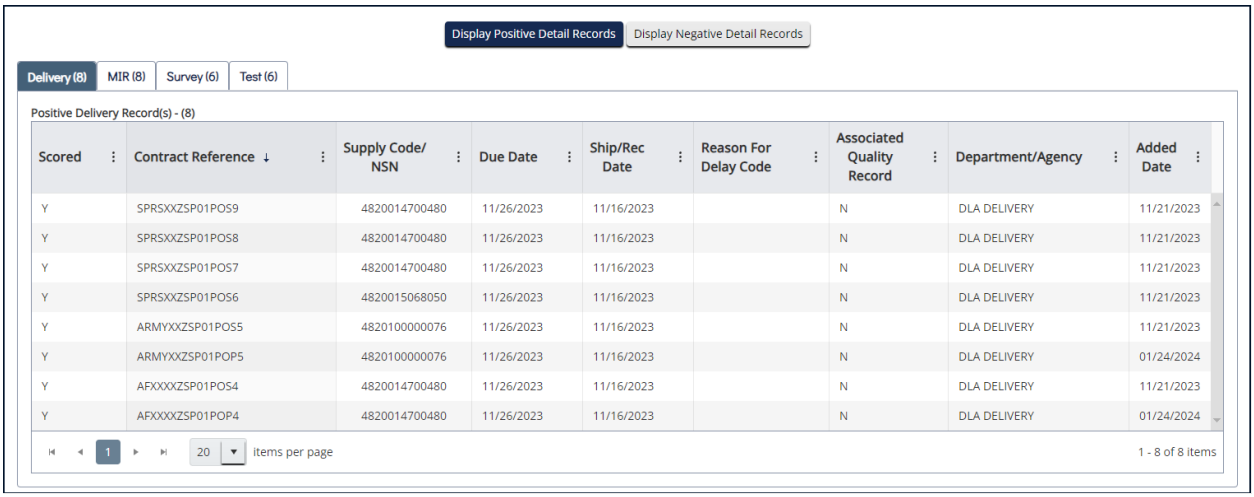


Figure 102: Summary Report Positive Detail

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.*

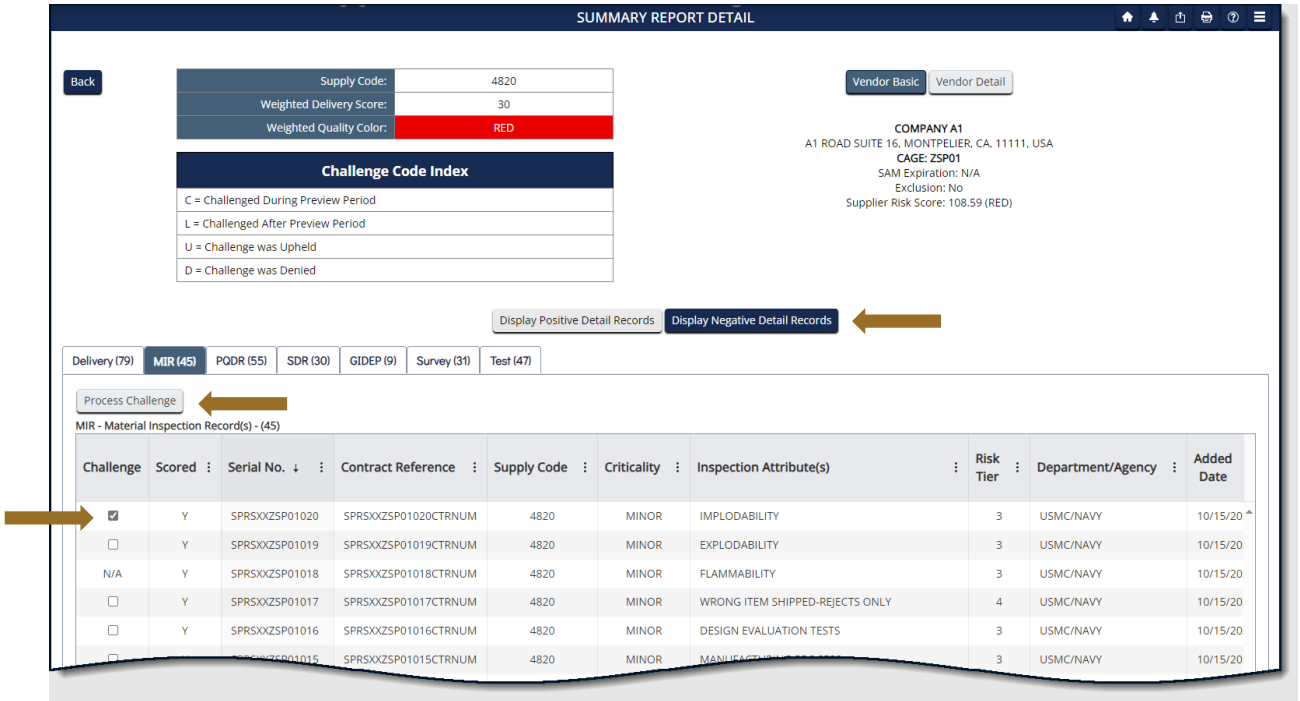


Figure 103: Contractor Detailed Report

After selecting one or many records, select the **Process Challenge** button to open the dated Challenge Submission pop-up with the destination email address, selected record(s), and record details. The 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

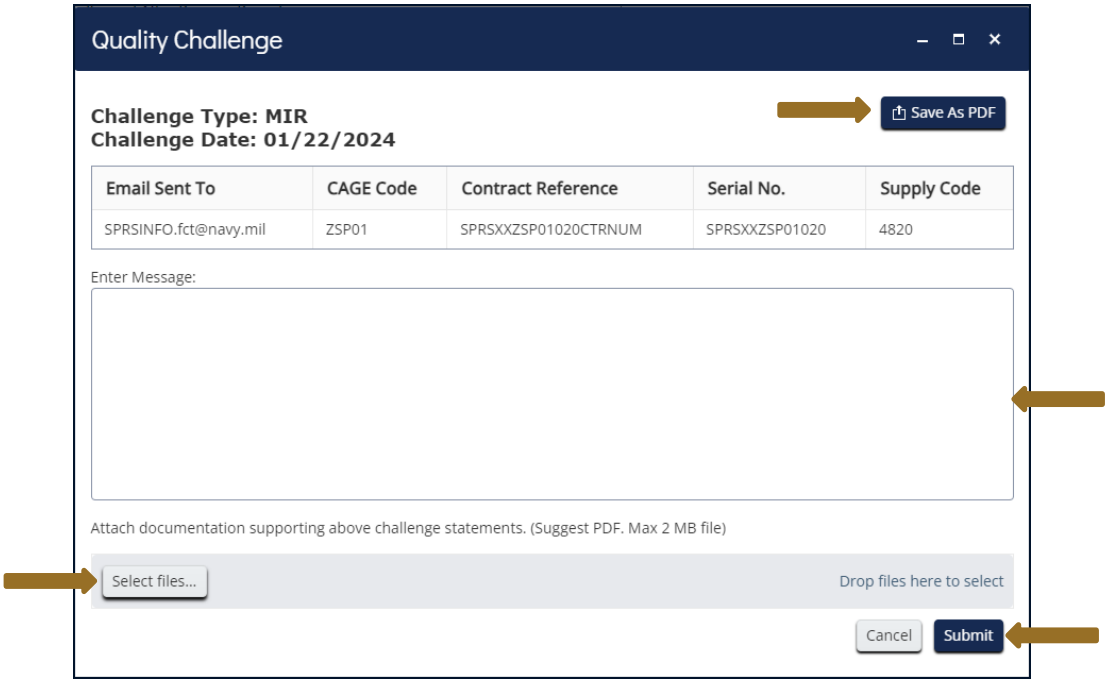


Figure 104: Challenge Record Email

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
- Select **Display Positive Detail Records** or **Display Negative Detail Records** button
- 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

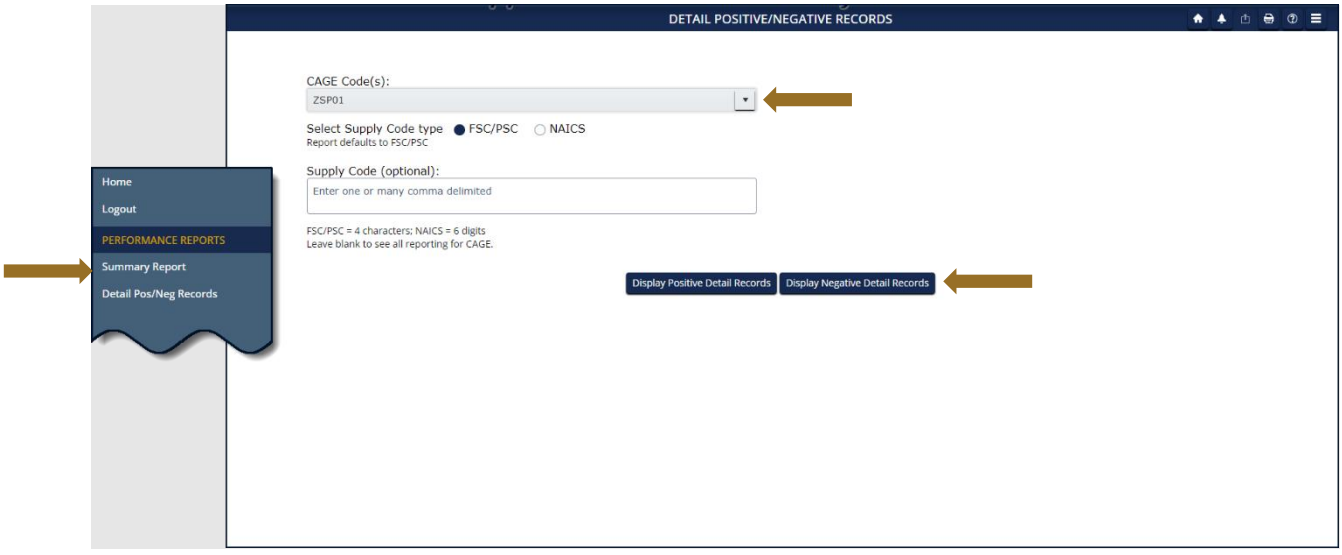


Figure 105: Detail Pos/Neg Records Report Request

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)

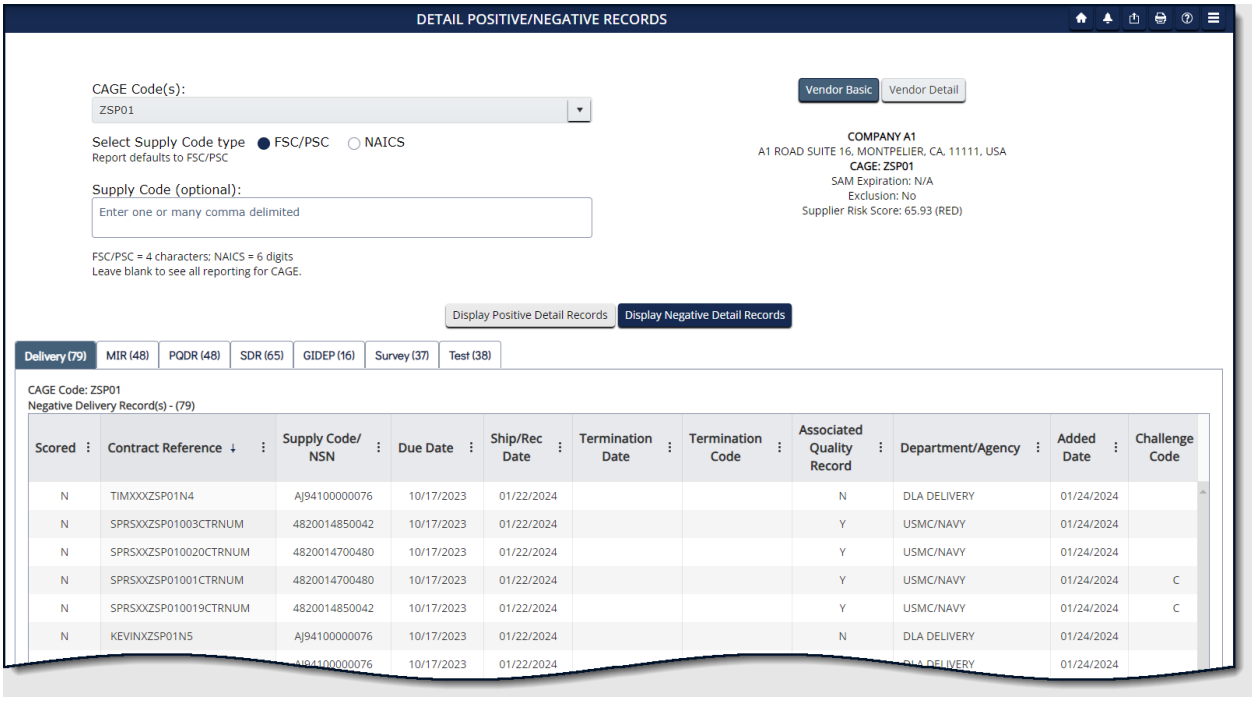


Figure 106: Detail Negative Recordshi

Positive Record Types:

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

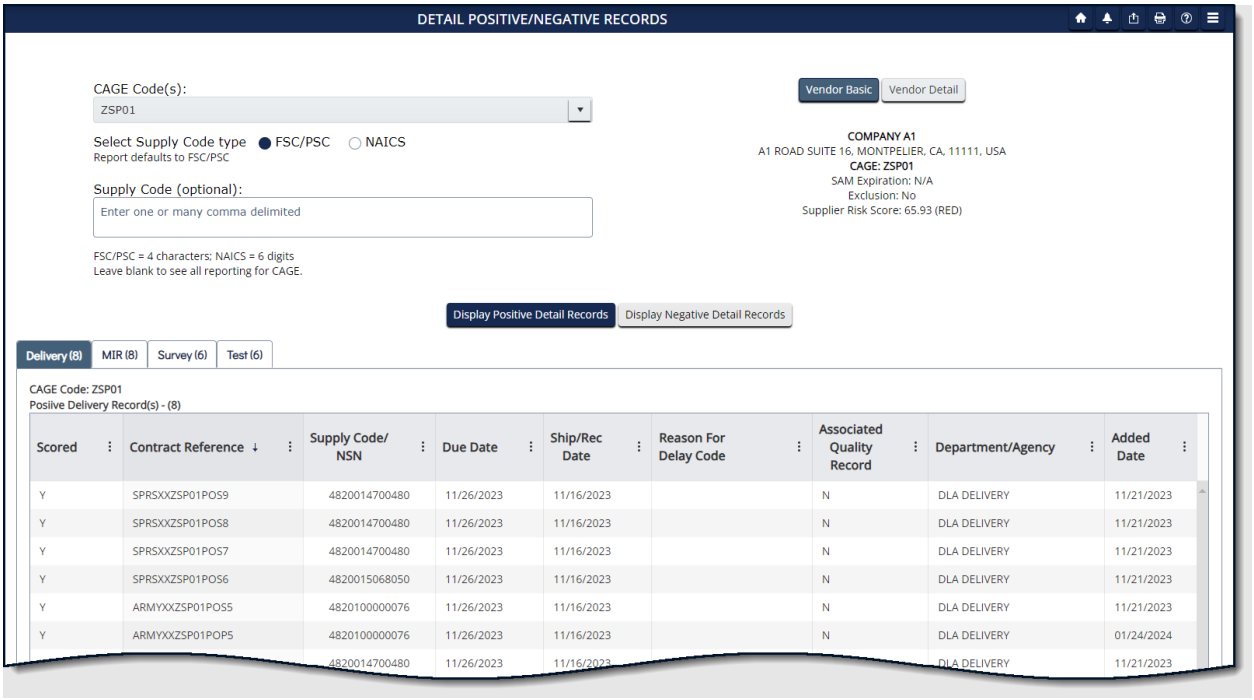


Figure 107: Detail Report Positive Records

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 PSC Tool, https://psctool.us/home, maintained by the Defense Pricing, Contracting, and Acquisition Policy (DPCAP) 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 Supply Code List
- Click **Search**

  Or
- Click Show All

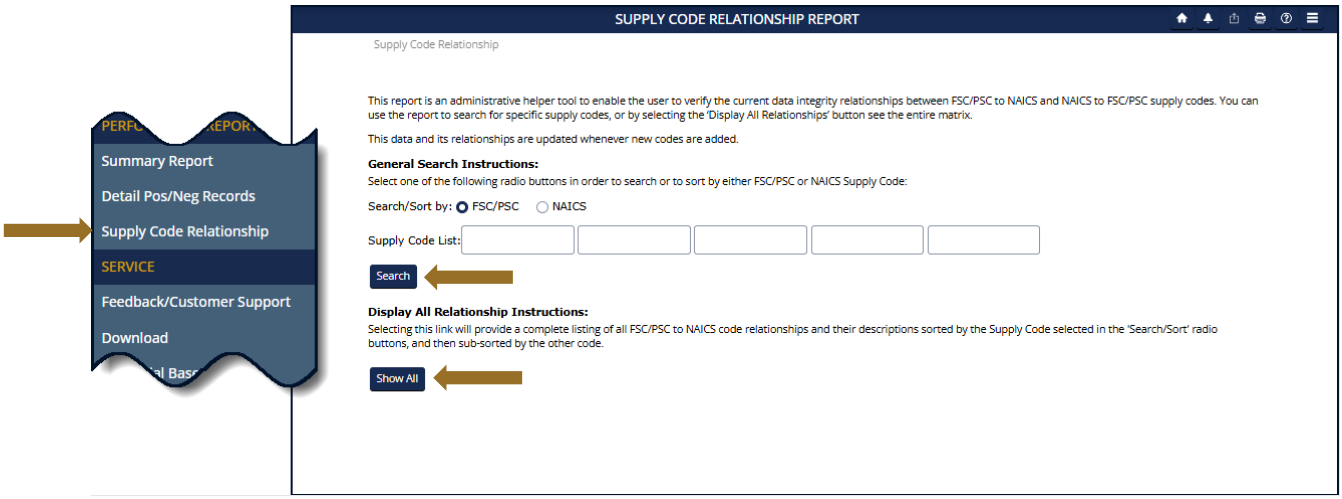


Figure 108: Supply Code Relationship Request

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.

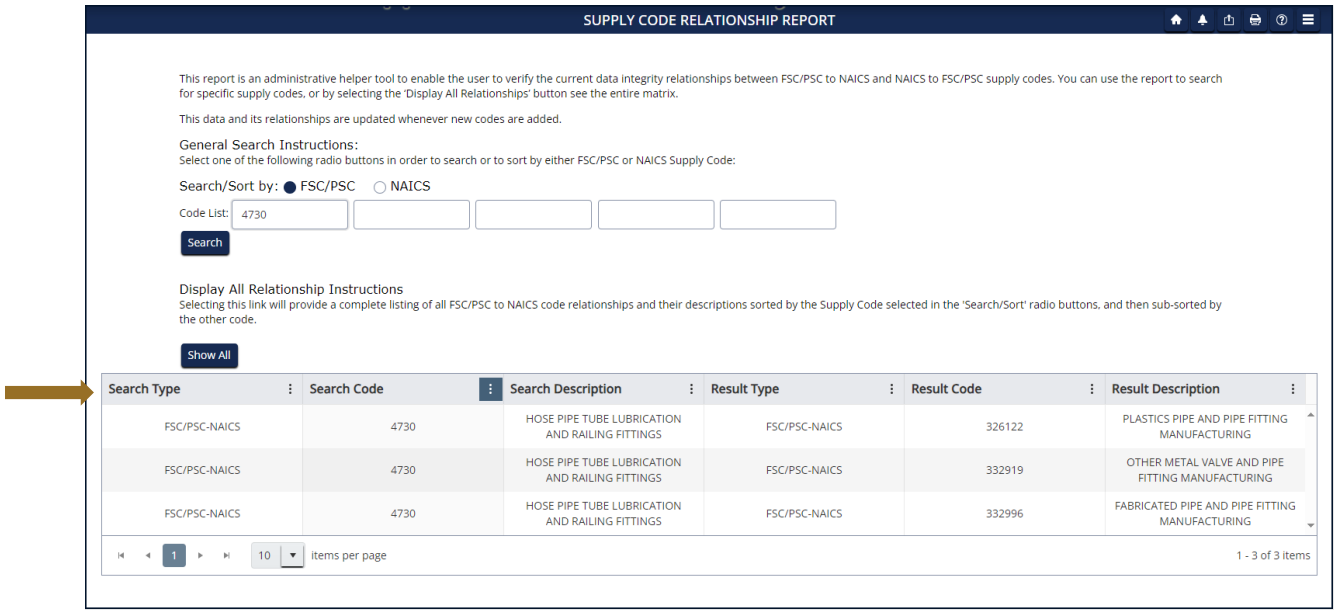


Figure 109: FSC/PSC to NAICS example

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

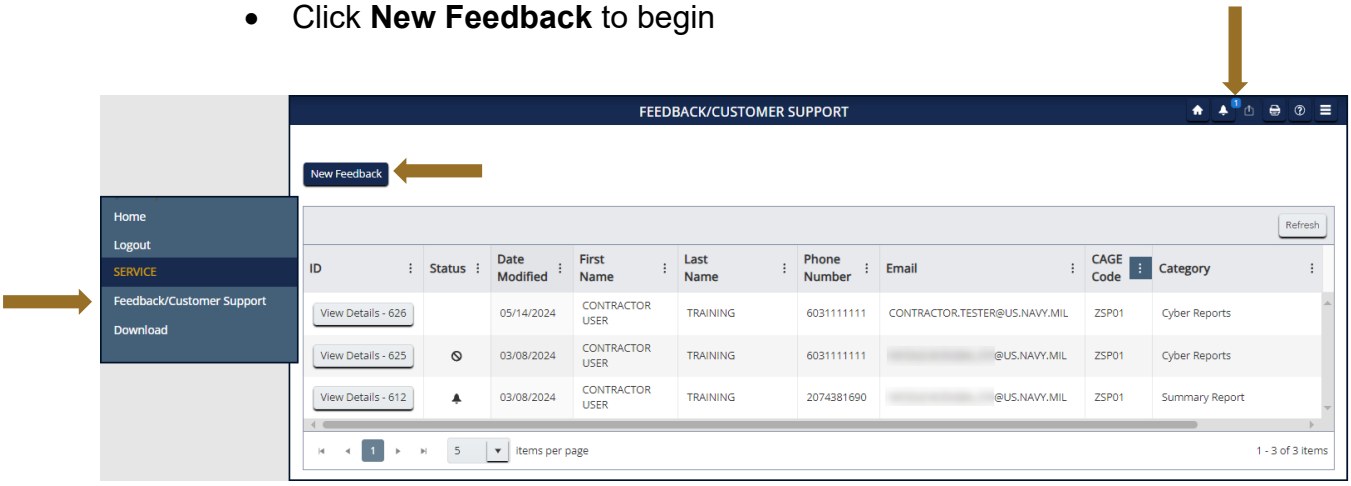


Figure 110: Feedback/Customer Support Window

- 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

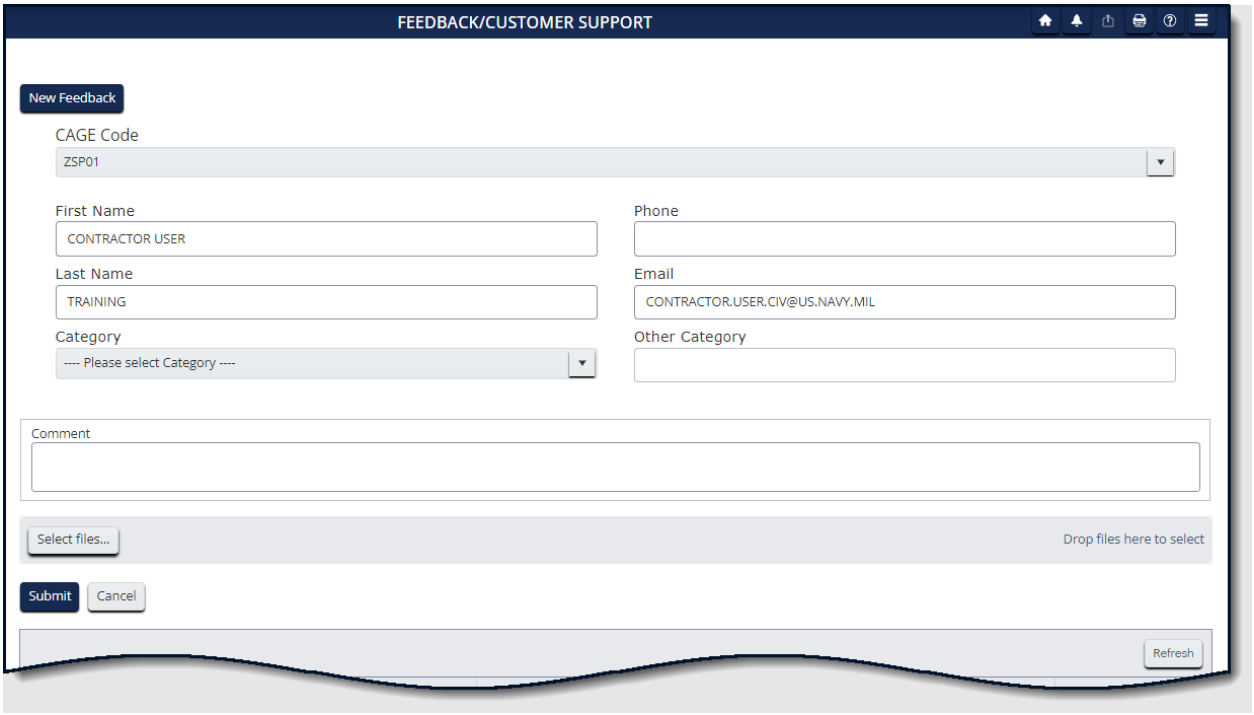


Figure 111: Feedback/Customer Support Window

- 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.
- Select the **View Details** button to view response(s) or add comments.

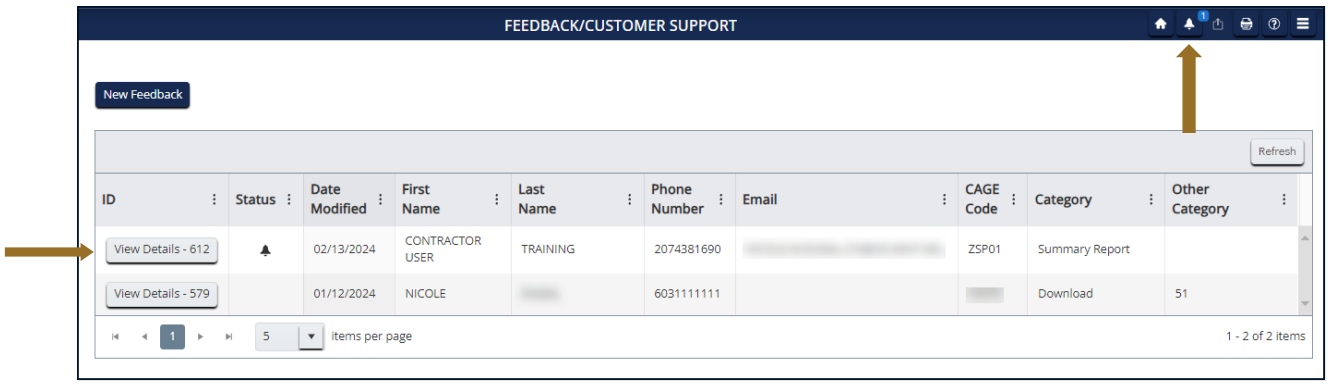


Figure 112: Feedback/Customer Support Submitted

- 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.

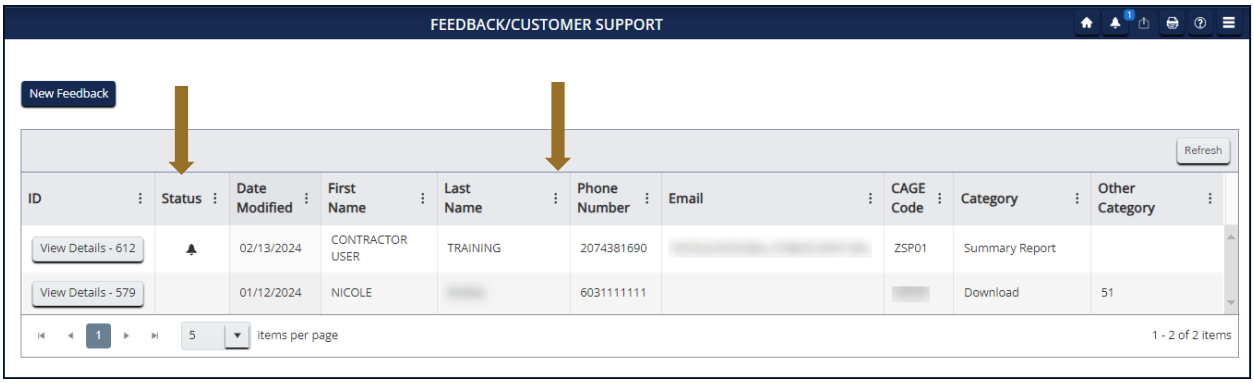


Figure 113: Feedback/Customer Support Status

8.2 DOWNLOAD

The Download module serves as a repository for file exports requested by the user throughout the application. Users monitor export requests and download files from this module.

When a SPRS module offers a report export, select the **Export** button in the Toolbar within that module.

Figure 114: Export Button

Export files are available for a period of five (5) days from the date they become available for download. After that they are removed and must be requested again through the report module.

SPRS sends an email notification to the email associated with the user's PIEE account indicating that a requested file is ready for download. The email is not required and may end up in the user's Spam or Junk folder. Users can see when the file is ready for download within the Download module.

To access Download:

Select **Download** from the Menu.

The table displayed contains the following information:

- **Requested Date** – the day and time the user requested the file
- **Export Module** – the report module where the file was requested
- **Export Criteria** – the values selected by the user and applied to the report
- **Filename** – system generated file name: module_CAGE_date/time_id
- **Download Status** – either In Queue or Ready to Download
- **Downloaded Date** – date and time the file was last retrieved by the user
- **Refresh** – allows the user to receive the latest download status without leaving the page

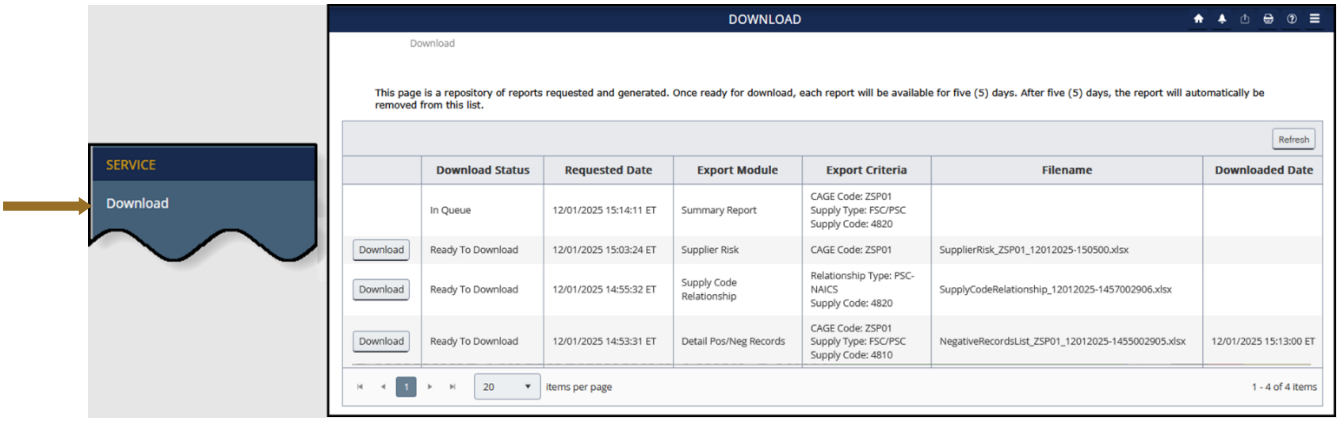


Figure 115: Download Module

When files are available to download the Download button will appear in the first column and the filename will appear in the Filename column.

Select the **Download** button.

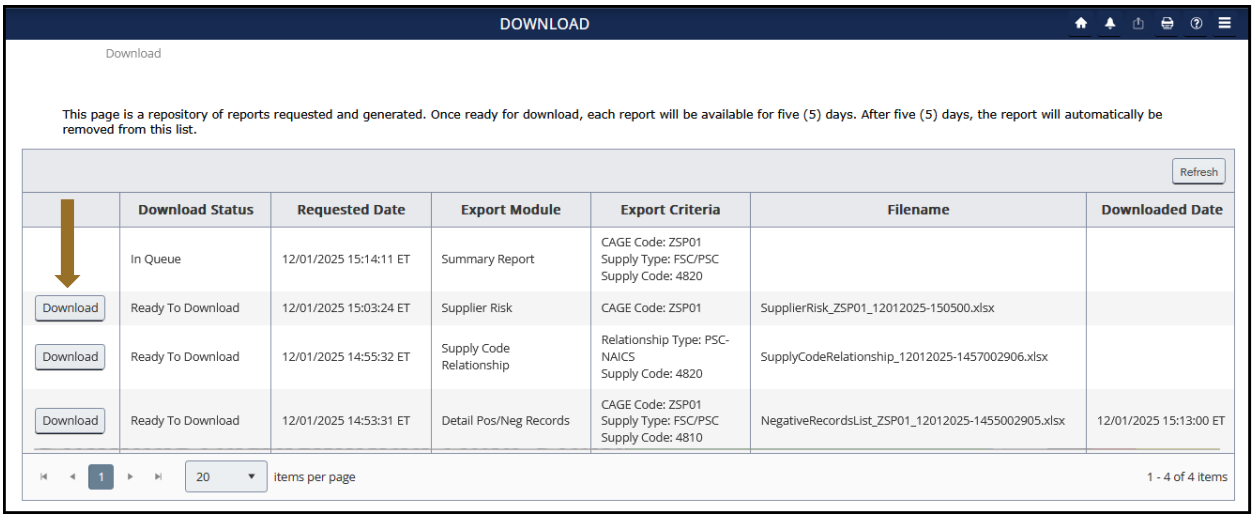


Figure 116: Download Button

The file will be downloaded to the user and the Downloaded Date column will populate. Previously downloaded files may be downloaded again. Reports remain available for five (5) days and then they are automatically deleted from the Download repository.

9. TRAINING MATERIALS

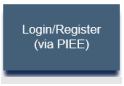
The SPRS web page provides a variety of public resources accessible by selecting from the pop-out menu and buttons.

To access the SPRS web page:

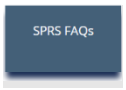
Select the  icon from the Menu in the SPRS application, or ***https://www.sprs.csd.disa.mil/***.

Figure 117: SPRS Web Landing Page

Navigation:



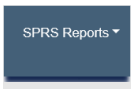
- Login/Register (via PIEE) button for redirection to the Procurement Integrated Enterprise Environment (PIEE)



- 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

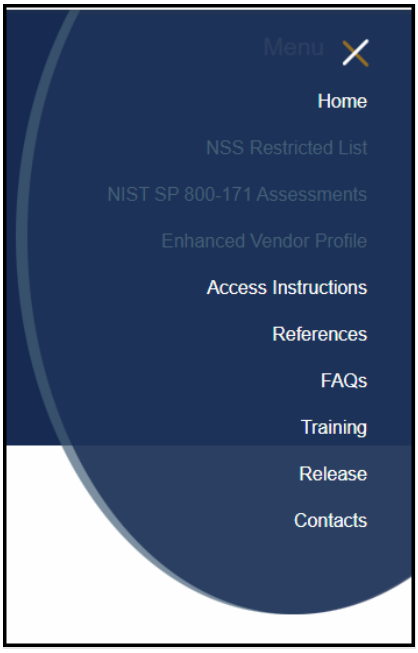
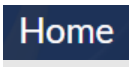


Figure 118: SPRS Pop-Out Menu



- Return to the SPRS web-landing page

- Restricted Government-only

- Restricted Government-only

Enhanced Vendor Profile - Restricted Government-only

Access Instructions - Access Instructions for Government and Supplier/Vendor

Reference - 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

10. 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	https://www.justice.gov/oip/foia-resources
SPRS Evaluation Criteria	https://www.sprs.csd.disa.mil/pdf/SPRS_DataEvaluationCriteria.pdf
SPRS CMMC Quick Entry Guide Level 1	https://www.sprs.csd.disa.mil/pdf/CMMCQuickEntryGuide.pdf
SPRS CMMC Quick Entry Guide Level 2	https://www.sprs.csd.disa.mil/pdf/CMMCL2SelfQuickEntryGuide.pdf
SPRS NIST Quick Entry Guide	https://www.sprs.csd.disa.mil/pdf/NISTSP800-171QuickEntryGuide.pdf
DFARS 204.7603	https://www.acquisition.gov/dfars/204.7603-procedures
DoDI 5000.79	https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500079p.PDF?ver=2019-10-15-115609-957

11. GLOSSARY

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

ACRONYM/ ABBREVIATION	DEFINITION
AO	Affirming Official
C3PAO	CMMC Third-Party Assessor Organization
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
DIBCAC	Defense Industrial Base Cybersecurity Assessment Center
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

ACRONYM/ ABBREVIATION	DEFINITION
SAM	System for Award Management
SPRS	Supplier Performance Risk System
UEI	Unique Entity Identifier
UID	Unique Identifier
WAWF	Wide Area Workflow

APPENDIX A: 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 Add/Edit/View company Industrial Base Surveys
SPRS Cyber Vendor User Access	Add/Affirm/Edit/View company CMMC and NIST SP 800-171 assessment results View CAGE Hierarchy Provide customer feedback Add/Edit/View company Industrial Base Surveys

PIEE activity:

- 45 days without accessing, users receive an email reminder
- 60 days without accessing, the account will become inactive
    - Contact the Company Account Administrator (CAM) or PIEE Helpdesk
- 90 days without accessing, the account will be archived
    - Contact the PIEE Helpdesk, **disa.global.servicedesk.mbx.eb-ticket-requests@mail.mil**

APPENDIX B: 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 ***sprs-helpdesk@us.navy.mil*** 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 sprs-helpdesk@us.navy.mil
SPRS is unavailable	SPRS may be running a batch job which typically run between 2300 and 0200 GMT	If outside batch job timeframe, email sprs-helpdesk@us.navy.mil
* 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*** for assistance.

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

APPENDIX C: 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
Industrial Base Surveys	Allows suppliers of components and equipment on naval vessels to provide voluntary company information

APPENDIX D: 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 and providing objective quality evidence (OQE).

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*

APPENDIX E: CMMC STATUS TYPES & DESCRIPTIONS

CMMC Level 1 (Self)

Incomplete	Partial details saved. No CMMC UID created. Not visible to authorized government users.
Pending Affirmation	Record details completed but not affirmed. No CMMC UID created. Not visible to authorized government users.
Final Level 1 Self-Assessment	Current for 1 year from Assessment Date. "Yes" selected for question "Are you compliant with each of the security requirements specified in FAR clause 52.204-21?". CMMC UID expires after 1 year period. Visible to authorized government users.
No CMMC Status	Not Current. "No" selected for question "Are you compliant with each of the security requirements specified in FAR clause 52.204-21?". CMMC UID expired. Visible to authorized government users.
No CMMC Status (Expired)	Not Current. Past Assessment Expiration Date. CMMC UID expired. Visible to authorized government users.

CMMC Level 2 (Self)

Incomplete	Partial details saved. No CMMC UID created. Not visible to authorized government users.
Pending Affirmation	Record details completed but not affirmed. No CMMC UID created. Not visible to authorized government users.
CMMC L2 Conditional Self-Assessment	Current for 180 days from Assessment Date. Met minimum requirements with score < 110. Can be updated within 180 day period. Visible to authorized government users.
CMMC L2 Conditional Self-Assessment (Retracted by Vendor)	Not Current. Assessment deleted by Vendor. CMMC UID expired. Visible to authorized government users.

CMMC Level 2 (Self) Cont'd

Pending Affirmation	Current until Affirmation Expiration Date. Conditional assessment updated but not affirmed. Can be updated within 180 day period. Visible to authorized government users.
CMMC L2 Final Self-Assessment	Current until Affirmation Expiration Date. Annual affirmation required. Can be updated until CMMC Status Expiration Date. Visible to authorized government users.
CMMC L2 Final Self-Assessment (Expired Affirmation)	Not Current. Affirmation required. Can be updated until CMMC Status Expiration Date. Visible to authorized government users.
CMMC L2 Final Self-Assessment (Retracted by Vendor)	Not Current. Assessment deleted by Vendor. CMMC UID expired. Visible to authorized government users.
No CMMC Status	Not Current. Past Assessment Expiration Date. CMMC UID expired. Visible to authorized government users.

CMMC Level 2 (C3PAO)

Pending Affirmation	Record details received but not affirmed. CMMC UID assigned. If never affirmed, not visible to authorized government users. If previously affirmed, visible.
Conditional Level 2 (C3PAO)	Current for 180 days from Assessment Date. Met minimum requirements with score < 110. Can be updated within 180 day period. Visible to authorized government users.
Conditional Level 2 (C3PAO) (Deleted by eMASS)	Not Current. CMMC UID expired. Visible to authorized government users.
Final Level 2 (C3PAO)	Current until Affirmation Expiration Date. Annual affirmation required. Can be updated until CMMC Status Expiration Date. Visible to authorized government users.

CMMC Level 2 (C3PAO) Cont'd

Final Level 2 (C3PAO) (Expired Affirmation)	Not Current. Affirmation required. Can be updated until CMMC Status Expiration Date. Visible to authorized government users.
Final Level 2 (C3PAO) (Deleted by eMASS)	Not Current. CMMC UID expired. Visible to authorized government users.
No CMMC Status (Expired)	Not Current. Past Assessment Expiration Date. CMMC UID expired. Visible to authorized government users.

CMMC Level 3 (DIBCAC)

Pending Affirmation	Record details received but not affirmed. CMMC UID assigned. If never affirmed, not visible to authorized government users. If previously affirmed, visible.
Conditional Level 3 (DIBCAC)	Current for 180 days from Assessment Date. Met minimum requirements with score < 110. Can be updated within 180 day period. Visible to authorized government users.
Conditional Level 3 (DIBCAC) (Deleted by eMASS)	Not Current. CMMC UID expired. Visible to authorized government users.
Final Level 3 (DIBCAC)	Current until Affirmation Expiration Date. Annual affirmation required. Can be updated until CMMC Status Expiration Date. Visible to authorized government users.
Final Level 3 (DIBCAC) (Expired Affirmation)	Not Current. Affirmation required. Can be updated until CMMC Status Expiration Date. Visible to authorized government users.
Final Level 3 (DIBCAC) (Deleted by eMASS)	Not Current. CMMC UID expired. Visible to authorized government users.
No CMMC Status (Expired)	Not Current. Past Assessment Expiration Date. CMMC UID expired. Visible to authorized government users.

This page intentionally left blank.