Overview of Cybersecurity Assessments in SPRS

SPRS

Supplier Performance Risk System

Disclaimer:

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

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

What is SPRS?

Supplier Performance Risk System

- *"… the authoritative source to retrieve supplier and product PI [performance information]" (DoDI 5000.79)*

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

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

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

What is SPRS?

Supplier Performance Risk System

- *"… the authoritative source to retrieve supplier and product PI [performance information]" (DoDI 5000.79)*

- *Vendor Performance*
  - *Quality Classifications & On-time Delivery scores by FSC/PSC/NAICS*
  - *Supplier Risk – Ranked risk of vendor performance – 79K+ CAGEs*
  - *Price Risk – Average Price, Expected Range, over/underprice alerts – 1.6M+ items*
  - *Item Risk – Suspected Counterfeit, CSI/CAI, DMSMS, etc. – 135K+ items*
- *Vendor Compliance*
  - *Debarments/exclusions, § 889, FASCA, representations/certifications (from SAM)*
  - ***Cyber Security Assessments: NIST SP 800-171, CMMC***
  - *NSS Restricted List (formerly § 806 "Do Not Buy List")*
  - *Vendor Threat Mitigation (§ 841 NCWtE)*
- *Supply Chain Illumination, contract history & analysis, corporate CAGE hierarchies*

Path to CS Self-Assessments in SPRS

Create
System Security Plan (SSP)

NIST SP 800-171 Basic Assessment?
Use DoD Assessment Methodology
https://www.acq.osd.mil/dpap/pdi/cyber/docs/NIST%20SP%20800-171%20Assessment%20Methodology%20Version%201.2.1%20%206.24.2020.pdf

SAM – create
User account

SAM – register
Entities

SAM – receive
UEIs

SAM - establish
EB POC

CAGE.mil – validate
Company data

SAM – establish
CAGE hierarchy

PIEE – establish
Vendor group

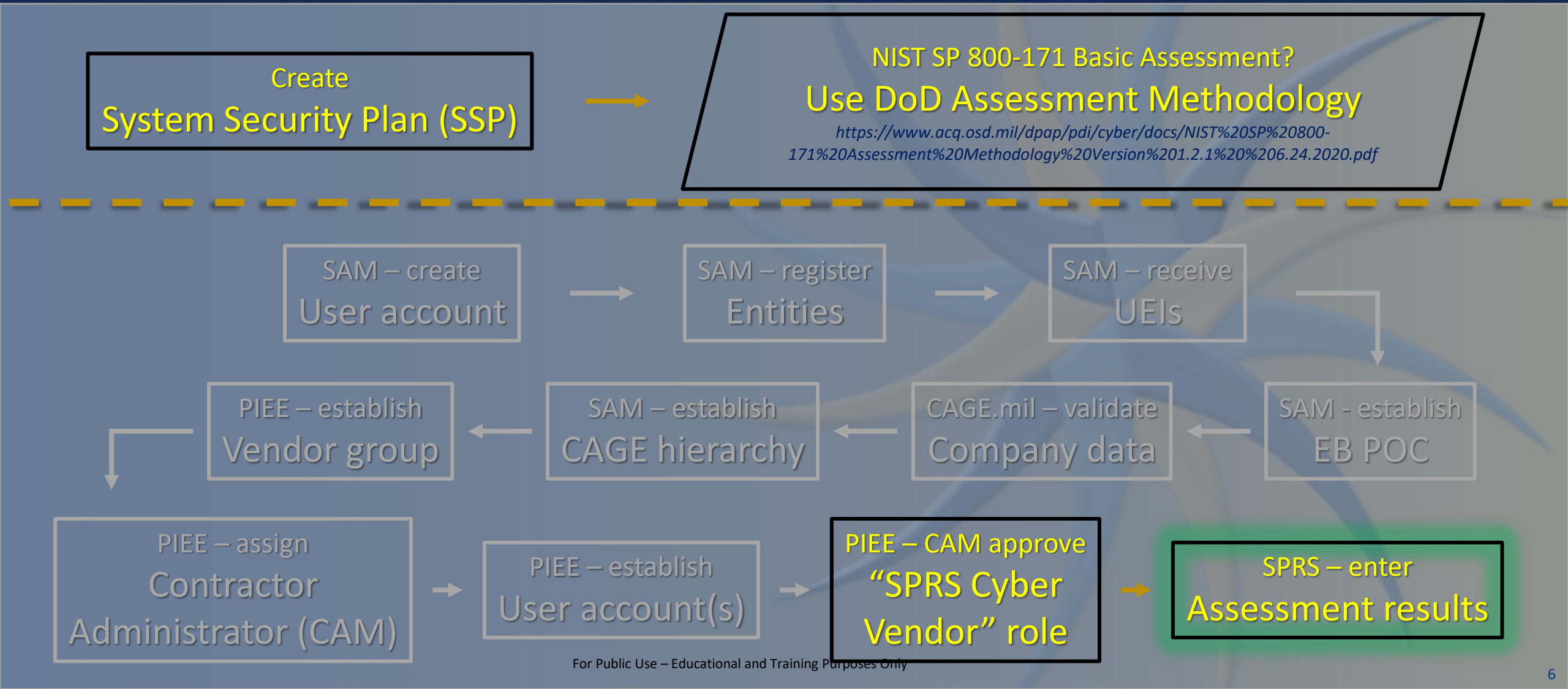
PIEE – assign
Contractor Administrator (CAM)

PIEE – establish
User account(s)

PIEE – CAM approve
"SPRS Cyber Vendor" role

SPRS – enter
Assessment results

Already using WAWF? You're in PIEE!



NIST SP 800-171 Assessments

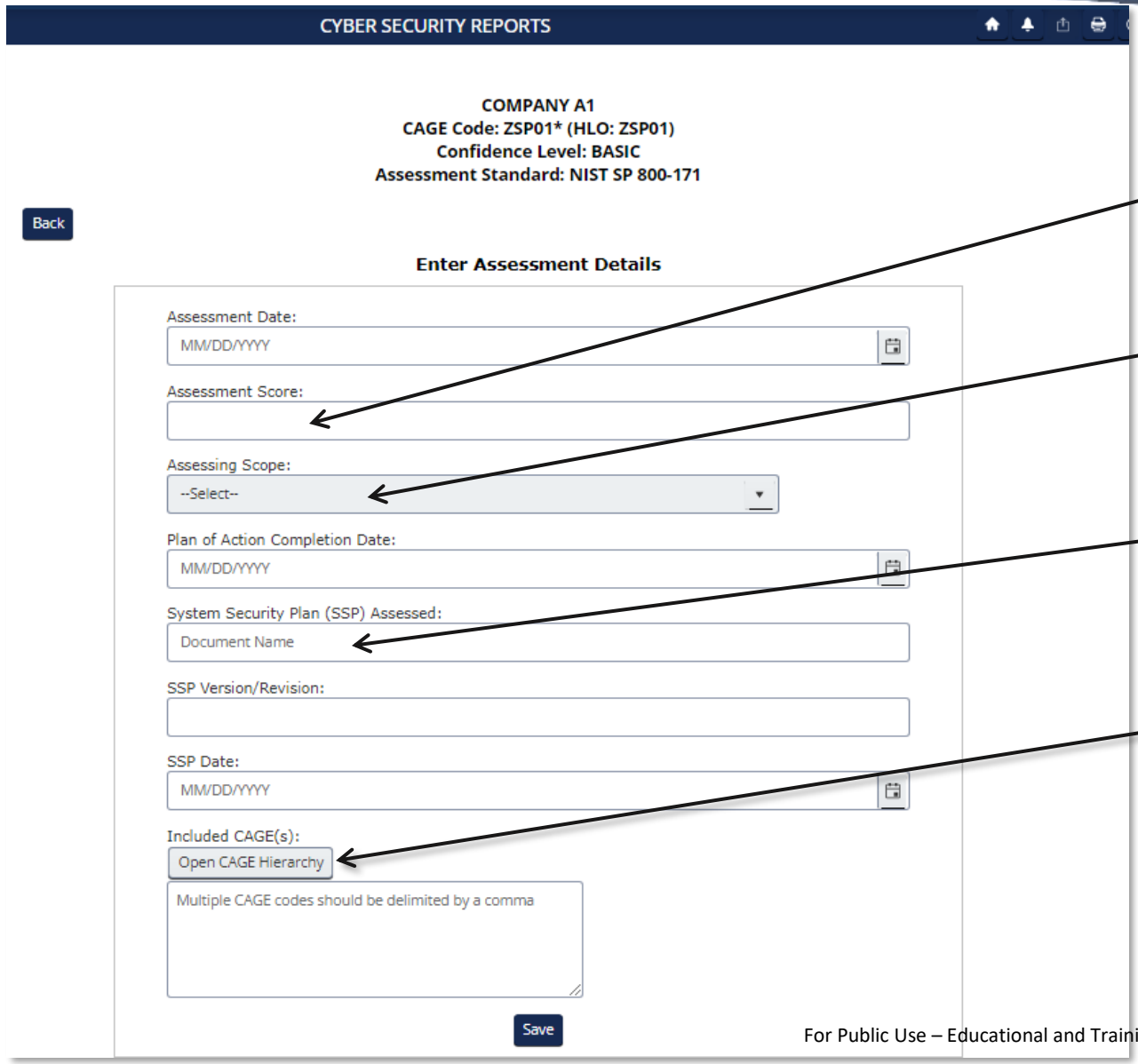
- ***Select Highest Level Owner (HLO) CAGE from hierarchy***

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

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

- ***Add assessment result(s)***

NIST SP 800-171 Assessment - Entry

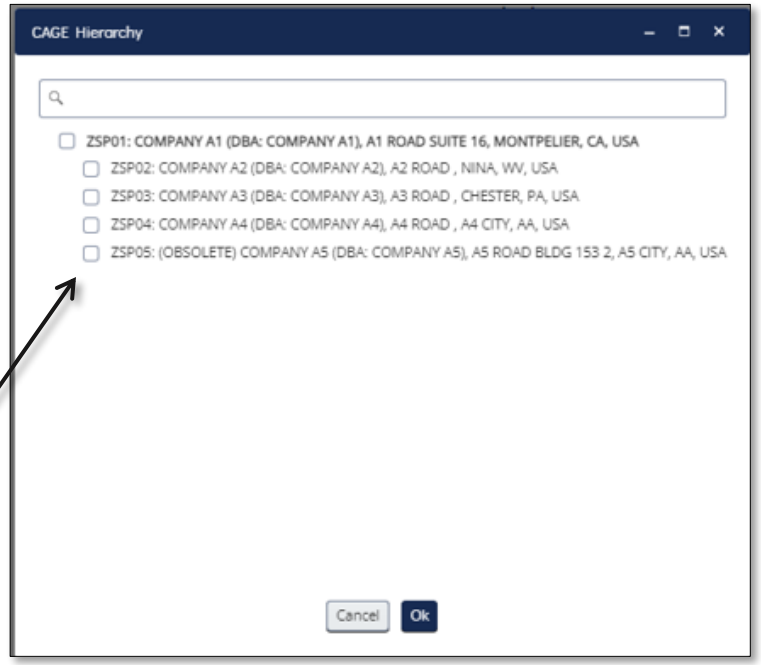


Max = 110

Enterprise, Enclave, Contract

Title of document

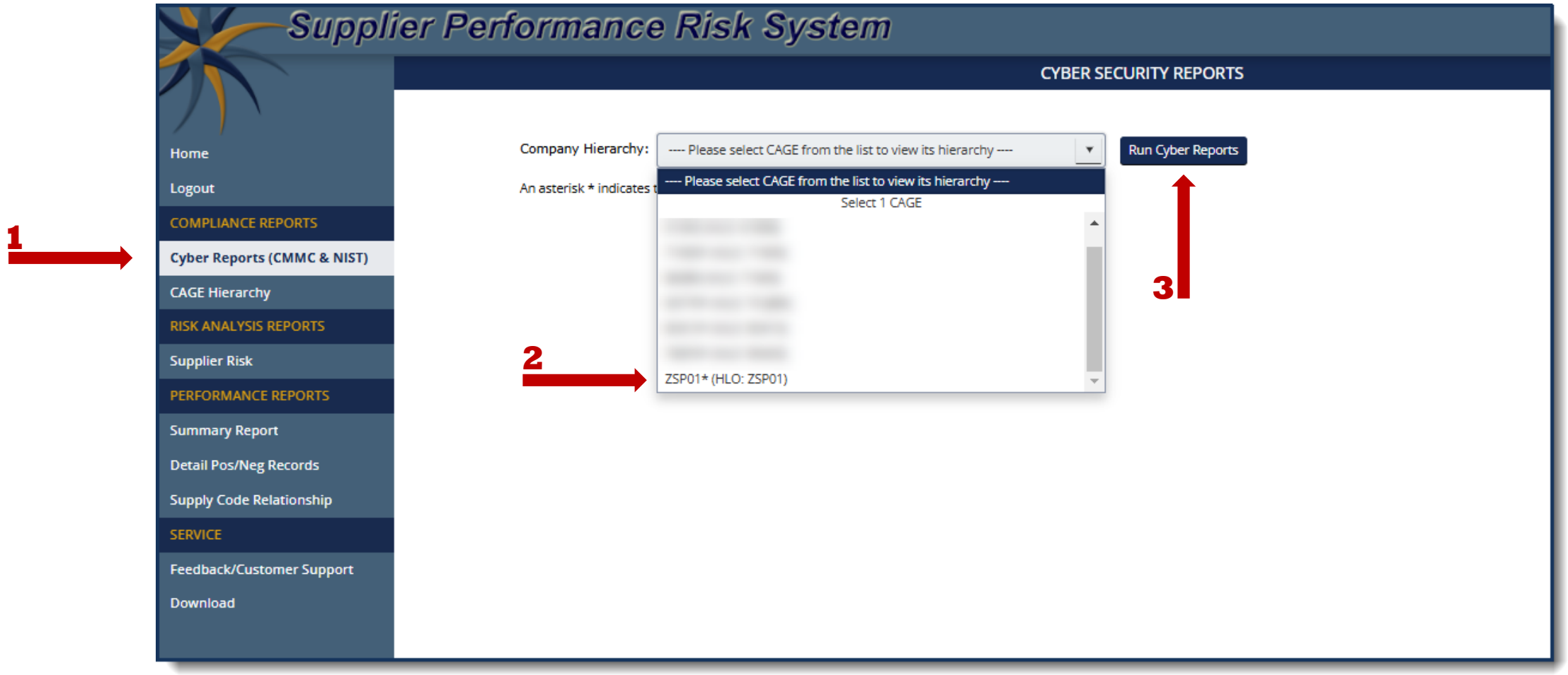
Select CAGEs subject to the assessed SSP



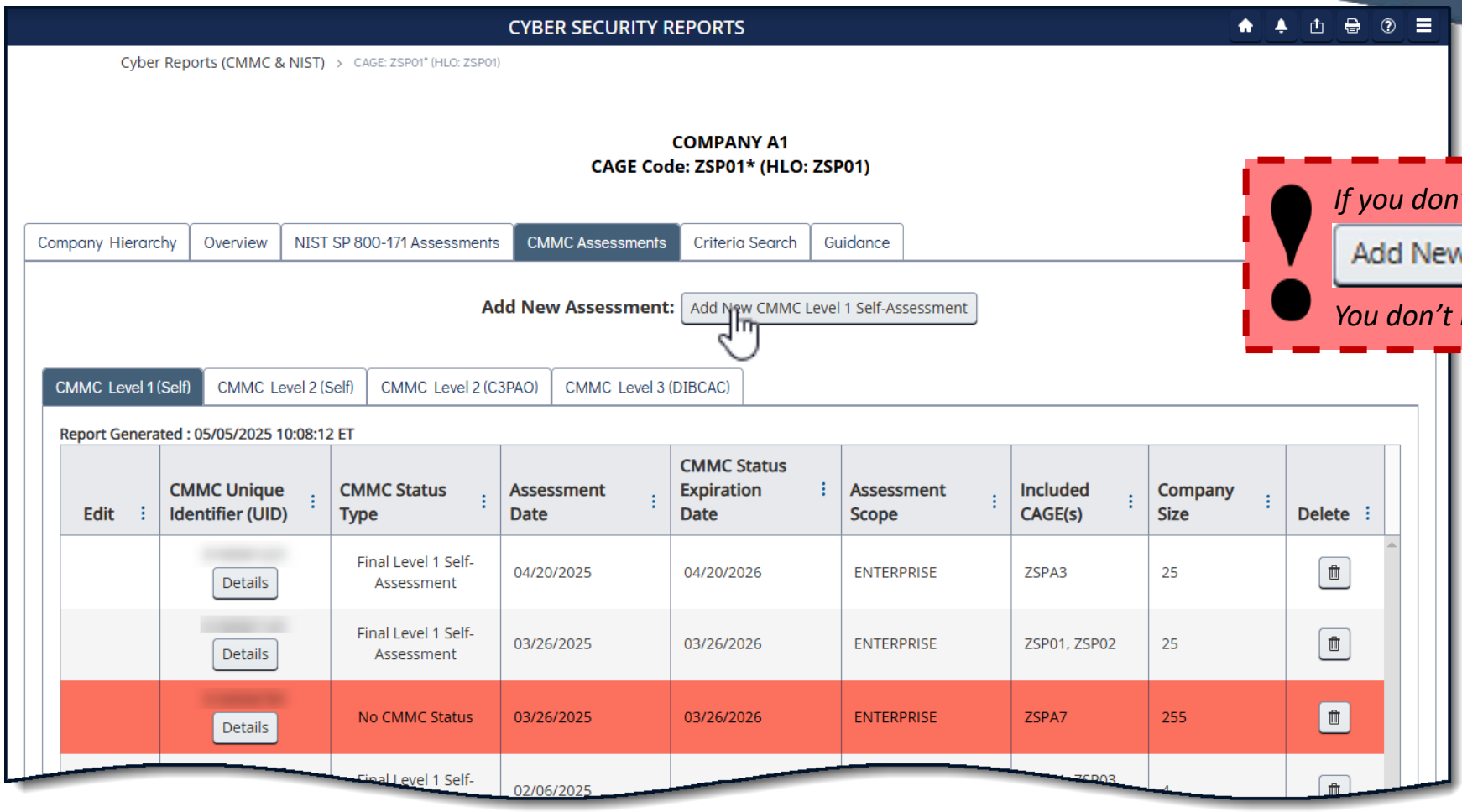
If your hierarchy is wrong, you won't be able to select all your CAGEs

CMMC Entry – Level 1 & 2

❖ ***Select CAGE from hierarchy***



CMMC Entry – Level 1



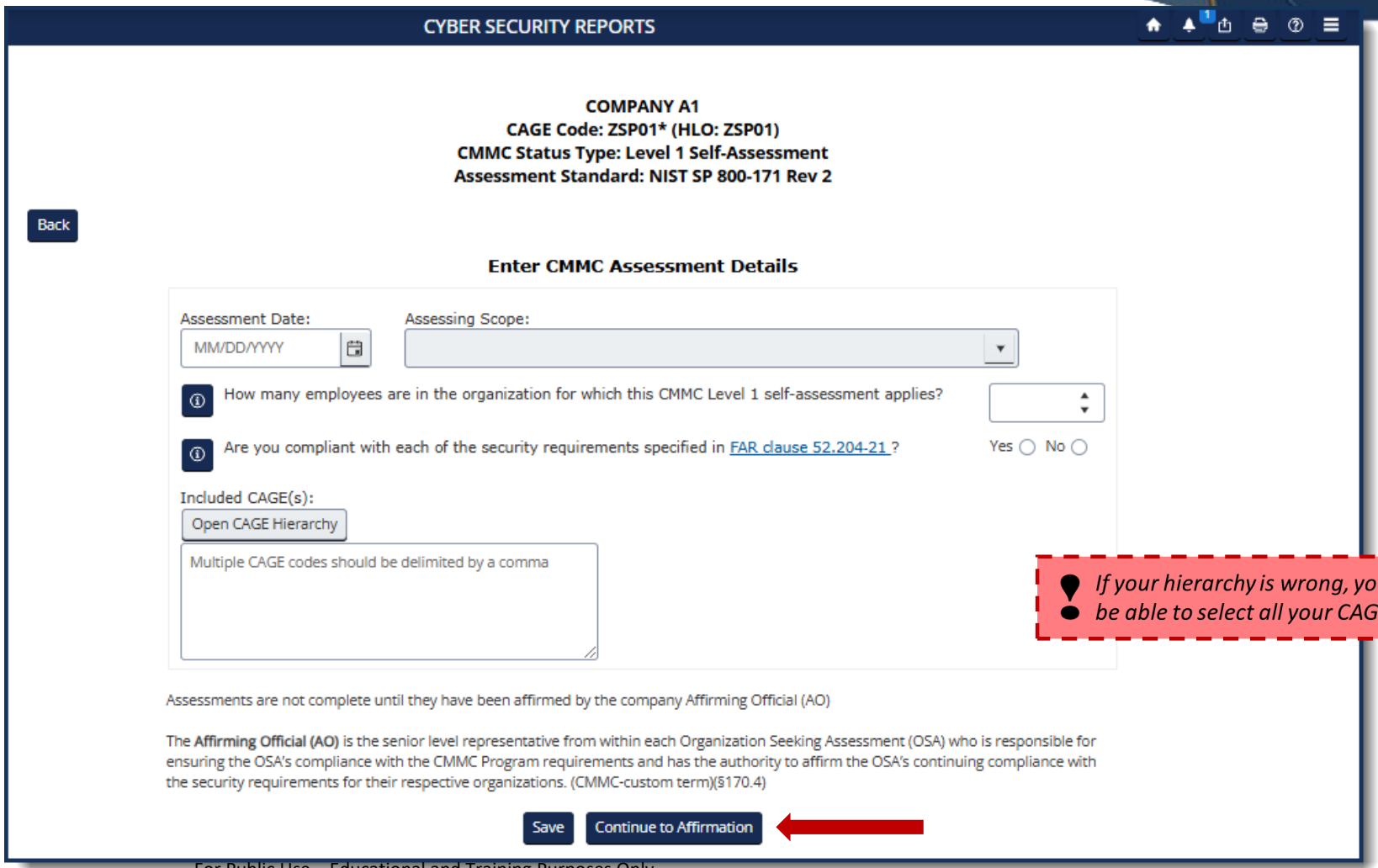
If you don't see this:

Add New CMMC Level 1 Self-Assessment

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

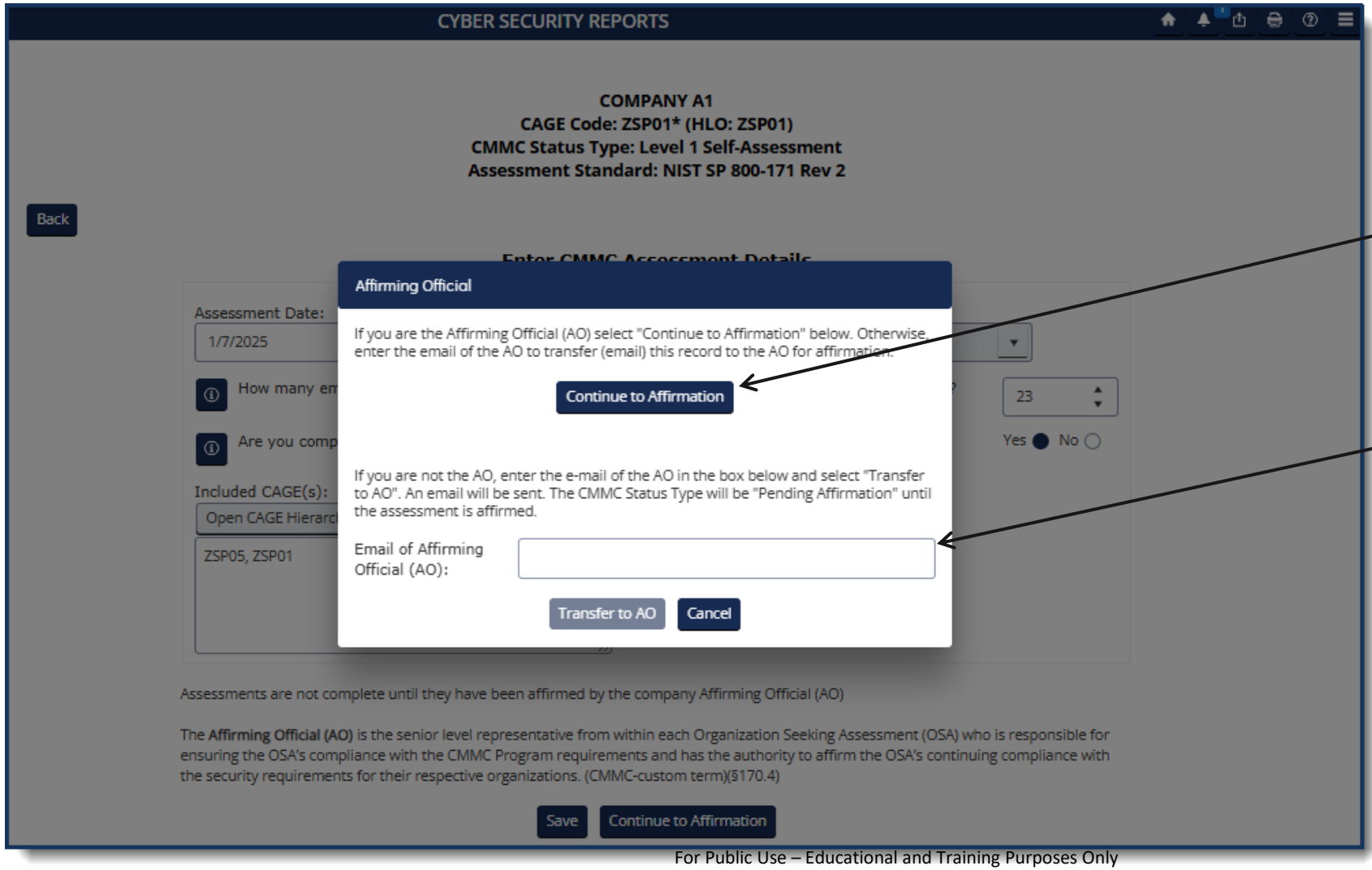
CMMC Entry – Level 1 Entry

- ***Assessment Date***
  - ***Date assessment was conducted***
- ***Assessing Scope***
  - ***Enterprise***
  - ***Enclave***
- ***# Employees***
- ***FAR 52.204-21 compliance***
- ***Included CAGEs***
  - ***CAGEs with access to IT system subject to the assessment scope***



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

CMMC Entry – Send to Affirming Official

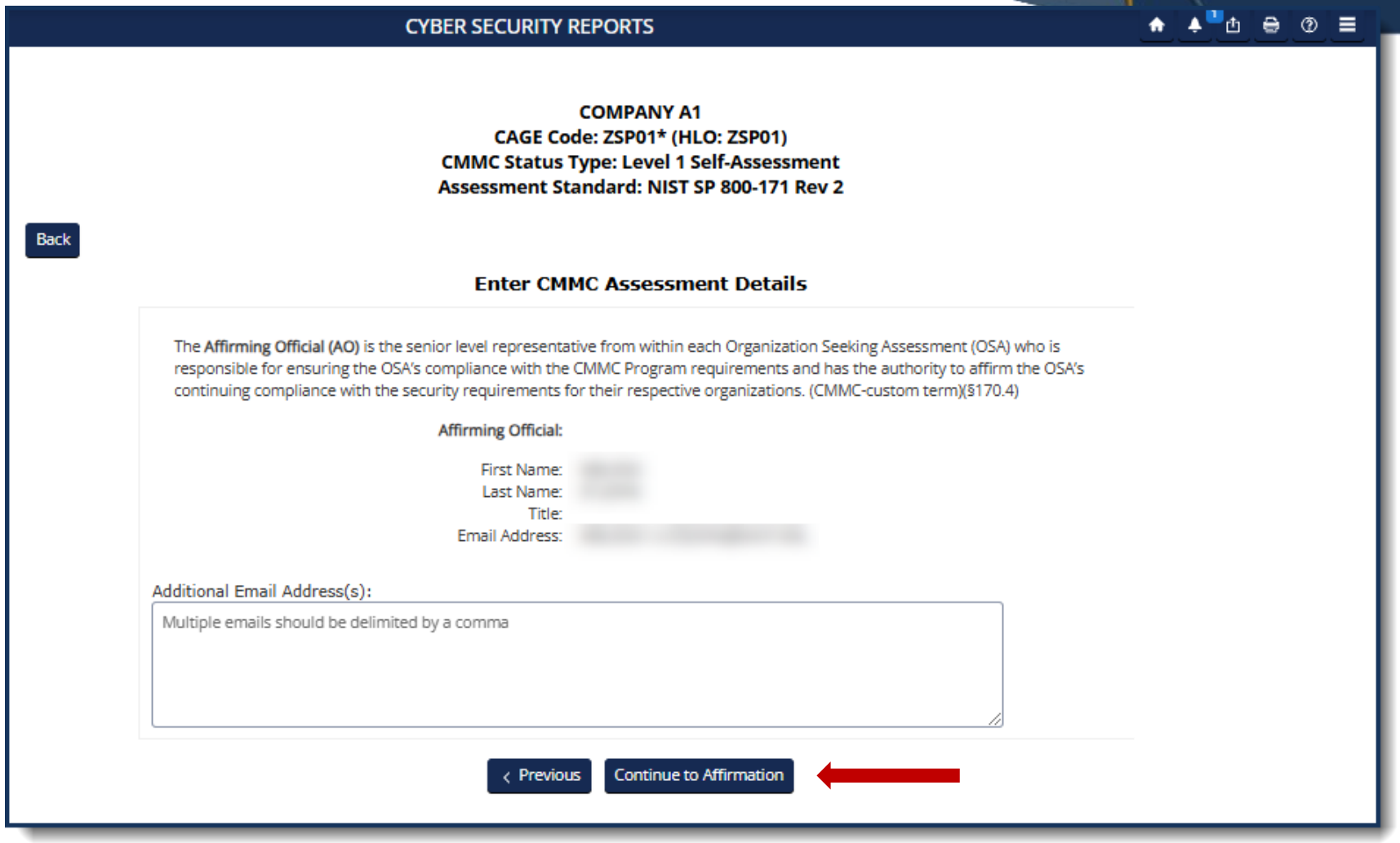


Are you the AO? Go to affirmation

Otherwise send email w/ instructions to AO

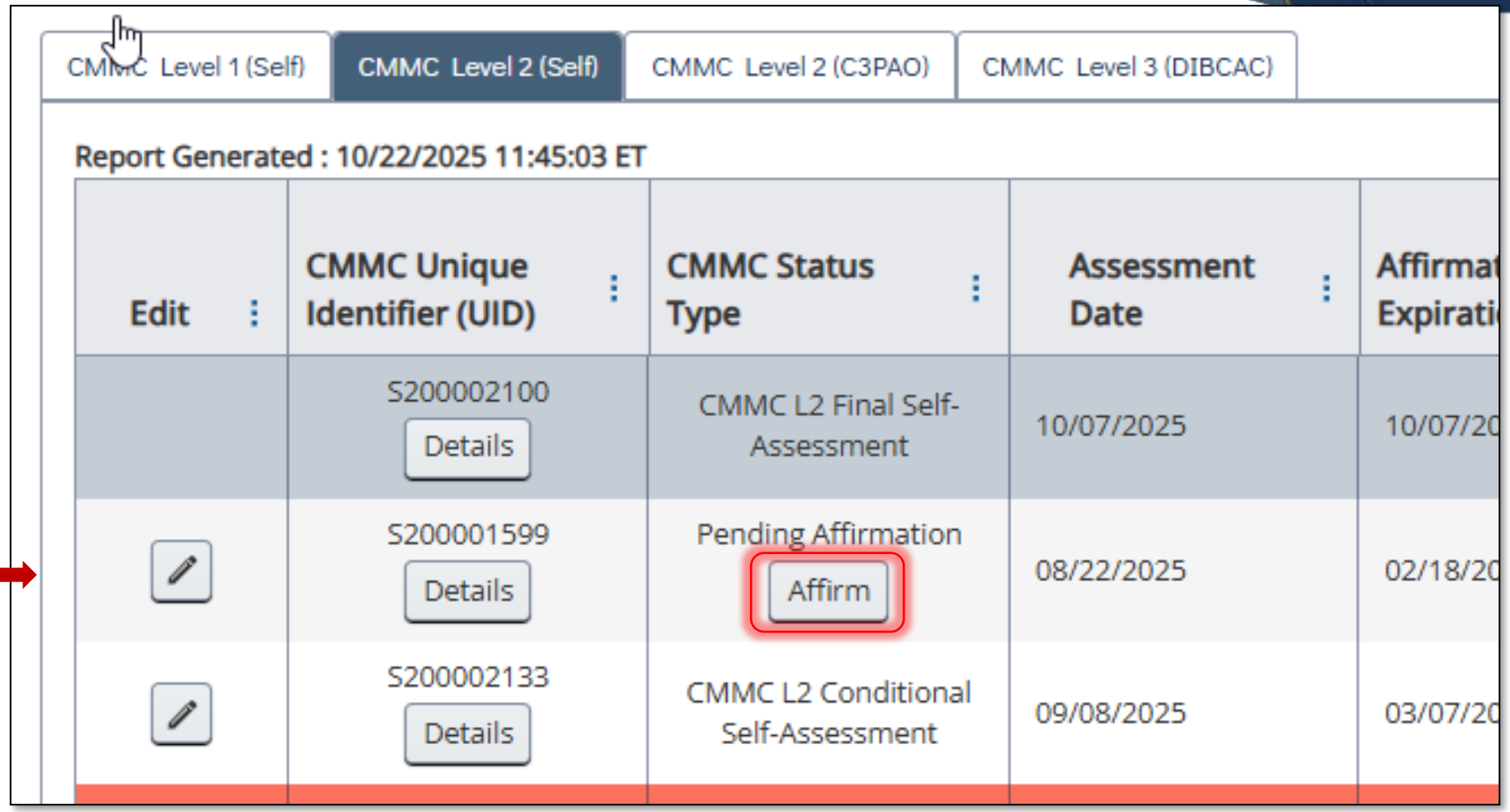
CMMC Affirmation Workflow

- ***AO verifies personal info and authority to affirm***
- ***Optional: additional POCs for government KOs to contact regarding this assessment***



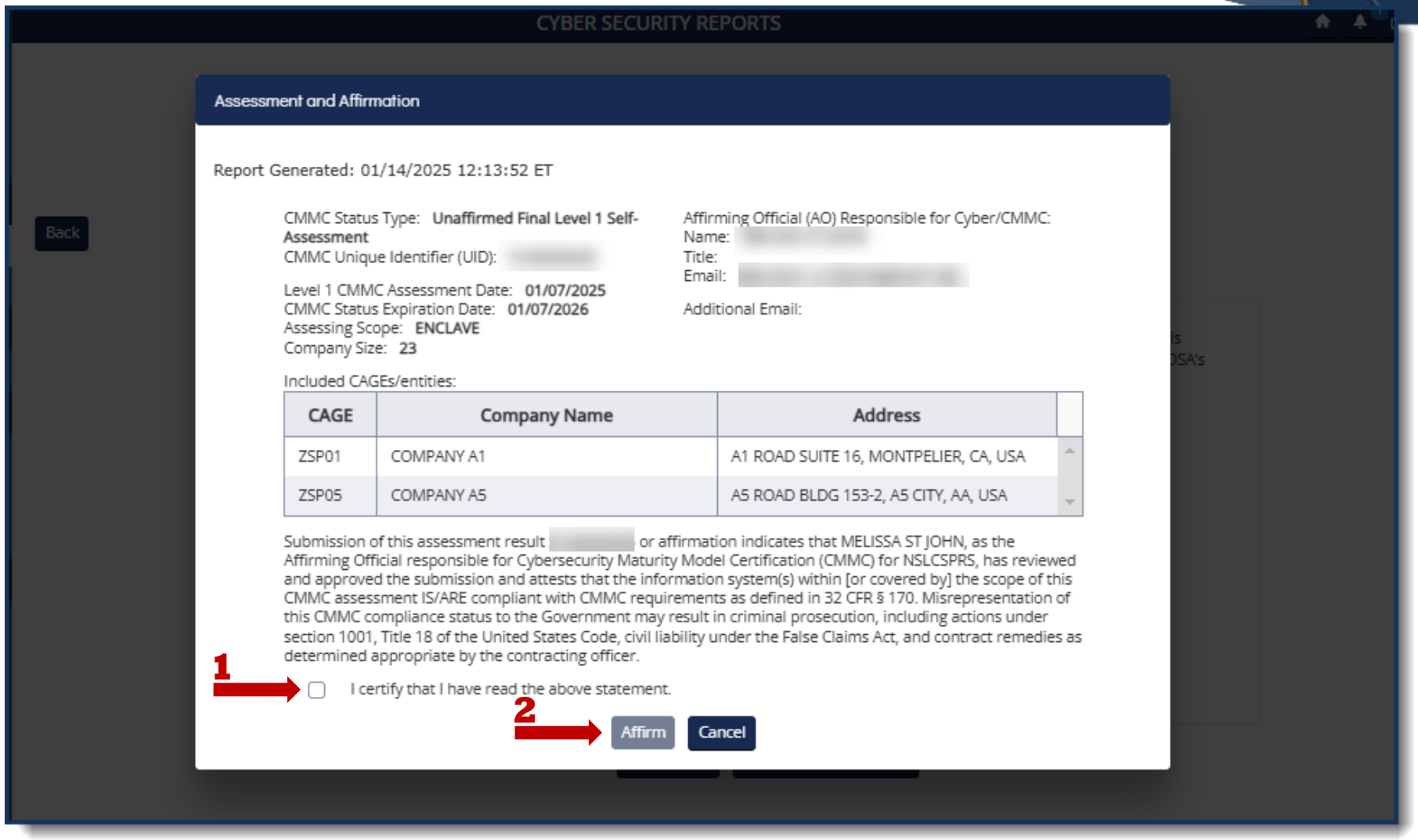
CMMC Affirmation Workflow

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



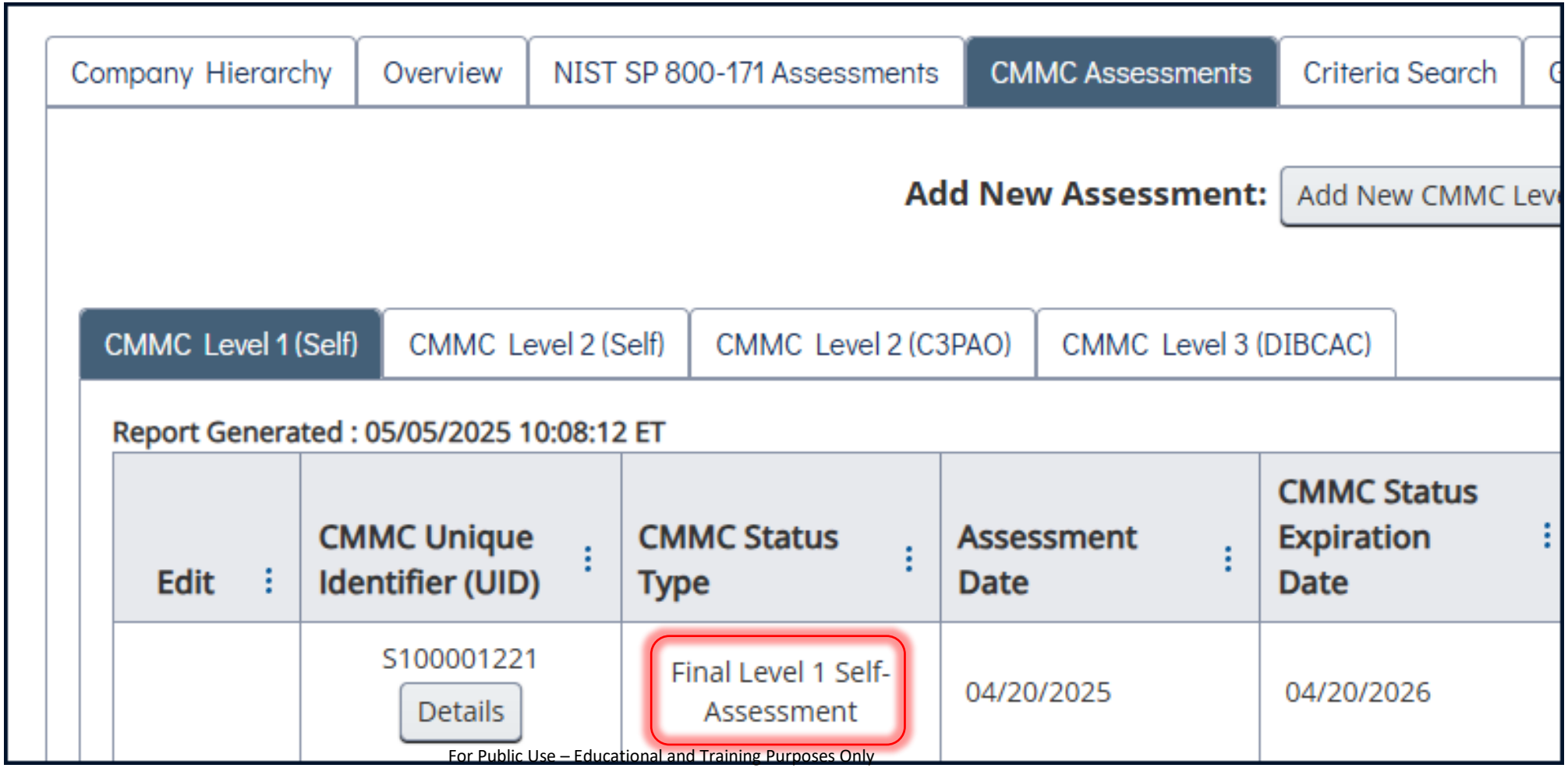
CMMC Affirmation Workflow

- ***AO reviews results and affirms***

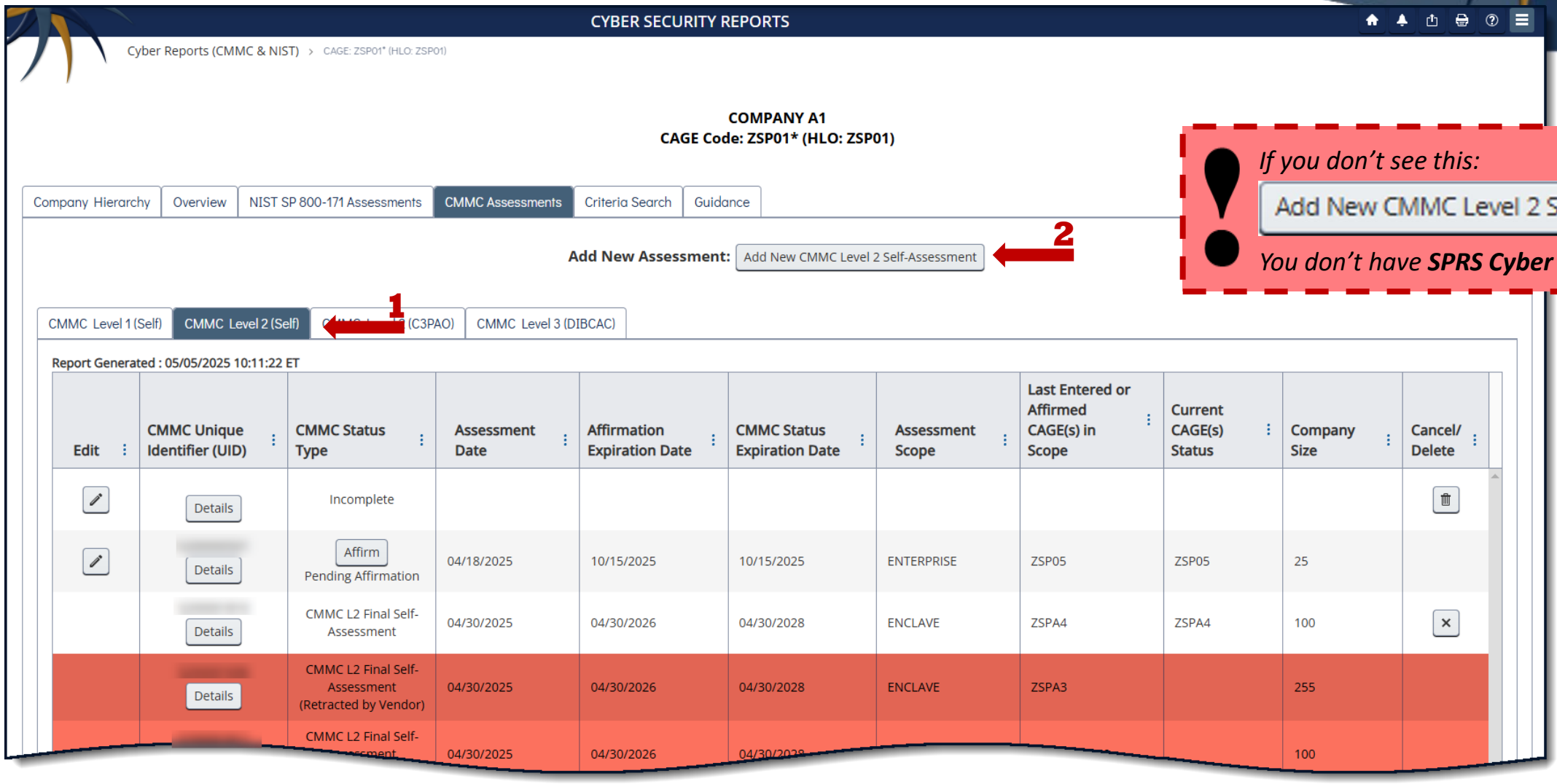


CMMC Affirmation Workflow

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



CMMC Entry – Level 2



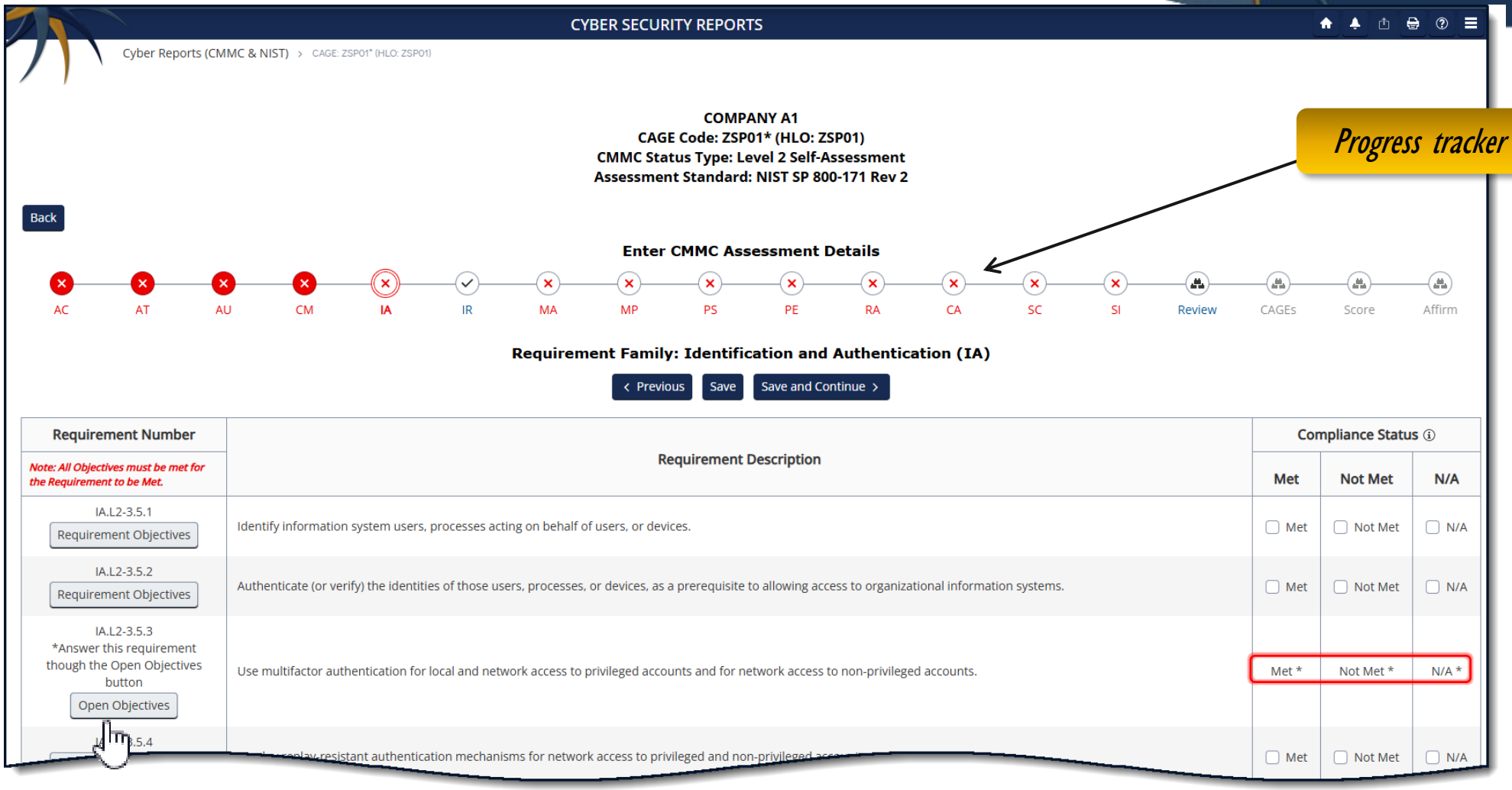
If you don't see this:

Add New CMMC Level 2 Self-Assessment

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

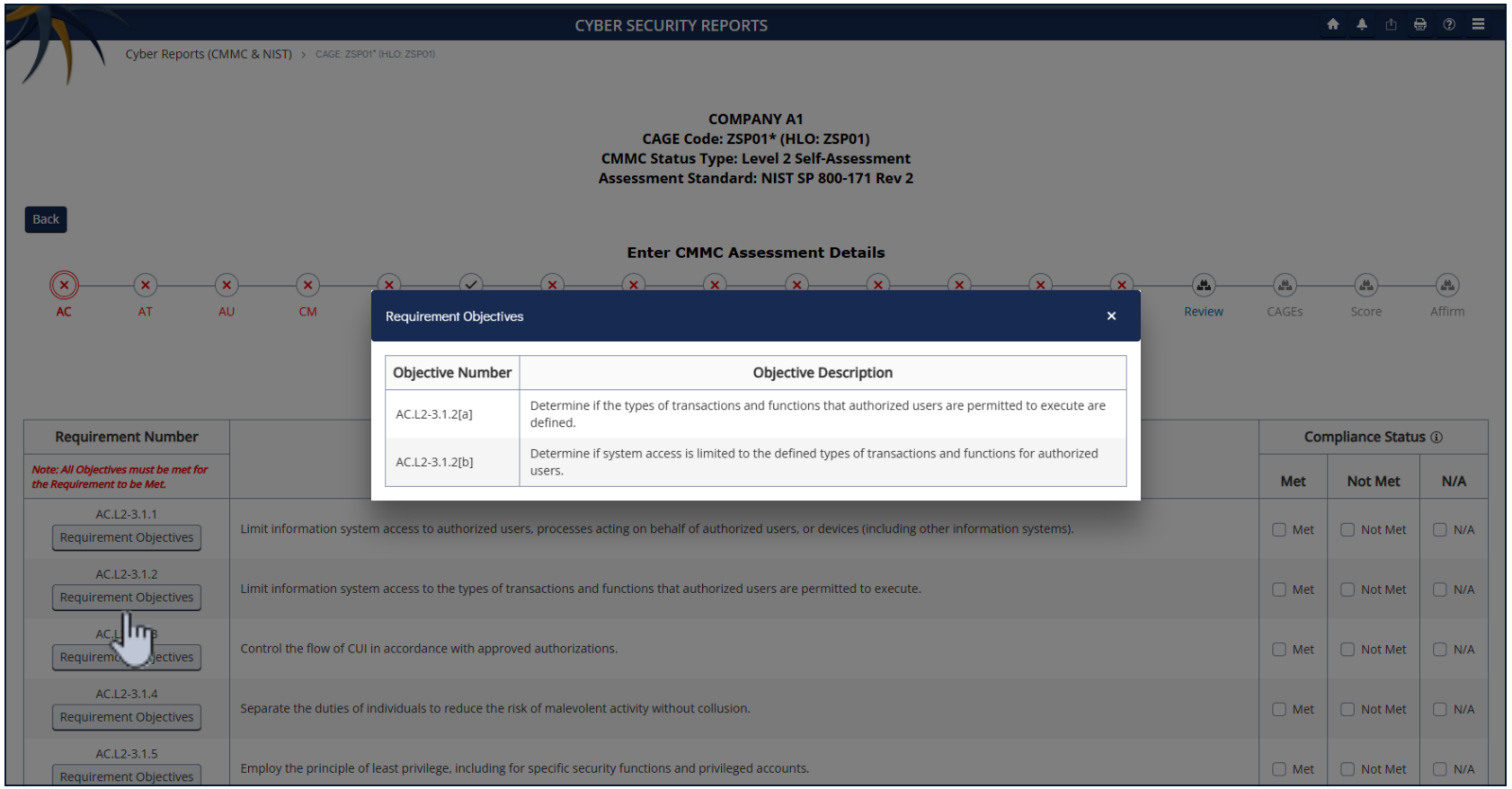
CMMC Entry – Level 2

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



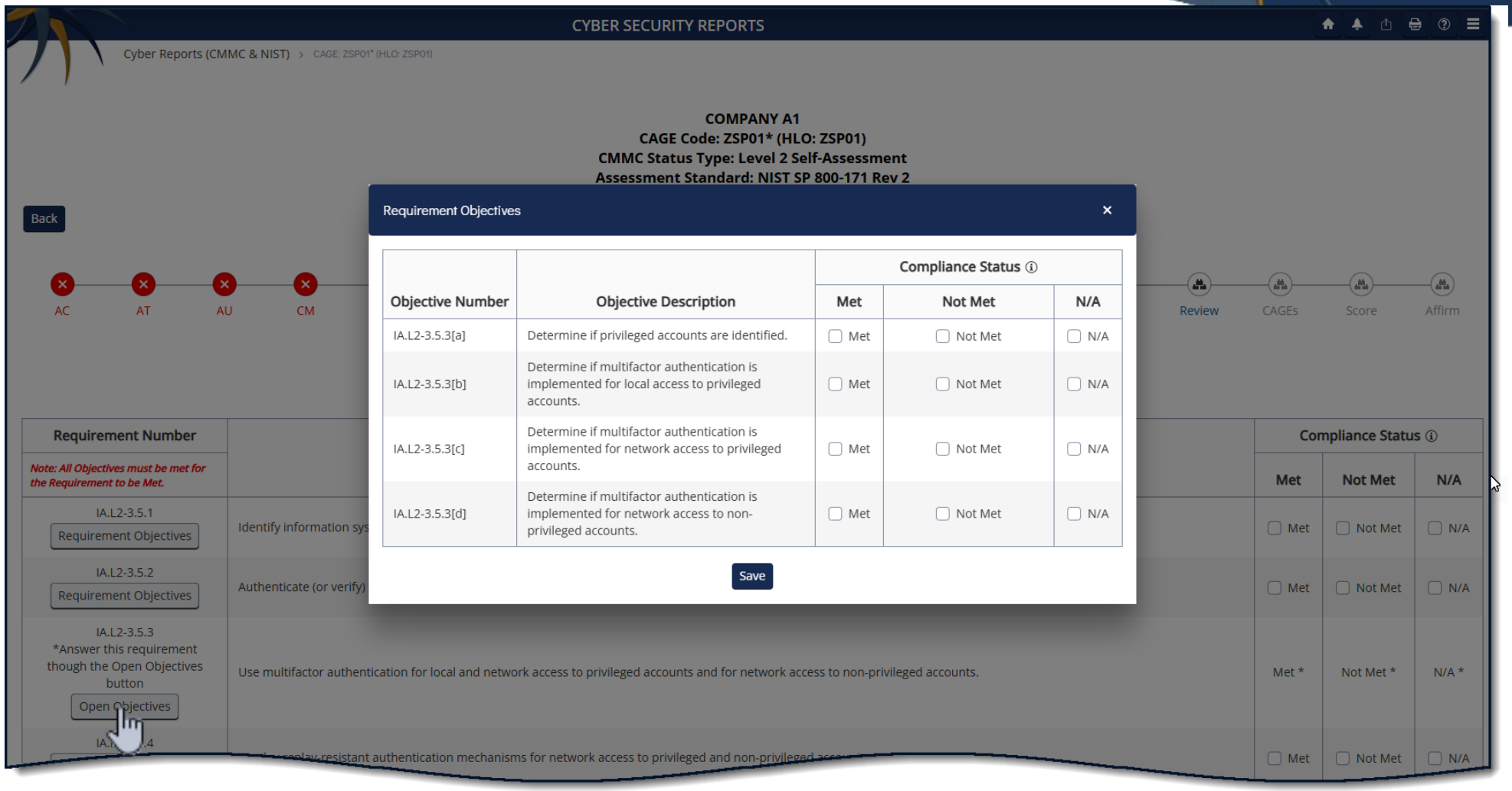
CMMC Entry – Level 2

- ***Objective details available in pop-up***



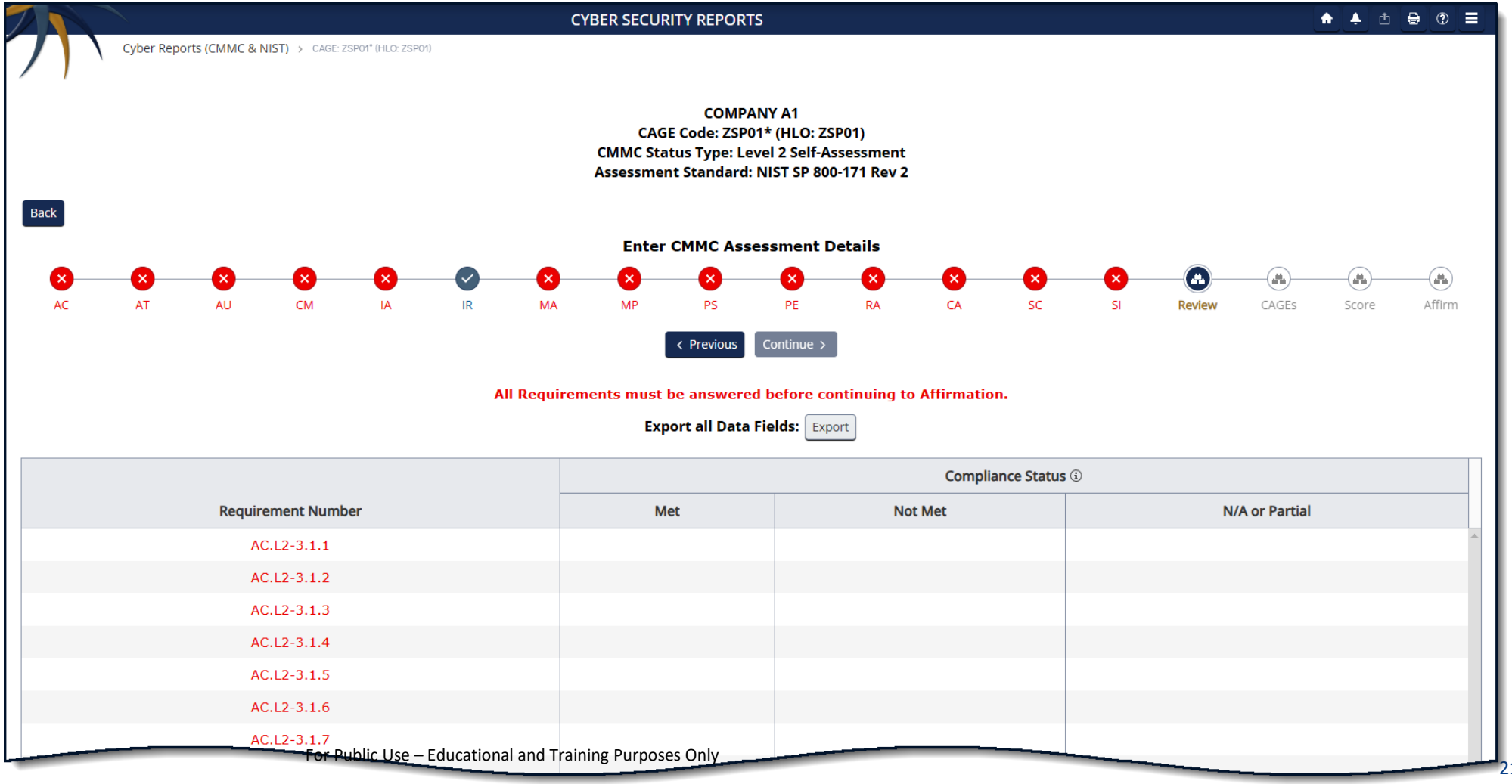
CMMC Entry – Level 2

- ***Individual objectives***



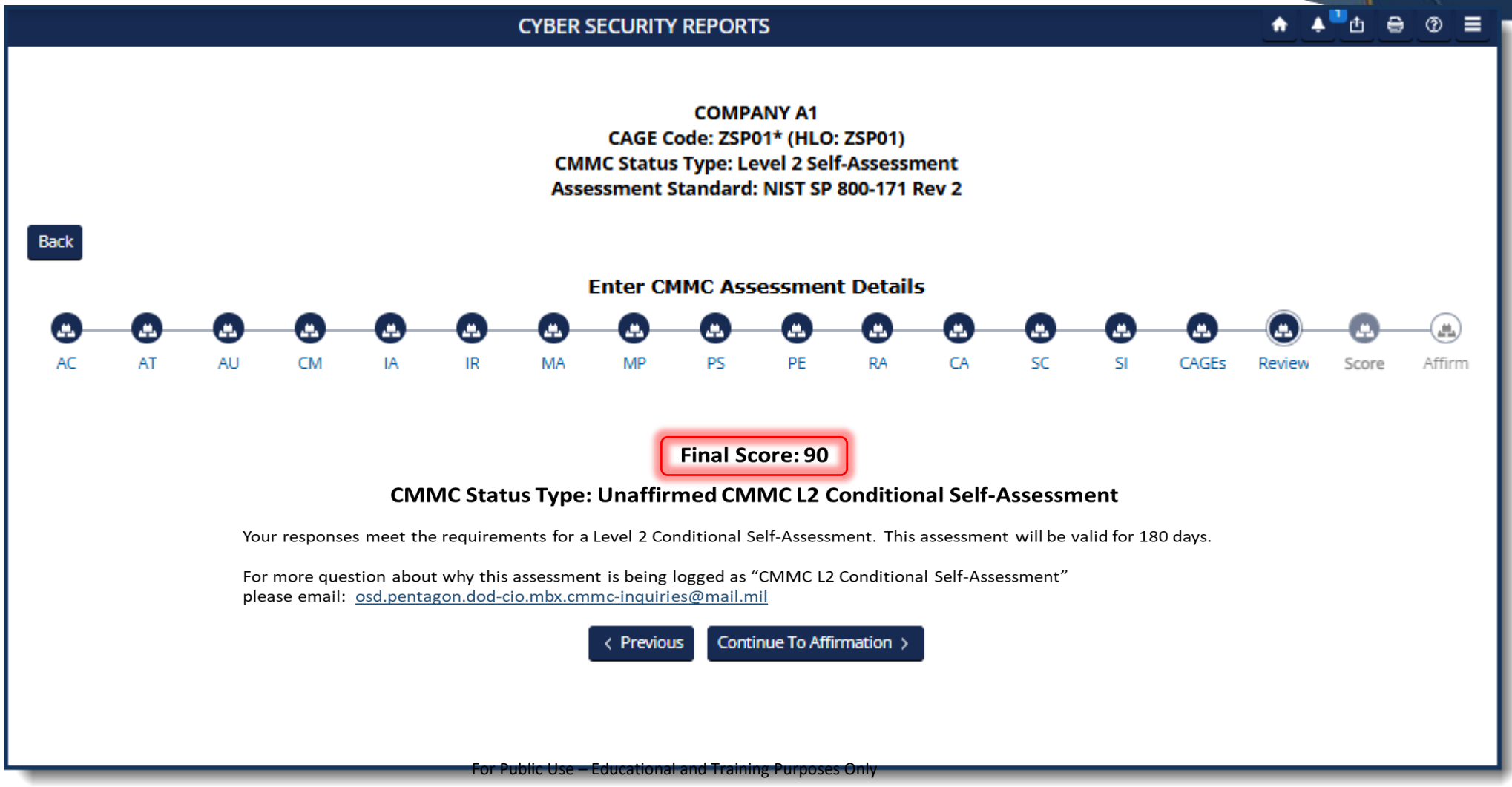
CMMC Affirmation – Level 2

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



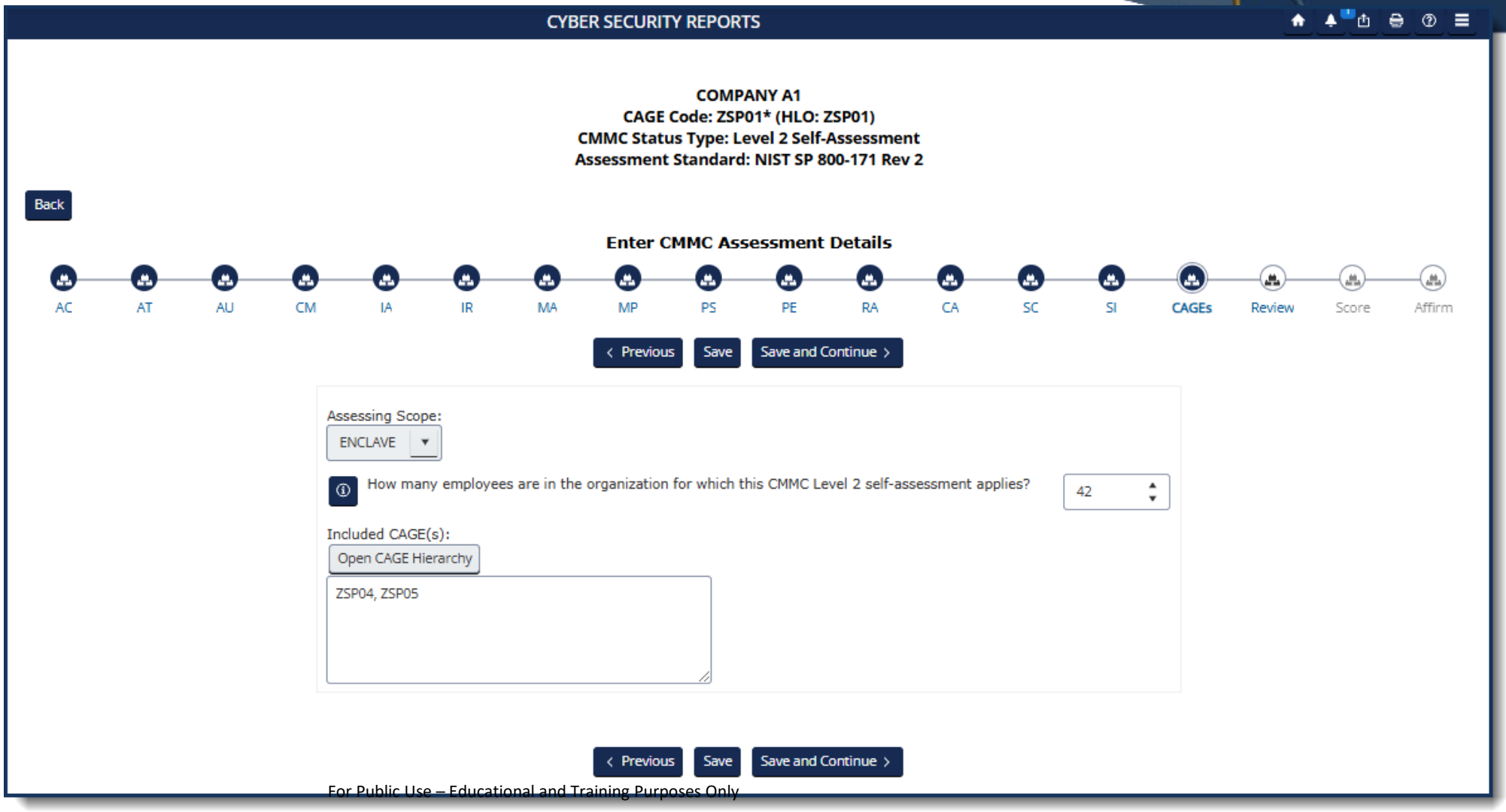
CMMC Affirmation – Level 2

- ***Score is calculated***



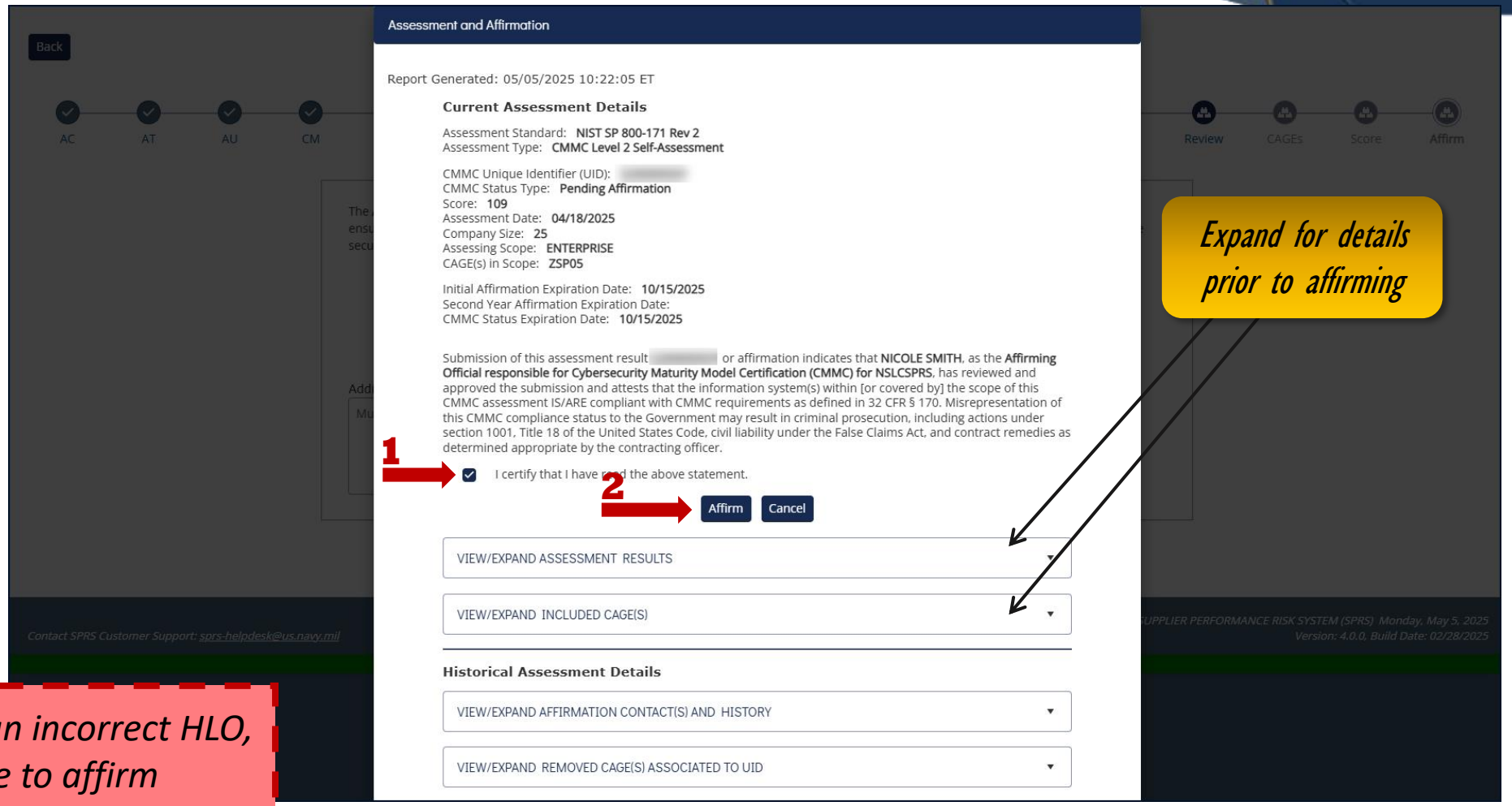
CMMC Affirmation – Level 2

- ***Affirmation process similar to Level 1***



CMMC Affirmation – Level 2

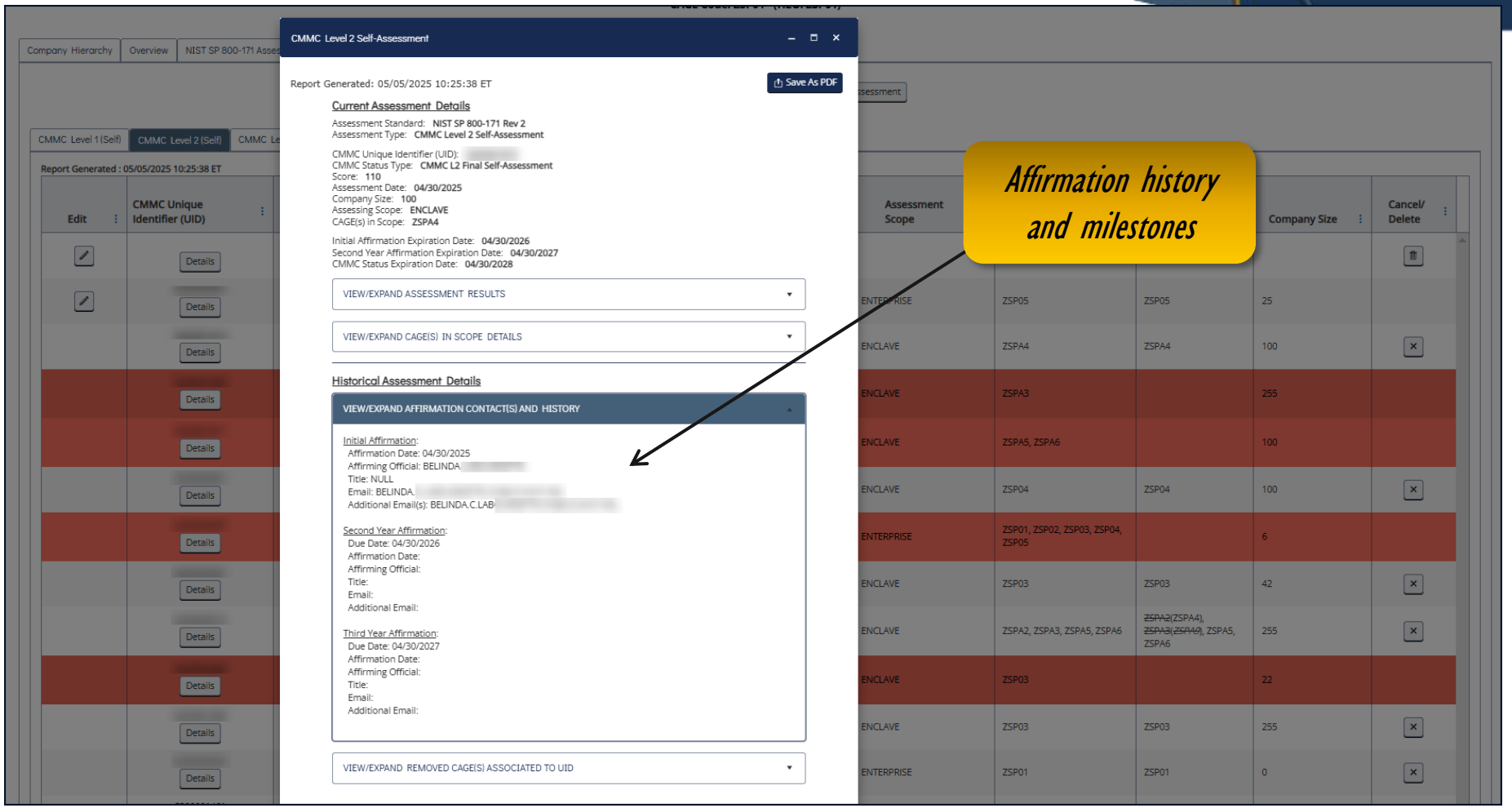
- ***AO verifies personal info, reviews results, and affirms***
- ***AO will NOT see the record if the HLO entered by the C3PAO is not yours (per SAM)***



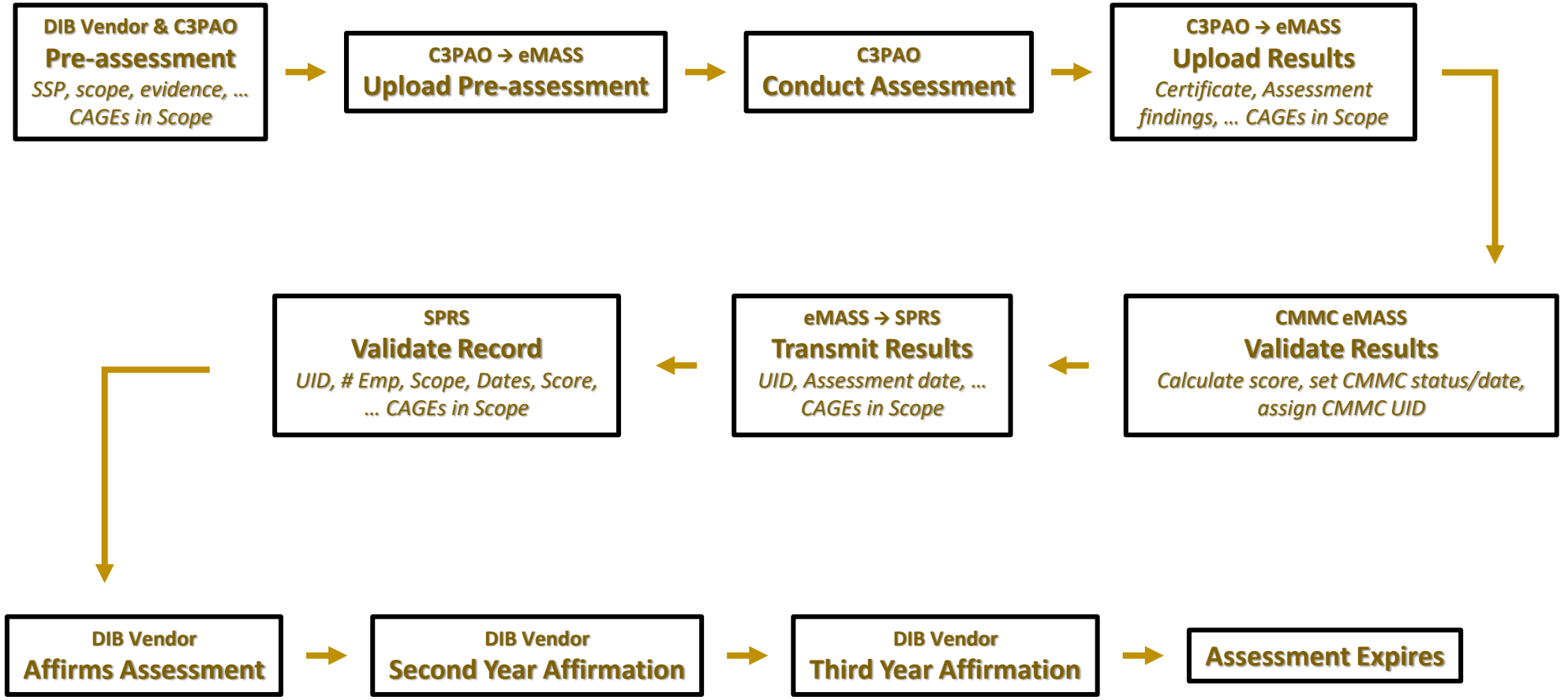
If your C3PAO sends an incorrect HLO, your AO won't be able to affirm

CMMC Affirmation Schedule

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



C3PAO CMMC Assessment Flow (notional)



CMMC Assessment Flow help

DIB Vendor
SAM CAGE data
Verify/correct ownership info in SAM

DIB Vendor & C3PAO
Pre-assessment
SSP, scope, evidence, … CAGEs in Scope

C3PAO → eMASS
Upload Pre-assessment

C3PAO
Conduct Assessment

C3PAO → eMASS
Upload Results
Certificate, Assessment findings, … CAGEs in Scope

CMMC eMASS
Validate Results
Calculate score, set CMMC status/date, assign CMMC UID

eMASS → SPRS
Transmit Results
UID, Assessment date, … CAGEs in Scope

SPRS
Validate Record
UID, # Emp, Scope, Dates, Score, … CAGEs in Scope

DIB Vendor
Affirms Assessment

DIB Vendor
Second Year Affirmation

DIB Vendor
Third Year Affirmation

Assessment Expires

CMMC Assessment Flow (notional)

DIB Vendor
SAM CAGE data
Verify/correct ownership info in SAM

DIB Vendor & C3PAO
Pre-assessment
SSP, scope, evidence, … CAGEs in Scope

C3PAO → eMASS
Upload Pre-assessment

C3PAO
Conduct Assessment

C3PAO → eMASS
Upload Results
Certificate, Assessment findings, … CAGEs in Scope

CMMC eMASS
Validate Results
Calculate score, set CMMC status/date, assign CMMC UID

eMASS → SPRS
Transmit Results
UID, Assessment date, … CAGEs in Scope

SPRS
Validate Record
UID, # Emp, Scope, Dates, Score, … CAGEs in Scope

SPRS
Valid Record?

NO

SPRS → DIB Vendor
Rejection Alert

DIB Vendor & C3PAO
Resolve Issues

YES

DIB Vendor
Affirms Assessment

DIB Vendor
Second Year Affirmation

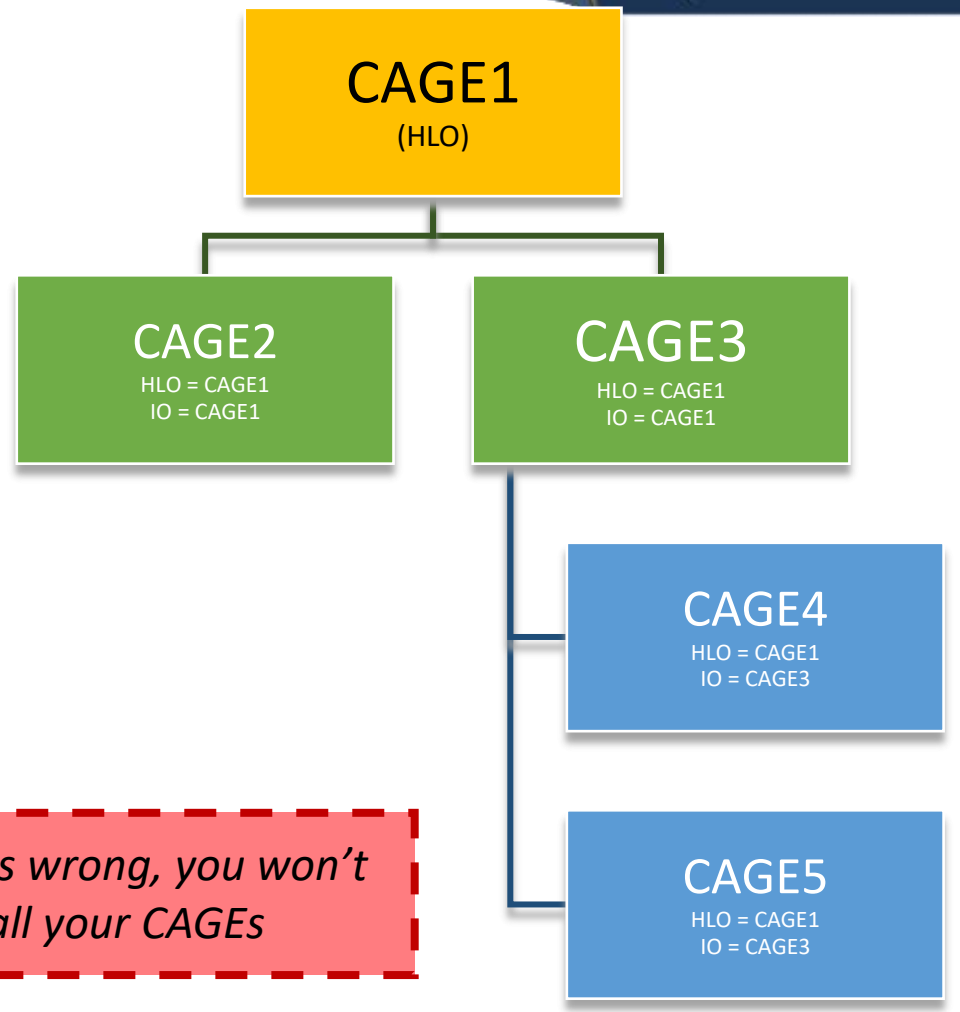
DIB Vendor
Third Year Affirmation

Assessment Expires

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

CMMC/NIST – CAGE Hierarchy

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



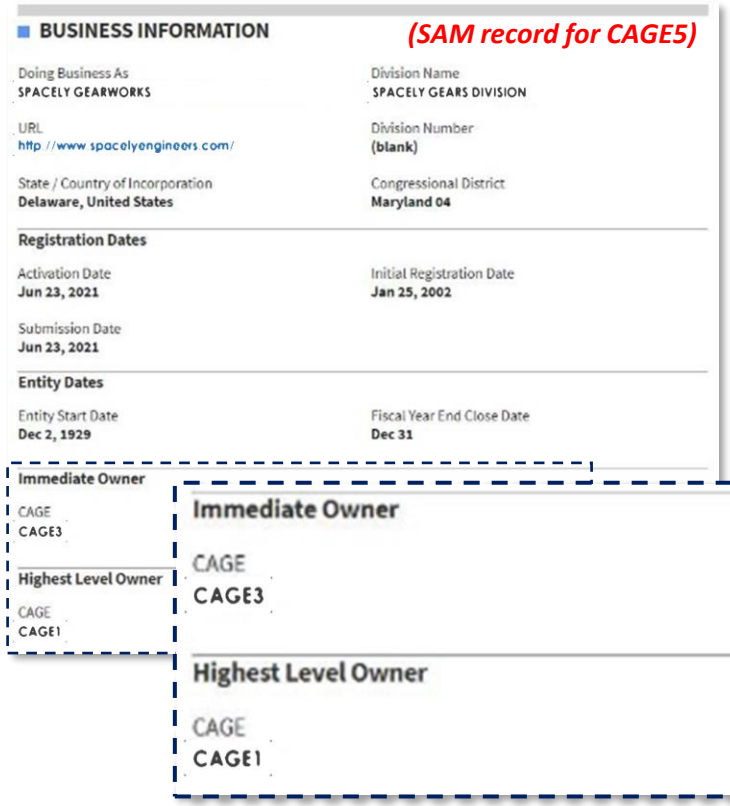
If your hierarchy is wrong, you won't be able to select all your CAGEs

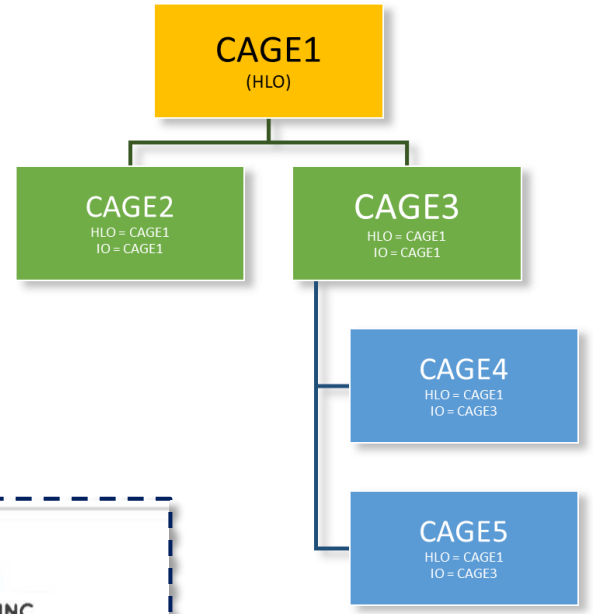
CMMC/NIST – Fixing Hierarchy

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

CAGE.dla.mil
[automatically updated]

Step 2: SPRS
Vendor checks hierarchy





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

Cybersecurity Assessment - Pointers

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

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

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

Q: Why don't I see this buttons? → 

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

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

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

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

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

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

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

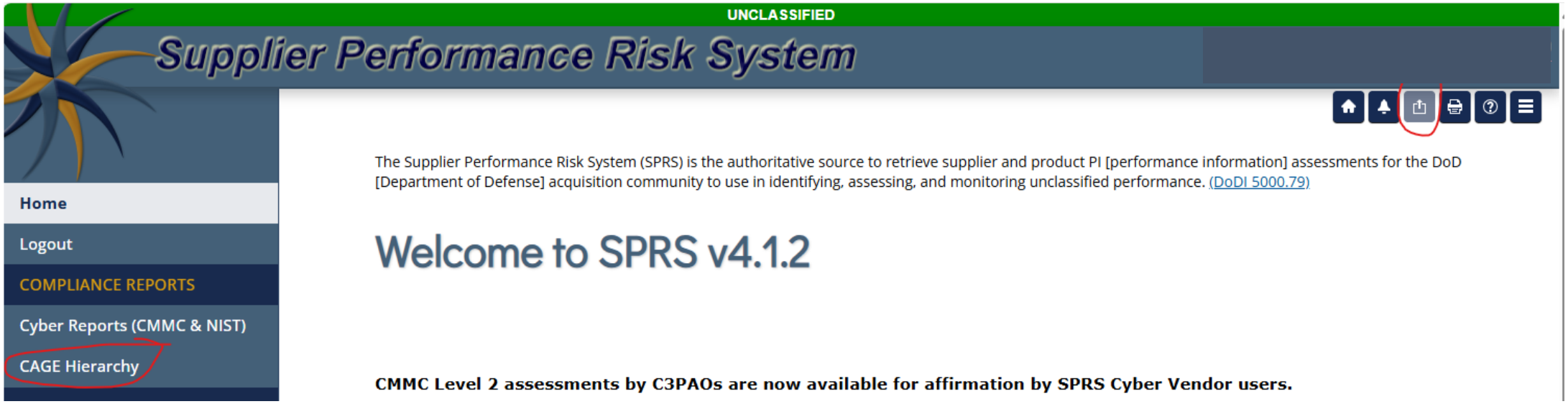
SPRS User Roles – PIEE single sign-on

- *Government (KOs, PMs, LOGgies, etc.)*
  - ***SPRS Acquisition Professional***
    - *Gives access to <u>all</u> scores/reports*

https://piee.eb.mil

- ***Contractor/Vendor***
  - ***SPRS Contractor/Vendor (Support Role)***
    - *View your company's scores/reports*
    - *View-only access to CS assessments*
    - *CAGE hierarchy*
  - ***SPRS Cyber Vendor User***
    - *Add/edit/delete/affirm CS assessments*
    - *CAGE hierarchy*

SPRS Downloads



Website and Help

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

Cyber help

References
User Guides
Quick Reference Guides
PIEE Access Help
Eval Criteria

Training
PPTs
Tutorial videos

SPRS Contact Information

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

NSLC Help Desk Email:
nslcports-helpdesk@us.navy.mil

Newly-improved **Feedback** (bottom of app menu)