Submitting NIST and CMMC Scores in PIEE/SPRS

Will McEllen, SAPPC, ISP
Armiger, LLC.
Industrial Security Consulting and Support

CMMC Status	Source & Number of Security Reqts.	Assessment Reqts.	Plan of Action & Milestones (POA&M) Reqts.	Affirmation Reqts.
Level 1 (Self)	• 15 required by FAR clause 52.204-21	• Conducted by Organization Seeking Assessment (OSA) annually • Results entered into the Supplier Performance Risk System (SPRS)	• Not permitted	• After each assessment • Entered into SPRS
Level 2 (Self)	• 110 NIST SP 800-171 R2 required by DFARS clause 252.204-7012	• Conducted by OSA every 3 years • Results entered into SPRS • CMMC Status will be valid for three years from the CMMC Status Date as defined in § 170.4	• Permitted as defined in § 170.21(a)(2) and must be closed out within 180 days • Final CMMC Status will be valid for three years from the Conditional CMMC Status Date	• After each assessment and annually thereafter • Assessment will lapse upon failure to annually affirm • Entered into SPRS
Level 2 (C3PAO)	• 110 NIST SP 800-171 R2 required by DFARS clause 252.204-7012	• Conducted by C3PAO every 3 years • Results entered into CMMC Enterprise Mission Assurance Support Service (eMASS) • CMMC Status will be valid for three years from the CMMC Status Date as defined in § 170.4	• Permitted as defined in § 170.21(a)(2) and must be closed out within 180 days • Final CMMC Status will be valid for three years from the Conditional CMMC Status Date	• After each assessment and annually thereafter • Assessment will lapse upon failure to annually affirm • Entered into SPRS
Level 3 (DIBCAC)	• 110 NIST SP 800-171 R2 required by DFARS clause 252.204-7012 • 24 selected from NIST SP 800-172 Feb2021, as detailed in table 1 to § 170.14(c)(4)	• Pre-requisite CMMC Status of Level 2 (C3PAO) for the same CMMC Assessment Scope, for each Level 3 certification assessment • Conducted by DIBCAC every 3 years • Results entered into CMMC eMASS • CMMC Status will be valid for three years from the CMMC Status Date as defined in § 170.4	• Permitted as defined in § 170.21(a)(3) and must be closed out within 180 days • Final CMMC Status will be valid for three years from the Conditional CMMC Status Date	• After each assessment and annually thereafter • Assessment will lapse upon failure to annually affirm • Level 2 (C3PAO) affirmation must also continue to be completed annually • Entered into SPRS

From: https://dodcio.defense.gov/cmmc/About/

Step 1: Register with System for Award Management (SAM)

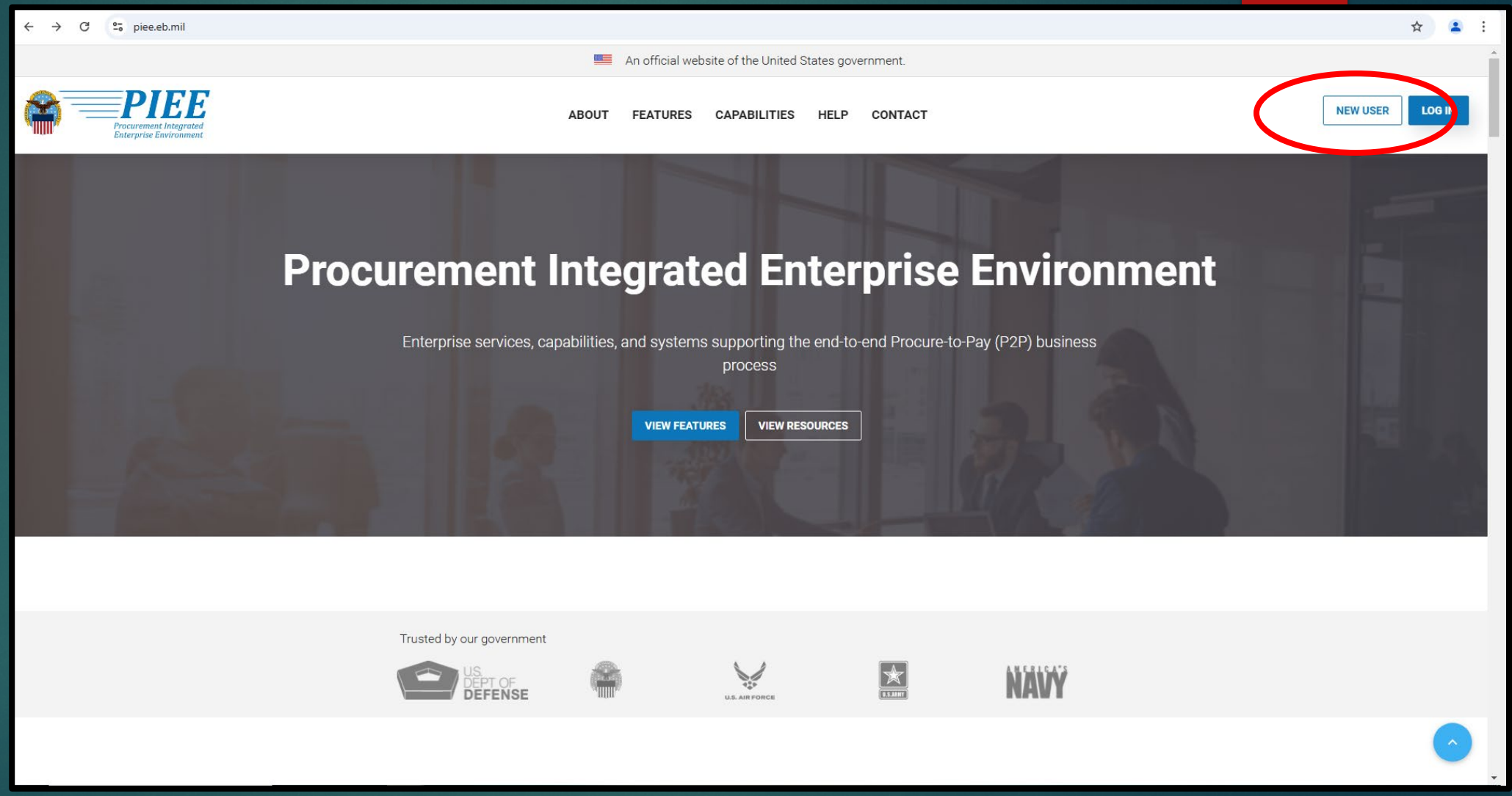
- All vendor companies must register in the SAM to sell goods and services to the Department of Defense (DoD), by going to https://www.sam.gov/.
- Establish a SAM Point of Contact (POC), if not already done. The SAM POC is responsible for updating the information in SAM.
- ***Vendors must also set up an Electronic Business (EB) POC for their company in SAM.***
- The EB POC is responsible for authorizing vendor employee(s) access to submit, modify and/or view data (contracts, invoices, payments, etc.). The SAM POC is responsible for entering or updating EB POC data in SAM. ***The EB POC should be the individual completing the PIEE registration.***
- To see if an EB POC is listed for your company, visit the SAM website, or consult your SAM POC.

Step 2: Have your CAGE Code added to the Procurement Integrated Enterprise Environment (PIEE) Vendor Group Structure.

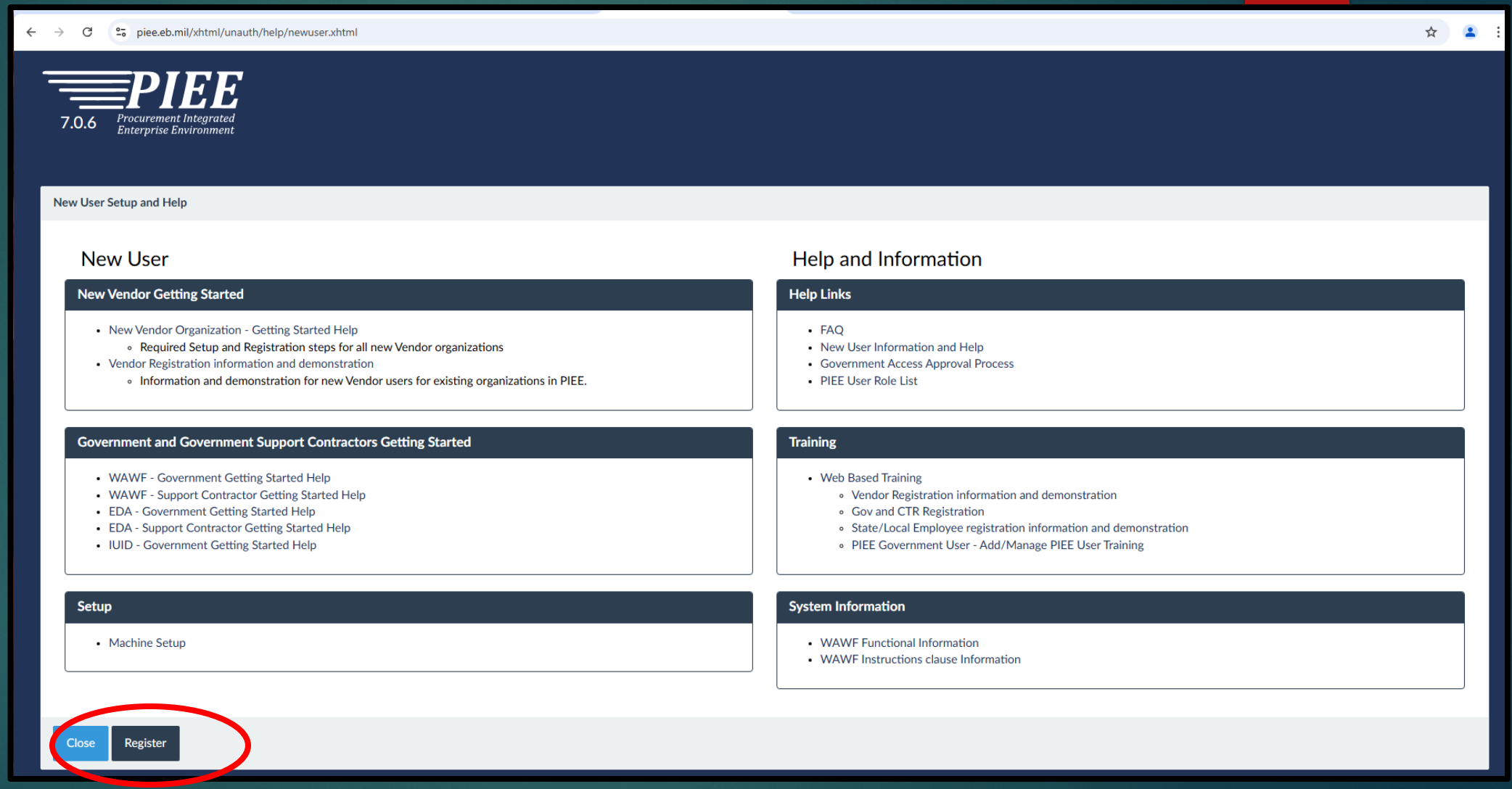
- The PIEE Help Desk must add your CAGE Code to a Group in the PIEE Vendor Group Structure, before any personnel can self-register for applications within PIEE.
- When requesting a new group, if a desired group name is not provided by the requestor, a group name will be assigned by the PIEE Help Desk based on your CAGE code or company name. ***You will be registering as a 'Vendor'***.
- To request the set up of a vendor group, a company representative must contact the PIEE Help Desk, by phone or email, and supply your CAGE code.

Call 866-618-5988
Select Option 1 and then Option 2

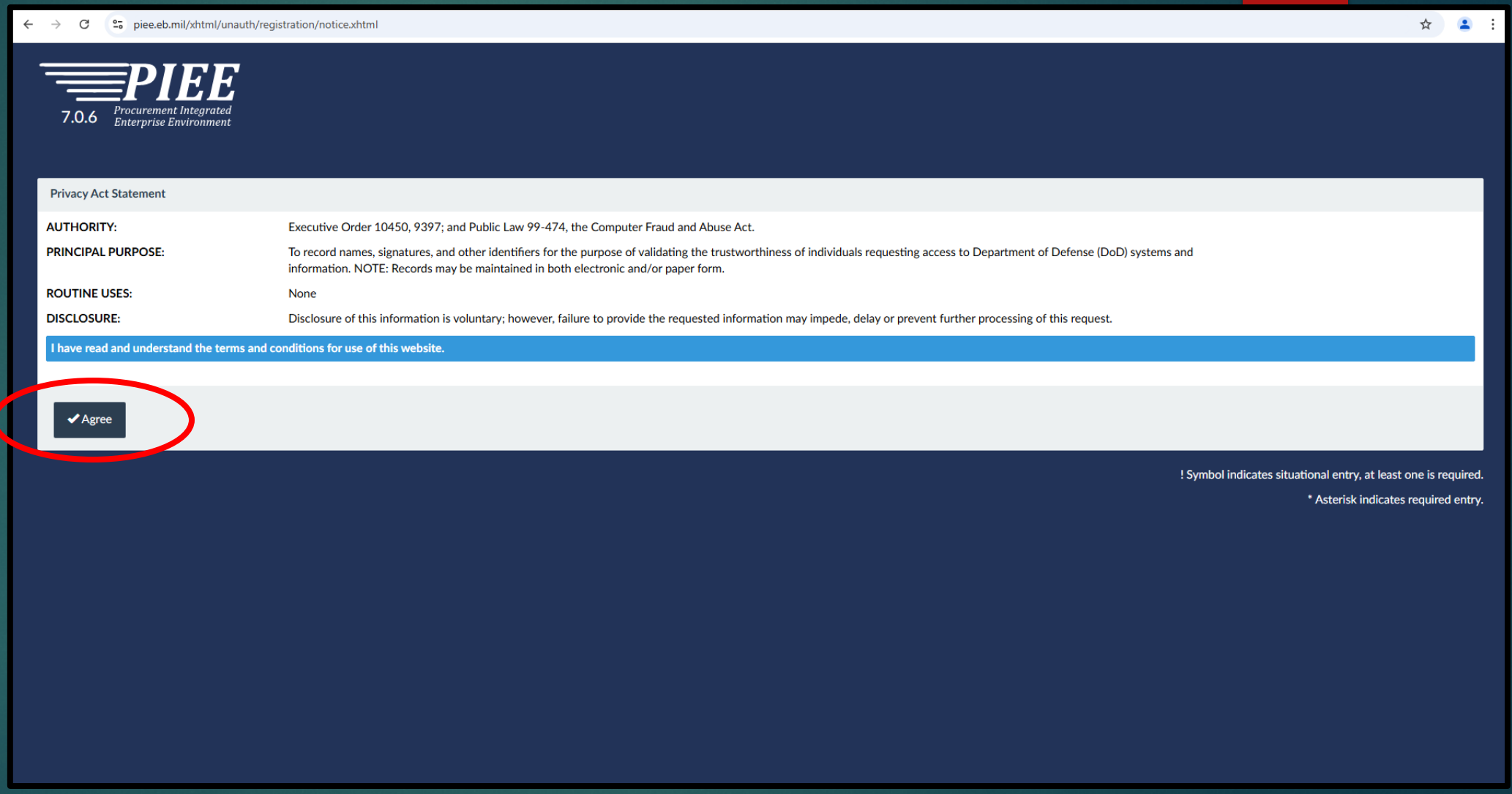
Go to *piee.eb.mil*. Select ‘New User’



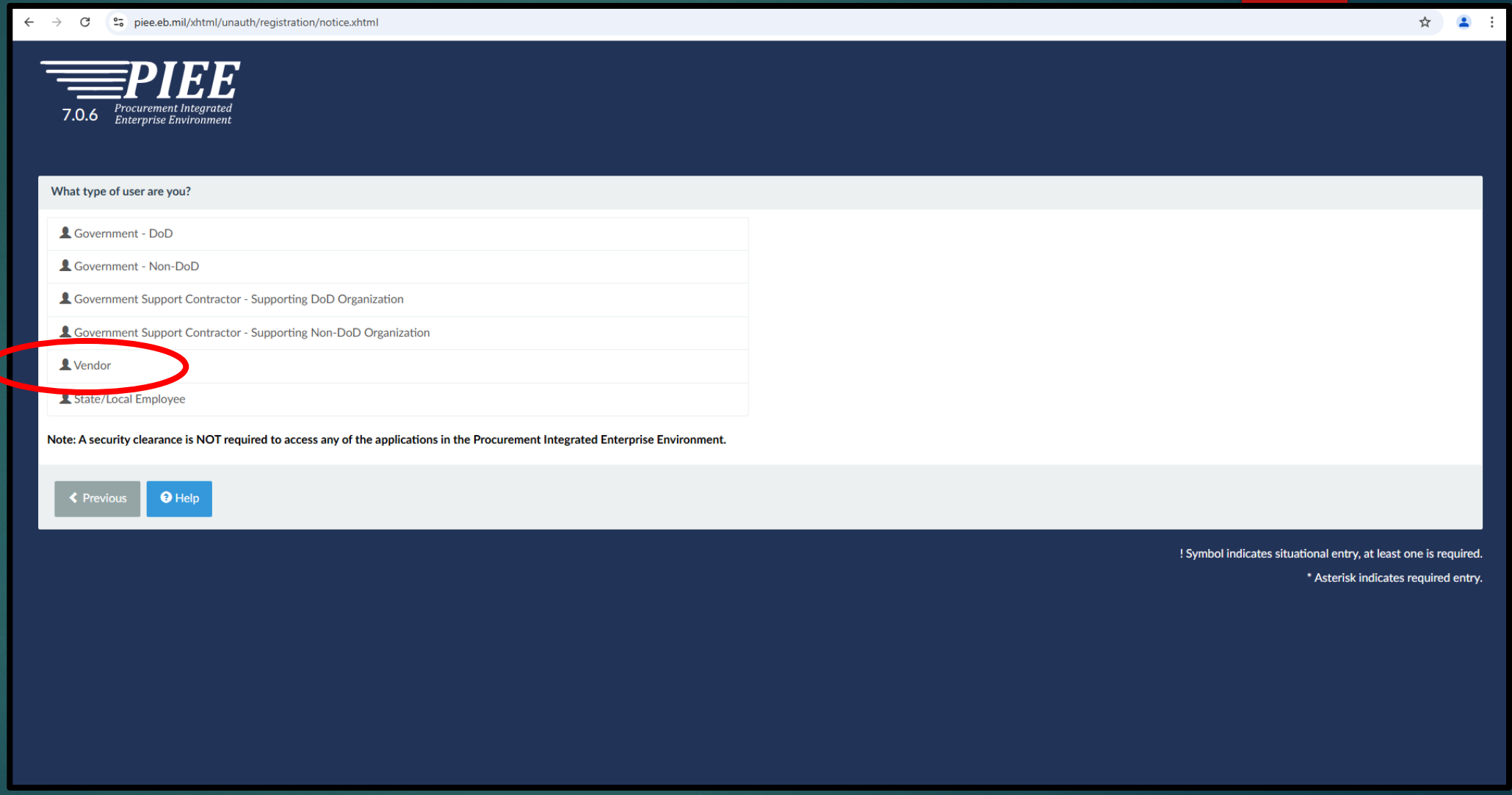
Select ‘Register’. Note that additional resources can be found here



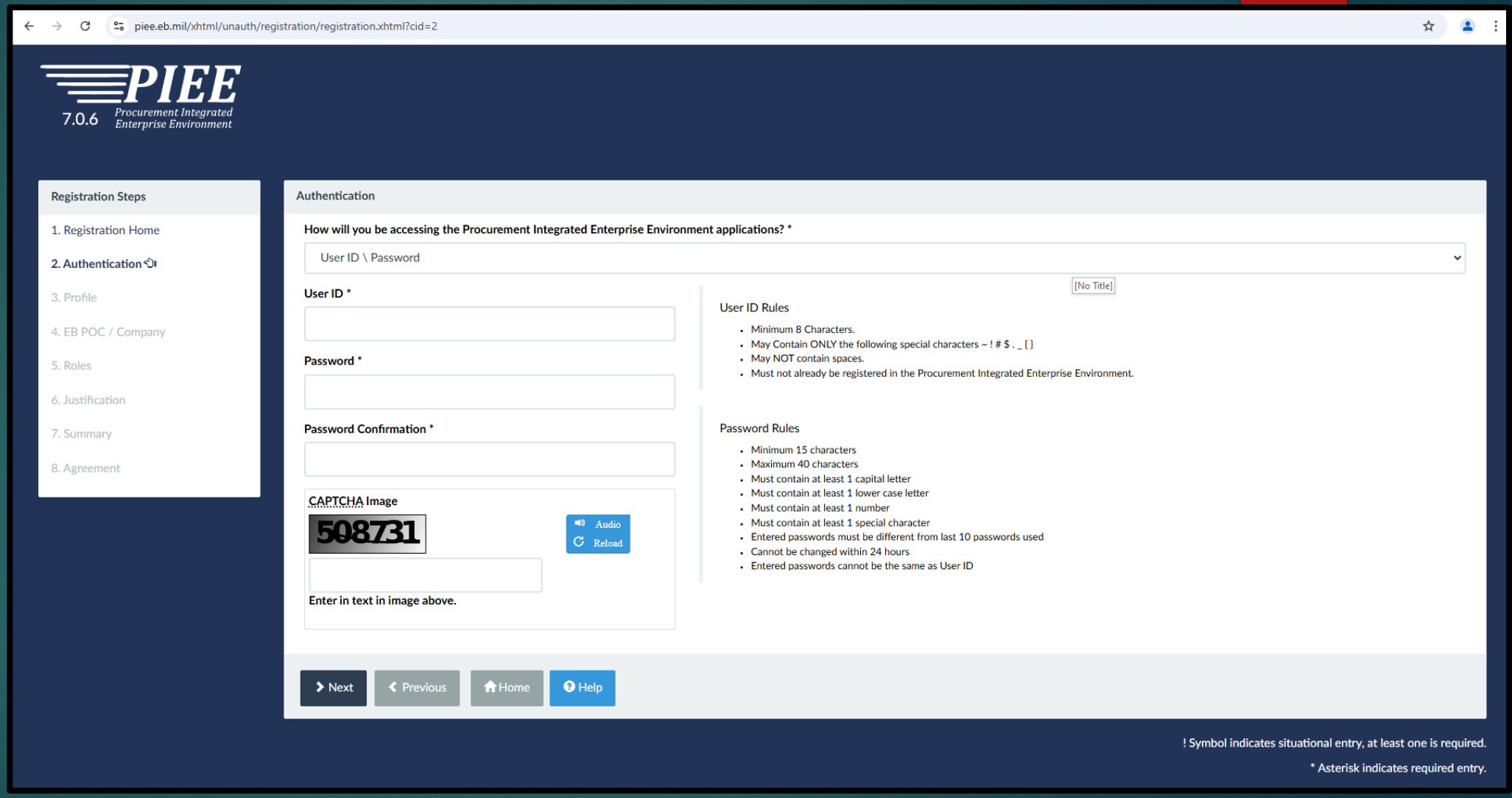
Select ‘Agree’



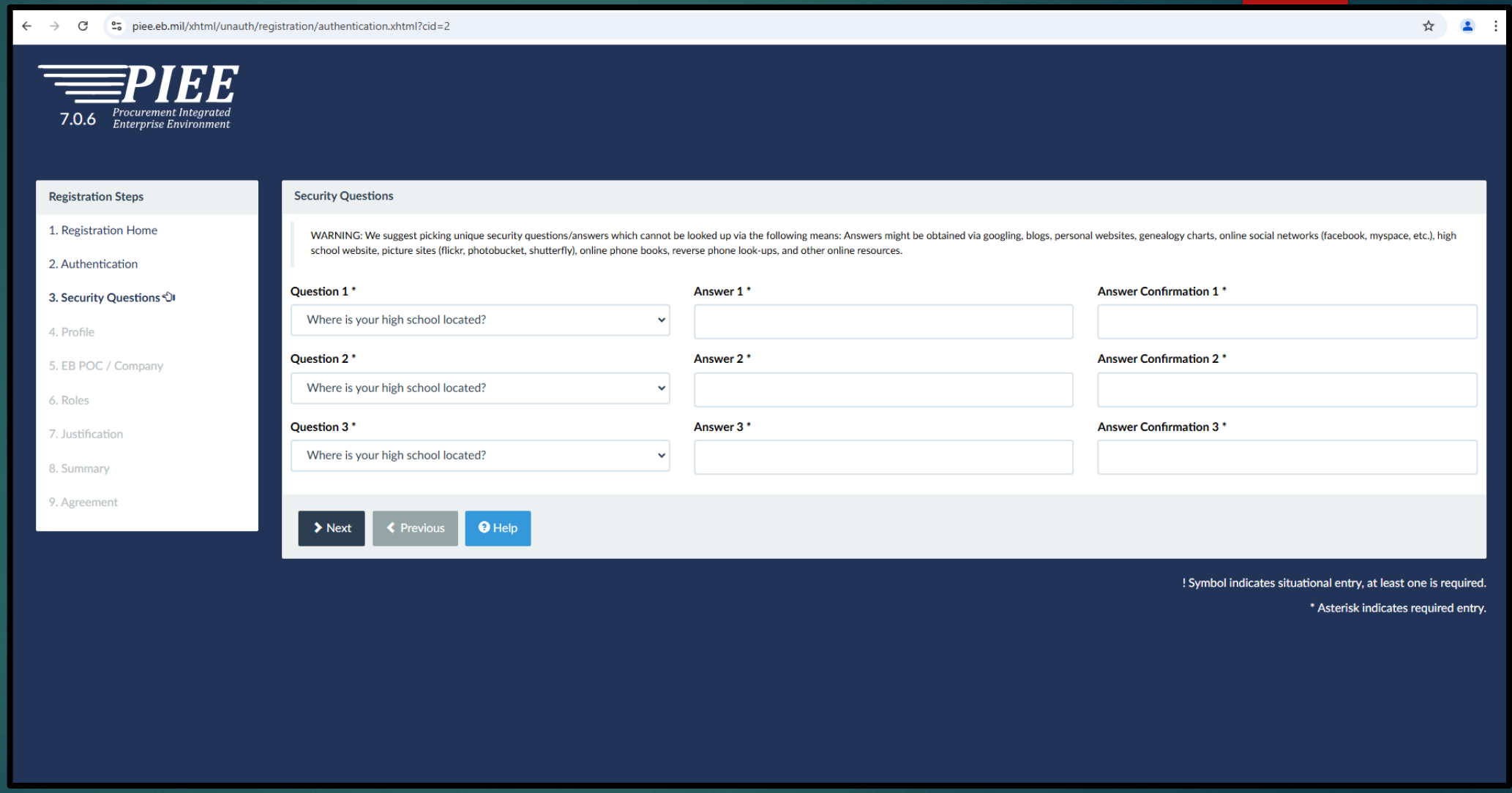
Register as a ‘Vendor’



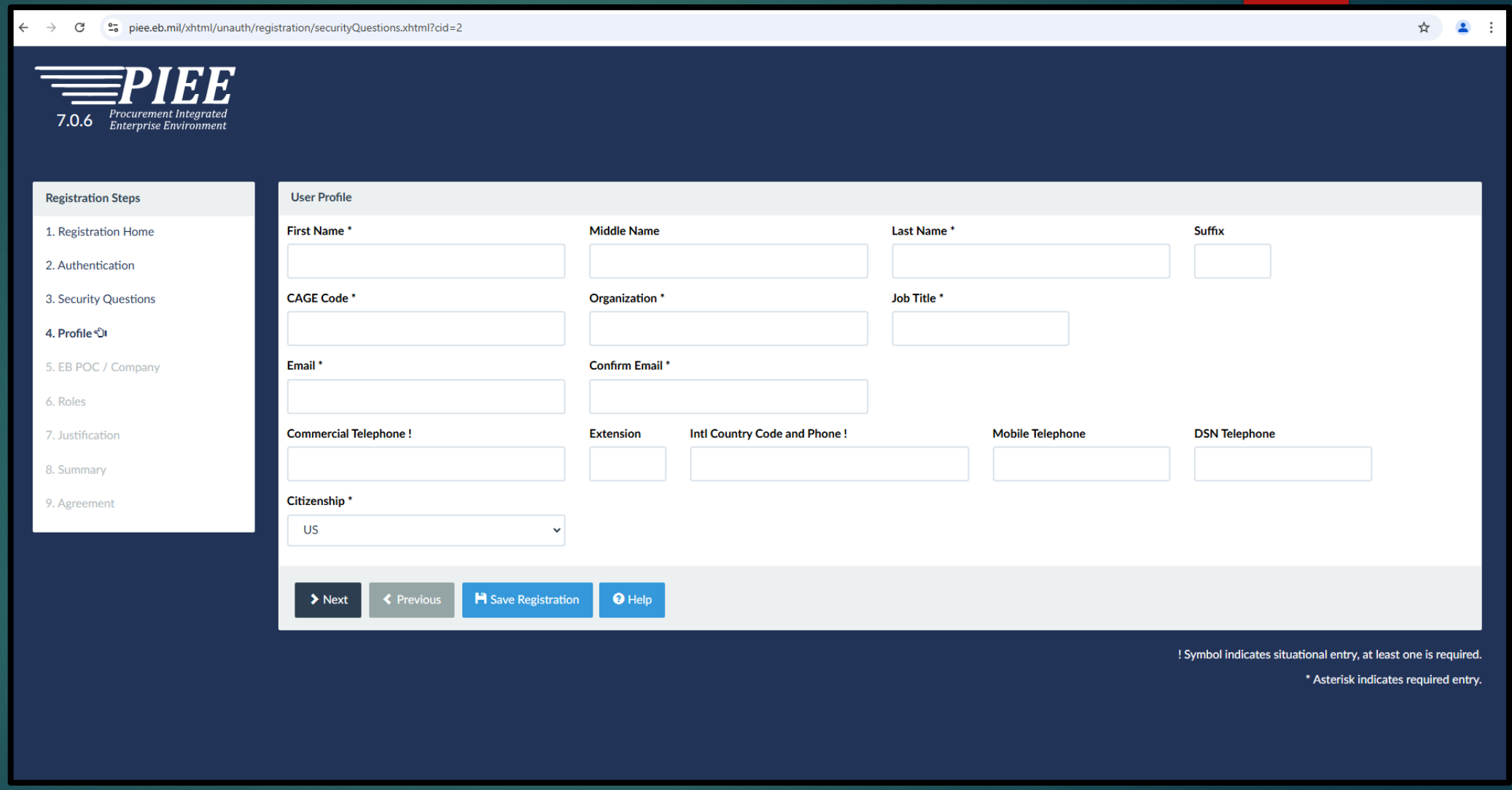
Create User ID and Password (CAC and Software Certificate are also options)



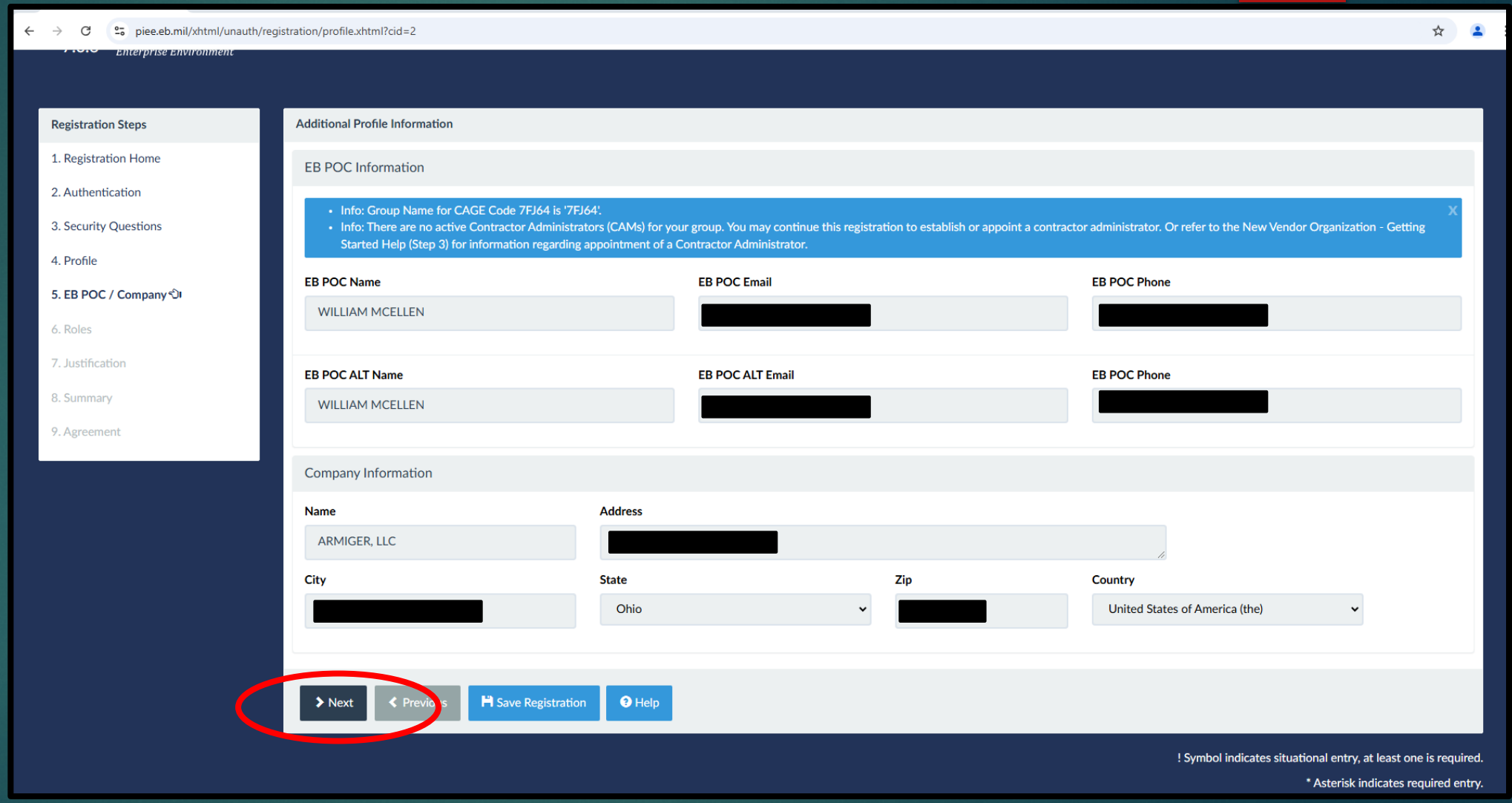
Create Security Questions



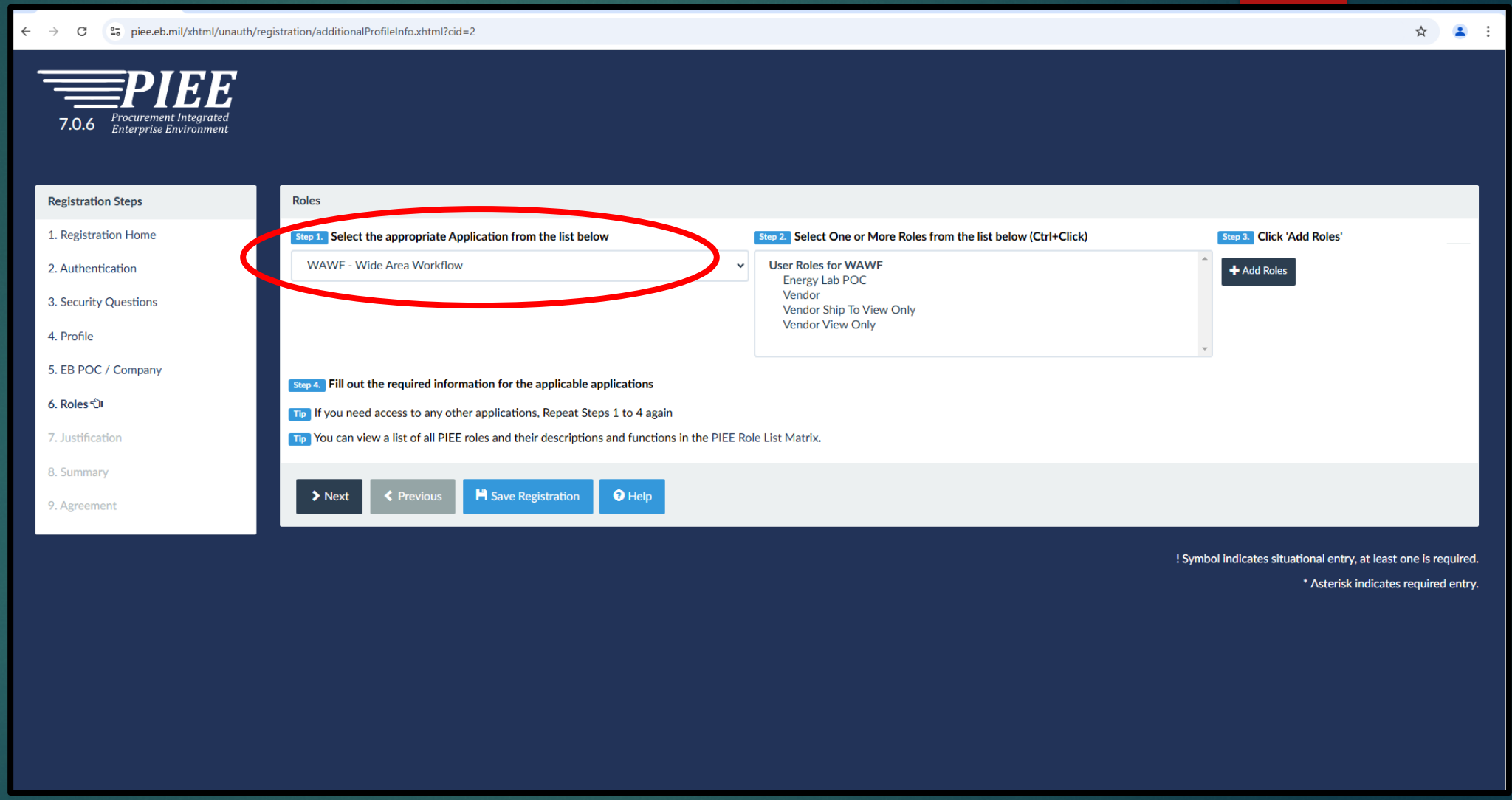
Complete your User Profile



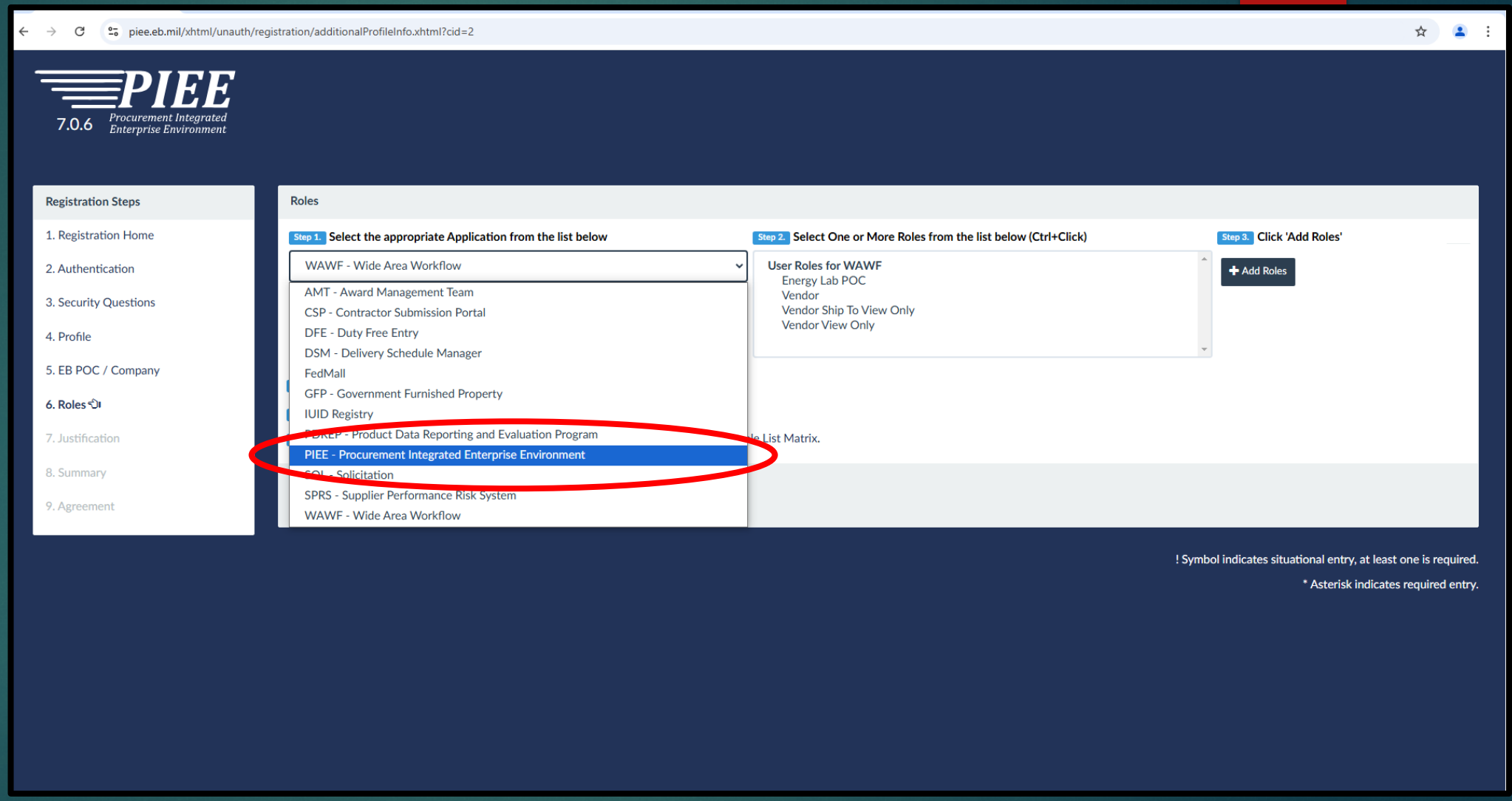
Click >Next


piee.eb.mil/xhtml/unauth/registration/profile.xhtml?cid=2
Enterprise Environment
Registration Steps
1. Registration Home
2. Authentication
3. Security Questions
4. Profile
5. EB POC / Company
6. Roles
7. Justification
8. Summary
9. Agreement
Additional Profile Information
EB POC Information
Info: Group Name for CAGE Code 7FJ64 is '7FJ64'.
Info: There are no active Contractor Administrators (CAMs) for your group. You may continue this registration to establish or appoint a contractor administrator. Or refer to the New Vendor Organization - Getting Started Help (Step 3) for information regarding appointment of a Contractor Administrator.
EB POC Name
WILLIAM MCELLEN
EB POC Email
EB POC Phone
EB POC ALT Name
WILLIAM MCELLEN
EB POC ALT Email
EB POC Phone
Company Information
Name
ARMIGER, LLC
Address
City
State
Ohio
Zip
Country
United States of America (the)
Next
Previous
Save Registration
Help
! Symbol indicates situational entry, at least one is required.
* Asterisk indicates required entry.

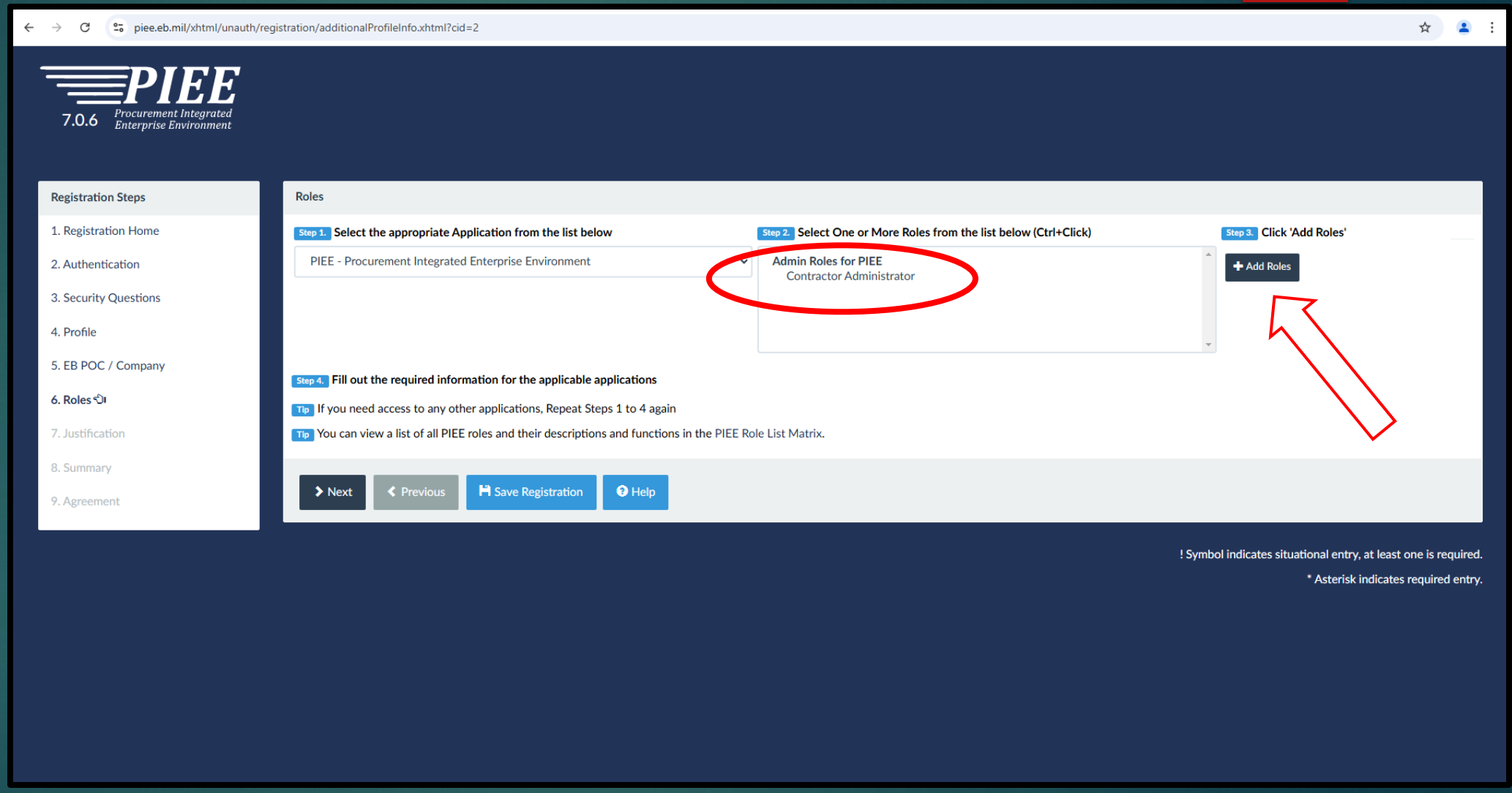
Select drop-down under Step 1



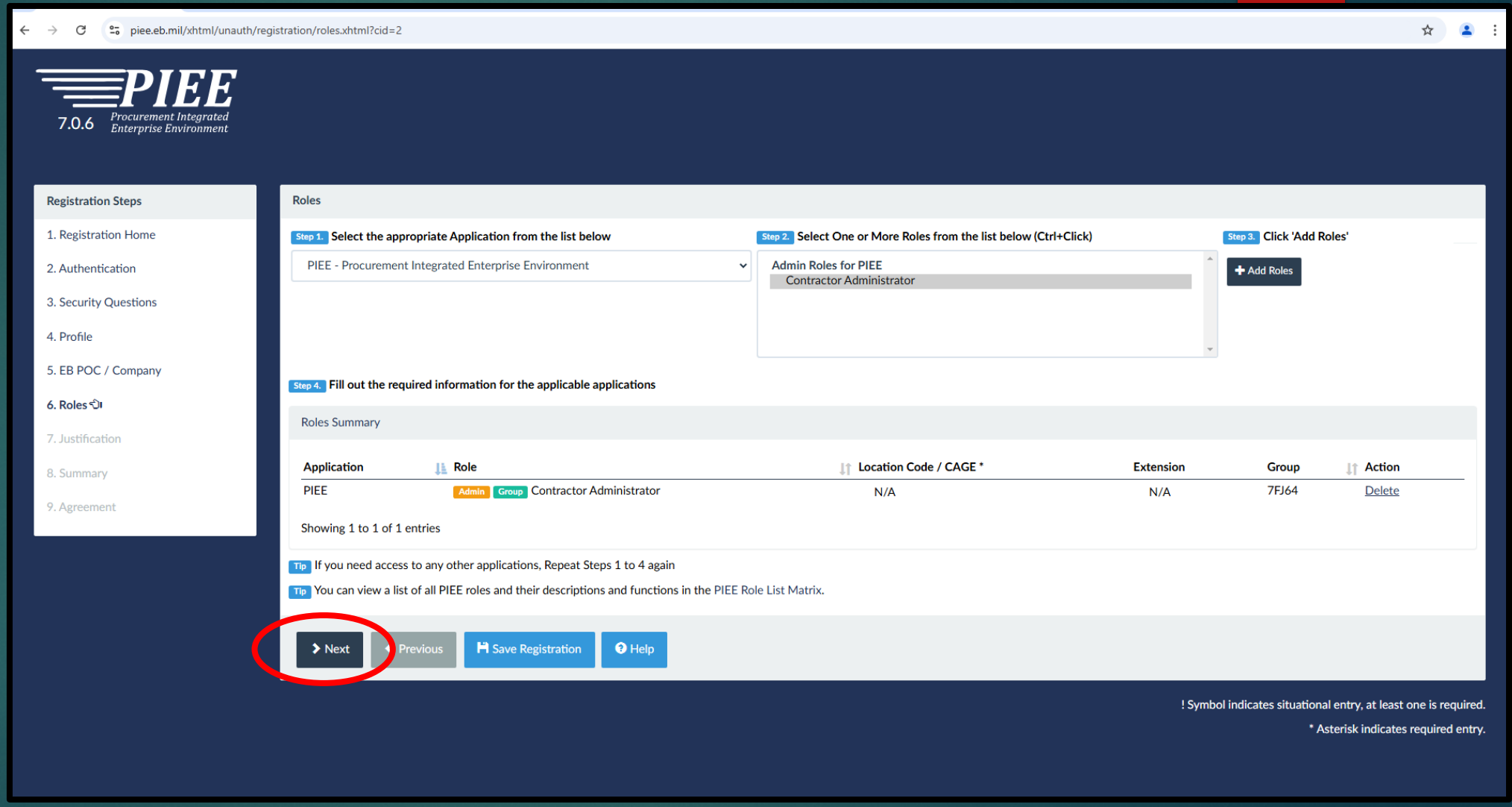
Select ‘PIEE – Procurement Integrated Enterprise Environment’



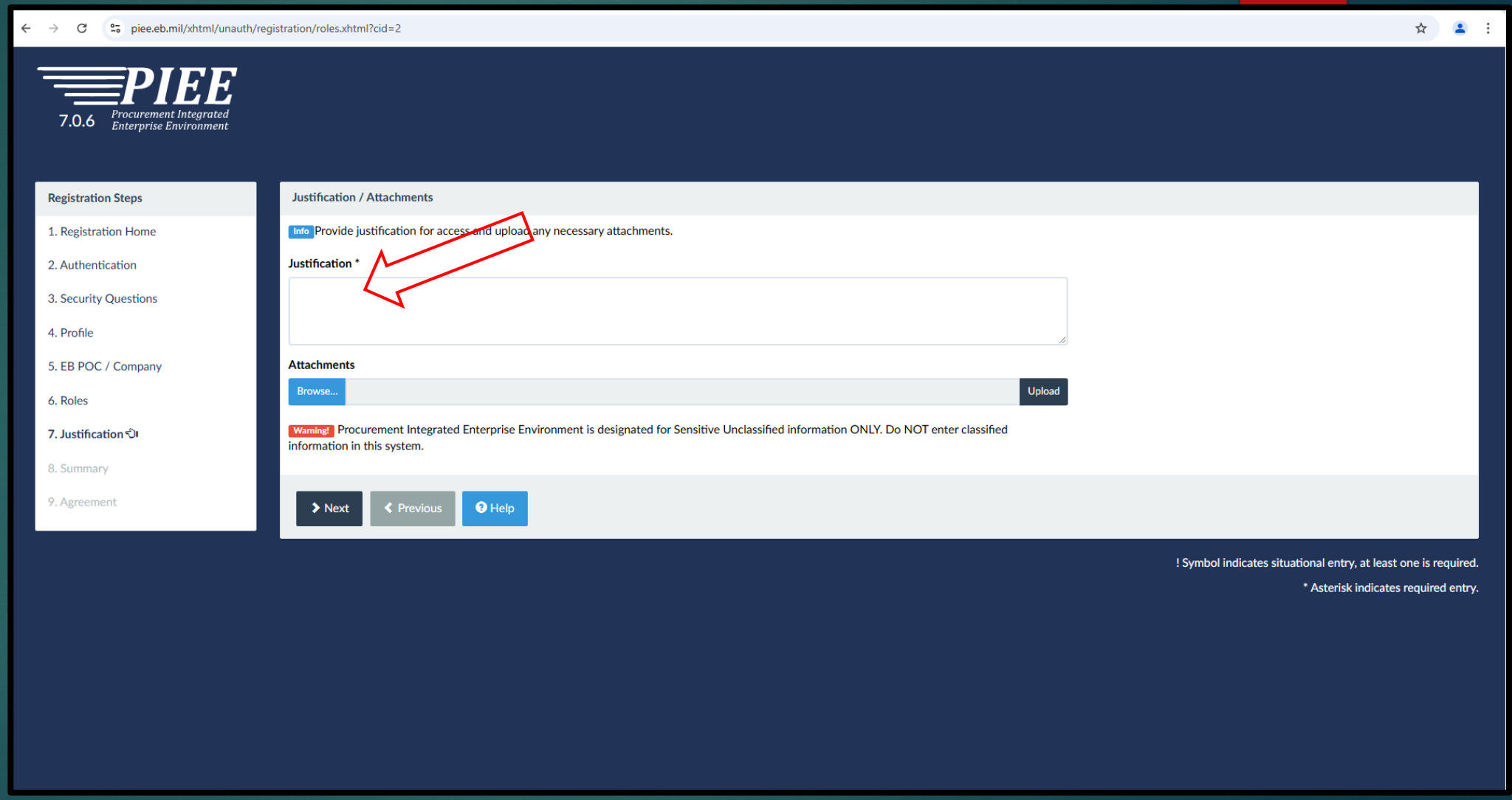
Select ‘Contract Administrator’ under Step 2 then click ‘+ Add Roles’



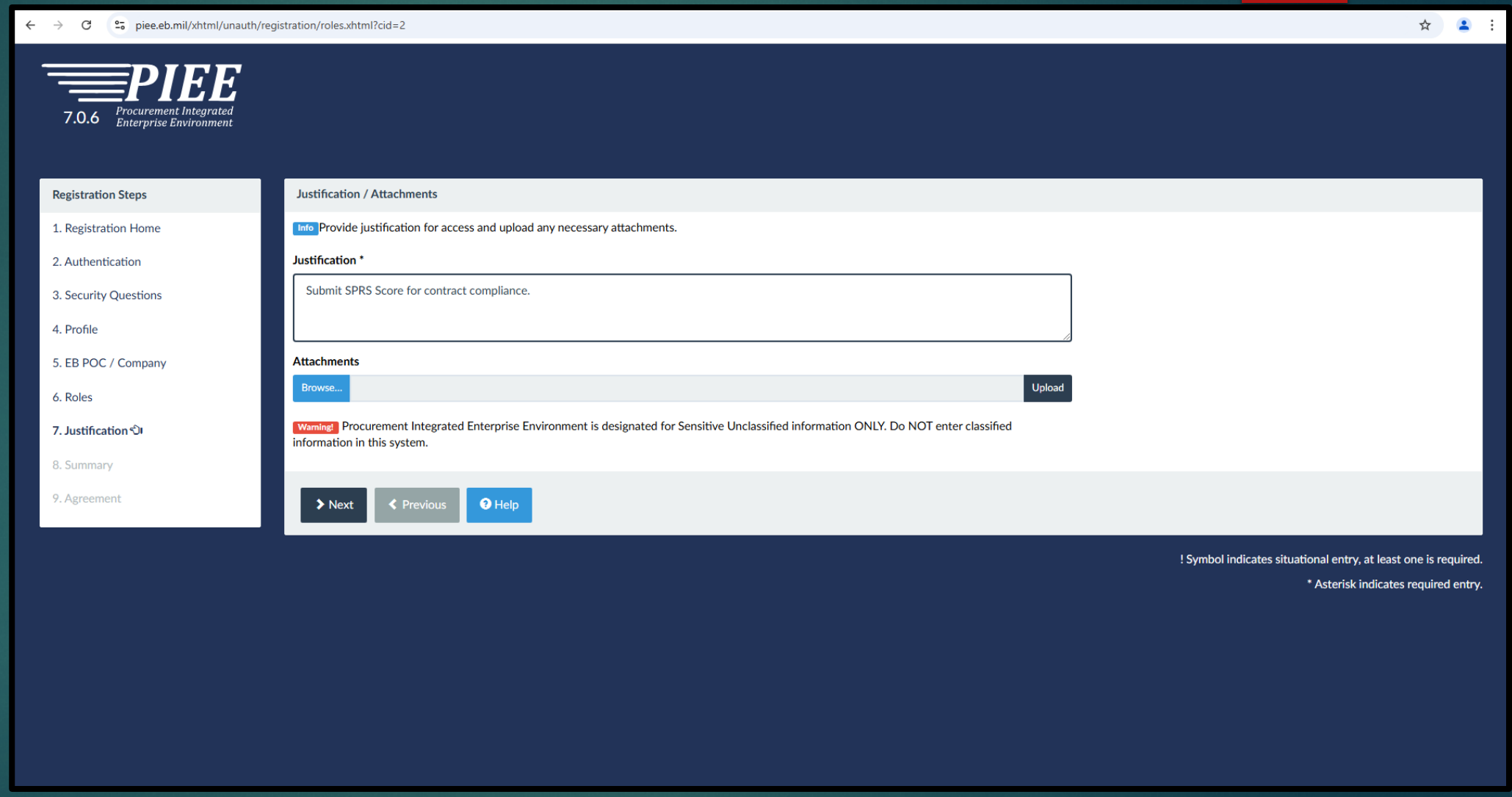
Step 4 should auto-fill. No changes possible. Click >Next



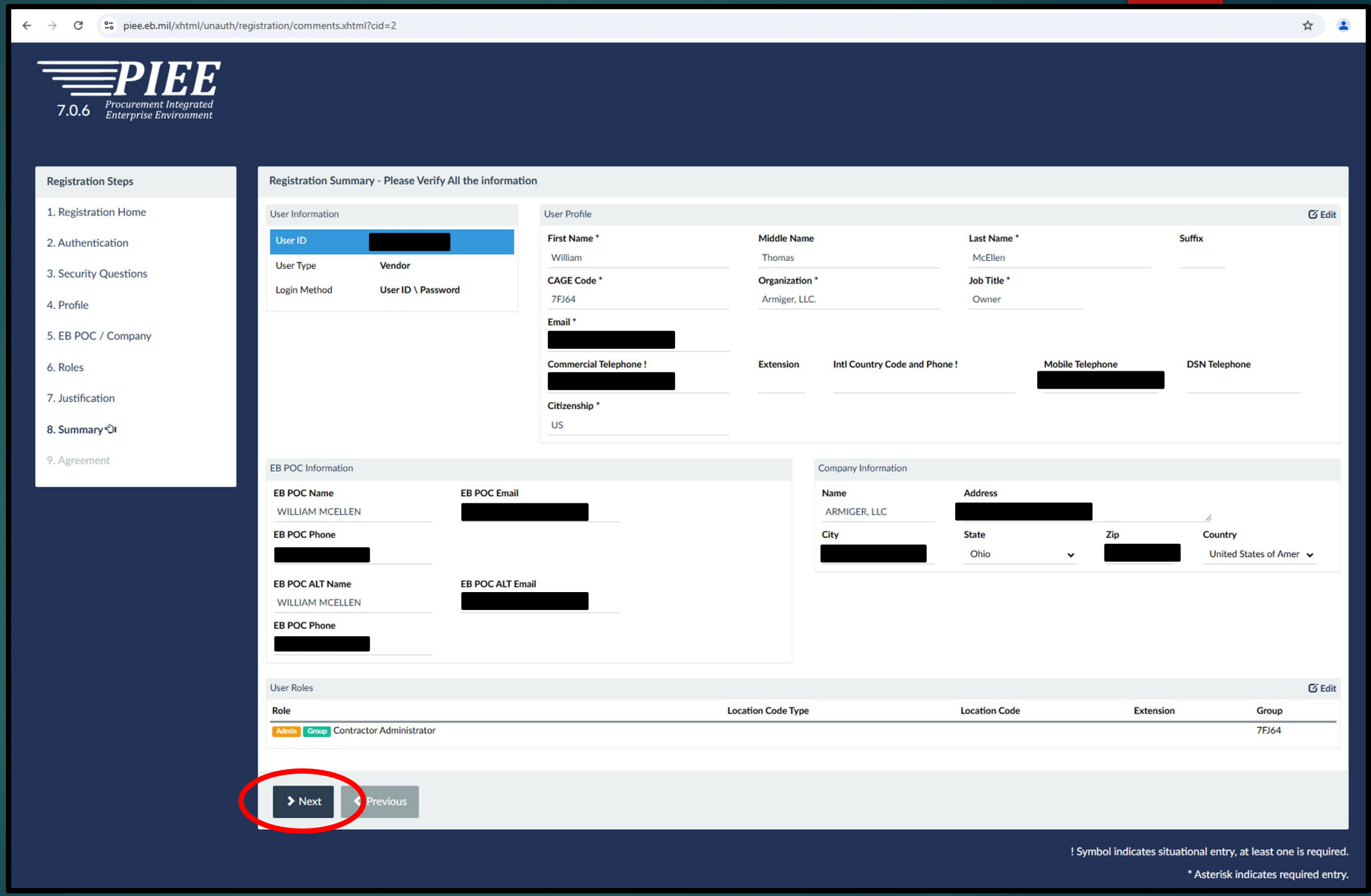
Provide a Justification – anything will do



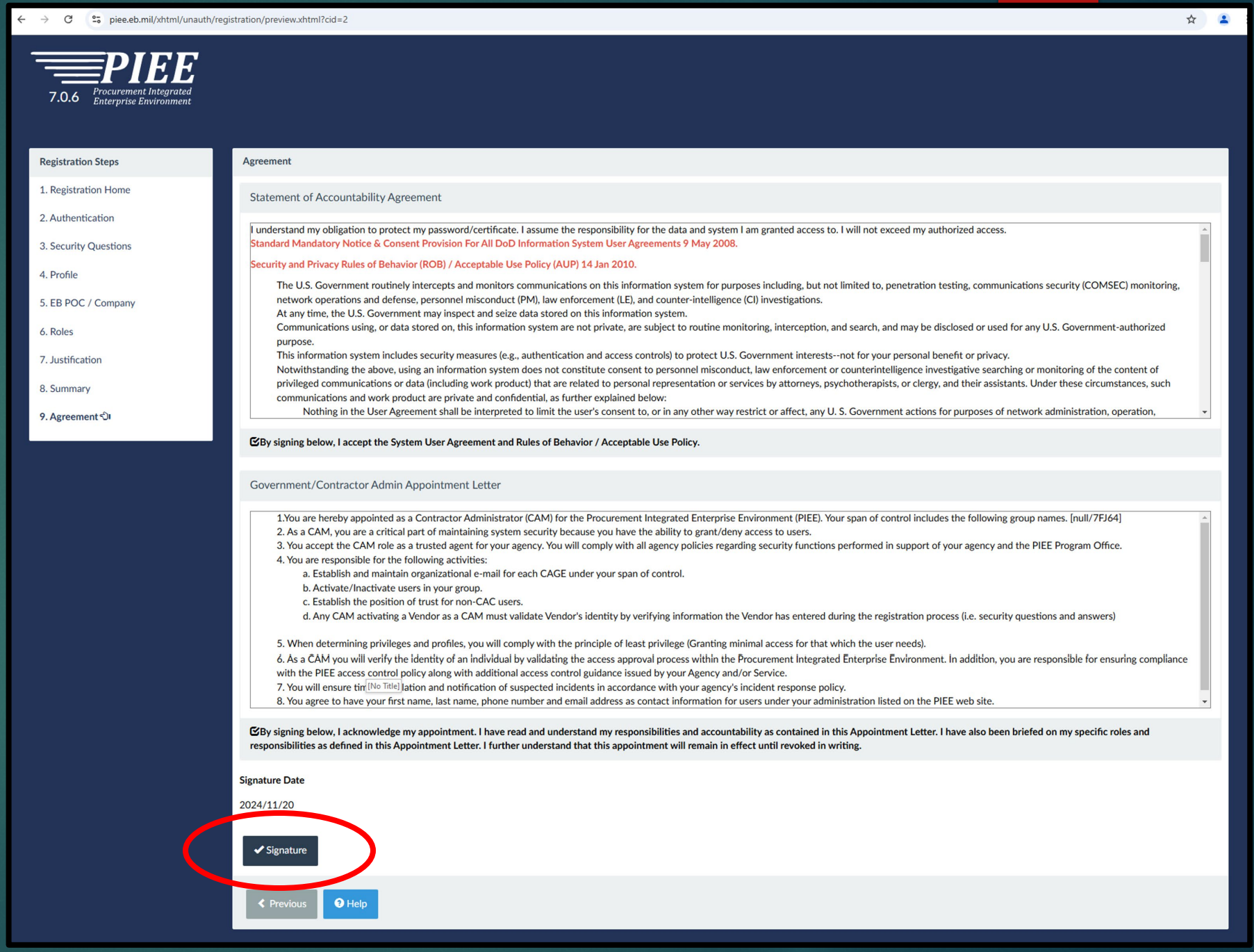
Sample Justification: *Submit SPRS Score for contract compliance*. Then >Next



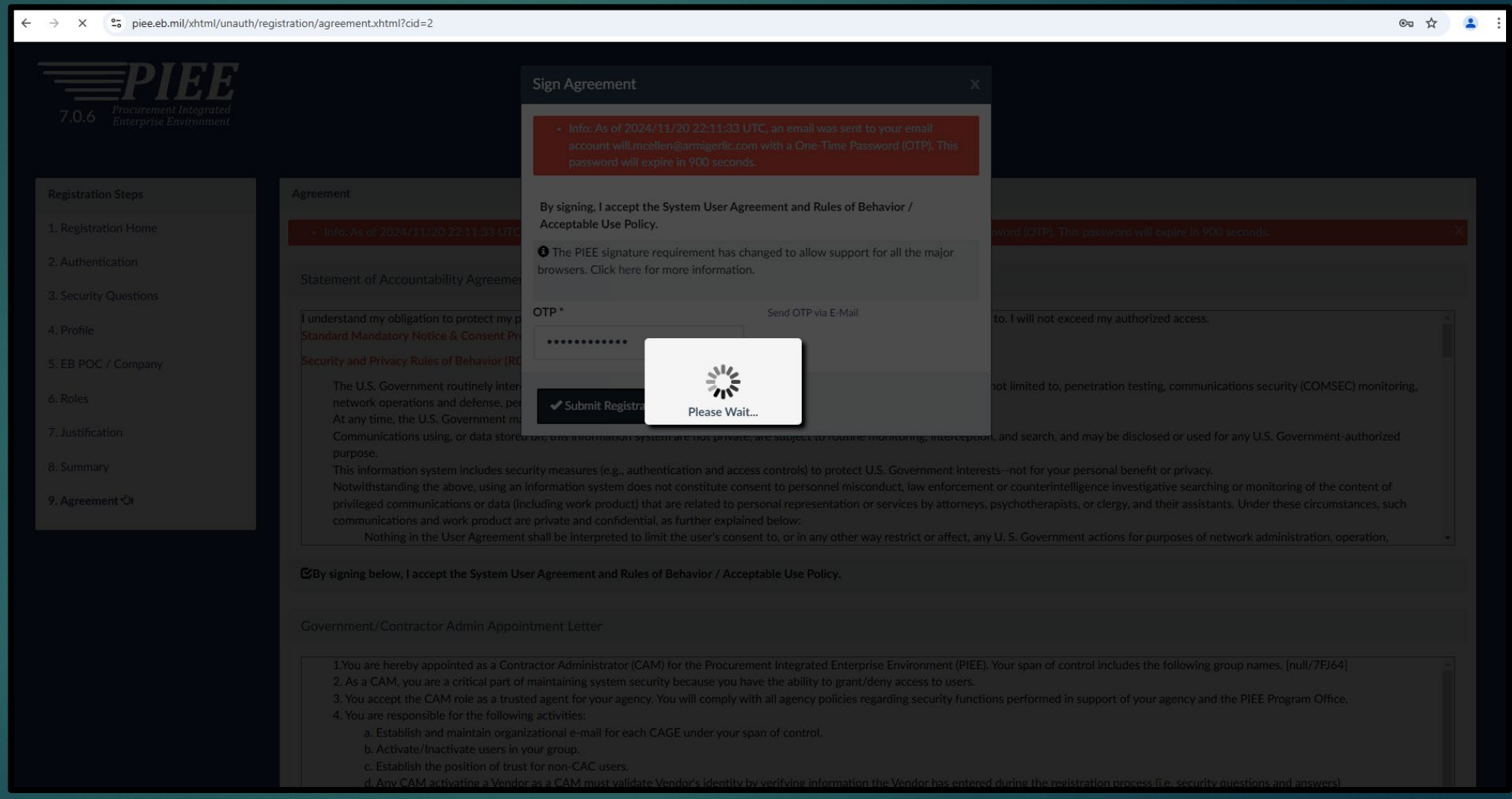
Review Info
then click >Next



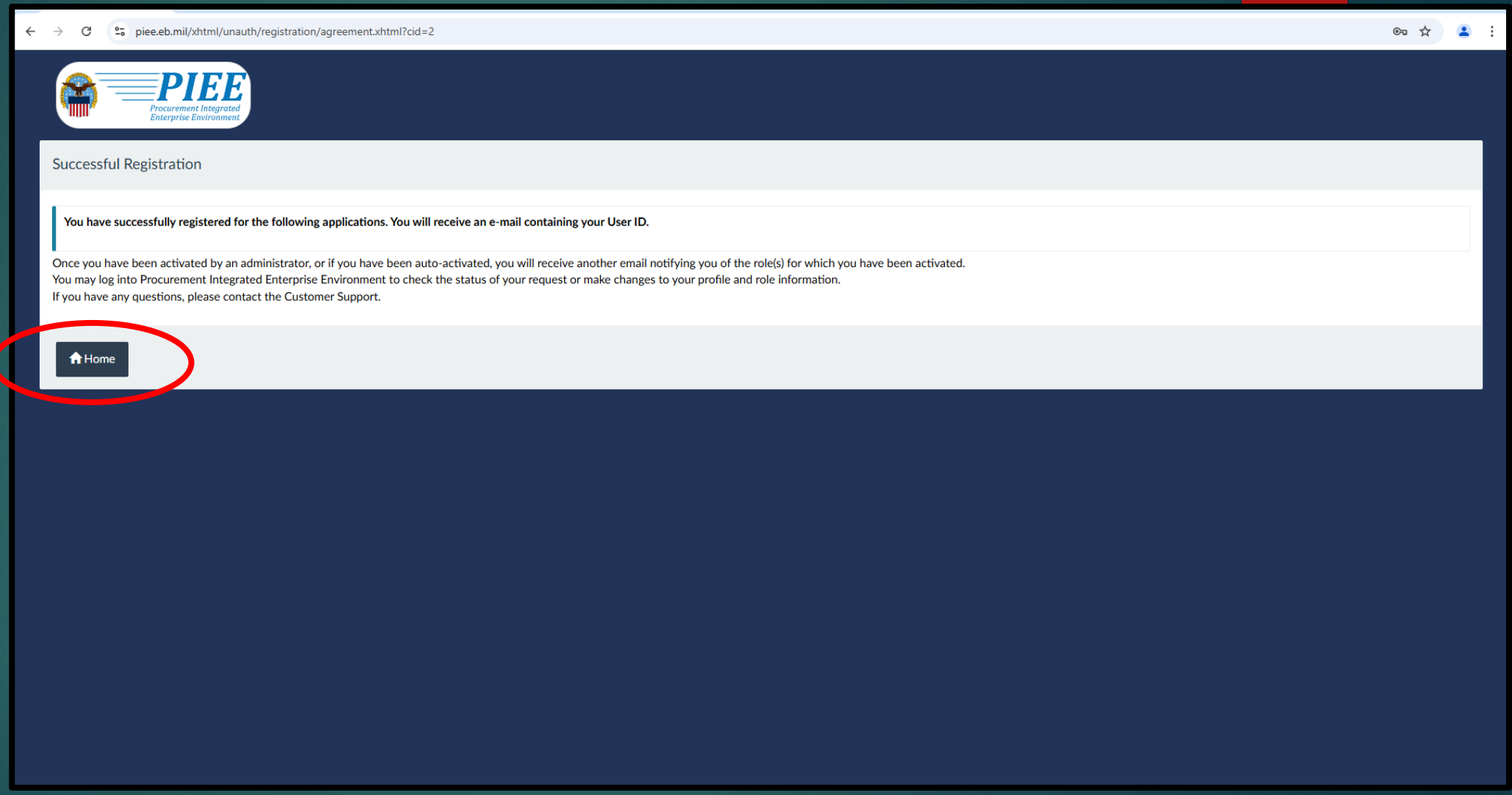
Review and click ‘Signature’



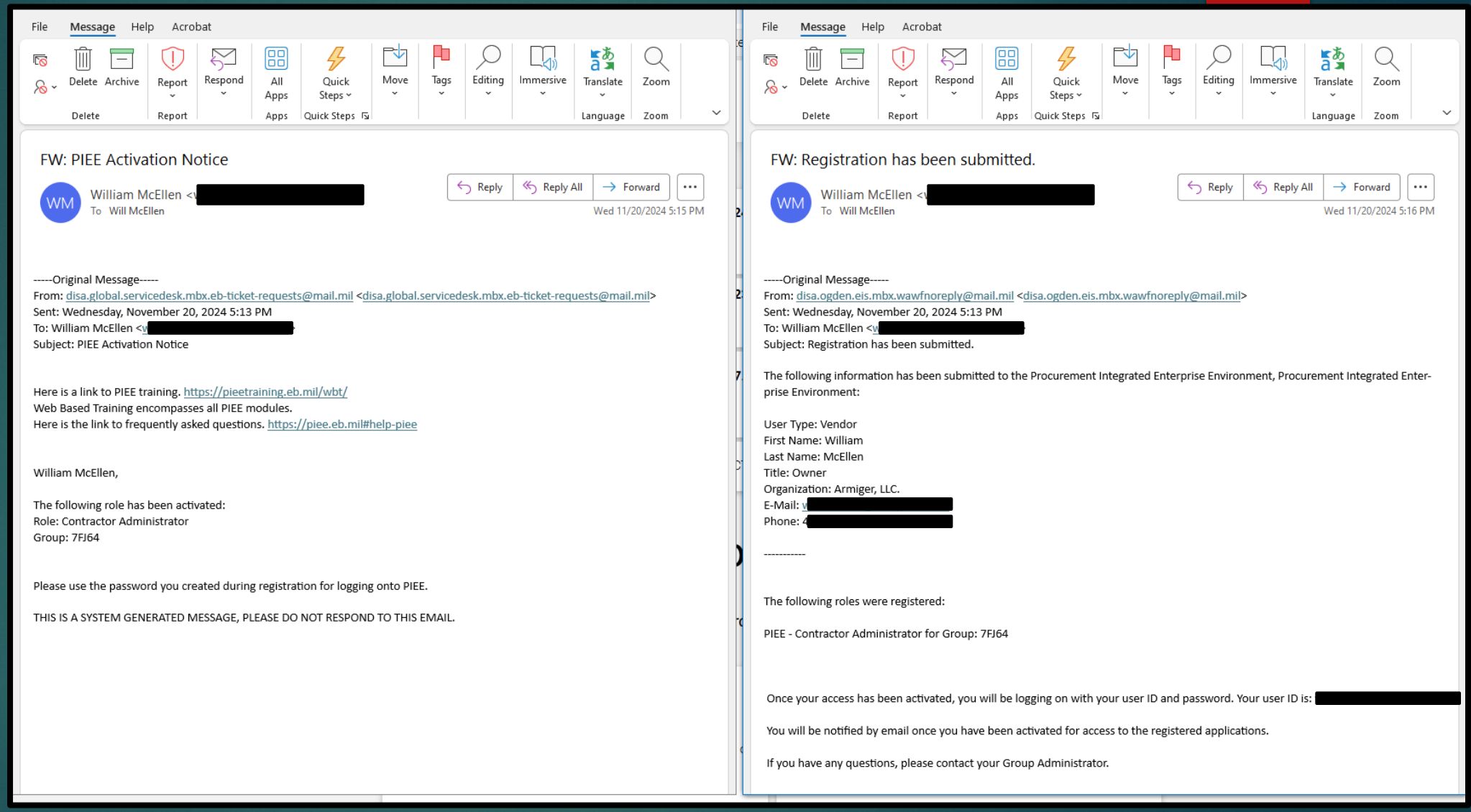
Check e-mail for One-Time Password. Submit Registration



Registration Complete. Click Home to return to the main PIEE page



You should be receiving Activation and Registration notices via e-mail



File Message Help Acrobat

Delete Archive Report Respond All Apps Quick Steps Move Tags Editing Immersive Translate Zoom

Delete Report Apps Quick Steps Language Zoom

FW: PIEE Activation Notice

WM William McEllen <[redacted]
To Will McEllen

Reply Reply All Forward

Wed 11/20/2024 5:15 PM

-----Original Message-----
From: disa.global.servicedesk.mbx.eb-ticket-requests@mail.mil <disa.global.servicedesk.mbx.eb-ticket-requests@mail.mil>
Sent: Wednesday, November 20, 2024 5:13 PM
To: William McEllen <[redacted]
Subject: PIEE Activation Notice

Here is a link to PIEE training. https://pieetraining.eb.mil/wbt/
Web Based Training encompasses all PIEE modules.
Here is the link to frequently asked questions. https://piee.eb.mil#help-piee

William McEllen,

The following role has been activated:
Role: Contractor Administrator
Group: 7FJ64

Please use the password you created during registration for logging onto PIEE.

THIS IS A SYSTEM GENERATED MESSAGE, PLEASE DO NOT RESPOND TO THIS EMAIL.

File Message Help Acrobat

Delete Archive Report Respond All Apps Quick Steps Move Tags Editing Immersive Translate Zoom

Delete Report Apps Quick Steps Language Zoom

FW: Registration has been submitted.

WM William McEllen <[redacted]
To Will McEllen

Reply Reply All Forward

Wed 11/20/2024 5:16 PM

-----Original Message-----
From: disa.ogden.eis.mbx.wawfnoreply@mail.mil <disa.ogden.eis.mbx.wawfnoreply@mail.mil>
Sent: Wednesday, November 20, 2024 5:13 PM
To: William McEllen <[redacted]
Subject: Registration has been submitted.

The following information has been submitted to the Procurement Integrated Enterprise Environment, Procurement Integrated Enterprise Environment:

User Type: Vendor
First Name: William
Last Name: McEllen
Title: Owner
Organization: Armiger, LLC.
E-Mail: [redacted]
Phone: [redacted]

The following roles were registered:

PIEE - Contractor Administrator for Group: 7FJ64

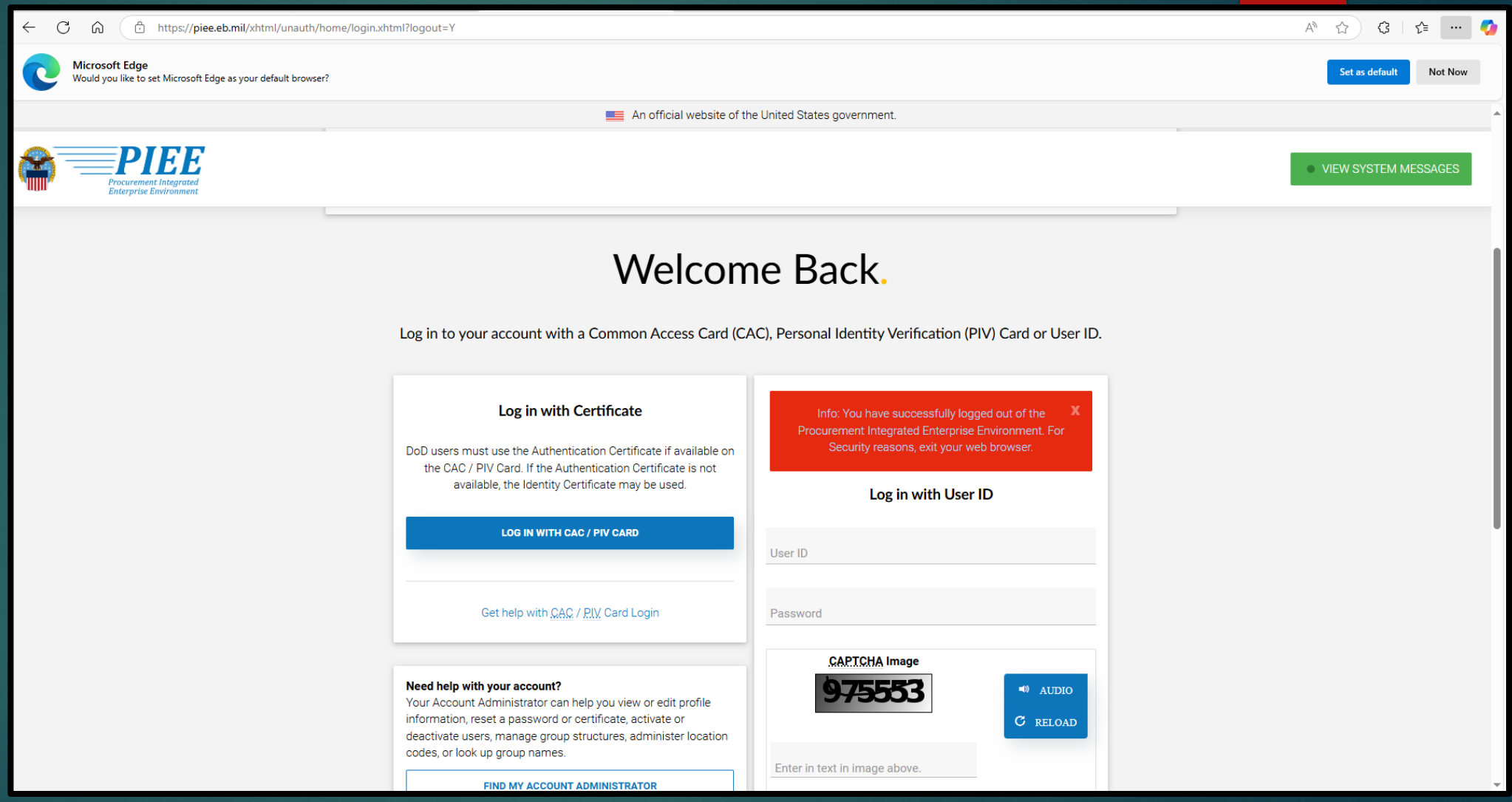
Once your access has been activated, you will be logging on with your user ID and password. Your user ID is: [redacted]

You will be notified by email once you have been activated for access to the registered applications.

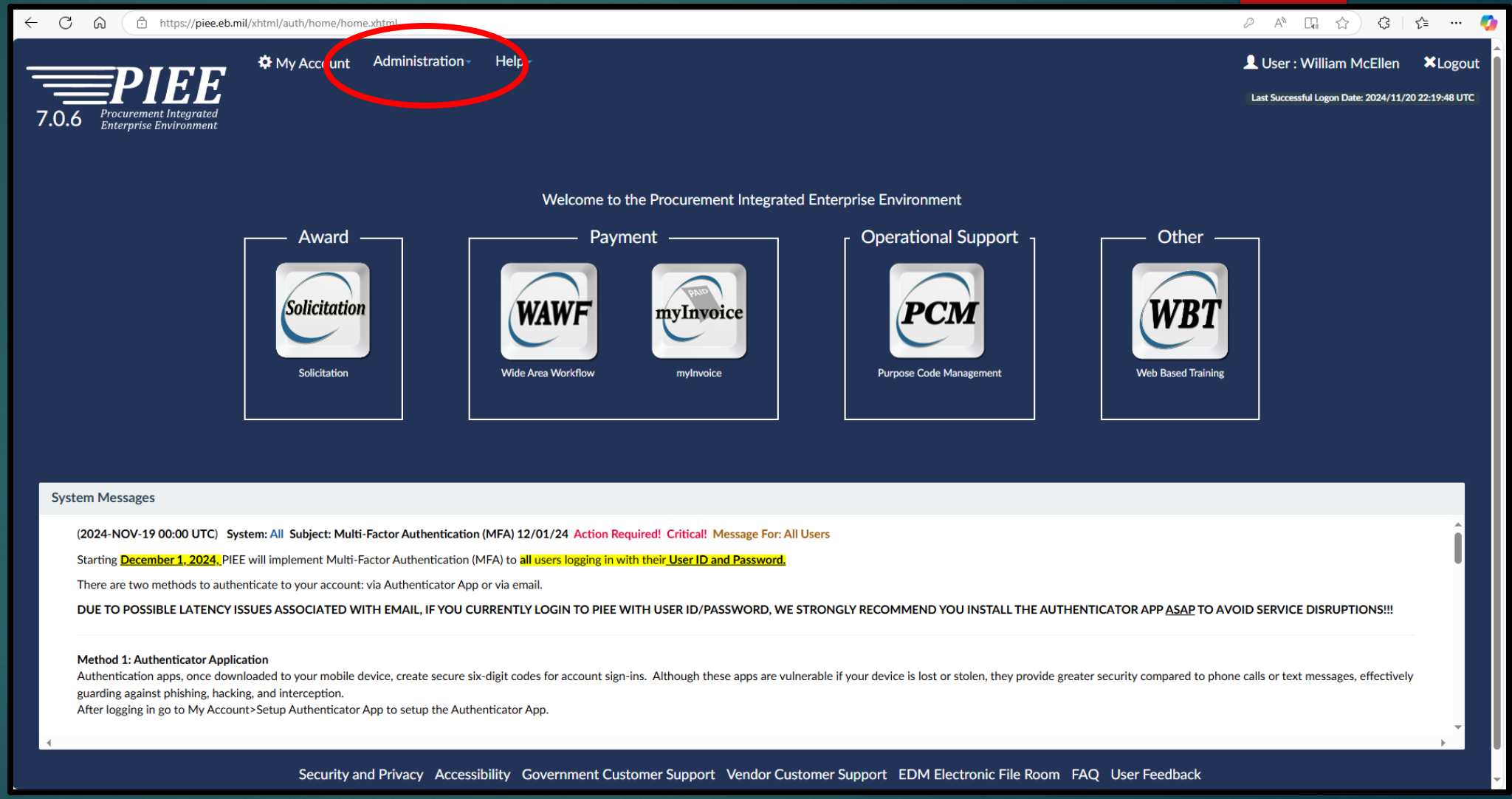
If you have any questions, please contact your Group Administrator.

Part 2 - Login and SPRS

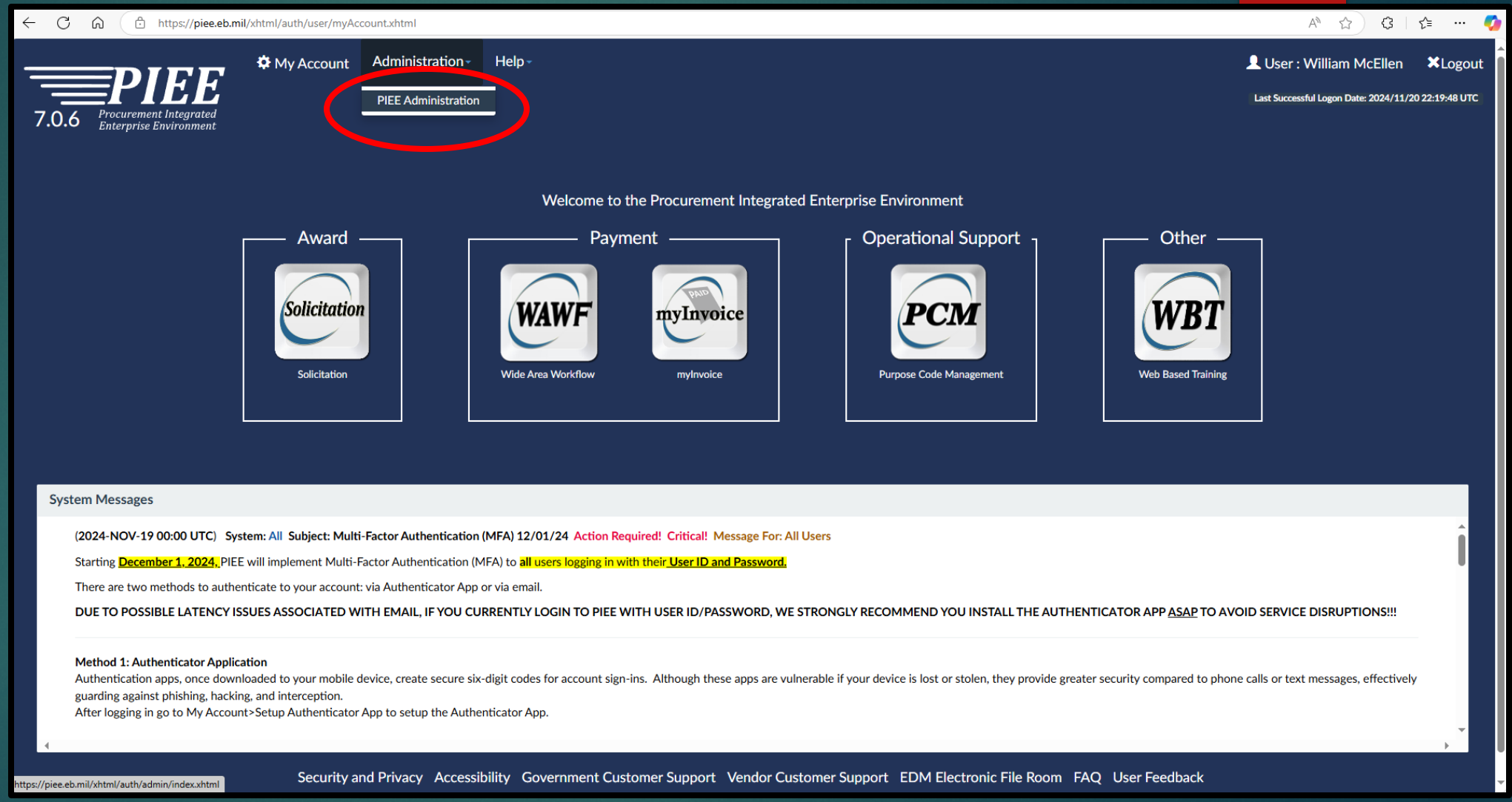
Return to piee.eb.mil. You can now log in with your Username and Password



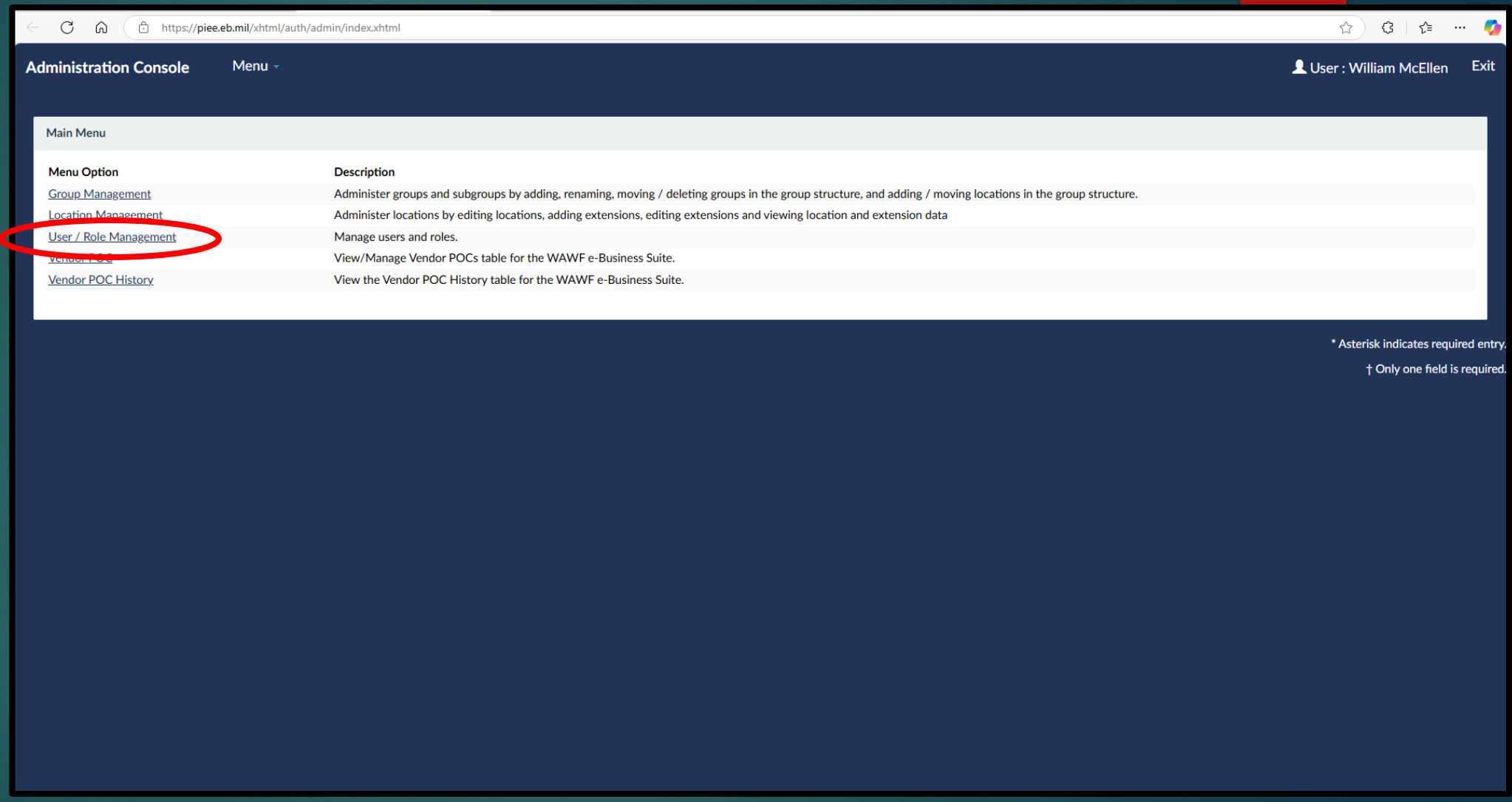
Select ‘Administration’ drop-down



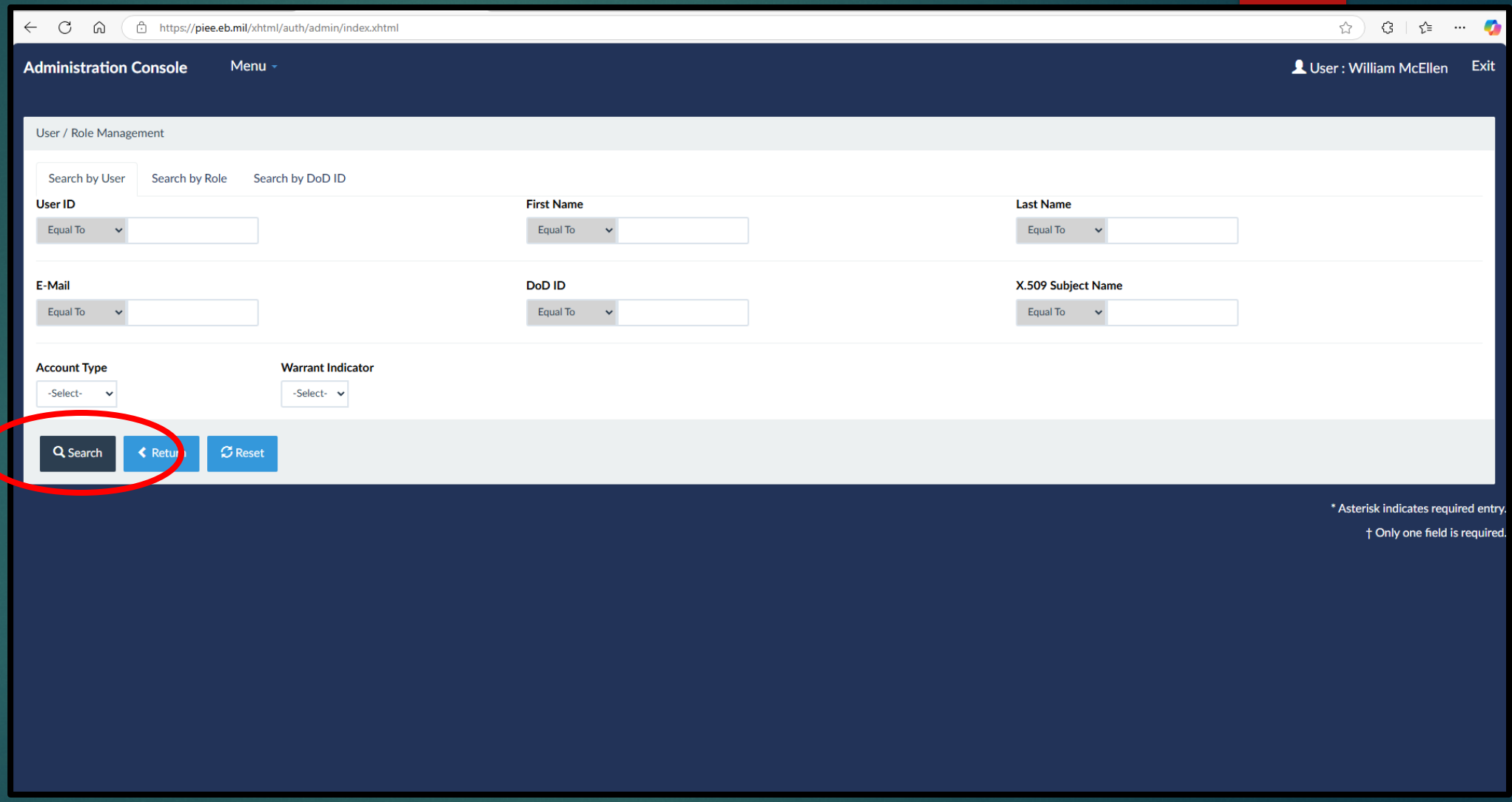
Select ‘PIEE Administration’



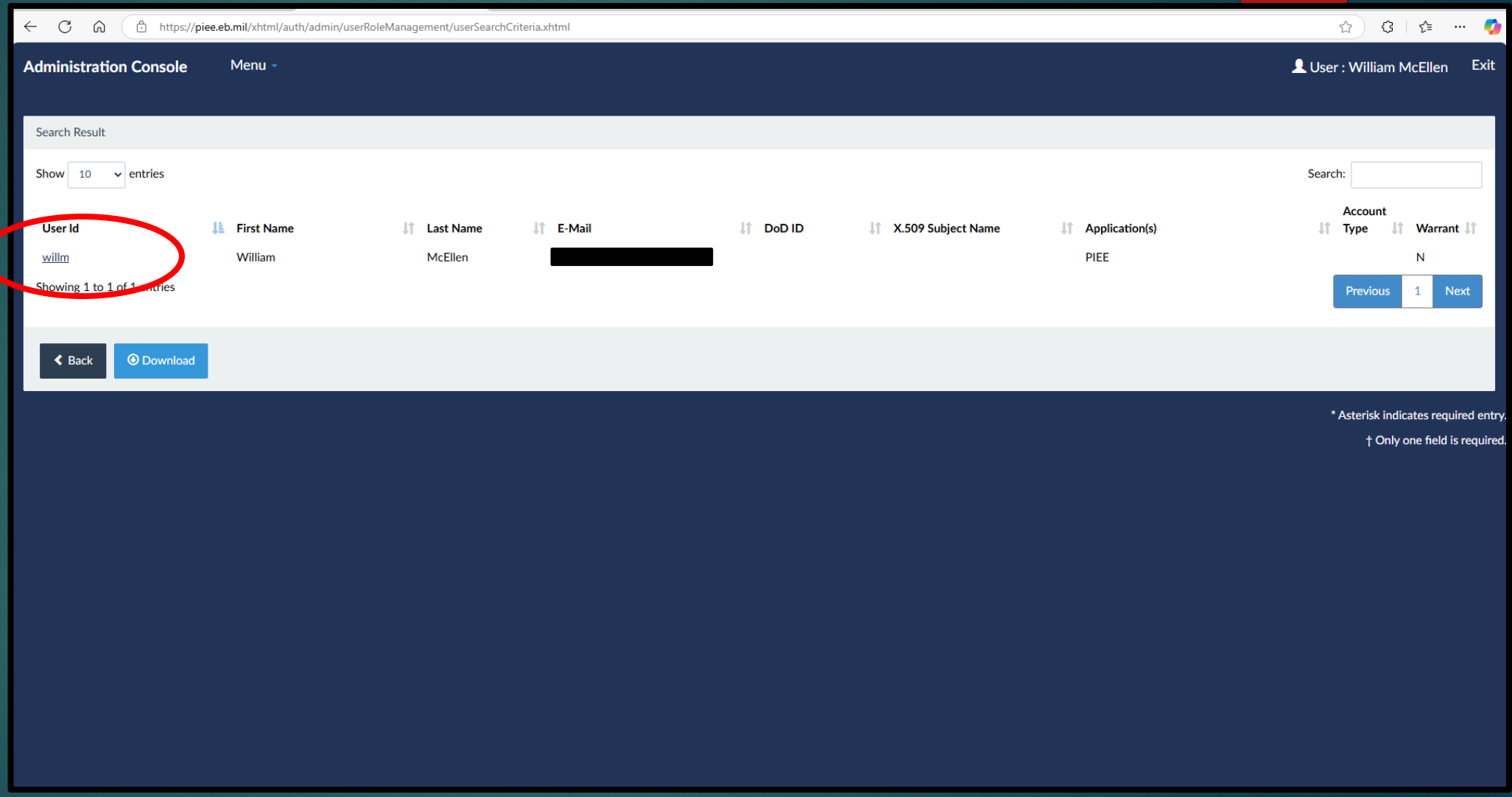
Select ‘User/Role Management’



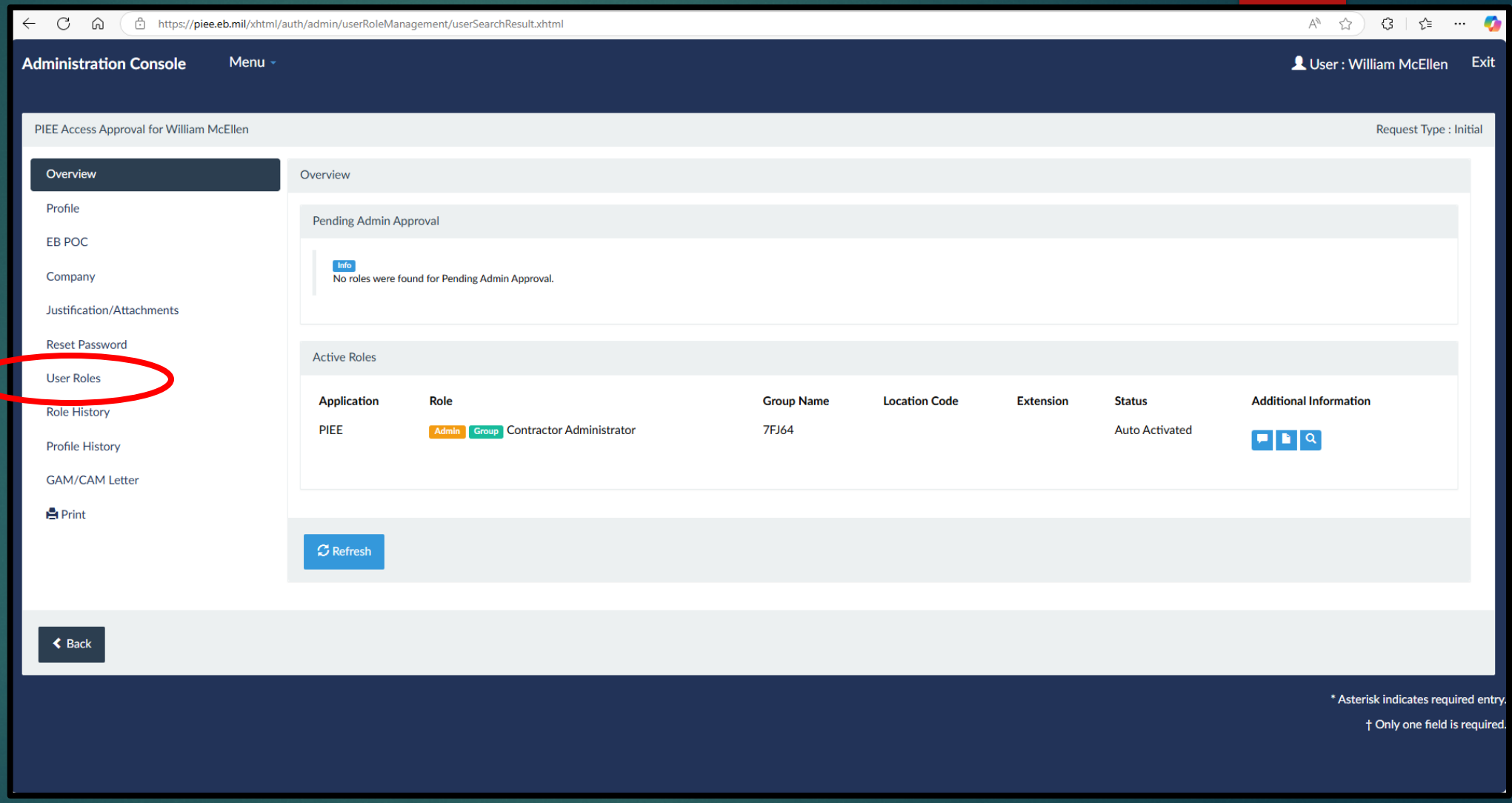
Select ‘Search’



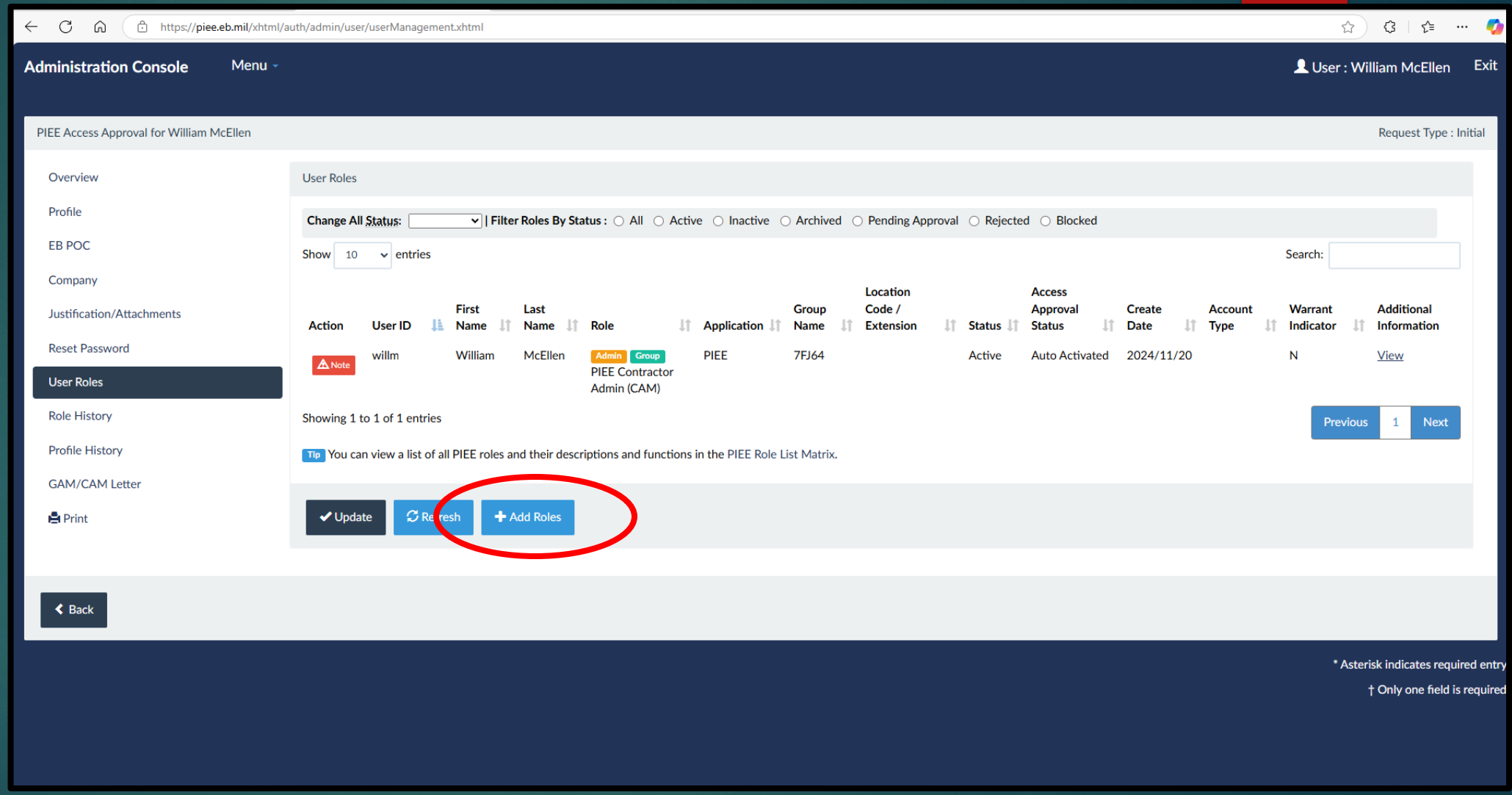
Select your ‘User ID’



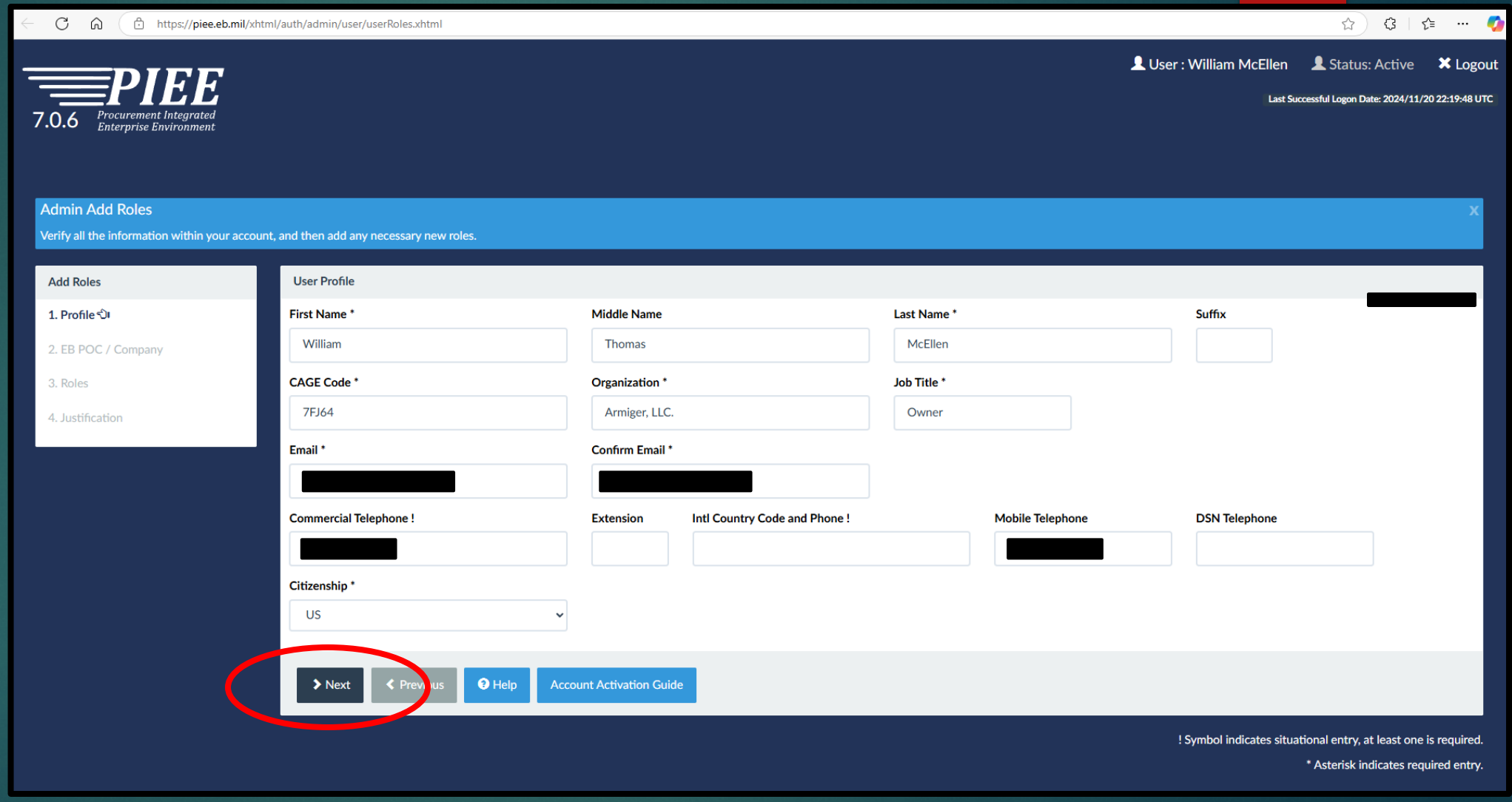
Select ‘User Roles’



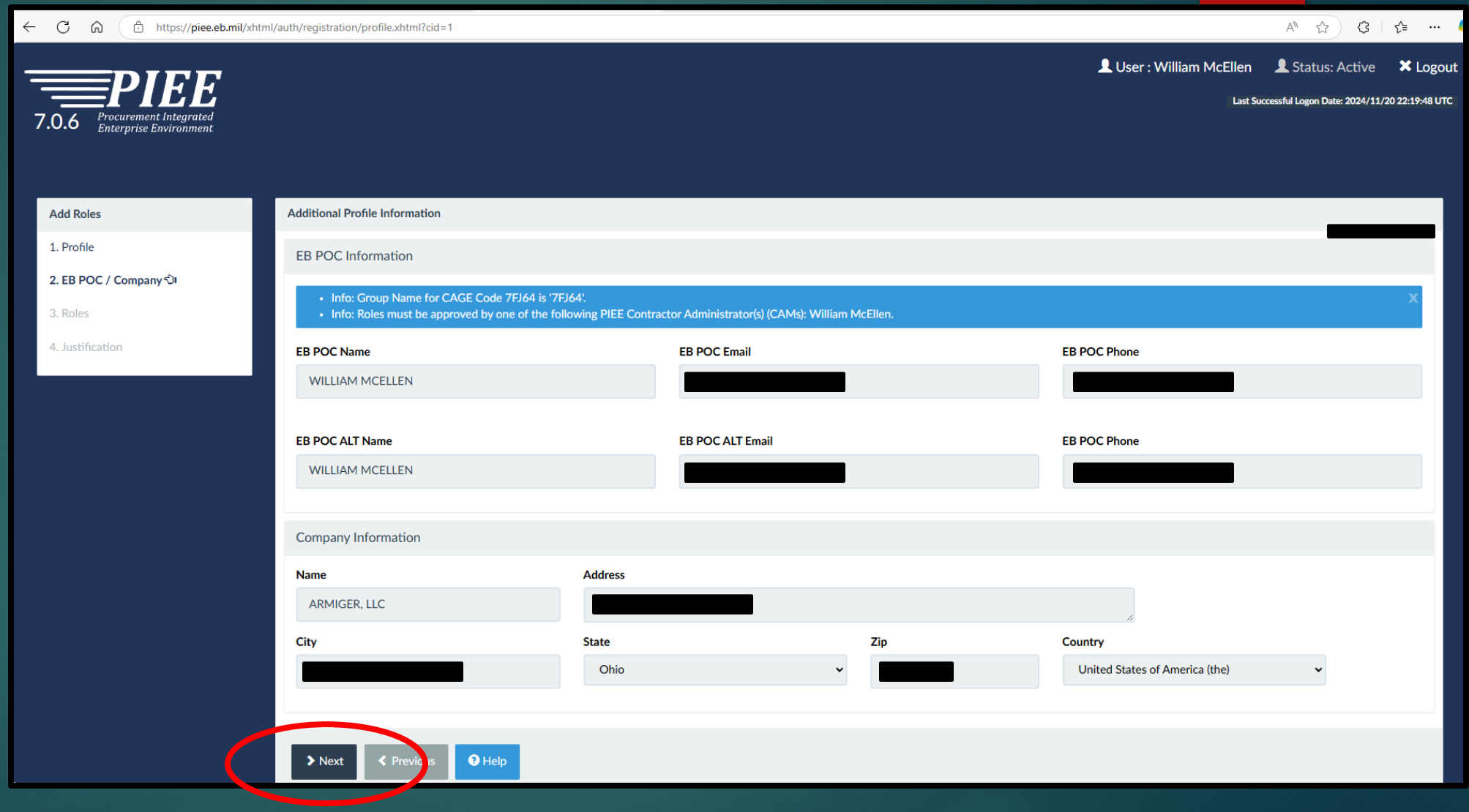
Select '+ Add Roles'



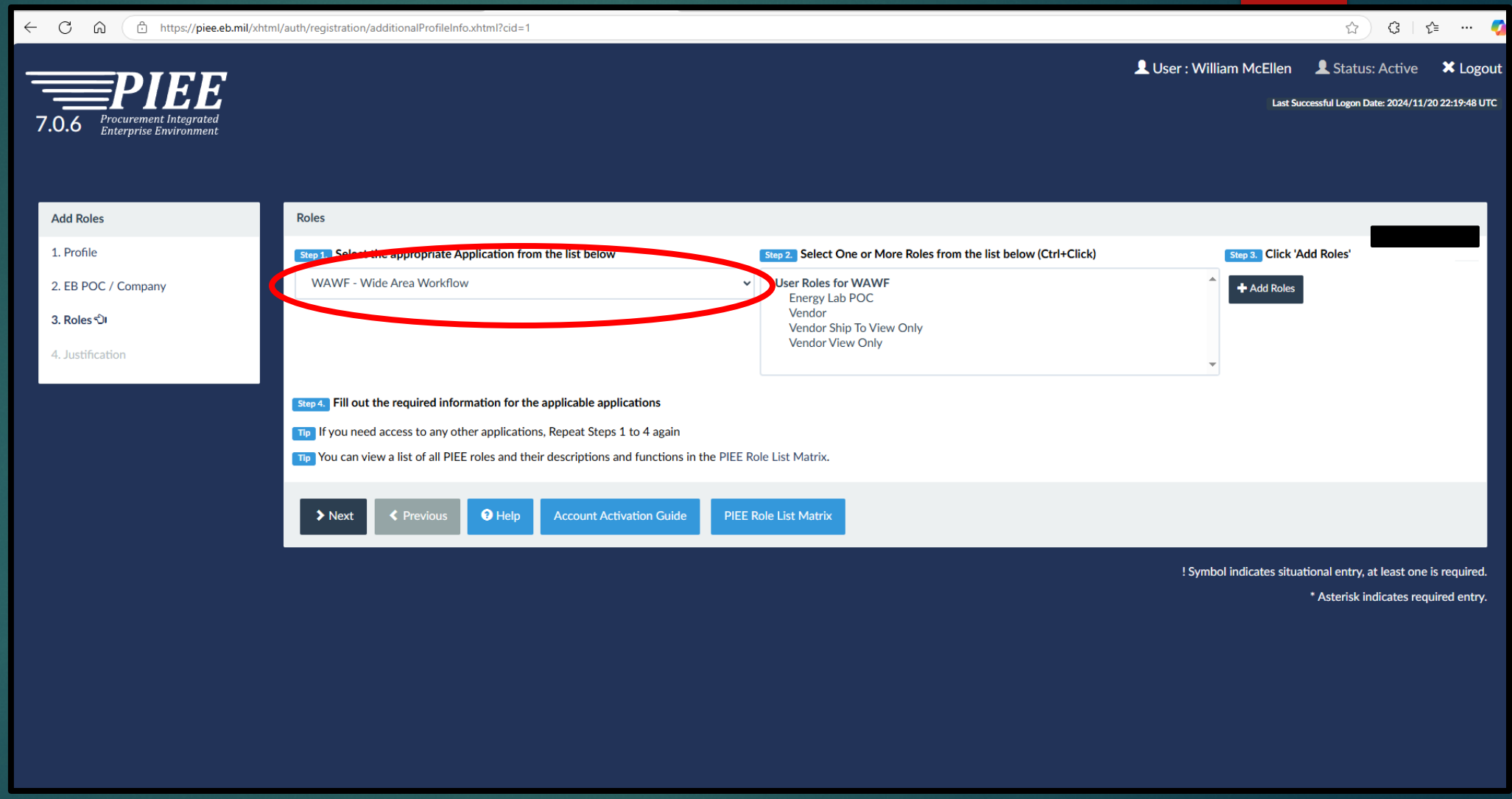
Verify all User Information and then >Next



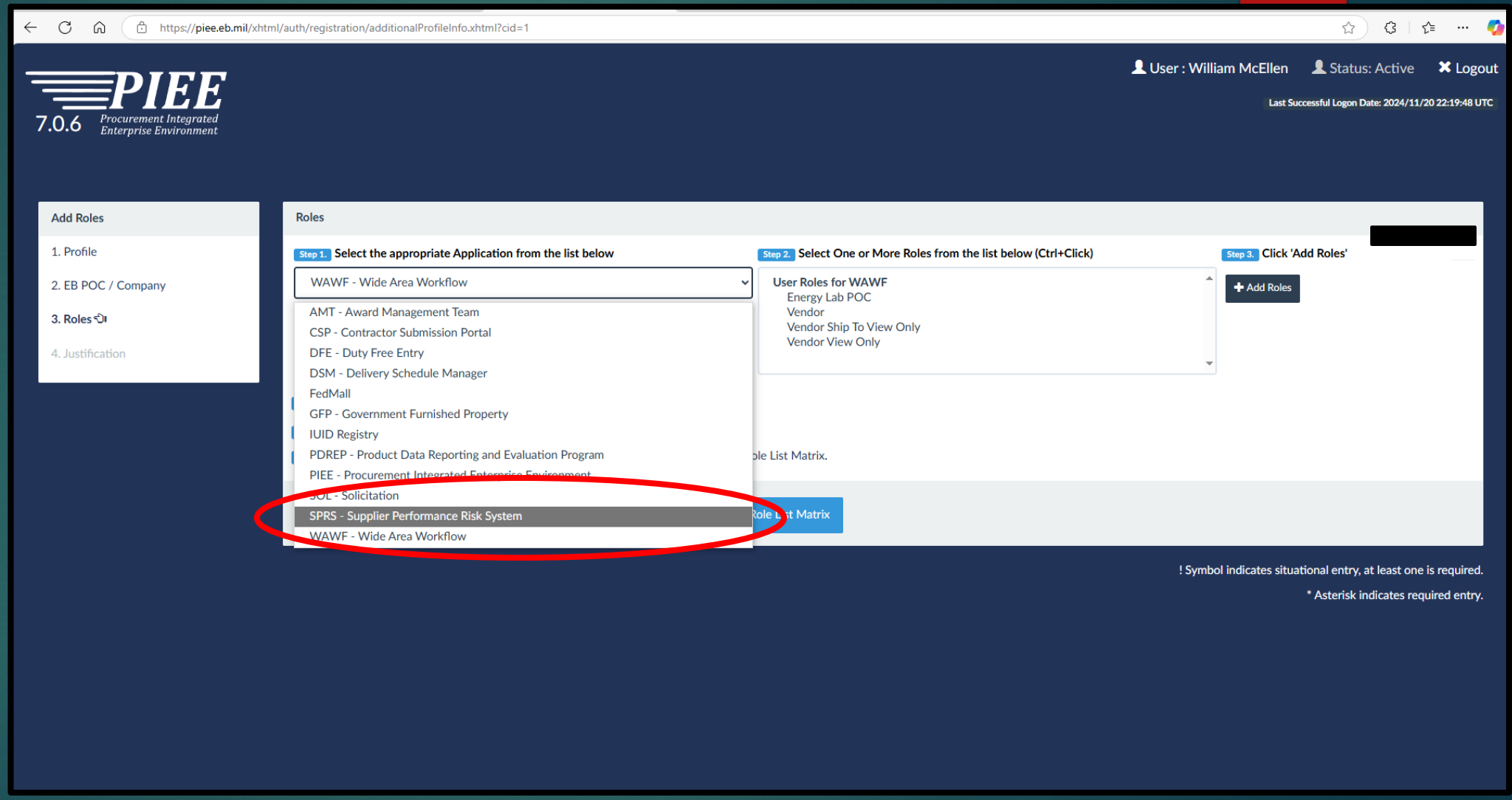
No changes can be made. Click >Next



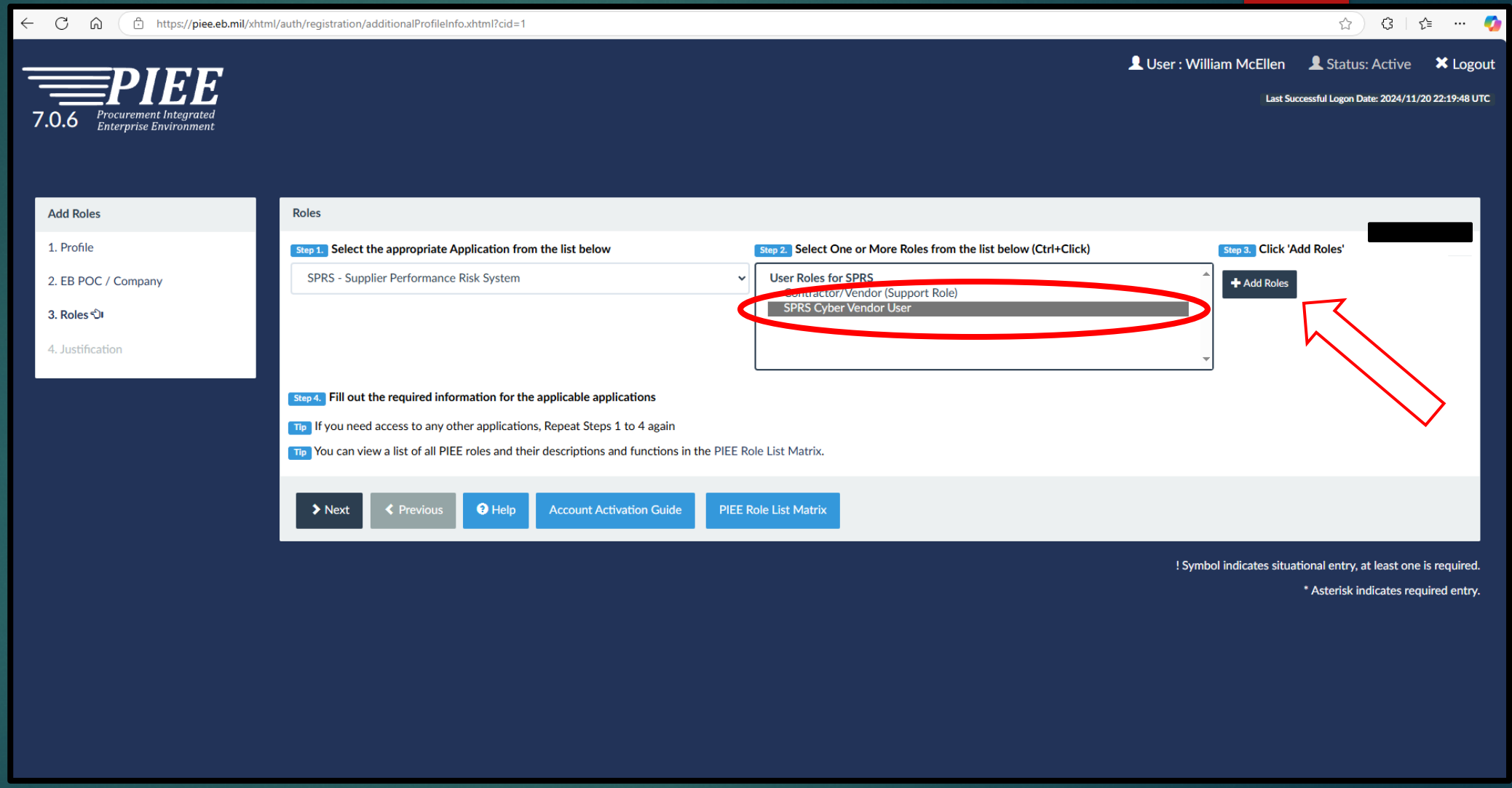
Click drop-down under Step 1.



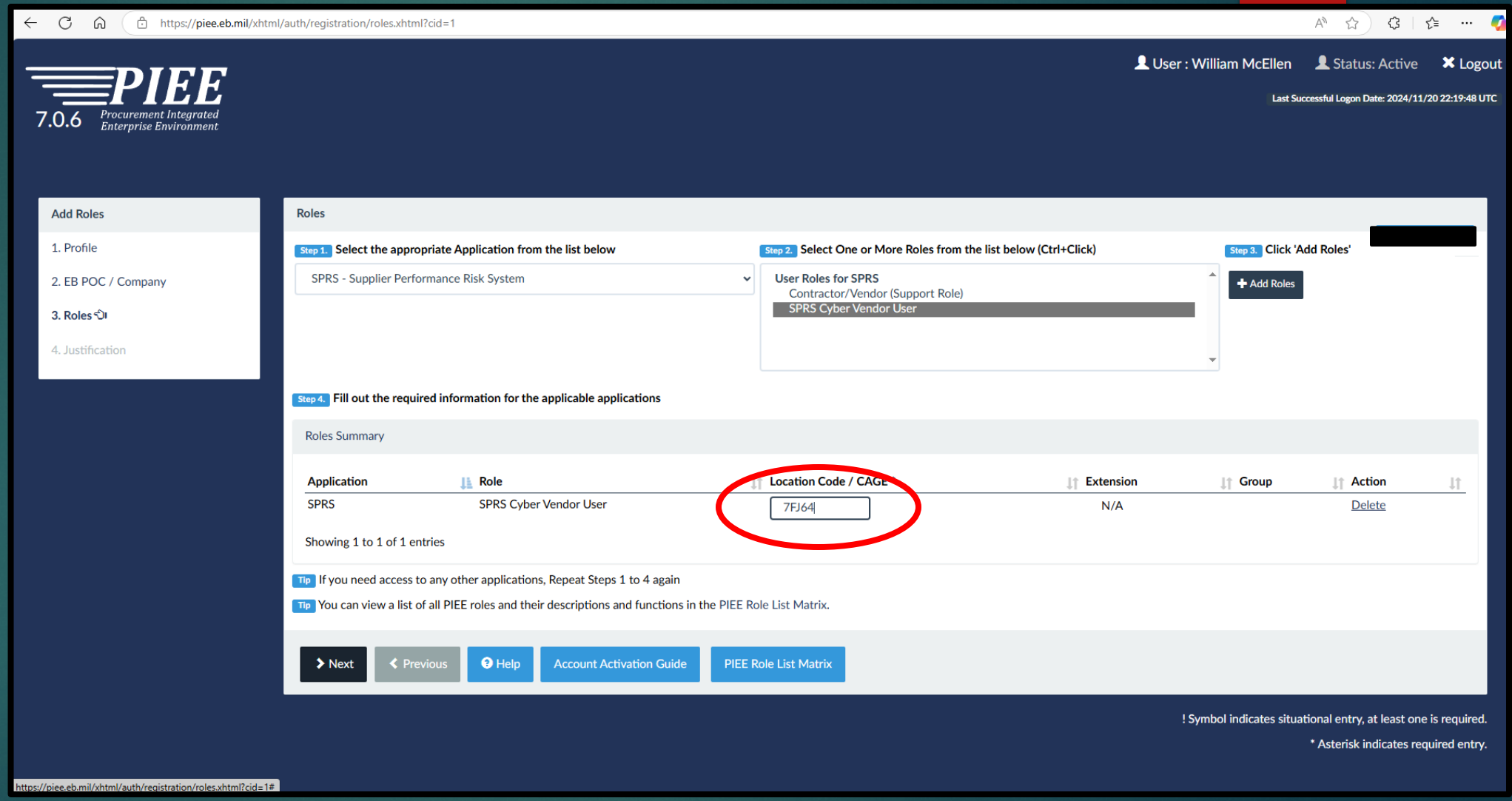
Select ‘SPRS – Supplier Performance Risk System’



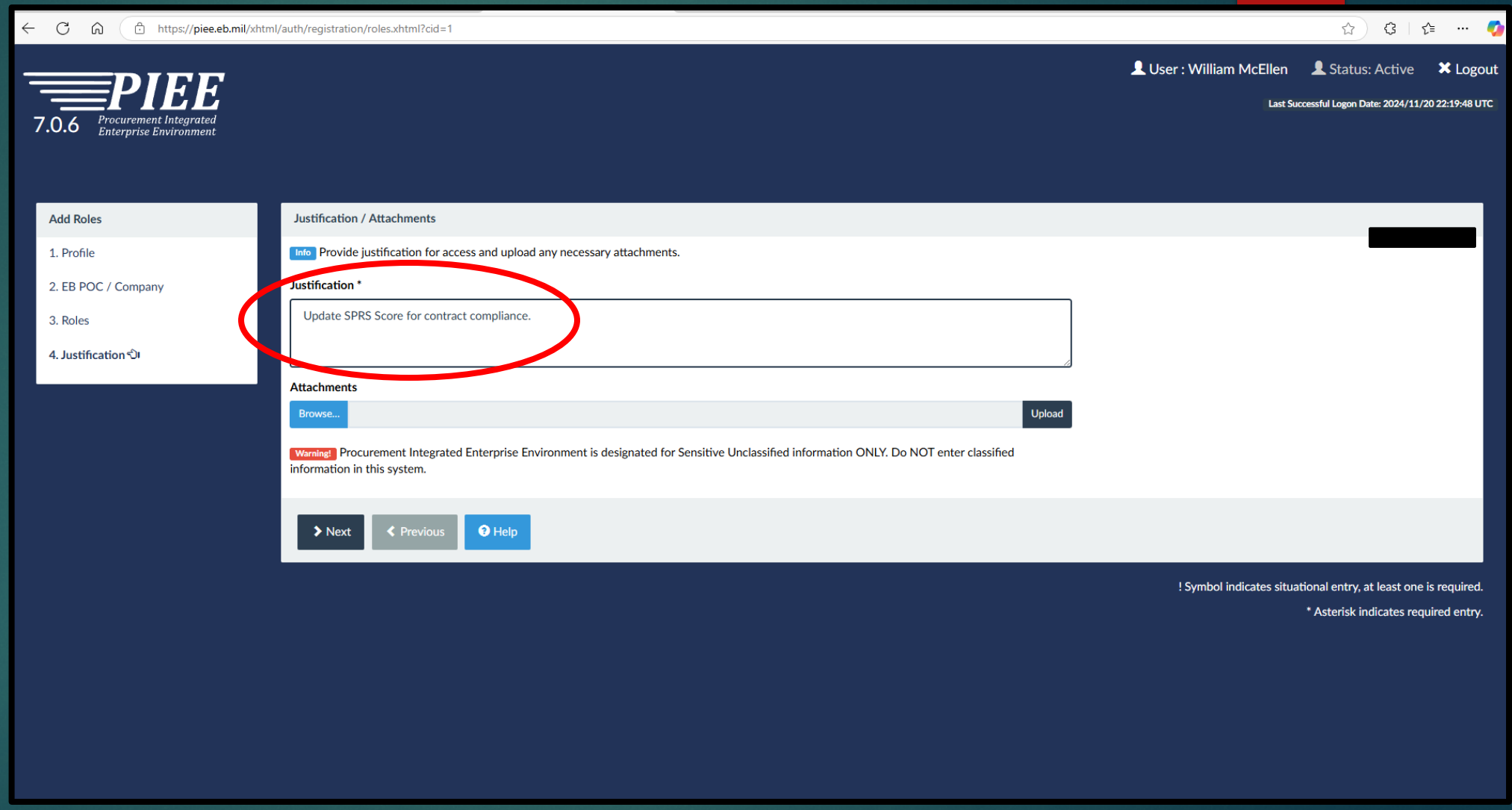
Select ‘SPRS Cyber Vendor User’ under Step 2 then click ‘+ Add Roles’



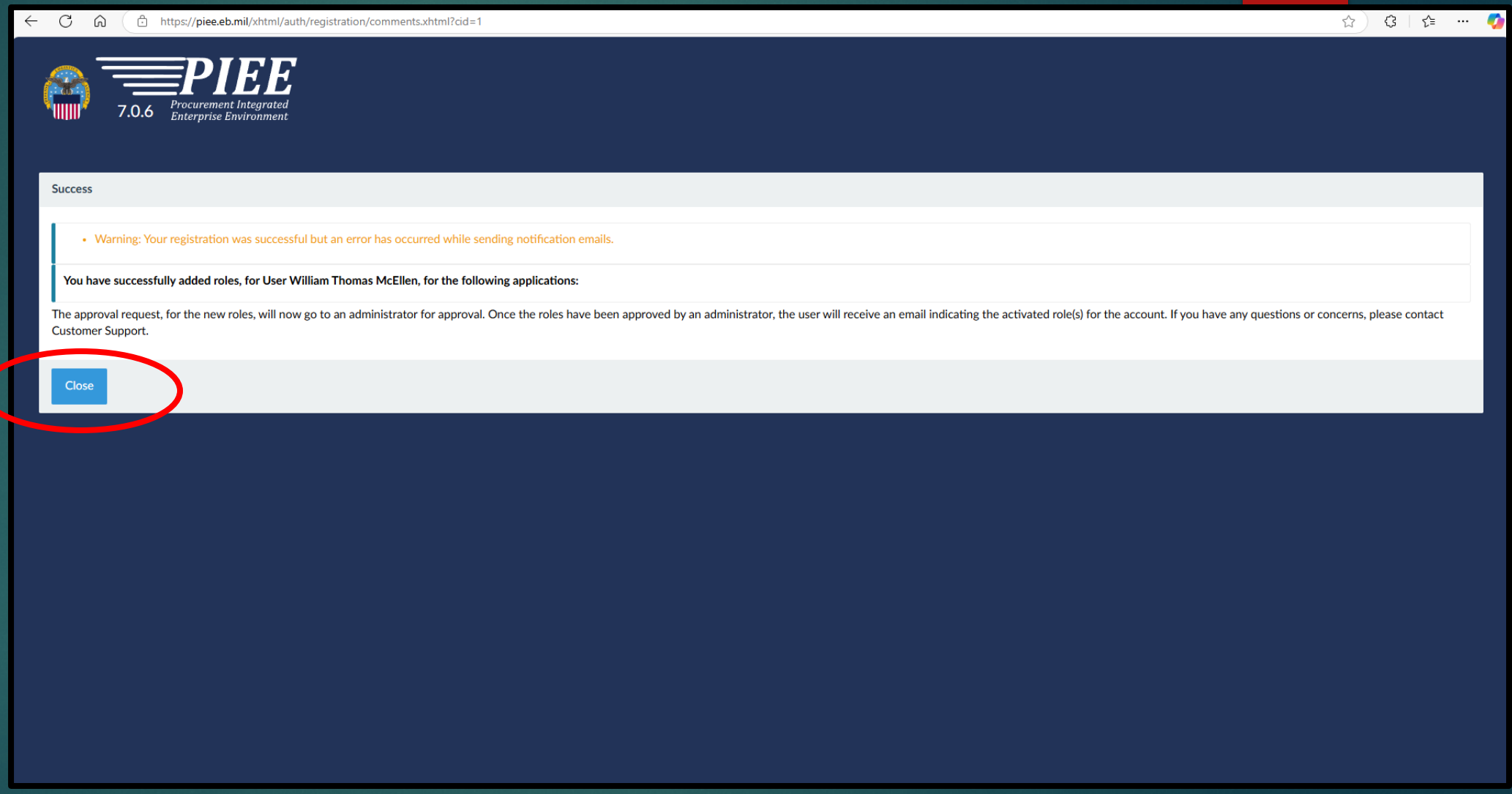
Enter CAGE Code and then >Next



Justification (Example: *Update SPRS Score for contract compliance) then >Next*

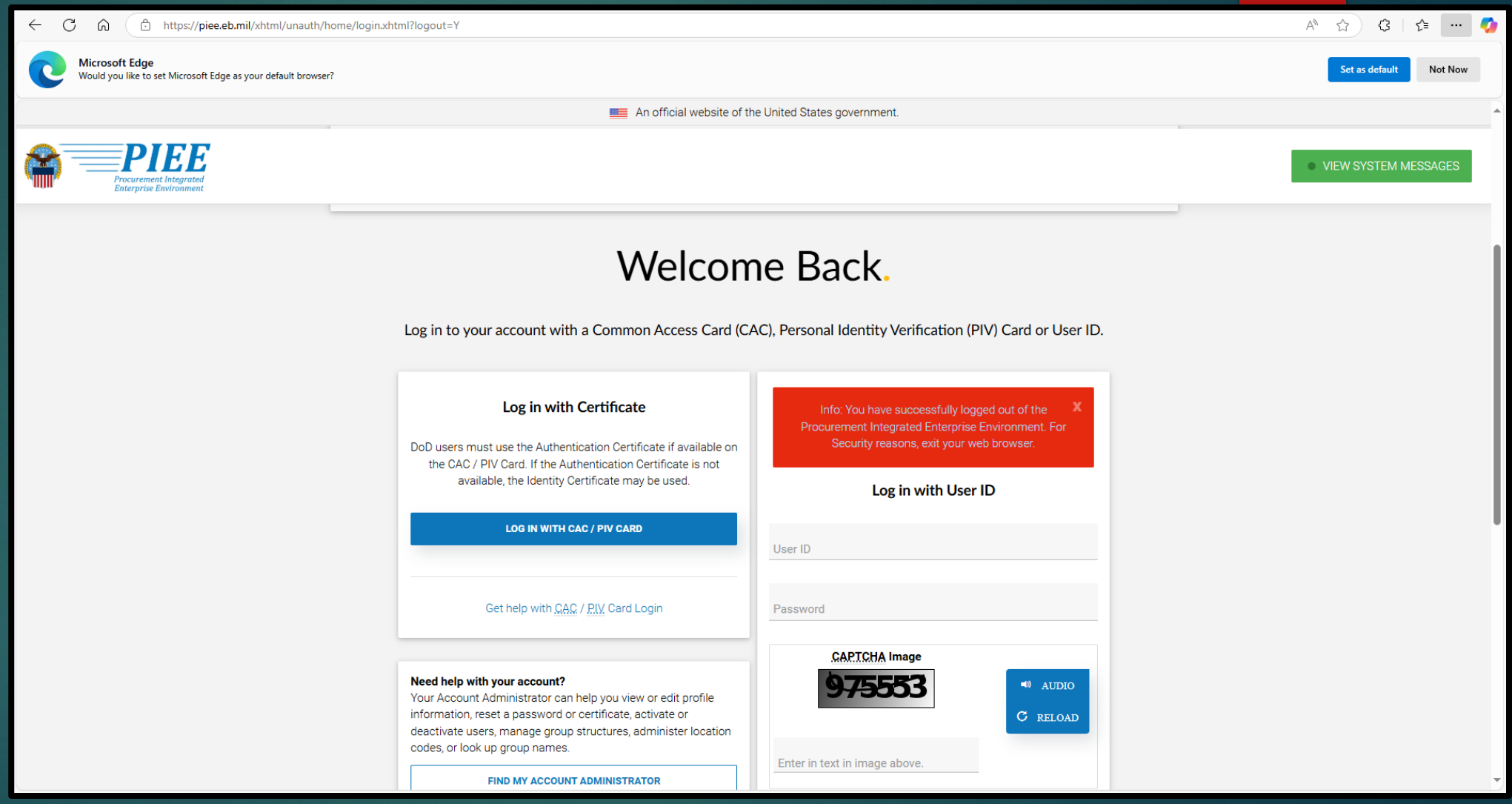


E-mail notification may, or may not, work. Go ahead and ‘Close’

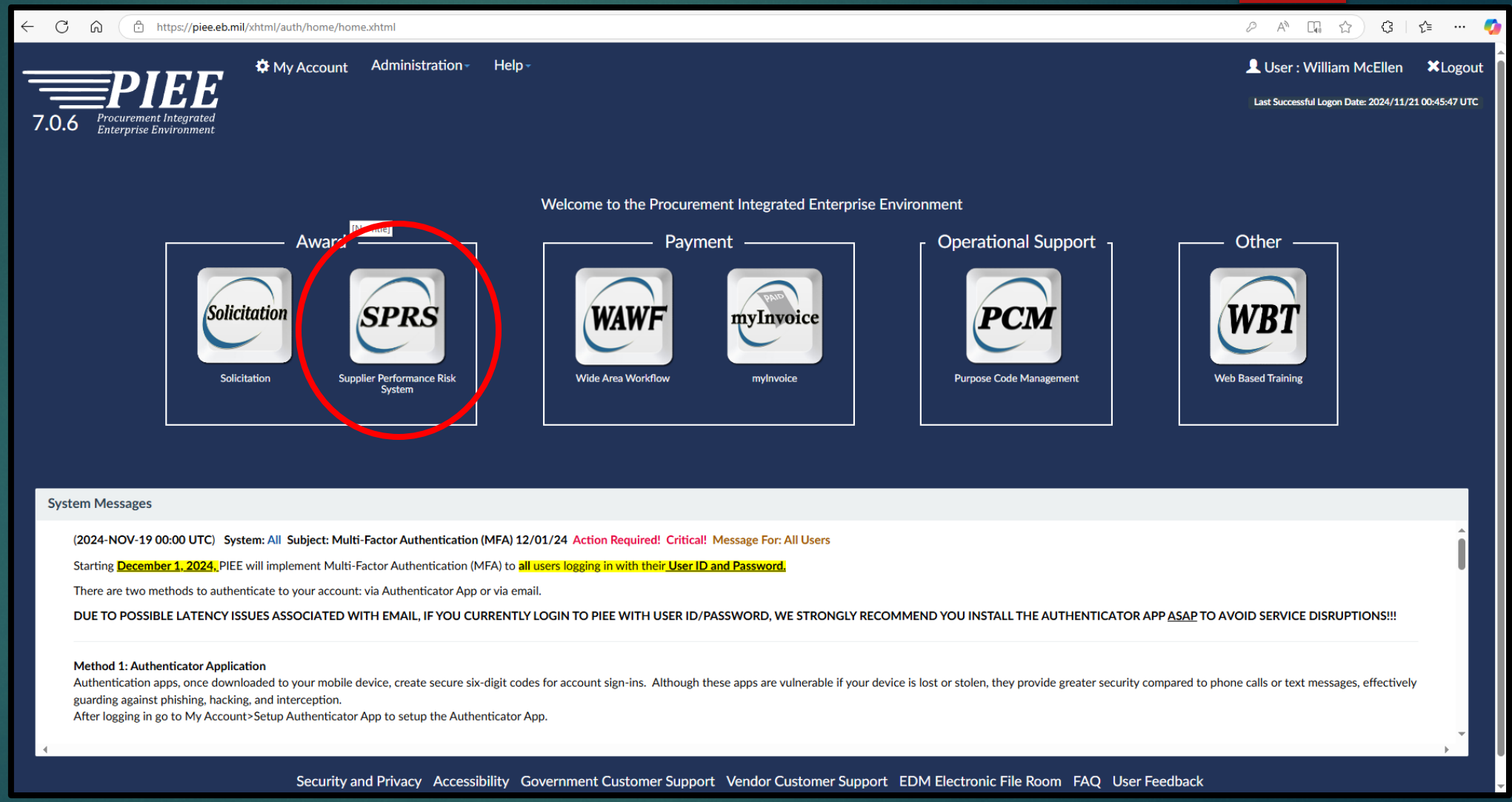


Part 3 – NIST and CMMC Scores

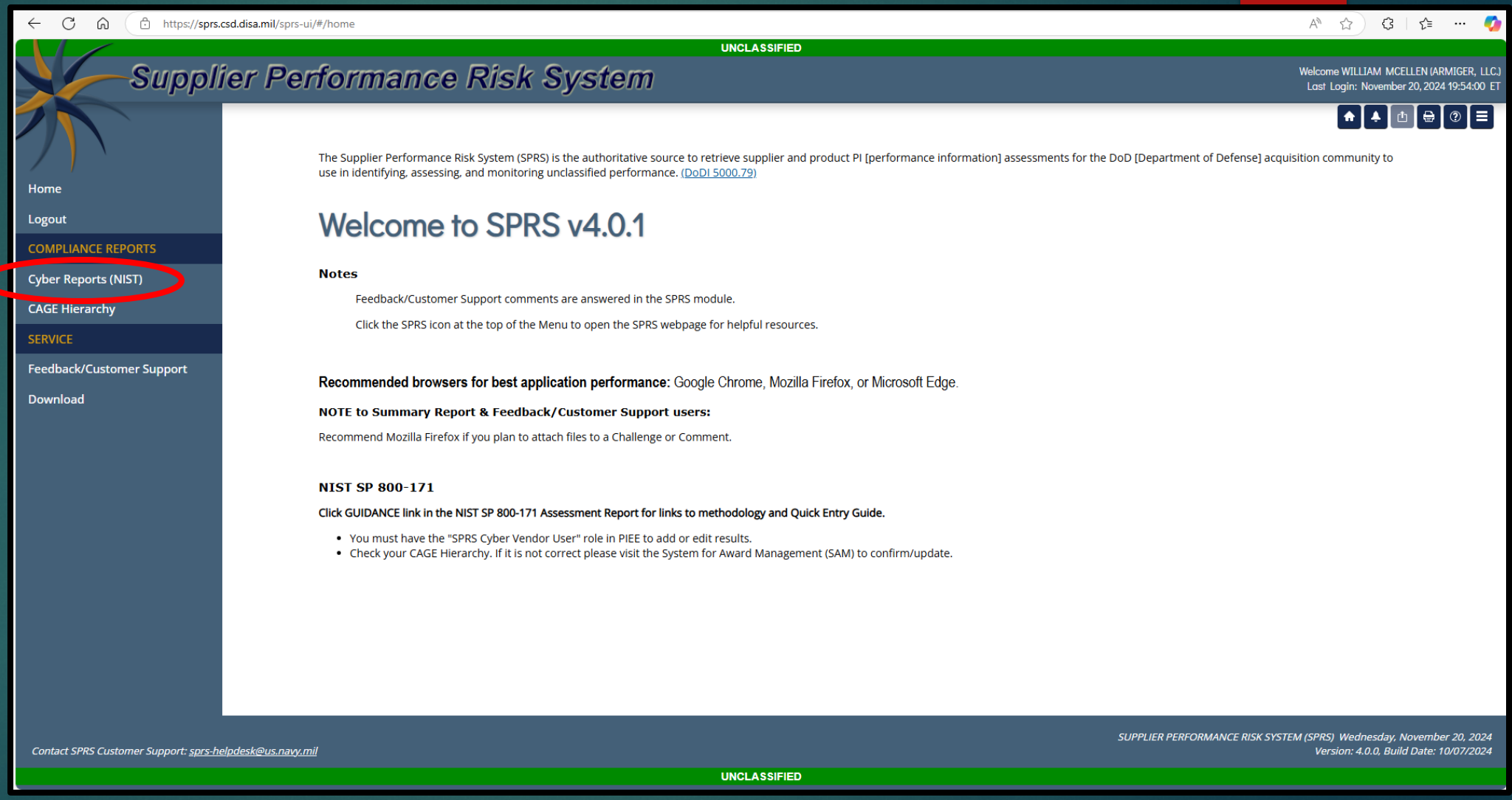
Back to *piee.eb.mil* and login one more time…



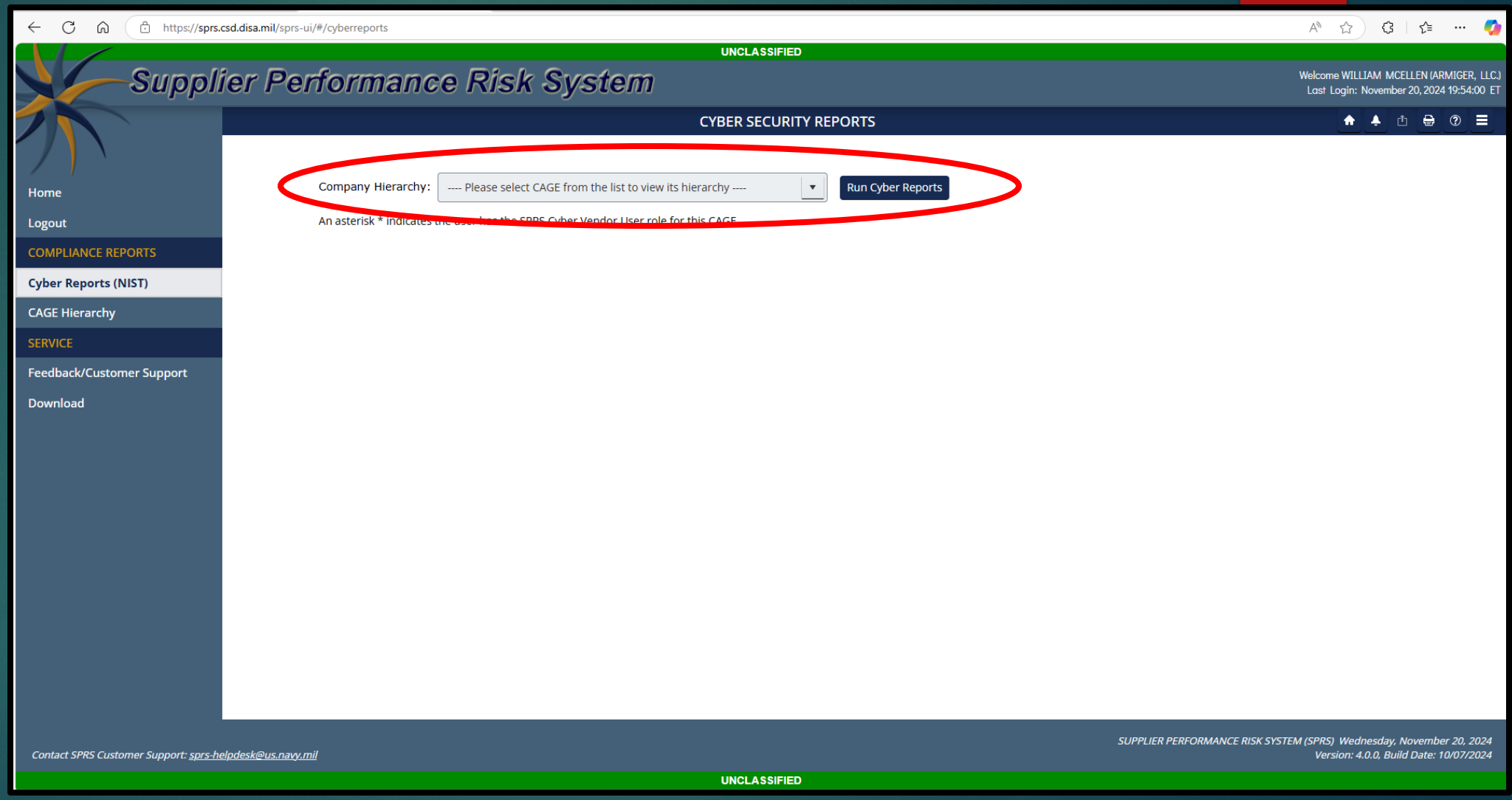
The SPRS option should now be available. Click it



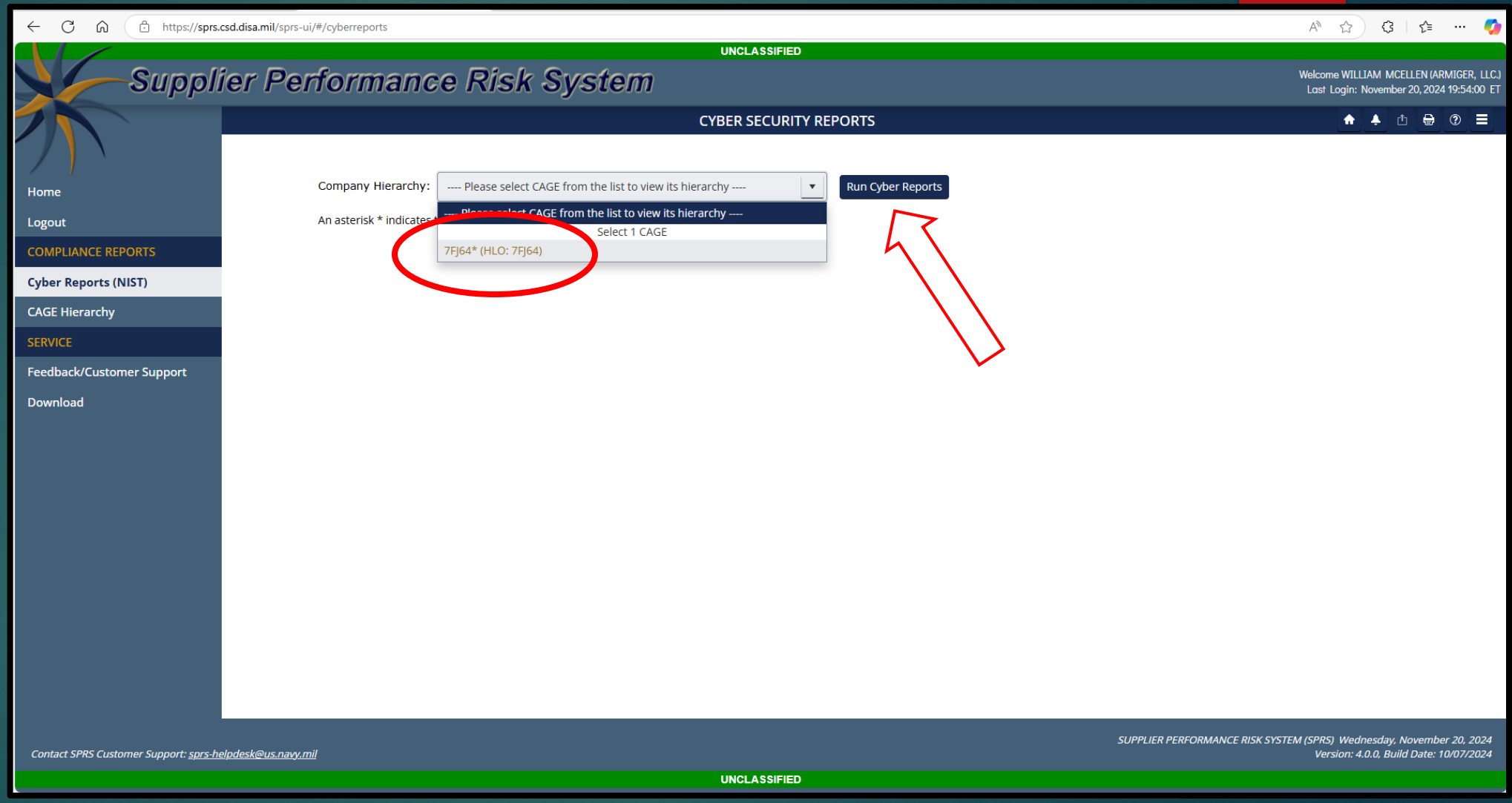
Select ‘Cyber Reports (NIST)’



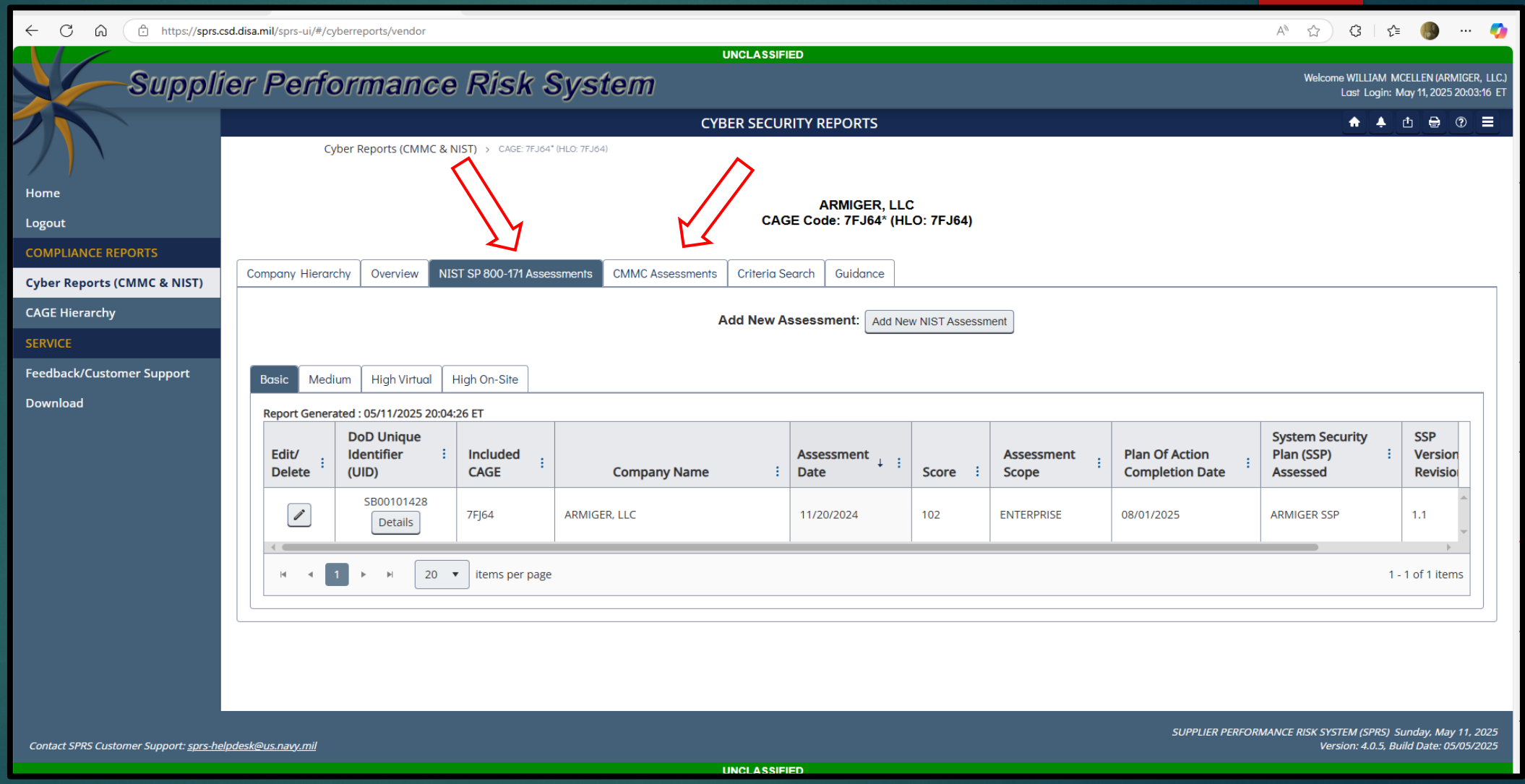
Select ‘Company Hierarchy’ drop-down



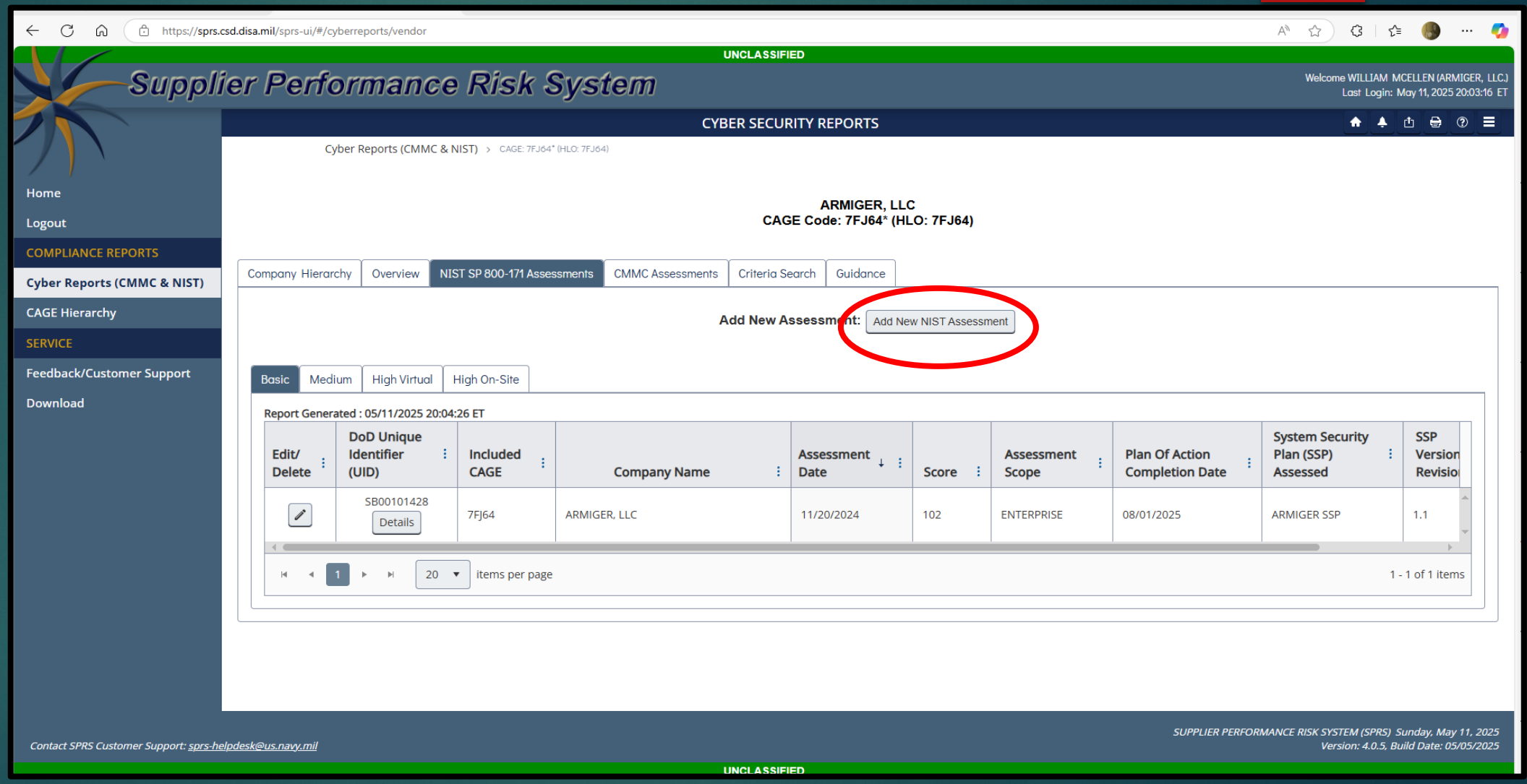
Select the appropriate CAGE then click ‘Run Cyber Reports’



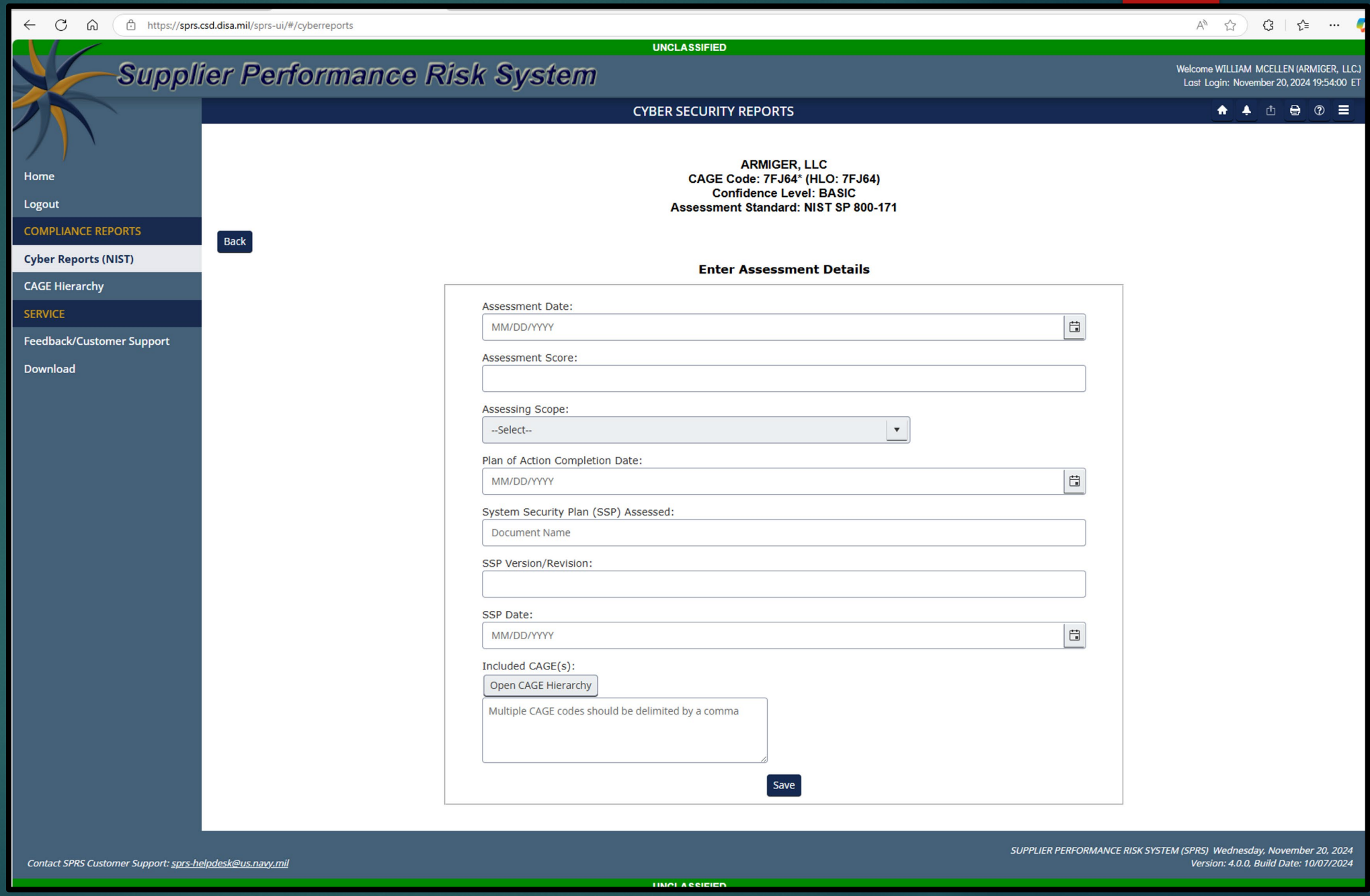
You will see options for both NIST SP 800-171 and CMMC Assessments



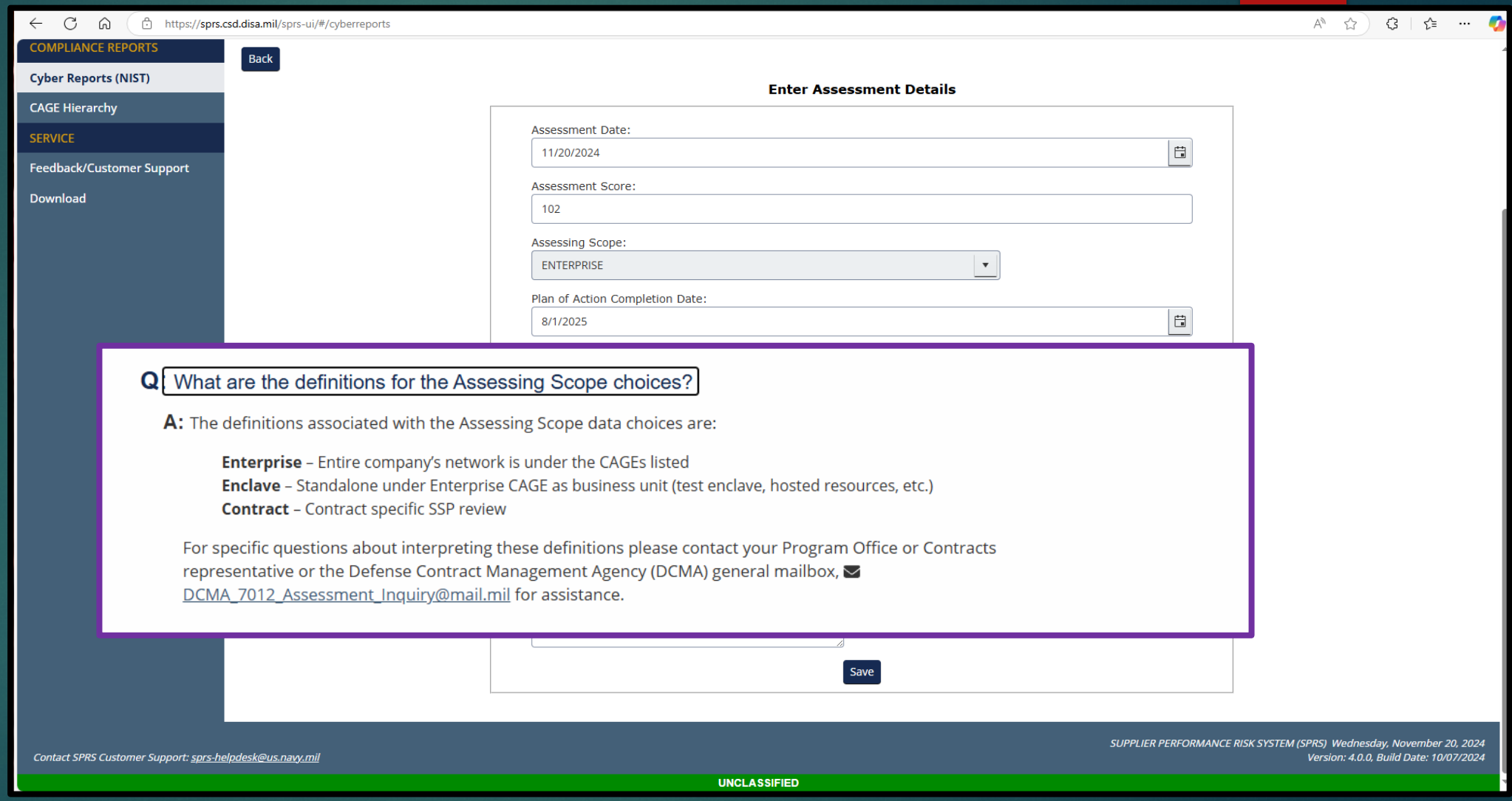
While under the NIST tab, click ‘Add New NIST Assessment’



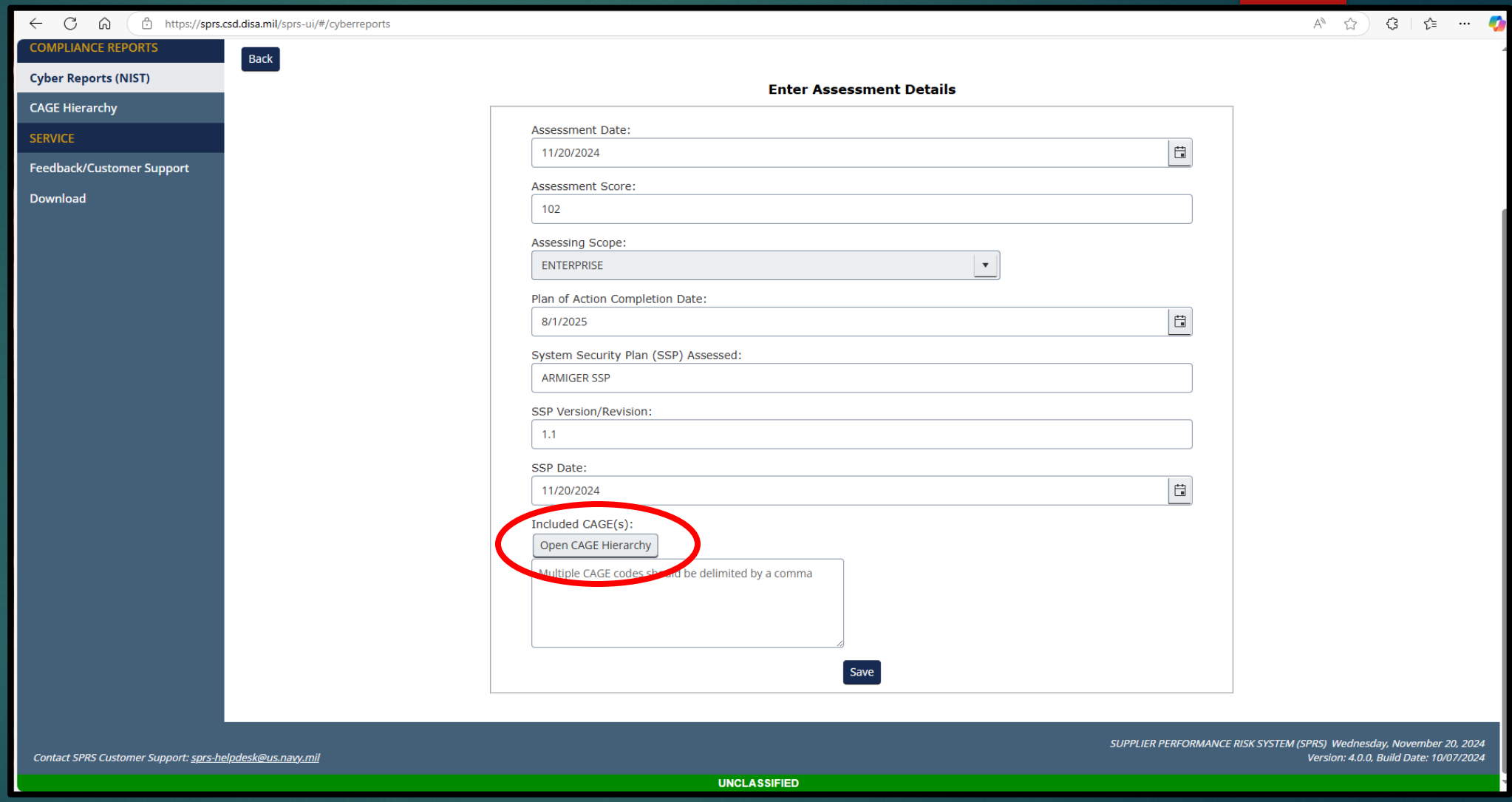
Fill in all fields. Check with your IT Manager to determine NIST score.



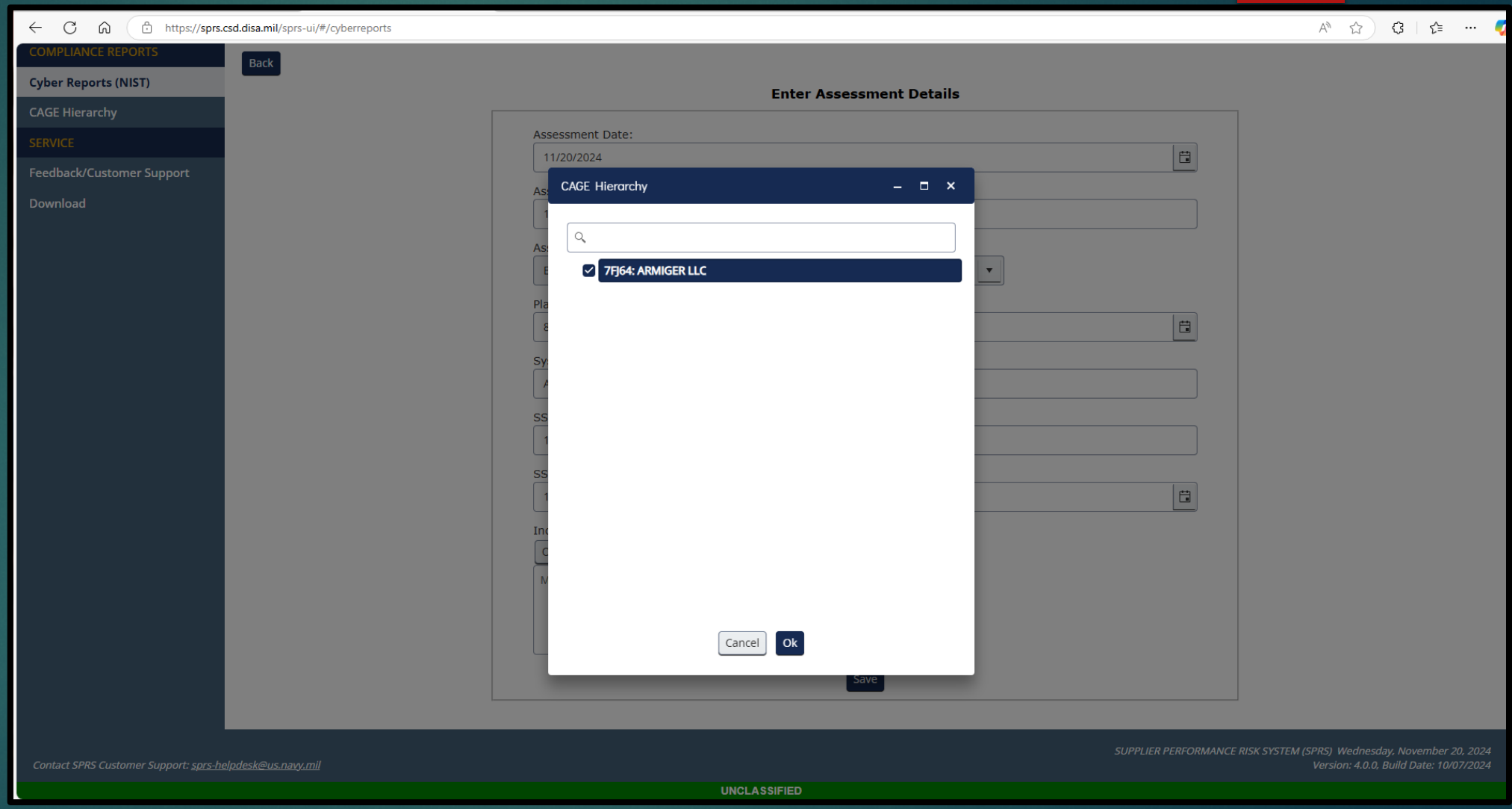
If you are unsure of the Assessing Scope…



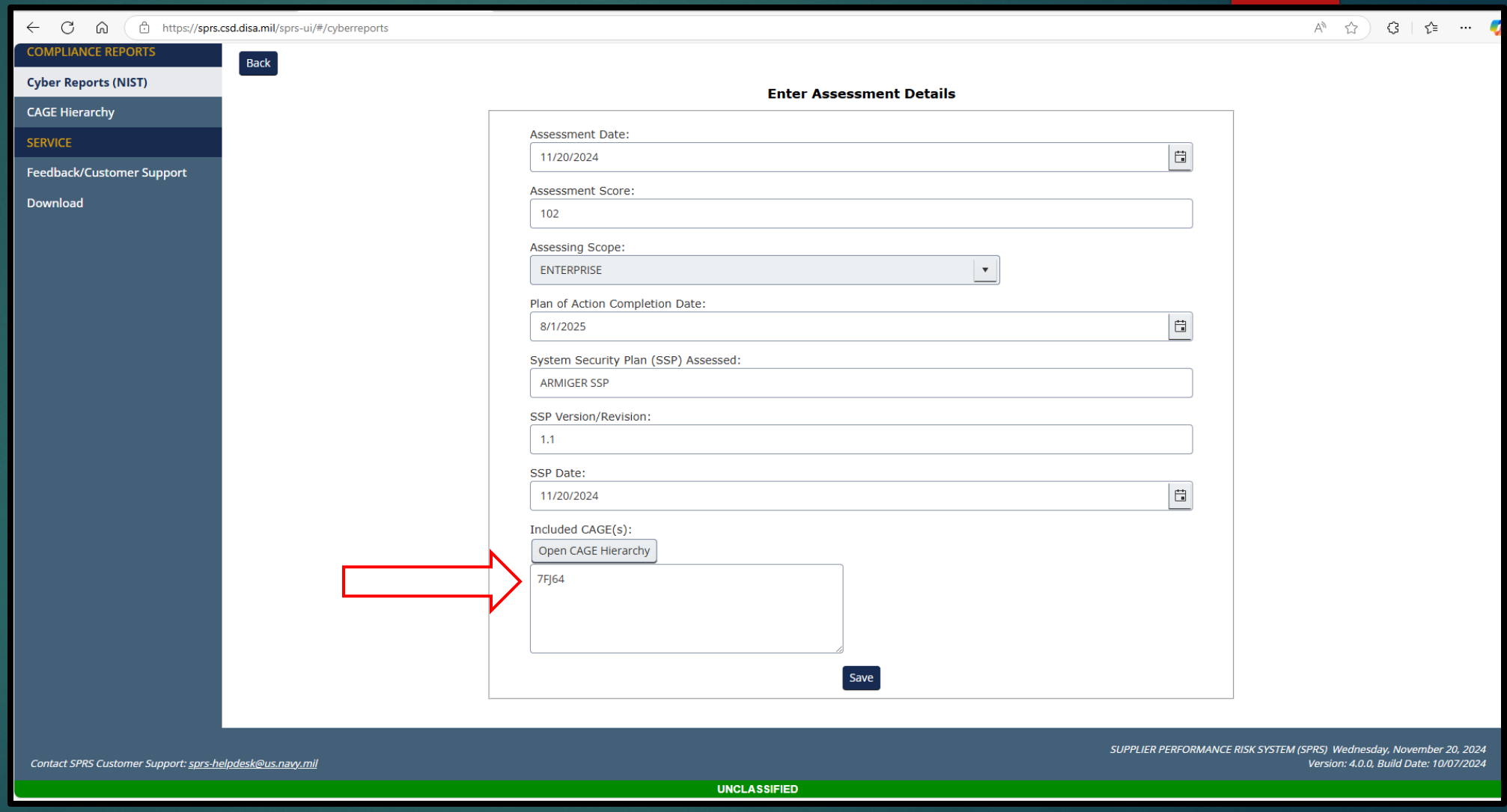
Sample of filled Assessment. Once complete, click ‘Open CAGE Hierarchy’



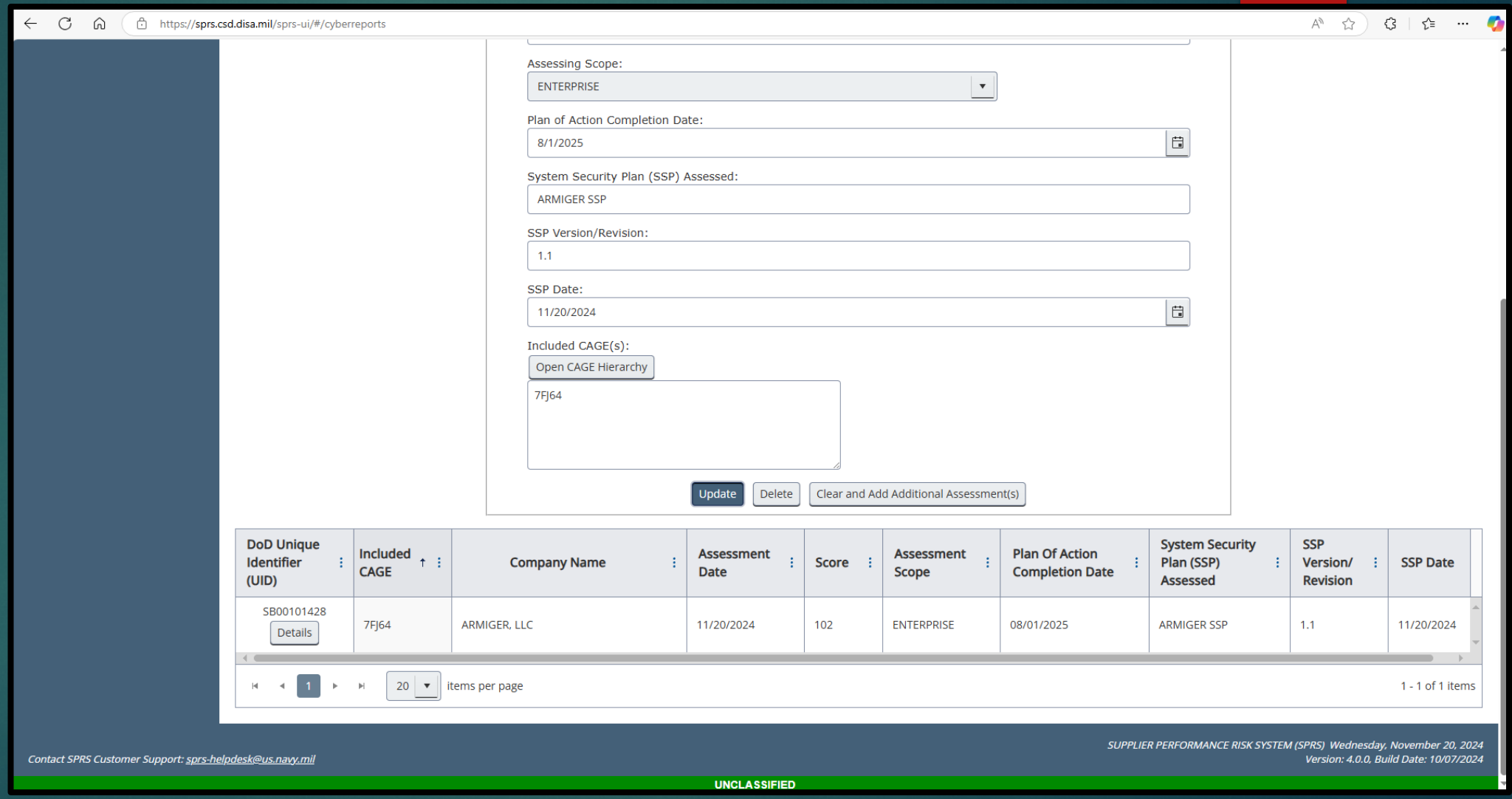
Select the appropriate CAGE and hit ‘OK’



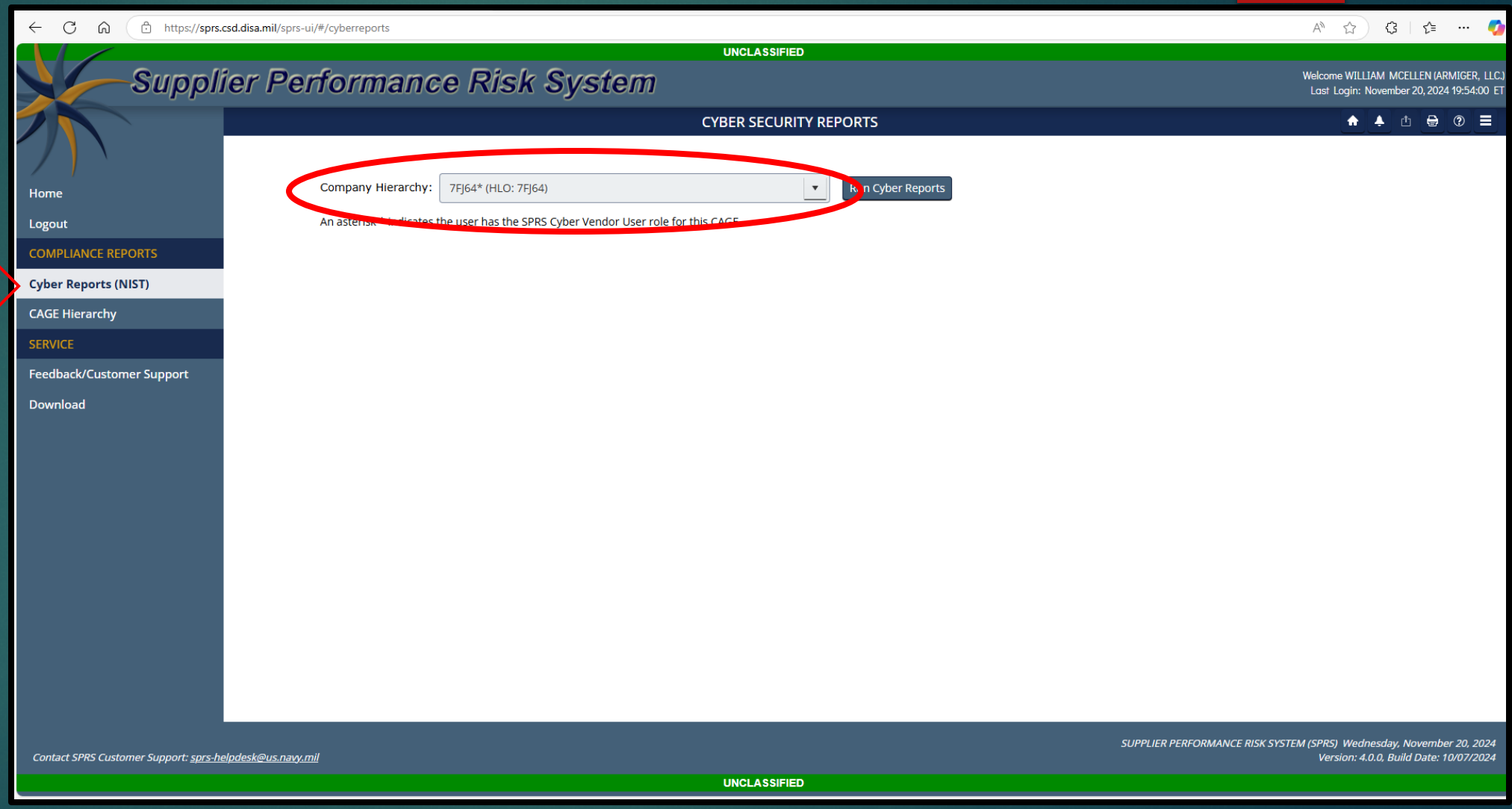
The CAGE should now be included on the Assessment. Click ‘Save’



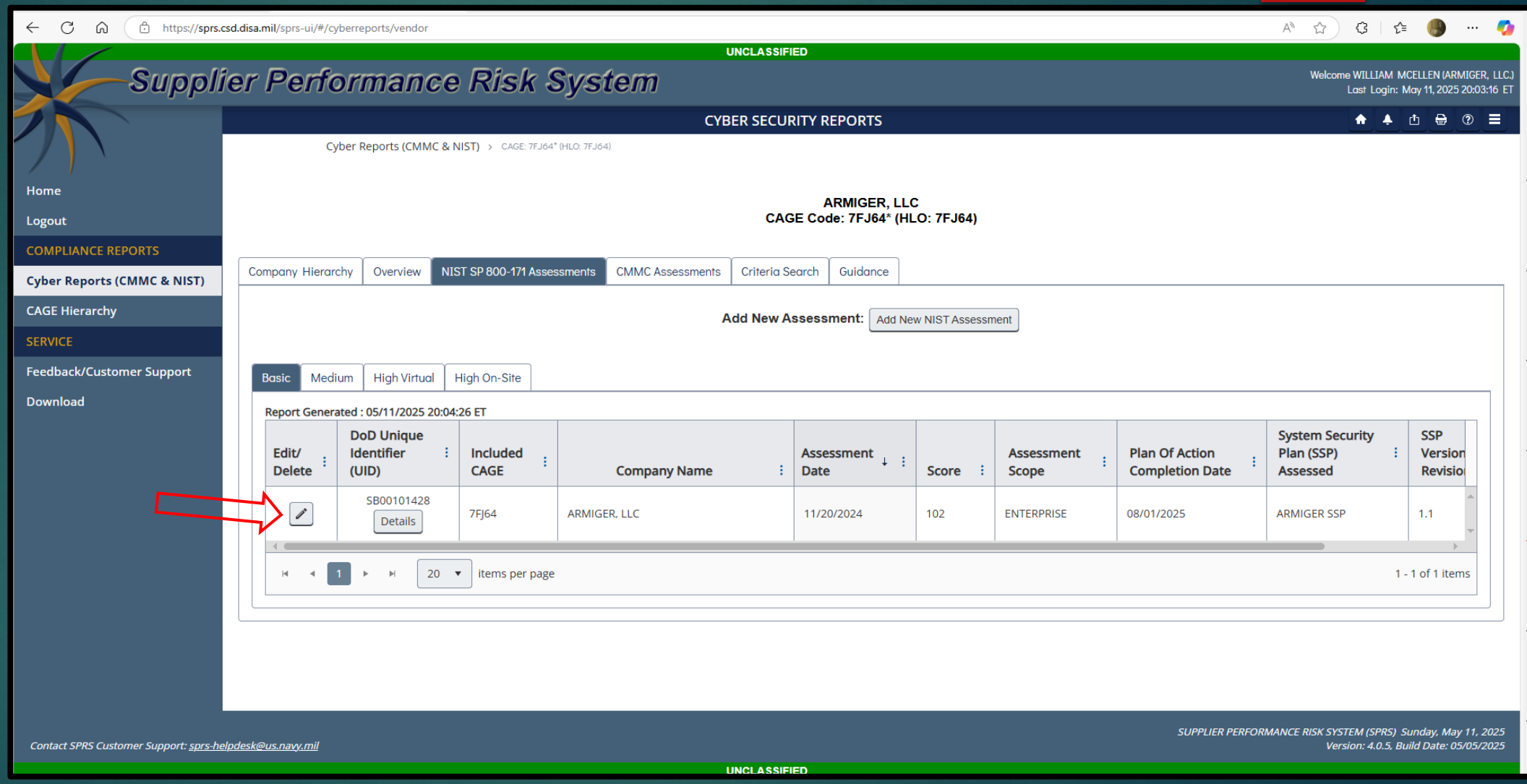
The overview will appear. If needed, you can make changes and ‘Update’



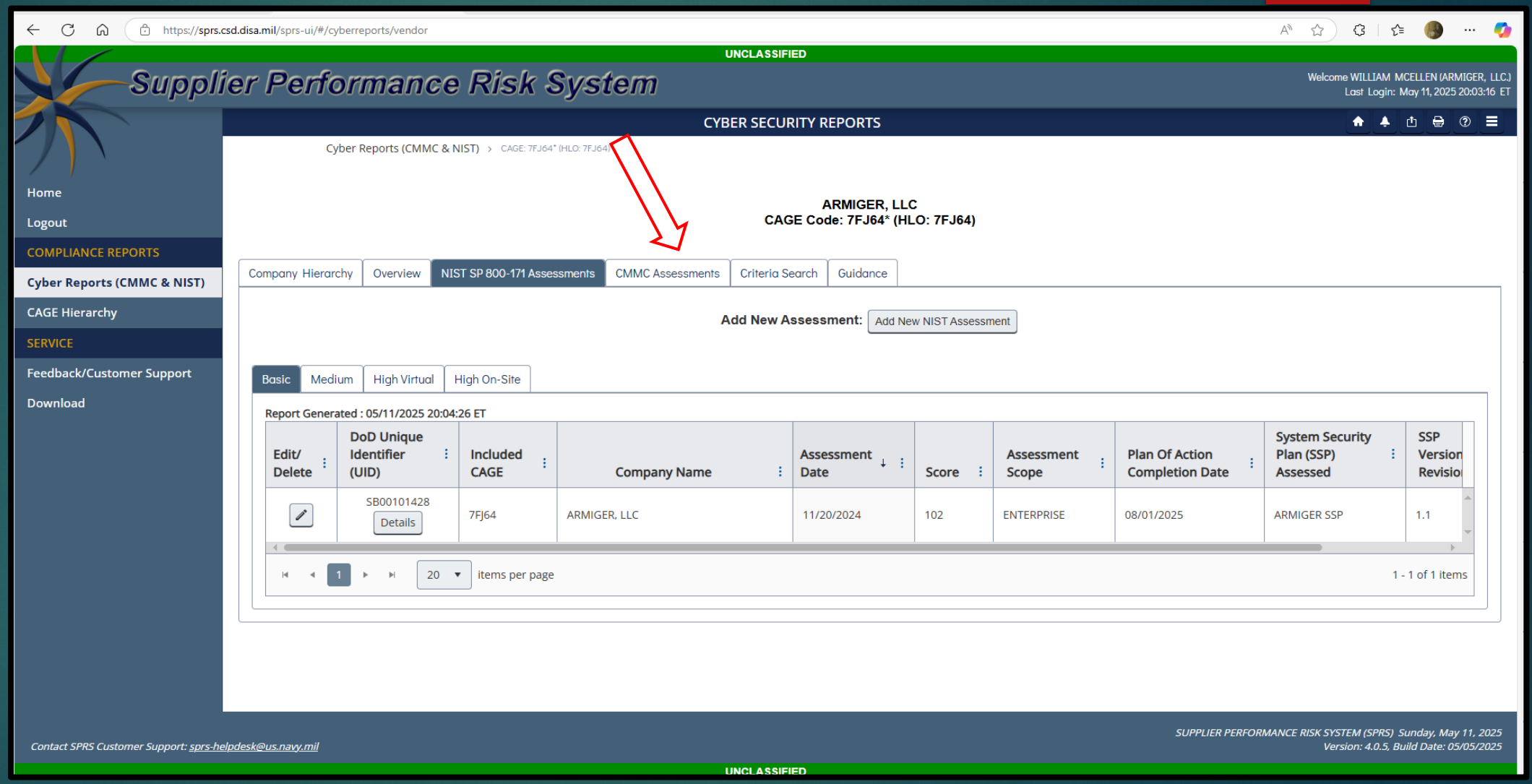
To review, or make changes, click Cyber Reports and select Hierarchy/Report



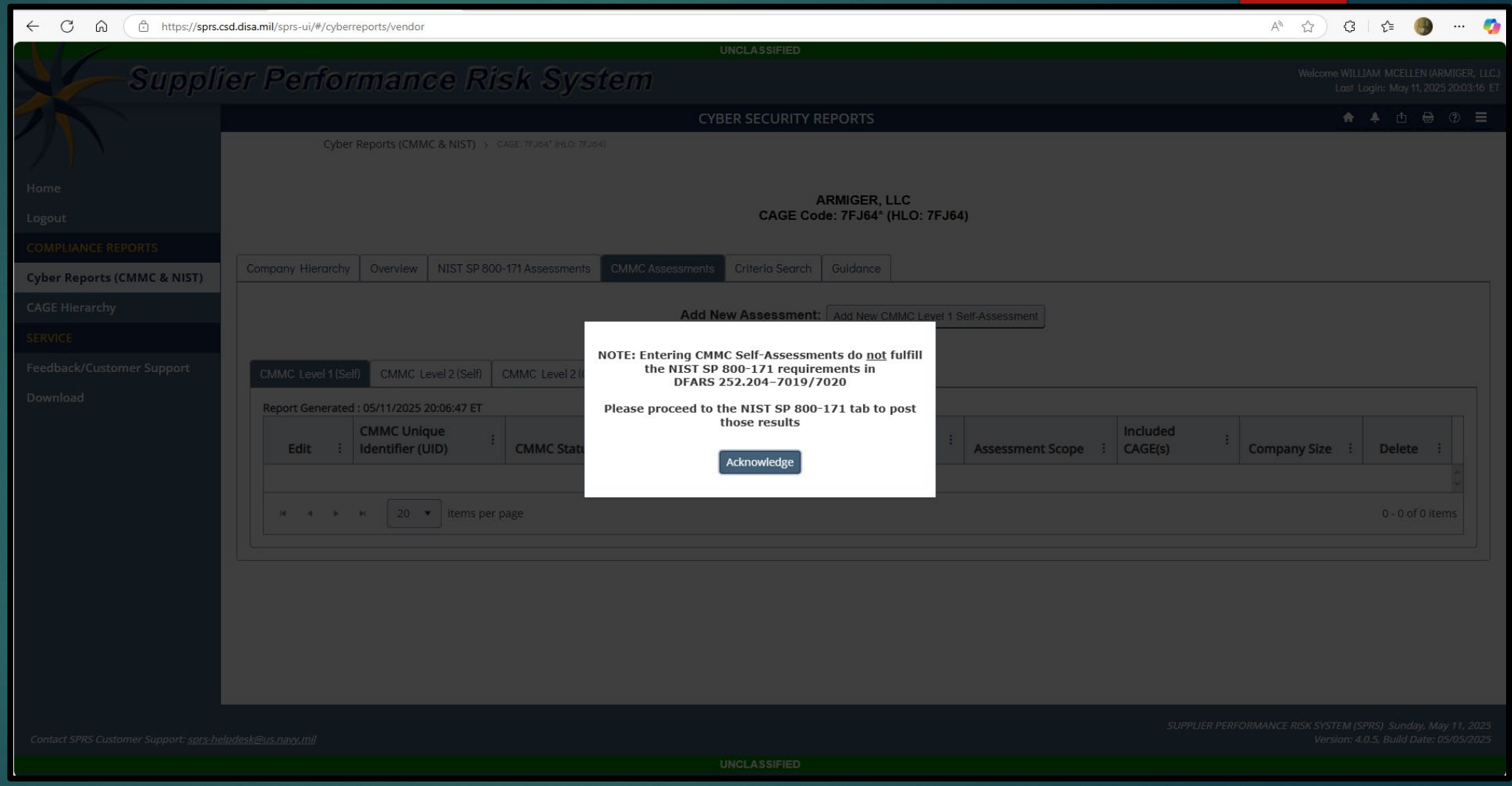
Your Assessment is listed. If needed, you can edit/delete or create a new one



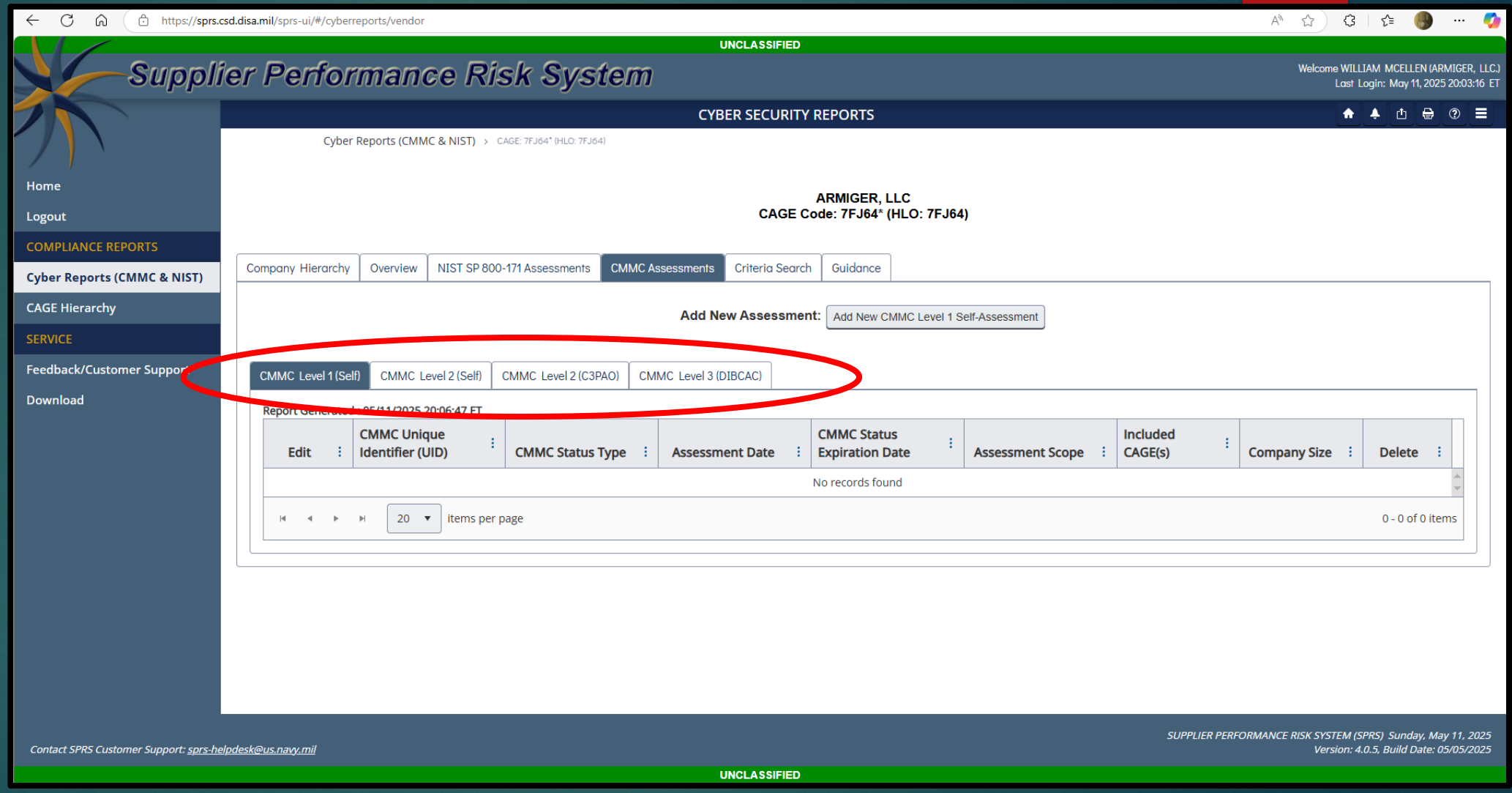
Next - Click on the CMMC Assessments tab to switch over



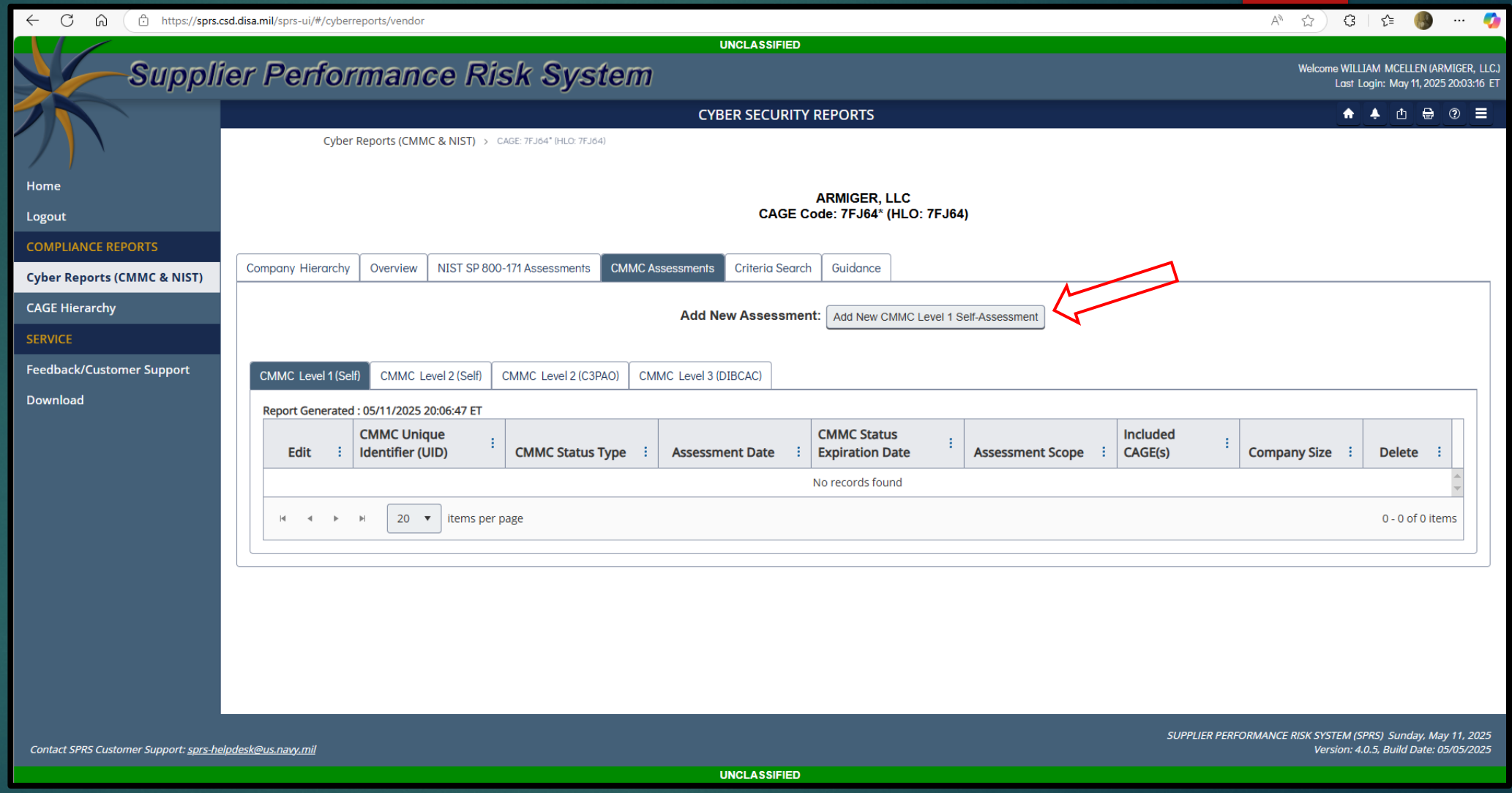
Note that CMMC Assessments do not remove the NIST Score requirement



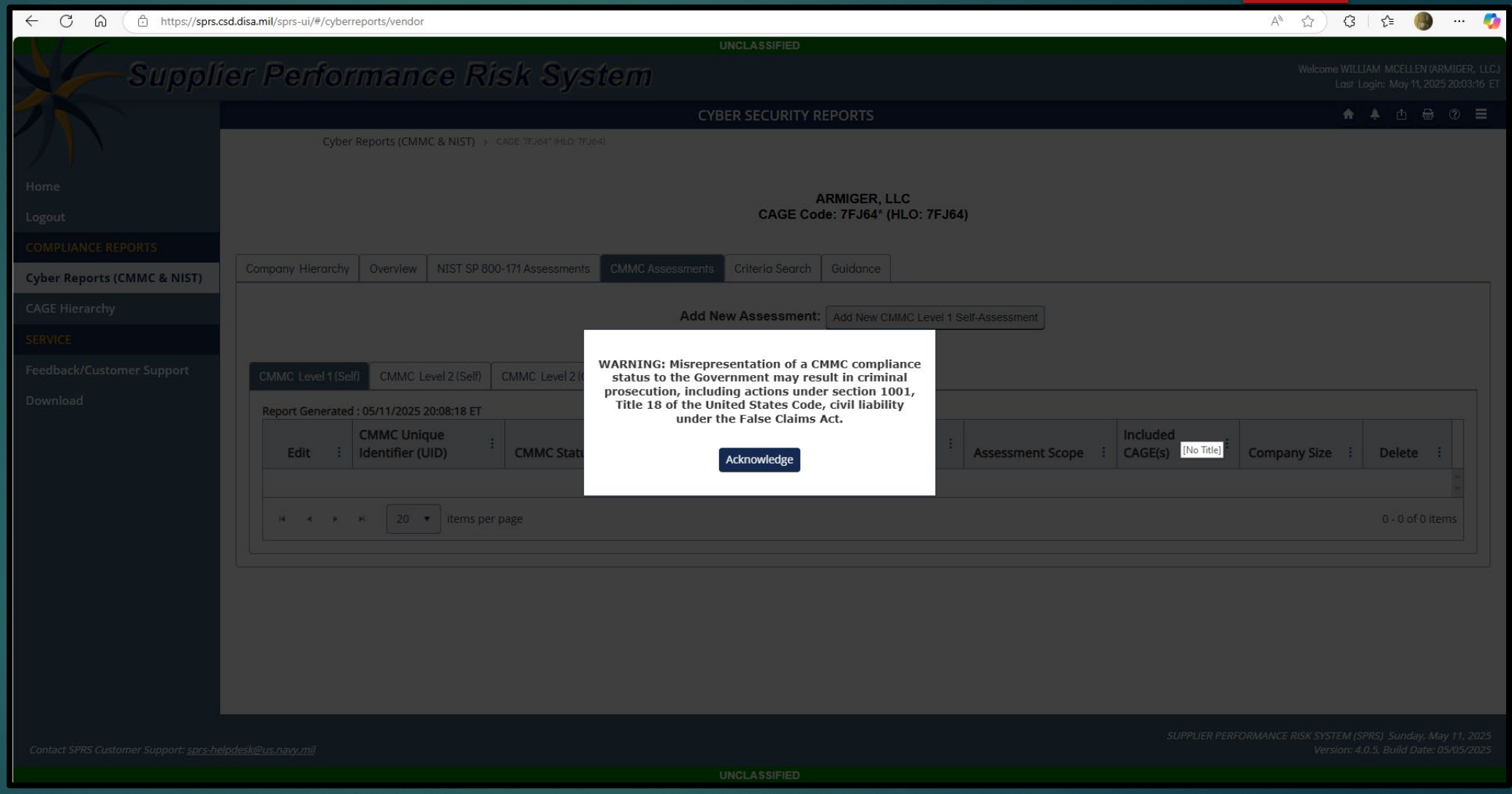
As of 28 March, Level 1, 2 (Self), 2 (C3PAO), and 3 (DIBCAC) are all available



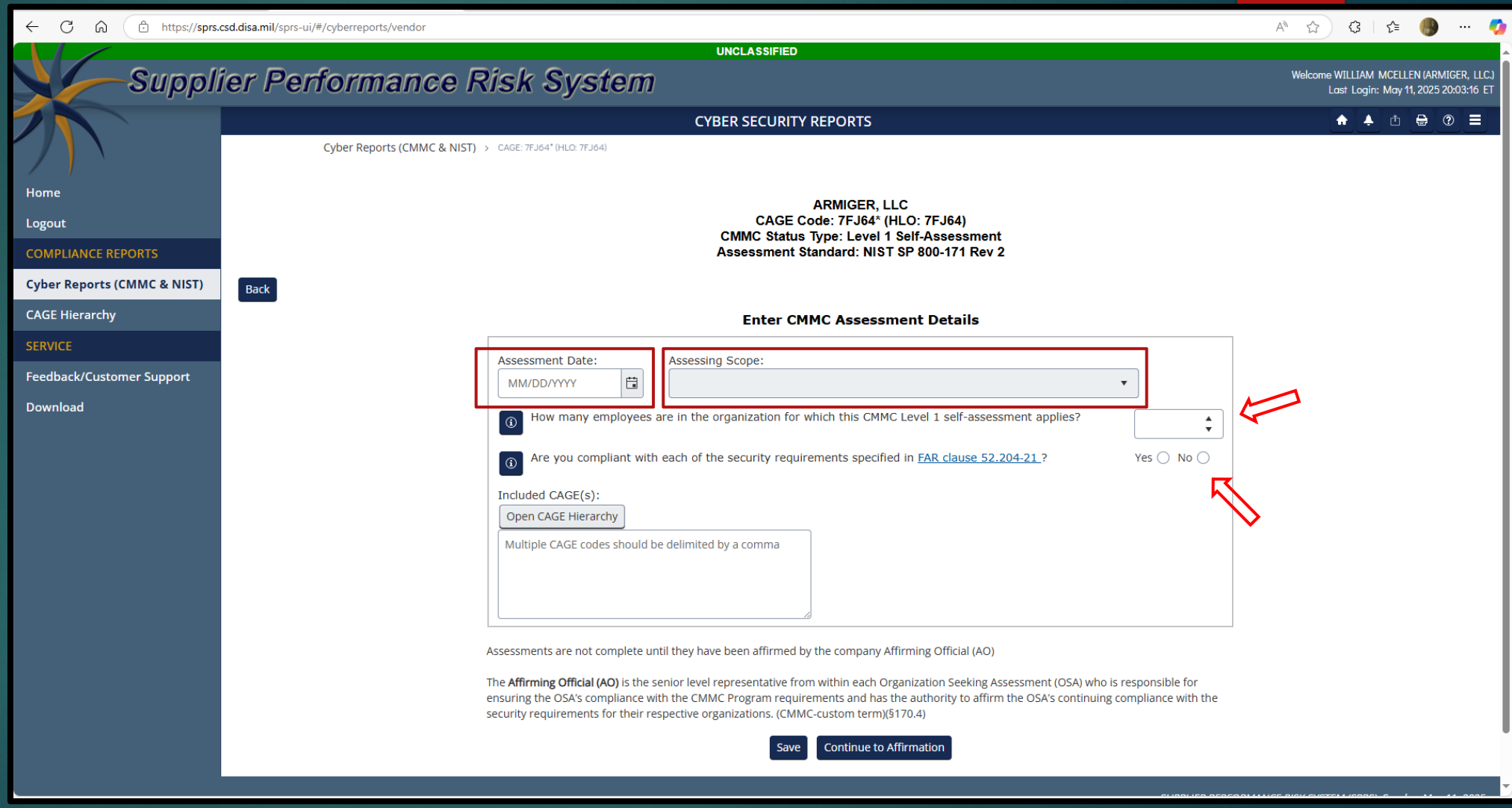
While on the Level 1 (Self) tab, click ‘Add New CMMC Level 1 Self-Assessment’



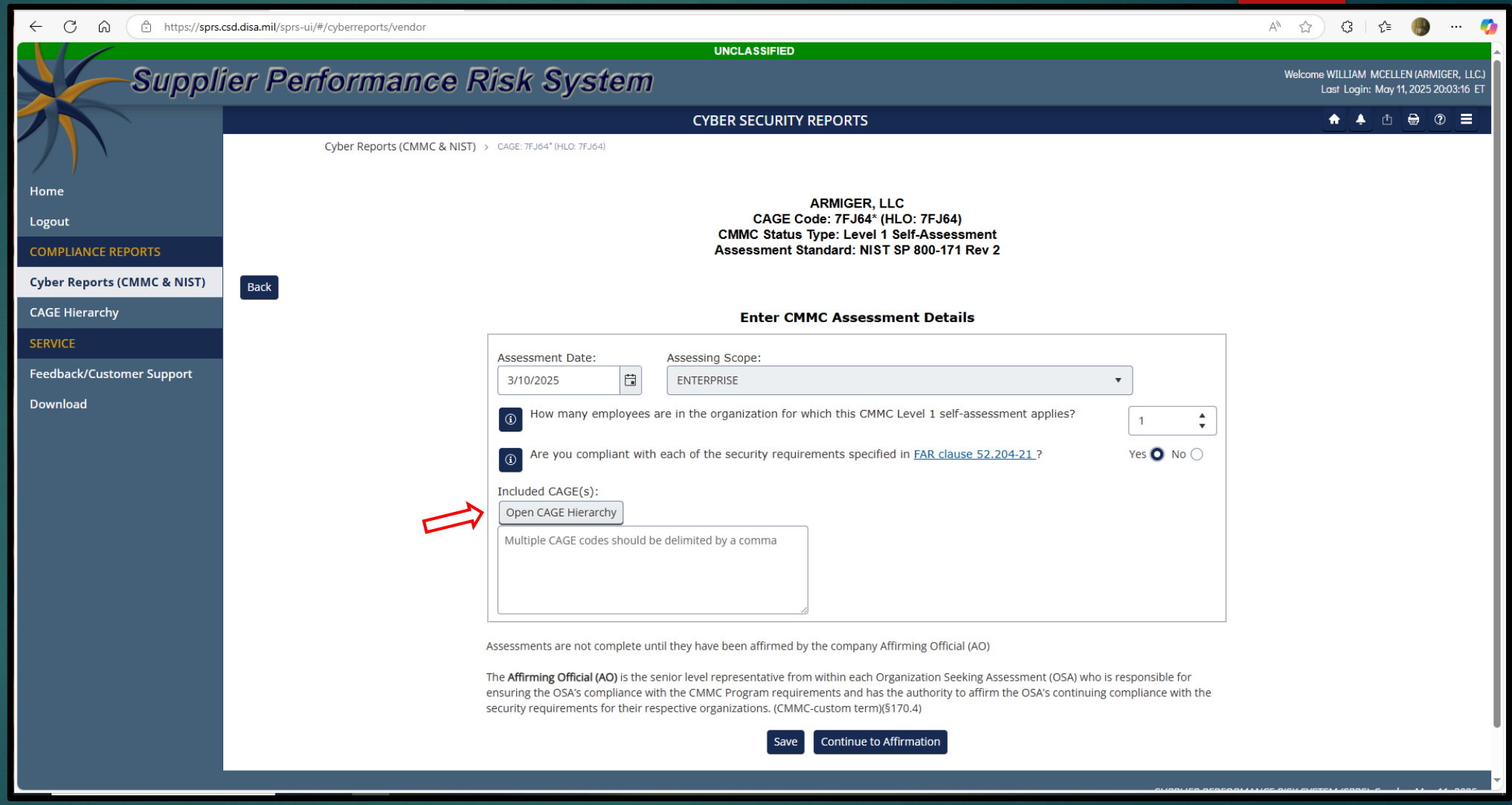
Review the warning and acknowledge



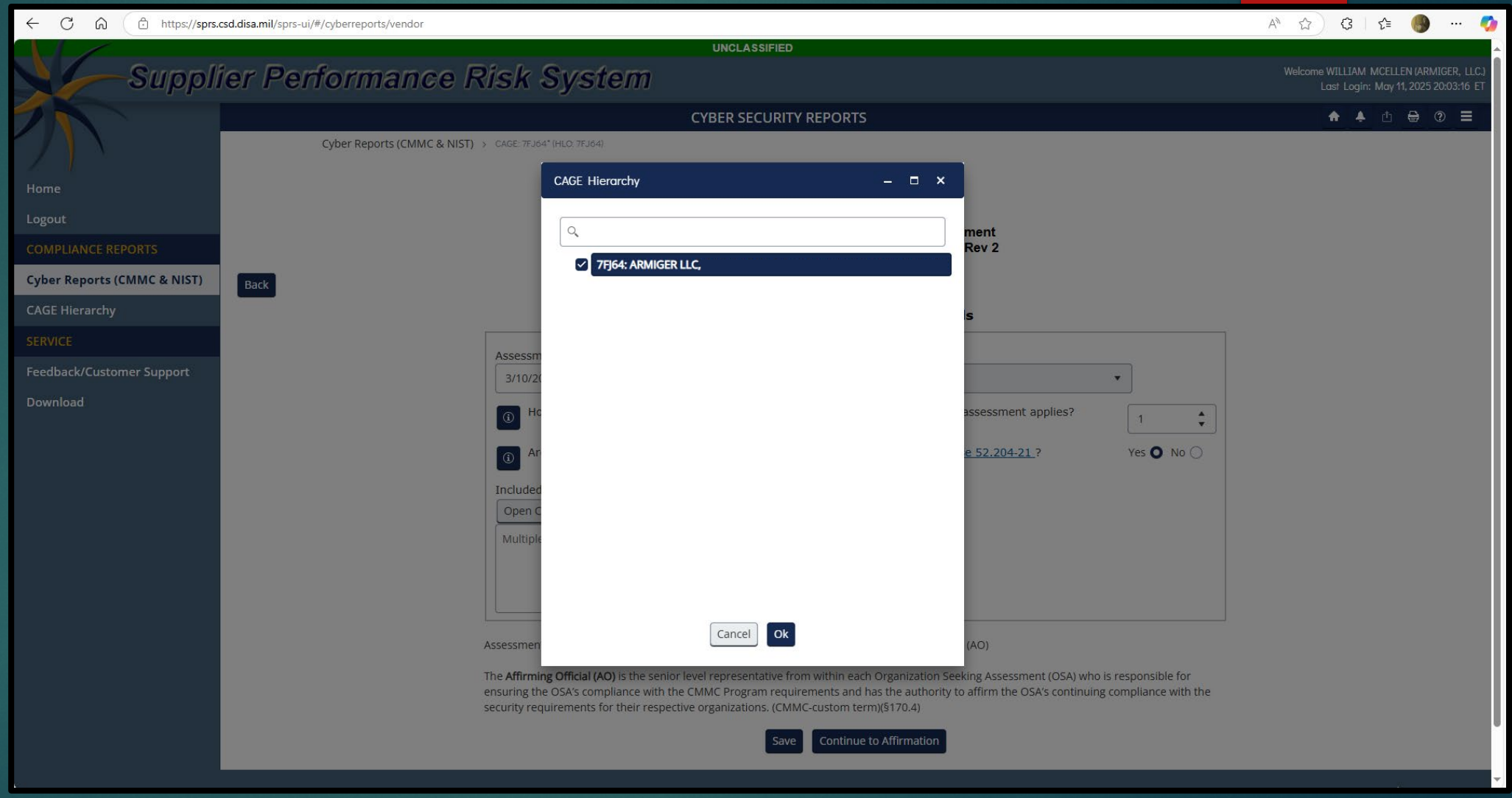
There are 4 items that need to be completed for Level 1 (Self)



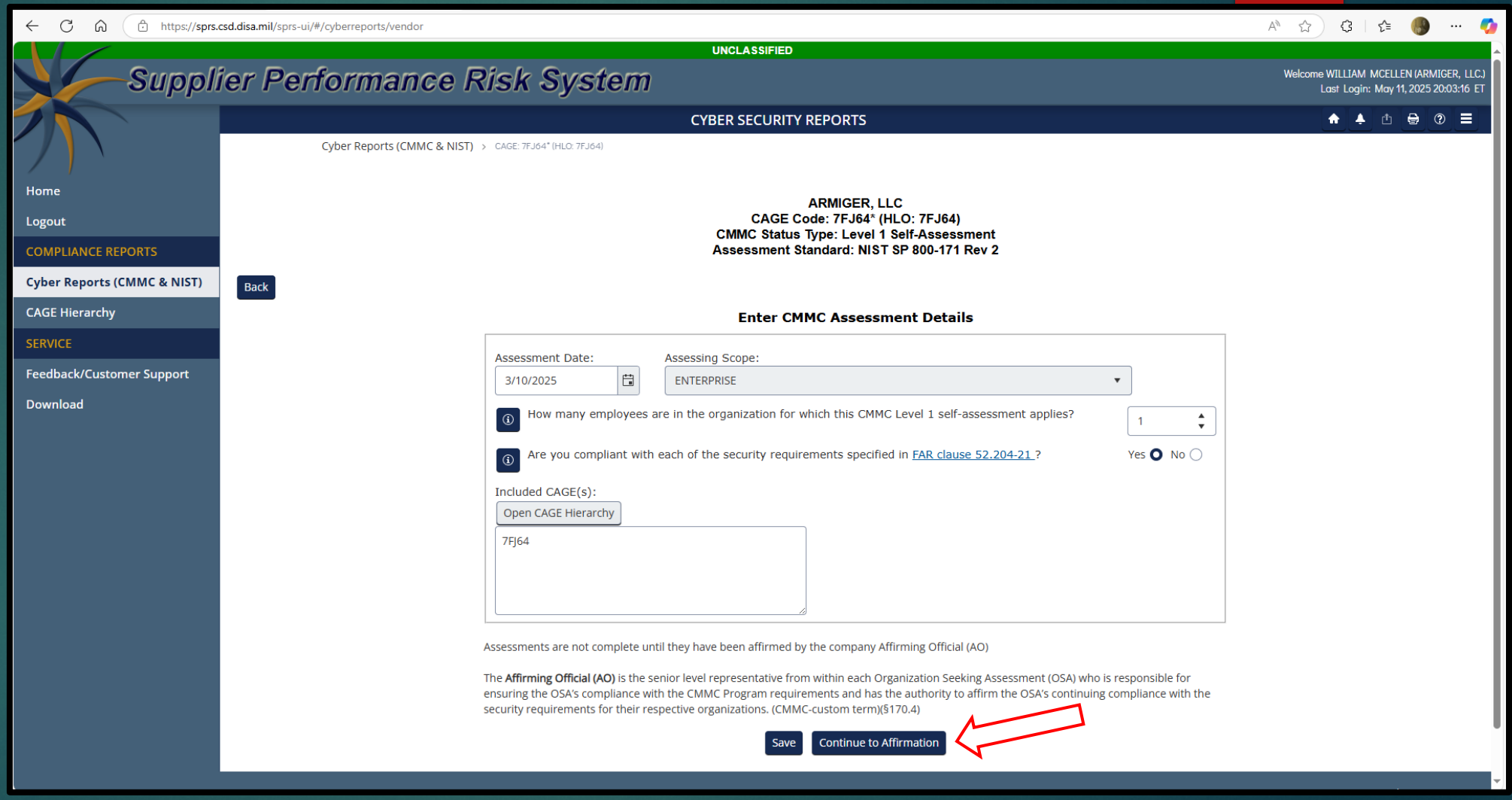
Once all items are complete, click on ‘Open CAGE Hierarchy’



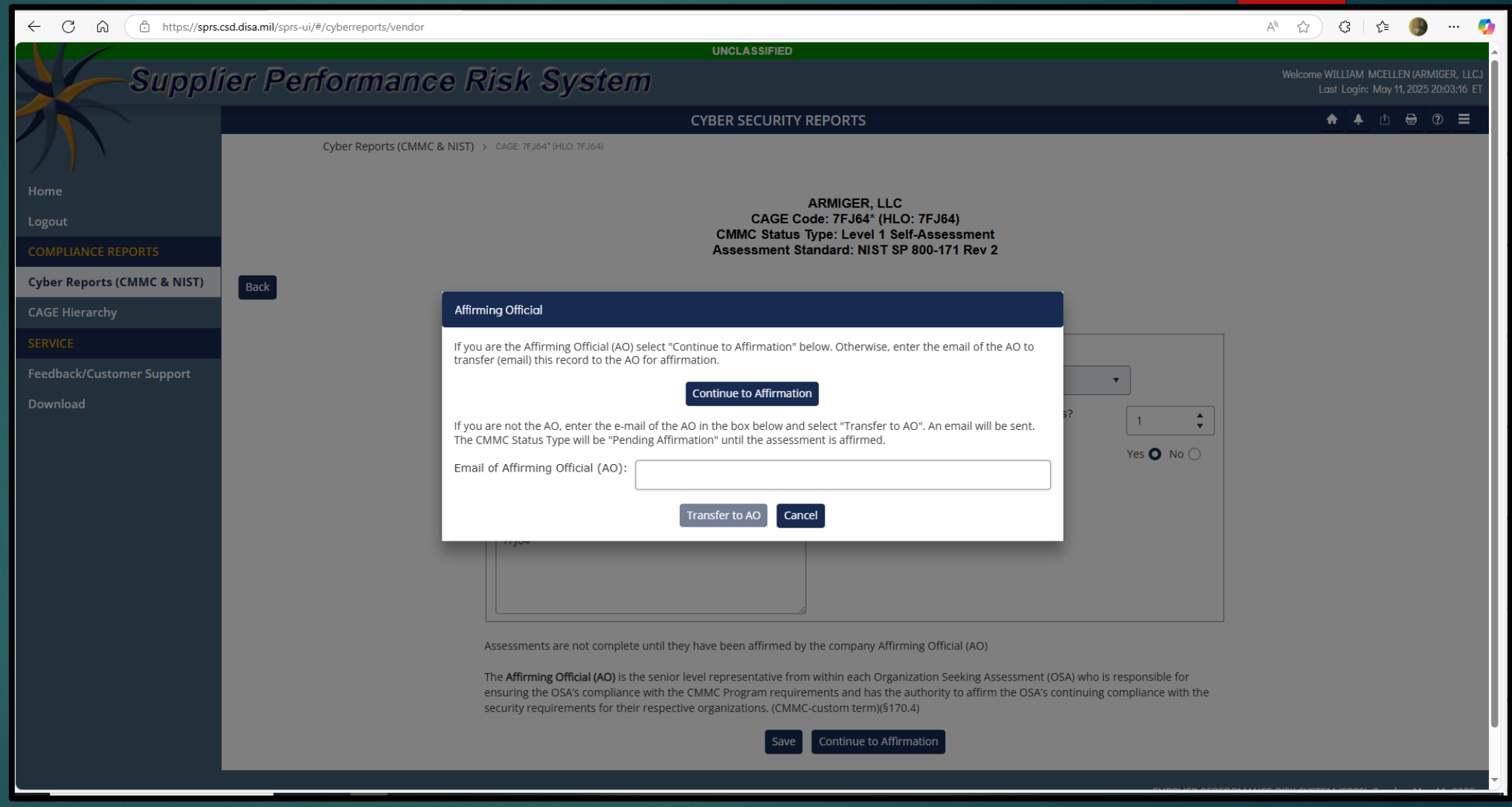
Select the appropriate CAGE



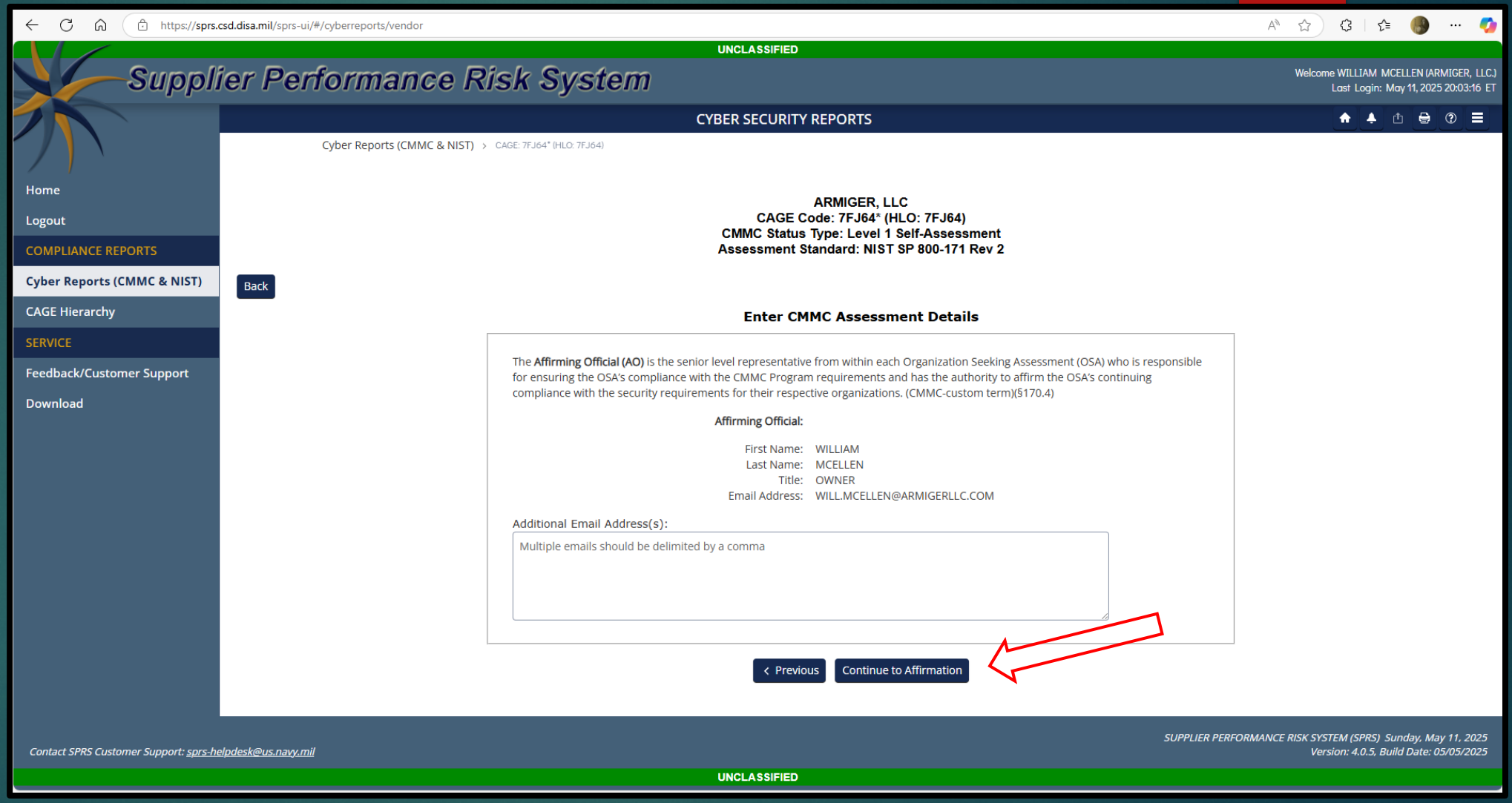
If everything is correct, ‘Continue to Affirmation’



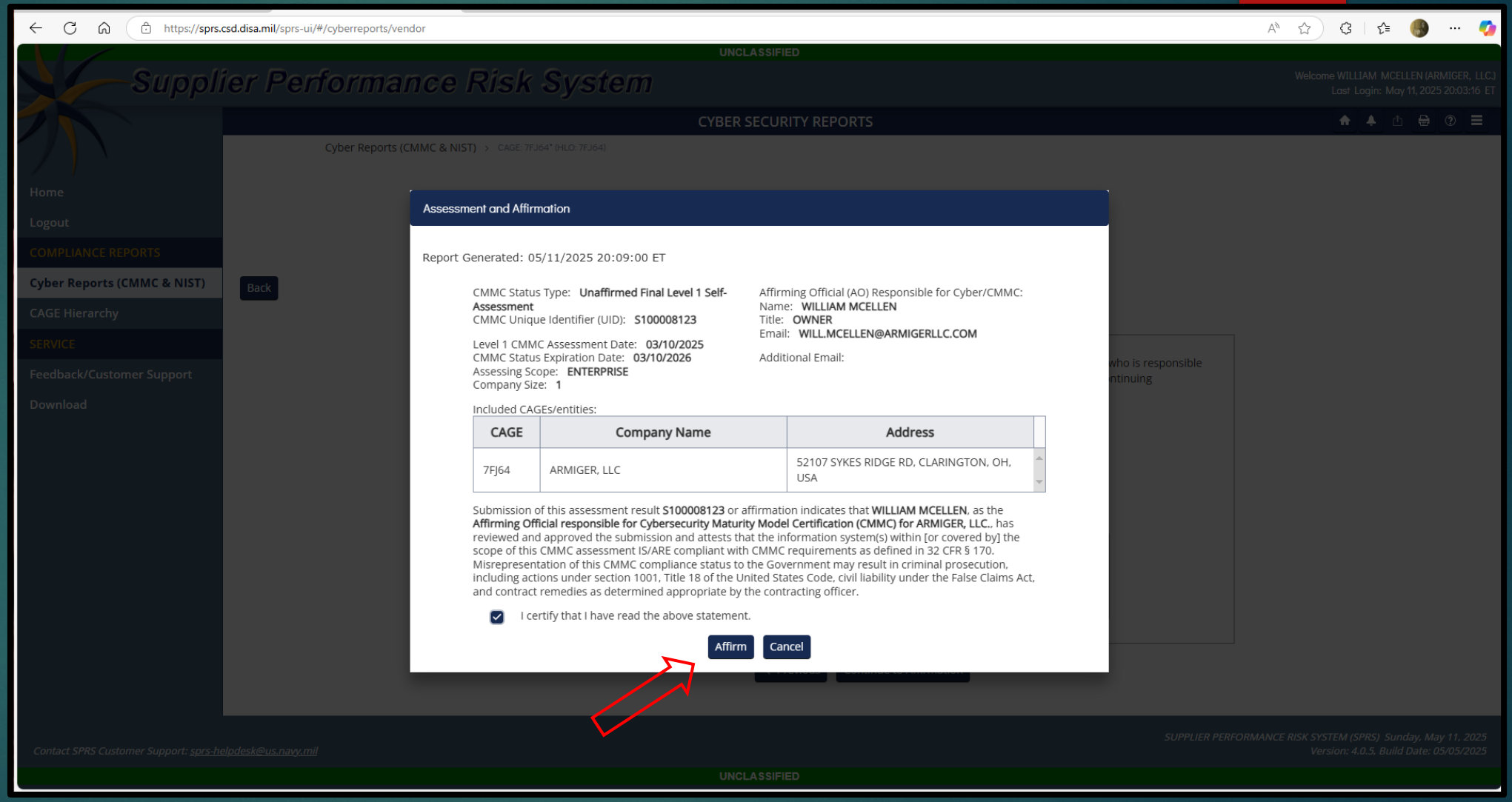
If you are the Affirmer, you can continue. If not, provide Affirmer's e-mail



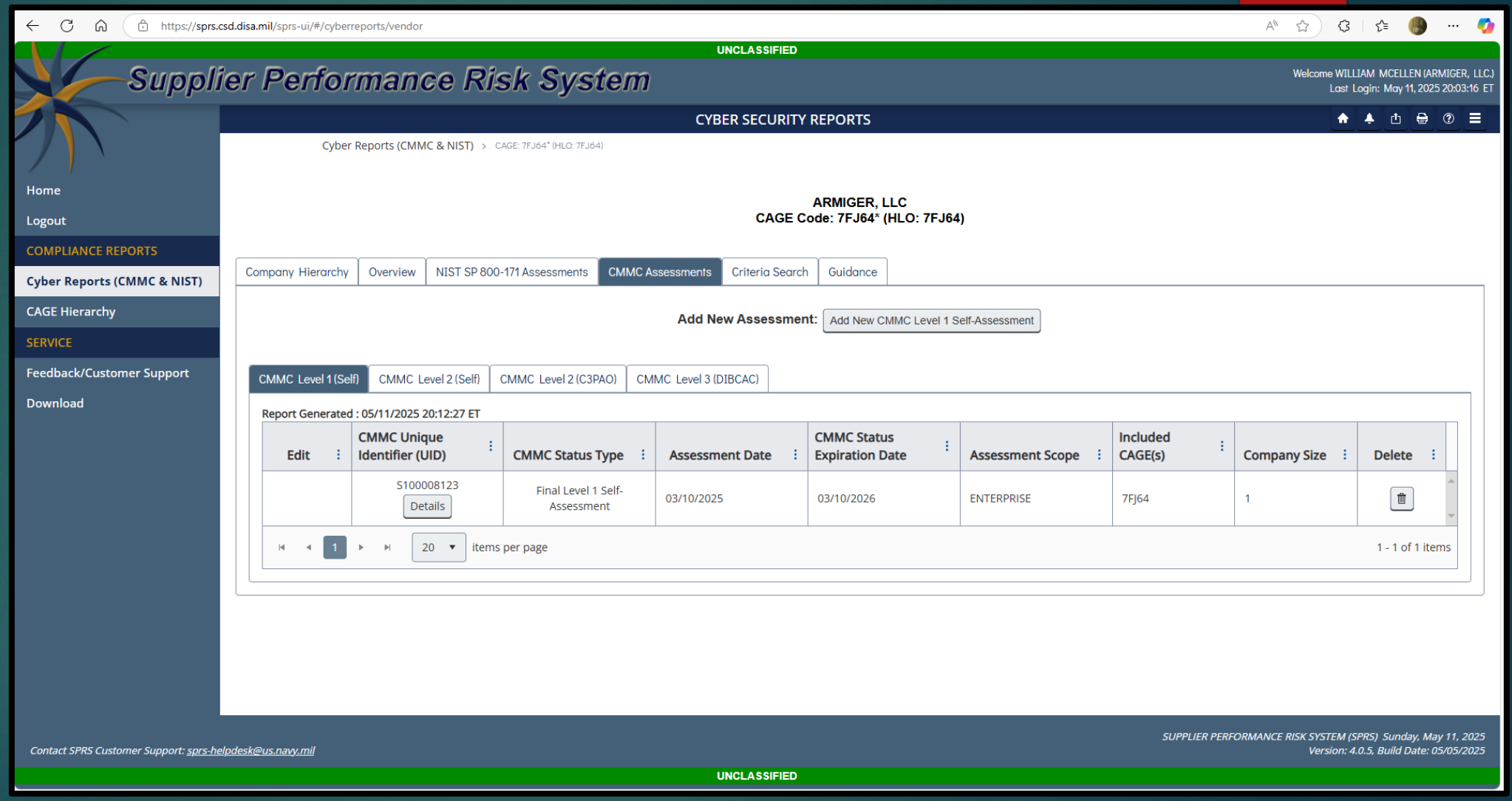
Verify your details as the Affirmer and ‘Continue to Affirmation’



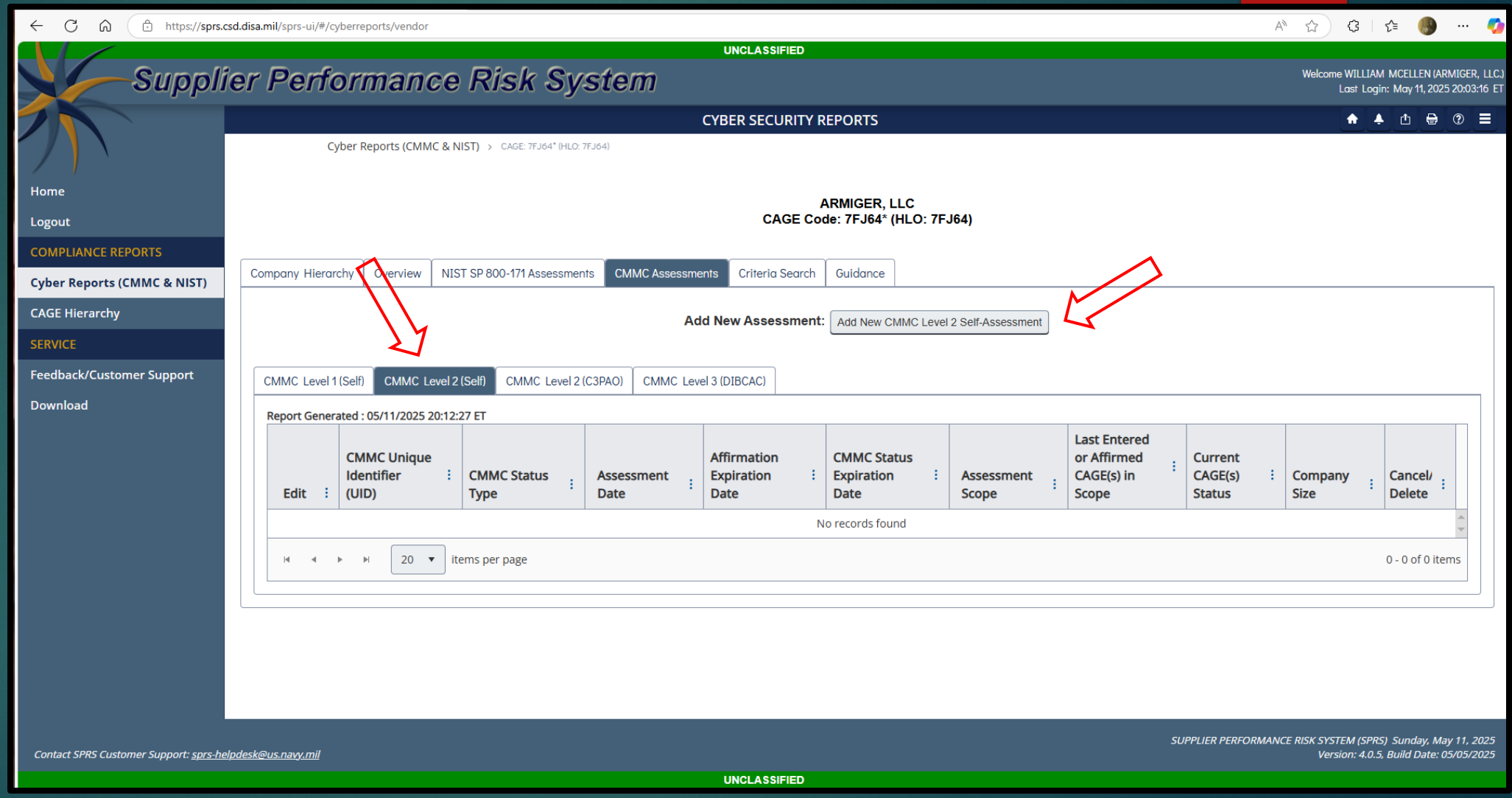
Read the certification statement, check the box, and click ‘Affirm’



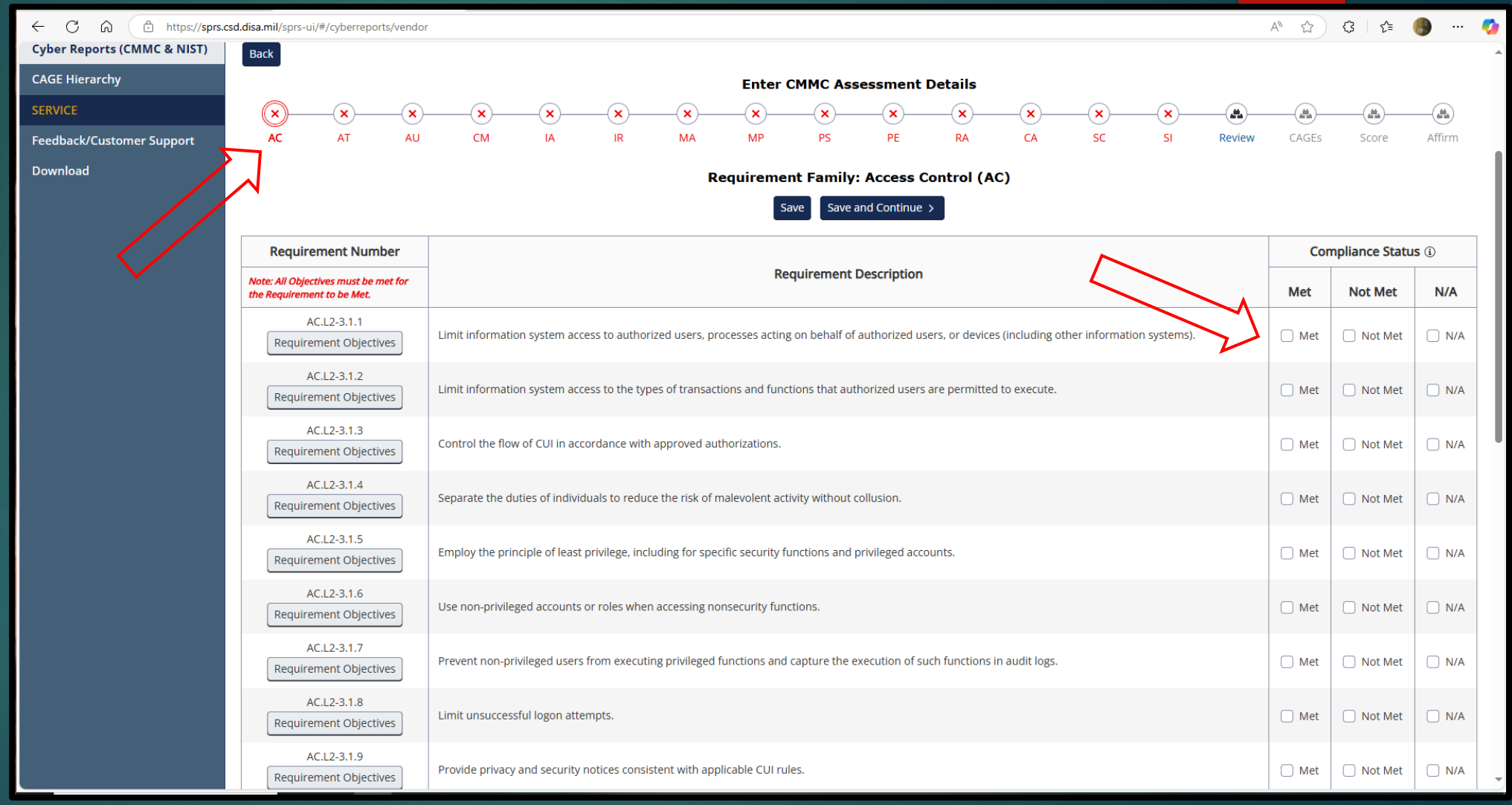
Your assessment is now entered. Note that it can't be edited, just deleted



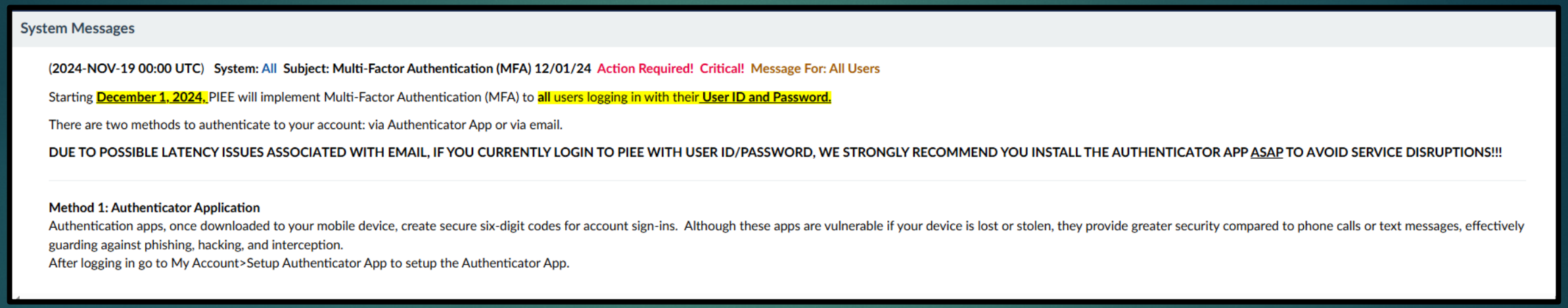
As a quick overview, additional CMMC Levels have increased requirements.



For Level 2 (Self) you will need to annotate compliance for each required control



One additional note:



System Messages

(2024-NOV-19 00:00 UTC) **System: All Subject: Multi-Factor Authentication (MFA) 12/01/24 Action Required! Critical! Message For: All Users**

Starting **December 1, 2024,** PIEE will implement Multi-Factor Authentication (MFA) to **all** users logging in with their **User ID and Password.**

There are two methods to authenticate to your account: via Authenticator App or via email.

DUE TO POSSIBLE LATENCY ISSUES ASSOCIATED WITH EMAIL, IF YOU CURRENTLY LOGIN TO PIEE WITH USER ID/PASSWORD, WE STRONGLY RECOMMEND YOU INSTALL THE AUTHENTICATOR APP ASAP TO AVOID SERVICE DISRUPTIONS!!!

Method 1: Authenticator Application

Authentication apps, once downloaded to your mobile device, create secure six-digit codes for account sign-ins. Although these apps are vulnerable if your device is lost or stolen, they provide greater security compared to phone calls or text messages, effectively guarding against phishing, hacking, and interception.

After logging in go to My Account>Setup Authenticator App to setup the Authenticator App.

Any Questions?

For a copy of this presentation…

Option 1: Please send an e-mail to, SPRS@ARMIGERLLC.COM (please include "FISWG Presentation" in subject line)

Option 2: It will be available in a few days on the FISWG site, https://fiswg.research.ucf.edu/education.html