



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)	<ul style="list-style-type: none"> 15 required by FAR clause 52.204-21 	<ul style="list-style-type: none"> Conducted by Organization Seeking Assessment (OSA) annually Results entered into the Supplier Performance Risk System (SPRS) 	<ul style="list-style-type: none"> Not permitted 	<ul style="list-style-type: none"> After each assessment Entered into SPRS
Level 2 (Self)	<ul style="list-style-type: none"> 110 NIST SP 800-171 R2 required by DFARS clause 252.204-7012 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> After each assessment and annually thereafter Assessment will lapse upon failure to annually affirm Entered into SPRS
Level 2 (C3PAO)	<ul style="list-style-type: none"> 110 NIST SP 800-171 R2 required by DFARS clause 252.204-7012 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> After each assessment and annually thereafter Assessment will lapse upon failure to annually affirm Entered into SPRS
Level 3 (DIBCAC)	<ul style="list-style-type: none"> 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) 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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

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'

The screenshot shows the homepage of the Procurement Integrated Enterprise Environment (PIEE). The browser address bar displays 'piee.eb.mil'. A banner at the top states 'An official website of the United States government.' The navigation menu includes 'ABOUT', 'FEATURES', 'CAPABILITIES', 'HELP', and 'CONTACT'. The 'NEW USER' and 'LOG IN' buttons are circled in red. The main heading is 'Procurement Integrated Enterprise Environment', followed by the subtitle 'Enterprise services, capabilities, and systems supporting the end-to-end Procure-to-Pay (P2P) business process'. Below this are 'VIEW FEATURES' and 'VIEW RESOURCES' buttons. The footer features the text 'Trusted by our government' and logos for the U.S. Department of Defense, U.S. Air Force, U.S. Army, and U.S. Navy. A blue 'back to top' button is located in the bottom right corner.

Select 'Register'. Note that additional resources can be found here

piee.eb.mil/xhtml/unauth/help/newuser.xhtml

PIEE
7.0.6 Procurement Integrated Enterprise Environment

New User Setup and Help

New User

New Vendor Getting Started

- New Vendor Organization - Getting Started Help
 - Required Setup and Registration steps for all new Vendor organizations
- Vendor Registration information and demonstration
 - Information and demonstration for new Vendor users for existing organizations in PIEE.

Government and Government Support Contractors Getting Started

- WAWF - Government Getting Started Help
- WAWF - Support Contractor Getting Started Help
- EDA - Government Getting Started Help
- EDA - Support Contractor Getting Started Help
- IUID - Government Getting Started Help

Setup

- Machine Setup

Help and Information

Help Links

- FAQ
- New User Information and Help
- Government Access Approval Process
- PIEE User Role List

Training

- Web Based Training
 - Vendor Registration information and demonstration
 - Gov and CTR Registration
 - State/Local Employee registration information and demonstration
 - PIEE Government User - Add/Manage PIEE User Training

System Information

- WAWF Functional Information
- WAWF Instructions clause Information

Close Register

Select 'Agree'

piee.eb.mil/xhtml/unauth/registration/notice.xhtml

PIEE
7.0.6 Procurement Integrated Enterprise Environment

Privacy Act Statement

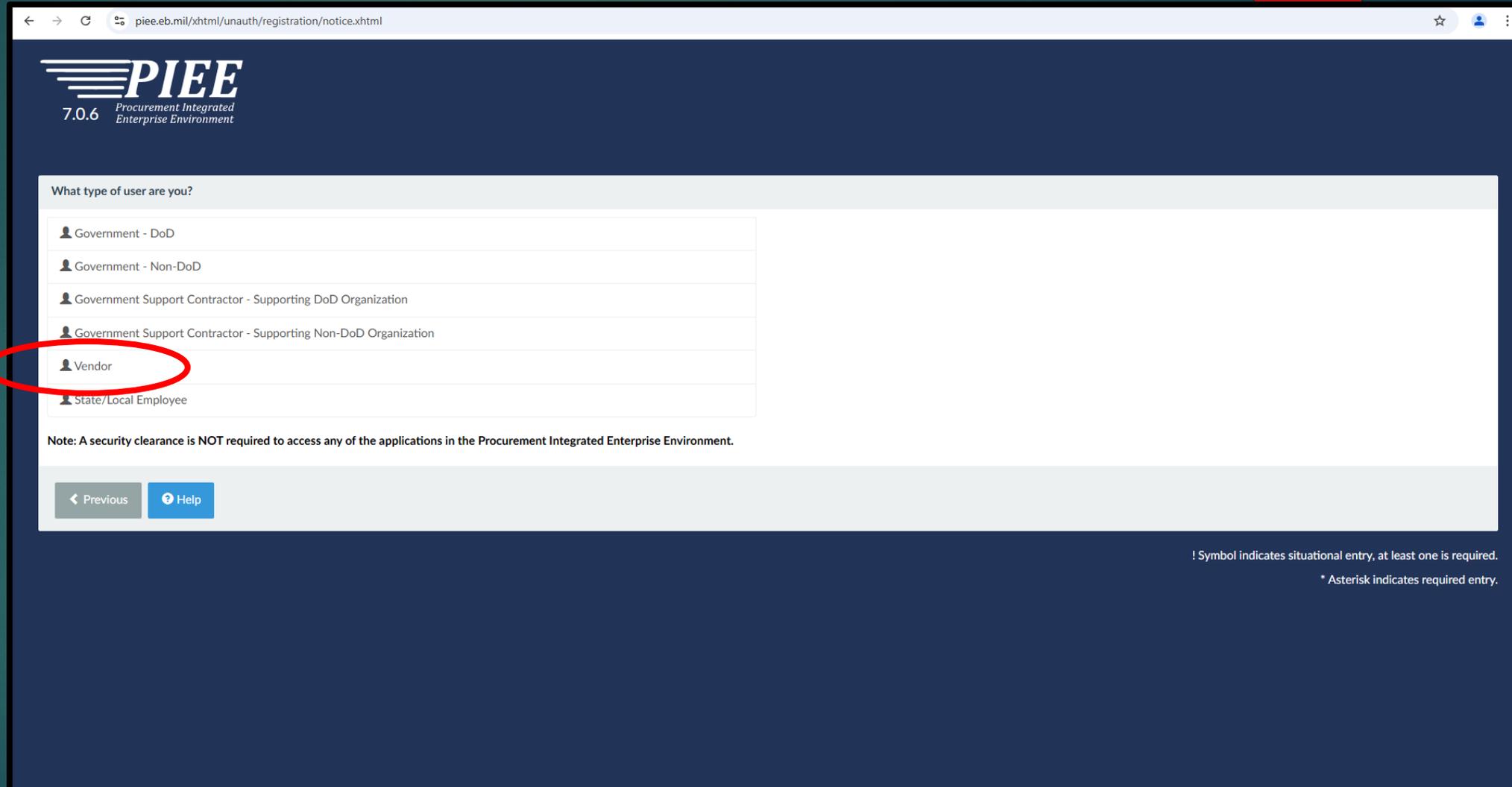
AUTHORITY:	Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act.
PRINCIPAL PURPOSE:	To record names, signatures, and other identifiers for the purpose of validating the trustworthiness of individuals requesting access to Department of Defense (DoD) systems and information. NOTE: Records may be maintained in both electronic and/or paper form.
ROUTINE USES:	None
DISCLOSURE:	Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.

I have read and understand the terms and conditions for use of this website.

Agree

! Symbol indicates situational entry, at least one is required.
* Asterisk indicates required entry.

Register as a 'Vendor'



The screenshot shows a web browser window with the URL `piee.eb.mil/xhtml/unauth/registration/notice.xhtml`. The page header features the PIEE logo (Procurement Integrated Enterprise Environment) and version 7.0.6. The main content area is titled "What type of user are you?" and contains a list of user roles. The "Vendor" option is circled in red. Below the list is a note about security clearance requirements and navigation buttons for "Previous" and "Help".

7.0.6 Procurement Integrated Enterprise Environment

What type of user are you?

- Government - DoD
- Government - Non-DoD
- Government Support Contractor - Supporting DoD Organization
- Government Support Contractor - Supporting Non-DoD Organization
- Vendor
- State/Local Employee

Note: A security clearance is NOT required to access any of the applications in the Procurement Integrated Enterprise Environment.

[← Previous](#) [? Help](#)

! Symbol indicates situational entry, at least one is required.
* Asterisk indicates required entry.

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

piee.eb.mil/xhtml/unauth/registration/registration.xhtml?cid=2



Registration Steps

1. Registration Home
- 2. Authentication**
3. Profile
4. EB POC / Company
5. Roles
6. Justification
7. Summary
8. Agreement

Authentication

How will you be accessing the Procurement Integrated Enterprise Environment applications? *

User ID \ Password

User ID *

Password *

Password Confirmation *

CAPTCHA Image

508731

Audio Reload

Enter in text in image above.

User ID Rules

- Minimum 8 Characters.
- May Contain ONLY the following special characters ~ ! # \$. _ { }
- May NOT contain spaces.
- Must not already be registered in the Procurement Integrated Enterprise Environment.

Password Rules

- Minimum 15 characters
- Maximum 40 characters
- Must contain at least 1 capital letter
- Must contain at least 1 lower case letter
- Must contain at least 1 number
- Must contain at least 1 special character
- Entered passwords must be different from last 10 passwords used
- Cannot be changed within 24 hours
- Entered passwords cannot be the same as User ID

Next Previous Home Help

! Symbol indicates situational entry, at least one is required.
* Asterisk indicates required entry.

Create Security Questions

The screenshot shows a web browser window with the URL `piee.eb.mil/xhtml/unauth/registration/authentication.xhtml?cid=2`. The page header features the PIEE logo (Procurement Integrated Enterprise Environment) and version 7.0.6. A left sidebar lists registration steps: 1. Registration Home, 2. Authentication, 3. Security Questions (active), 4. Profile, 5. EB POC / Company, 6. Roles, 7. Justification, 8. Summary, and 9. Agreement. The main content area is titled "Security Questions" and includes a warning: "WARNING: We suggest picking unique security questions/answers which cannot be looked up via the following means: Answers might be obtained via googling, blogs, personal websites, genealogy charts, online social networks (facebook, myspace, etc.), high school website, picture sites (flickr, photobucket, shutterfly), online phone books, reverse phone look-ups, and other online resources." Below this, there are three rows of input fields. Each row consists of a "Question" dropdown menu (all containing "Where is your high school located?"), an "Answer" text input field, and an "Answer Confirmation" text input field. All fields are marked with an asterisk (*). At the bottom of the form are three buttons: "Next", "Previous", and "Help".

Registration Steps

1. Registration Home
2. Authentication
3. Security Questions
4. Profile
5. EB POC / Company
6. Roles
7. Justification
8. Summary
9. Agreement

Security Questions

WARNING: We suggest picking unique security questions/answers which cannot be looked up via the following means: Answers might be obtained via googling, blogs, personal websites, genealogy charts, online social networks (facebook, myspace, etc.), high school website, picture sites (flickr, photobucket, shutterfly), online phone books, reverse phone look-ups, and other online resources.

Question 1 *	Answer 1 *	Answer Confirmation 1 *
Where is your high school located?	<input type="text"/>	<input type="text"/>
Question 2 *	Answer 2 *	Answer Confirmation 2 *
Where is your high school located?	<input type="text"/>	<input type="text"/>
Question 3 *	Answer 3 *	Answer Confirmation 3 *
Where is your high school located?	<input type="text"/>	<input type="text"/>

[Next](#) [Previous](#) [Help](#)

! Symbol indicates situational entry, at least one is required.
* Asterisk indicates required entry.

Complete your User Profile

piee.eb.mil/xhtml/unauth/registration/securityQuestions.xhtml?cid=2



Registration Steps

- 1. Registration Home
- 2. Authentication
- 3. Security Questions
- 4. Profile**
- 5. EB POC / Company
- 6. Roles
- 7. Justification
- 8. Summary
- 9. Agreement

User Profile

First Name *	Middle Name	Last Name *	Suffix	
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	
CAGE Code *	Organization *	Job Title *		
<input type="text"/>	<input type="text"/>	<input type="text"/>		
Email *	Confirm Email *			
<input type="text"/>	<input type="text"/>			
Commercial Telephone !	Extension	Intl Country Code and Phone !	Mobile Telephone	DSN Telephone
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Citizenship *				
<input type="text" value="US"/>				

[Next](#) [Previous](#) [Save Registration](#) [Help](#)

! Symbol indicates situational entry, at least one is required.
* Asterisk indicates required entry.

Click >Next

71010 Enterprise Environment

piee.eb.mil/xhtml/unauth/registration/profile.xhtml?cid=2

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	EB POC Email	EB POC Phone
WILLIAM MCELLEN	[REDACTED]	[REDACTED]

EB POC ALT Name	EB POC ALT Email	EB POC Phone
WILLIAM MCELLEN	[REDACTED]	[REDACTED]

Company Information

Name	Address		
ARMIGER, LLC	[REDACTED]		
City	State	Zip	Country
[REDACTED]	Ohio	[REDACTED]	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

The screenshot displays the PIEE (Procurement Integrated Enterprise Environment) registration interface. The browser address bar shows the URL: `piee.eb.mil/xhtml/unauth/registration/additionalProfileInfo.xhtml?cid=2`. The PIEE logo and version (7.0.6) are visible in the top left. A sidebar on the left lists the registration steps, with '6. Roles' selected. The main content area is titled 'Roles' and contains the following steps:

- Step 1. Select the appropriate Application from the list below**: A dropdown menu is shown with 'WAWF - Wide Area Workflow' selected. This dropdown is circled in red.
- Step 2. Select One or More Roles from the list below (Ctrl+Click)**: A list of roles is displayed under the heading 'User Roles for WAWF', including 'Energy Lab POC', 'Vendor', 'Vendor Ship To View Only', and 'Vendor View Only'. An 'Add Roles' button is present.
- Step 3. Click 'Add Roles'**: A button labeled '+ Add Roles' is shown.
- Step 4. Fill out the required information for the applicable applications**: Includes two tips:
 - Tip** If you need access to any other applications, Repeat Steps 1 to 4 again
 - Tip** You can view a list of all PIEE roles and their descriptions and functions in the PIEE Role List Matrix.

At the bottom of the main content area, there are navigation buttons: 'Next', 'Previous', 'Save Registration', and 'Help'.

! Symbol indicates situational entry, at least one is required.
* Asterisk indicates required entry.

Select 'PIEE – Procurement Integrated Enterprise Environment'

The screenshot shows the registration interface for the Procurement Integrated Enterprise Environment (PIEE) 7.0.6. On the left, a 'Registration Steps' sidebar lists steps from 1 to 9, with '6. Roles' selected. The main content area is titled 'Roles' and contains three steps: 'Step 1. Select the appropriate Application from the list below', 'Step 2. Select One or More Roles from the list below (Ctrl+Click)', and 'Step 3. Click 'Add Roles''. Under Step 1, a dropdown menu is open, showing a list of applications. The 'PIEE - Procurement Integrated Enterprise Environment' option is highlighted with a red circle. Under Step 2, a list of roles for the selected application (WAWF) is shown, including 'Energy Lab POC', 'Vendor', 'Vendor Ship To View Only', and 'Vendor View Only'. A '+ Add Roles' button is visible next to the role list.

Registration Steps

1. Registration Home
2. Authentication
3. Security Questions
4. Profile
5. EB POC / Company
6. Roles
7. Justification
8. Summary
9. Agreement

Roles

Step 1. Select the appropriate Application from the list below

- WAWF - Wide Area Workflow
- AMT - Award Management Team
- CSP - Contractor Submission Portal
- DFE - Duty Free Entry
- DSM - Delivery Schedule Manager
- FedMall
- GFP - Government Furnished Property
- IUID Registry
- PEREP - Product Data Reporting and Evaluation Program
- PIEE - Procurement Integrated Enterprise Environment**
- RFQ - Solicitation
- SPRS - Supplier Performance Risk System
- WAWF - Wide Area Workflow

Step 2. Select One or More Roles from the list below (Ctrl+Click)

User Roles for WAWF

- Energy Lab POC
- Vendor
- Vendor Ship To View Only
- Vendor View Only

+ Add Roles

! Symbol indicates situational entry, at least one is required.
* Asterisk indicates required entry.

Select 'Contract Administrator' under Step 2 then click '+ Add Roles'

The screenshot shows the PIEE 7.0.6 registration interface. On the left is a 'Registration Steps' sidebar with 9 items, where '6. Roles' is selected. The main content area is titled 'Roles' and contains three steps:

- Step 1:** Select the appropriate Application from the list below. A dropdown menu shows 'PIEE - Procurement Integrated Enterprise Environment'.
- Step 2:** Select One or More Roles from the list below (Ctrl+Click). A list of roles is shown, with 'Admin Roles for PIEE' and 'Contract Administrator' selected and circled in red.
- Step 3:** Click 'Add Roles'. A button labeled '+ Add Roles' is visible, with a red arrow pointing to it.

Step 4: Fill out the required information for the applicable applications.

Tip: If you need access to any other applications, Repeat Steps 1 to 4 again

Tip: You can view a list of all PIEE roles and their descriptions and functions in the PIEE Role List Matrix.

At the bottom, there are navigation buttons: 'Next', 'Previous', 'Save Registration', and 'Help'.

! Symbol indicates situational entry, at least one is required.
* Asterisk indicates required entry.

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

The screenshot shows the PIEE 7.0.6 registration interface. The left sidebar lists registration steps from 1 to 9, with '6. Roles' selected. The main content area is titled 'Roles' and contains three steps: Step 1 (Application selection), Step 2 (Role selection), and Step 4 (Information filling). Step 4 is completed, showing a 'Roles Summary' table with one entry: 'PIEE' with role 'Contractor Administrator'. The 'Next' button at the bottom is circled in red.

Registration Steps

1. Registration Home
2. Authentication
3. Security Questions
4. Profile
5. EB POC / Company
6. Roles
7. Justification
8. Summary
9. Agreement

Roles

Step 1. Select the appropriate Application from the list below

PIEE - Procurement Integrated Enterprise Environment

Step 2. Select One or More Roles from the list below (Ctrl+Click)

Admin Roles for PIEE
Contractor Administrator

Step 3. Click 'Add Roles'

+ Add Roles

Step 4. Fill out the required information for the applicable applications

Roles Summary

Application	Role	Location Code / CAGE *	Extension	Group	Action
PIEE	Admin Group Contractor Administrator	N/A	N/A	7FJ64	Delete

Showing 1 to 1 of 1 entries

Tip If you need access to any other applications, Repeat Steps 1 to 4 again

Tip You can view a list of all PIEE roles and their descriptions and functions in the PIEE Role List Matrix.

> Next Previous Save Registration Help

! Symbol indicates situational entry, at least one is required.

* Asterisk indicates required entry.

Provide a Justification – anything will do

The screenshot shows a web browser window with the URL `piee.eb.mil/xhtml/unauth/registration/roles.xhtml?cid=2`. The page header includes the PIEE logo and version `7.0.6 Procurement Integrated Enterprise Environment`. A left sidebar lists registration steps, with `7. Justification` selected. The main content area is titled `Justification / Attachments` and contains an information message, a required text field for justification, an attachment upload section, and a warning message. Navigation buttons for `Next`, `Previous`, and `Help` are at the bottom.

Registration Steps

- 1. Registration Home
- 2. Authentication
- 3. Security Questions
- 4. Profile
- 5. EB POC / Company
- 6. Roles
- 7. Justification
- 8. Summary
- 9. Agreement

Justification / Attachments

info Provide justification for access and upload any necessary attachments.

Justification *

Attachments

Browse... Upload

Warning! Procurement Integrated Enterprise Environment is designated for Sensitive Unclassified information ONLY. Do NOT enter classified information in this system.

Next Previous Help

! Symbol indicates situational entry, at least one is required.

* Asterisk indicates required entry.

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

The screenshot shows a web browser window with the URL `piee.eb.mil/xhtml/unauth/registration/roles.xhtml?cid=2`. The page header features the **PIEE** logo (Procurement Integrated Enterprise Environment) and version **7.0.6**. A left sidebar lists the registration steps, with **7. Justification** selected and marked with a red asterisk. The main content area is titled **Justification / Attachments** and includes an information icon and text: "Provide justification for access and upload any necessary attachments." Below this is a **Justification *** section with a text input field containing "Submit SPRS Score for contract compliance." An **Attachments** section contains a "Browse..." button, a file upload progress bar, and an "Upload" button. A red warning icon and text state: "Warning! Procurement Integrated Enterprise Environment is designated for Sensitive Unclassified information ONLY. Do NOT enter classified information in this system." At the bottom, there are "Next", "Previous", and "Help" buttons. A footer note reads: "! Symbol indicates situational entry, at least one is required. * Asterisk indicates required entry."

Registration Steps

- 1. Registration Home
- 2. Authentication
- 3. Security Questions
- 4. Profile
- 5. EB POC / Company
- 6. Roles
- 7. Justification
- 8. Summary 
- 9. Agreement

Registration Summary - Please Verify All the information

User Information

User ID [Redacted]

User Type Vendor

Login Method User ID \ Password

User Profile 

First Name * William Middle Name Thomas Last Name * McEllen Suffix

CAGE Code * 7FJ64 Organization * Armiger, LLC. Job Title * Owner

Email * [Redacted]

Commercial Telephone ! [Redacted] Extension Intl Country Code and Phone ! Mobile Telephone [Redacted] DSN Telephone

Citizenship * US

EB POC Information

EB POC Name WILLIAM MCELLEN EB POC Email [Redacted]

EB POC Phone [Redacted]

EB POC ALT Name WILLIAM MCELLEN EB POC ALT Email [Redacted]

EB POC Phone [Redacted]

Company Information

Name Address

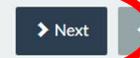
ARMIGER, LLC [Redacted]

City State Zip Country

[Redacted] Ohio [Redacted] United States of Amer

User Roles 

Role	Location Code Type	Location Code	Extension	Group
Admin Group Contractor Administrator				7FJ64

Review Info then click >Next

Registration Steps

- 1. Registration Home
- 2. Authentication
- 3. Security Questions
- 4. Profile
- 5. EB POC / Company
- 6. Roles
- 7. Justification
- 8. Summary
- 9. Agreement

Agreement

Statement of Accountability Agreement

I understand my obligation to protect my password/certificate. I assume the responsibility for the data and system I am granted access to. I will not exceed my authorized access.
[Standard Mandatory Notice & Consent Provision For All DoD Information System User Agreements 9 May 2008.](#)

[Security and Privacy Rules of Behavior \(ROB\) / Acceptable Use Policy \(AUP\) 14 Jan 2010.](#)

The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counter-intelligence (CI) investigations.

At any time, the U.S. Government may inspect and seize data stored on this information system. Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose.

This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests--not for your personal benefit or privacy.

Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:

Nothing in the User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operation,

By signing below, I accept the System User Agreement and Rules of Behavior / Acceptable Use Policy.

Government/Contractor Admin Appointment Letter

1. You are hereby appointed as a Contractor Administrator (CAM) for the Procurement Integrated Enterprise Environment (PIEE). Your span of control includes the following group names. [null/7FJ64]

2. As a CAM, you are a critical part of maintaining system security because you have the ability to grant/deny access to users.

3. You accept the CAM role as a trusted agent for your agency. You will comply with all agency policies regarding security functions performed in support of your agency and the PIEE Program Office.

4. You are responsible for the following activities:

a. Establish and maintain organizational e-mail for each CAGE under your span of control.

b. Activate/Inactivate users in your group.

c. Establish the position of trust for non-CAC users.

d. Any CAM activating a Vendor as a CAM must validate Vendor's identity by verifying information the Vendor has entered during the registration process (i.e. security questions and answers)

5. When determining privileges and profiles, you will comply with the principle of least privilege (Granting minimal access for that which the user needs).

6. As a CAM you will verify the identity of an individual by validating the access approval process within the Procurement Integrated Enterprise Environment. In addition, you are responsible for ensuring compliance with the PIEE access control policy along with additional access control guidance issued by your Agency and/or Service.

7. You will ensure timely notification and notification of suspected incidents in accordance with your agency's incident response policy.

8. You agree to have your first name, last name, phone number and email address as contact information for users under your administration listed on the PIEE web site.

By signing below, I acknowledge my appointment. I have read and understand my responsibilities and accountability as contained in this Appointment Letter. I have also been briefed on my specific roles and responsibilities as defined in this Appointment Letter. I further understand that this appointment will remain in effect until revoked in writing.

Signature Date

2024/11/20

Signature

< Previous

Help

Review and click
'Signature'

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

piee.eb.mil/xhtml/unauth/registration/agreement.xhtml?cid=2



Registration Steps

1. Registration Home
2. Authentication
3. Security Questions
4. Profile
5. EB POC / Company
6. Roles
7. Justification
8. Summary
9. Agreement

Agreement

Info: As of 2024/11/20 22:11:33 UTC, an email was sent to your email account will.mccillen@armigerllc.com with a One-Time Password (OTP). This password will expire in 900 seconds.

By signing, I accept the System User Agreement and Rules of Behavior / Acceptable Use Policy.

The PIEE signature requirement has changed to allow support for all the major browsers. Click here for more information.

OTP * Send OTP via E-Mail

Submit Registration

Please Wait...

Statement of Accountability Agreement

I understand my obligation to protect my personal information and the information of others. I agree to the Standard Mandatory Notice & Consent Privacy Practices that apply to the information that will be collected, used, and disclosed by the U.S. Government.

Security and Privacy Rules of Behavior (RBOB)

The U.S. Government routinely intercepts and monitors communications used for network operations and defense, personnel protection, and intelligence gathering. At any time, the U.S. Government may intercept and monitor your communications and any information you provide to a contractor or service provider, as well as information you provide to any system or device you use to access any information system or service provided by the U.S. Government. Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose. This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests—not for your personal benefit or privacy. Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below: Nothing in the User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U. S. Government actions for purposes of network administration, operation, or maintenance.

By signing below, I accept the System User Agreement and Rules of Behavior / Acceptable Use Policy.

Government/Contractor Admin Appointment Letter

1. You are hereby appointed as a Contractor Administrator (CAM) for the Procurement Integrated Enterprise Environment (PIEE). Your span of control includes the following group names. [null/7FJ64]
2. As a CAM, you are a critical part of maintaining system security because you have the ability to grant/deny access to users.
3. You accept the CAM role as a trusted agent for your agency. You will comply with all agency policies regarding security functions performed in support of your agency and the PIEE Program Office.
4. You are responsible for the following activities:
 - a. Establish and maintain organizational e-mail for each CAGE under your span of control.
 - b. Activate/Inactivate users in your group.
 - c. Establish the position of trust for non-CAC users.
 - d. Any CAM activating a Vendor as a CAM must validate Vendor's identity by verifying information the Vendor has entered during the registration process (i.e. security questions and answers).

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

The screenshot shows a web browser window with the URL `piee.eb.mil/xhtml/unauth/registration/agreement.xhtml?cid=2`. The page features the PIEE logo at the top left, which includes the text "Procurement Integrated Enterprise Environment". Below the logo, the heading "Successful Registration" is displayed. A message box contains the text: "You have successfully registered for the following applications. You will receive an e-mail containing your User ID." Below this, a paragraph states: "Once you have been activated by an administrator, or if you have been auto-activated, you will receive another email notifying you of the role(s) for which you have been activated. You may log into Procurement Integrated Enterprise Environment to check the status of your request or make changes to your profile and role information. If you have any questions, please contact the Customer Support." At the bottom left of the page, there is a dark button with a white house icon and the text "Home", which is circled in red.

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 Move Tags Editing Immersive Translate Zoom

FW: PIEE Activation Notice

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 Move Tags Editing Immersive Translate Zoom

FW: Registration has been submitted.

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

The screenshot shows the Microsoft Edge browser window with the URL <https://piee.eb.mil/xhtml/unauth/home/login.xhtml?logout=Y>. The page header includes the Microsoft Edge logo and a notification: "Would you like to set Microsoft Edge as your default browser?" with "Set as default" and "Not Now" buttons. Below the header is a banner with the PIEE logo (Procurement Integrated Enterprise Environment) and a "VIEW SYSTEM MESSAGES" button. The main content area features a "Welcome Back." heading and a sub-heading: "Log in to your account with a Common Access Card (CAC), Personal Identity Verification (PIV) Card or User ID." There are two primary login options: "Log in with Certificate" and "Log in with User ID". The "Log in with Certificate" section includes a blue button labeled "LOG IN WITH CAC / PIV CARD" and a link for "Get help with CAC / PIV Card Login". The "Log in with User ID" section has input fields for "User ID" and "Password". A red information box above the "Log in with User ID" section states: "Info: You have successfully logged out of the Procurement Integrated Enterprise Environment. For Security reasons, exit your web browser." Below the login options is a "Need help with your account?" section with a link for "FIND MY ACCOUNT ADMINISTRATOR". A CAPTCHA section is also present, showing a CAPTCHA image with the number "975553", an "AUDIO" button, and a "RELOAD" button. An input field below the CAPTCHA is labeled "Enter in text in image above."

Select 'Administration' drop-down

https://piee.eb.mil/xhtml/auth/home/home.xhtml

PIEE 7.0.6 Procurement Integrated Enterprise Environment

My Account Administration - Help

User : William McEllen Logout

Last Successful Logon Date: 2024/11/20 22:19:48 UTC

Welcome to the Procurement Integrated Enterprise Environment

Award

- Solicitation

Payment

- Wide Area Workflow (WAWF)
- myInvoice

Operational Support

- Purpose Code Management (PCM)

Other

- Web Based Training (WBT)

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.

Security and Privacy Accessibility Government Customer Support Vendor Customer Support EDM Electronic File Room FAQ User Feedback

Select 'PIEE Administration'

The screenshot shows the PIEE Administration interface. At the top left is the PIEE logo (7.0.6 Procurement Integrated Enterprise Environment). The navigation menu includes 'My Account', 'Administration', and 'Help'. The 'Administration' menu is expanded, and 'PIEE Administration' is highlighted with a red circle. The user is identified as William McEllen, with a last successful login date of 2024/11/20 22:19:48 UTC. The main content area is titled 'Welcome to the Procurement Integrated Enterprise Environment' and features four categories of services: Award (Solicitation), Payment (WAWF, myInvoice), Operational Support (PCM), and Other (WBT). A System Messages section at the bottom contains a critical message about Multi-Factor Authentication (MFA) implementation starting on December 1, 2024, and provides instructions for users to install an authenticator app.

https://piee.eb.mil/xhtml/auth/user/myAccount.xhtml

PIEE 7.0.6 Procurement Integrated Enterprise Environment

My Account Administration Help

PIEE Administration

User : William McEllen Logout

Last Successful Logon Date: 2024/11/20 22:19:48 UTC

Welcome to the Procurement Integrated Enterprise Environment

Award Payment Operational Support Other

Solicitation WAWF myInvoice PCM WBT

Solicitation Wide Area Workflow myInvoice Purpose Code Management Web Based Training

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

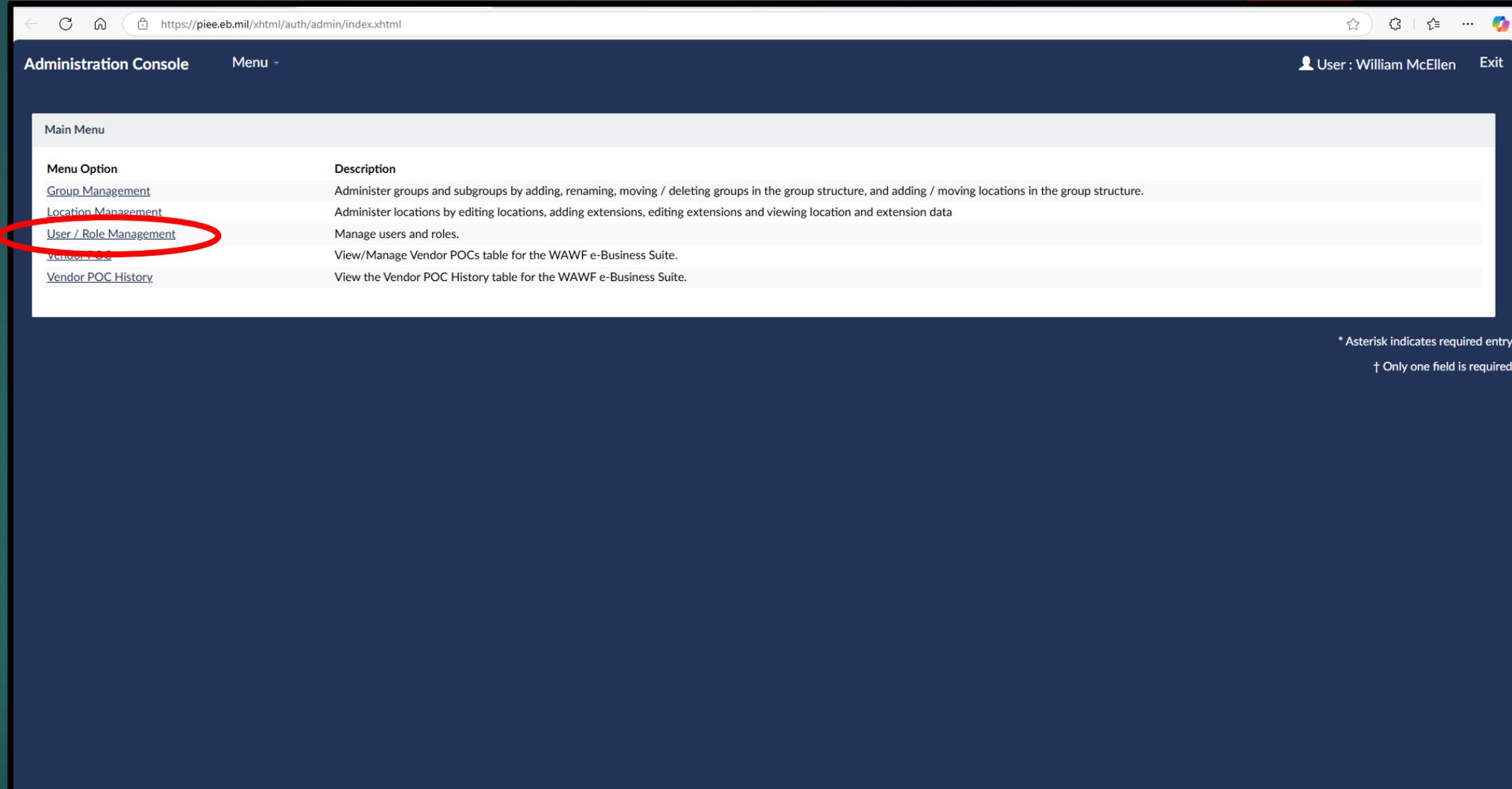
Authentication apps, once downloaded to your mobile device, create secure six-digit codes for account sign-ins. Although these apps are vulnerable if your device is lost or stolen, they provide greater security compared to phone calls or text messages, effectively guarding against phishing, hacking,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

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

https://piee.eb.mil/xhtml/auth/admin/index.xhtml

Security and Privacy Accessibility Government Customer Support Vendor Customer Support EDM Electronic File Room FAQ User Feedback

Select 'User/Role Management'



The screenshot shows a web browser window with the URL <https://piee.eb.mil/xhtml/auth/admin/index.xhtml>. The page title is "Administration Console" and the user is logged in as "User : William McEllen". The main content area displays a "Main Menu" table with the following items:

Menu Option	Description
Group Management	Administer groups and subgroups by adding, renaming, moving / deleting groups in the group structure, and adding / moving locations in the group structure.
Location Management	Administer locations by editing locations, adding extensions, editing extensions and viewing location and extension data
User / Role Management	Manage users and roles.
Vendor POC	View/Manage Vendor POCs table for the WAWF e-Business Suite.
Vendor POC History	View the Vendor POC History table for the WAWF e-Business Suite.

The "User / Role Management" link is circled in red. At the bottom right of the page, there are two footnotes: "* Asterisk indicates required entry." and "† Only one field is required."

Select 'Search'

The screenshot shows the 'Administration Console' interface for 'User / Role Management'. At the top, the browser address bar shows 'https://piee.eb.mil/xhtml/auth/admin/index.xhtml'. The page header includes 'Administration Console', a 'Menu' dropdown, and a user profile for 'User : William McEllen' with an 'Exit' link. The main content area contains search filters for 'User ID', 'First Name', 'Last Name', 'E-Mail', 'DoD ID', and 'X.509 Subject Name'. Each filter has an 'Equal To' dropdown and an input field. Below these are 'Account Type' and 'Warrant Indicator' dropdowns. At the bottom, there are three buttons: 'Search' (circled in red), 'Return', and 'Reset'. A footer note states: '* Asterisk indicates required entry. † Only one field is required.'

Select your 'User ID'

The screenshot shows a web browser window with the URL <https://piee.eb.mil/xhtml/auth/admin/userRoleManagement/userSearchCriteria.xhtml>. The page title is "Administration Console" and the user is logged in as "User : William McEllen".

The search results section is titled "Search Result" and shows "Show 10 entries". A search box is present on the right. The results are displayed in a table with the following columns: User Id, First Name, Last Name, E-Mail, DoD ID, X.509 Subject Name, Application(s), Account Type, and Warrant. The first row of data shows the user ID "willm", first name "William", last name "McEllen", and application "PIEE". The "User Id" column is circled in red.

At the bottom of the table, there are "Back" and "Download" buttons. On the right side, there are "Previous", "1", and "Next" buttons. A footer note states: "* Asterisk indicates required entry. † Only one field is required."

User Id	First Name	Last Name	E-Mail	DoD ID	X.509 Subject Name	Application(s)	Account Type	Warrant
<u>willm</u>	William	McEllen	[REDACTED]			PIEE		N

Select 'User Roles'

The screenshot shows a web browser window with the URL <https://piee.eb.mil/xhtml/auth/admin/userRoleManagement/userSearchResult.xhtml>. The page title is "Administration Console" and the user is identified as "User : William McEllen". The main content area is titled "PIEE Access Approval for William McEllen" with a "Request Type : Initial" indicator. A left-hand navigation menu includes items such as "Overview", "Profile", "EB POC", "Company", "Justification/Attachments", "Reset Password", "User Roles", "Role History", "Profile History", "GAM/CAM Letter", and "Print". The "User Roles" item is circled in red. The main content area shows a "Pending Admin Approval" section with an information message: "No roles were found for Pending Admin Approval." Below this is an "Active Roles" table with one entry for the "PIEE" application, assigned the "Contractor Administrator" role. A "Refresh" button is located at the bottom of the table. A "Back" button is visible at the bottom left of the page.

Administration Console Menu

User : William McEllen Exit

PIEE Access Approval for William McEllen Request Type : Initial

Overview

Pending Admin Approval

No roles were found for Pending Admin Approval.

Active Roles

Application	Role	Group Name	Location Code	Extension	Status	Additional Information
PIEE	Admin Group Contractor Administrator	7FJ64			Auto Activated	  

Refresh

Back

* Asterisk indicates required entry.
† Only one field is required.

Select '+ Add Roles'

Administration Console Menu User : William McEllen Exit

PIEE Access Approval for William McEllen Request Type : Initial

Overview

Profile

EB POC

Company

Justification/Attachments

Reset Password

User Roles

Role History

Profile History

GAM/CAM Letter

Print

User Roles

Change All Status: | Filter Roles By Status : All Active Inactive Archived Pending Approval Rejected Blocked

Show entries Search:

Action	User ID	First Name	Last Name	Role	Application	Group Name	Location Code / Extension	Status	Access Approval Status	Create Date	Account Type	Warrant Indicator	Additional Information
	willm	William	McEllen	Admin Group PIEE Contractor Admin (CAM)	PIEE	7FJ64		Active	Auto Activated	2024/11/20		N	View

Showing 1 to 1 of 1 entries Previous 1 Next

Tip You can view a list of all PIEE roles and their descriptions and functions in the PIEE Role List Matrix.

Back

* Asterisk indicates required entry
† Only one field is required

Verify all User Information and then >Next

The screenshot shows the 'Admin Add Roles' page in the PIEE system. The page header includes the PIEE logo (7.0.6 Procurement Integrated Enterprise Environment) and user information: 'User : William McEllen', 'Status: Active', and 'Logout'. A blue notification bar at the top states: 'Admin Add Roles. Verify all the information within your account, and then add any necessary new roles.' The main content area is titled 'User Profile' and contains a form with the following fields:

- First Name *: William
- Middle Name: Thomas
- Last Name *: McEllen
- Suffix: [Redacted]
- CAGE Code *: 7FJ64
- Organization *: Armiger, LLC.
- Job Title *: Owner
- Email *: [Redacted]
- Confirm Email *: [Redacted]
- Commercial Telephone !: [Redacted]
- Extension: [Empty]
- Intl Country Code and Phone !: [Empty]
- Mobile Telephone: [Redacted]
- DSN Telephone: [Empty]
- Citizenship *: US

At the bottom of the form, there are four buttons: '> Next', '< Previous', 'Help', and 'Account Activation Guide'. The '> Next' button is circled in red. A legend at the bottom right explains the symbols: '! Symbol indicates situational entry, at least one is required.' and '* Asterisk indicates required entry.'

No changes can be made. Click >Next

← ↻ 🏠 <https://piee.eb.mil/xhtml/auth/registration/profile.xhtml?cid=1> 🔊 ☆ ⚙️ 🏠 ...

PIEE
7.0.6 Procurement Integrated Enterprise Environment

User : William McEllen Status: Active Logout
Last Successful Logon Date: 2024/11/20 22:19:48 UTC

Add Roles

- 1. Profile
- 2. EB POC / Company
- 3. Roles
- 4. Justification

Additional Profile Information

EB POC Information

- Info: Group Name for CAGE Code 7FJ64 is '7FJ64'.
- Info: Roles must be approved by one of the following PIEE Contractor Administrator(s) (CAMs): William McEllen.

EB POC Name: WILLIAM MCELLEN
EB POC Email: [REDACTED]
EB POC Phone: [REDACTED]

EB POC ALT Name: WILLIAM MCELLEN
EB POC ALT Email: [REDACTED]
EB POC Phone: [REDACTED]

Company Information

Name: ARMIGER, LLC
Address: [REDACTED]

City: [REDACTED] State: Ohio Zip: [REDACTED] Country: United States of America (the)

> Next < Previous ? Help

Click drop-down under Step 1.

The screenshot shows the PIEE 7.0.6 registration interface. On the left is a sidebar with 'Add Roles' and a list of steps: 1. Profile, 2. EB POC / Company, 3. Roles (highlighted with a mouse cursor), and 4. Justification. The main content area is titled 'Roles' and contains four steps: Step 1 (circled in red) is 'Select the appropriate Application from the list below', with a dropdown menu showing 'WAWF - Wide Area Workflow'. Step 2 is 'Select One or More Roles from the list below (Ctrl+Click)', with a dropdown menu showing 'User Roles for WAWF', 'Energy Lab POC', 'Vendor', 'Vendor Ship To View Only', and 'Vendor View Only'. Step 3 is 'Click 'Add Roles'', with an '+ Add Roles' button. Step 4 is 'Fill out the required information for the applicable applications'. Below the steps are two tip boxes and a navigation bar with buttons for 'Next', 'Previous', 'Help', 'Account Activation Guide', and 'PIEE Role List Matrix'. The top right of the page shows user information: 'User: William McEllen', 'Status: Active', and 'Logout', along with the last successful login date: '2024/11/20 22:19:48 UTC'.

! Symbol indicates situational entry, at least one is required.
* Asterisk indicates required entry.

Select 'SPRS – Supplier Performance Risk System'

The screenshot shows the PIEE 7.0.6 registration interface. The user is William McEllen, Status: Active, with a last successful login on 2024/11/20 22:19:48 UTC. The 'Add Roles' section is active, showing a list of applications. The 'SPRS - Supplier Performance Risk System' option is highlighted with a red circle. The 'User Roles for WAWF' list includes Energy Lab POC, Vendor, Vendor Ship To View Only, and Vendor View Only. The 'Add Roles' button is visible.

PIEE 7.0.6 Procurement Integrated Enterprise Environment

User : William McEllen | Status: Active | Logout

Last Successful Logon Date: 2024/11/20 22:19:48 UTC

Add Roles

1. Profile
2. EB POC / Company
3. Roles
4. Justification

Roles

Step 1. Select the appropriate Application from the list below

- WAWF - Wide Area Workflow
- AMT - Award Management Team
- CSP - Contractor Submission Portal
- DFE - Duty Free Entry
- DSM - Delivery Schedule Manager
- FedMall
- GFP - Government Furnished Property
- IUID Registry
- PDREP - Product Data Reporting and Evaluation Program
- PIEE - Procurement Integrated Enterprise Environment
- SOL - Solicitation
- SPRS - Supplier Performance Risk System**
- WAWF - Wide Area Workflow

Step 2. Select One or More Roles from the list below (Ctrl+Click)

User Roles for WAWF

- Energy Lab POC
- Vendor
- Vendor Ship To View Only
- Vendor View Only

Step 3. Click 'Add Roles'

+ Add Roles

! Symbol indicates situational entry, at least one is required.
* Asterisk indicates required entry.

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

The screenshot displays the PIEE 7.0.6 registration interface. The top navigation bar includes the PIEE logo, the user name 'William McEllen', status 'Active', and a 'Logout' button. The main content area is titled 'Roles' and is divided into four steps:

- Step 1:** Select the appropriate Application from the list below. A dropdown menu shows 'SPRS - Supplier Performance Risk System'.
- Step 2:** Select One or More Roles from the list below (Ctrl+Click). A list of roles is shown, with 'SPRS Cyber Vendor User' selected and circled in red.
- Step 3:** Click 'Add Roles'. A red arrow points to the '+ Add Roles' button.
- Step 4:** Fill out the required information for the applicable applications. This step includes two tips: 'If you need access to any other applications, Repeat Steps 1 to 4 again' and 'You can view a list of all PIEE roles and their descriptions and functions in the PIEE Role List Matrix.'

At the bottom of the page, there are navigation buttons: 'Next', 'Previous', 'Help', 'Account Activation Guide', and 'PIEE Role List Matrix'. A footer note states: '! Symbol indicates situational entry, at least one is required. * Asterisk indicates required entry.'

Enter CAGE Code and then >Next

PIEE 7.0.6 Procurement Integrated Enterprise Environment

User : William McEllen | Status: Active | Logout | Last Successful Logon Date: 2024/11/20 22:19:48 UTC

Add Roles

- 1. Profile
- 2. EB POC / Company
- 3. Roles
- 4. Justification

Roles

Step 1. Select the appropriate Application from the list below

SPRS - Supplier Performance Risk System

Step 2. Select One or More Roles from the list below (Ctrl+Click)

User Roles for SPRS
Contractor/Vendor (Support Role)
SPRS Cyber Vendor User

Step 3. Click 'Add Roles'

+ Add Roles

Step 4. Fill out the required information for the applicable applications

Roles Summary

Application	Role	Location Code / CAGE	Extension	Group	Action
SPRS	SPRS Cyber Vendor User	7FJ64	N/A		Delete

Showing 1 to 1 of 1 entries

Tip If you need access to any other applications, Repeat Steps 1 to 4 again

Tip You can view a list of all PIEE roles and their descriptions and functions in the PIEE Role List Matrix.

> Next | < Previous | ? Help | Account Activation Guide | PIEE Role List Matrix

! Symbol indicates situational entry, at least one is required.
* Asterisk indicates required entry.

https://piee.eb.mil/xhtml/auth/registration/roles.xhtml?cid=1#

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

PIEE 7.0.6 Procurement Integrated Enterprise Environment

User : William McEllen Status: Active Logout
Last Successful Logon Date: 2024/11/20 22:19:48 UTC

Add Roles

- 1. Profile
- 2. EB POC / Company
- 3. Roles
- 4. Justification

Justification / Attachments

Info Provide justification for access and upload any necessary attachments.

Justification *

Update SPRS Score for contract compliance.

Attachments

Browse... Upload

Warning! Procurement Integrated Enterprise Environment is designated for Sensitive Unclassified information ONLY. Do NOT enter classified information in this system.

Next Previous Help

! Symbol indicates situational entry, at least one is required.
* Asterisk indicates required entry.

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

The screenshot shows a web browser window with the URL <https://piee.eb.mil/xhtml/auth/registration/comments.xhtml?cid=1>. The page header features the PIEE logo (Procurement Integrated Enterprise Environment) and version 7.0.6. The main content area displays a 'Success' message with a warning: 'Warning: Your registration was successful but an error has occurred while sending notification emails.' Below this, it states: 'You have successfully added roles, for User William Thomas McEllen, for the following applications:'. A paragraph follows: 'The approval request, for the new roles, will now go to an administrator for approval. Once the roles have been approved by an administrator, the user will receive an email indicating the activated role(s) for the account. If you have any questions or concerns, please contact Customer Support.' At the bottom left of the message box, a blue 'Close' button is circled in red.



Part 3 – NIST and CMMC Scores

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

The screenshot shows a Microsoft Edge browser window with the URL <https://piee.eb.mil/xhtml/unauth/home/login.xhtml?logout=Y>. The browser's address bar and tabs are visible at the top. Below the browser, a banner indicates it is an official website of the United States government. The main content area features the PIEE logo (Procurement Integrated Enterprise Environment) on the left and a green button labeled "VIEW SYSTEM MESSAGES" on the right. The central heading reads "Welcome Back." Below this, a message states: "Log in to your account with a Common Access Card (CAC), Personal Identity Verification (PIV) Card or User ID." There are three main login options: 1. "Log in with Certificate" with a blue button "LOG IN WITH CAC / PIV CARD" and a link "Get help with CAC / PIV Card Login". 2. "Log in with User ID" with input fields for "User ID" and "Password". 3. A CAPTCHA section with a "CARTCHA Image" showing the number "975553", an "AUDIO" button, a "RELOAD" button, and a text input field labeled "Enter in text in image above." A red notification box at the top right of the login area says: "Info: You have successfully logged out of the Procurement Integrated Enterprise Environment. For Security reasons, exit your web browser." At the bottom left, there is a section titled "Need help with your account?" with a link "FIND MY ACCOUNT ADMINISTRATOR".

The SPRS option should now be available. Click it

The screenshot shows the PIEE 7.0.6 Procurement Integrated Enterprise Environment home page. The URL is <https://piee.eb.mil/xhtml/auth/home/home.xhtml>. The user is logged in as William McEllen. The page features a navigation menu with "My Account", "Administration", and "Help". The main content area is titled "Welcome to the Procurement Integrated Enterprise Environment" and displays several application icons: Solicitation, SPRS (circled in red), WAWF, myInvoice, PCM, and WBT. A "System Messages" section is visible at the bottom, containing a message about Multi-Factor Authentication (MFA) implementation starting on December 1, 2024.

PIEE 7.0.6 Procurement Integrated Enterprise Environment

My Account Administration Help

User: William McEllen Logout

Last Successful Logon Date: 2024/11/21 00:45:47 UTC

Welcome to the Procurement Integrated Enterprise Environment

Award [Milestone]

Solicitation SPRS

Wide Area Workflow myInvoice

Operational Support PCM

Other WBT

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.

Security and Privacy Accessibility Government Customer Support Vendor Customer Support EDM Electronic File Room FAQ User Feedback

Select 'Cyber Reports (NIST)'

The screenshot shows the homepage of the Supplier Performance Risk System (SPRS) v4.0.1. The browser address bar displays <https://sprs.csd.disa.mil/sprs-ui/#/home>. The page features a green header with the text "UNCLASSIFIED" and the "Supplier Performance Risk System" logo. A navigation sidebar on the left includes links for Home, Logout, COMPLIANCE REPORTS, Cyber Reports (NIST) (circled in red), CAGE Hierarchy, SERVICE, Feedback/Customer Support, and Download. The main content area contains a welcome message, a "Notes" section, browser recommendations, and a "NIST SP 800-171" section with a list of instructions.

UNCLASSIFIED

Welcome WILLIAM MCELLEN (ARMIGER, LLC)
Last Login: November 20, 2024 19:54:00 ET

Home
Logout
COMPLIANCE REPORTS
Cyber Reports (NIST)
CAGE Hierarchy
SERVICE
Feedback/Customer Support
Download

The Supplier Performance Risk System (SPRS) is the authoritative source to retrieve supplier and product PI [performance information] assessments for the DoD [Department of Defense] acquisition community to use in identifying, assessing, and monitoring unclassified performance. ([DoDI 5000.79](#))

Welcome to SPRS v4.0.1

Notes

Feedback/Customer Support comments are answered in the SPRS module.

Click the SPRS icon at the top of the Menu to open the SPRS webpage for helpful resources.

Recommended browsers for best application performance: Google Chrome, Mozilla Firefox, or Microsoft Edge.

NOTE to Summary Report & Feedback/Customer Support users:
Recommend Mozilla Firefox if you plan to attach files to a Challenge or Comment.

NIST SP 800-171

Click **GUIDANCE** link in the **NIST SP 800-171 Assessment Report** for links to **methodology** and **Quick Entry Guide**.

- You must have the "SPRS Cyber Vendor User" role in PIEE to add or edit results.
- Check your CAGE Hierarchy. If it is not correct please visit the System for Award Management (SAM) to confirm/update.

Contact SPRS Customer Support: sprs-helpdesk@us.navy.mil

SUPPLIER PERFORMANCE RISK SYSTEM (SPRS) Wednesday, November 20, 2024
Version: 4.0.0, Build Date: 10/07/2024

UNCLASSIFIED

Select 'Company Hierarchy' drop-down

The screenshot displays the Supplier Performance Risk System (SPRS) interface. The browser address bar shows the URL <https://sprs.csd.disa.mil/sprs-ui/#/cyberreports>. The page is marked as UNCLASSIFIED. The main header includes the system name "Supplier Performance Risk System" and the user information "Welcome WILLIAM MCELLEN (ARMIGER, LLC.) Last Login: November 20, 2024 19:54:00 ET". The navigation bar shows "CYBER SECURITY REPORTS" and various utility icons. The left sidebar contains navigation links: Home, Logout, COMPLIANCE REPORTS, Cyber Reports (NIST), CAGE Hierarchy, SERVICE, Feedback/Customer Support, and Download. The main content area features a "Company Hierarchy:" label, a drop-down menu with the text "---- Please select CAGE from the list to view its hierarchy ----", and a "Run Cyber Reports" button. A red circle highlights this section. Below the drop-down, a note states: "An asterisk * indicates the user has the SPRS Cyber Vendor User role for this CAGE". The footer includes contact information for SPRS Customer Support (sprs-helpdesk@us.navy.mil) and system details: "SUPPLIER PERFORMANCE RISK SYSTEM (SPRS) Wednesday, November 20, 2024 Version: 4.0.0, Build Date: 10/07/2024".

Select the appropriate CAGE then click 'Run Cyber Reports'

The screenshot displays the Supplier Performance Risk System (SPRS) interface. The page title is "Supplier Performance Risk System" and the sub-header is "CYBER SECURITY REPORTS". The user is logged in as WILLIAM MCELLEN (ARMIGER, LLC) and the last login was on November 20, 2024 at 19:54:00 ET. The page is marked as UNCLASSIFIED.

The main content area features a "Company Hierarchy" dropdown menu with the text "Please select CAGE from the list to view its hierarchy ----". Below the dropdown, a red circle highlights the selected option "7FJ64* (HLO: 7FJ64)". To the right of the dropdown is a "Run Cyber Reports" button, which is also highlighted by a red arrow.

The left sidebar contains the following navigation items: Home, Logout, COMPLIANCE REPORTS, Cyber Reports (NIST), CAGE Hierarchy, SERVICE, Feedback/Customer Support, and Download.

The footer includes the contact information for SPRS Customer Support: sprs-helpdesk@us.navy.mil and the system version information: SUPPLIER PERFORMANCE RISK SYSTEM (SPRS) Wednesday, November 20, 2024 Version: 4.0.0, Build Date: 10/07/2024.

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

The screenshot displays the Supplier Performance Risk System (SPRS) interface. The page title is "Supplier Performance Risk System" and the status is "UNCLASSIFIED". The user is logged in as WILLIAM MCELLEN (ARMIGER, LLC) with a last login of May 11, 2025 20:03:16 ET. The main navigation menu includes Home, Logout, COMPLIANCE REPORTS, Cyber Reports (CMMC & NIST), CAGE Hierarchy, SERVICE, Feedback/Customer Support, and Download. The current page is "CYBER SECURITY REPORTS" for "Cyber Reports (CMMC & NIST) > CAGE: 7FJ64* (HLO: 7FJ64)". The company name is "ARMIGER, LLC" with CAGE Code: 7FJ64* (HLO: 7FJ64). The "NIST SP 800-171 Assessments" tab is selected, and a red arrow points to it. Another red arrow points to the "Add New NIST Assessment" button. The table below shows one assessment record.

Edit/ Delete	DoD Unique Identifier (UID)	Included CAGE	Company Name	Assessment Date	Score	Assessment Scope	Plan Of Action Completion Date	System Security Plan (SSP) Assessed	SSP Version Revisio
	SB00101428 Details	7FJ64	ARMIGER, LLC	11/20/2024	102	ENTERPRISE	08/01/2025	ARMIGER SSP	1.1

Report Generated : 05/11/2025 20:04:26 ET

1 - 1 of 1 items

Contact SPRS Customer Support: sprs-helpdesk@us.navy.mil

SUPPLIER PERFORMANCE RISK SYSTEM (SPRS) Sunday, May 11, 2025
Version: 4.0.5, Build Date: 05/05/2025

While under the NIST tab, click 'Add New NIST Assessment'

The screenshot displays the Supplier Performance Risk System (SPRS) interface. The browser address bar shows the URL: <https://sprs.csd.disa.mil/sprs-ui/#/cyberreports/vendor>. The page is labeled "UNCLASSIFIED" and "Supplier Performance Risk System". The user is logged in as WILLIAM MCELLEN (ARMIGER, LLC) with a last login of May 11, 2025 20:03:16 ET. The main navigation menu includes Home, Logout, COMPLIANCE REPORTS, Cyber Reports (CMMC & NIST), CAGE Hierarchy, SERVICE, Feedback/Customer Support, and Download. The current view is "CYBER SECURITY REPORTS" for "ARMIGER, LLC" with CAGE Code: 7FJ64* (HLO: 7FJ64). The "NIST SP 800-171 Assessments" tab is selected. The "Add New Assessment" section contains a button labeled "Add New NIST Assessment" which is circled in red. Below this, there are tabs for "Basic", "Medium", "High Virtual", and "High On-Site". A table displays assessment data with the following columns: Edit/Delete, DoD Unique Identifier (UID), Included CAGE, Company Name, Assessment Date, Score, Assessment Scope, Plan Of Action Completion Date, System Security Plan (SSP) Assessed, and SSP Version. The table contains one row of data for ARMIGER, LLC. The footer includes contact information for SPRS Customer Support and the system version: 4.0.5, Build Date: 05/05/2025.

UNCLASSIFIED

Welcome WILLIAM MCELLEN (ARMIGER, LLC)
Last Login: May 11, 2025 20:03:16 ET

CYBER SECURITY REPORTS

Cyber Reports (CMMC & NIST) > CAGE: 7FJ64* (HLO: 7FJ64)

ARMIGER, LLC
CAGE Code: 7FJ64* (HLO: 7FJ64)

Company Hierarchy Overview **NIST SP 800-171 Assessments** CMMC Assessments Criteria Search Guidance

Add New Assessment: **Add New NIST Assessment**

Basic Medium High Virtual High On-Site

Report Generated : 05/11/2025 20:04:26 ET

Edit/ Delete	DoD Unique Identifier (UID)	Included CAGE	Company Name	Assessment Date	Score	Assessment Scope	Plan Of Action Completion Date	System Security Plan (SSP) Assessed	SSP Version
	SB00101428 Details	7FJ64	ARMIGER, LLC	11/20/2024	102	ENTERPRISE	08/01/2025	ARMIGER SSP	1.1

1 - 1 of 1 items

Contact SPRS Customer Support: sprs-helpdesk@us.navy.mil

SUPPLIER PERFORMANCE RISK SYSTEM (SPRS) Sunday, May 11, 2025
Version: 4.0.5, Build Date: 05/05/2025

UNCLASSIFIED

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

UNCLASSIFIED

Supplier Performance Risk System

Welcome WILLIAM MCELLEN (ARMIGER, LLC)
Last Login: November 20, 2024 19:54:00 ET

CYBER SECURITY REPORTS

ARMIGER, LLC
CAGE Code: 7FJ64* (HLO: 7FJ64)
Confidence Level: BASIC
Assessment Standard: NIST SP 800-171

Home
Logout
COMPLIANCE REPORTS
Cyber Reports (NIST)
CAGE Hierarchy
SERVICE
Feedback/Customer Support
Download

Back

Enter Assessment Details

Assessment Date:

Assessment Score:

Assessing Scope:

Plan of Action Completion Date:

System Security Plan (SSP) Assessed:

SSP Version/Revision:

SSP Date:

Included CAGE(s):

Save

Contact SPRS Customer Support: sprs-helpdesk@us.navy.mil

SUPPLIER PERFORMANCE RISK SYSTEM (SPRS) Wednesday, November 20, 2024
Version: 4.0.0, Build Date: 10/07/2024

UNCLASSIFIED

If you are unsure of the Assessing Scope...

COMPLIANCE REPORTS

Cyber Reports (NIST)

CAGE Hierarchy

SERVICE

Feedback/Customer Support

Download

Back

Enter Assessment Details

Assessment Date: 11/20/2024

Assessment Score: 102

Assessing Scope: ENTERPRISE

Plan of Action Completion Date: 8/1/2025

Save

Q What are the definitions for the Assessing Scope choices?

A: The definitions associated with the Assessing Scope data choices are:

- Enterprise** – Entire company's network is under the CAGEs listed
- Enclave** – Standalone under Enterprise CAGE as business unit (test enclave, hosted resources, etc.)
- Contract** – Contract specific SSP review

For specific questions about interpreting these definitions please contact your Program Office or Contracts representative or the Defense Contract Management Agency (DCMA) general mailbox, [✉](mailto:DCMA_7012_Assessment_Inquiry@mail.mil) DCMA_7012_Assessment_Inquiry@mail.mil for assistance.

Contact SPRS Customer Support: sprs-helpdesk@us.navy.mil

SUPPLIER PERFORMANCE RISK SYSTEM (SPRS) Wednesday, November 20, 2024
Version: 4.0.0, Build Date: 10/07/2024

UNCLASSIFIED

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

COMPLIANCE REPORTS

Cyber Reports (NIST)

CAGE Hierarchy

SERVICE

Feedback/Customer Support

Download

Back

Enter Assessment Details

Assessment Date: 11/20/2024

Assessment Score: 102

Assessing Scope: ENTERPRISE

Plan of Action Completion Date: 8/1/2025

System Security Plan (SSP) Assessed: ARMIGER SSP

SSP Version/Revision: 1.1

SSP Date: 11/20/2024

Included CAGE(s): **Open CAGE Hierarchy**

Multiple CAGE codes should be delimited by a comma

Save

Contact SPRS Customer Support: sprs-helpdesk@us.navy.mil

SUPPLIER PERFORMANCE RISK SYSTEM (SPRS) Wednesday, November 20, 2024
Version: 4.0.0, Build Date: 10/07/2024

UNCLASSIFIED

Select the appropriate CAGE and hit 'OK'

The screenshot shows a web browser window with the URL <https://sprs.csd.disa.mil/sprs-ui/#/cyberreports>. The main page is titled "Enter Assessment Details" and contains several form fields, including "Assessment Date" (set to 11/20/2024). A modal window titled "CAGE Hierarchy" is open, displaying a search bar and a list of results. The first result, "7FJ64: ARMIGER LLC", is selected with a checkmark. The modal has "Cancel" and "Ok" buttons at the bottom. The background form is dimmed, and a "save" button is visible at the bottom right of the form area.

COMPLIANCE REPORTS

Cyber Reports (NIST)

CAGE Hierarchy

SERVICE

Feedback/Customer Support

Download

Back

Enter Assessment Details

Assessment Date: 11/20/2024

CAGE Hierarchy

7FJ64: ARMIGER LLC

Cancel Ok

save

Contact SPRS Customer Support: sprs-helpdesk@us.navy.mil

SUPPLIER PERFORMANCE RISK SYSTEM (SPRS) Wednesday, November 20, 2024
Version: 4.0.0, Build Date: 10/07/2024

UNCLASSIFIED

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

COMPLIANCE REPORTS

Cyber Reports (NIST)

CAGE Hierarchy

SERVICE

Feedback/Customer Support

Download

Back

Enter Assessment Details

Assessment Date: 11/20/2024

Assessment Score: 102

Assessing Scope: ENTERPRISE

Plan of Action Completion Date: 8/1/2025

System Security Plan (SSP) Assessed: ARMIGER SSP

SSP Version/Revision: 1.1

SSP Date: 11/20/2024

Included CAGE(s):

Open CAGE Hierarchy

7FJ64

Save

Contact SPRS Customer Support: sprs_helpdesk@us.navy.mil

SUPPLIER PERFORMANCE RISK SYSTEM (SPRS) Wednesday, November 20, 2024
Version: 4.0.0, Build Date: 10/07/2024

UNCLASSIFIED

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

The screenshot displays the SPRS web application interface. At the top, the browser address bar shows the URL: <https://sprs.csd.disa.mil/sprs-ui/#/cyberreports>. The main content area is a form for editing an assessment. The form fields are as follows:

- Assessing Scope:** A dropdown menu currently set to "ENTERPRISE".
- Plan of Action Completion Date:** A date field set to "8/1/2025" with a calendar icon.
- System Security Plan (SSP) Assessed:** A text field containing "ARMIGER SSP".
- SSP Version/Revision:** A text field containing "1.1".
- SSP Date:** A date field set to "11/20/2024" with a calendar icon.
- Included CAGE(s):** A section with a button "Open CAGE Hierarchy" and a text area containing "7FJ64".

Below the form are three buttons: "Update", "Delete", and "Clear and Add Additional Assessment(s)".

At the bottom of the screen is a table with the following data:

DoD Unique Identifier (UID)	Included CAGE	Company Name	Assessment Date	Score	Assessment Scope	Plan Of Action Completion Date	System Security Plan (SSP) Assessed	SSP Version/ Revision	SSP Date
SB00101428 Details	7FJ64	ARMIGER, LLC	11/20/2024	102	ENTERPRISE	08/01/2025	ARMIGER SSP	1.1	11/20/2024

Below the table is a pagination control showing "1" of "20" items per page, and "1 - 1 of 1 items" on the right.

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

The screenshot displays the Supplier Performance Risk System (SPRS) interface. The browser address bar shows the URL <https://sprs.csd.disa.mil/sprs-ui/#/cyberreports>. The page is marked as UNCLASSIFIED. The main header includes the system name "Supplier Performance Risk System" and the user information "Welcome WILLIAM MCELLEN (ARMIGER, LLC.)" with a last login time of "November 20, 2024 19:54:00 ET". The navigation menu on the left includes "Home", "Logout", "COMPLIANCE REPORTS", "Cyber Reports (NIST)", "CAGE Hierarchy", "SERVICE", "Feedback/Customer Support", and "Download". The "Cyber Reports (NIST)" menu item is highlighted with a red arrow. The main content area shows the "CYBER SECURITY REPORTS" section with a "Company Hierarchy" dropdown menu set to "7FJ64* (HLO: 7FJ64)". A red oval highlights the dropdown menu and the "View Cyber Reports" button. Below the dropdown, a note states: "An asterisk indicates the user has the SPRS Cyber Vendor User role for this CAGE." The footer contains the contact information "Contact SPRS Customer Support: sprs-helpdesk@us.navy.mil" and the system version information "SUPPLIER PERFORMANCE RISK SYSTEM (SPRS) Wednesday, November 20, 2024 Version: 4.0.0. Build Date: 10/07/2024".

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

The screenshot displays the Supplier Performance Risk System (SPRS) interface. The page title is "Supplier Performance Risk System" and the user is logged in as WILLIAM MCELLEN (ARMIGER, LLC). The main content area shows "CYBER SECURITY REPORTS" for "ARMIGER, LLC" with CAGE Code: 7FJ64* (HLO: 7FJ64). The "NIST SP 800-171 Assessments" tab is active, showing a table of assessments. A red arrow points to the "Edit/Delete" icon for the assessment with DoD Unique Identifier SB00101428.

UNCLASSIFIED

Supplier Performance Risk System

Welcome WILLIAM MCELLEN (ARMIGER, LLC)
Last Login: May 11, 2025 20:03:16 ET

CYBER SECURITY REPORTS

Cyber Reports (CMMC & NIST) > CAGE: 7FJ64* (HLO: 7FJ64)

ARMIGER, LLC
CAGE Code: 7FJ64* (HLO: 7FJ64)

Company Hierarchy Overview **NIST SP 800-171 Assessments** CMMC Assessments Criteria Search Guidance

Add New Assessment: Add New NIST Assessment

Basic Medium High Virtual High On-Site

Report Generated : 05/11/2025 20:04:26 ET

Edit/ Delete	DoD Unique Identifier (UID)	Included CAGE	Company Name	Assessment Date	Score	Assessment Scope	Plan Of Action Completion Date	System Security Plan (SSP) Assessed	SSP Version
	SB00101428 Details	7FJ64	ARMIGER, LLC	11/20/2024	102	ENTERPRISE	08/01/2025	ARMIGER SSP	1.1

1 - 1 of 1 items

Contact SPRS Customer Support: sprs-helpdesk@us.navy.mil

SUPPLIER PERFORMANCE RISK SYSTEM (SPRS) Sunday, May 11, 2025
Version: 4.0.5, Build Date: 05/05/2025

UNCLASSIFIED

Next - Click on the CMMC Assessments tab to switch over

The screenshot displays the Supplier Performance Risk System (SPRS) interface. The browser address bar shows the URL: <https://sprs.csd.disa.mil/sprs-ui/#/cyberreports/vendor>. The page title is "Supplier Performance Risk System" and the user is identified as WILLIAM MCELLEN (ARMIGER, LLC) with a last login of May 11, 2025 20:03:16 ET. The main navigation bar includes "CYBER SECURITY REPORTS" and a breadcrumb trail: "Cyber Reports (CMMC & NIST) > CAGE: 7FJ64* (HLO: 7FJ64)". A red arrow points to the "CMMC Assessments" tab in the navigation bar. The page content shows the company name "ARMIGER, LLC" and CAGE Code "7FJ64* (HLO: 7FJ64)". Below this, there are tabs for "Company Hierarchy", "Overview", "NIST SP 800-171 Assessments", "CMMC Assessments", "Criteria Search", and "Guidance". An "Add New Assessment" button is visible. The main content area features a table with columns: "Edit/Delete", "DoD Unique Identifier (UID)", "Included CAGE", "Company Name", "Assessment Date", "Score", "Assessment Scope", "Plan Of Action Completion Date", "System Security Plan (SSP) Assessed", and "SSP Version Revision". The table contains one row of data for ARMIGER, LLC. The page footer includes contact information for SPRS Customer Support and the system version: "SUPPLIER PERFORMANCE RISK SYSTEM (SPRS) Sunday, May 11, 2025 Version: 4.0.5, Build Date: 05/05/2025".

UNCLASSIFIED

Supplier Performance Risk System

Welcome WILLIAM MCELLEN (ARMIGER, LLC)
Last Login: May 11, 2025 20:03:16 ET

CYBER SECURITY REPORTS

Cyber Reports (CMMC & NIST) > CAGE: 7FJ64* (HLO: 7FJ64)

ARMIGER, LLC
CAGE Code: 7FJ64* (HLO: 7FJ64)

Company Hierarchy Overview **NIST SP 800-171 Assessments** CMMC Assessments Criteria Search Guidance

Add New Assessment:

Basic Medium High Virtual High On-Site

Report Generated : 05/11/2025 20:04:26 ET

Edit/Delete	DoD Unique Identifier (UID)	Included CAGE	Company Name	Assessment Date	Score	Assessment Scope	Plan Of Action Completion Date	System Security Plan (SSP) Assessed	SSP Version Revision
	SB00101428 Details	7FJ64	ARMIGER, LLC	11/20/2024	102	ENTERPRISE	08/01/2025	ARMIGER SSP	1.1

1 20 items per page 1 - 1 of 1 items

Contact SPRS Customer Support: sprs-helpdesk@us.navy.mil

SUPPLIER PERFORMANCE RISK SYSTEM (SPRS) Sunday, May 11, 2025
Version: 4.0.5, Build Date: 05/05/2025

UNCLASSIFIED

Note that CMMC Assessments do not remove the NIST Score requirement

The screenshot shows the Supplier Performance Risk System (SPRS) interface. The page title is "Supplier Performance Risk System" and the user is logged in as WILLIAM MCELLEN (ARMIGER, LLC). The page is categorized under "CYBER SECURITY REPORTS" and "Cyber Reports (CMMC & NIST)". The user is viewing the "CMMC Assessments" tab for the company "ARMIGER, LLC" with CAGE Code 7FJ64* (HLO: 7FJ64).

A notification box is displayed in the center of the screen, stating:

NOTE: Entering CMMC Self-Assessments do not fulfill the NIST SP 800-171 requirements in DFARS 252.204-7019/7020

Please proceed to the NIST SP 800-171 tab to post those results

Acknowledge

The background interface shows a table with columns for "CMMC Unique Identifier (UID)", "CMMC Status", "Assessment Scope", "Included CAGE(s)", "Company Size", and "Delete". The table is currently empty, showing "0 - 0 of 0 items".

At the bottom of the page, there is a footer with the text: "Contact SPRS Customer Support: sprs-helpdesk@us.navy.mil" and "SUPPLIER PERFORMANCE RISK SYSTEM (SPRS) Sunday, May 11, 2025 Version: 4.0.5, Build Date: 05/05/2025".

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

The screenshot displays the Supplier Performance Risk System (SPRS) interface. The main header includes the system name and a navigation menu. The current view is for 'CYBER SECURITY REPORTS' for 'ARMIGER, LLC' with CAGE Code: 7FJ64* (HLO: 7FJ64). The 'CMMC Assessments' tab is active, showing options for 'CMMC Level 1 (Self)', 'CMMC Level 2 (Self)', 'CMMC Level 2 (C3PAO)', and 'CMMC Level 3 (DIBCAC)'. A red circle highlights these assessment level options. Below the options is a table with columns for 'Edit', 'CMMC Unique Identifier (UID)', 'CMMC Status Type', 'Assessment Date', 'CMMC Status Expiration Date', 'Assessment Scope', 'Included CAGE(s)', 'Company Size', and 'Delete'. The table currently shows 'No records found' and a pagination control for 20 items per page.

UNCLASSIFIED

Supplier Performance Risk System

Welcome WILLIAM MCELLEN (ARMIGER, LLC.)
Last Login: May 11, 2025 20:03:16 ET

CYBER SECURITY REPORTS

Cyber Reports (CMMC & NIST) > CAGE: 7FJ64* (HLO: 7FJ64)

ARMIGER, LLC
CAGE Code: 7FJ64* (HLO: 7FJ64)

Company Hierarchy Overview NIST SP 800-171 Assessments **CMMC Assessments** Criteria Search Guidance

Add New Assessment: Add New CMMC Level 1 Self-Assessment

CMMC Level 1 (Self) CMMC Level 2 (Self) CMMC Level 2 (C3PAO) CMMC Level 3 (DIBCAC)

Report Generated: 05/11/2025 20:06:47 ET

Edit	CMMC Unique Identifier (UID)	CMMC Status Type	Assessment Date	CMMC Status Expiration Date	Assessment Scope	Included CAGE(s)	Company Size	Delete
No records found								

20 items per page 0 - 0 of 0 items

Contact SPRS Customer Support: sprs_helpdesk@us.navy.mil

SUPPLIER PERFORMANCE RISK SYSTEM (SPRS) Sunday, May 11, 2025
Version: 4.0.5, Build Date: 05/05/2025

UNCLASSIFIED

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

The screenshot displays the Supplier Performance Risk System (SPRS) interface. The page title is "Supplier Performance Risk System" and the status is "UNCLASSIFIED". The user is logged in as WILLIAM MCELLEN (ARMIGER, LLC) with a last login of May 11, 2025 20:03:16 ET. The main navigation menu includes Home, Logout, COMPLIANCE REPORTS, Cyber Reports (CMMC & NIST), CAGE Hierarchy, SERVICE, Feedback/Customer Support, and Download. The current page is "CYBER SECURITY REPORTS" for "ARMIGER, LLC" with CAGE Code: 7FJ64* (HLO: 7FJ64). The "CMMC Assessments" tab is selected, and the "Add New Assessment" button is highlighted with a red arrow. Below the button, there are tabs for "CMMC Level 1 (Self)", "CMMC Level 2 (Self)", "CMMC Level 2 (C3PAO)", and "CMMC Level 3 (DIBCAC)". The "CMMC Level 1 (Self)" tab is active. A table with columns for Edit, CMMC Unique Identifier (UID), CMMC Status Type, Assessment Date, CMMC Status Expiration Date, Assessment Scope, Included CAGE(s), Company Size, and Delete is shown. The table contains no records, and the footer indicates "0 - 0 of 0 items".

Supplier Performance Risk System
UNCLASSIFIED
Welcome WILLIAM MCELLEN (ARMIGER, LLC)
Last Login: May 11, 2025 20:03:16 ET

CYBER SECURITY REPORTS

Cyber Reports (CMMC & NIST) > CAGE: 7FJ64* (HLO: 7FJ64)

ARMIGER, LLC
CAGE Code: 7FJ64* (HLO: 7FJ64)

Company Hierarchy Overview NIST SP 800-171 Assessments **CMMC Assessments** Criteria Search Guidance

Add New Assessment: Add New CMMC Level 1 Self-Assessment

CMMC Level 1 (Self) CMMC Level 2 (Self) CMMC Level 2 (C3PAO) CMMC Level 3 (DIBCAC)

Report Generated : 05/11/2025 20:06:47 ET

Edit	CMMC Unique Identifier (UID)	CMMC Status Type	Assessment Date	CMMC Status Expiration Date	Assessment Scope	Included CAGE(s)	Company Size	Delete
No records found								

20 items per page 0 - 0 of 0 items

Contact SPRS Customer Support: sprs_helpdesk@us.navy.mil

SUPPLIER PERFORMANCE RISK SYSTEM (SPRS) Sunday, May 11, 2025
Version: 4.0.5, Build Date: 05/05/2025

UNCLASSIFIED

Review the warning and acknowledge

The screenshot displays the Supplier Performance Risk System (SPRS) interface. The browser address bar shows the URL <https://sprs.csd.disa.mil/sprs-ui/#/cyberreports/vendor>. The page title is "Supplier Performance Risk System" and the status is "UNCLASSIFIED". The user is logged in as WILLIAM MCELLEN (ARMIGER, LLC) with a last login of May 11, 2025 20:03:16 ET.

The main content area is titled "CYBER SECURITY REPORTS" and shows the vendor "ARMIGER, LLC" with CAGE Code: 7FJ64* (HLO: 7FJ64). The navigation tabs include "Company Hierarchy", "Overview", "NIST SP 800-171 Assessments", "CMMC Assessments", "Criteria Search", and "Guidance". The "CMMC Assessments" tab is active, showing an "Add New Assessment" button for "Add New CMMC Level 1 Self-Assessment".

A warning message is displayed in a white box with black text: "WARNING: Misrepresentation of a CMMC compliance status to the Government may result in criminal prosecution, including actions under section 1001, Title 18 of the United States Code, civil liability under the False Claims Act." Below the warning is an "Acknowledge" button.

The interface also shows a table with columns for "Edit", "CMMC Unique Identifier (UID)", "CMMC Status", "Assessment Scope", "Included CAGE(s)", "Company Size", and "Delete". The table is currently empty, showing "0 - 0 of 0 items".

At the bottom of the page, there is contact information for SPRS Customer Support: sprs-helpdesk@us.navy.mil and the version information: "SUPPLIER PERFORMANCE RISK SYSTEM (SPRS) Sunday, May 11, 2025 Version: 4.0.5, Build Date: 05/05/2025". The status "UNCLASSIFIED" is also present at the bottom.

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

UNCLASSIFIED

Supplier Performance Risk System

Welcome WILLIAM MCELLEN (ARMIGER, LLC.)
Last Login: May 11, 2025 20:03:16 ET

CYBER SECURITY REPORTS

Cyber Reports (CMMC & NIST) > CAGE: 7FJ64* (HLO: 7FJ64)

ARMIGER, LLC
CAGE Code: 7FJ64* (HLO: 7FJ64)
CMMC Status Type: Level 1 Self-Assessment
Assessment Standard: NIST SP 800-171 Rev 2

Enter CMMC Assessment Details

Assessment Date: MM/DD/YYYY

Assessing Scope:

How many employees are in the organization for which this CMMC Level 1 self-assessment applies?

Are you compliant with each of the security requirements specified in [FAR clause 52.204-21](#)? Yes No

Included CAGE(s):

Multiple CAGE codes should be delimited by a comma

Assessments are not complete until they have been affirmed by the company Affirming Official (AO)

The **Affirming Official (AO)** is the senior level representative from within each Organization Seeking Assessment (OSA) who is responsible for ensuring the OSA's compliance with the CMMC Program requirements and has the authority to affirm the OSA's continuing compliance with the security requirements for their respective organizations. (CMMC-custom term)(§170.4)

Once all items are complete, click on 'Open CAGE Hierarchy'

The screenshot displays the 'Supplier Performance Risk System' interface. The top navigation bar includes 'UNCLASSIFIED' and 'CYBER SECURITY REPORTS'. The user is logged in as WILLIAM MCELLEN (ARMIGER, LLC.). The main content area shows the 'Enter CMMC Assessment Details' form for ARMIGER, LLC. The form includes fields for 'Assessment Date' (3/10/2025), 'Assessing Scope' (ENTERPRISE), 'How many employees' (1), and 'Are you compliant with each of the security requirements specified in FAR clause 52.204-21?' (Yes). A red arrow points to the 'Open CAGE Hierarchy' button in the 'Included CAGE(s):' section. Below the form, there is a note about the Affirming Official (AO) and buttons for 'Save' and 'Continue to Affirmation'.

Supplier Performance Risk System

UNCLASSIFIED

Welcome WILLIAM MCELLEN (ARMIGER, LLC.)
Last Login: May 11, 2025 20:03:16 ET

CYBER SECURITY REPORTS

Cyber Reports (CMMC & NIST) > CAGE: 7FJ64* (HLO: 7FJ64)

ARMIGER, LLC
CAGE Code: 7FJ64* (HLO: 7FJ64)
CMMC Status Type: Level 1 Self-Assessment
Assessment Standard: NIST SP 800-171 Rev 2

Back

Enter CMMC Assessment Details

Assessment Date: 3/10/2025
Assessing Scope: ENTERPRISE

How many employees are in the organization for which this CMMC Level 1 self-assessment applies? 1

Are you compliant with each of the security requirements specified in FAR clause 52.204-21? Yes No

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

Assessments are not complete until they have been affirmed by the company Affirming Official (AO)

The Affirming Official (AO) is the senior level representative from within each Organization Seeking Assessment (OSA) who is responsible for ensuring the OSA's compliance with the CMMC Program requirements and has the authority to affirm the OSA's continuing compliance with the security requirements for their respective organizations. (CMMC-custom term)(§170.4)

Save Continue to Affirmation

Select the appropriate CAGE

The screenshot displays the Supplier Performance Risk System (SPRS) interface. The browser address bar shows the URL: <https://sprs.csd.disa.mil/sprs-ui/#/cyberreports/vendor>. The page title is "Supplier Performance Risk System" and the user is logged in as WILLIAM MCELLEN (ARMIGER, LLC). The current page is "CYBER SECURITY REPORTS" for "Cyber Reports (CMMC & NIST) > CAGE: 7FJ64* (HLO: 7FJ64)".

A modal window titled "CAGE Hierarchy" is open, featuring a search bar and a list of results. The first result, "7FJ64: ARMIGER, LLC", is selected with a checkmark. The modal includes "Cancel" and "Ok" buttons at the bottom.

The background interface includes a sidebar with navigation options: Home, Logout, COMPLIANCE REPORTS, Cyber Reports (CMMC & NIST), CAGE Hierarchy, SERVICE, Feedback/Customer Support, and Download. The main content area shows a "Back" button and a "CAGE Hierarchy" section with a search bar and a list of results. Below this, there are fields for "Assessment" (3/10/2025), "How many assessments apply?" (1), and "Assessment applies?" (Yes/No). A "Save" button and a "Continue to Affirmation" button are visible at the bottom of the page.

The Affirming Official (AO) is the senior level representative from within each Organization Seeking Assessment (OSA) who is responsible for ensuring the OSA's compliance with the CMMC Program requirements and has the authority to affirm the OSA's continuing compliance with the security requirements for their respective organizations. (CMMC-custom term)(§170.4)

If everything is correct, 'Continue to Affirmation'

The screenshot displays the 'Supplier Performance Risk System' interface. The header includes the system name, 'UNCLASSIFIED' status, and user information: 'Welcome WILLIAM MCELLEN (ARMIGER, LLC.) Last Login: May 11, 2025 20:03:16 ET'. The main navigation bar shows 'CYBER SECURITY REPORTS'. The breadcrumb trail is 'Cyber Reports (CMMC & NIST) > CAGE: 7FJ64* (HLO: 7FJ64)'. The left sidebar contains links for Home, Logout, COMPLIANCE REPORTS, Cyber Reports (CMMC & NIST), CAGE Hierarchy, SERVICE, Feedback/Customer Support, and Download. The main content area displays the following information:

ARMIGER, LLC
CAGE Code: 7FJ64* (HLO: 7FJ64)
CMMC Status Type: Level 1 Self-Assessment
Assessment Standard: NIST SP 800-171 Rev 2

Enter CMMC Assessment Details

Assessment Date: 3/10/2025
Assessing Scope: ENTERPRISE

How many employees are in the organization for which this CMMC Level 1 self-assessment applies? 1

Are you compliant with each of the security requirements specified in [FAR clause 52.204-21?](#) Yes No

Included CAGE(s):
Open CAGE Hierarchy
7FJ64

Assessments are not complete until they have been affirmed by the company Affirming Official (AO)

The **Affirming Official (AO)** is the senior level representative from within each Organization Seeking Assessment (OSA) who is responsible for ensuring the OSA's compliance with the CMMC Program requirements and has the authority to affirm the OSA's continuing compliance with the security requirements for their respective organizations. (CMMC-custom term)(§170.4)

Buttons: Save, Continue to Affirmation (highlighted with a red arrow)

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

The screenshot displays the Supplier Performance Risk System (SPRS) interface. The browser address bar shows the URL: <https://sprs.csd.disa.mil/sprs-ui/#/cyberreports/vendor>. The page header includes "UNCLASSIFIED" and "Supplier Performance Risk System". The user is logged in as WILLIAM MCELLEN (ARMIGER, LLC) with a last login of May 11, 2025 20:03:16 ET. The main navigation bar shows "CYBER SECURITY REPORTS". The breadcrumb trail indicates the current location: "Cyber Reports (CMMC & NIST) > CAGE: 7FJ64* (HLO: 7FJ64)".

The main content area displays the following information for the selected vendor:

- ARMIGER, LLC
- CAGE Code: 7FJ64* (HLO: 7FJ64)
- CMMC Status Type: Level 1 Self-Assessment
- Assessment Standard: NIST SP 800-171 Rev 2

A modal dialog titled "Affirming Official" is open, containing the following text:

If you are the Affirming Official (AO) select "Continue to Affirmation" below. Otherwise, enter the email of the AO to transfer (email) this record to the AO for affirmation.

If you are not the AO, enter the e-mail of the AO in the box below and select "Transfer to AO". An email will be sent. The CMMC Status Type will be "Pending Affirmation" until the assessment is affirmed.

Email of Affirming Official (AO):

Below the modal, there is a "Back" button and a "Save" button. At the bottom of the page, there is a "Continue to Affirmation" button.

Assessments are not complete until they have been affirmed by the company Affirming Official (AO)

The **Affirming Official (AO)** is the senior level representative from within each Organization Seeking Assessment (OSA) who is responsible for ensuring the OSA's compliance with the CMMC Program requirements and has the authority to affirm the OSA's continuing compliance with the security requirements for their respective organizations. (CMMC-custom term)(§170.4)

Verify your details as the Affirmer and 'Continue to Affirmation'

The screenshot shows the Supplier Performance Risk System (SPRS) interface. The browser address bar displays <https://sprs.csd.disa.mil/sprs-ui/#/cyberreports/vendor>. The page header includes the text "UNCLASSIFIED" and "Supplier Performance Risk System". The user is logged in as WILLIAM MCELLEN (ARMIGER, LLC.) with a last login time of May 11, 2025 20:03:16 ET. The main navigation menu on the left includes Home, Logout, COMPLIANCE REPORTS, Cyber Reports (CMMC & NIST), CAGE Hierarchy, SERVICE, Feedback/Customer Support, and Download. The current page is titled "CYBER SECURITY REPORTS" and shows the path "Cyber Reports (CMMC & NIST) > CAGE: 7FJ64* (HLO: 7FJ64)". The main content area displays the following information:

ARMIGER, LLC
CAGE Code: 7FJ64* (HLO: 7FJ64)
CMMC Status Type: Level 1 Self-Assessment
Assessment Standard: NIST SP 800-171 Rev 2

Enter CMMC Assessment Details

The **Affirming Official (AO)** is the senior level representative from within each Organization Seeking Assessment (OSA) who is responsible for ensuring the OSA's compliance with the CMMC Program requirements and has the authority to affirm the OSA's continuing compliance with the security requirements for their respective organizations. (CMMC-custom term)(§170.4)

Affirming Official:

First Name: WILLIAM
Last Name: MCELLEN
Title: OWNER
Email Address: WILL.MCELLEN@ARMIGERLLC.COM

Additional Email Address(s):
Multiple emails should be delimited by a comma

At the bottom of the form, there are two buttons: "< Previous" and "Continue to Affirmation". A red arrow points to the "Continue to Affirmation" button. The footer of the page includes the text "UNCLASSIFIED" and "SUPPLIER PERFORMANCE RISK SYSTEM (SPRS) Sunday, May 11, 2025 Version: 4.0.5, Build Date: 05/05/2025".

Read the certification statement, check the box, and click 'Affirm'

UNCLASSIFIED

Supplier Performance Risk System

Welcome WILLIAM MCELLEN (ARMIGER, LLC)
Last Login: May 11, 2025 20:03:16 ET

CYBER SECURITY REPORTS

Cyber Reports (CMMC & NIST) > CAGE: 7FJ64 (HLD: 7FJ64)

Home
Logout
COMPLIANCE REPORTS
Cyber Reports (CMMC & NIST)
CAGE Hierarchy
SERVICE
Feedback/Customer Support
Download

Assessment and Affirmation

Report Generated: 05/11/2025 20:09:00 ET

Back

CMMC Status Type: **Unaffirmed Final Level 1 Self-Assessment**
CMMC Unique Identifier (UID): **S100008123**
Level 1 CMMC Assessment Date: **03/10/2025**
CMMC Status Expiration Date: **03/10/2026**
Assessing Scope: **ENTERPRISE**
Company Size: **1**

Affirming Official (AO) Responsible for Cyber/CMMC:
Name: **WILLIAM MCELLEN**
Title: **OWNER**
Email: **WILL.MCELLEN@ARMIGERLLC.COM**
Additional Email:

Included CAGES/entities:

CAGE	Company Name	Address
7FJ64	ARMIGER, LLC	52107 SYKES RIDGE RD, CLARINGTON, OH, USA

Submission of this assessment result **S100008123** or affirmation indicates that **WILLIAM MCELLEN**, as the **Affirming Official responsible for Cybersecurity Maturity Model Certification (CMMC) for ARMIGER, LLC.**, has reviewed and approved the submission and attests that the information system(s) within [or covered by] the scope of this CMMC assessment IS/ARE compliant with CMMC requirements as defined in 32 CFR § 170. Misrepresentation of this CMMC compliance status to the Government may result in criminal prosecution, including actions under section 1001, Title 18 of the United States Code, civil liability under the False Claims Act, and contract remedies as determined appropriate by the contracting officer.

I certify that I have read the above statement.

Affirm **Cancel**

Contact SPRS Customer Support: sprs-helpdesk@us.navy.mil

SUPPLIER PERFORMANCE RISK SYSTEM (SPRS) Sunday, May 11, 2025
Version: 4.0.5, Build Date: 05/05/2025

UNCLASSIFIED

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

The screenshot displays the Supplier Performance Risk System (SPRS) interface. The browser address bar shows the URL: <https://sprs.csd.disa.mil/sprs-ui/#/cyberreports/vendor>. The page is labeled "UNCLASSIFIED" in the top right corner. The main header features the "Supplier Performance Risk System" logo and the text "CYBER SECURITY REPORTS". A navigation sidebar on the left includes links for Home, Logout, COMPLIANCE REPORTS, Cyber Reports (CMMC & NIST), CAGE Hierarchy, SERVICE, Feedback/Customer Support, and Download. The main content area shows the path "Cyber Reports (CMMC & NIST) > CAGE: 7FJ64* (HLO: 7FJ64)". The company name "ARMIGER, LLC" and "CAGE Code: 7FJ64* (HLO: 7FJ64)" are displayed. Below this, there are tabs for "Company Hierarchy", "Overview", "NIST SP 800-171 Assessments", "CMMC Assessments", "Criteria Search", and "Guidance". An "Add New Assessment" button is present, with a sub-button for "Add New CMMC Level 1 Self-Assessment". Further down, there are tabs for "CMMC Level 1 (Self)", "CMMC Level 2 (Self)", "CMMC Level 2 (C3PAO)", and "CMMC Level 3 (DIBCAC)". A "Report Generated" timestamp of "05/11/2025 20:12:27 ET" is shown above a table. The table has columns for Edit, CMMC Unique Identifier (UID), CMMC Status Type, Assessment Date, CMMC Status Expiration Date, Assessment Scope, Included CAGE(s), Company Size, and Delete. A single row of data is visible, with a "Details" button under the UID. The footer includes contact information for SPRS Customer Support and the system version: "SUPPLIER PERFORMANCE RISK SYSTEM (SPRS) Sunday, May 11, 2025 Version: 4.0.5, Build Date: 05/05/2025".

UNCLASSIFIED

Welcome WILLIAM MCELLEN (ARMIGER, LLC)
Last Login: May 11, 2025 20:03:16 ET

CYBER SECURITY REPORTS

Cyber Reports (CMMC & NIST) > CAGE: 7FJ64* (HLO: 7FJ64)

ARMIGER, LLC
CAGE Code: 7FJ64* (HLO: 7FJ64)

Company Hierarchy Overview NIST SP 800-171 Assessments CMMC Assessments Criteria Search Guidance

Add New Assessment: Add New CMMC Level 1 Self-Assessment

CMMC Level 1 (Self) CMMC Level 2 (Self) CMMC Level 2 (C3PAO) CMMC Level 3 (DIBCAC)

Report Generated : 05/11/2025 20:12:27 ET

Edit	CMMC Unique Identifier (UID)	CMMC Status Type	Assessment Date	CMMC Status Expiration Date	Assessment Scope	Included CAGE(s)	Company Size	Delete
	S100008123 Details	Final Level 1 Self-Assessment	03/10/2025	03/10/2026	ENTERPRISE	7FJ64	1	

1 - 1 of 1 items

Contact SPRS Customer Support: sprs-helpdesk@us.navy.mil

SUPPLIER PERFORMANCE RISK SYSTEM (SPRS) Sunday, May 11, 2025
Version: 4.0.5, Build Date: 05/05/2025

UNCLASSIFIED

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

UNCLASSIFIED

Supplier Performance Risk System

Welcome WILLIAM MCELLEN (ARMIGER, LLC)
Last Login: May 11, 2025 20:03:16 ET

CYBER SECURITY REPORTS

Cyber Reports (CMMC & NIST) > CAGE: 7FJ64* (HLO: 7FJ64)

ARMIGER, LLC
CAGE Code: 7FJ64* (HLO: 7FJ64)

Company Hierarchy Overview NIST SP 800-171 Assessments **CMMC Assessments** Criteria Search Guidance

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

CMMC Level 1 (Self) **CMMC Level 2 (Self)** CMMC Level 2 (C3PAO) CMMC Level 3 (DIBCAC)

Report Generated : 05/11/2025 20:12:27 ET

Edit	CMMC Unique Identifier (UID)	CMMC Status Type	Assessment Date	Affirmation Expiration Date	CMMC Status Expiration Date	Assessment Scope	Last Entered or Affirmed CAGE(s) in Scope	Current CAGE(s) Status	Company Size	Cancel/Delete
No records found										

20 items per page 0 - 0 of 0 items

Contact SPRS Customer Support: sprs-helpdesk@us.navy.mil

SUPPLIER PERFORMANCE RISK SYSTEM (SPRS) Sunday, May 11, 2025
Version: 4.0.5, Build Date: 05/05/2025

UNCLASSIFIED

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

Enter CMMC Assessment Details

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

Requirement Family: Access Control (AC)

Save Save and Continue >

Requirement Number	Requirement Description	Compliance Status ^③		
		Met	Not Met	N/A
<i>Note: All Objectives must be met for the Requirement to be Met.</i>				
AC.L2-3.1.1 Requirement Objectives	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<input type="checkbox"/> Met	<input type="checkbox"/> Not Met	<input type="checkbox"/> N/A
AC.L2-3.1.2 Requirement Objectives	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	<input type="checkbox"/> Met	<input type="checkbox"/> Not Met	<input type="checkbox"/> N/A
AC.L2-3.1.3 Requirement Objectives	Control the flow of CUI in accordance with approved authorizations.	<input type="checkbox"/> Met	<input type="checkbox"/> Not Met	<input type="checkbox"/> N/A
AC.L2-3.1.4 Requirement Objectives	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	<input type="checkbox"/> Met	<input type="checkbox"/> Not Met	<input type="checkbox"/> N/A
AC.L2-3.1.5 Requirement Objectives	Employ the principle of least privilege, including for specific security functions and privileged accounts.	<input type="checkbox"/> Met	<input type="checkbox"/> Not Met	<input type="checkbox"/> N/A
AC.L2-3.1.6 Requirement Objectives	Use non-privileged accounts or roles when accessing nonsecurity functions.	<input type="checkbox"/> Met	<input type="checkbox"/> Not Met	<input type="checkbox"/> N/A
AC.L2-3.1.7 Requirement Objectives	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	<input type="checkbox"/> Met	<input type="checkbox"/> Not Met	<input type="checkbox"/> N/A
AC.L2-3.1.8 Requirement Objectives	Limit unsuccessful logon attempts.	<input type="checkbox"/> Met	<input type="checkbox"/> Not Met	<input type="checkbox"/> N/A
AC.L2-3.1.9 Requirement Objectives	Provide privacy and security notices consistent with applicable CUI rules.	<input type="checkbox"/> Met	<input type="checkbox"/> Not Met	<input type="checkbox"/> N/A

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>

