



SERDP & ESTCP Management System (SEMS)

**Account Setup and Multi-Factor Authentication
(MFA) Setup Guide
(UPDATED Spring 2025)**

Contents

- Overview3
- Homepage4
- Existing User6
- New User7
 - Create Account8
 - Create DOD CAC Account10
- Set Up MFA Verification Method13
 - Login to SEMS Account14
 - Select Verification Method18
 - Okta Verify20
 - Other Authentication23
- After Setting Up MFA Verification Method26
- Managing MFA Verification Method27
- Adding PIV/CAC to an Account31

Overview

Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA) has now been enabled for The SERDP & ESTCP Management System (SEMS). MFA is an authentication method that requires more than one verification method for users when signing into the system.

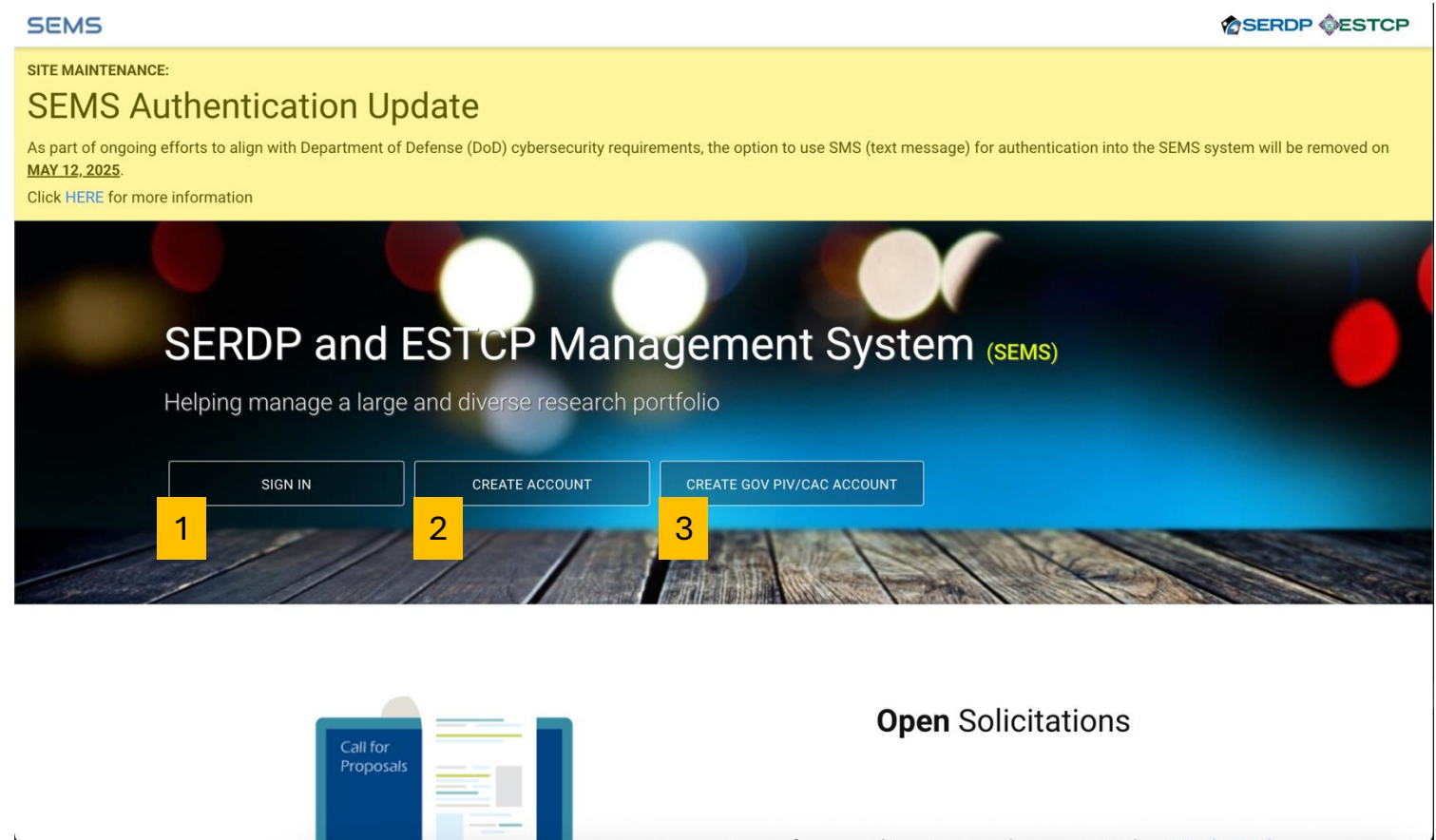
Standard accounts (not linked to CAC card):

When you log into your SEMS account, you will be required to enter your email address and password, as well as a verification code. To receive the code, a one-time setup of the MFA verification method is required. This guide explains how to create an account and setup the MFA verification method.

Homepage

Homepage

1. Sign in
 - If you already have an account
2. Create Account
 - If you are a new user
3. Create Gov CAC Account
 - If you are a new user and wish to link your CAC to your SEMS account



Existing User

The SERDP & ESTCP Management System (SEMS) has upgraded its login process to meet DOD security requirements. Following this upgrade, any users using SMS verification will need to update your MFA method to an app-based authenticator.

- If you need login assistance, please contact sems@serdp-estcp.org

New User

You must create an account in order to access the SERDP & ESTCP Management System (SEMS). There are two ways to set up an account:

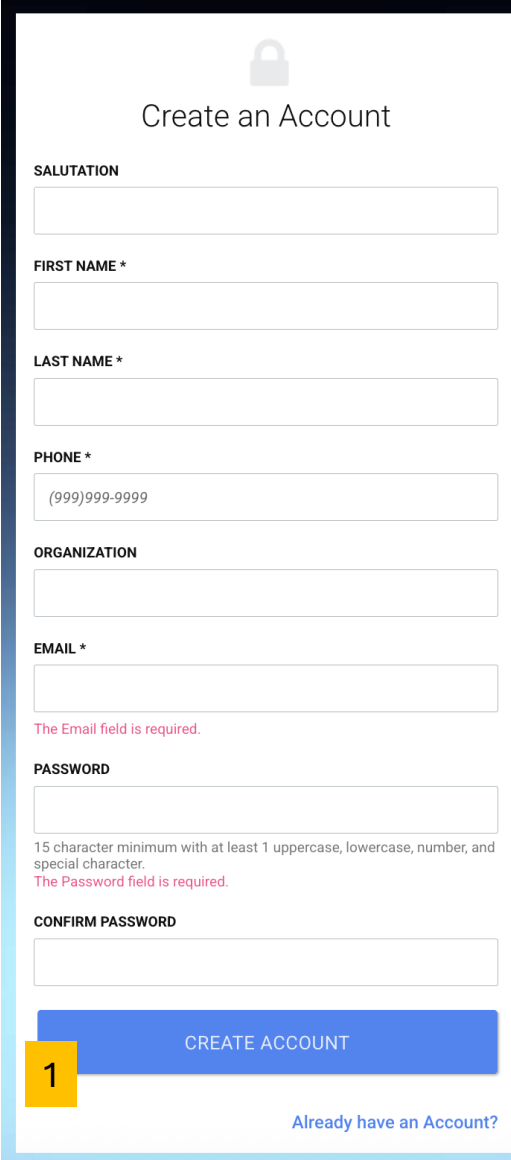
- **Standard Login:** Use the 'Create Account' option from the homepage. This uses an email address and password, as well as an MFA verification method, in order to allow access.
- **DoD CAC Login:** Use the 'Create DOD CAC Account' option from the homepage. This will link your CAC card to the account you create. CAC login is not required. DoD users may use the standard login.

Note: *CAC Accounts do not require an MFA verification method. However, if you choose to login with your registered email address and password, you will be prompted to set up an MFA verification method.*


Create Account

Create Account

1. Fill out the registration form and select “Create Account”
2. Account Confirmation
 - An email will be sent to the registered email address. Click the link provided in the email to confirm your account.
 - Once logged in, you will be prompted to set up MFA for your account.



The image shows a web form titled "Create an Account" with a lock icon. The form contains several input fields: SALUTATION, FIRST NAME *, LAST NAME *, PHONE * (with a placeholder (999)999-9999), ORGANIZATION, EMAIL *, PASSWORD, and CONFIRM PASSWORD. There are two red error messages: "The Email field is required." and "The Password field is required." A blue button labeled "CREATE ACCOUNT" is at the bottom. A yellow box with the number "1" is placed over the button. A link "Already have an Account?" is at the bottom right.


Create an Account

SALUTATION

FIRST NAME *

LAST NAME *

PHONE *

ORGANIZATION

EMAIL *

The Email field is required.

PASSWORD

15 character minimum with at least 1 uppercase, lowercase, number, and special character.
The Password field is required.

CONFIRM PASSWORD


1

[Already have an Account?](#)

Create DOD CAC Account

Create DOD CAC Account

1. Confirm your CAC certificate is displayed
2. Fill out the registration form and select “Create Account”
3. Account Confirmation
 - An email will be sent to the registered email address. Click the link provided in the email to confirm your account


Create an Account
Fill out the register form below

GOV PIV/CAC
C=US, O=U.S. Government, OU=DoD, OU=PKI, OU=CONTRACTOR,
[Redacted]

SALUTATION FIRST NAME * LAST NAME *

PHONE * ORGANIZATION

EMAIL

PASSWORD CONFIRM PASSWORD

15 character minimum with at least 1 uppercase, lowercase, number, and special character.
The Password field is required.

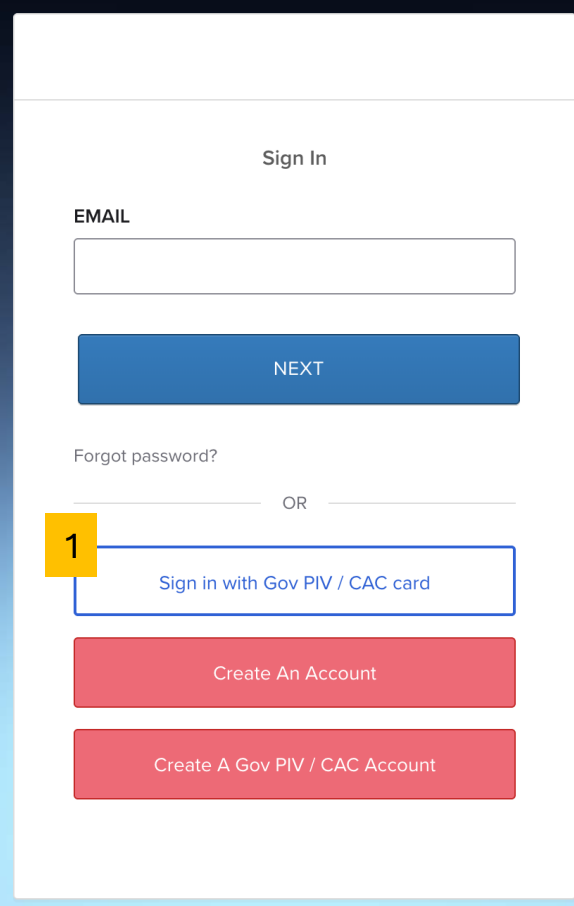
2 CREATE ACCOUNT

[Already have an Account?](#)

CAC Sign In

1. Sign In

- Select “Sign in with PIV/CAC card” when signing into the site



The image shows a web interface for signing in. At the top, it says "Sign In". Below that is an "EMAIL" label and a text input field. Under the input field is a blue button labeled "NEXT". Below the "NEXT" button is the text "Forgot password?". Below that is a horizontal line with "OR" in the center. Below the line is a yellow box with the number "1" next to a button labeled "Sign in with Gov PIV / CAC card". Below this button are two red buttons: "Create An Account" and "Create A Gov PIV / CAC Account".

Sign In

EMAIL

NEXT

Forgot password?

OR

1 Sign in with Gov PIV / CAC card

Create An Account

Create A Gov PIV / CAC Account

Setup MFA Verification Method

- Once you have set up an account, you will be prompted to set up the MFA verification method upon first login. You can select one of the available methods in the table below. How you receive the verification code will depend on the method you select.

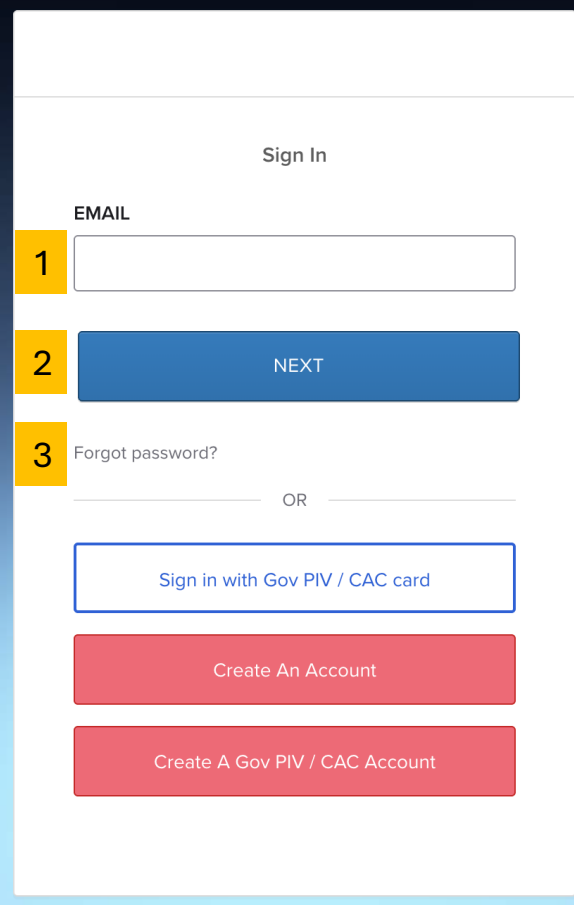
Verification Method	Verification Code/Notification
Okta Verify	Use a push notification sent to the Okta Verify app; single-use code inside the app
Other Authenticator App (any authentication app the user prefers; government employees are recommended Microsoft Authenticator, as it's pre-installed on government phones)	Single-use code inside the chosen app

- You may change the verification method after setup
- You may set up more than one method. This is a good idea if you have concerns about one not working or changing mobile devices.

Login to SEMS Account

Standard Login

1. Enter Email Address
2. Sign In
3. Forgot Password?
 - Select this link to reset password



The diagram illustrates a standard login form with three numbered steps highlighted in yellow boxes on the left. Step 1 points to an email input field. Step 2 points to a blue 'NEXT' button. Step 3 points to a 'Forgot password?' link. Below these are three additional options: a blue-outlined box for 'Sign in with Gov PIV / CAC card', and two red buttons for 'Create An Account' and 'Create A Gov PIV / CAC Account'. The form is titled 'Sign In' at the top.

Sign In

EMAIL

1

2 NEXT

3 [Forgot password?](#)

OR

[Sign in with Gov PIV / CAC card](#)

[Create An Account](#)

[Create A Gov PIV / CAC Account](#)

1. Password

2. Verify

- Moves you to the next step to choose your MFA method

Verify with your password

teresa.kostick@noblis.org

PASSWORD

1

2

VERIFY

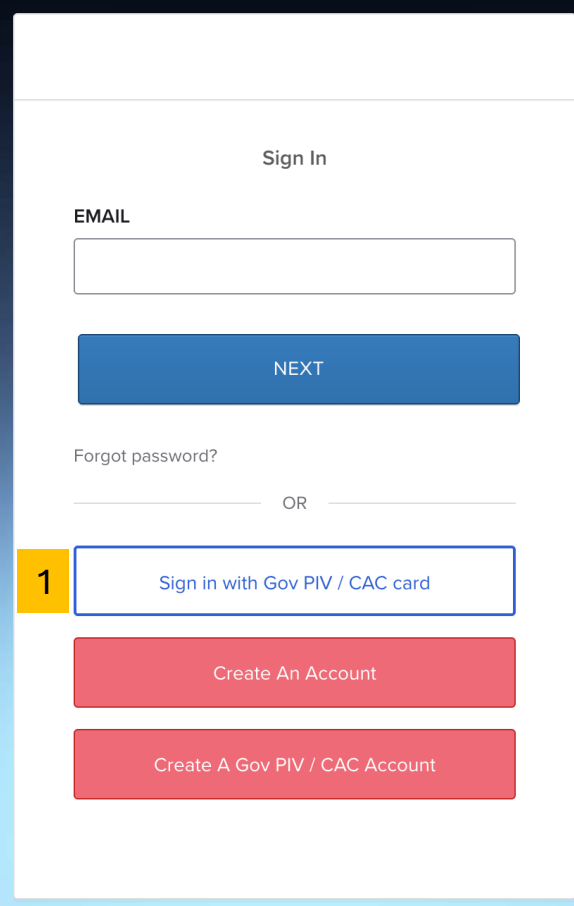
[Forgot password?](#)

[Verify with something else](#)

[Back to sign in](#)

CAC Login

1. Sign in with PIV/CAC card
 - This option does not require an MFA verification method.



The screenshot shows a web interface for signing in. At the top, it says "Sign In". Below that is an "EMAIL" label and a text input field. A blue "NEXT" button is positioned below the input field. Underneath the button is the text "Forgot password?". Below this is a horizontal line with "OR" in the center. A yellow callout box with the number "1" points to a button labeled "Sign in with Gov PIV / CAC card". Below this button are two red buttons: "Create An Account" and "Create A Gov PIV / CAC Account".

Sign In

EMAIL

NEXT

Forgot password?

OR

1 Sign in with Gov PIV / CAC card

Create An Account

Create A Gov PIV / CAC Account

Select Verification

One time setup of MFA verification method is required.

- You may change the verification method after setup
- You may setup more than one verification method. This is a good idea if you have concerns about one method not working, or you change mobile devices.

Note: *All authentication options are apps on your smartphone or mobile device and are downloaded through your app store. The recommended apps are free and do not require a subscription. At this time, no laptop or desktop authenticators are available.*

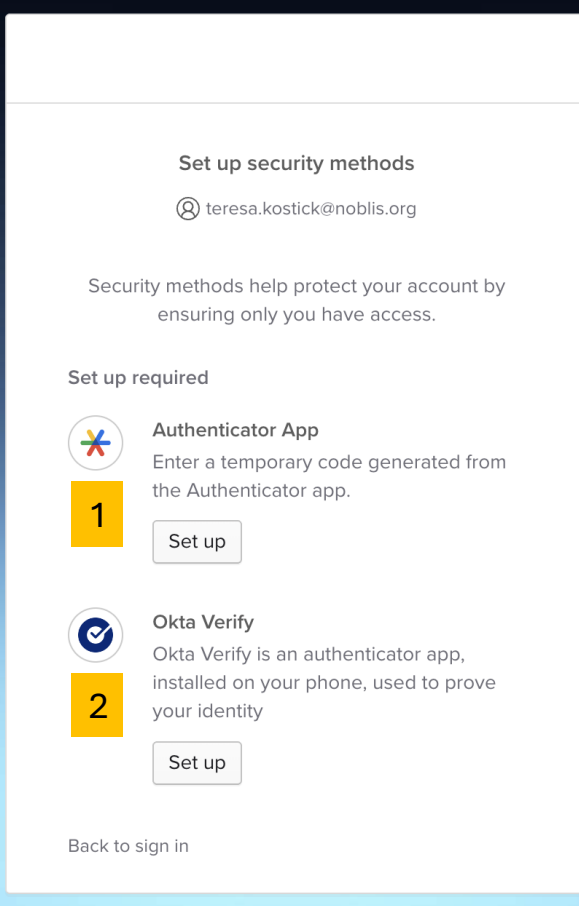
Set Up Multifactor Authentication (MFA)

1. Authenticator app

- Choose this option to use the authenticator app of your choosing
- The icon shown is for Google Authenticator, but this setup should work for most authenticator apps

2. Okta Verify

- Choose this option to set up the Okta Verify authenticator app



The screenshot shows a web interface for setting up security methods. At the top, it says "Set up security methods" with a user icon and email "teresa.kostick@noblis.org". Below this is a message: "Security methods help protect your account by ensuring only you have access." A section titled "Set up required" lists two options. The first option, "Authenticator App", is marked with a yellow box containing the number "1" and includes a "Set up" button. The second option, "Okta Verify", is marked with a yellow box containing the number "2" and also includes a "Set up" button. At the bottom left, there is a link that says "Back to sign in".

Set up security methods

teresa.kostick@noblis.org

Security methods help protect your account by ensuring only you have access.

Set up required

1 Authenticator App
Enter a temporary code generated from the Authenticator app.
Set up

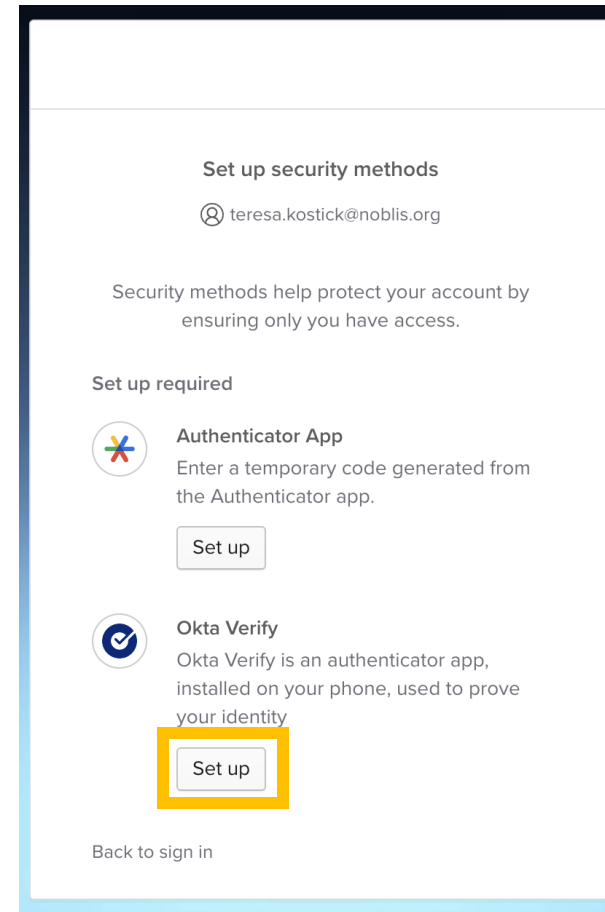
2 Okta Verify
Okta Verify is an authenticator app, installed on your phone, used to prove your identity
Set up

[Back to sign in](#)

Okta Verify

Okta Verify

- Click "Set up" for the Okta Verify option




Set up security methods


teresa.kostick@noblis.org

Security methods help protect your account by ensuring only you have access.

Set up required

 **Authenticator App**
Enter a temporary code generated from the Authenticator app.

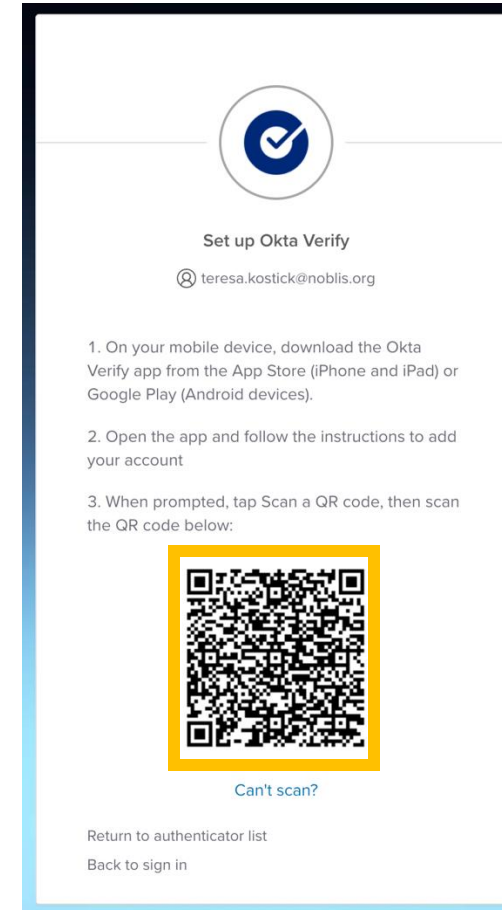
[Set up](#)

 **Okta Verify**
Okta Verify is an authenticator app, installed on your phone, used to prove your identity

[Set up](#)

[Back to sign in](#)

- Download the Okta Verify App to your phone
- Select “Organization”
- Skip adding account from another device
- Select “Yes, ready to scan”
- Using your phone camera, scan the QR code generated by SEMS
- Select next step:
 - “Return to authenticator list” to set up another MFA option
 - “Back to sign in” to return to the sign in form



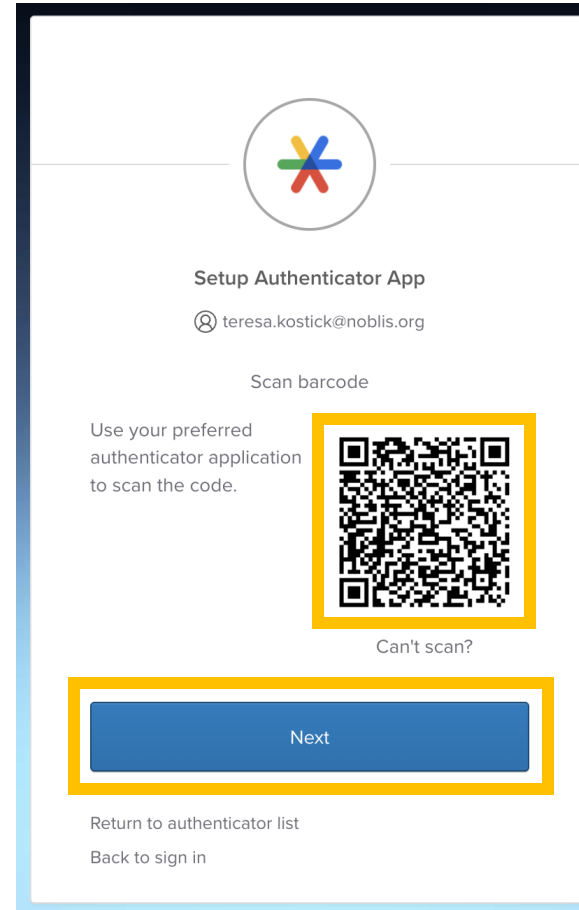
Other Authenticator

Use any authenticator app you prefer.

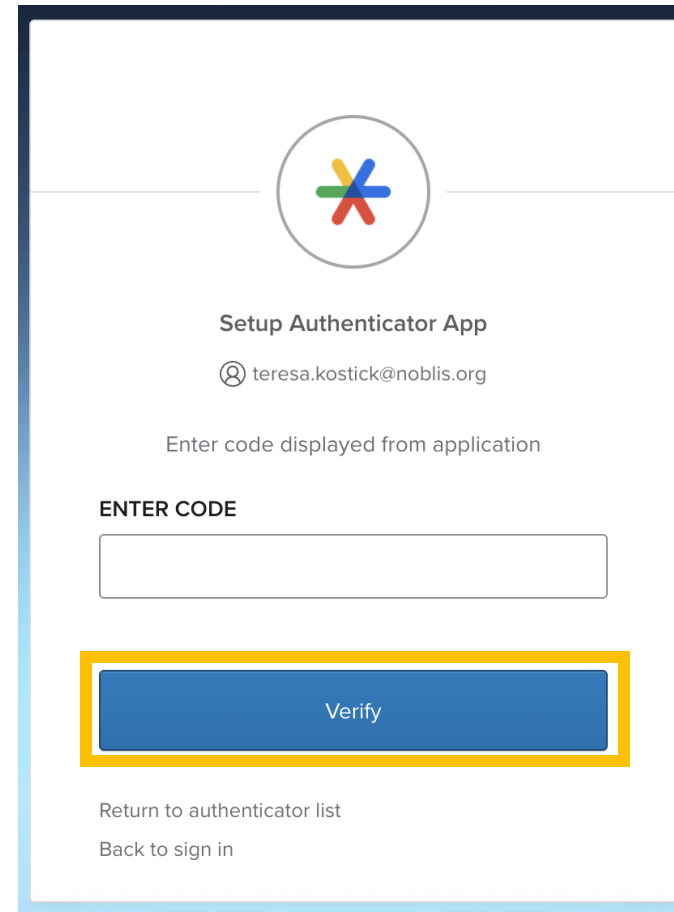
Government employees: Microsoft Authenticator is recommended, as it comes pre-installed on all government-issued phones.

Other Authenticator

- Download the Authenticator app of your choosing and add an account
- When ready, scan the QR code generated by SEMS
- Click “Next”



- Type in the code generated by your Authenticator app
- Click “Verify”



The screenshot shows the Microsoft Authenticator app setup interface. At the top is the Microsoft logo. Below it, the text "Setup Authenticator App" is displayed. Underneath, the email address "teresa.kostick@noblis.org" is shown next to a person icon. The instruction "Enter code displayed from application" is followed by the label "ENTER CODE" and a text input field. A blue "Verify" button is highlighted with a yellow border. At the bottom, there are two links: "Return to authenticator list" and "Back to sign in".

Microsoft

Setup Authenticator App

teresa.kostick@noblis.org

Enter code displayed from application

ENTER CODE

Verify

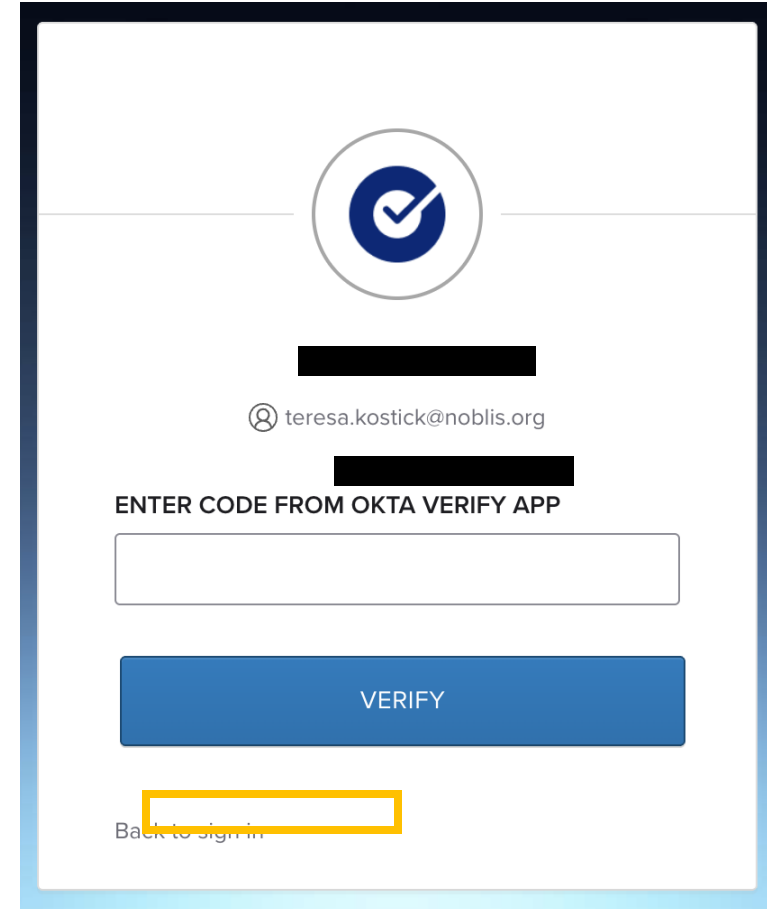
[Return to authenticator list](#)

[Back to sign in](#)

After MFA Setup

The next time you log into SEMS, after you enter your email address and password, you will be prompted to enter the code received by the verification method that you have setup for your account.

- Have multiple set up? Don't want to use the default? Use the "Verify with something else" link to choose a different MFA method.

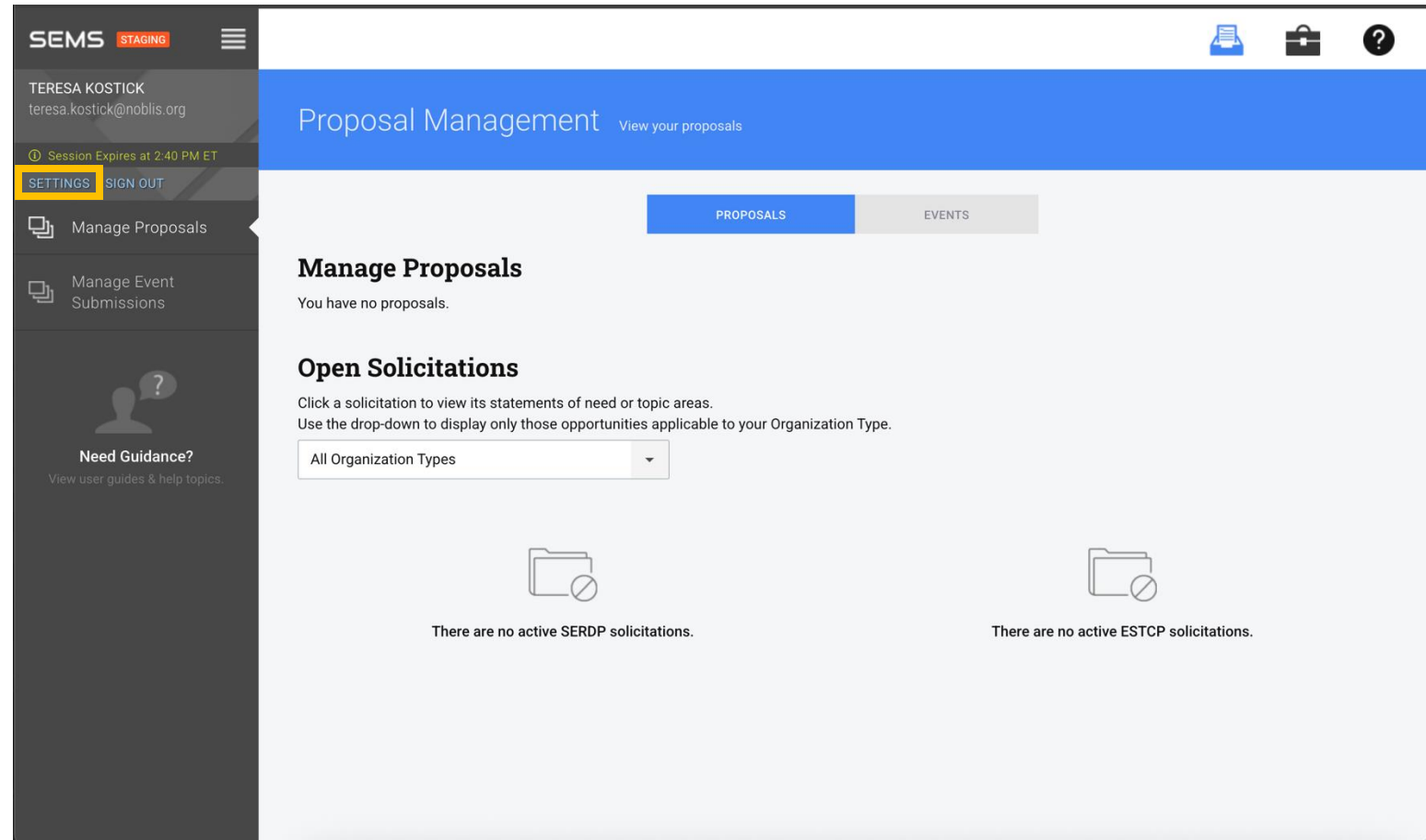


The screenshot shows a login verification page. At the top is a blue circular icon with a white checkmark. Below it is a black redaction bar. Underneath is the email address 'teresa.kostick@noblis.org' next to a person icon. Another black redaction bar is below the email. The text 'ENTER CODE FROM OKTA VERIFY APP' is displayed above a white input field. Below the input field is a blue button labeled 'VERIFY'. At the bottom left, there is a link 'Back to sign in' next to a yellow rectangular button.

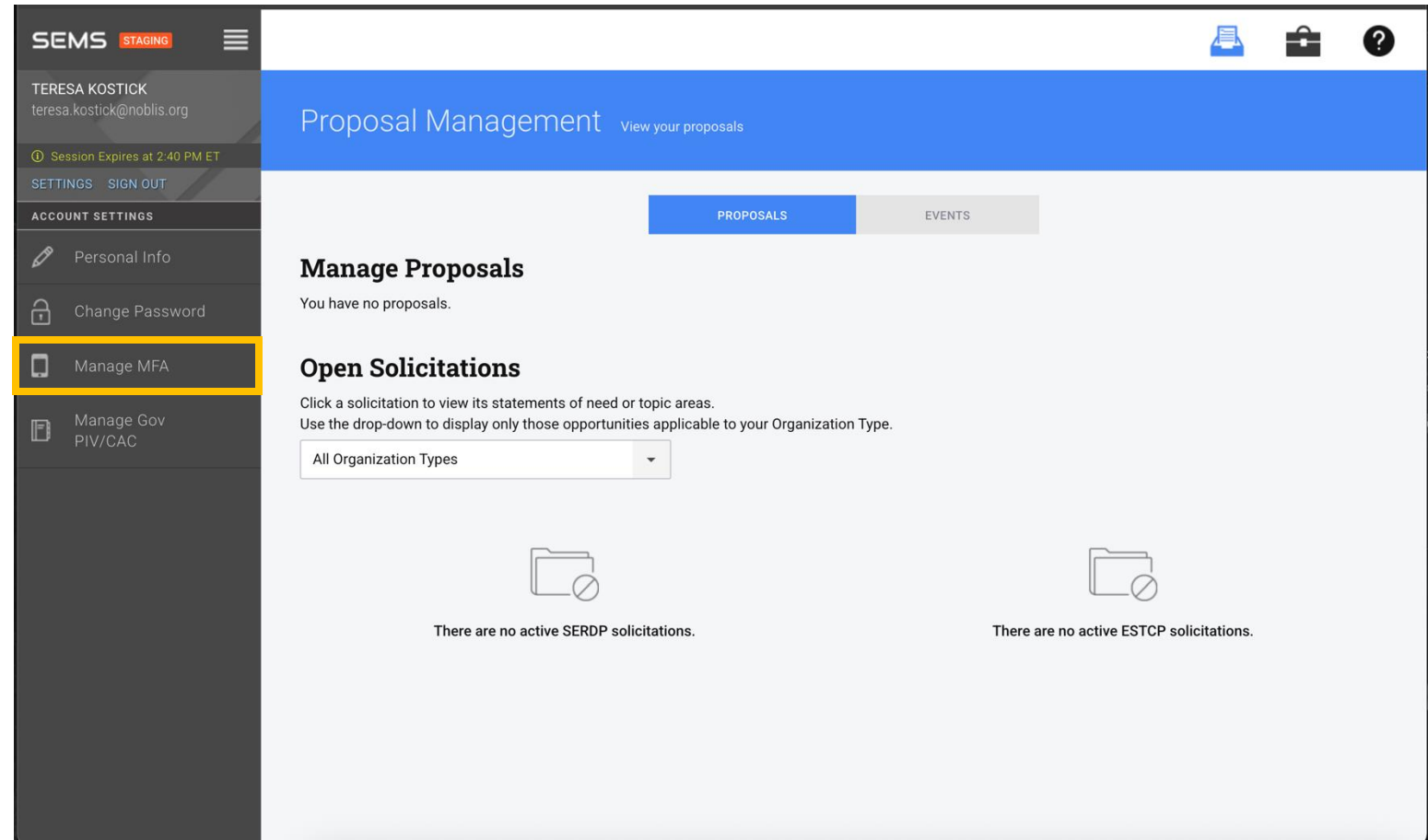
Managing MFA Verification Method

To reset your MFA factors:

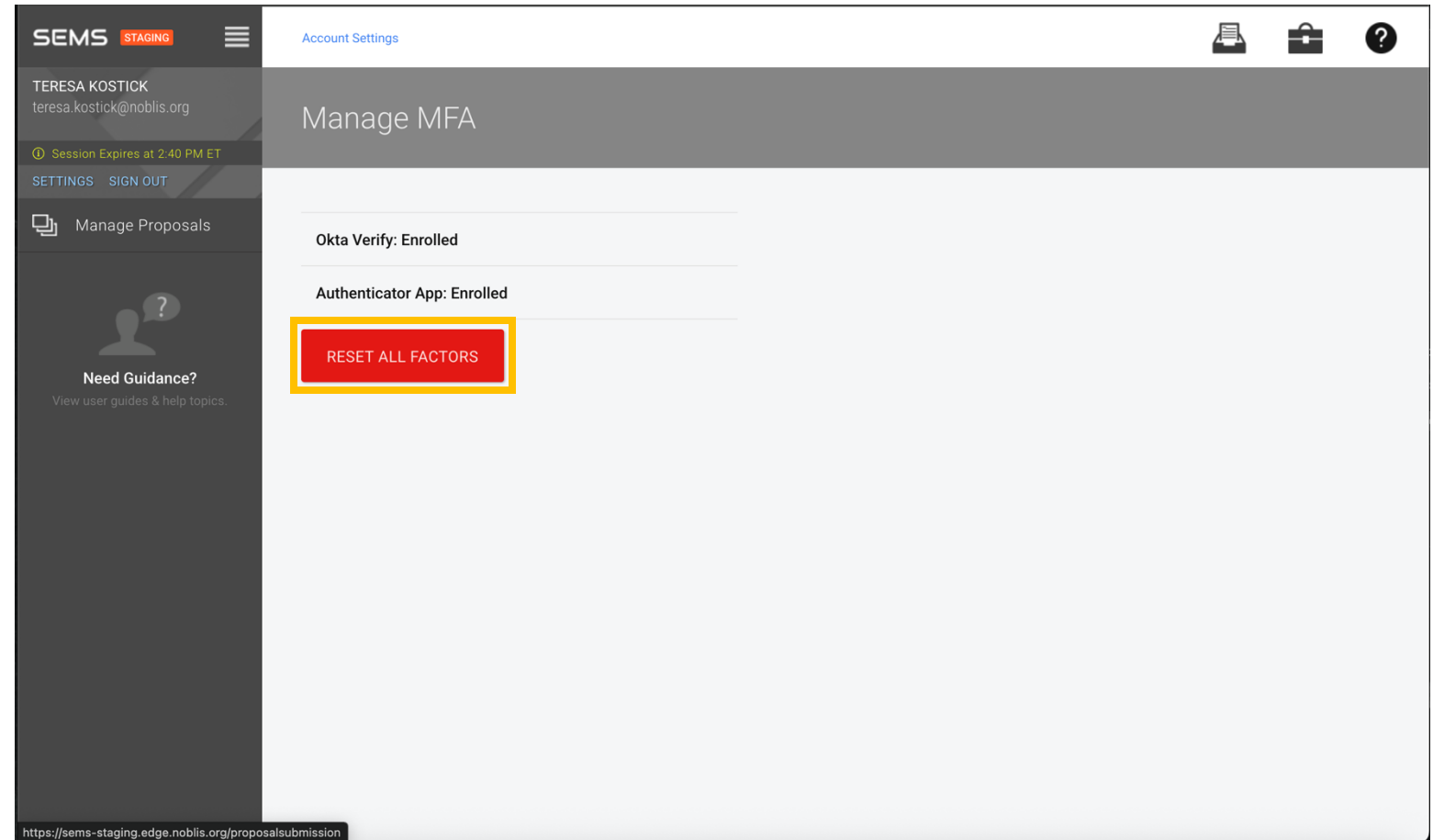
- Click “Settings” in the gray sidebar



- Click
“Manage
MFA”



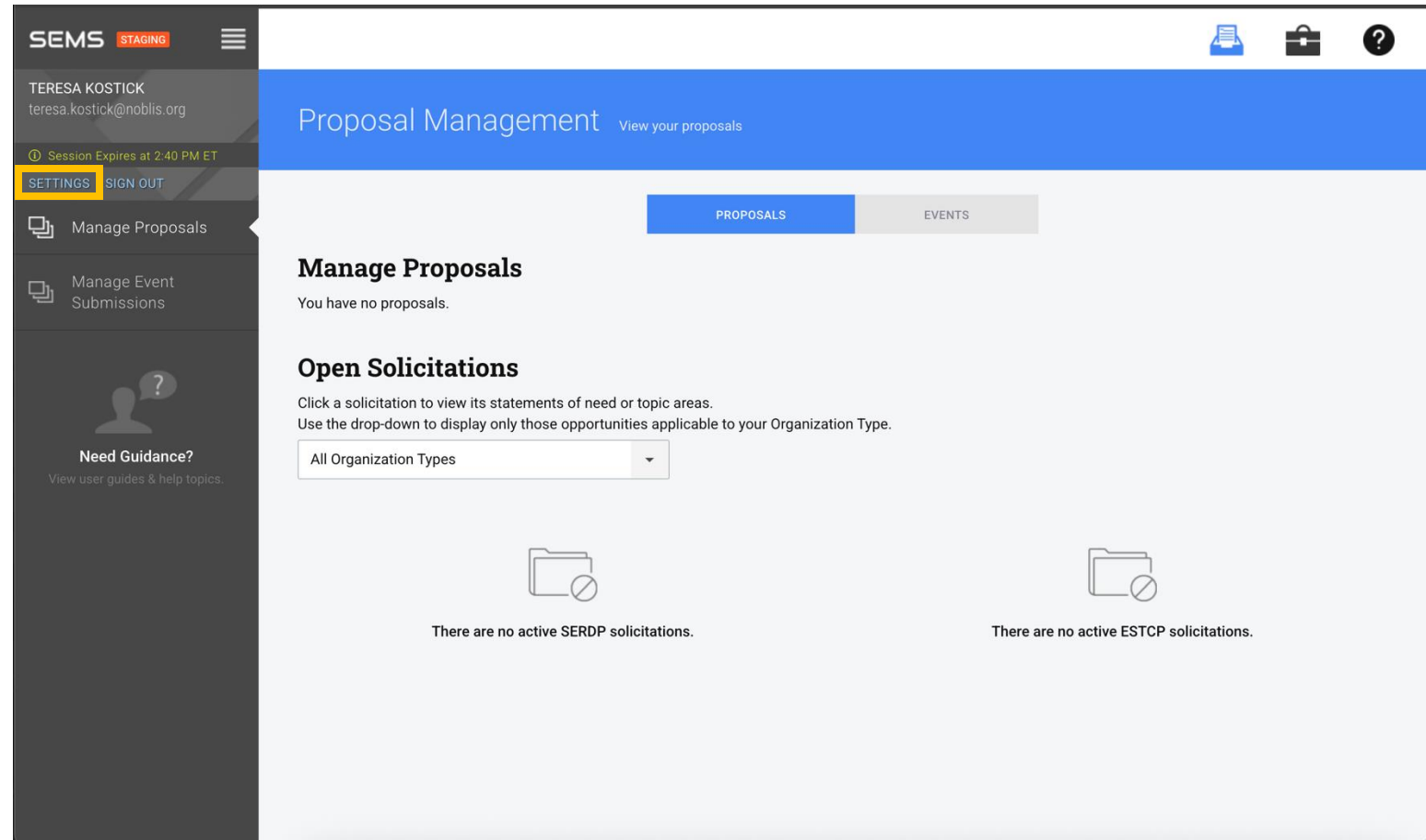
- Click “Reset All Factors” to clear all MFA methods
- SEMS will prompt you to set up new factors the next time you sign in



Adding PIV/CAC to an Account

To add your PIV/CAC to your account:

- Click “Settings” in the gray sidebar



- Click
“Manage Gov
PIV/CAC”

The screenshot displays the SEMS STAGING web application interface. On the left is a dark sidebar with the SEMS logo and 'STAGING' label at the top. Below the logo, the user's name 'TERESA KOSTICK' and email 'teresa.kostick@noblis.org' are shown. A session expiration notice states 'Session Expires at 2:40 PM ET'. Navigation links include 'SETTINGS', 'SIGN OUT', and 'ACCOUNT SETTINGS'. Under 'ACCOUNT SETTINGS', there are four menu items: 'Personal Info', 'Change Password', 'Manage MFA', and 'Manage Gov PIV/CAC'. The 'Manage Gov PIV/CAC' item is highlighted with a yellow border. The main content area has a blue header bar with the text 'Proposal Management' and a link 'View your proposals'. Below this, there are two tabs: 'PROPOSALS' (active) and 'EVENTS'. The 'Manage Proposals' section states 'You have no proposals.' The 'Open Solicitations' section includes instructions to click a solicitation to view its details and use a drop-down to filter by organization type. A drop-down menu currently shows 'All Organization Types'. Below this, there are two large empty boxes with folder icons and a slash, each containing the text 'There are no active [SERDP/ESTCP] solicitations.'

- Click “Link Gov PIV/CAC” to use your ID card to log in

