Centers for Medicare & Medicaid Services

Enterprise Portal User Guide

Table of Contents

1. Introduction

The Centers for Medicare & Medicaid Services (CMS) Enterprise Portal project supports the implementation of a viable and effective portal program. The essence of the CMS Enterprise Portal strategy is the user interface (UI) presented by a portal as an “Integration Glass,” a single window through which users may see and access information and applications from multiple sources, based on each individual user’s roles and permissions. A portal combines and displays content and forms from multiple applications and information sources, supports users with navigation and cross-enterprise search tools, supports simplified sign-on, and uses role-based access and personalization to present each user with only relevant content and applications. Portal benefits include enhanced productivity, efficiency, workflows, communication, and the exchange of ideas among CMS user communities.

CMS Enterprise Portal is the common user presentation layer providing a secure, browser-based, centralized point of entry for users to access the underlying data. CMS Enterprise Portal logically consolidates information and business functions, helping to ensure consistent delivery and presentation of information across the user base. Users can collaborate; share queries and reports; use browser-based reporting applications; manipulate data and information; and save that data and information in the portal layer, all without having to exit the portal to use other applications. CMS established the Enterprise Portal to provide business partners with a means to create a single user ID that they can use to access one or more CMS applications.

This user guide provides the information necessary for users to effectively use CMS Enterprise Portal. This document will be updated as new features and functionality are added to CMS Enterprise Portal.

There are no privacy or security concerns for this document because it does not contain any Personal Health Information (PHI) or Personally Identifiable Information (PII).

1.1. Conventions

This document provides figures and corresponding narrative to describe how to use CMS Enterprise Portal. There are no specific stylistic commands or syntax used within this document. Typically, a direction or step is described, followed by a screen print that shows the corresponding action or result.

1.2. Cautions and Warnings

CMS Enterprise Portal users are provisioned by the Enterprise User Administration (EUA) process or the CMS Enterprise Portal process. Users must have their CMS identifier (ID) added to the relevant Portal job code or role (additional information is in *Section 2.2 - User Access Considerations*) prior to accessing CMS Enterprise Portal.

2. Getting Started

This section provides information about setting up, accessing, navigating, and exiting CMS Enterprise Portal.

2.1. Set-up Considerations

CMS Enterprise Portal users are provisioned either by the Enterprise User Administration (EUA) process or the CMS Enterprise Portal setup process. CMS Enterprise Portal users can only view the applications to which they have been granted access through the respective job code(s) or approved role request(s).

The following additional considerations optimize access to CMS Enterprise Portal:

Use one of the following browsers with JavaScript enabled:

- Google Chrome
- Microsoft Edge (Chromium)
- Mozilla Firefox
- Apple Safari

Note

CMS Enterprise Portal no longer supports Microsoft's Internet Explorer web browser.

Please be sure to disable pop-up blockers (if allowed by your organization), enable JavaScript, and disable your Chrome browser extensions as these can impact the use of the CMS Enterprise Portal.

The only computer input device needed to access CMS Enterprise Portal is a keyboard; a mouse is not required, although it is recommended.

2.2. User Access Considerations

CMS Enterprise Portal users are provisioned by the EUA process or the CMS Enterprise Portal process, depending on the application(s) they will be accessing. These provisioning processes are described in *Section 2.2.1 - EUA Process* and *Section 2.2.2 - CMS Enterprise Portal Process*. CMS Enterprise Portal users can only view the applications to which they have been granted access through the respective job code(s) or approved role request(s).

2.2.1. EUA Process

For applications provisioned via EUA, if a user does not have a EUA CMS user ID or the proper Portal job code, they must file a EUA workflow request by completing an application for access to CMS computer systems. An online version of that application can be found at the following URL: http://www.cms.gov/InformationSecurity/Downloads/EUAaccessform.pdf.

This application is used to request access to any of the job codes that will relate to CMS Enterprise Portal and the EUA applications it hosts. If access is granted, the user will be notified

by email with the appropriate job code and/or CMS user ID.

Note

CMS user IDs created using the EUA process are exactly four characters in length.

If the user already has a CMS user ID and password provisioned via EUA and wishes to change the password, they can click the following link, follow the log-in procedures, and click on the **Change My Password** link after signing into the EUA system:

- https://eua.cms.gov/iam/im/pri/

The EUA process is described at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/EUA.html.

Once an EUA Enterprise Portal user is registered and logged into CMS Enterprise Portal, they can manage their Multi-factor Authentication (MFA) Devices by clicking the **My Profile** link in the drop-down menu displayed next to the user name in the top navigation bar.

An EUA user cannot change their profile information or request access to application(s) within the CMS Enterprise Portal system. Those activities must be performed from within the EUA system at https://eua.cms.gov/iam/im/pri/.

2.2.2. CMS Enterprise Portal Process

For applications provisioned via CMS Enterprise Portal, if a user does not have a CMS Enterprise Portal user ID, they must register for a CMS Enterprise Portal user account from the CMS Enterprise Portal public home page by clicking on the **New User Registration** button. Detailed steps are in Section 3 - *Registering for CMS Enterprise Portal*.

Note

CMS user IDs created using the CMS Enterprise Portal process are a minimum of six and maximum of 74 characters in length.

Once a user is registered in CMS Enterprise Portal and logged into CMS Enterprise Portal, they can view and change profile information and request access to applications by clicking the **My Profile** and **My Access** links, respectively, in the drop-down menu displayed next to the user name in the top navigation bar.

2.3. Accessing the System

To access CMS Enterprise Portal, open a browser window (refer to the list of approved browsers in *Section 2.1 - Set-up Considerations*) and type the following URL into the address bar: https://portal.cms.gov (Internet) or https://portal.cms.cmsnet (CMS VPN or CMS network).

The system displays the CMS Enterprise Portal public home page, as shown in *Figure 1: CMS Enterprise Portal Public Home Page*.

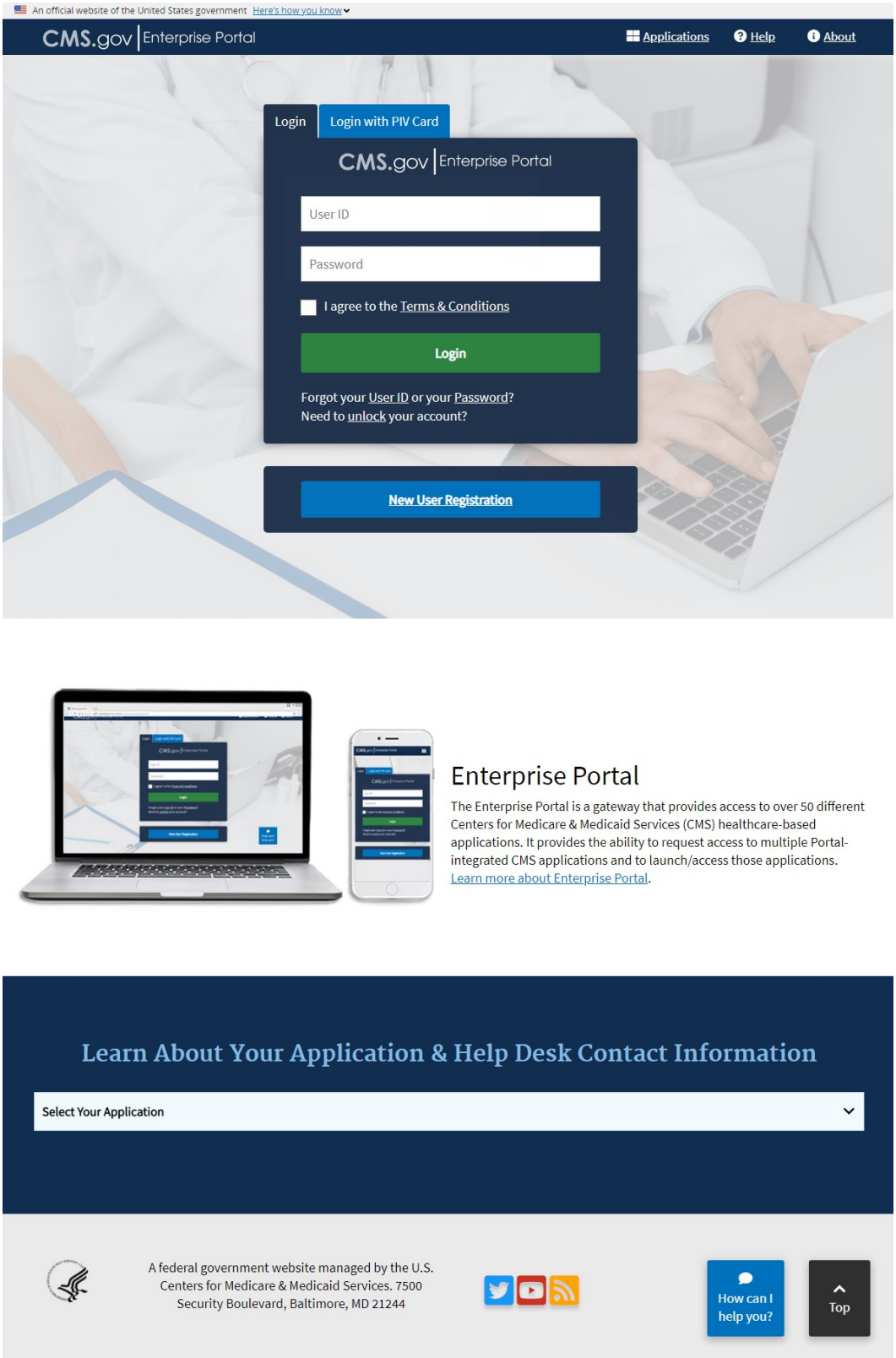

Figure 1: CMS Enterprise Portal Public Home Page

2.4. Public Home Page

The first page users will see when accessing CMS Enterprise Portal is the public home page as shown in *Figure 1: CMS Enterprise Portal Public Home Page*.

The header is designed to contain the following navigation elements:

- **CMS.gov | Enterprise Portal link:** Clicking this link performs a page refresh of the CMS Enterprise Portal public home page.

- **Applications link:** Clicking this link allows users to select their application from a drop-down menu and view their application's Help Desk and support information.
- **Help link:** Clicking this link directs you to the Help Center where you can view the the answers to frequently asked questions, view the Enterprise Portal user guides, or view the Enterprise Portal how-to videos.
- **About link:** Clicking this link displays information about CMS Enterprise Portal.

The footer contains the Department of Health and Human Services (HHS) logo along with following widgets for social media: CMS Twitter, CMS YouTube, and CMS RSS Feed.

The public home page also provides the registration functionality for new users (refer to section 3 - *Registering for CMS Enterprise Portal* for more details) and login functionality for users who have already registered (refer to section 4 - Logging In for more details).

2.5. Session Timeout

Session timeout occurs if users do not perform any action on the CMS Enterprise Portal website and remain inactive for 30 minutes. When this happens, a session pop-up message is displayed allowing a user to either stay logged in or log out from the system.

2.6. Exiting the System

To exit CMS Enterprise Portal, click the **Log Out** link located at the top-right of the page, as shown in *Figure 2: Logging Out of CMS Enterprise Portal*. The system logs you out and returns to the CMS Enterprise Portal public home page.

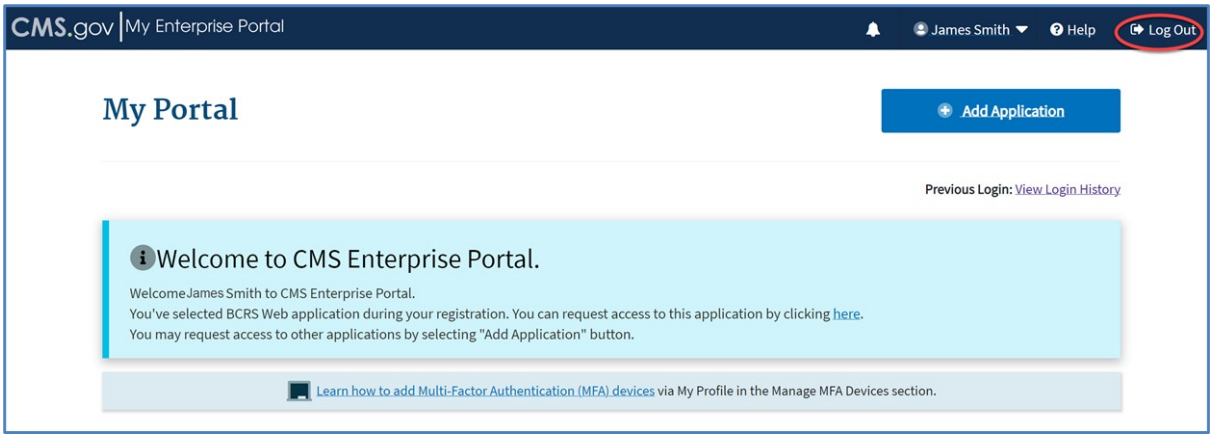

Figure 2: Logging Out of CMS Enterprise Portal

3. Registering for CMS Enterprise Portal

This section provides information on how to register and create a user ID and password through the CMS Enterprise Portal process. The following are the step-by-step instructions.

1. On the CMS Enterprise Portal home page, click the **New User Registration** button, as shown in *Figure 3: New User Registration Button on Public Home Page*.

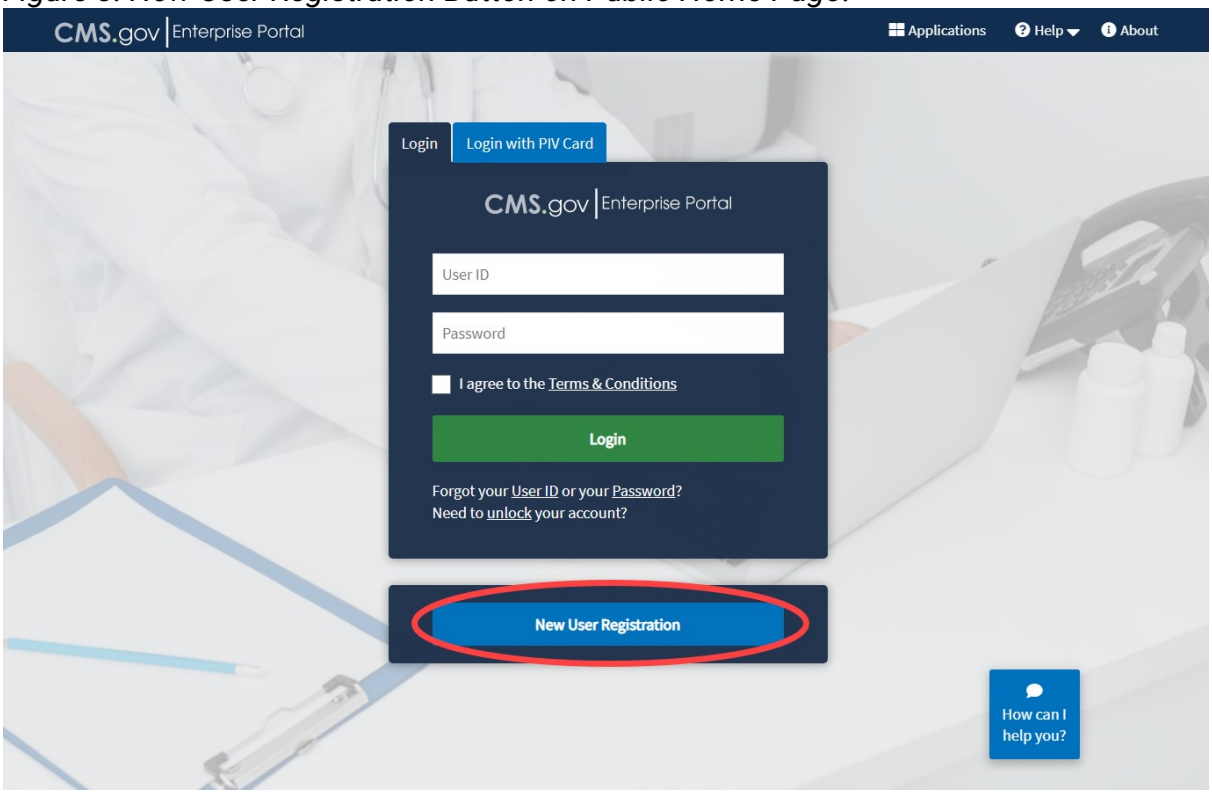

Figure 3: New User Registration Button on Public Home Page

2. On **Step #1: Select Your Application** page, select your application from the **Select Your Application** drop-down list, as shown in *Figure 4: Step 1 of New User Registration – Choose Your Application*.

Figure 4: Step 1 of New User Registration – Choose Your Application

The Terms & Conditions information displays, as shown in *Figure 5: Terms & Conditions Information Displayed on Selecting CMS Enterprise Portal-Provisioned Application*.

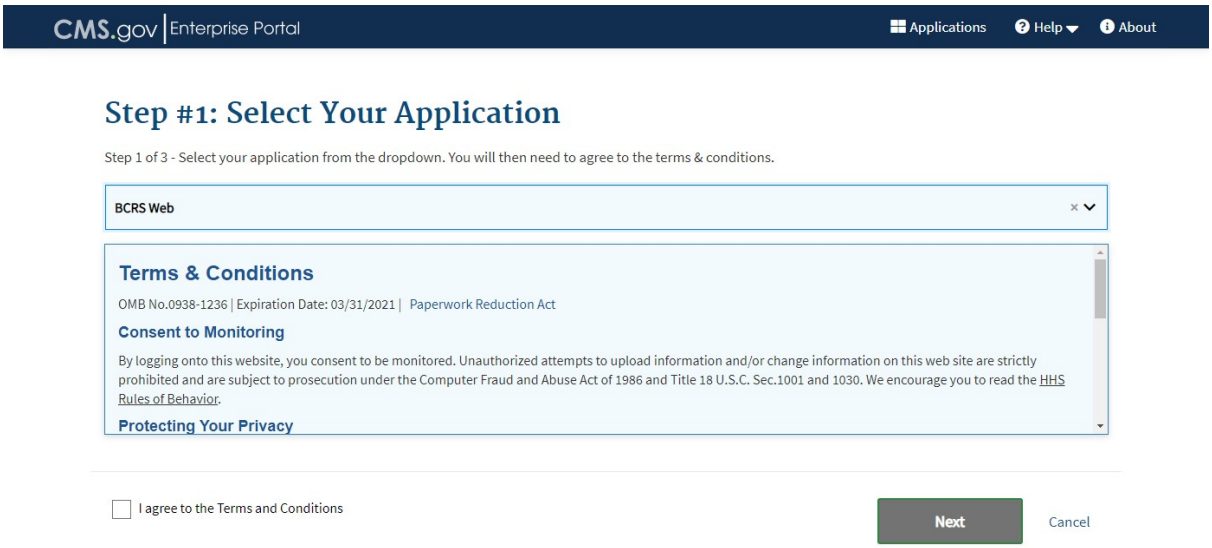

Figure 5: Terms & Conditions Information Displayed on Selecting CMS Enterprise Portal-Provisioned Application

Note

Terms & Conditions are displayed only when a CMS Enterprise Portal-provisioned application is selected from the **Select Your Application** drop-down list. Selecting an EUA-provisioned application displays information, as shown in *Figure 6: Help Message Displayed on Selecting EUA-Provisioned Application*.

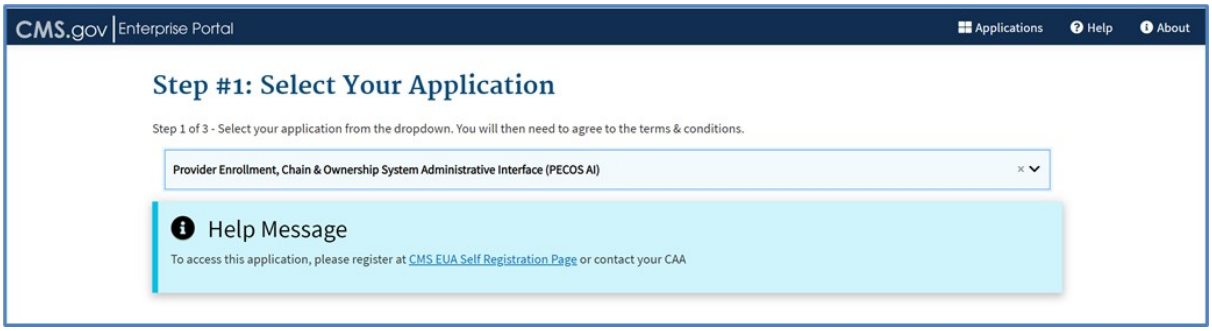

Figure 6: Help Message Displayed on Selecting EUA-Provisioned Application

Note

Selecting an IDM-provisioned application displays information, as shown in *Figure 7: Help Message Displayed on Selecting IDM-Provisioned Application*.

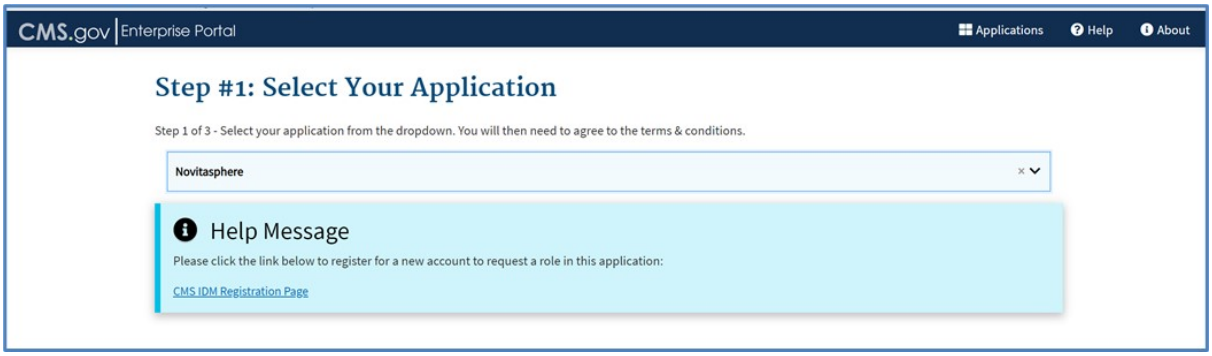

Figure 7: Help Message Displayed on Selecting IDM-Provisioned Application

3. Read the Terms & Conditions, select **I agree to the Terms and Conditions**, and then click **Next** to continue with the registration process, as shown in *Figure 8: Agreeing to Terms and Conditions*.

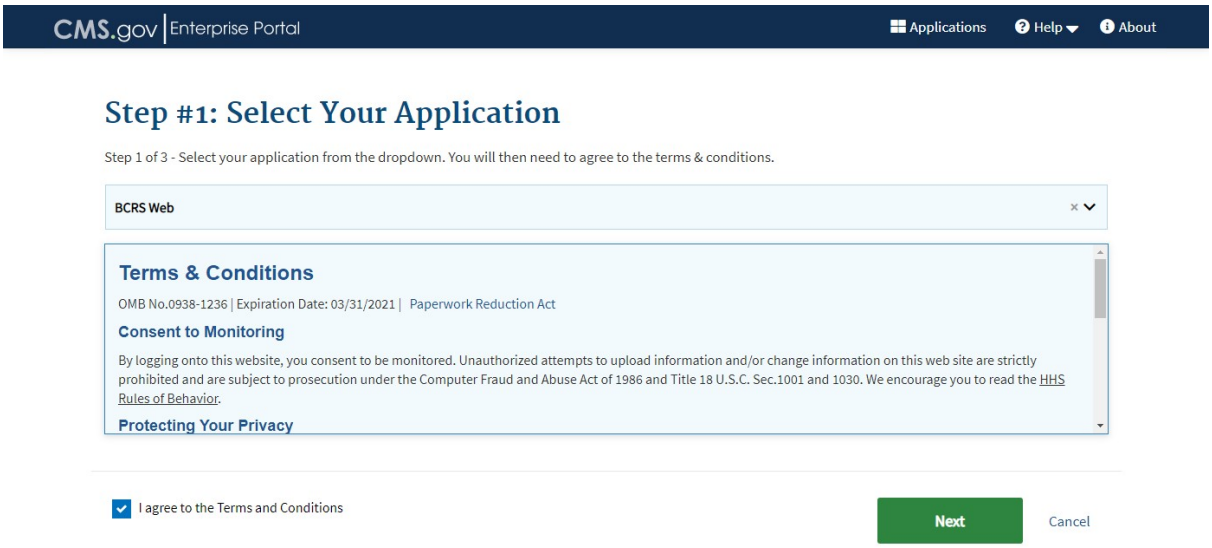

Figure 8: Agreeing to Terms and Conditions

The **Step #2: Register Your Information** page displays, as shown in *Figure 9: Step 2 of New User Registration - Register Your Information (Blank)*.

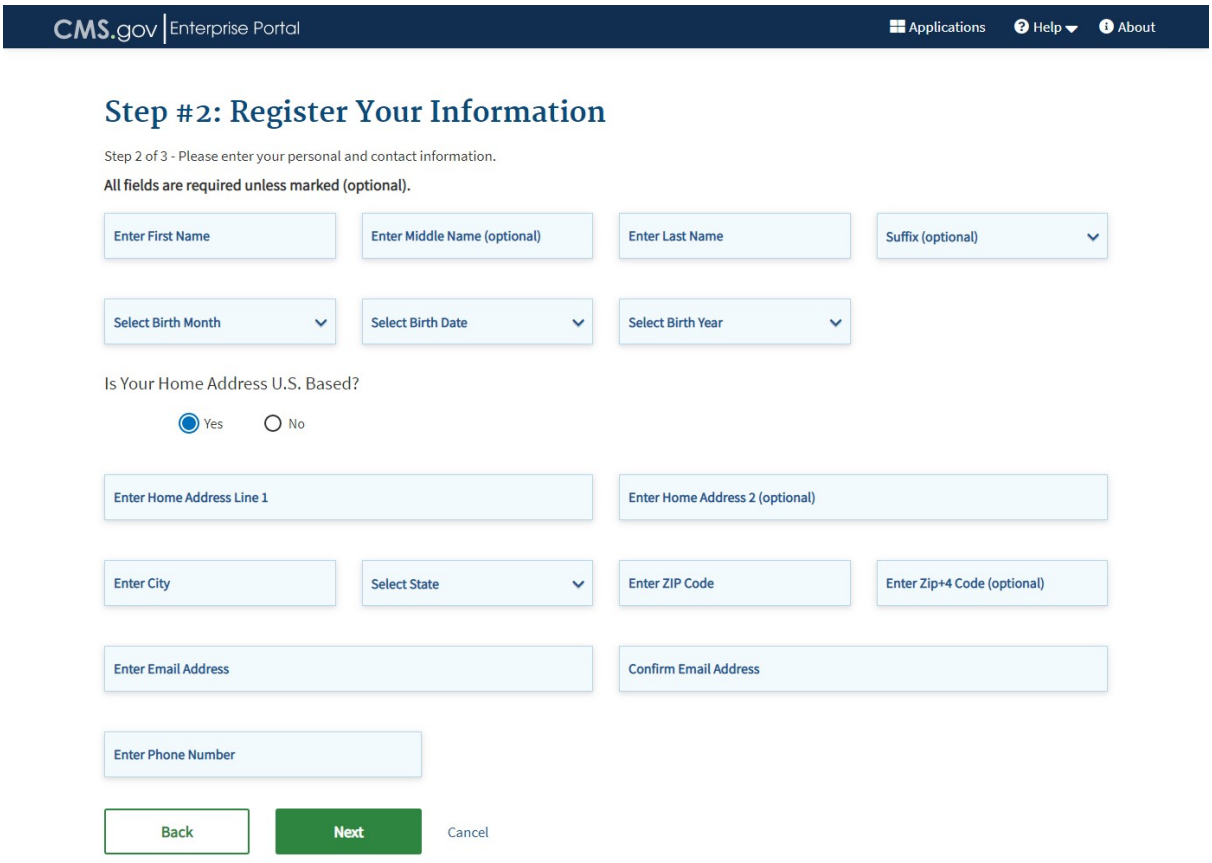

Figure 9: Step 2 of New User Registration - Register Your Information (Blank)

4. Provide the information requested on the **Step #2: Register Your Information** page, as shown in *Figure 10: Step 2 of New User Registration - Register Your Information (Completed)*. All fields are required and must be completed unless marked “Optional”. After all required information has been provided, click **Next** to continue.

Note

You may click Cancel at any time to exit out of the registration process. Changes entered will not be saved. To go to the previous step, click the **Back** button.

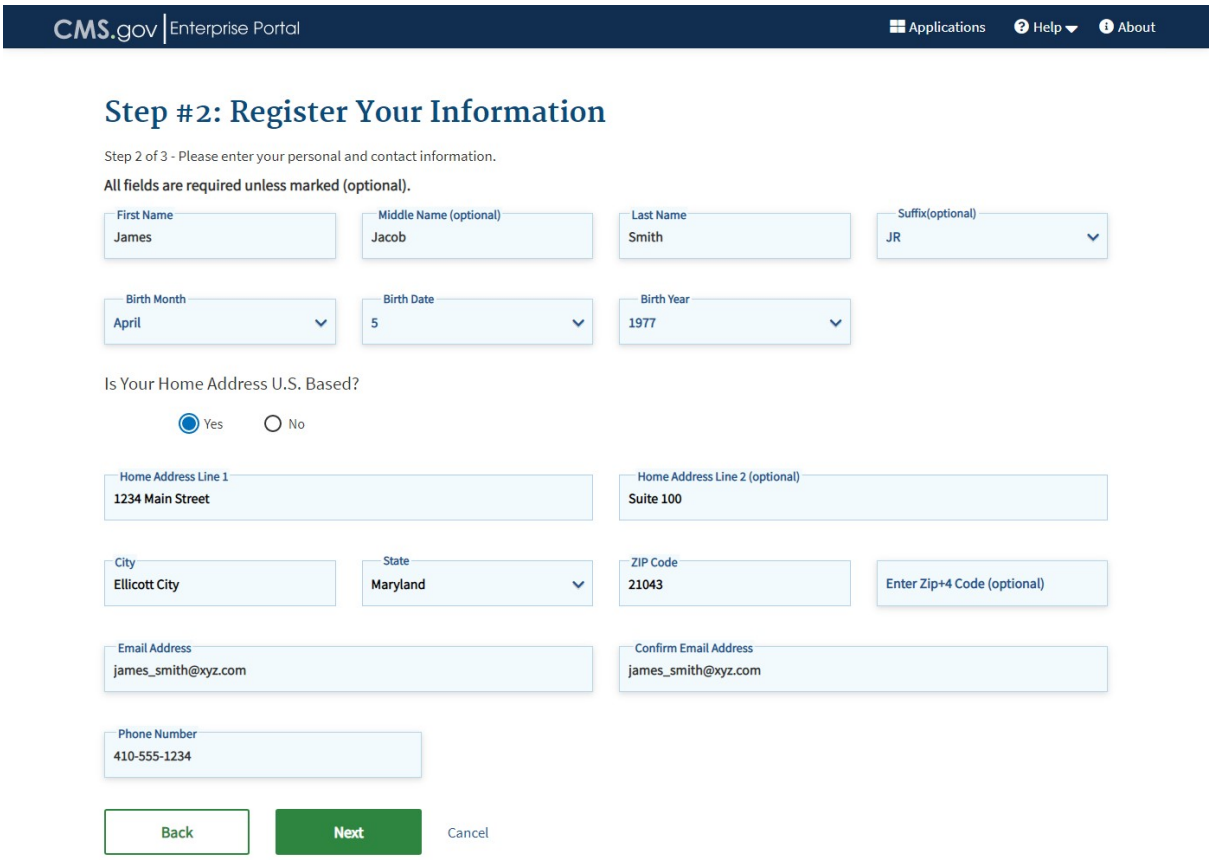

Figure 10: Step 2 of New User Registration - Register Your Information (Completed)

The **Step #3: Create User ID, Password & Security Question/Answer** page displays, as shown in *Figure 11: Step 3 of New User Registration – Create User ID, Password & Security Question/ Answer* (Blank).

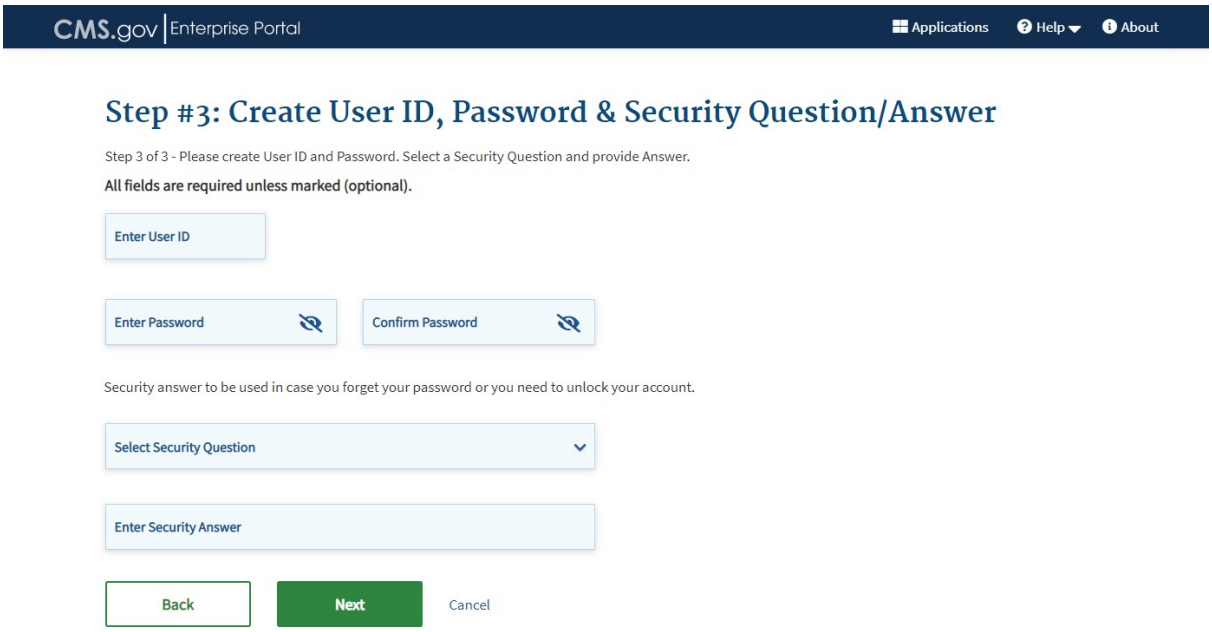

Figure 11: Step 3 of New User Registration – Create User ID, Password & Security Question/ Answer (Blank)

5. Create and enter a user ID in the **Enter User ID** field based on the requirements for creating a user ID, as shown in Figure 12: Step 3 of New User Registration – User ID Entered.

Note

Instructions are displayed, in the form of tool tip, on what you are required to include in your user ID.

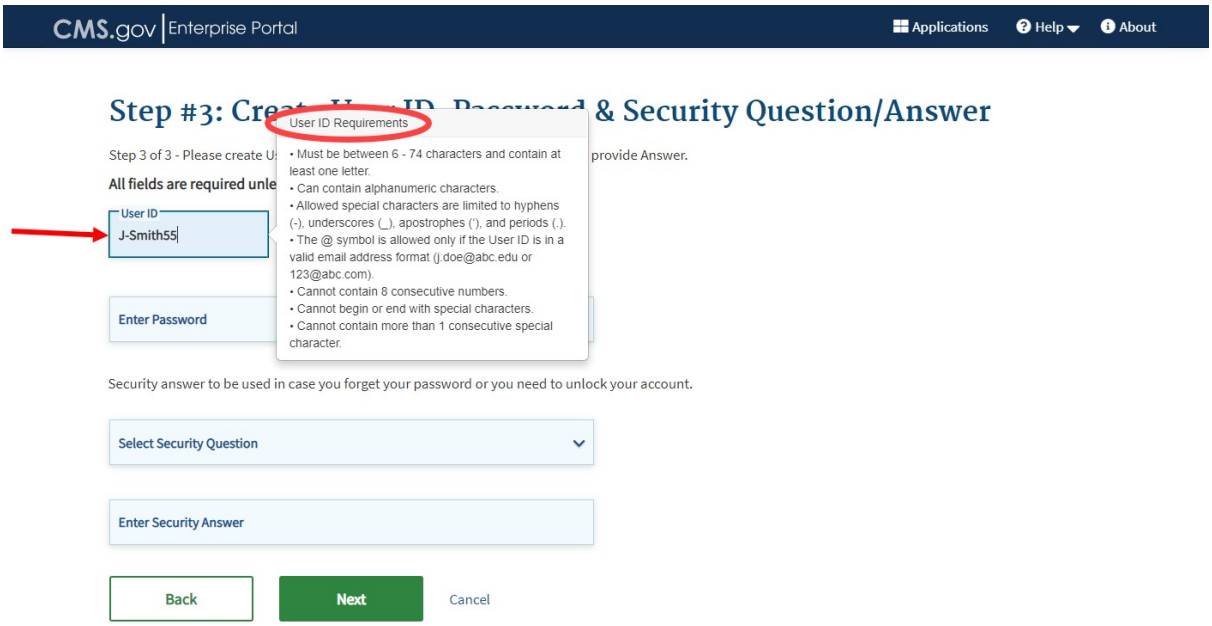

Figure 12: Step 3 of New User Registration – User ID Entered

6. Create and enter a password in the **Enter Password** field based on the requirements for creating a password, as shown in Figure 13: Step 3 of New User Registration – Password Entered. Enter the same password in the **Enter Confirm Password** field.
   Note

   Instructions are displayed, in the form of tool tip, on what you are required to include in your password.

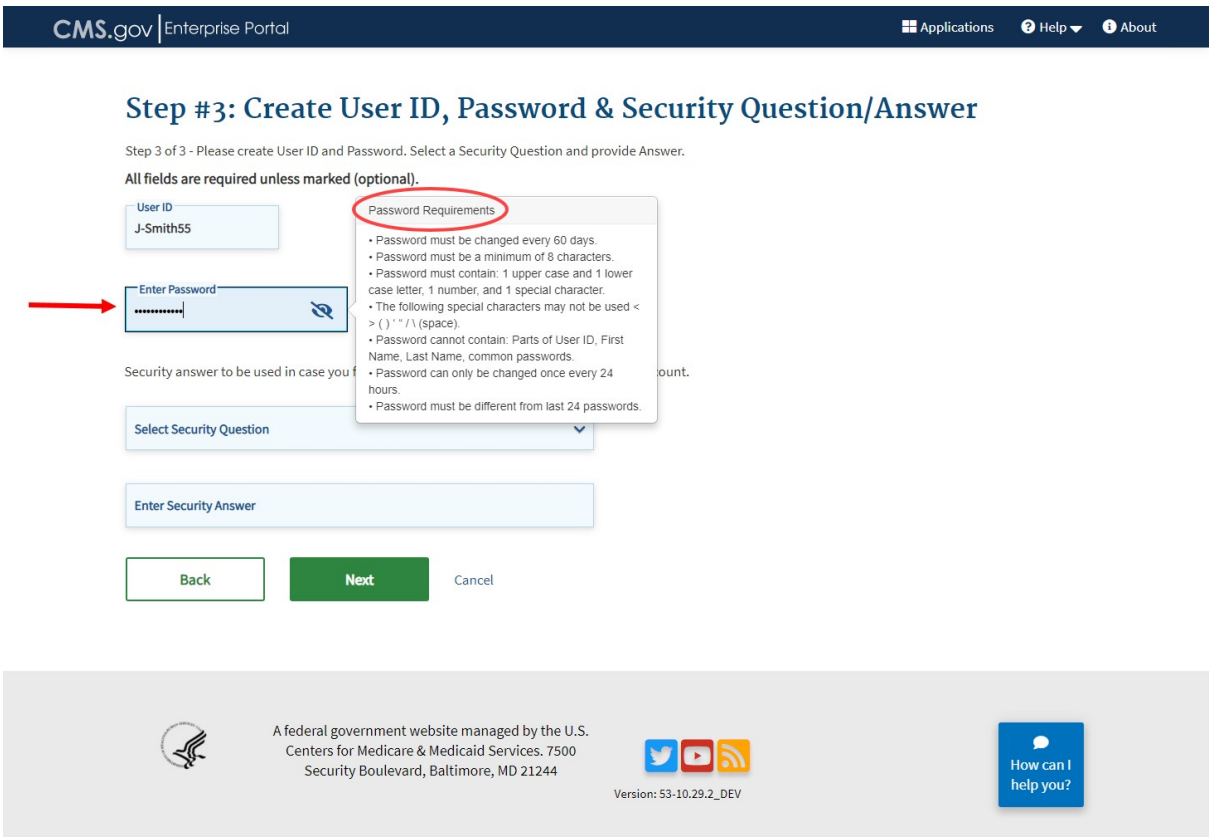

Figure 13: Step 3 of New User Registration – Password Entered

7. After entering the user ID and password, select a question in the **Select Your Security Question** drop-down list and enter the answer you want to be saved with the question, as shown in *Figure 14: Step 3 of New User Registration – Create User ID, Password & Security Question/ Answer* (Completed). Your security answer is used in case you forget your password, or you need to unlock your account. Click **Next** to complete the registration process.
   Note

Instructions are displayed, in the form of tool tip, on what you are required to include in your security question answer.

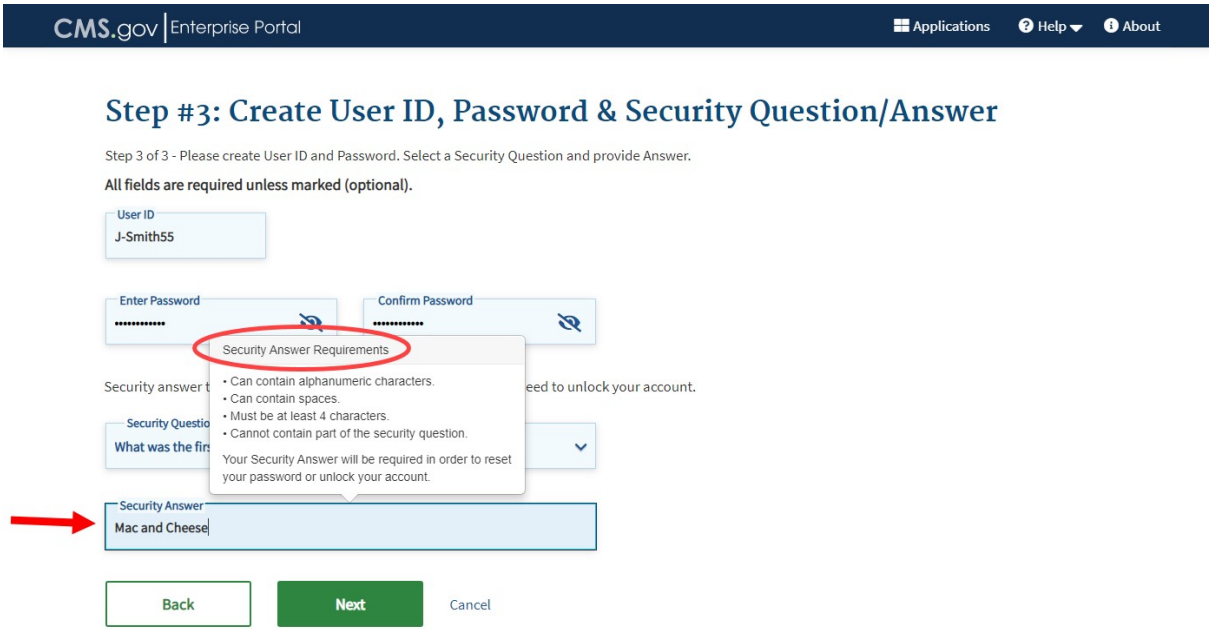

Figure 14: Step 3 of New User Registration – Create User ID, Password & Security Question/ Answer (Completed)

The **New User Registration Summary** page displays, as shown in Figure 15: New User Registration – Registration Summary.

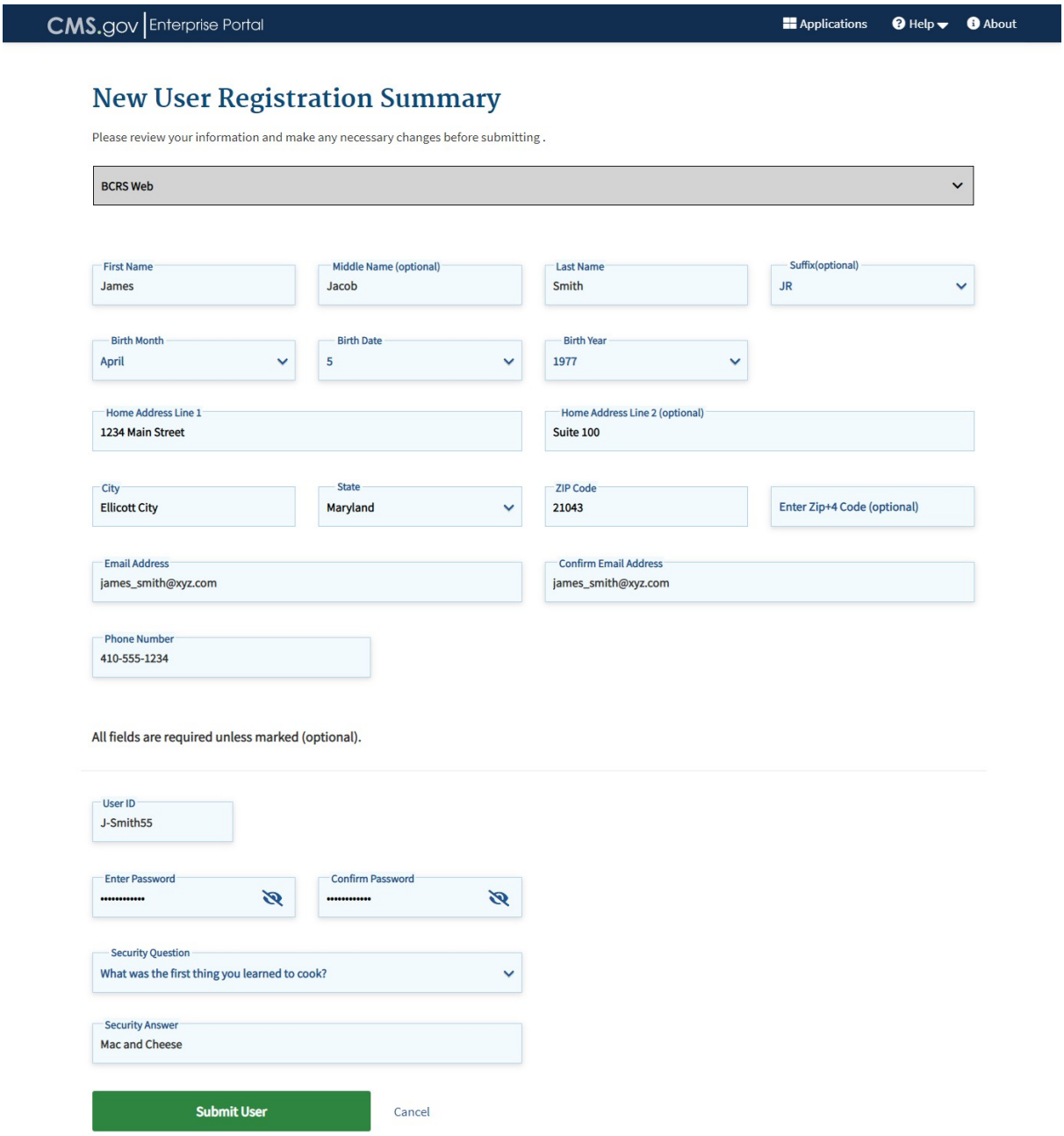

Figure 15: New User Registration – Registration Summary

8. Review the information you entered, make any necessary changes and then click the **Submit User** button.The **Confirmation** page is displayed acknowledging your successful registration and informs you that you should receive a confirmation email, as shown in *Figure 16: New User Registration – Confirmation*.

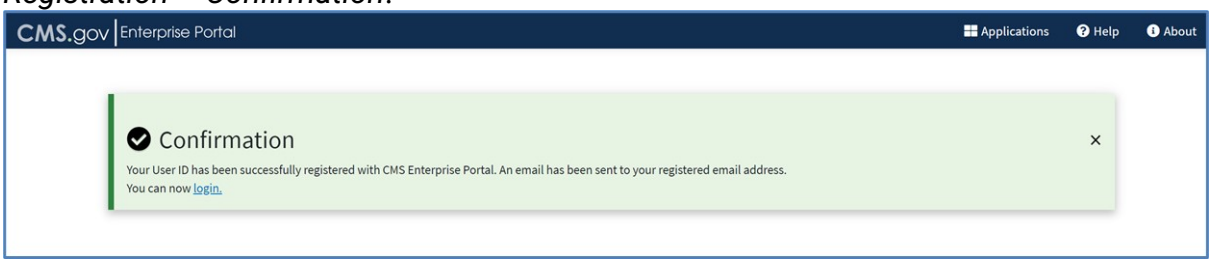

Figure 16: New User Registration – Confirmation

4. Logging In

4.1. User Login Without a Registered MFA Device

The instructions in this section demonstrate the login process for users who do not need to provide a Multi-Factor Authentication (MFA) at login. For more information about MFA, see section *8.6 - Managing Multi-Factor Authentication (MFA)*.

Note

Whether you need to provide an MFA at login will depend on what roles you have.

1. Navigate to the CMS Enterprise Portal public home page, as shown in Figure 17: Login Portlet on CMS Enterprise Portal Public Home Page.

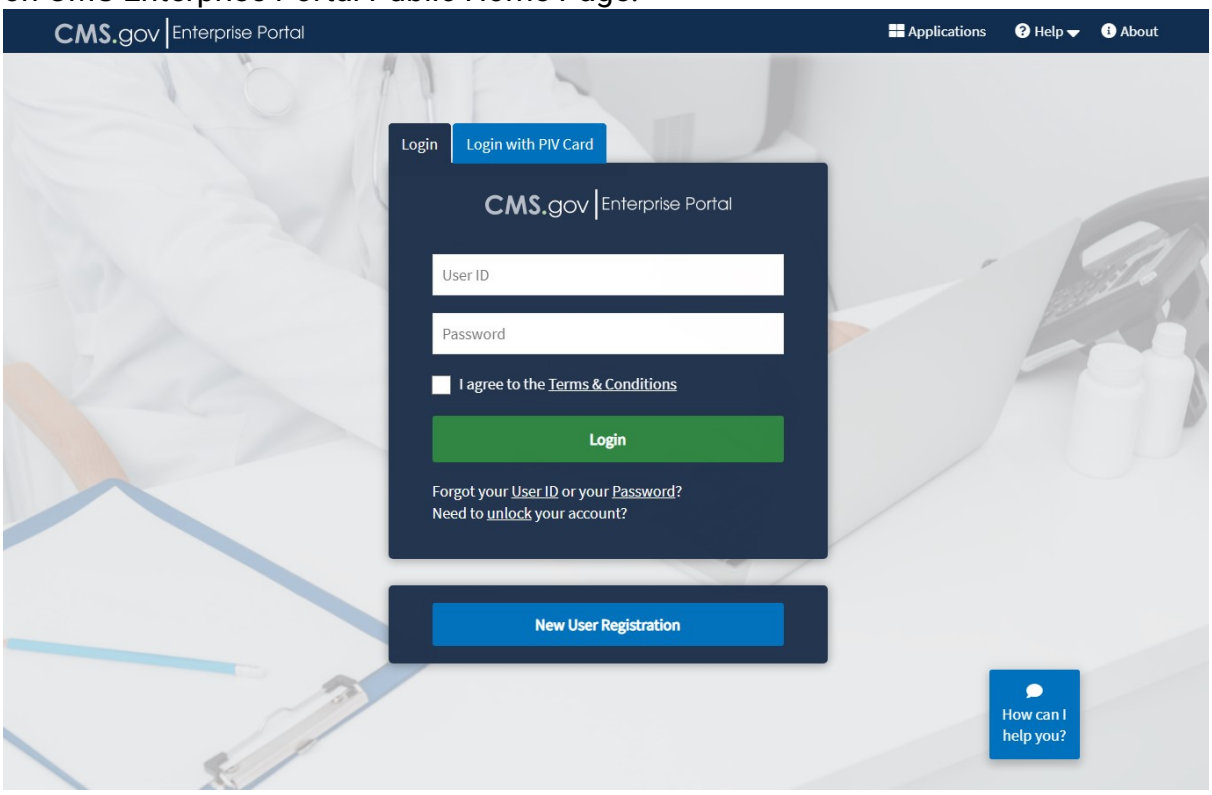

Figure 17: Login Portlet on CMS Enterprise Portal Public Home Page

2. Enter the CMS user ID in the **User ID** field.

3. Enter the CMS password in the **Password** field.

4. Read the important Terms and Conditions information and indicate your agreement by clicking the checkbox. Ensure the checkbox next to **Agree to our Terms & Conditions** remains checked.

5. Click **Login**.

Upon initial login, the CMS Enterprise Portal **My Portal** page is displayed, as shown in *Figure 18: My Portal Page – First Login*.

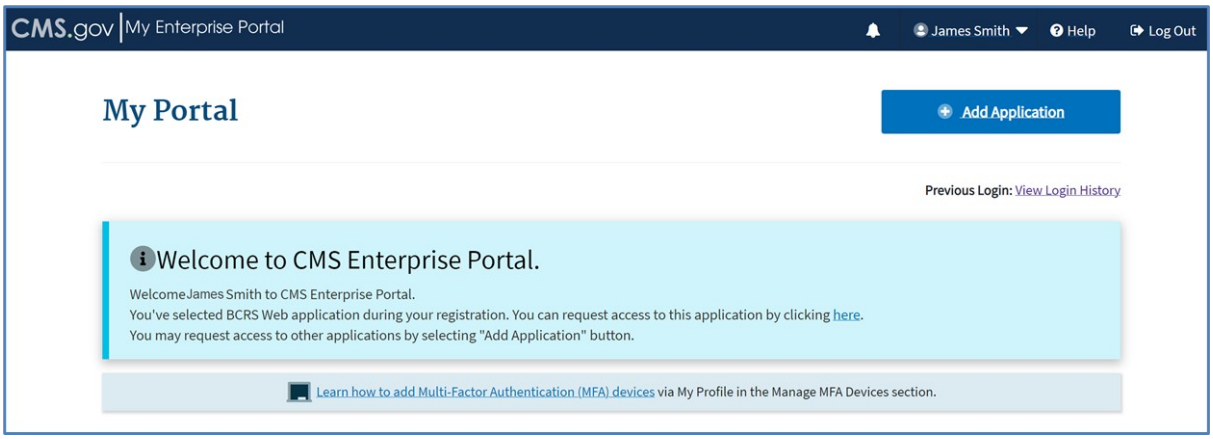

Figure 18: My Portal Page – First Login

The **My Portal** page displays a Welcome message with a link to request access to the application that the user selected during registration. The **Add Application** button, also displayed on the **My Portal** page, allows you to request access (role) to a CMS Enterprise Portal application.

For accounts that already have access to CMS Enterprise Portal provisioned-applications, the **My Portal** page displays one or more tiles (depending on how many CMS applications are associated with your account), as shown in *Figure 19: My Portal Page with Applications*.

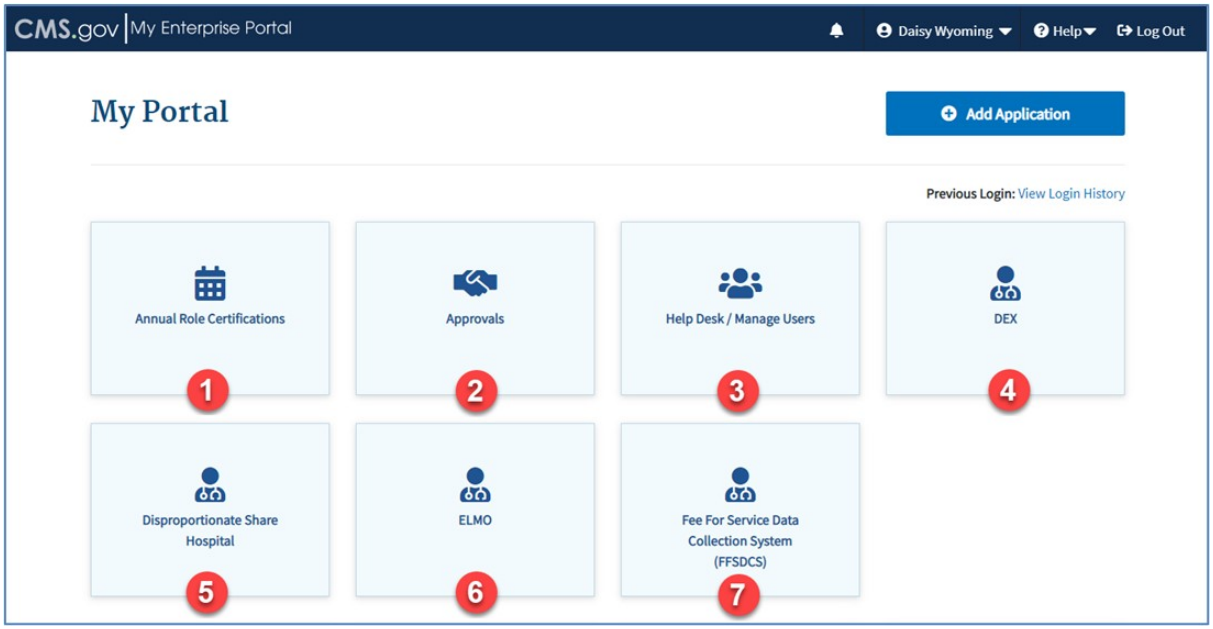

Figure 19: My Portal Page with Applications

The first tile (1) is **Annual Role Certifications**, which is available only to users with an Annual Role Certification related role. Clicking this tile takes you to the **My Annual Role Certifications** page where you can review and certify or revoke roles.

The second tile (2) **Approvals**, which is available only to users with an Approver related role. Clicking this tile takes you to the **My Pending Approvals** page where you can approve or reject role requests.

The third tile (3) is **Help Desk/Manage Users**, which is available only to users with a Help Desk related role. Clicking this tile takes you to the Help Desk/Manage Users page where you can search for a user and perform Help Desk functions.

Note

The details about the Annual Role Certifications, Approvals, and Help Desk/Manage Users functionality is provided in separate user guides.

The next four tiles (4-7) display the CMS applications you have access to.

A single application role may give you access to multiple tiles for that application.

The My Portal Page also provides visibility into an application's status as a round icon on the application tile.

If an application is performing as expected, then the application tile will remain unchanged (i.e., there will not be any colored icon on the tile).

If an application is currently experiencing intermittent issues, then an orange color-coded indicator will be displayed. Some users may experience degraded application performance.

The picture shows an application tile for BCRS application with an orange round icon at the bottom right.

If an application's performance is impacted and preventing users' normal operations, then a red color-coded indicator will be displayed.

The picture shows an application tile for Business Intelligence application with a red round icon at the bottom right.

Users can refresh the My Portal Landing page after approximately 5 minutes to determine if the application status improves. Please contact the tier 1 Help Desk for your application if the color indicator remains the same for more than 10 min.

4.2. User Login Using an MFA Device

4.2.1. First Time Login

The following instructions demonstrate the login process for users who are logging in for the first time and must provide an MFA.

1. Navigate to the CMS Enterprise Portal public home page.

2. Enter the CMS user ID in the **User ID** field

3. Enter the CMS password in the **Password** field.

4. Agree to the terms and conditions and click **Login**.
   You will be asked to select and register an MFA device, as shown in *Figure 20: Login with MFA Device - First Login*.

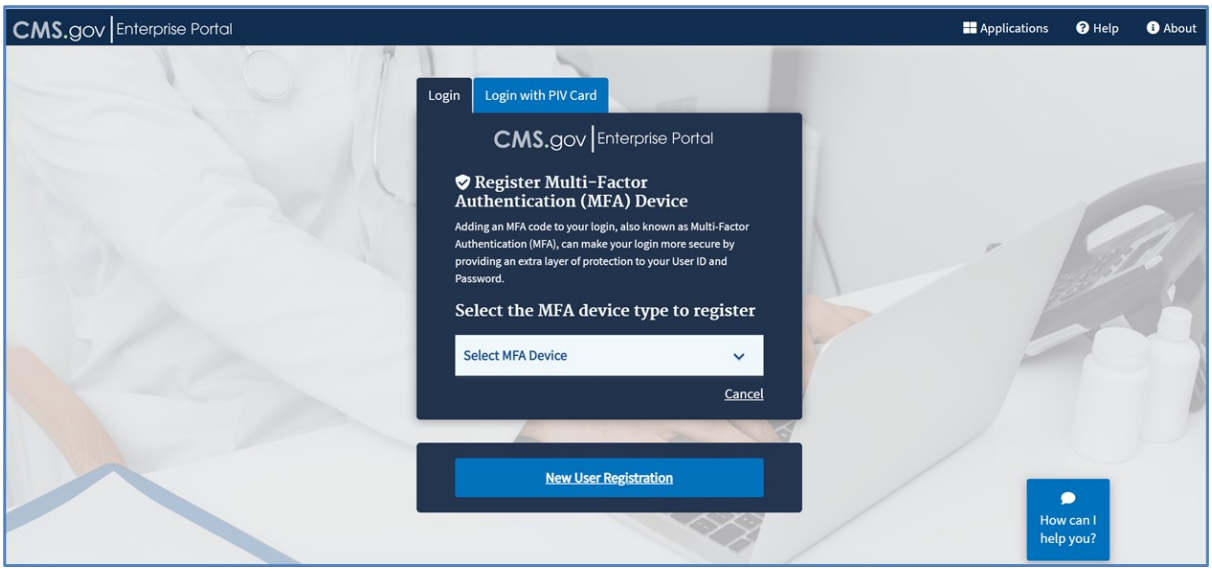

Figure 20: Login with MFA Device - First Login

5. Select an MFA device from the drop-down list, as shown in *Figure 21: Selecting an MFA Device*. For example, select **Email**.

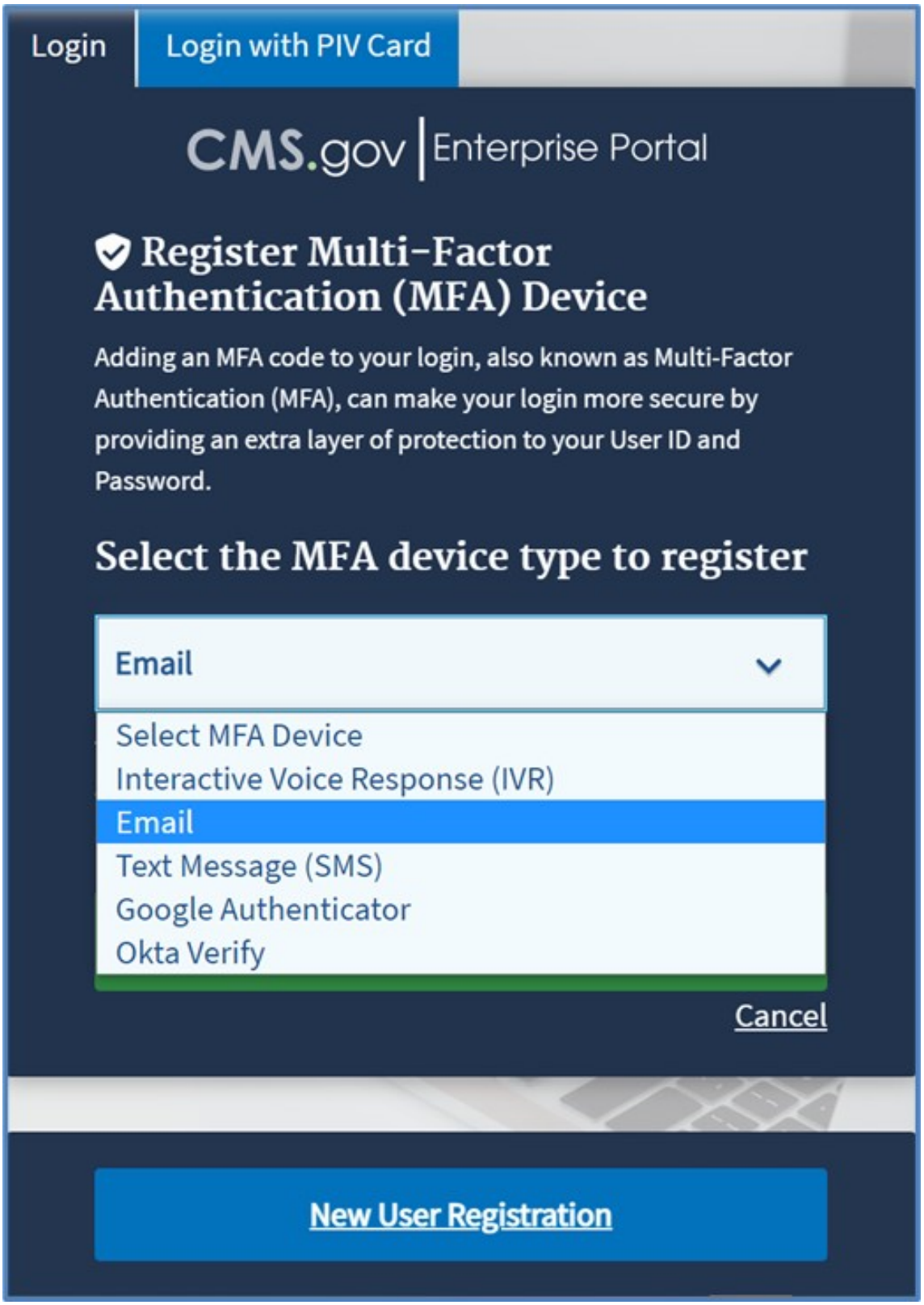

Figure 21: Selecting an MFA Device

6. Click **Send MFA Code**, as shown in *Figure 22: Sending MFA code to the Selected MFA Device*, to have the code emailed to your registered email address.

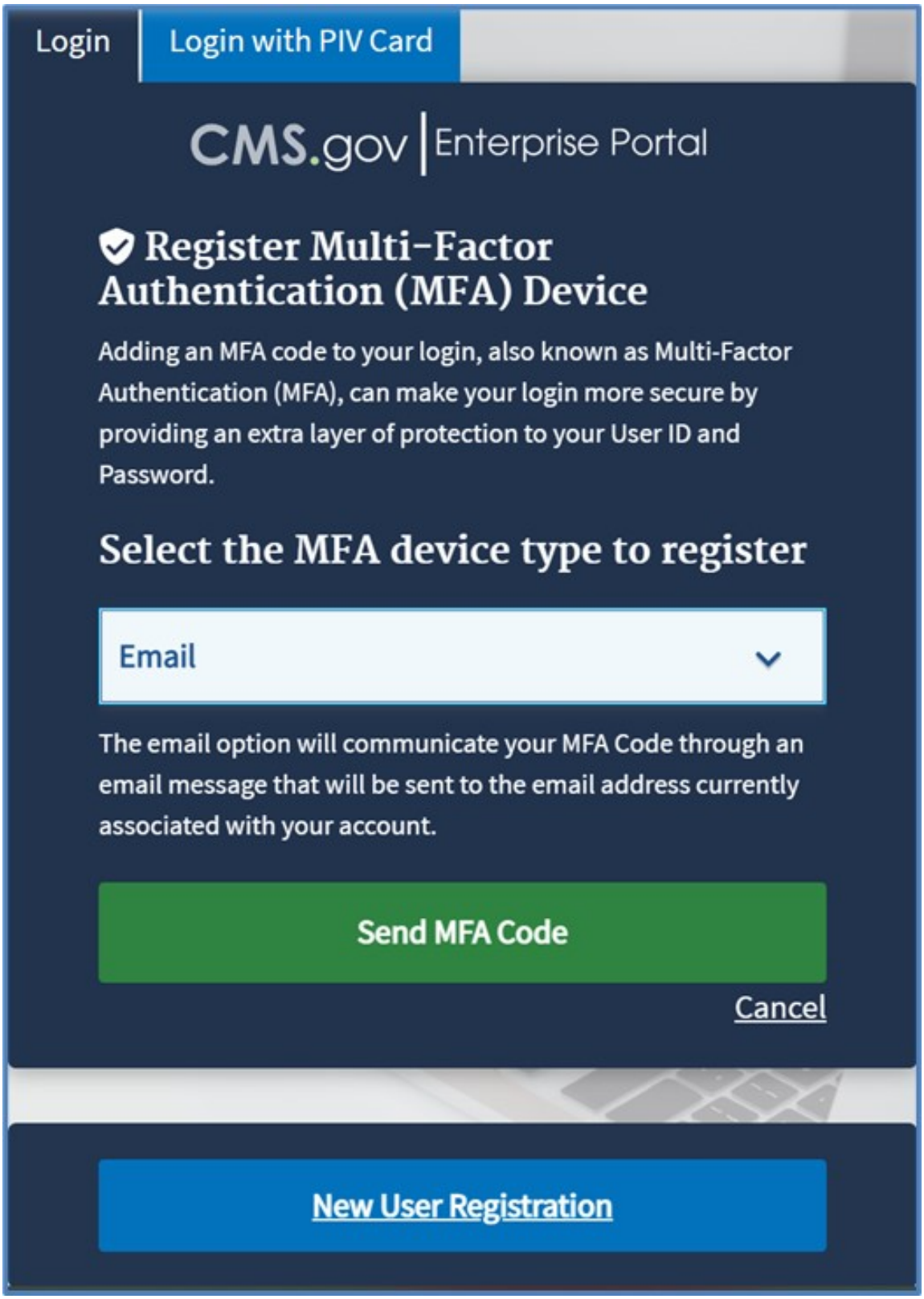

Figure 22: Sending MFA code to the Selected MFA Device

7. Enter the security code from the email and click **Add Device**, as shown in *Figure 23: Entering MFA Code*.

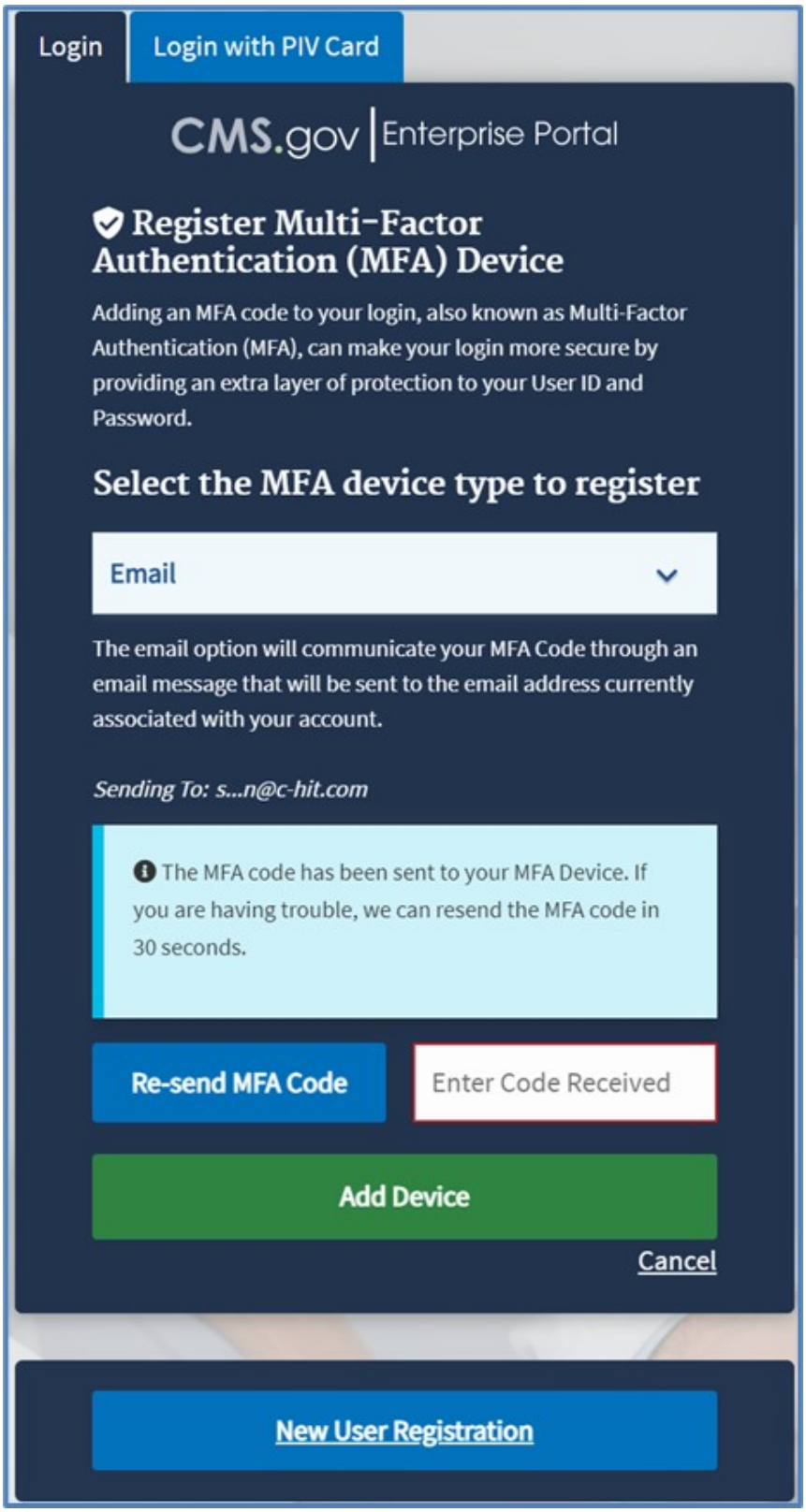

Figure 23: Entering MFA Code

This takes you to your **My Portal** page, as shown in *Figure 18: My Portal Page – First Login*.

4.2.2. Login Using Email MFA Device

The following instructions demonstrate the login process for users who must provide an MFA at login.

Note

Only LOA 3 users are required to login using MFA. All other users (LOA 1 and LOA 2) will login

with just user ID and password.

1. Navigate to the CMS Enterprise Portal public home page.

2. Enter the CMS user ID in the **User ID** field

3. Enter the CMS password in the **Password** field.

4. Agree to the terms and conditions and click **Login**.
   Upon entering a user name that is configured with MFA, an additional Multi-factor Authentication screen is displayed, as shown in *Figure 24: Login with MFA Device*. You will be presented with the MFA Devices that you have previously setup.

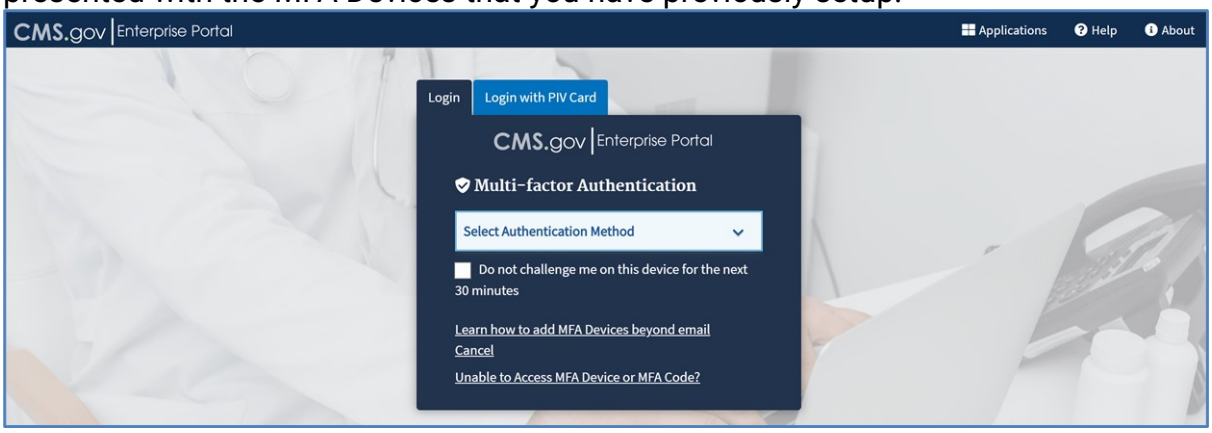

Figure 24: Login with MFA Device

5. Select **Email** as the Authentication Method.
   Additional fields and checkboxes are displayed as shown in *Figure 25: Selecting Email Option as MFA Method*. See the MFA Device options described in the subsections *4.2.2* through *4.2.6*.

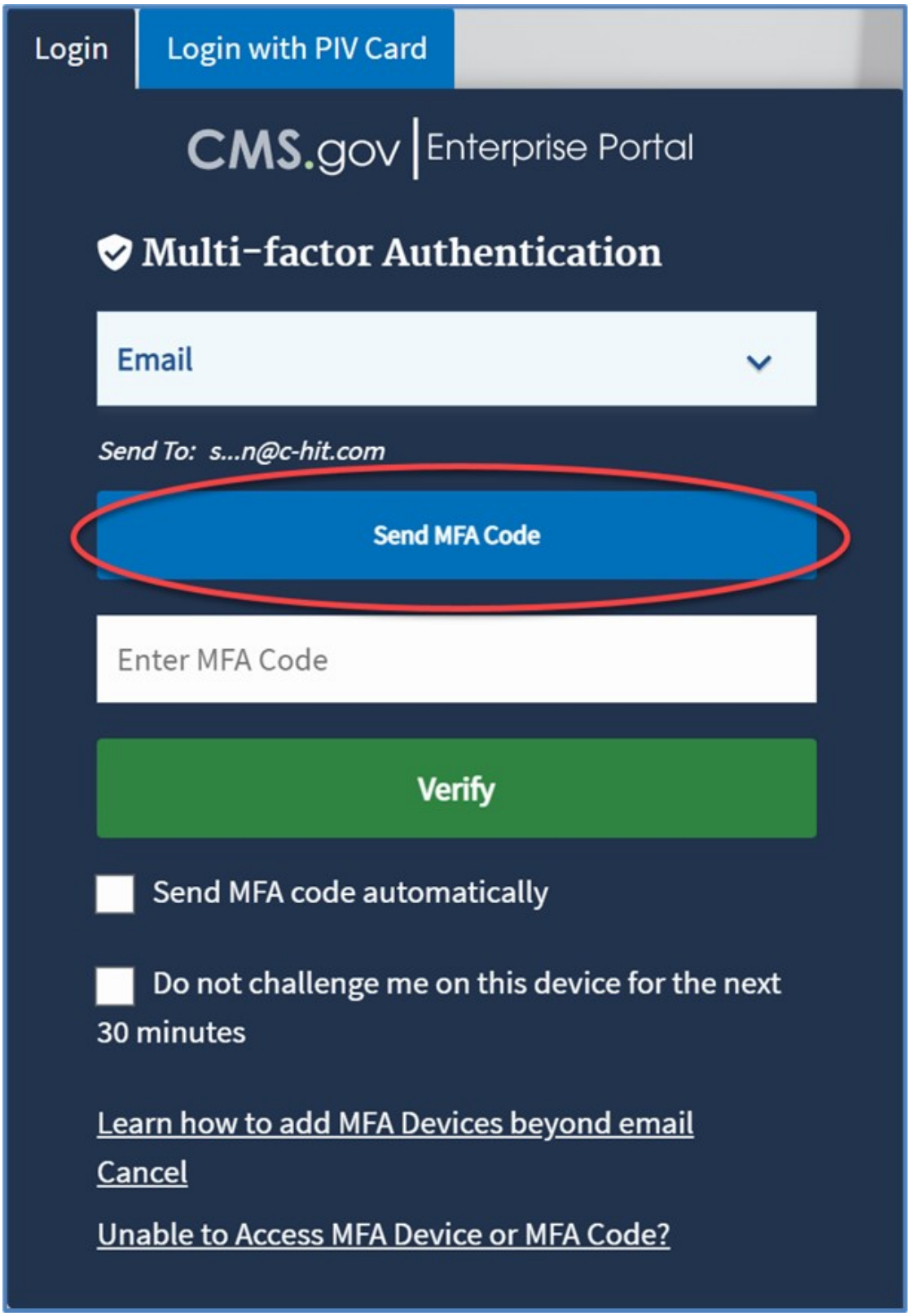

Figure 25: Selecting Email Option as MFA Method

6. Click **Send MFA Code** to have the code emailed to your registered email address.

7. Enter the security code from the email and click **Verify**.
   This takes you to your **My Portal** page, as shown in *Figure 18: My Portal Page – First Login* or *Figure 19: My Portal Page with Applications*.
   If you select Email option as the MFA device and the checkbox for **Send MFA code automatically**, the next time you login into the system using the same MFA, the system will automatically send the MFA code to your registered email address without having to click the "Send MFA Code" button.
   If you select the checkbox for **Do not challenge me on this device for the next 30 minutes**, you

will bypass the MFA verification if you log out and log back into the system again within 30 minutes of your initial login.
Clicking on the **Cancel** link will cancel the MFA verification process and redirect you to the Enterprise Portal home page.
Note

If you enter an incorrect MFA code five times in a row, your account will be locked and you will be directed to the **Unlock My Account** page. See section 7 - *Unlocking Account* (starting at step #3) for details on how to unlock your account.

4.2.3. Login Using Text Message (SMS) MFA Device

1. If you select **Text Message (SMS)**, the Send **MFA Code** button and **Enter MFA Code** fields display, as shown in *Figure 26: Selecting Text Message (SMS) Option as MFA Device*.
2. Click **Send MFA Code** to have the code texted to your registered device.

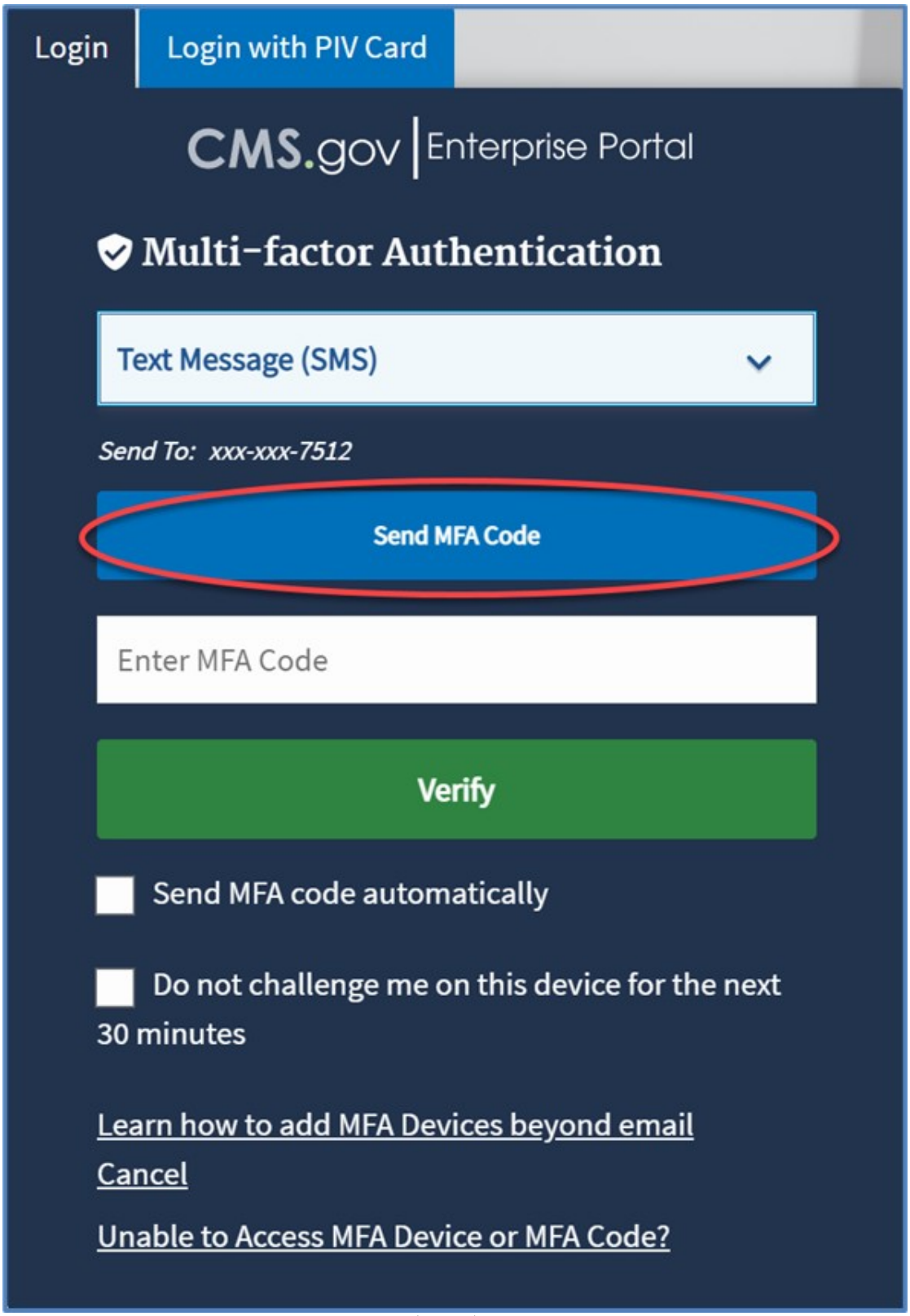

Figure 26: Selecting Text Message (SMS) Option as MFA Device

3. Enter the MFA code from the text message and click **Verify**.
   If you select Text Message (SMS) option as the MFA device and the checkbox for **Send MFA code automatically**, the next time you login into the system using the same MFA, the system will automatically send the MFA code to your registered SMS MFA device without having to click the "Send MFA Code" button.
   If you select the checkbox for **Do not challenge me on this device for the next 30 minutes**, you will bypass the MFA verification if you log out and log back into the system again within 30 minutes of your initial login.
   Clicking on the **Cancel** link will cancel the MFA verification process and redirect you to the Enterprise Portal home page.

Note

If you enter an incorrect MFA code five times in a row, your account will be locked and you will be directed to the **Unlock My Account** page. See section 7 - *Unlocking Account* (starting at step #3) for details on how to unlock your account.

4.2.4. Login Using Interactive Voice Response (IVR) MFA Device

1. If you select **Interactive Voice Response (IVR)**, the **Send MFA Code** button and Enter MFA Code fields display, as shown in *Figure 27: Selecting IVR Option as MFA Device*.
2. Click **Send MFA Code** to have the code provided to you via phone call.

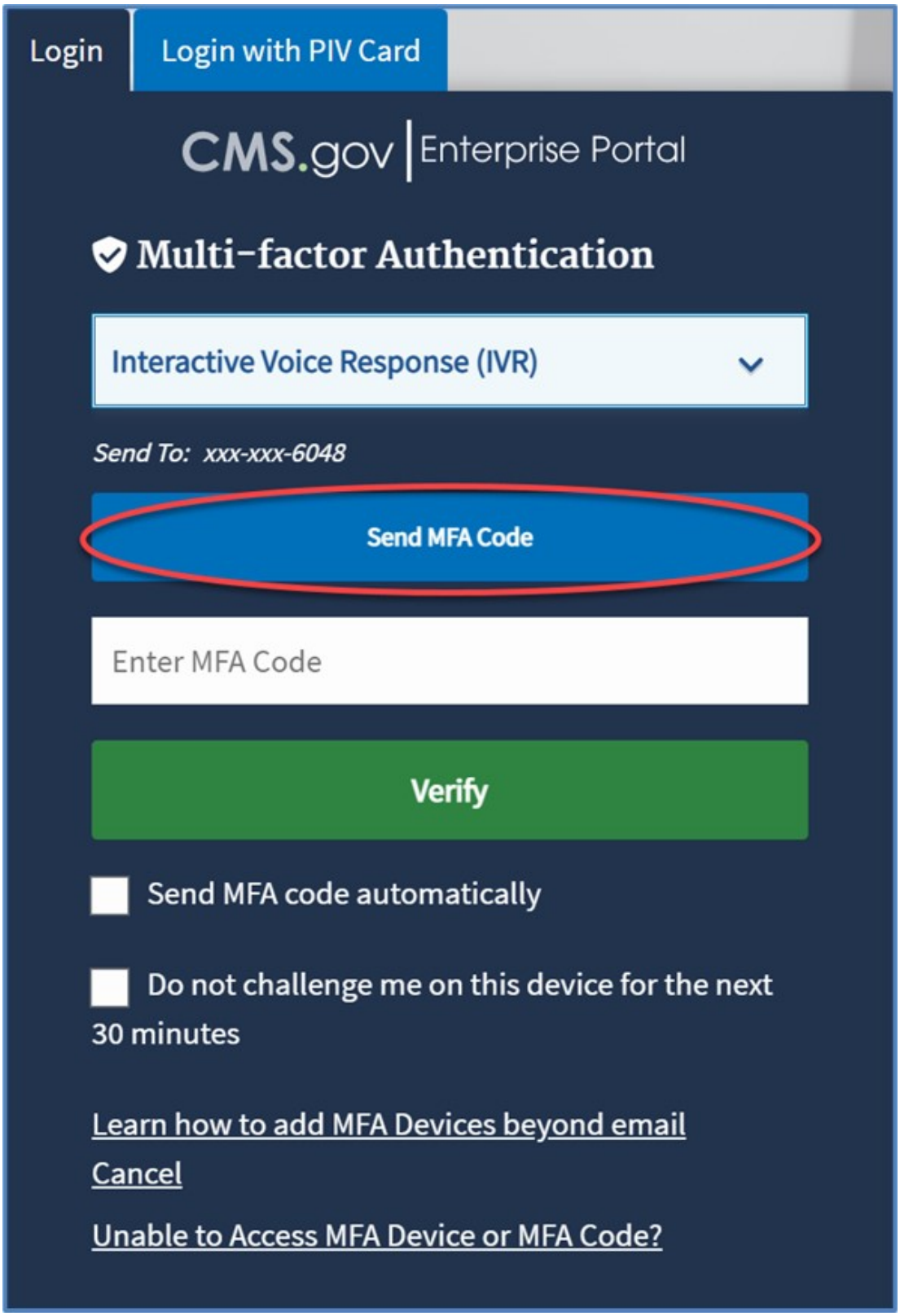

Figure 27: Selecting IVR Option as MFA Device

3. Enter the MFA code from the phone call and click **Verify**.
   If you select Interactive Voice Response (IVR) option as the MFA device and the checkbox for **Send MFA code automatically**, the next time you login into the system using the same MFA, the system will automatically send the MFA code to your registered IVR MFA device without having to click the "Send MFA Code" button.
   If you select the checkbox for **Do not challenge me on this device for the next 30 minutes**, you will bypass the MFA verification if you log out and log back into the system again within 30 minutes of your initial login.
   Clicking on the **Cancel** link will cancel the MFA verification process and redirect you to the Enterprise Portal home page.

Note

If you enter an incorrect MFA code five times in a row, your account will be locked and you will be directed to the **Unlock My Account** page. See section 7 - *Unlocking Account* (starting at step #3) for details on how to unlock your account.

4.2.5. Login Using Google Authenticator MFA Device

1. If you select **Google Authenticator**, the **MFA Code is required** field displays, as shown in *Figure 28: Selecting Google Authenticator Option as MFA Device*.

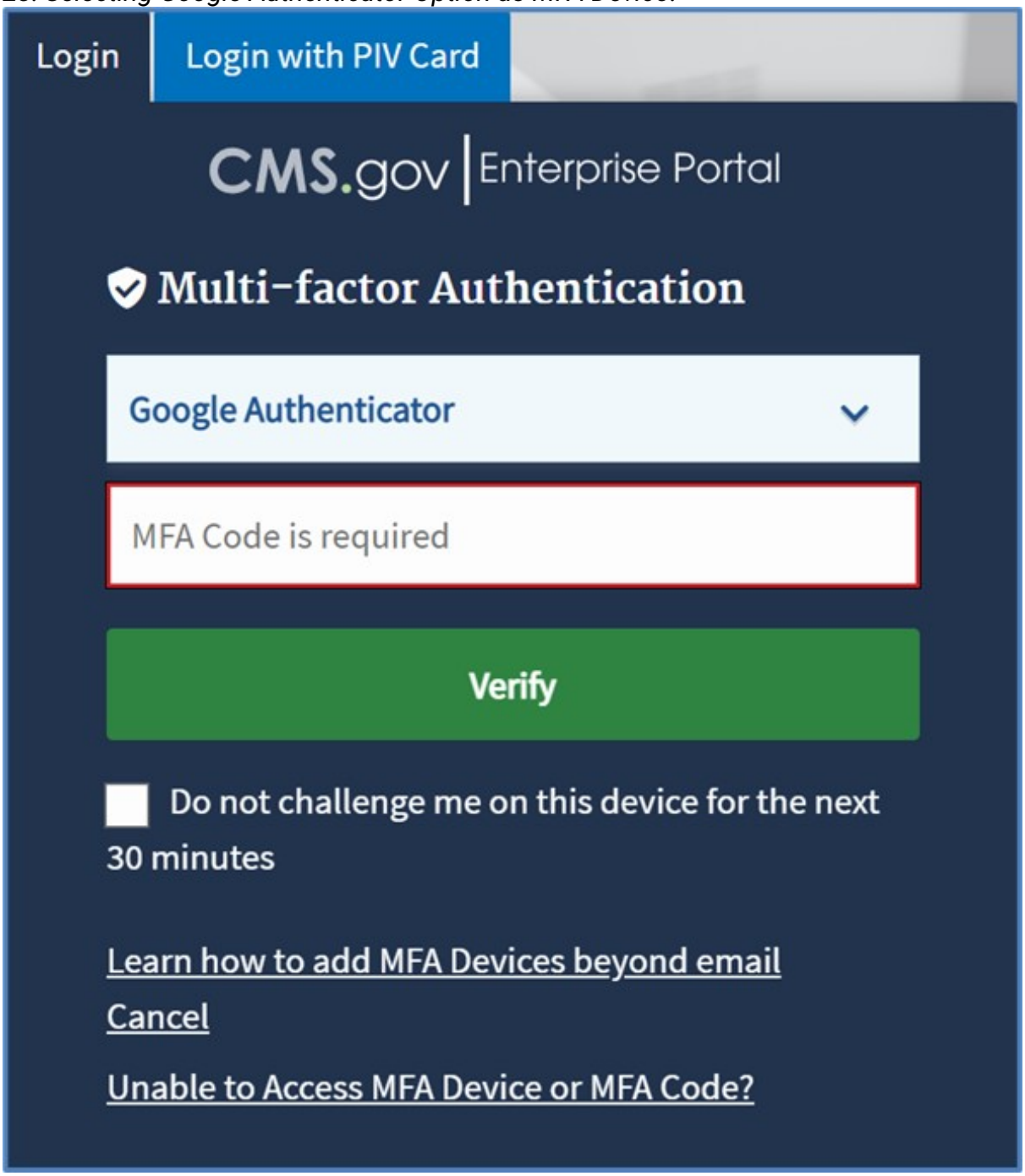

Figure 28: Selecting Google Authenticator Option as MFA Device

2. Open up the Google Authenticator app on your phone.
3. Enter the MFA code displayed in the Google Authenticator app for your account and click **Verify**.
   If you select the checkbox for **Do not challenge me on this device for the next 30 minutes**, you will bypass the MFA verification if you log out and log back into the system again within 30

minutes of your initial login.
Clicking on the **Cancel** link will cancel the MFA verification process and redirect you to the Enterprise Portal home page.

Note

If you enter an incorrect MFA code five times in a row, your account will be locked and you will be directed to the **Unlock My Account** page. See section 7 - *Unlocking Account* (starting at step #3) for details on how to unlock your account.

4.2.6. Login Using Okta Verify MFA Device

1. If you select **Okta Verify**, the **Send Push** button and the **Enter Code Manually link** display, as shown in *Figure 29: Selecting Okta Verify Option as MFA Device*.
Use either Option 1 or Option 2 to log in using Okta Verify.

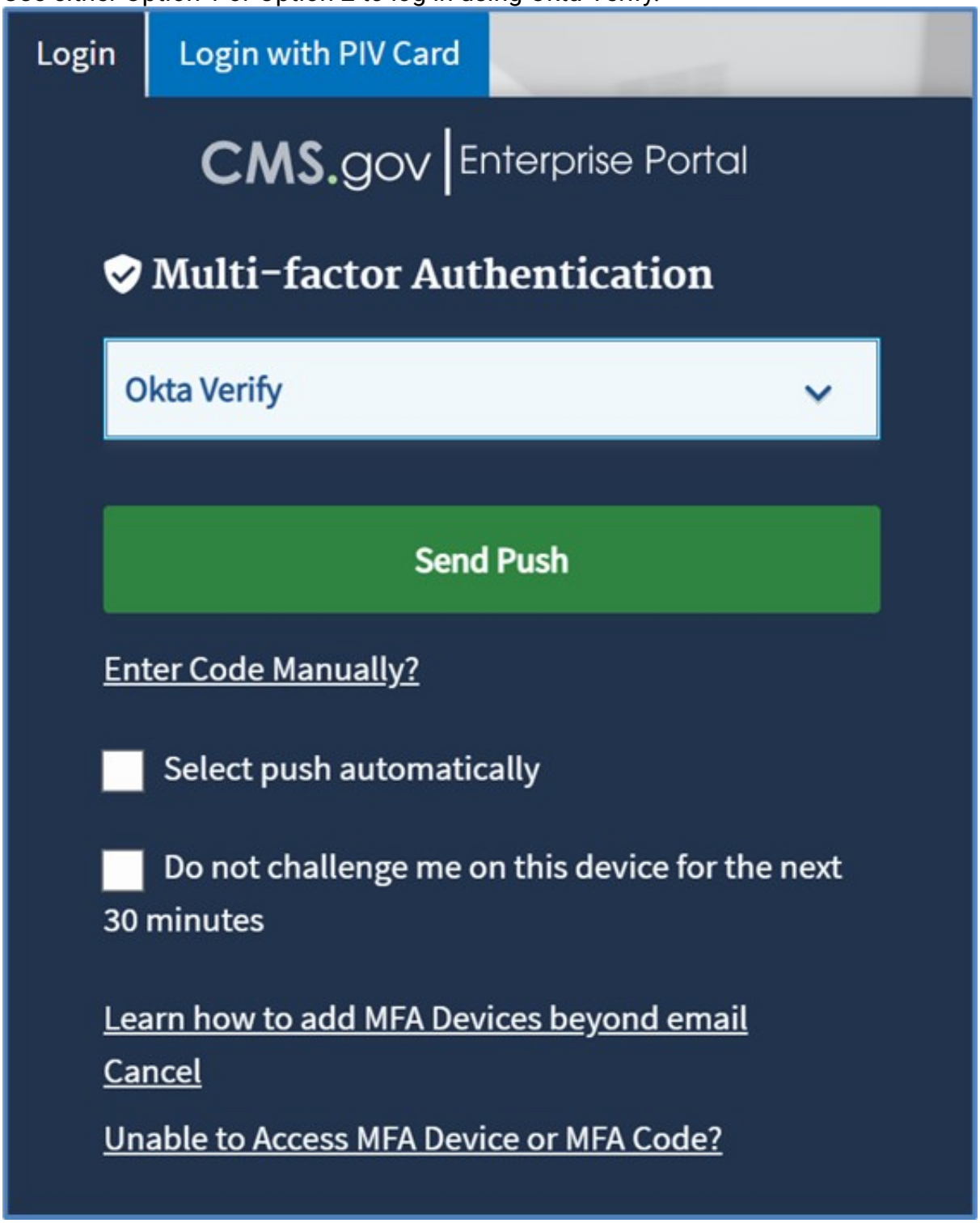

Figure 29: Selecting Okta Verify Option as MFA Device

Option 1: Send Push

- Click the **Send Push** button to send a notification to your smart phone.
- Check your smart phone for a pop-up notification from **Okta Verify**.
- Tap the option to confirm that you are the one signing in.
  If you select the checkbox for **Select push automatically**, the next time you login into the system using the same MFA, the system will automatically send the push notification to your registered smart phone.

Option 2: Enter Code Manually (continue after step 1)

- Click the **Enter Code Manually** link.
  The **MFA Code is required** field displays, as shown in *Figure 30: Okta Verify Option – Enter Code Manually*.

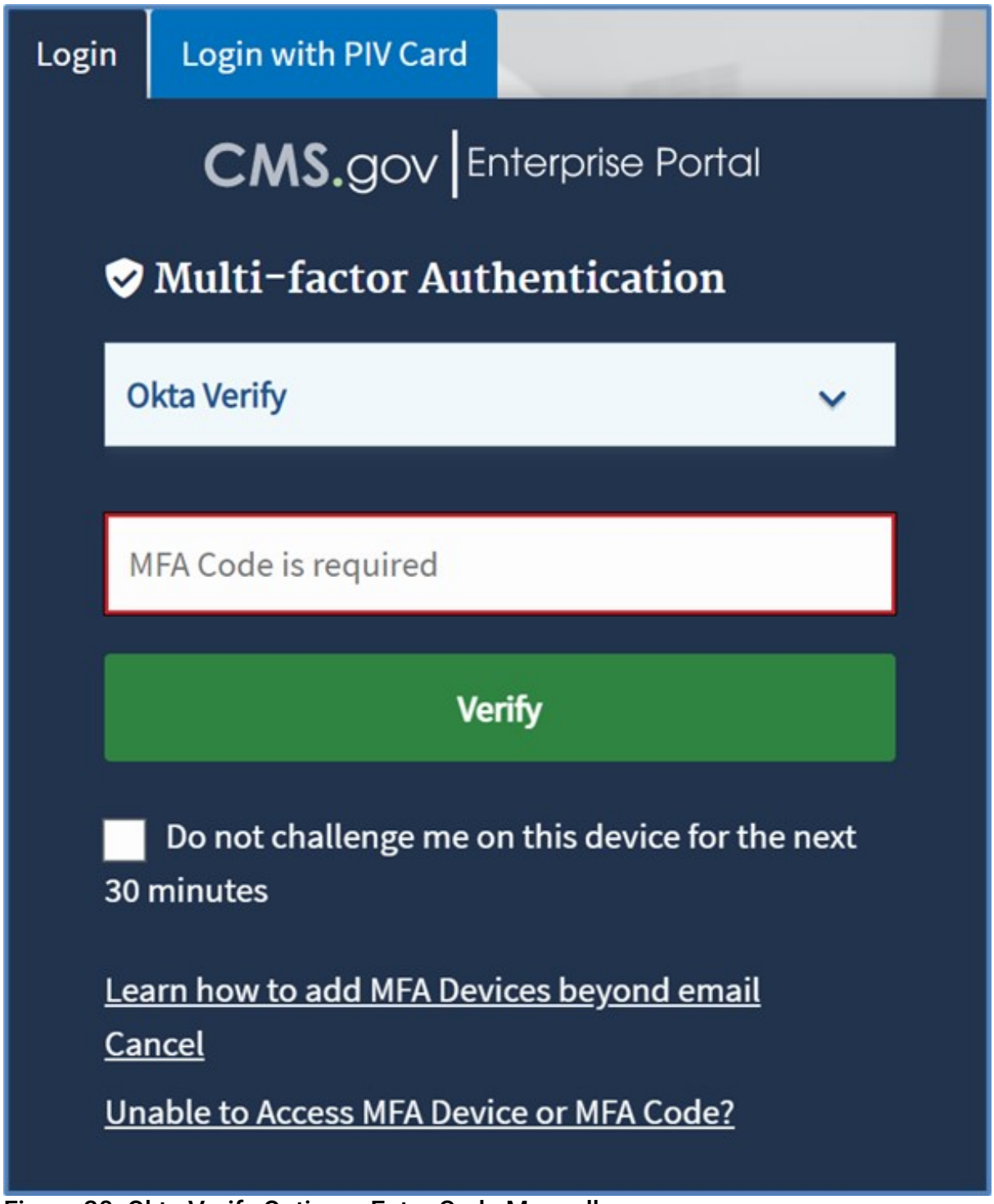

Figure 30: Okta Verify Option – Enter Code Manually

2. Enter the security code from **Okta Verify** and click **Verify**.
If you select the checkbox for **Do not challenge me on this device for the next 30 minutes**, you will bypass the MFA verification if you log out and log back into the system again within 30 minutes of your initial login.
Clicking on the **Cancel** link will cancel the MFA verification process and redirect you to the Enterprise Portal home page.

4.2.7. Login Using YubiKey MFA Device

1. If you select **YubiKey**, the Code field displays, as shown in *Figure 31: Selecting YubiKey Option as MFA Device*.

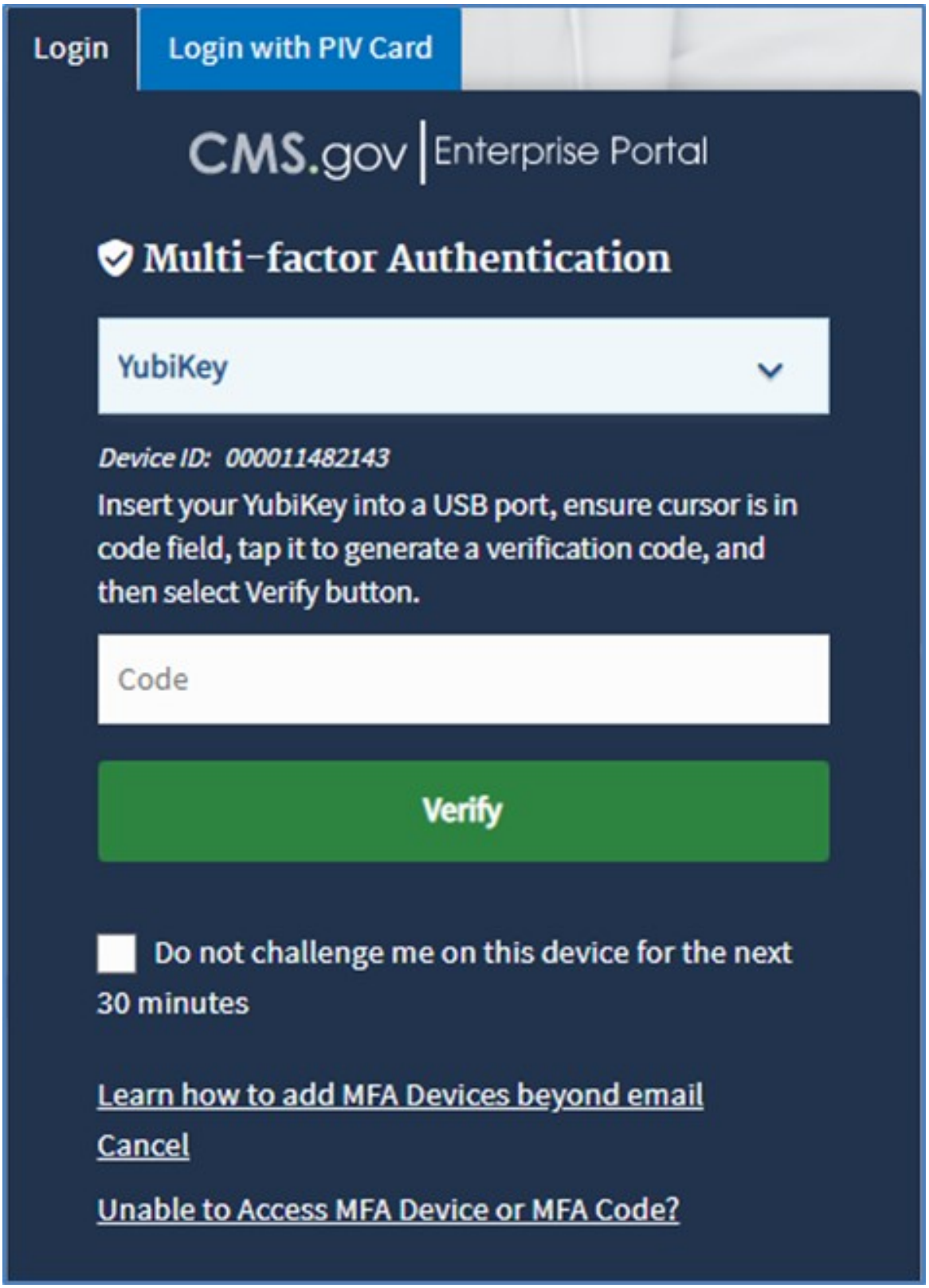

Figure 31: Selecting YubiKey Option as MFA Device

2. Follow the instructions on the screen to generate a security code.
   The **Code** field is populated with the security code, which is masked by dots, as shown in *Figure 32: Code Field Populated with Security Code*.

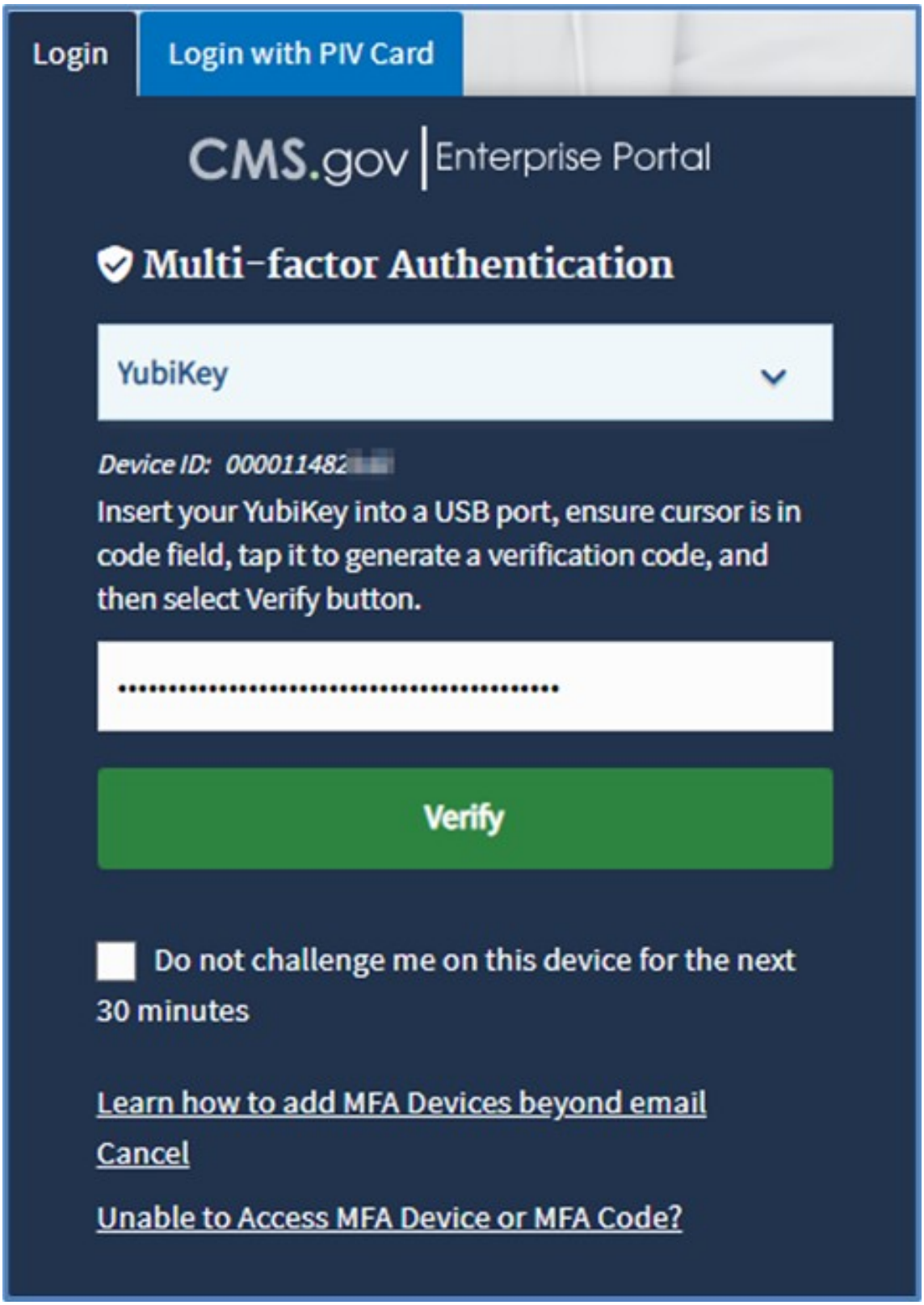

Figure 32: Code Field Populated with Security Code

3. Click **Verify**.
   If you select the checkbox for **Do not challenge me on this device for the next 30 minutes**, you will bypass the MFA verification if you log out and log back into the system again within 30 minutes of your initial login.
   Clicking on the **Cancel** link will cancel the MFA verification process and redirect you to the Enterprise Portal home page.

4.3. User Login Using a PIV Card

If you have an active EUA user account and a Personal Identity Verification (PIV) card, you can use that PIV card to log in to CMS Enterprise Portal. PIV credentials are U.S. Federal government credentials that are used to access Federal government controlled facilities and information systems as assigned.

Note

Before logging in with your PIV card, you must first log in to CMS Enterprise Portal one time with your EUA user ID/password. After the first successful log in with an EUA user ID/password via the regular Login portlet of the Enterprise Portal home page, you can subsequently log in with your PIV card.

The following instructions demonstrate the login process for EUA users who have an active PIV card.

1. Navigate to the CMS Enterprise Portal public home page.
2. Click the **Login with PIV Card** tab, as shown in Figure 33: Selecting Login with PIV Card Tab on Enterprise Portal Home Page.

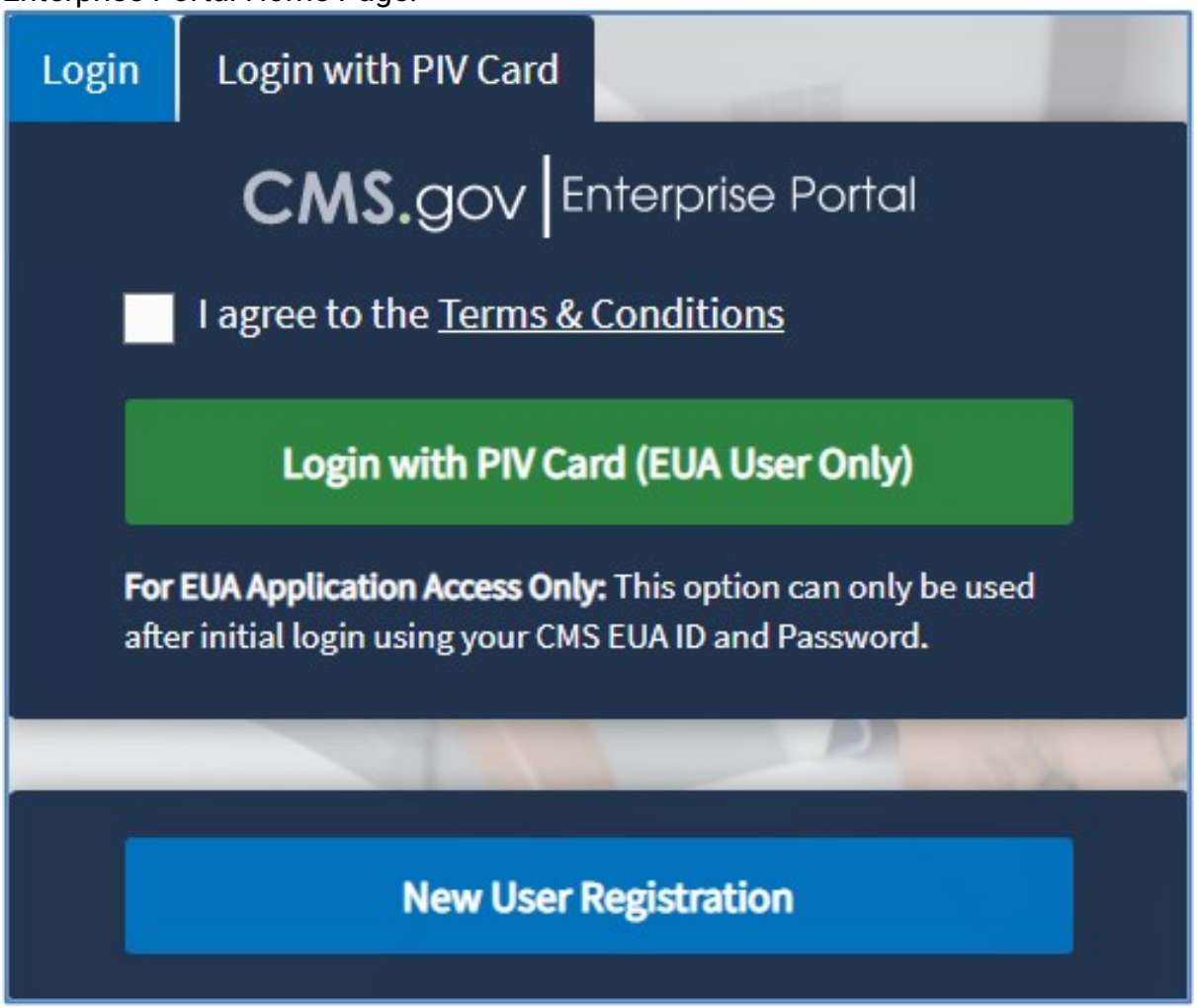

Figure 34: Login with PIV Card Tab Portlet

3. Agree to the terms and conditions and then click the **Login with PIV Card (EUA User Only)** button, as shown in Figure 34: Login with PIV Card Tab Portlet.
4. Follow the instructions on the screen to select a certificate (if applicable).
5. Follow the instructions to enter your Personal Identification Number (PIN).

Note

The Login with PIV Card feature is not available using the Firefox browser.

4.4. Troubleshooting Login with PIV

4.4.1. Login with PIV as First Time User or with Newly Assigned PIV Card

If you have a newly assigned PIV card, or login into Portal environment for the first time then:

1. Login to CMS Enterprise Portal using your EUA user ID and password, and

2. Use your PIV card to login to Enterprise Portal.

4.4.2. Login with PIV when Wrong Certificate is Selected

If you have selected the incorrect certificate and you see a certificate validation failed error message (as shown on *Figure 35: Login with PIV Error – Certification Validation Failed*), then close your browser (all the tabs), restart browser, and try again. Look for a certificate with an issuer of "HHS-FPKI-Intermediate-CA-E1".

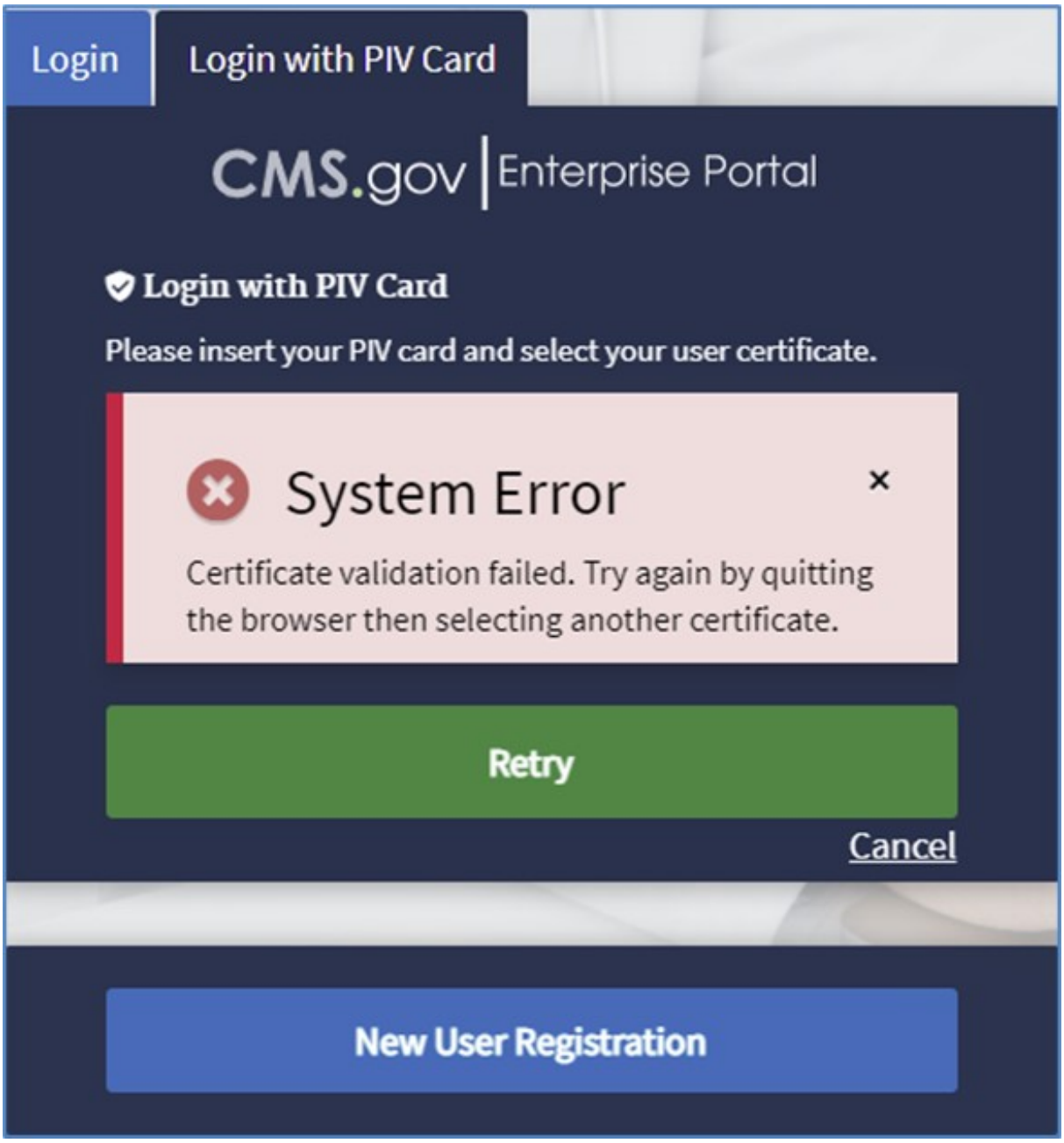

Figure 35: Login with PIV Error – Certification Validation Failed

4.4.3. Login with PIV when Incorrect PIN is Entered

If you mistyped your PIN, please try again. If you continue to get the error try to close the browser and open again to retry.

If you forgot your PIN, then your PIN can be reset by following CMS guidelines.

4.4.4. Login with PIV when PIV Card has Expired

If you try to login to CMS Enterprise Portal with your PIV card and your PIV card digital certificate has expired, then you will need to renew your certificate by following CMS guidelines.

4.4.5. Login with PIV when Multiple Versions of PIV Certificates are Available

If you are seeing multiple versions of your PIV certificates to choose from, then:

1. Remove your PIV card from reader,

2. Erase all available PIV certificates from the browser security settings, and

3. Put your PIV card back in your card reader to recreate the certificate.

4.4.6. Login with PIV and Dialog for Certificates is Not Showing

If you have clicked on the **Login with PIV Card (EUA User Only)** button and you do not see the PIV dialog for selecting a certificate (as shown in *Figure 36: Login with PIV Dialog Certificates*), then look to see if the dialog is on your primary monitor or is hidden behind another window. If you still cannot find the dialog, then close your browser, restart browser, and try again. If you are still having issues, try using a different supported browser or contact your IT helpdesk to check if company security policies is blocking the PIV certificate dialog to be displayed.

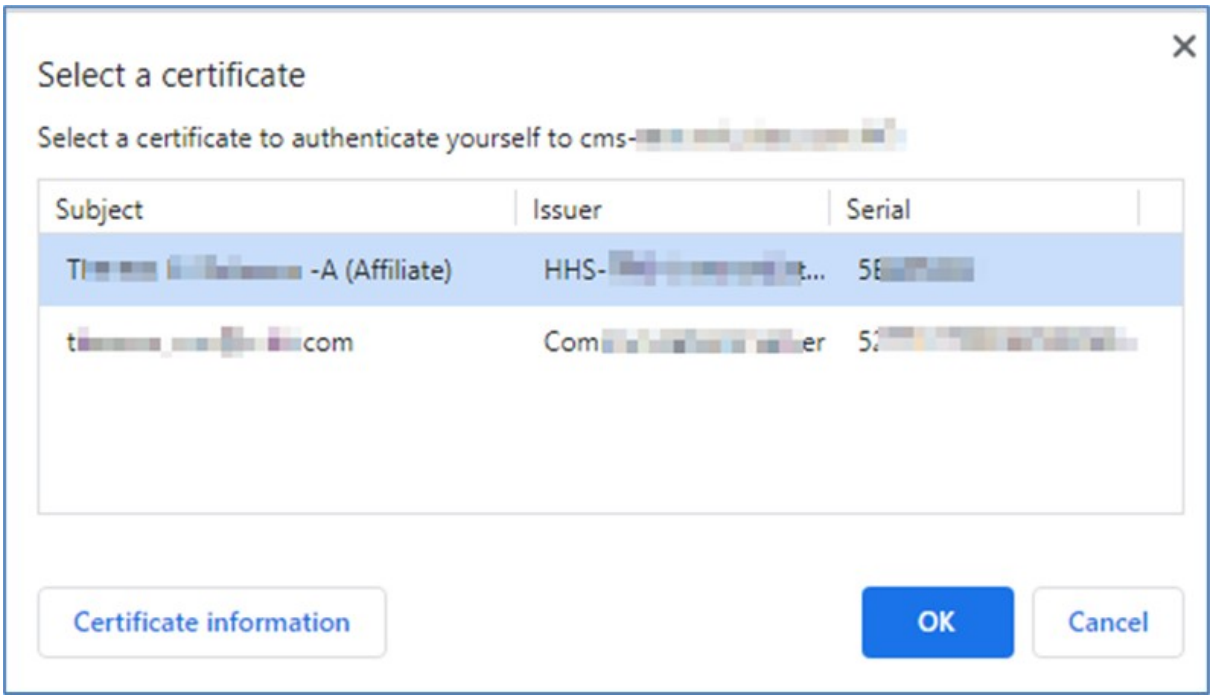

Figure 36: Login with PIV Dialog Certificates

5. Forgot User ID

The instructions in this section demonstrate the 'Forgot User ID' process for users who do not remember their registered CMS Enterprise Portal-related user ID to login.

1. Navigate to the CMS Enterprise Portal public home page, and click the **User ID** link, as shown in Figure 37: Forgot User ID Link.

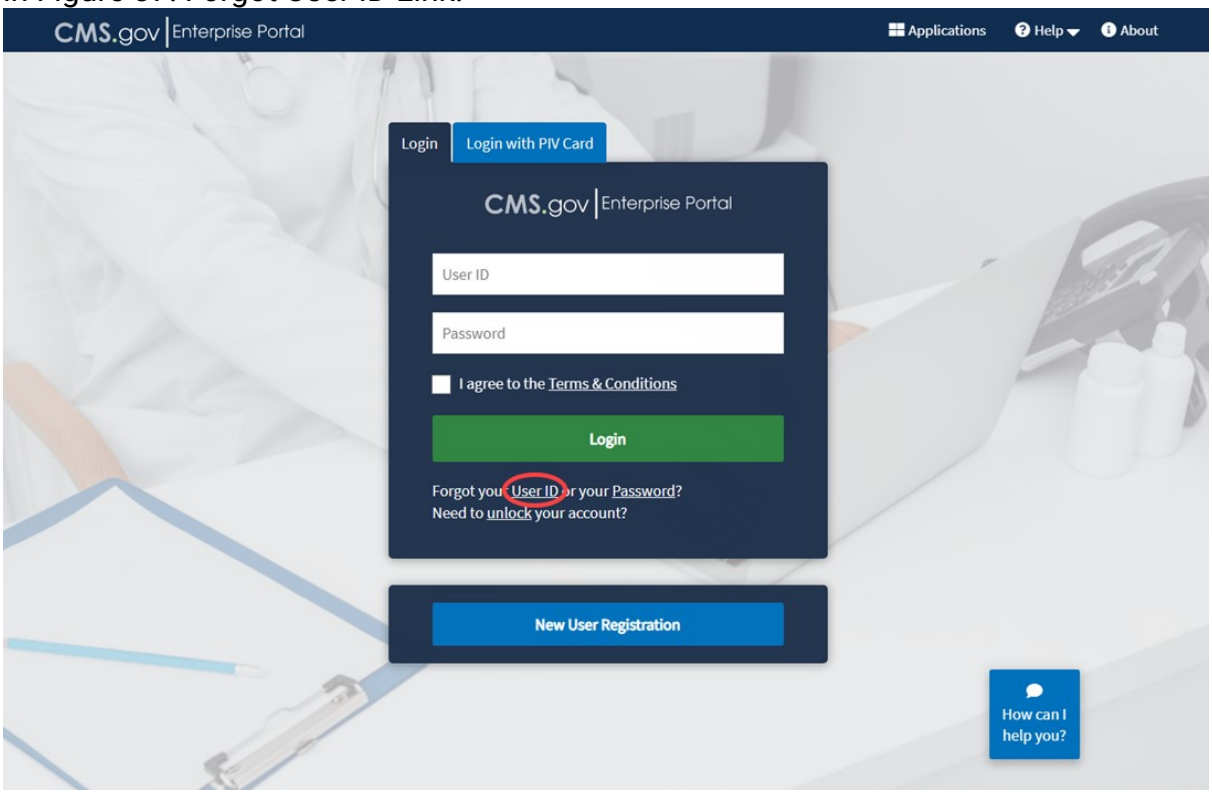

Figure 37: Forgot User ID Link

2. Enter the information shown in Figure 38: Forgot User ID – Blank Page and click **Submit**.

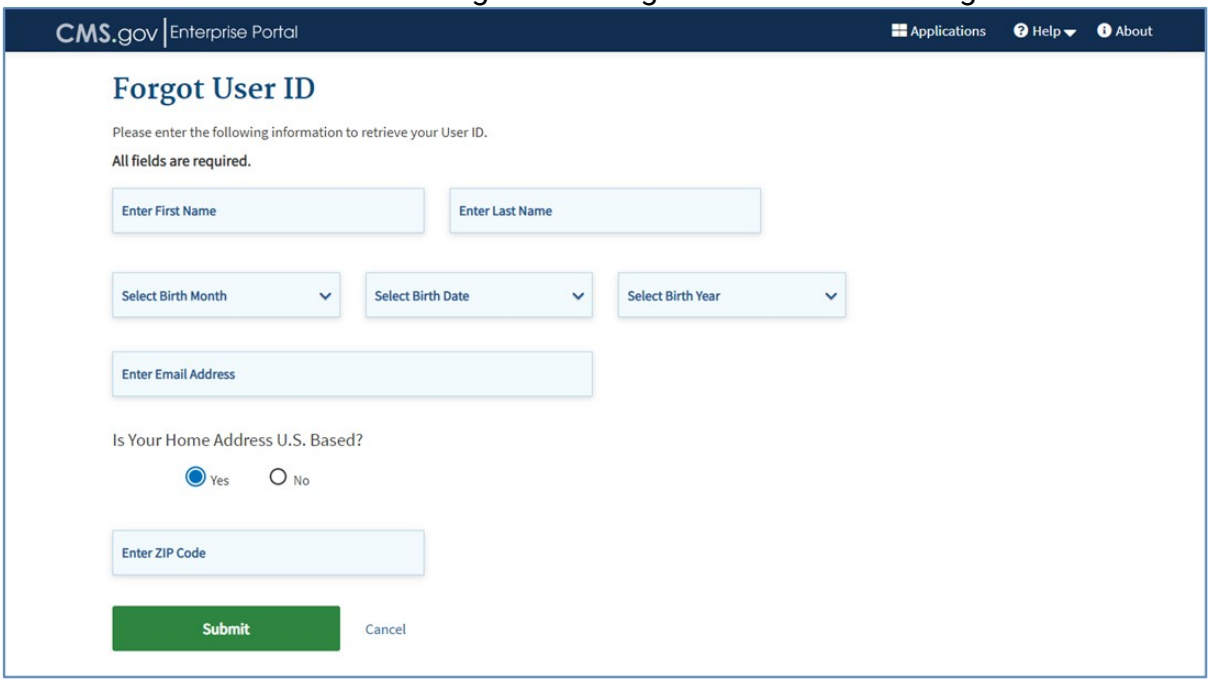

Figure 38: Forgot User ID – Blank Page

Note

A message will display if invalid data is entered, as shown in *Figure 39: Forgot User ID – Invalid Data Error*. For security reasons, this is the same message that is displayed if you enter the correct information. No email will be sent out if the information is not correct. You must re-enter the correct information and submit again.

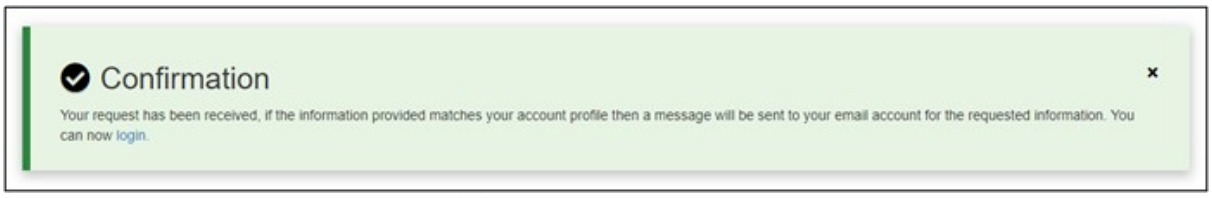

Figure 39: Forgot User ID – Invalid Data Error

3. After successfully submitting your information, you will receive confirmation that your information has been successfully verified, as shown in *Figure 40: Forgot User ID – Successful Confirmation*.

   Note

   If you have entered the information correctly, you will receive an email notification that will contain your User ID. This email will be sent to the email address on your profile.

4. Click the link in the confirmation message, as shown in *Figure 40: Forgot User ID – Successful Confirmation*, to login with your user ID (retrieve from the email notification).

6. Forgot Password

These instructions demonstrate the 'Forgot Password' process for users who do not remember their registered user password to login.

1. Navigate to the CMS Enterprise Portal public home page, and click the **Password** link, as shown in *Figure 41: Forgot Password Link*.

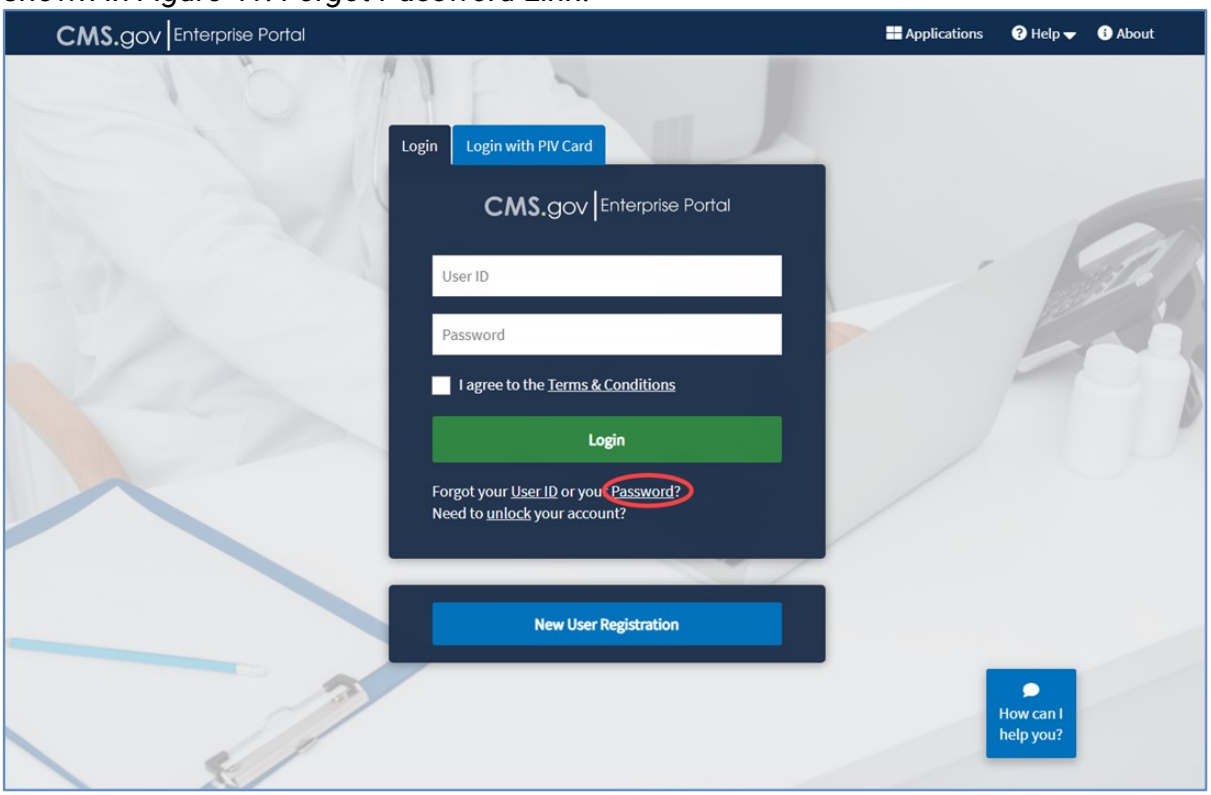

Figure 41: Forgot Password Link

2. Enter your user ID and click **Next**, as shown in *Figure 42: Forgot/Reset Password – Enter User ID*.

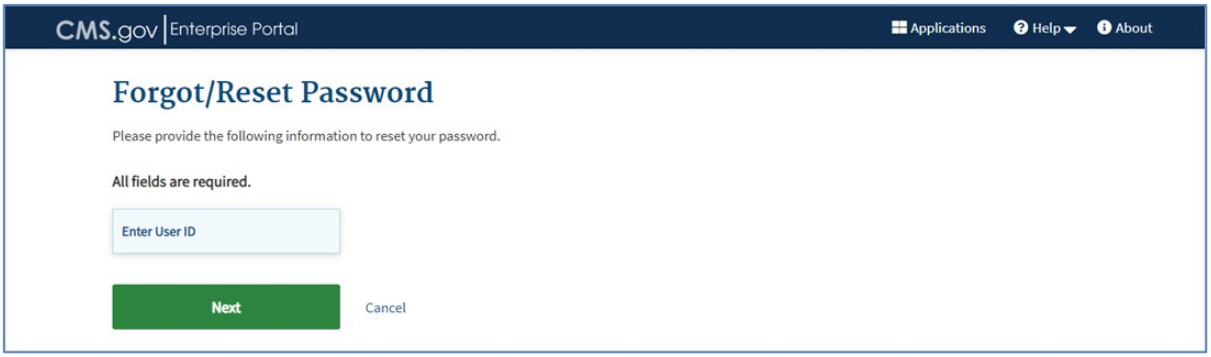

Figure 42: Forgot/Reset Password – Enter User ID

Note

An error is displayed if invalid data is entered, as shown in *Figure 43: Invalid Data Error Message*. You must re-enter the correct information and click Next.

Figure 43: Invalid Data Error Message

3. Choose **Email** as the recovery method from the drop-down menu and click Send Recovery Email, as shown in Figure 44: Forgot/Reset Password – Select Recovery Method. You may also choose SMS or IVR as the recovery method if those MFA devices have been registered previously.

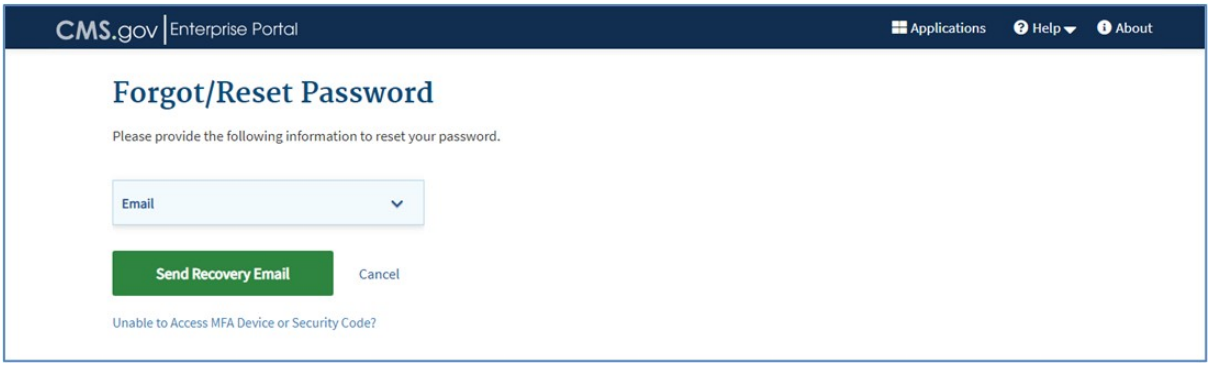

Figure 44: Forgot/Reset Password – Select Recovery Method

Note

If you do not have access to your email, then contact your Application Help Desk to have your email address updated or to request reset of your password. The Help Desk contact information can be found on the CMS Enterprise Portal public page by going to the **Learn About Your Application** drop-down box and selecting your application.

A confirmation message is displayed, as shown in Figure 45: Forgot/Reset Password – Confirmation of Message Delivery.

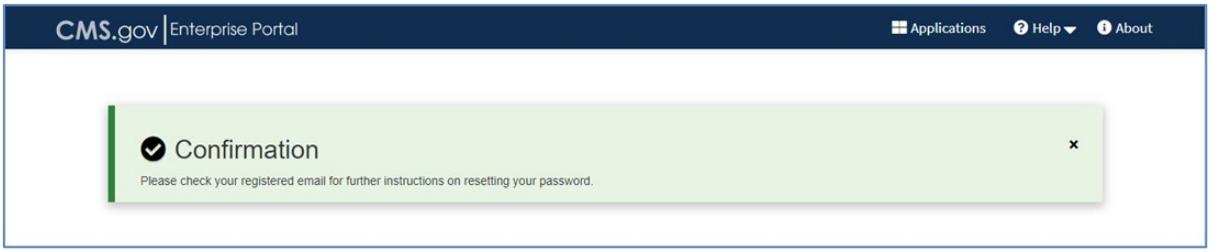

Figure 45: Forgot/Reset Password – Confirmation of Message Delivery

Note

You will receive an email on your registered email address with a link to reset your password.

4. Click on the link provided in the email to reset your password.
5. Answer the security question and click **Submit**, as shown in Figure 46: Forgot/Reset Password – Enter Security Answer.

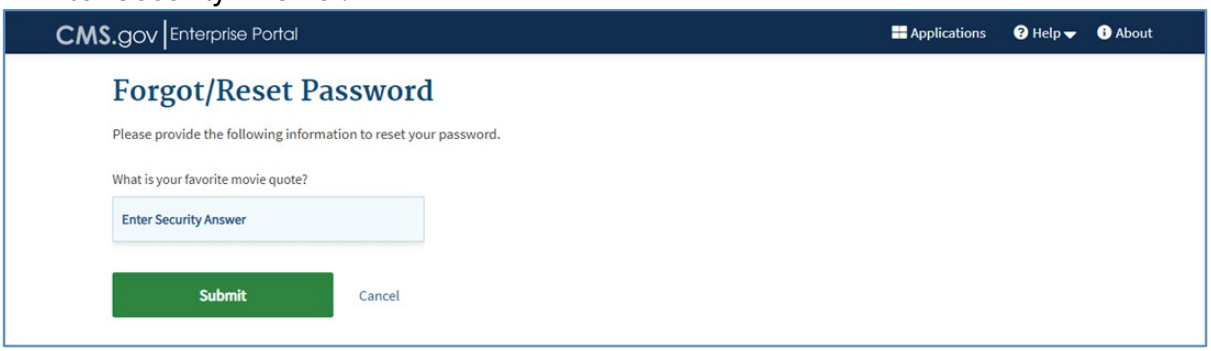

Figure 46: Forgot/Reset Password – Enter Security Answer

Note

An error will display if invalid data is entered, as shown in Figure 47: Invalid Data Error. You must re-enter the correct information and click **Submit**.

Figure 47: Invalid Data Error

6. Enter a new password in the **New Password** field and again in the **Confirm Password** field, as shown in Figure 48: Forgot/Reset Password – Enter New Password. Then, click **Reset Password**.

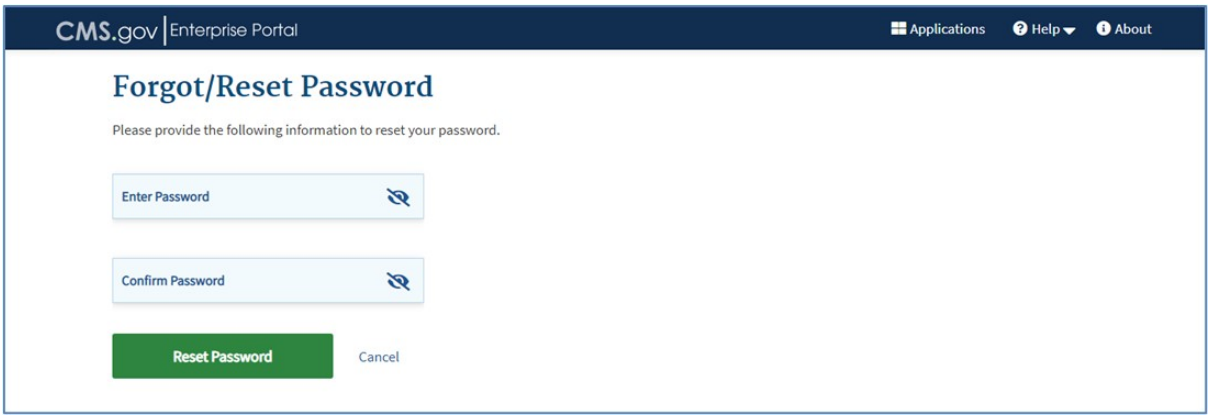

Figure 48: Forgot/Reset Password – Enter New Password

7. After successfully submitting your information, you will receive confirmation that your password has been reset successfully, as shown in Figure 49: Forgot/Reset Password – Successful Confirmation.

   Note

   You will receive an email notification indicating that you successfully changed your password.

7. Unlocking Account

These instructions demonstrate the 'Unlock Account' process for users who lock themselves out during login after multiple failed login attempts.

1. Each time you enter an incorrect combination of user ID and password, an error occurs, as shown in *Figure 50: Incorrect Credentials Error Message*.

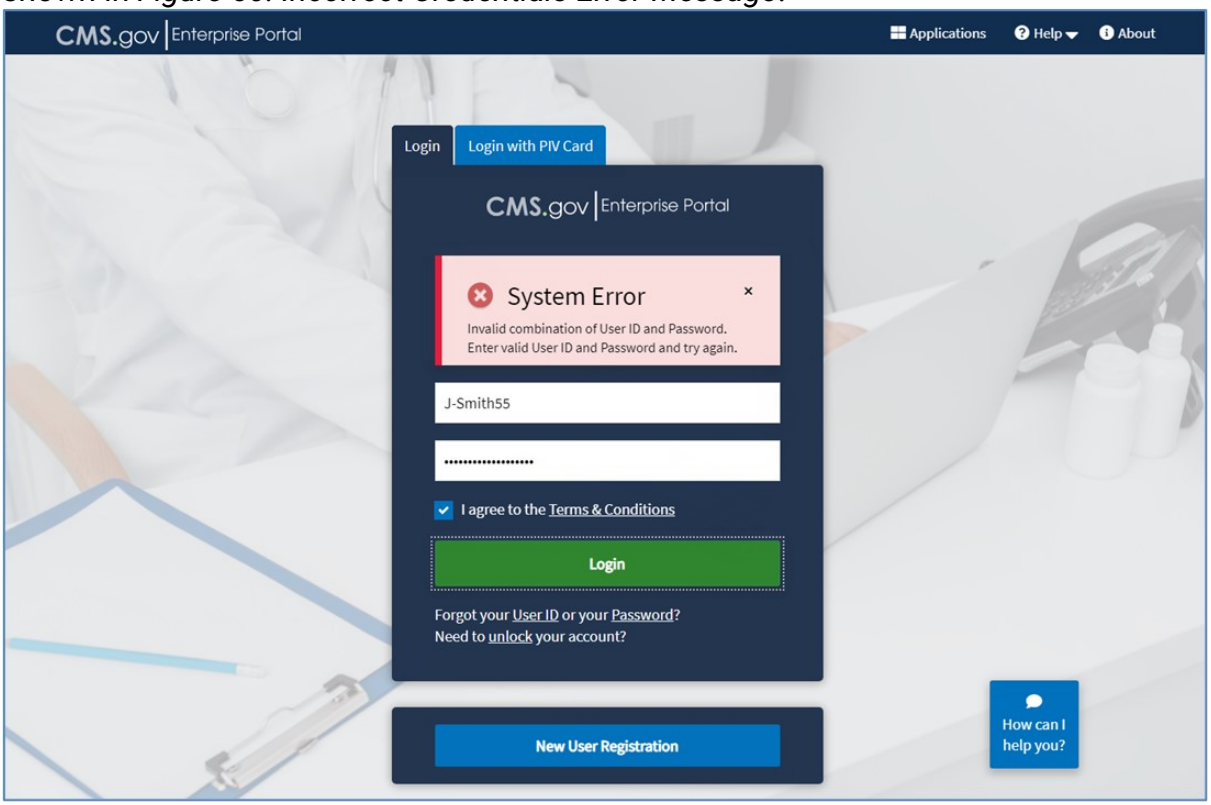

Figure 50: Incorrect Credentials Error Message

2. After entering an incorrect combination of user ID and password three times, your account locks, as shown in Figure 51: Account Locked Message and you are directed to the **Unlock My Account** page.

Note

Your account is also locked if you enter an incorrect MFA code five times in a row, and you are directed to the **Unlock My Account** page. The process for unlocking your account in this case is the same as the steps listed below.

3. On the **Unlock My Account** page, enter your user ID and click Next, as shown in Figure 52: Unlock My Account – Enter User ID.

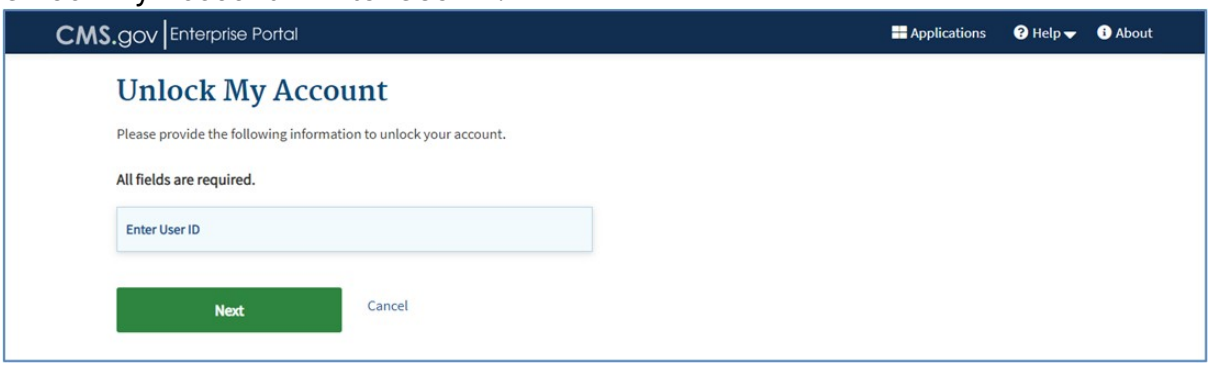

Figure 52: Unlock My Account – Enter User ID

Note

If an incorrect user ID is entered, an error occurs, as shown in *Figure 53: Incorrect User ID Error Message on Unlock My Account Page*.

Figure 53: Incorrect User ID Error Message on Unlock My Account Page

4. Choose **Email** as the recovery method from the drop-down menu and click **Send Recovery Email**, as shown in Figure 54: Unlock My Account – Select Recovery Method. You may also choose SMS or IVR as the recovery method if those MFA devices have been registered previously.

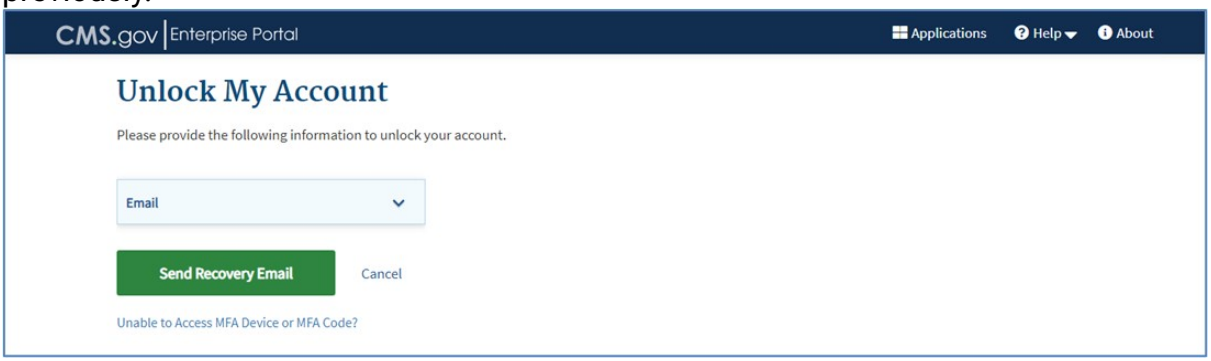

Figure 54: Unlock My Account – Select Recovery Method
Note

If you do not have access to your email, then contact your Application Help Desk to have your email address updated or unlock your account. The Help Desk contact information can be found on the CMS Enterprise Portal public page by going to the **Learn About Your Application** drop-down box and selecting your application.

A confirmation message is displayed, as shown in Figure 55: Unlock My Account – Confirmation of Message Delivery.

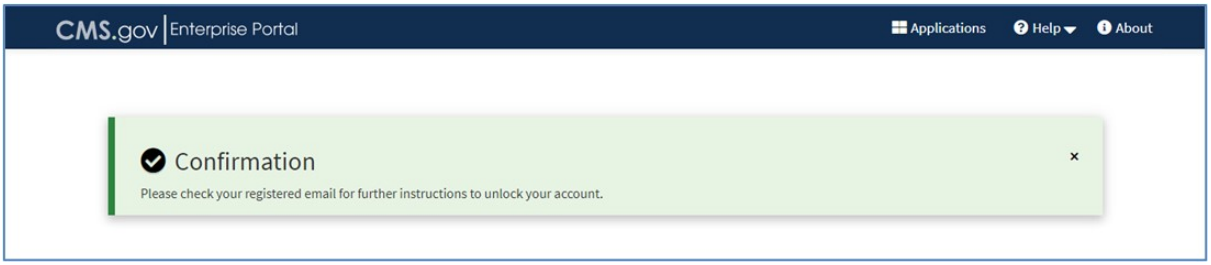

Figure 55: Unlock My Account – Confirmation of Message Delivery
Note

You will receive an email on your registered email address with a link to unlock your account.

5. Click on the link provided in the email to unlock your account.

6. Answer the security question, as shown in Figure 56: Unlock My Account – Enter Security Answer. Then, click **Submit**.

Figure 56: Unlock My Account – Enter Security Answer
Note

If incorrect information is entered in the fields, an error occurs, as shown in Figure 57: Security Question – Invalid Data.

Figure 57: Security Question – Invalid Data

7. After successfully submitting your information, you will receive confirmation that your account has been unlocked, as shown in *Figure 58: Unlock My Account – Successful Confirmation*.

Note

You will receive an email on your registered email address indicating that your account has been unlocked.

8. User Profile

Users can perform the following functions related to their user account from the **My Profile** page once they are logged into CMS Enterprise Portal:

- **View Profile** - allows viewing user's account information, such as first name, last name, date of birth, email address and phone number.
- **Change Profile** - allows modifying the following information related to user account: email address, phone number, home address, city, state, zip code, and foreign address (if applicable).
- **Change Business Contact Information** - – allows modifying user's business contact information, such as company name, company address, and company phone number.
- **Change Password** - allows changing the current password associated with the user account.
- **Change Security Question and Answer** - allows changing the security question and answer associated with the user account used for identity authentication.
- **Manage MFA Devices** - allows performing functions to manage MFA devices, including viewing the list of all MFA devices that are registered to the user's account, registering an MFA device, activating a previously registered MFA device that is in the state of Pending, editing and removing an MFA device.
- **Login History** - allows viewing the list of past successful and failed login attempts made by the user.
- **My Help Desk Contact Information** - allows viewing the help desk contact information for each application in which the user has a role.

8.1. Viewing Your Profile

The following are the instructions on how to use the 'View Profile' feature to view your profile information.

1. Navigate to the CMS Enterprise Portal public home page.

2. Login using your user ID and password.
   The CMS Enterprise Portal **My Portal** page is displayed, as shown in *Figure 59: My Portal Page – My Profile Drop-down*.

3. Select the down arrow icon that appears next to your name at the top of page. Then select **My Profile** from the drop-down list to continue.

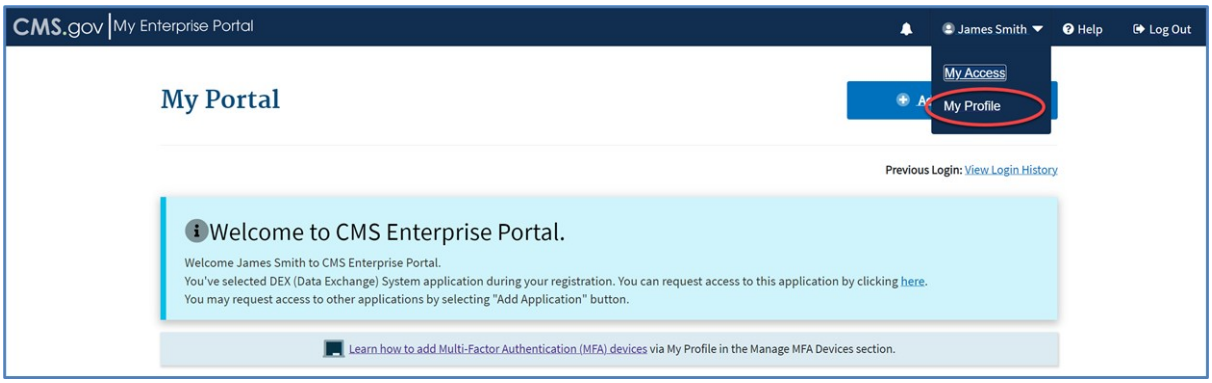

Figure 59: My Portal Page – My Profile Drop-down

The **View Profile** page displays, as shown in *Figure 60: View Profile*.

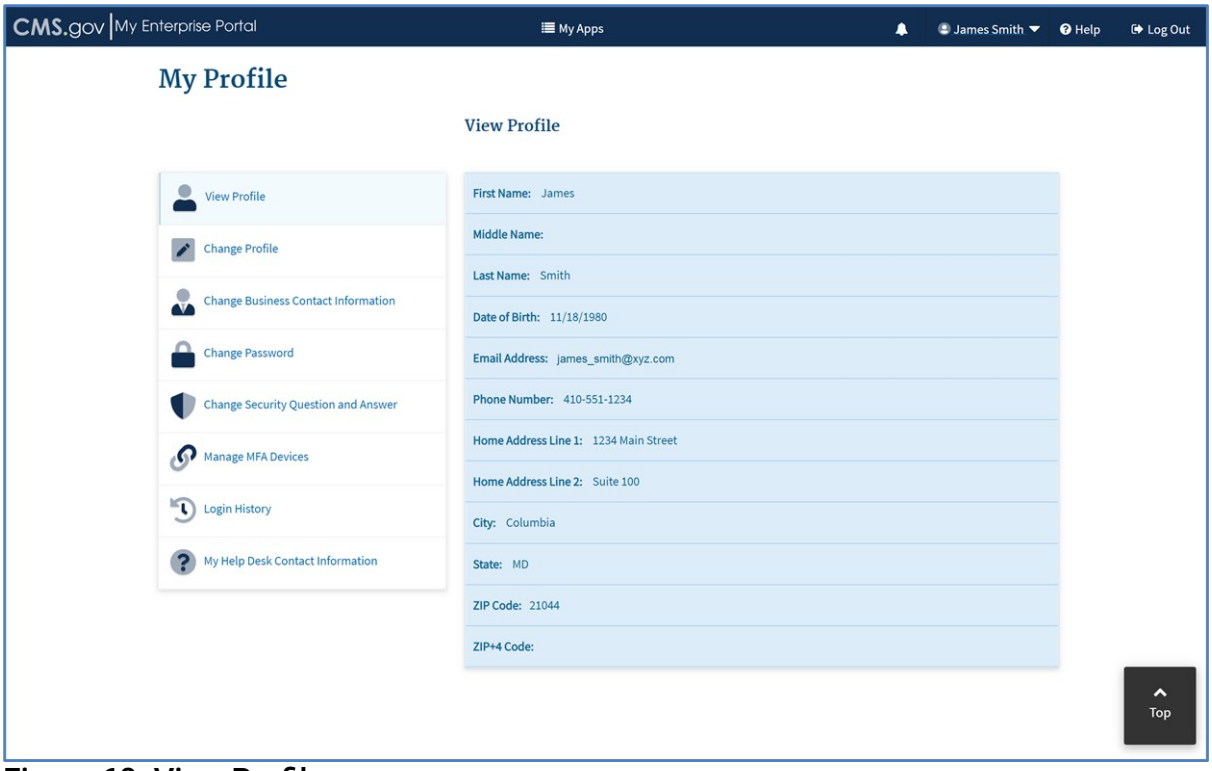

Figure 60: View Profile

8.2. Changing Your Profile

The following are the instructions on how to use the 'Change Profile' feature to update your profile information.

1. Navigate to the CMS Enterprise Portal public home page.

2. Login using your user ID and password.
   The CMS Enterprise Portal **My Portal** page is displayed, as shown in *Figure 59: My Portal Page – My Profile Drop-down*.

3. Select the down arrow icon that appears next to your name at the top of page. Then select **My Profile** from the drop-down list to continue.
   The **View Profile** page displays, as shown in *Figure 60: View Profile*.

4. Select **Change Profile** in the left pane, as shown in *Figure 61: Selecting Change Profile*.

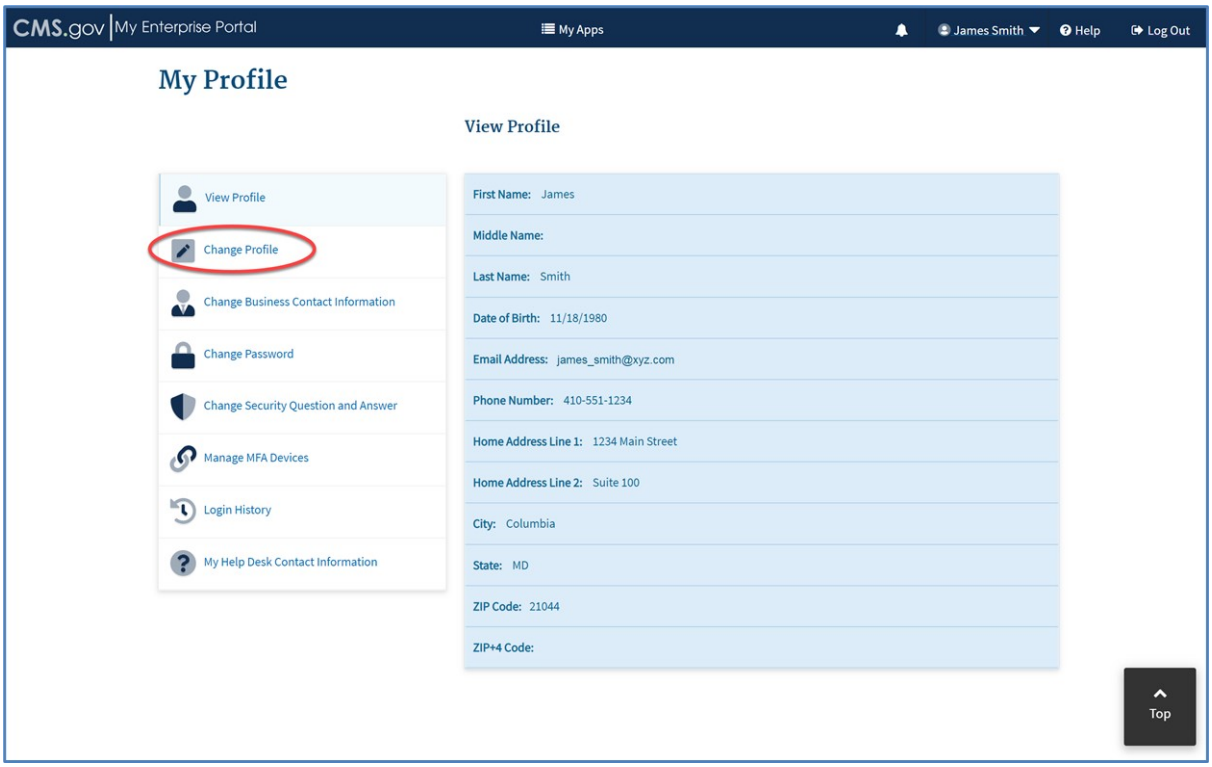

Figure 61: Selecting Change Profile

The **Change Profile** page displays, as shown in *Figure 62: Change Profile*.

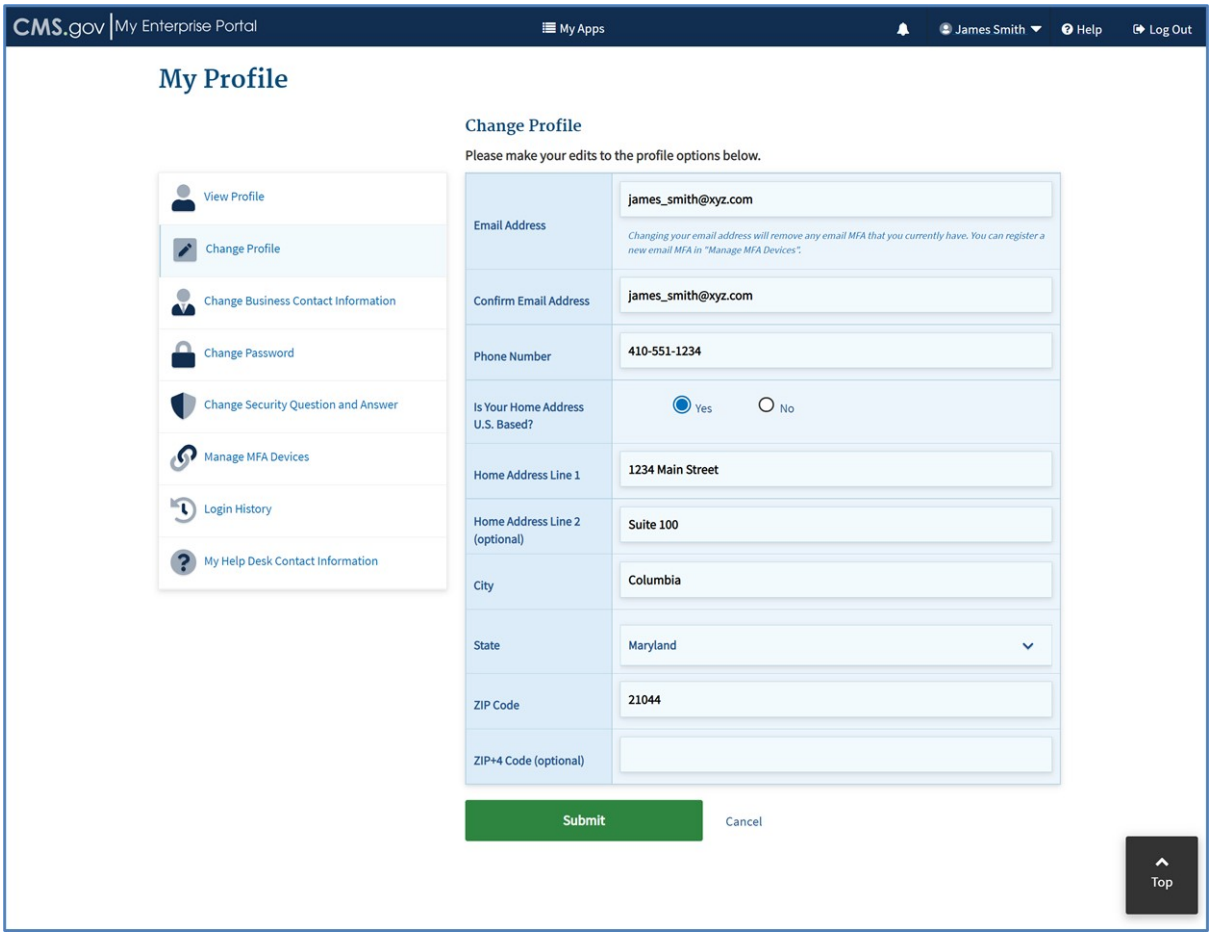

Figure 62: Change Profile

5. You can use **Change Profile** to modify items, such as email address, phone number, and home address. Update the profile information, as needed, and click **Submit**. If you click **Cancel**, you will be redirected to the **View Profile** page and your changes will not be saved.

Note

User account is considered a duplicate if the first name plus last name plus email address combination already exists in the system.

6. **Note**

   Changing your email address using Change Profile will remove any email MFA that you currently have. After changing your email address, you can register a new email MFA for the new email address from 'Manage MFA Devices'.

7. After submitting the updated information, you will receive confirmation that the changes to your profile were submitted successfully, as shown in *Figure 63: Change Profile – Successful Confirmation*.
   Note

   You will receive an email notification indicating that you successfully changed your profile. If the email address was changed, an email notification will be sent to both old and new addresses.

8.3. Changing Your Business Contact Information

The following are the instructions on how to use the 'Change Business Contact Information' feature to change your business contact details.

1. Navigate to the CMS Enterprise Portal public home page.

2. Login using your user ID and password.
   The CMS Enterprise Portal **My Portal** page is displayed, as shown in *Figure 59: My Portal Page – My Profile Drop-down*.

3. Select the down arrow icon that appears next to your name at the top of page. Then select **My Profile** from the drop-down list to continue.
   The **View Profile** page displays, as shown in *Figure 60: View Profile*.

4. Select **Change Business Contact Information** in the left pane, as shown in *Figure 64: Change Business Contact Information*.
   The Change Business Contact Information page displays, as shown in *Figure 64: Change Business Contact Information*.

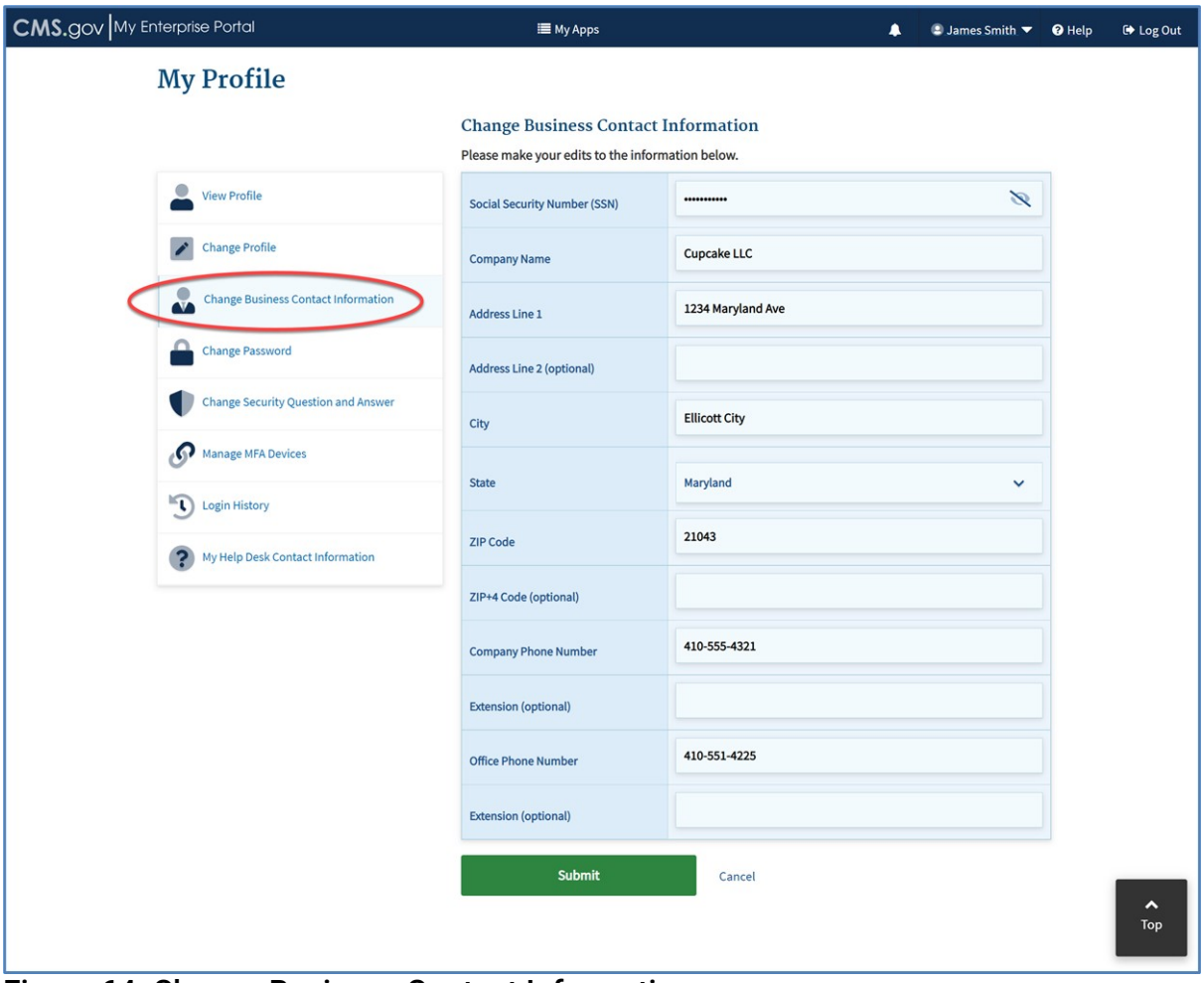

Figure 64: Change Business Contact Information

5. You can use **Change Business Contact Information** to modify items, such as company name, company address, and company phone number. Update the business contact information (BCI), as needed, and click **Submit**. If you click **Cancel**, you will be redirected to the **View Profile** page and your changes will not be saved.
   Note

   If the Social Security Number (SSN) has been previously entered, then it will be displayed as read-only (non-editable) on the Change Business Contact Information page. If the SSN has not been previously entered, you must enter it in the Change Business Contact Information page in order to save BCI. BCI is sometimes collected during an application role request process depending on the application and role that is being requested. During the role request process, if the SSN has not been previously entered, you will be required to enter it during the 'Enter BCI' step in order to continue with role request. If the SSN has been previously entered, then the SSN will be read-only during the 'Enter BCI' step of the role request process. See section 9.3 - *Requesting a Role* for more information. The SSN can be entered/edited by a Help Desk user as long as the user is not at LOA 3.

6. After submitting the updated information, you will receive confirmation that the changes to your profile were submitted successfully, as shown in *Figure 65: Change Business Contact Information – Successful Confirmation*.
   Note

   You will receive an email notification indicating that you successfully changed your BCI.

8.4. Changing Your Password

The following are the instructions on how to use the 'Change Password' feature to change your password.

1. Navigate to the CMS Enterprise Portal public home page.

2. Login using your user ID and password.
   The CMS Enterprise Portal **My Portal** page is displayed, as shown in *Figure 59: My Portal Page – My Profile Drop-down*.

3. Select the down arrow icon that appears next to your name at the top of page. Then select **My Profile** from the drop-down list to continue.
   The **View Profile** page displays, as shown in *Figure 60: View Profile*.

4. Select **Change Password** in the left pane, as shown in Figure 66: Change Password. The Change Password page displays, as shown in Figure 66: Change Password.

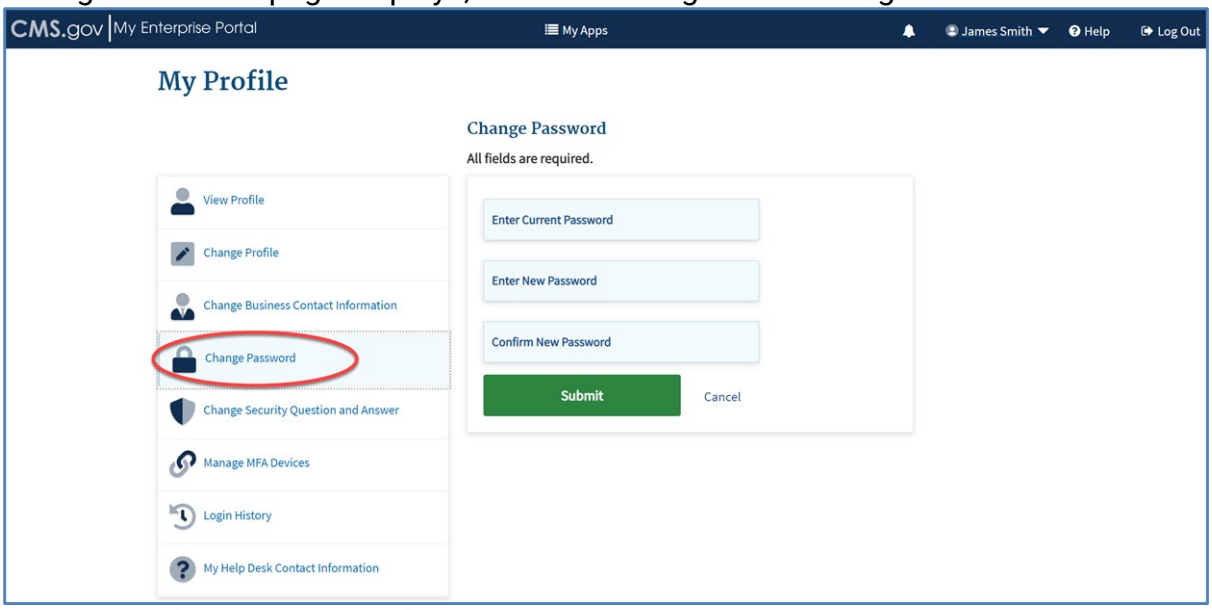

Figure 66: Change Password

5. Enter your old password in the **Enter Current Password** field.

6. Enter a new password in the **Enter New Password** field and again in the **Confirm New Password** field. Then, click Submit. If you click Cancel, you will be redirected to the **View Profile** page and your changes will not be saved.
   A tool tip is enabled that provides the password requirements, as shown in *Figure 67: Change Password – Tool Tip*.

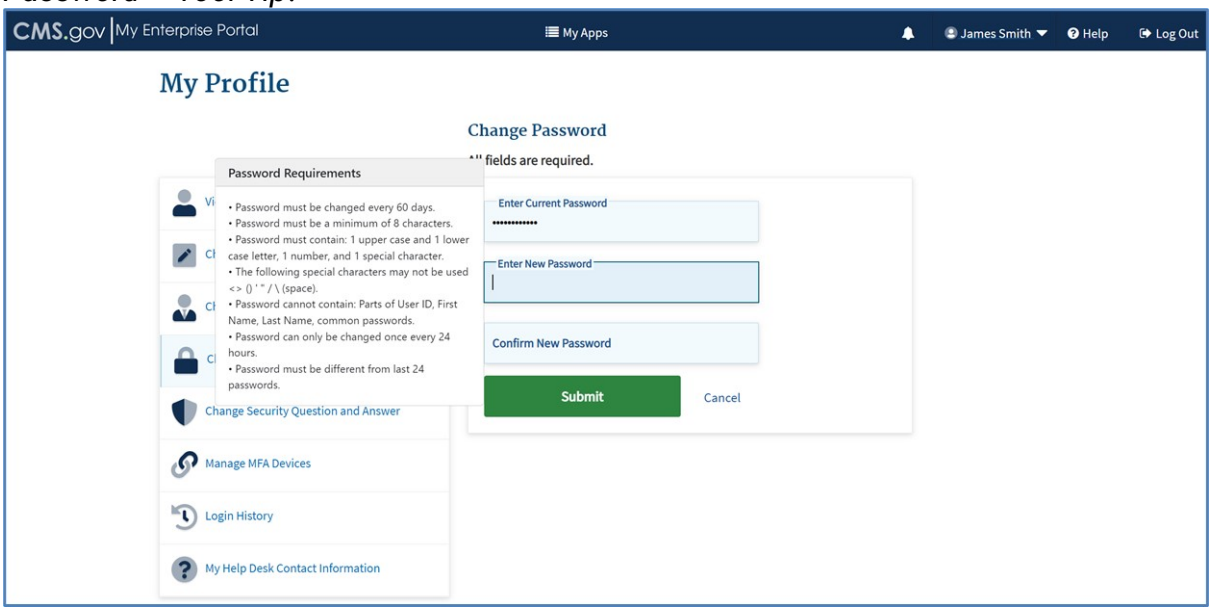

Figure 67: Change Password – Tool Tip

7. After submitting the updated password information, you will receive confirmation that the

changes to your profile were submitted successfully, as shown in *Figure 68: Change Password – Successful Confirmation*.

Note

You will receive an email notification indicating that you successfully changed your password.

8.5. Changing Your Security Question

The following are the instructions on how to use the 'Change Security Question' feature to change your security question and answer.

1. Navigate to the CMS Enterprise Portal public home page.

2. Login using your user ID and password.
   The CMS Enterprise Portal **My Portal** page is displayed, as shown in *Figure 59: My Portal Page – My Profile Drop-down*.

3. Select the down arrow icon that appears next to your name at the top of page. Then select **My Profile** from the drop-down list to continue.
   The **My Profile** page displays, as shown in *Figure 60: View Profile*.

4. Select **Change Security Question** in the left pane, as shown in *Figure 69: Change Security Question and Answer – Update Information*.
   The **Change Security Question and Answer** page displays, as shown in *Figure 69: Change Security Question and Answer – Update Information*.

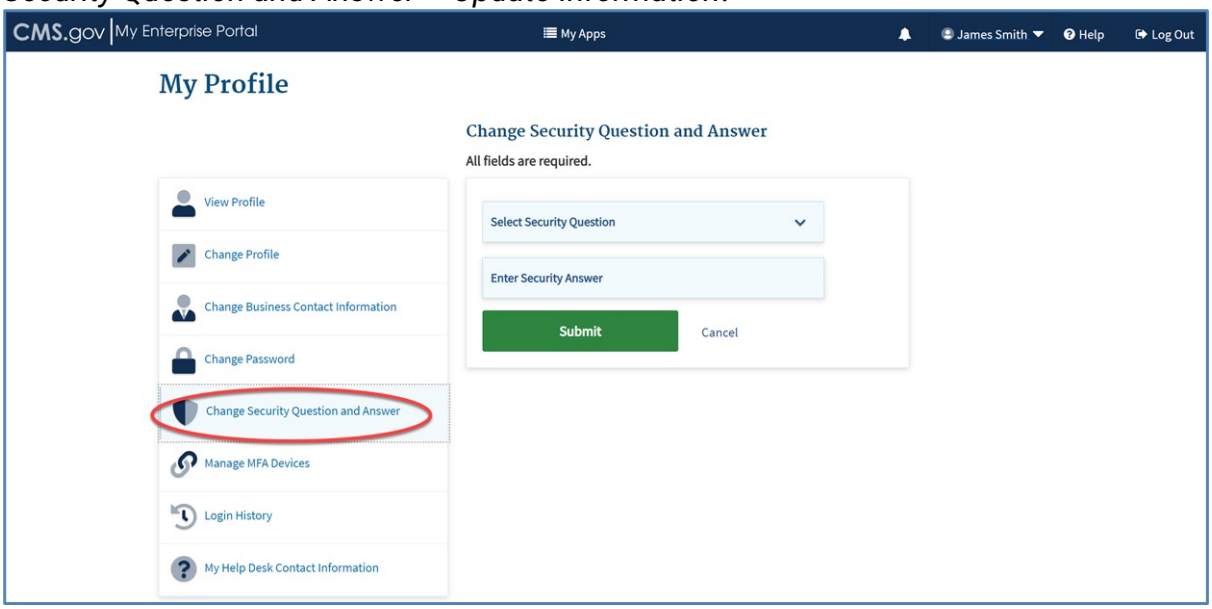

Figure 69: Change Security Question and Answer – Update Information

5. Select a question and then provide an answer of your choosing. Click Submit. If you click **Cancel**, you will be redirected to the **View Profile** page and your changes will not be saved.

6. After submitting the updated information, you will receive confirmation that the changes to your profile were submitted successfully, as shown in *Figure 70: Change Security Question – Successful Confirmation*.

   Note

   You will receive an email notification indicating that you successfully changed your profile.

8.6. Managing Multi-Factor Authentication (MFA)

MFA is a security mechanism that is implemented to provide an extra layer of security such as a security code, when logging into CMS Enterprise Portal with a user ID and password.

Registered CMS Enterprise Portal users who wish to access a CMS MFA-protected application are directed through the MFA process at login.

During the MFA registration process (when an MFA device is added), the CMS Enterprise Portal system allows the user to register a phone or email to add an additional level of security to a user's account. The user is given five MFA Device options from which to select, to complete the registration process:

- **Email:** Users can select the Email option to receive an email containing the security code required at login. The email address on the user's profile is used.
- **Short Message Service (SMS):** Users can use the SMS option (sometimes called text message) to have their security code texted to their phone. The user must enter a valid phone number during SMS registration. The phone must be capable of receiving text messages. Carrier charges may apply.
- **Interactive Voice Response (IVR):** Users can select the IVR option to receive a phone call containing their security code (voiced by a computer). The user must provide a valid phone number and (optional) phone extension during IVR registration.
- **Google Authenticator:** Users can select the Google Authenticator option to read a passcode on their smart phone. Supported phones include iPhone, Android Phone, and Blackberry.
- **Okta Verify:** Users can select the Okta Verify option to receive push notifications on their mobile device. Supported phones include iPhone, Android Phone, and Windows Phone.
  Note

  Some users may see a sixth MFA device option for **YubiKey**. The Yubikey option allows users of certain applications to use a hardware device that attaches to the computer via a USB port, if their account this setup to use this device. Users should contact their application Help Desk to see if their application is eligible to use YubiKey and to get assistance with setting up their account to use the YubiKey device.

After registering an MFA device at login, you can then register additional devices or manage your currently registered devices, i.e. view, edit, or remove an MFA device from the **Manage MFA Devices** page under My Profile.

To register a device for MFA, please follow each step listed below unless otherwise noted.

1. Navigate to the CMS Enterprise Portal public home page.

2. Login using your user ID and password.
   The CMS Enterprise Portal **My Portal** page is displayed, as shown in *Figure 59: My Portal Page – My Profile Drop-down*.

3. Select the down arrow icon that appears next to your name at the top of page. Then select **My Profile** from the drop-down list to continue.
   The **My Profile** page displays, as shown in *Figure 60: View Profile*.

4. Select **Manage MFA Devices** in the left pane, as shown in *Figure 71: Manage MFA Devices*.
   A list of registered MFA devices is displayed.

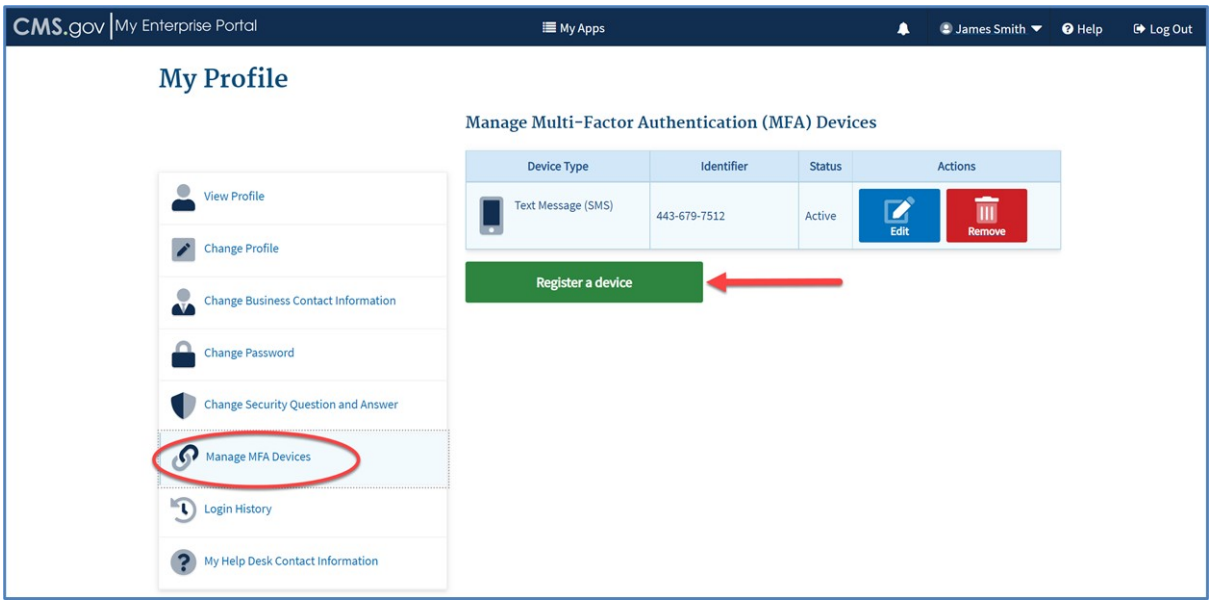

Figure 71: Manage MFA Devices

5. Click on **Register a device** button, as shown in *Figure 71: Manage MFA Devices*.
   The registration section of the page displays, as shown in *Figure 72: Manage MFA Devices – Registering an MFA Device*.

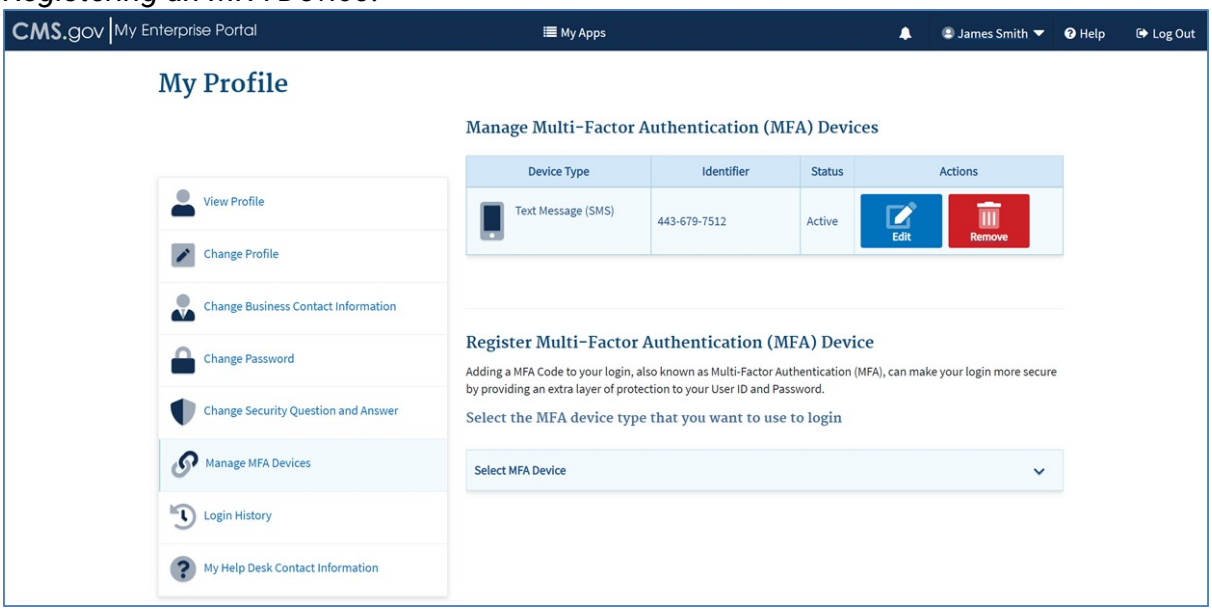

Figure 72: Manage MFA Devices – Registering an MFA Device

6. Expand the **Select MFA Device** drop-down list, as shown in *Figure 73: Manage MFA Devices – Select MFA Device*.

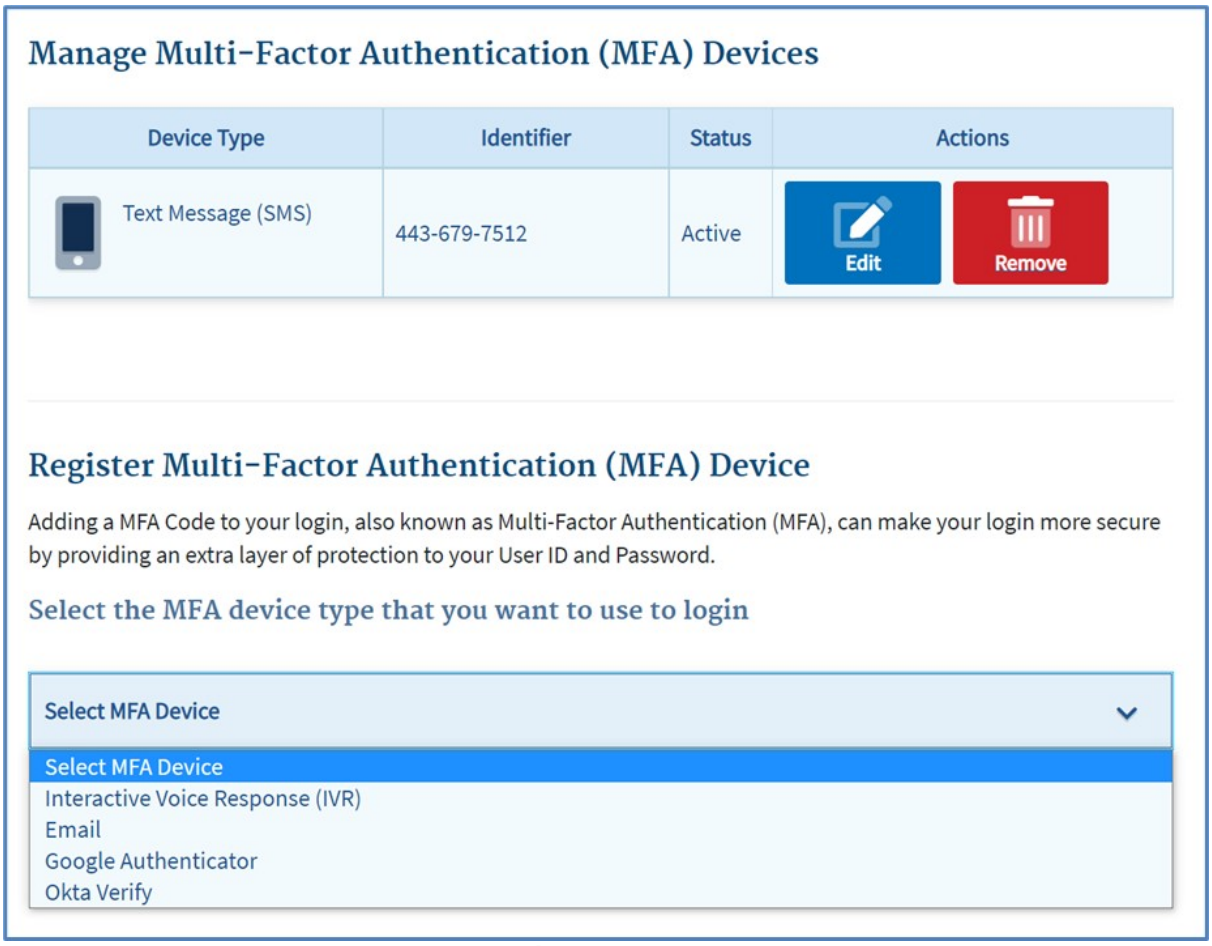

Figure 73: Manage MFA Devices – Select MFA Device

7. Select your MFA Device.
   Specific directions are displayed depending on your selection. See the MFA device options in the subsections *8.6.1* through *8.6.5*.

8.6.1. Register Text Message (SMS) MFA Device

1. If you select **Text Message (SMS)** as the MFA device type, read the information under the **Text Message (SMS)** drop-down, as shown in *Figure 74: Register Text Message (SMS)*.

2. Enter the Phone Number that will be used to obtain the security code in the **Enter Phone Number** field. Then, click **Send MFA Code**. If you click **Cancel**, you will exit out of the registration process.

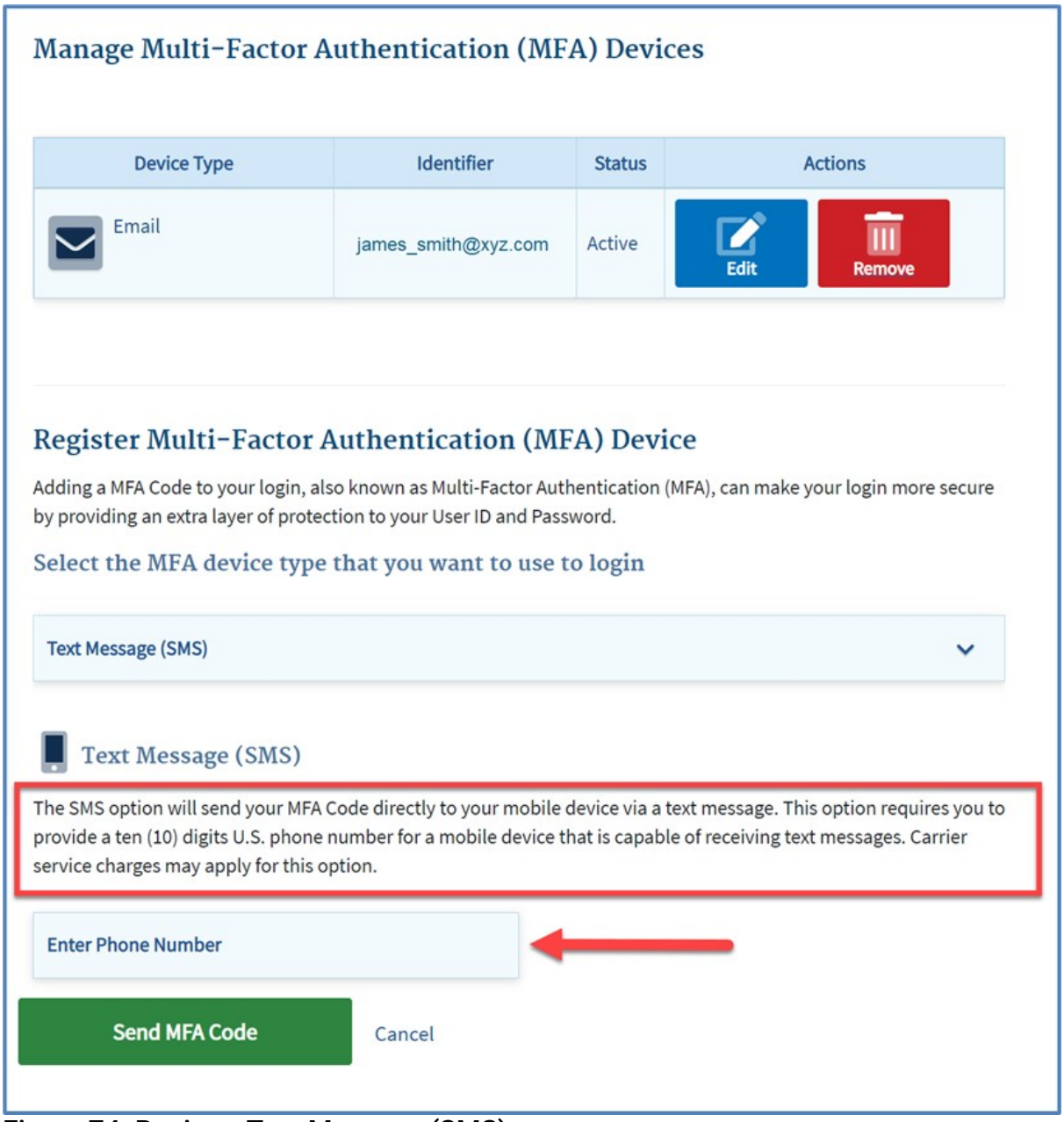

Figure 74: Register Text Message (SMS)

3. After submitting the information, you will receive confirmation that the MFA code has been sent to your MFA device, as shown in *Figure 75: Register Text Message (SMS) – Successful Submission*.

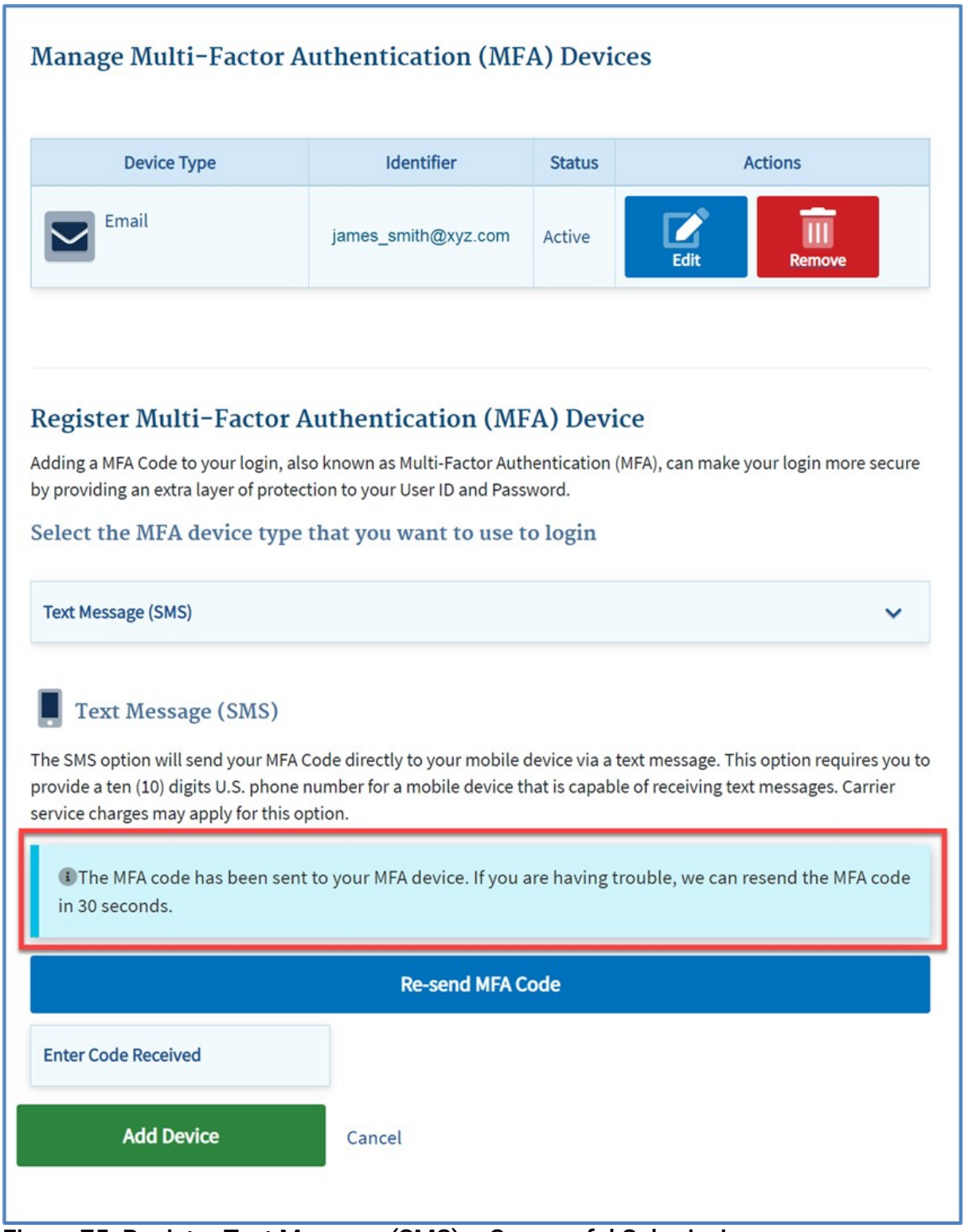

Figure 75: Register Text Message (SMS) – Successful Submission

4. Enter the security code you received on your phone into the **Enter Code Received** field and then click **Add Device**.
   You will receive a confirmation that the changes to your profile were submitted successfully, as shown in *Figure 76: Register MFA Device – Success Message*.

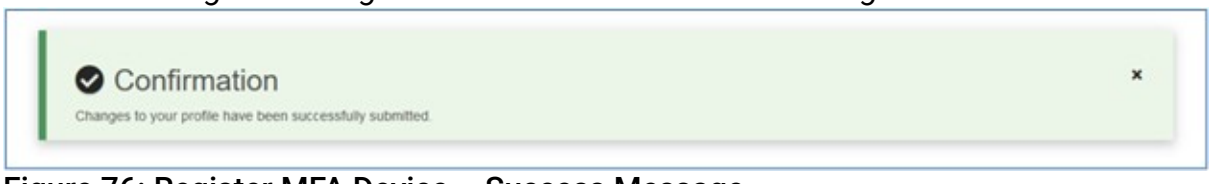

Figure 76: Register MFA Device – Success Message

The Text Message (SMS) device is added to the list of available devices with “Active” status and two actions: Edit and Remove, as shown in *Figure 77: Manage/View Available Devices –*

SMS MFA Device Added in Active Status.

Your registration of the MFA device is now complete, and you will receive an email notification indicating that you successfully registered the MFA device.

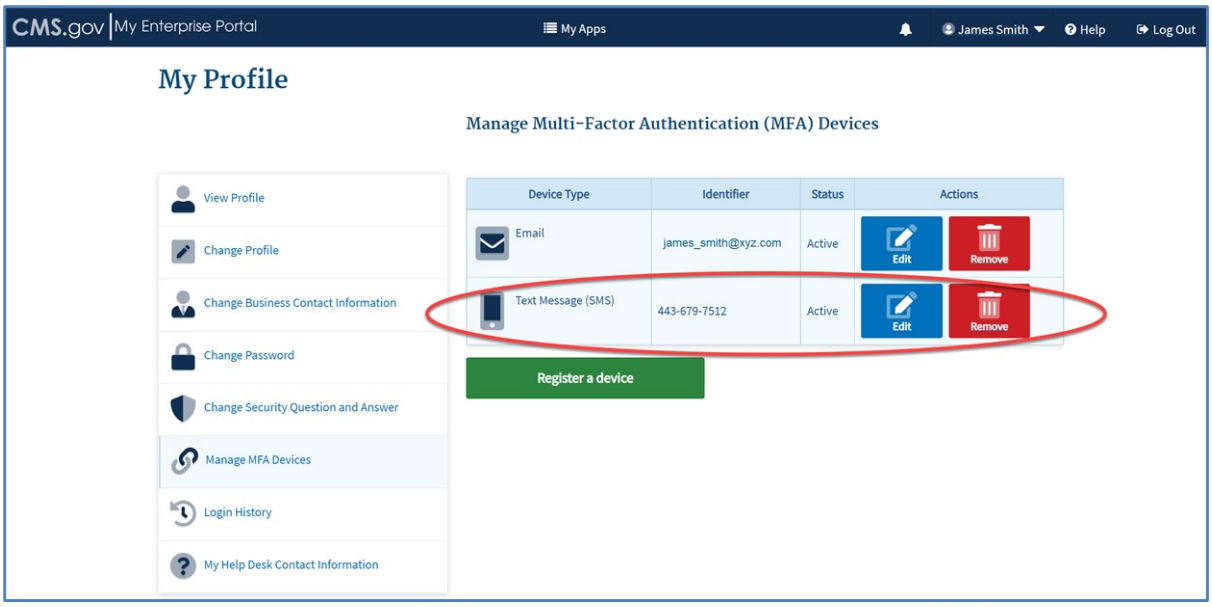

Figure 77: Manage/View Available Devices – SMS MFA Device Added in Active Status

Note

If you click **Cancel** instead of entering the security code after it has been sent, then the SMS device will display with a "Pending" status on the Manage/View MFA Devices page and an additional action: Activate, as shown in *Figure 78: Manage/View Available Devices – SMS MFA Device Added in Pending Status*. See section *8.6.8 - Activating MFA Device* for how to activate a device in "Pending" status.

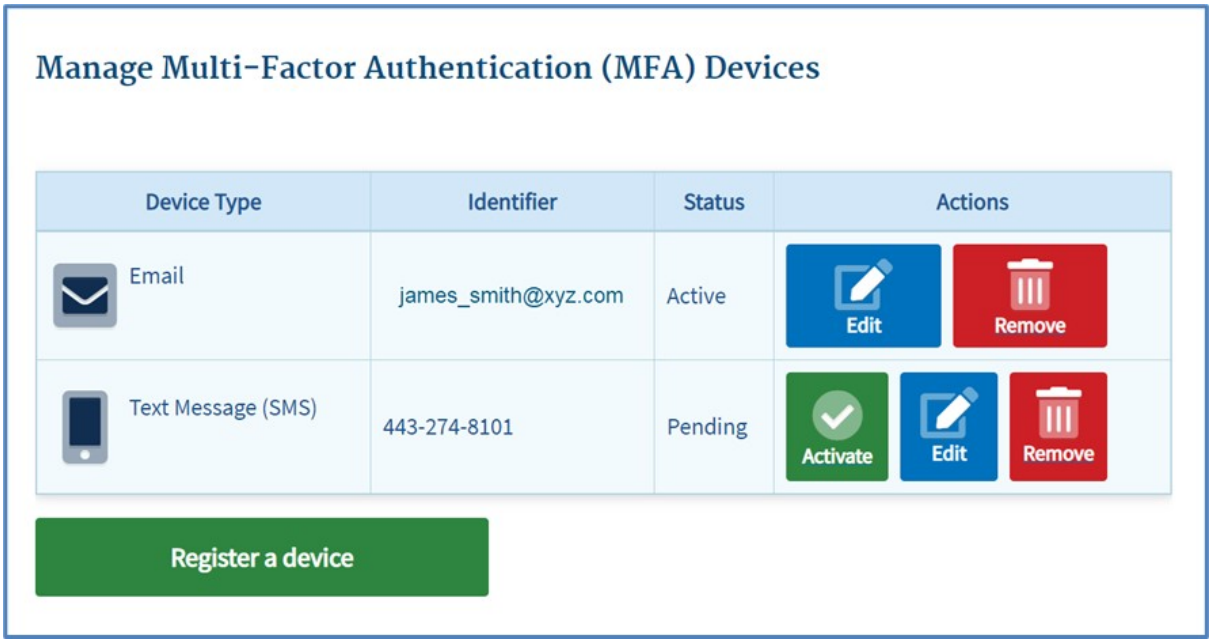

Figure 78: Manage/View Available Devices – SMS MFA Device Added in Pending Status

8.6.2. Register Email MFA Device

1. If you select **Email** as the MFA device type, read the information under the **Email** drop-down, as shown in *Figure 79: Register Email*.
2. Click **Send MFA Code**. If you click **Cancel**, you will exit out of the registration process.

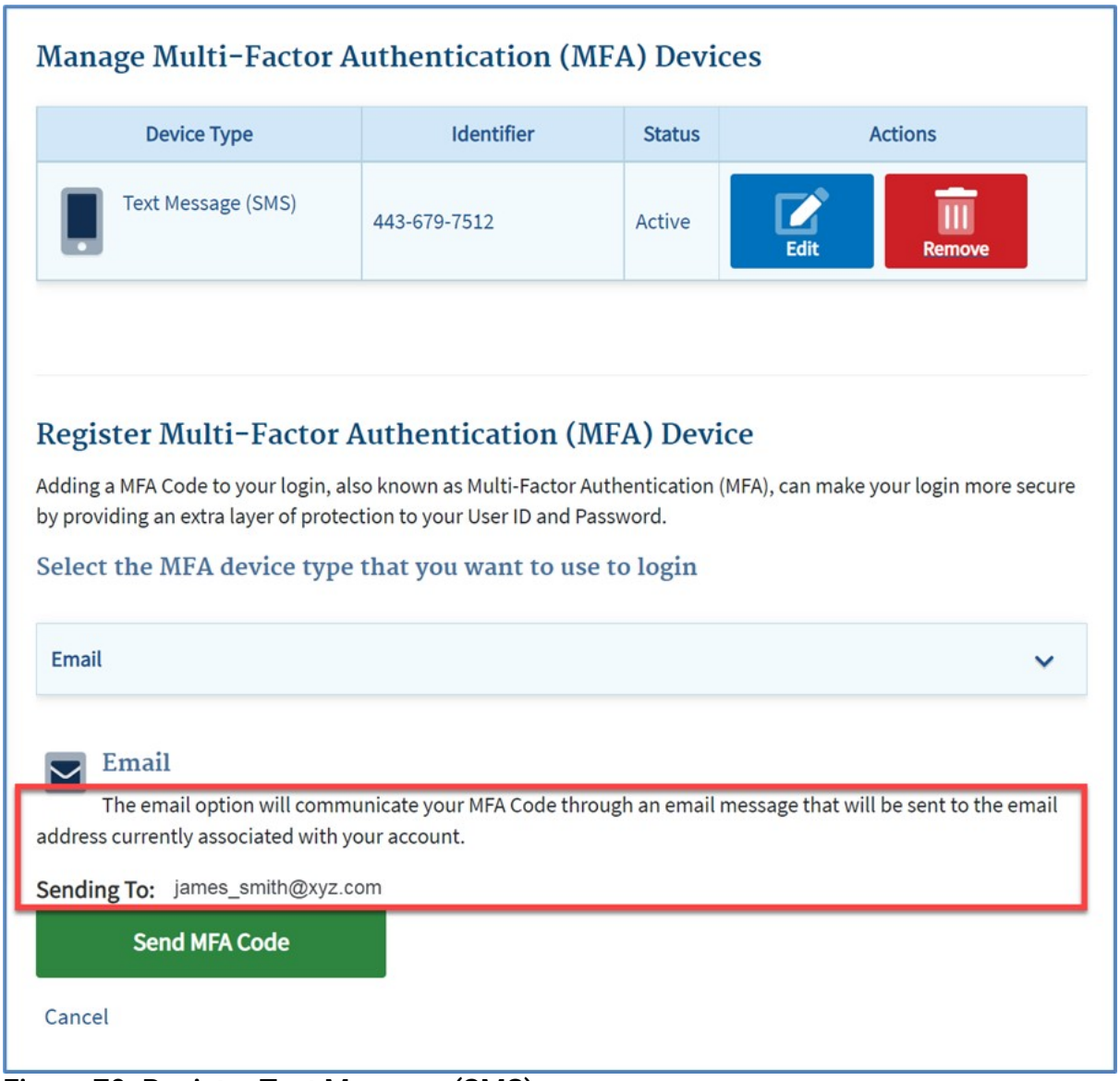

Figure 79: Register Text Message (SMS)

3. Enter the security code received via email in the **Enter Code Received** field, as shown in *Figure 80: Register Email – Entering Security Code*. Then, click **Add Device**. If you click **Cancel**, you will exit out of the registration process.

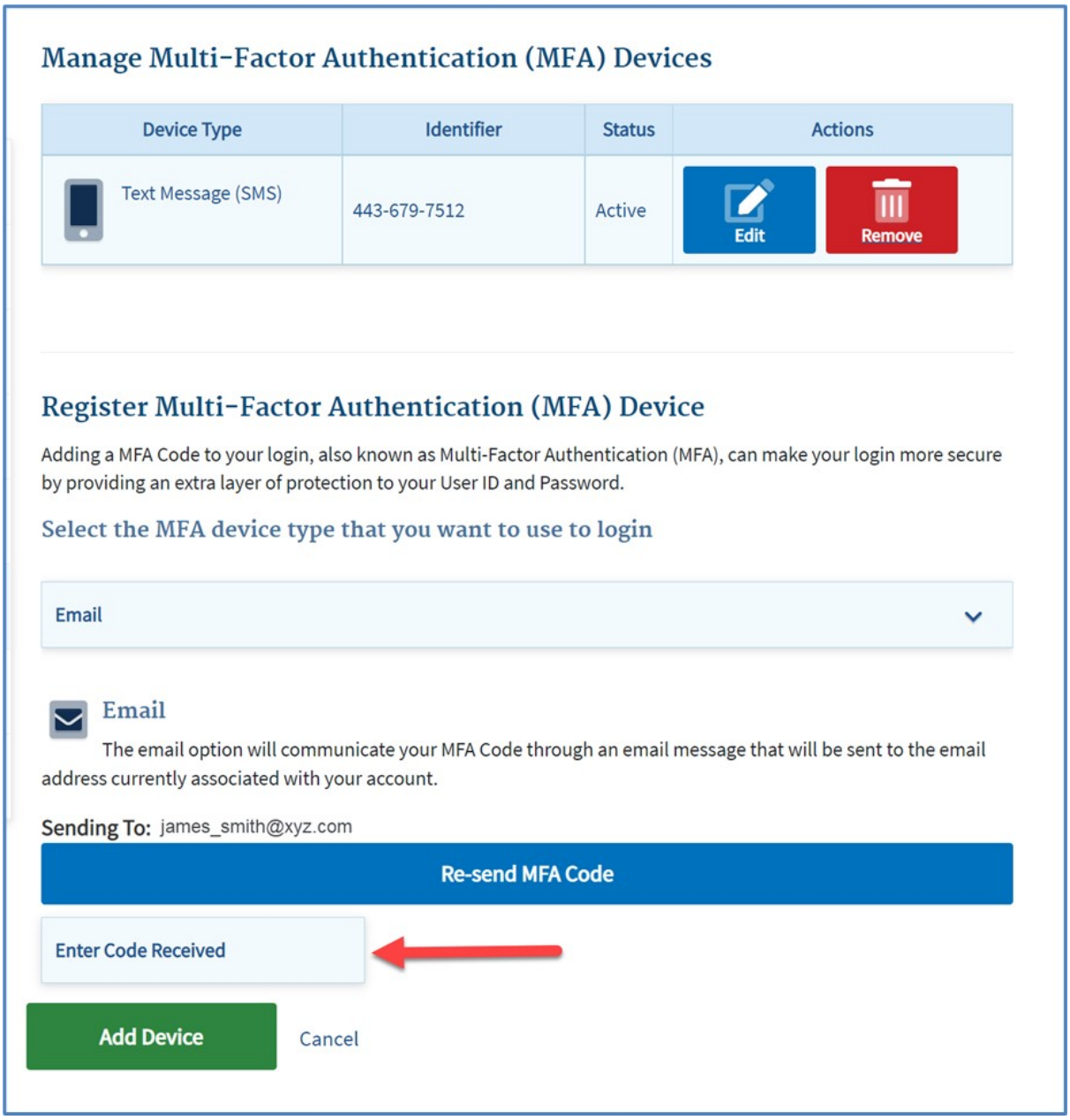

Figure 80: Register Email – Entering Security Code

You will receive a confirmation that the changes to your profile were submitted successfully, as shown in *Figure 81: Register MFA Device – Success Message*.

Figure 81: Register MFA Device – Success Message

The Email device is added to the list of available devices with "Active" status and two actions: Edit and Remove, as shown in *Figure 82: Manage/View Available Devices – Email MFA Device Added in Active Status*.

Your registration of the MFA device is now complete, and you will receive an email notification indicating that you successfully registered the MFA device.

Figure 82: Manage/View Available Devices – Email MFA Device Added in Active Status

Note

If you click **Cancel** instead of entering the security code after it has been sent, then the Email device will display with a "Pending" status on the Manage/View MFA Devices page and an additional action: Activate. See section *8.6.8 – Activating MFA Device* for how to activate a device in "Pending" status.

8.6.3. Register Interactive Voice Response (IVR) MFA Device

1. If you select **Interactive Voice Response (IVR)** as the MFA device type, read the information under the **Interactive Voice Response (IVR)** drop-down, as shown in *Figure 83: Register Interactive Voice Response (IVR)*.

2. Enter the Phone Number and corresponding extension (optional) that will be used to obtain the security code in the **Enter Phone Number** field. Then, click **Send MFA Code**.

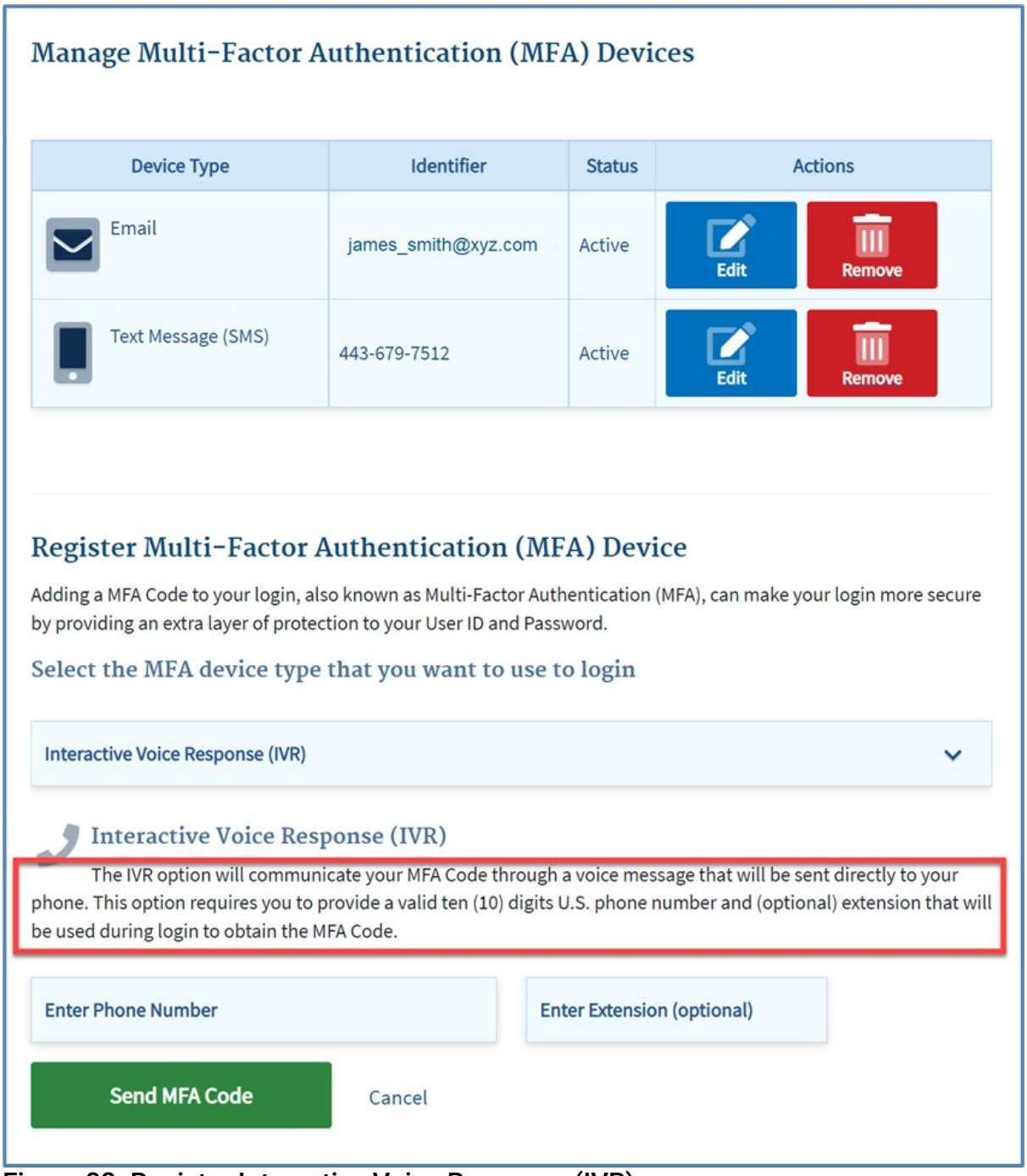

Figure 83: Register Interactive Voice Response (IVR)

3. After submitting the information, you will receive confirmation that the MFA code has been sent to your MFA device, as shown in *Figure 84: Register Interactive Voice Response (IVR) – Successful Submission*.

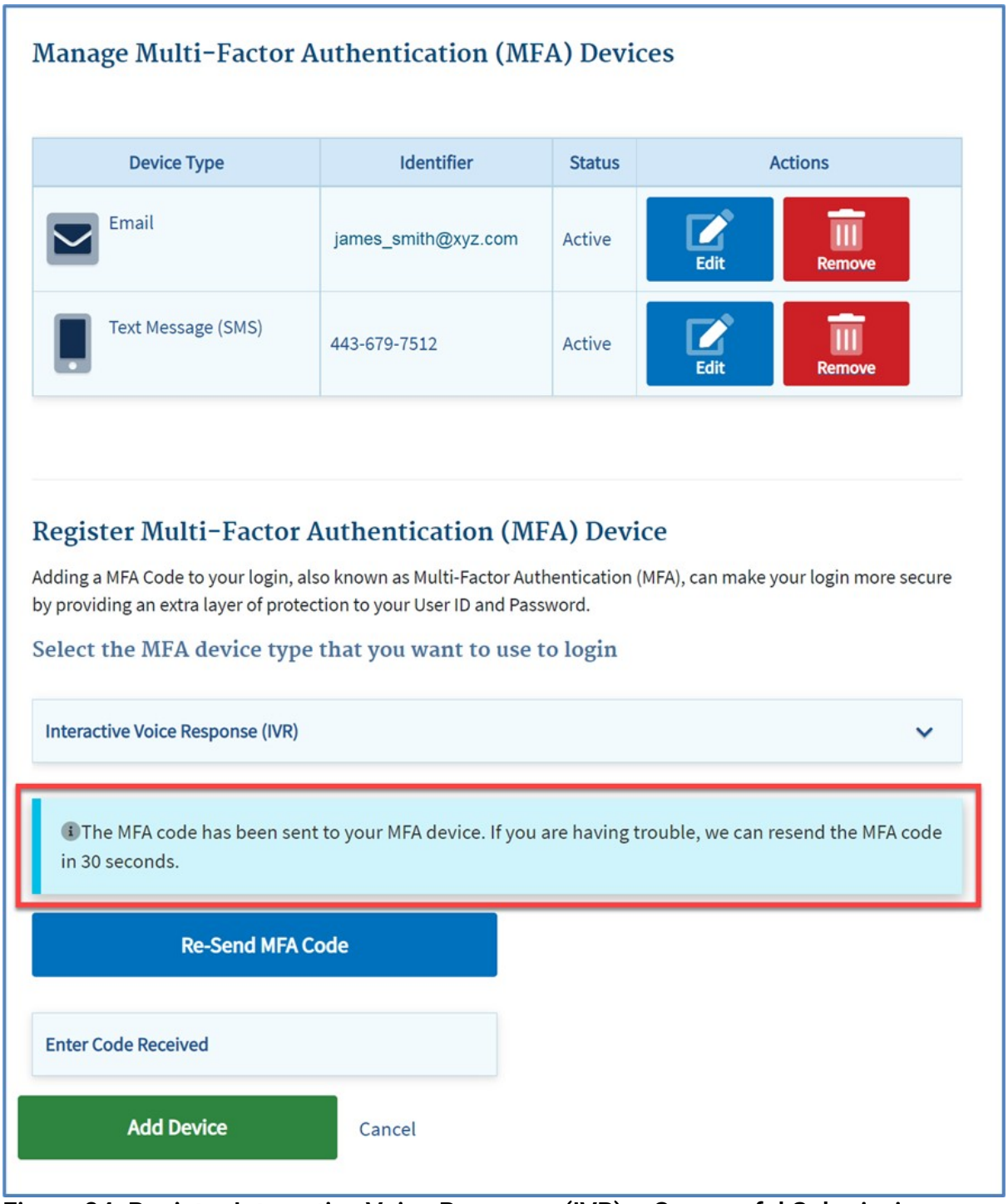

Figure 84: Register Interactive Voice Response (IVR) – Successful Submission

4. Enter the security code you received from the phone call into the **Enter Code Received** field and then click **Add Device**.
   You will receive a confirmation that the changes to your profile were submitted successfully, as shown in *Figure 85: Register Interactive Voice Response (IVR) – Success Message*.

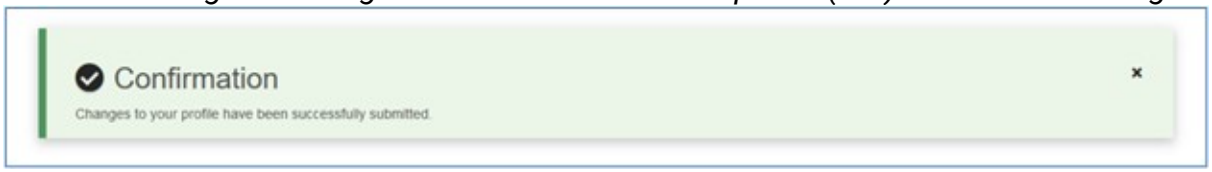

Figure 85: Register Interactive Voice Response (IVR) – Success Message

The Interactive Voice Response (IVR) device is added to the list of available devices with "Active" status and two actions: Edit and Remove, as shown in *Figure 86: Manage/View Available Devices – IVR MFA Device Added in Active Status*.
Your registration of the MFA device is now complete, and you will receive an email notification indicating that you successfully registered the MFA device.

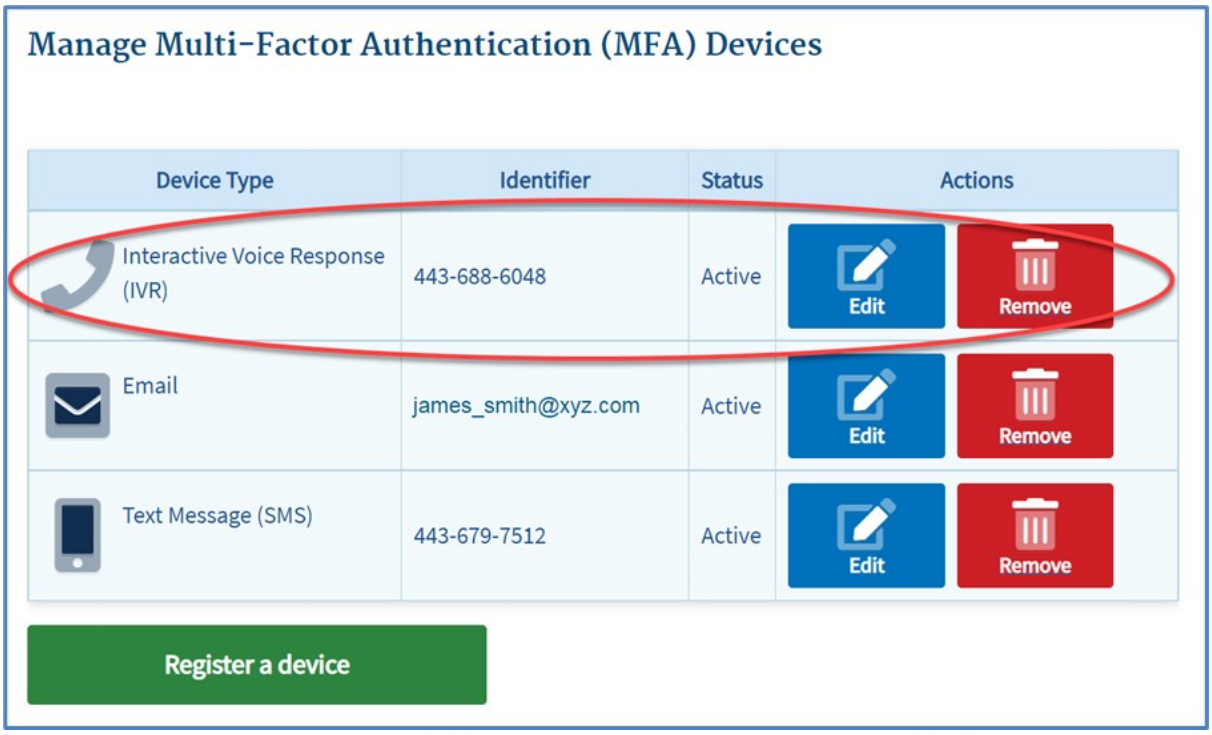

Figure 86: Manage/View Available Devices – IVR MFA Device Added in Active Status

Note

If you click **Cancel** instead of entering the security code, then the IVR device will display with a "Pending" status on the Manage/View MFA Devices page and an additional action: Activate. See section *8.6.8 - Activating MFA Device* for how to activate a device in "Pending" status.

8.6.4. Register Google Authenticator MFA Device

1. If you select **Google Authenticator** as the MFA device type, read the information under the **Google Authenticator** drop-down, as shown in *Figure 87: Register Google Authenticator – Start Setup*. If Google Authenticator is not installed on your phone, then use your phone's application store to find and install the app. Then, click **Next**.

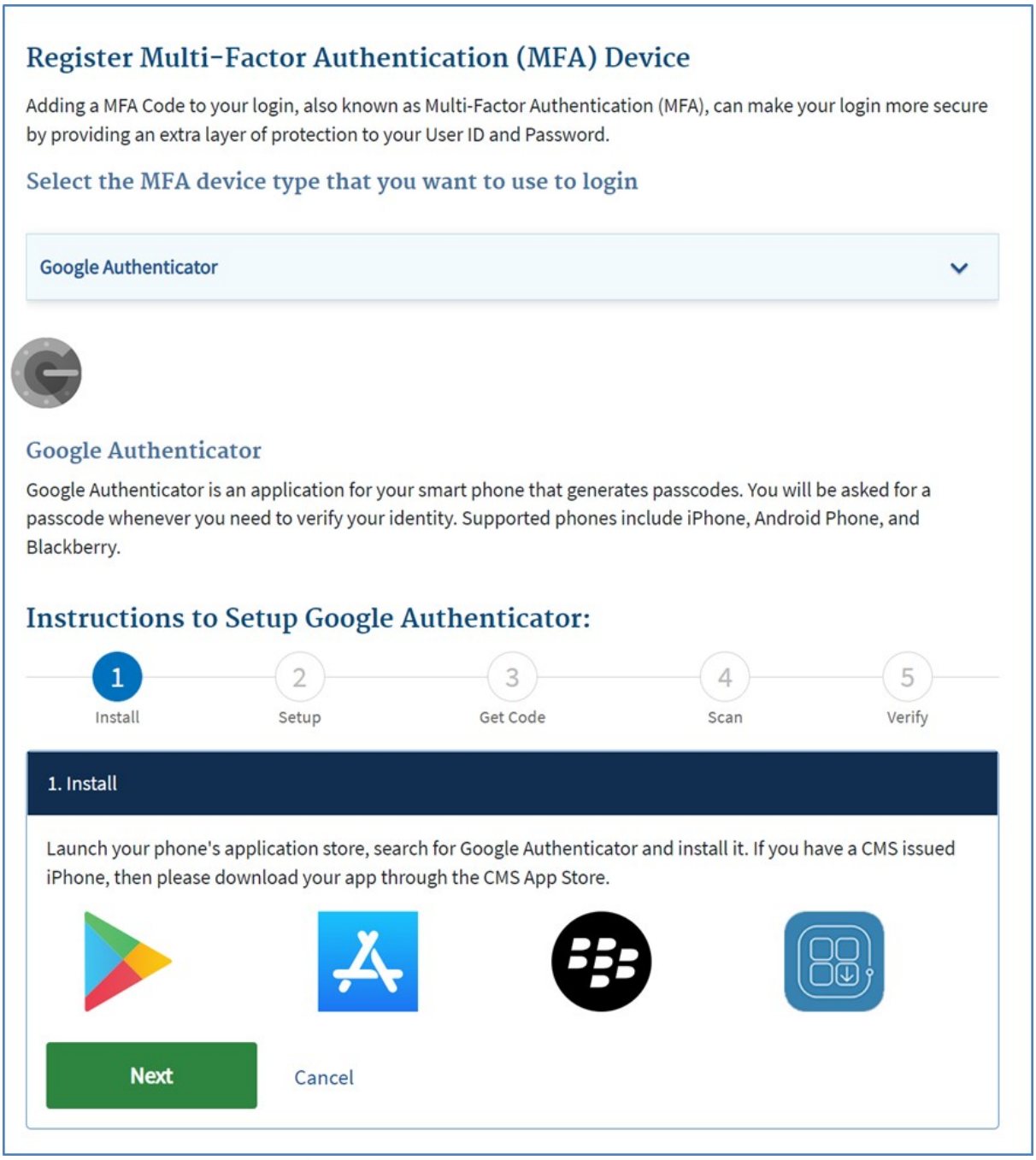

Figure 87: Register Google Authenticator – Start Setup

2. In the step **2. Setup** screen, click **Next**.

3. In the step **3. Get Code** screen, click the **Register Device** button.
   A barcode appears in the step **4. Scan** screen, as shown in *Figure 88: Register Google Authenticator – Barcode Generated*.

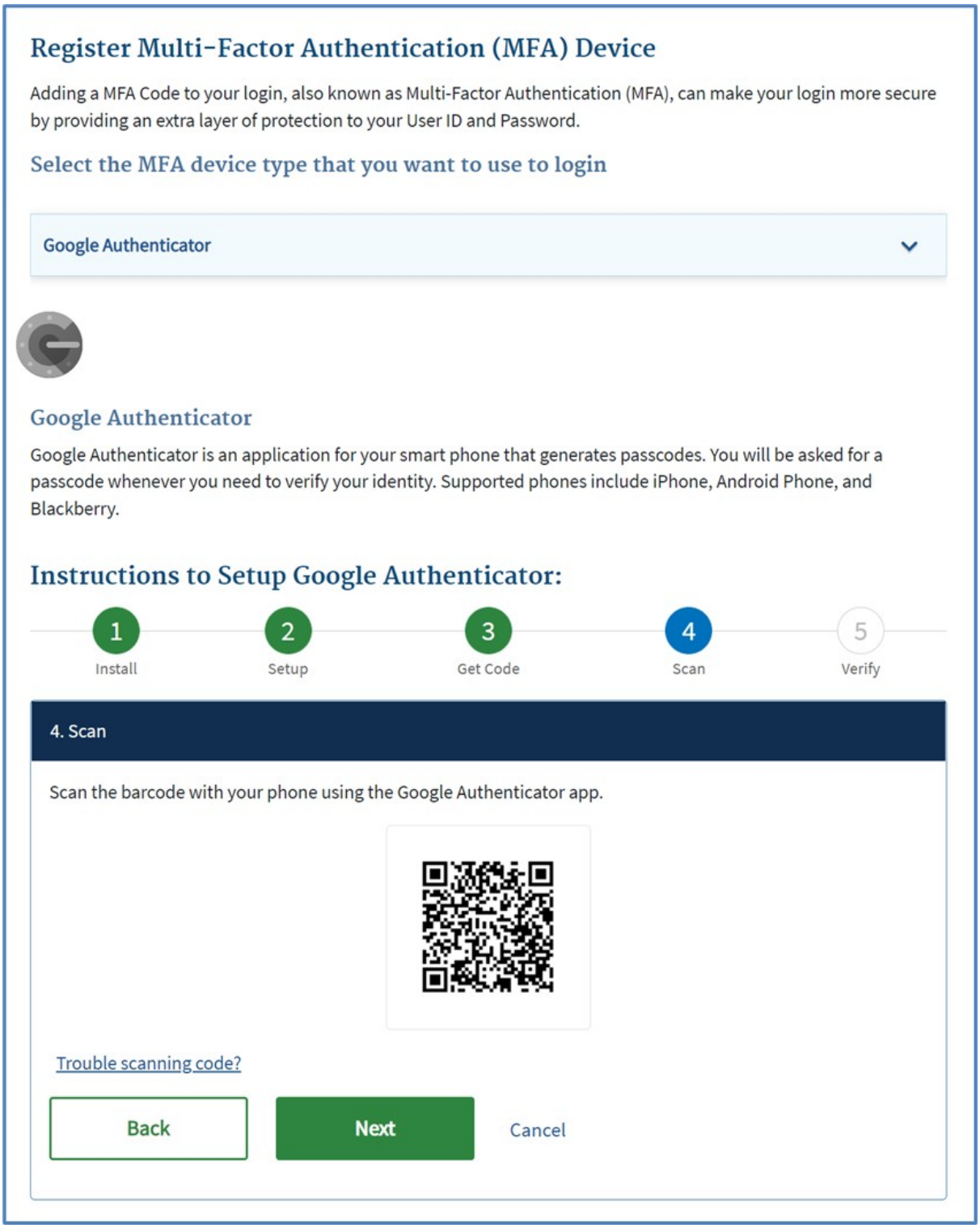

Figure 88: Register Google Authenticator – Barcode Generated

4. Using a smart phone, open the Google Authenticator app to scan the barcode.

5. In the **step 4. Scan** screen, click **Next**.

6. Read the security code from your Google Authenticator app and enter it in the **Enter Code Received** field on the step 5. Verify screen, as shown in *Figure 89: Register Google Authenticator – Entering Security Code*. Then, click **Add Device**.

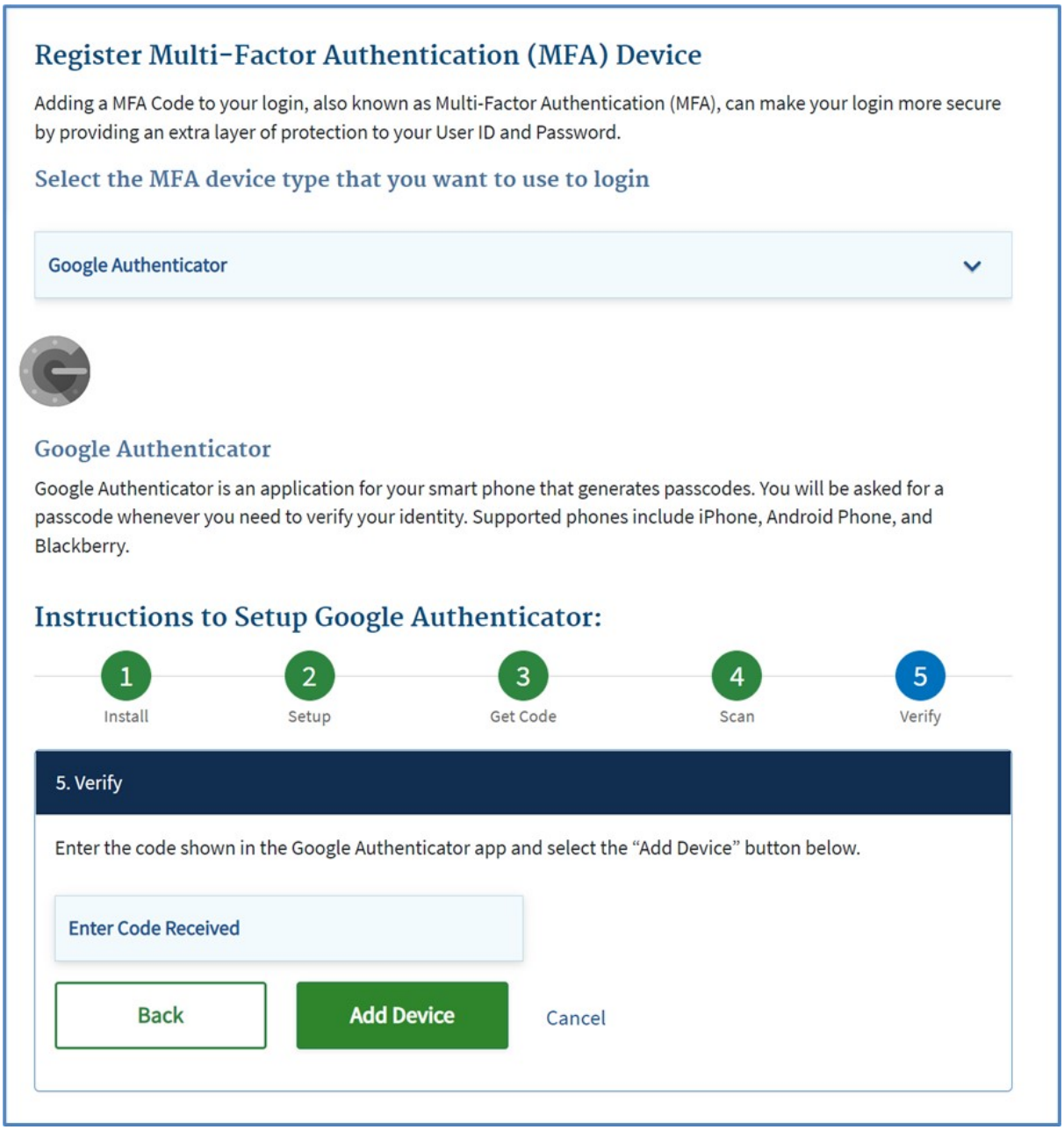

Figure 89: Register Google Authenticator – Entering Security Code

You will receive a confirmation that the changes to your profile were submitted successfully, as shown in *Figure 90: Register MFA Device – Success Message*.

Figure 90: Register MFA Device – Success Message

The Google Authenticator device is added to the list of available devices with "Active" status and one action: Remove, as shown in *Figure 91: Manage/View Available Devices – Google Authenticator MFA Added in Active Status*.
Your registration of the MFA device is now complete, and you will receive an email notification indicating that you successfully registered the MFA device.

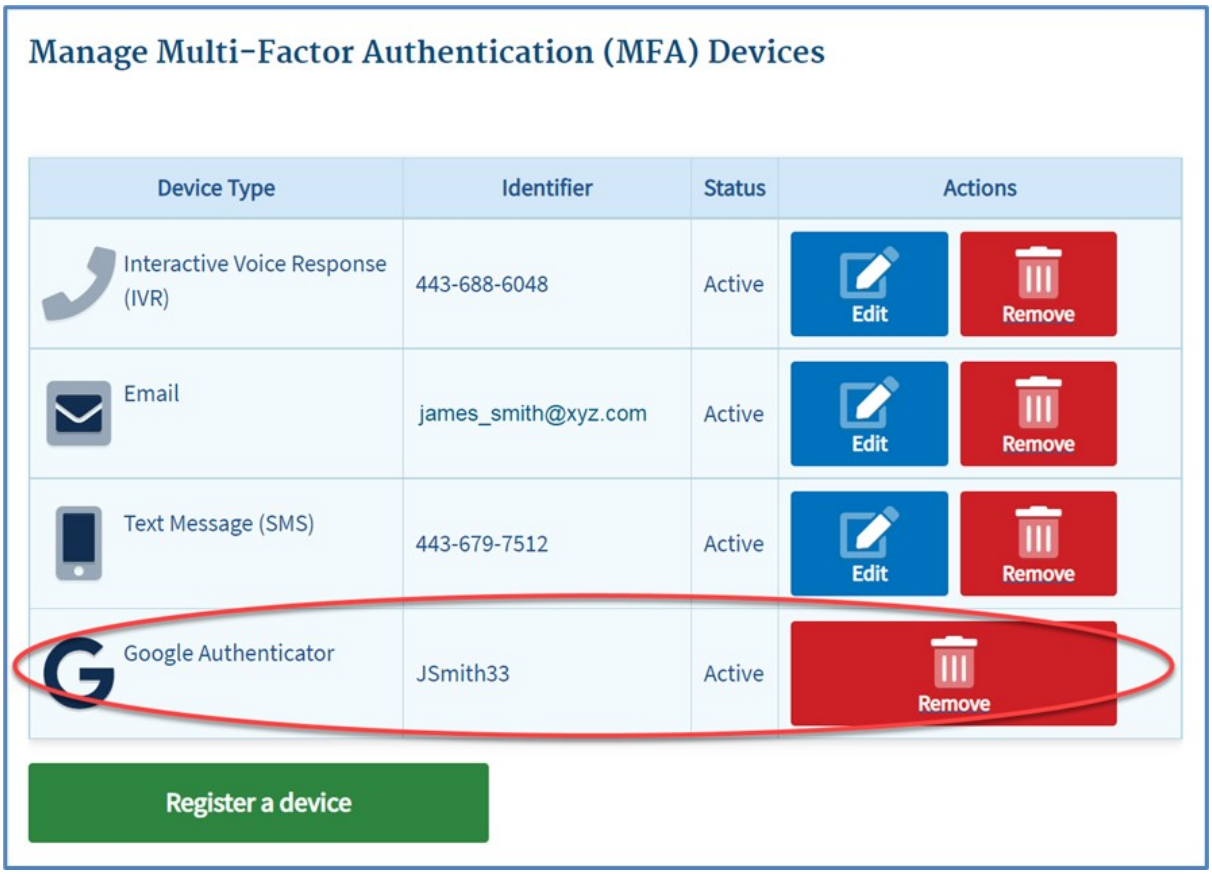

Figure 91: Manage/View Available Devices – Google Authenticator MFA Added in Active Status

8.6.5. Register Okta Verify MFA Device

1. If you select **Okta Verify** as the MFA device type, read the information under the **Okta Verify** drop-down, as shown in *Figure 92: Register Okta Verify – Start Setup*. If Okta Verify is not installed on your phone, then use your phone's application store to find and install the app. Then, click **Next**.

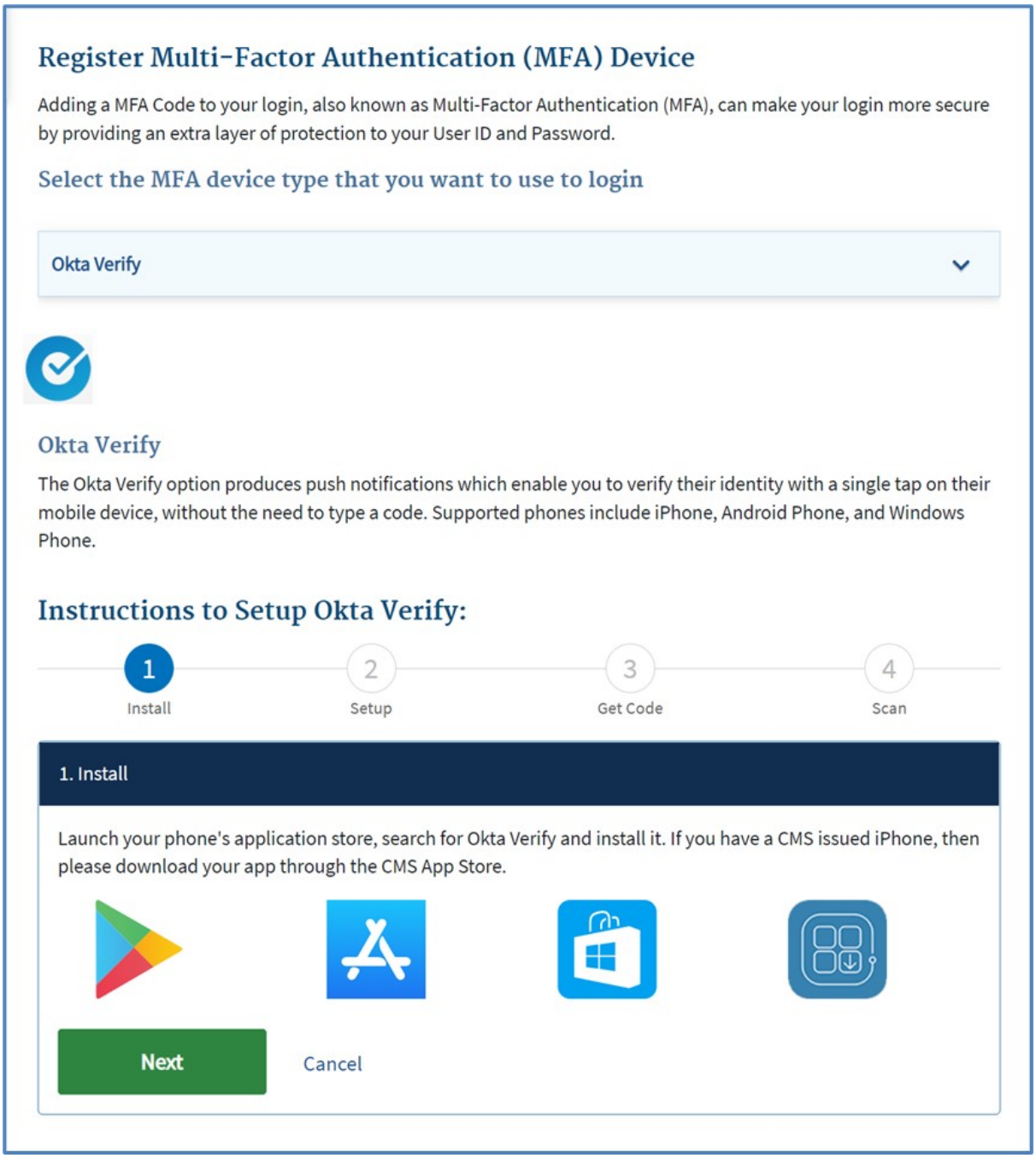

Figure 92: Register Okta Verify – Start Setup

2. In the **step 2. Setup** screen, click **Next**.
3. In the **step 3. Get Code** screen, click the **Register Device** button to generate a barcode. A barcode appears in the **step 4. Scan** screen, as shown in *Figure 93: Register Okta Verify – Barcode Generated*.

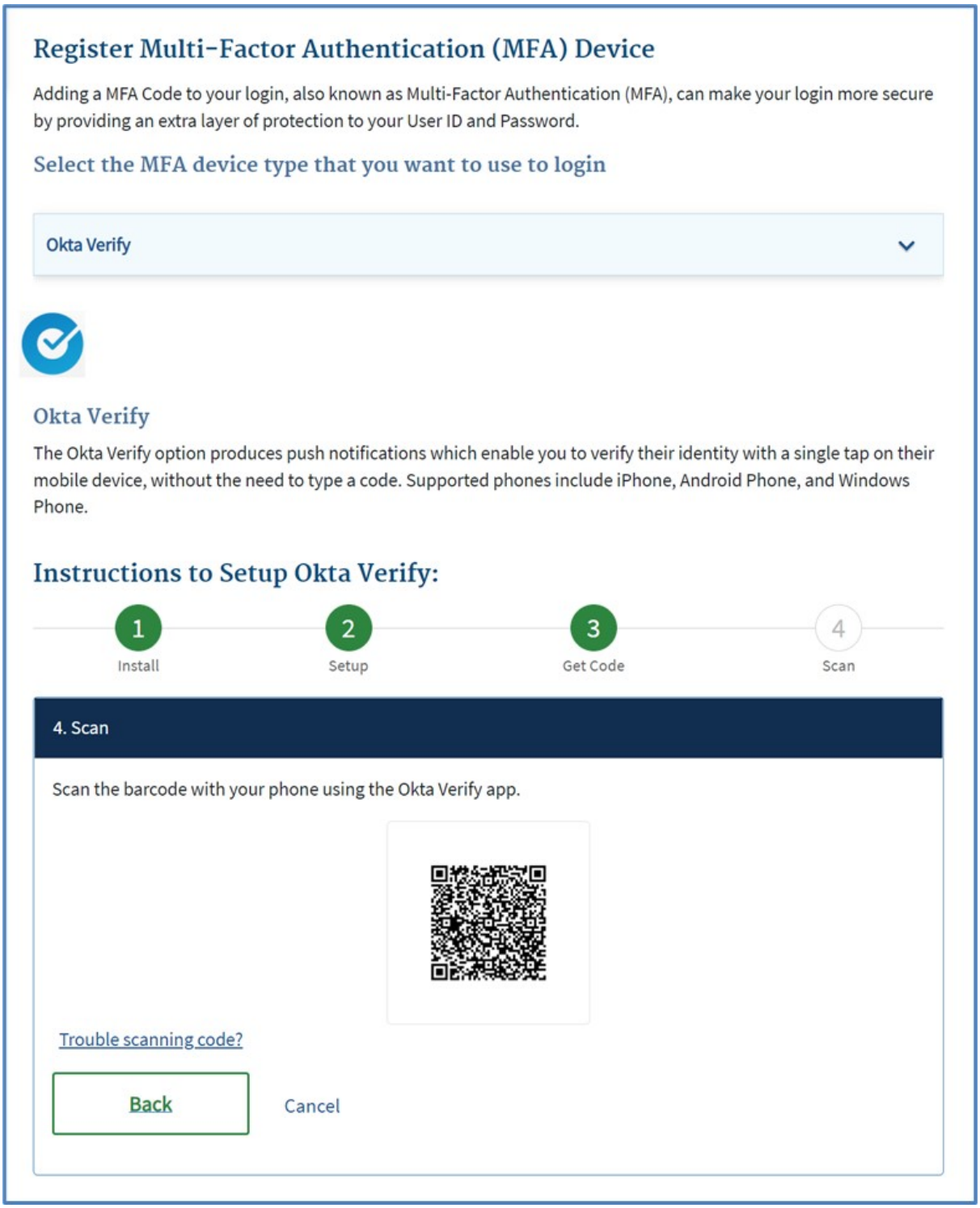

Figure 93: Register Okta Verify – Barcode Generated

4. Using a smart phone, open the Okta Verify app and scan the barcode. You will receive a confirmation that the changes to your profile were submitted successfully, as shown in *Figure 94: Register MFA Device – Success Message*.

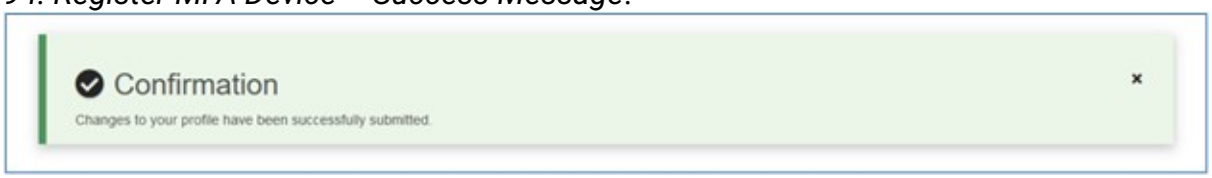

Figure 94: Register MFA Device – Success Message

Alternative Registration Using Activation Link

4. If you are having trouble scanning the barcode, click the **Trouble scanning code** link under the barcode, as shown in *Figure 93: Register Okta Verify – Barcode Generated*.

5. Enter the Phone Number of the mobile device in the **Enter Phone Number** field that will be used to obtain the activation link, as shown in *Figure 95: Register Okta Verify – Using Activation Link*. Then, click **Next**.

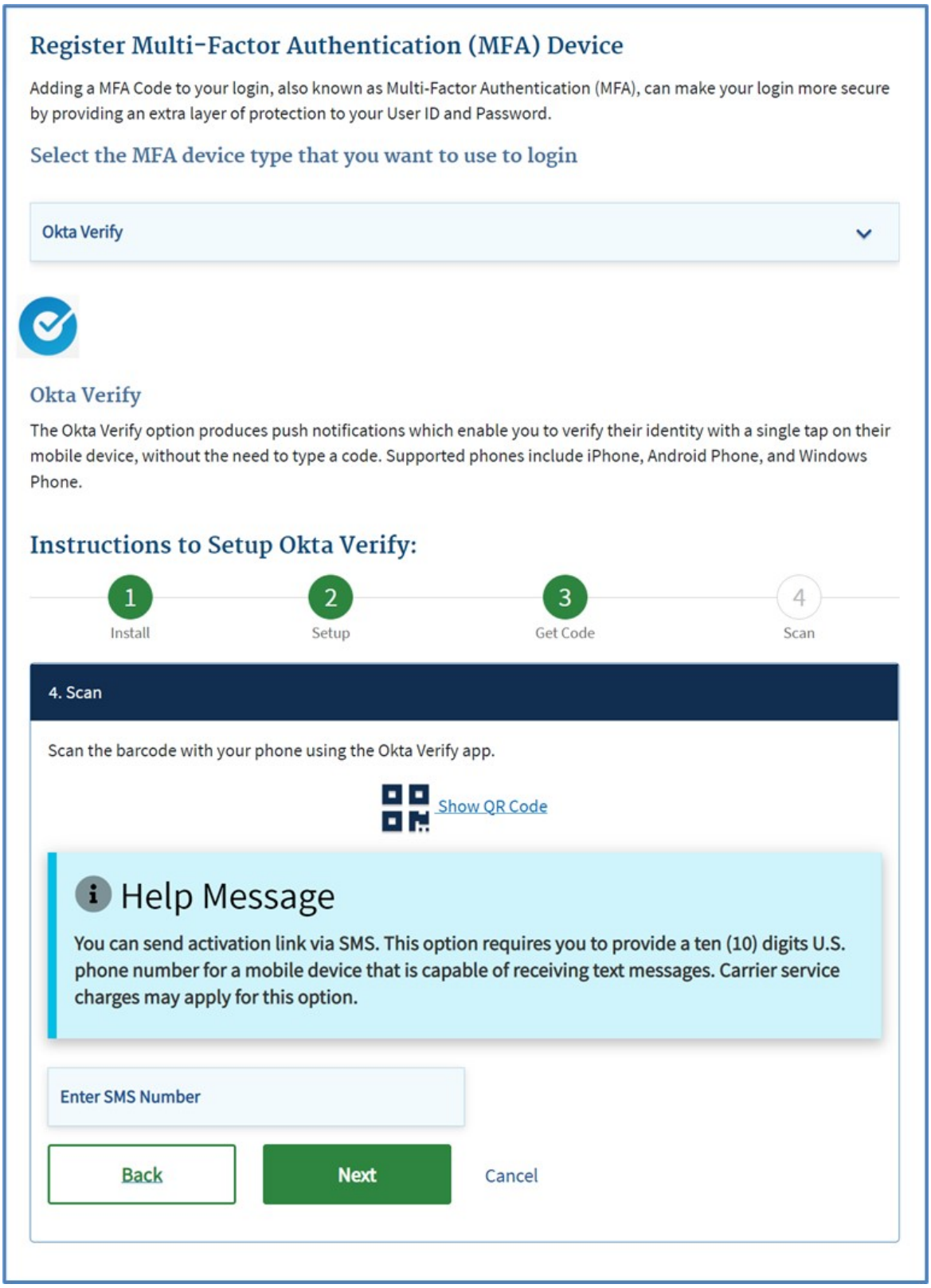

Figure 95: Register Okta Verify – Using Activation Link

You will see a confirmation message that an activation link has been sent to your mobile device.

6. On your mobile device, click the activation link to finish the enrollment process for Okta Verify registration.
You will receive a confirmation that the changes to your profile were submitted successfully, as shown in *Figure 94: Register MFA Device – Success Message*.

The Okta Verify device is added to the list of available devices with “Active” status and one action: Remove, as shown in *Figure 96: Manage/View Available Devices – Okta Verify MFA Added in Active Status*.
Your registration of the MFA device is now complete, and you will receive an email notification indicating that you successfully registered the MFA device.

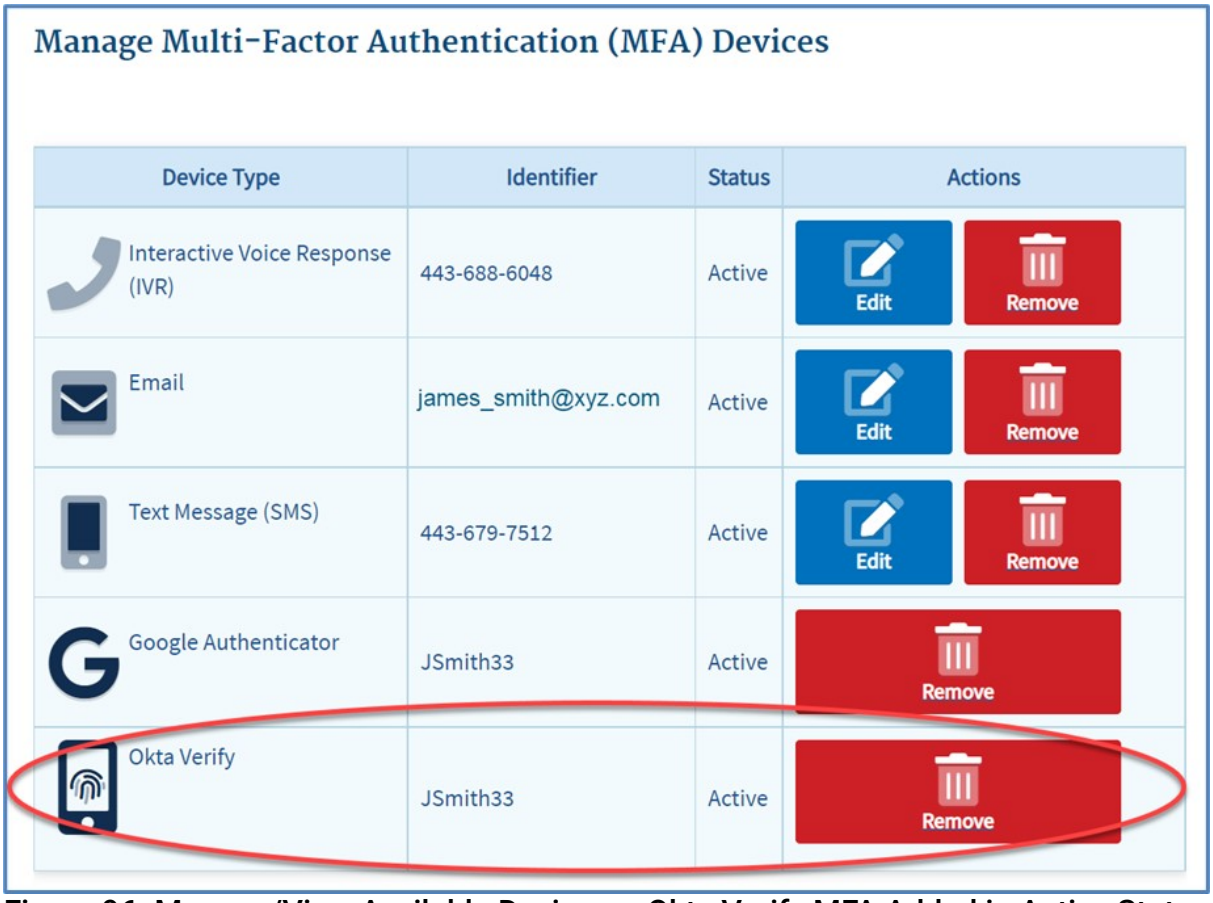

Figure 96: Manage/View Available Devices – Okta Verify MFA Added in Active Status

8.6.6. Register YubiKey MFA Device

Note

This MFA device is only available to users of certain applications.

1. If you select **YubiKey** as the MFA device type, read the information under the **YubiKey** drop-down, as shown in *Figure 97: Register YubiKey*.

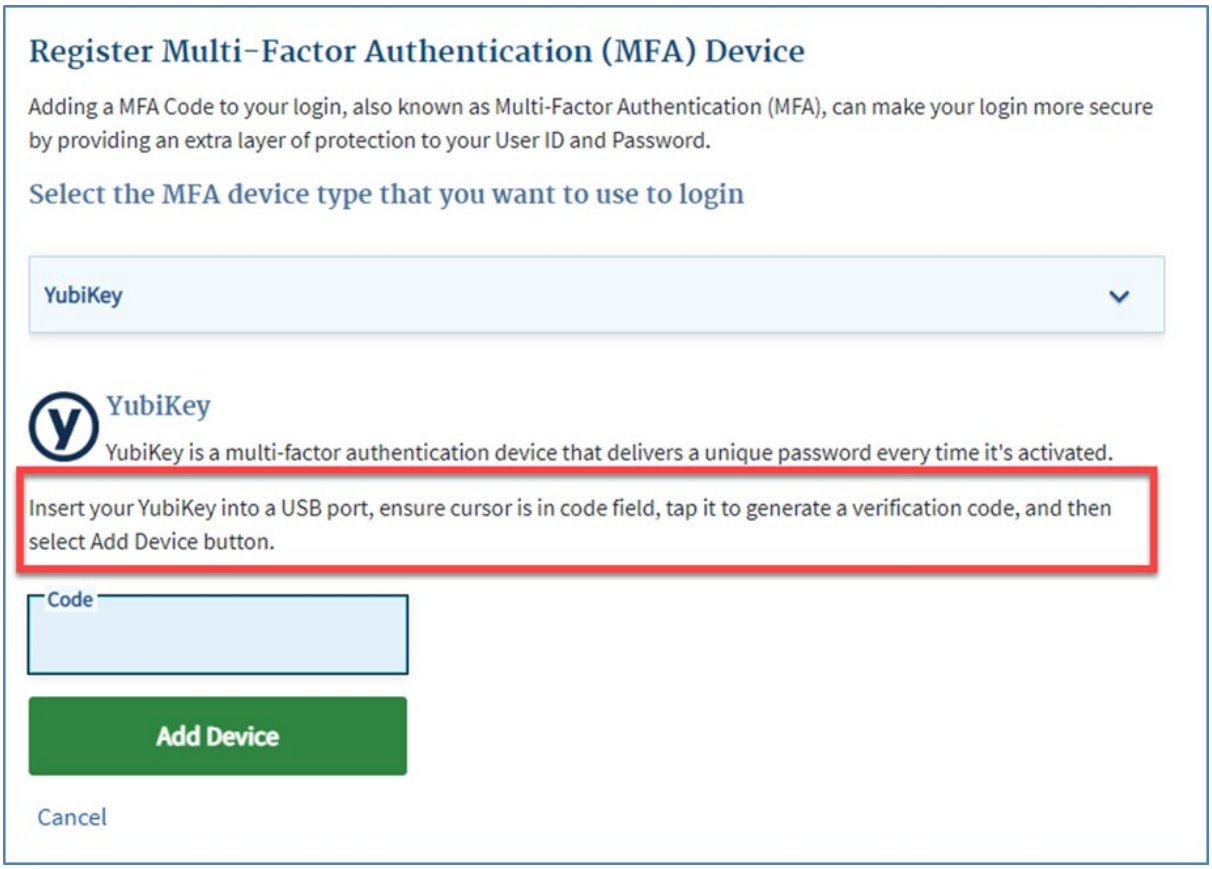

Figure 97: Register YubiKey

2. Insert your YubiKey device into a USB port, place the cursor in the **Code** field, and then tap it to generate a security code.
   The Code field is populated with a security code, as shown in *Figure 98: Register YubiKey – Code Field Populated with Security Code*.

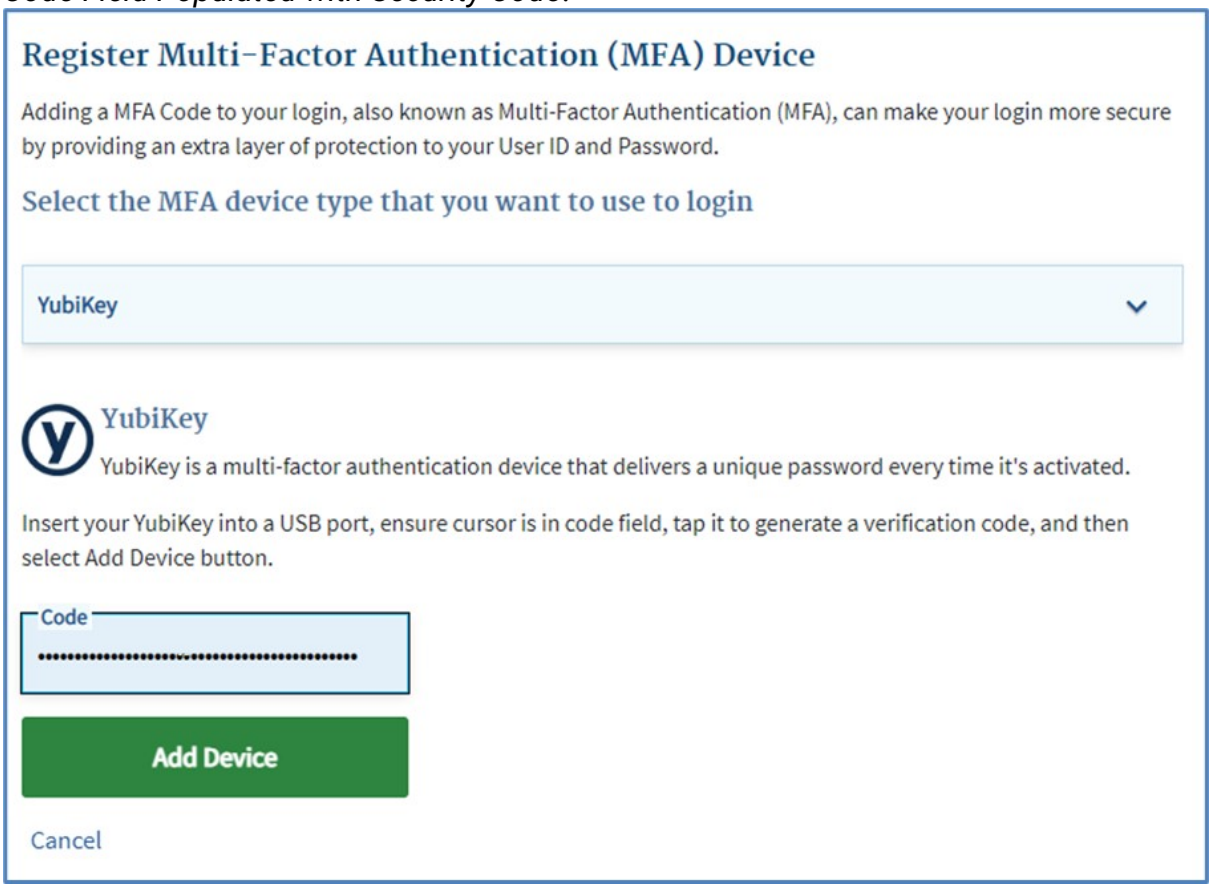

Figure 98: Register YubiKey – Code Field Populated with Security Code

3. Click **Add Device**.

You will receive a confirmation that the changes to your profile were submitted successfully, as shown in *Figure 99: Register MFA Device – Success Message*.

Figure 99: Register MFA Device – Success Message

The YubiKey device is added to the list of available devices with "Active" status and one action: Remove, as shown in *Figure 100: Manage/View Available Devices – YubiKey MFA Added in Active Status*.
Your registration of the MFA device is now complete, and you will receive an email notification indicating that you successfully registered the MFA device.

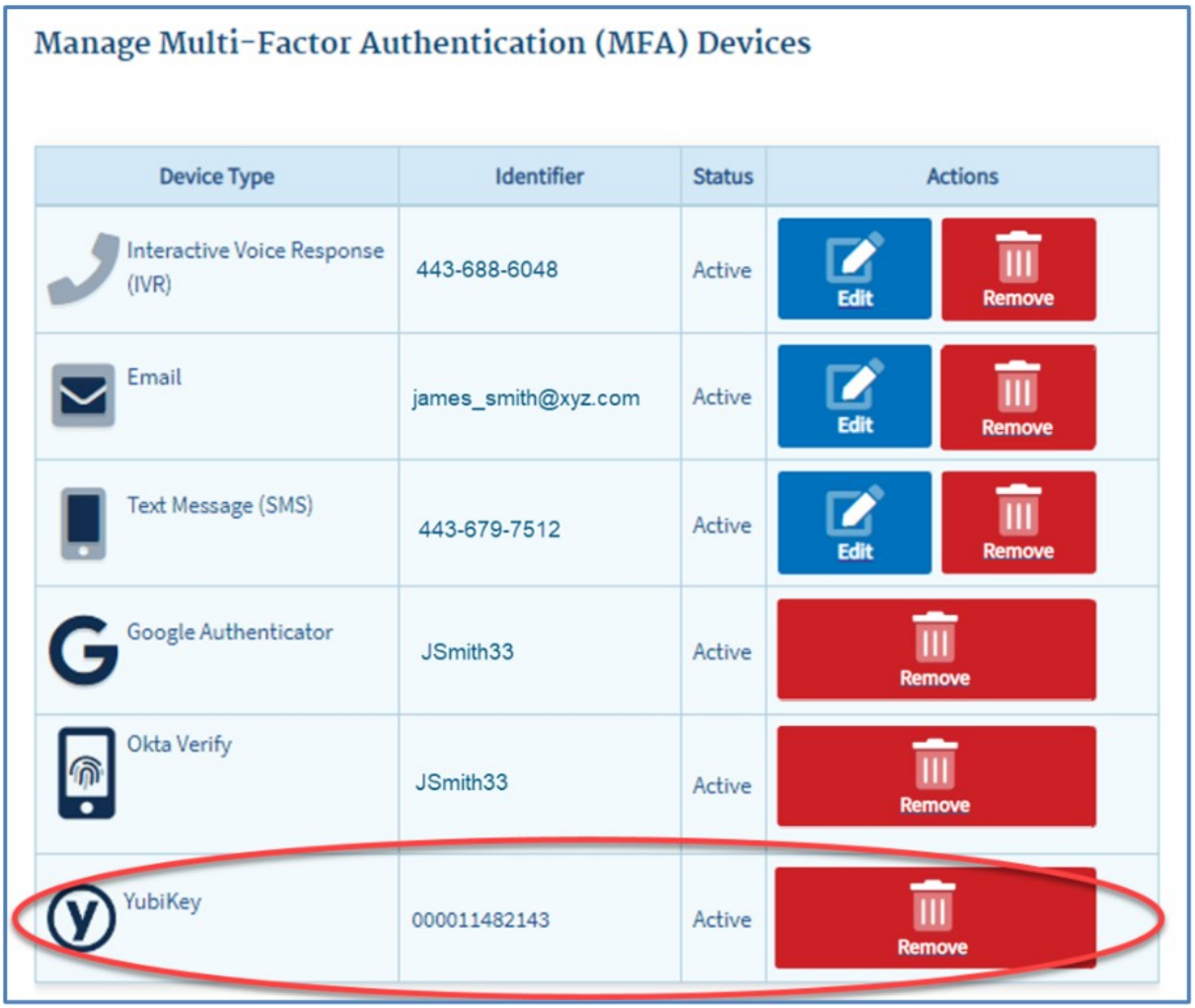

Figure 100: Manage/View Available Devices – YubiKey MFA Added in Active Status

8.6.7. Editing MFA Device

Note

Google Authenticator, YubiKey, and Okta Verify cannot be edited. They can only be registered or removed.

To edit a device for MFA, please follow each step listed below unless otherwise noted.

1. Navigate to the CMS Enterprise Portal public home page.

2. Login using your user ID and password.

The CMS Enterprise Portal **My Portal** page is displayed, as shown in *Figure 59: My Portal Page – My Profile Drop-down*.

3. Select the down arrow icon that appears next to your name at the top of page. Then select **My Profile** from the drop-down list to continue.
   The **My Profile** page displays, as shown in *Figure 60: View Profile*.

4. Select **Manage MFA Devices** in the left pane, as shown in *Figure 71: Manage MFA Devices*.
   A list of registered MFA devices is displayed, as shown in *Figure 101: Registered MFA Devices*.

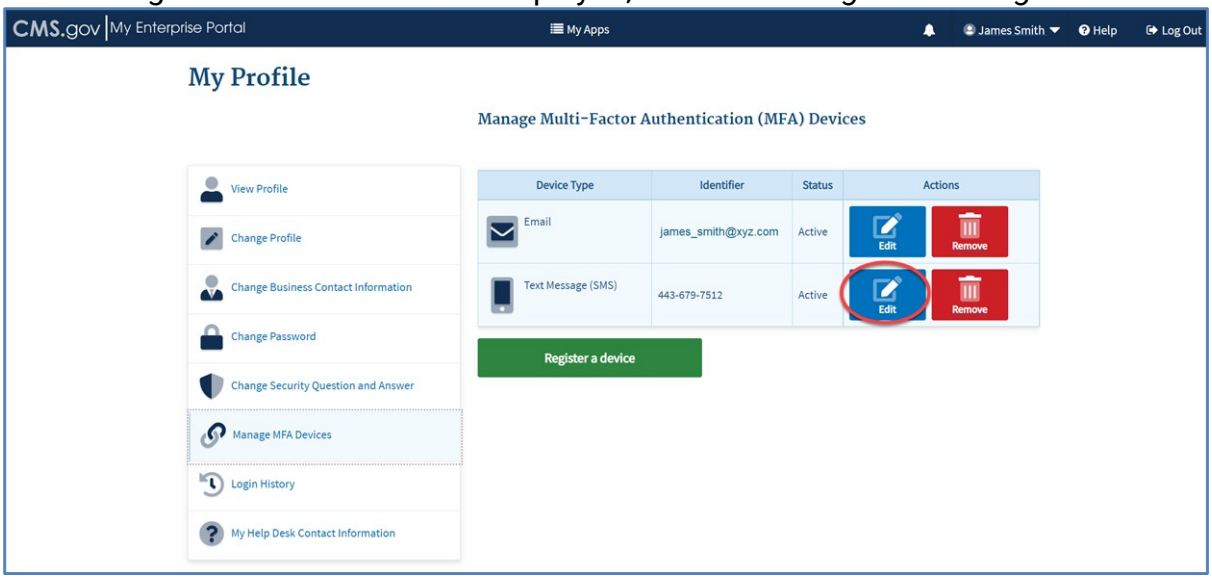

Figure 101: Registered MFA Devices

5. Click on the **Edit** button next to the registered device type you want to edit.

If Email is the device type :

6. You will be redirected to the View Profile – Change Profile page where you may change the email address. *See Changing Your Profile* above.

If SMS or IVR is the device type :

6. Enter a new phone number of the device selected in the text field, as shown in *Figure 102: Edit MFA – Entering New Device*. For IVR, you can add an optional extension.

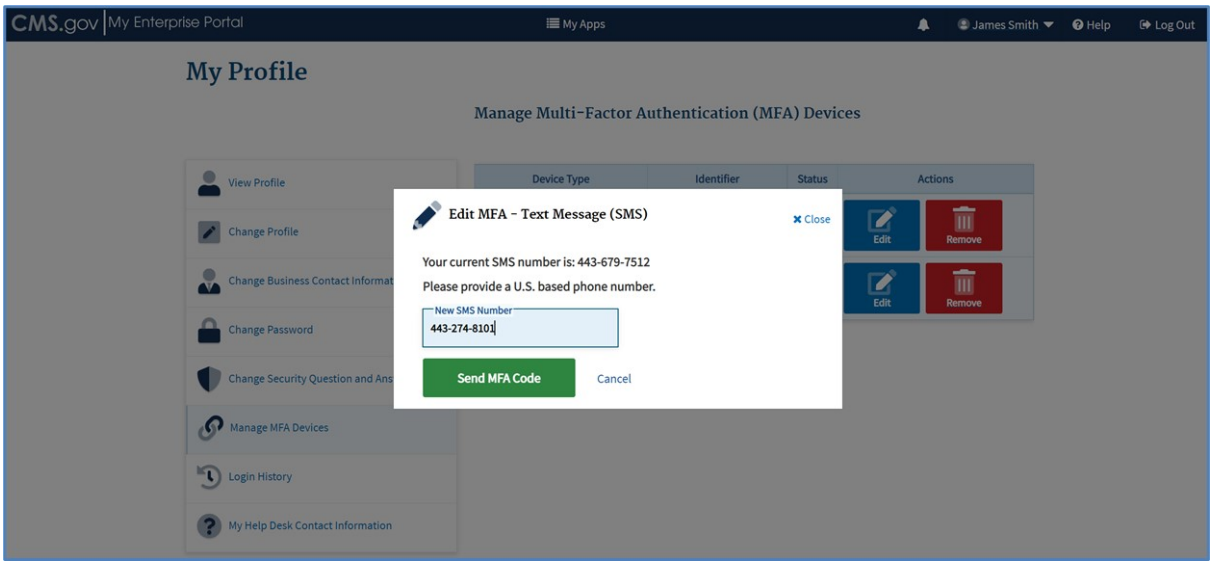

Figure 102: Edit MFA – Entering New Device

7. Click **Send MFA Code**.
You will receive confirmation that the MFA code has been sent to your MFA device, as shown in *Figure 103: Edit MFA – Entering Security Code*.

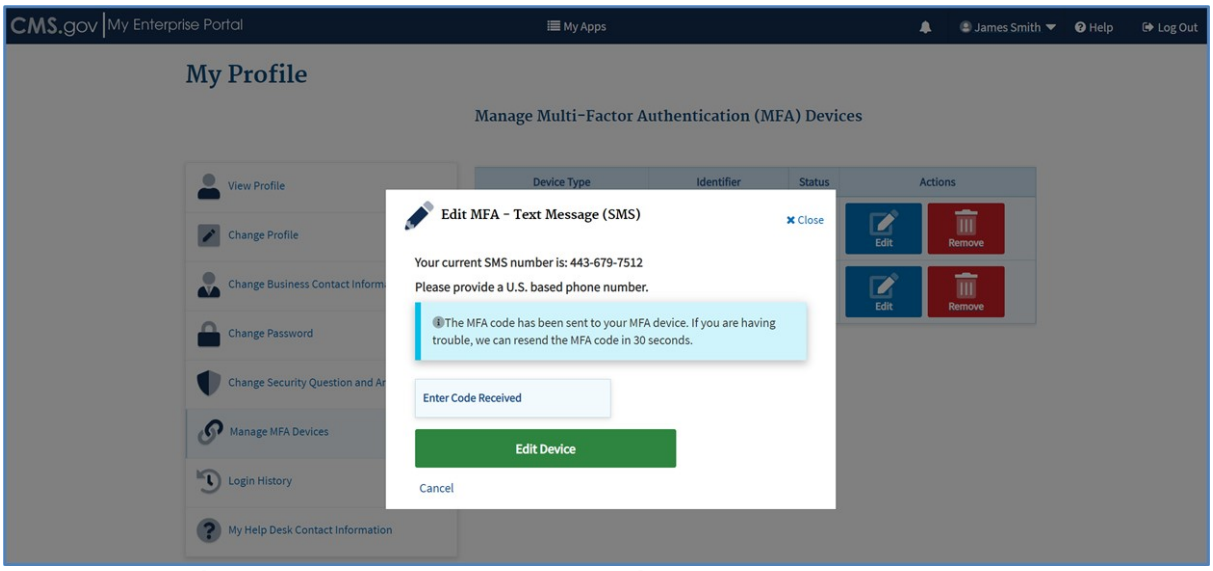

Figure 103: Edit MFA – Entering Security Code

8. Enter the security code you received in the **Enter Code Received** field. Then, click **Edit Device**.
You will receive a confirmation that the changes to your profile were submitted successfully, as shown in *Figure 104: Edit MFA – Success Message*.

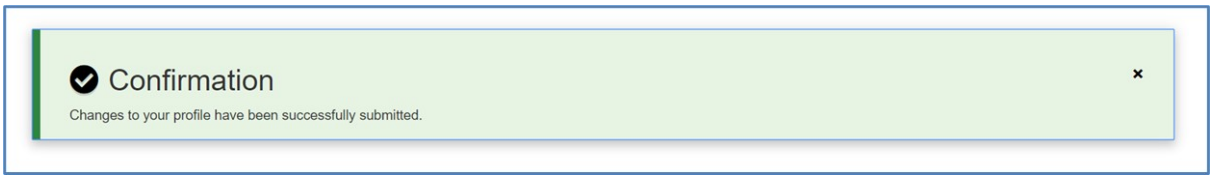

Figure 104: Edit MFA – Success Message

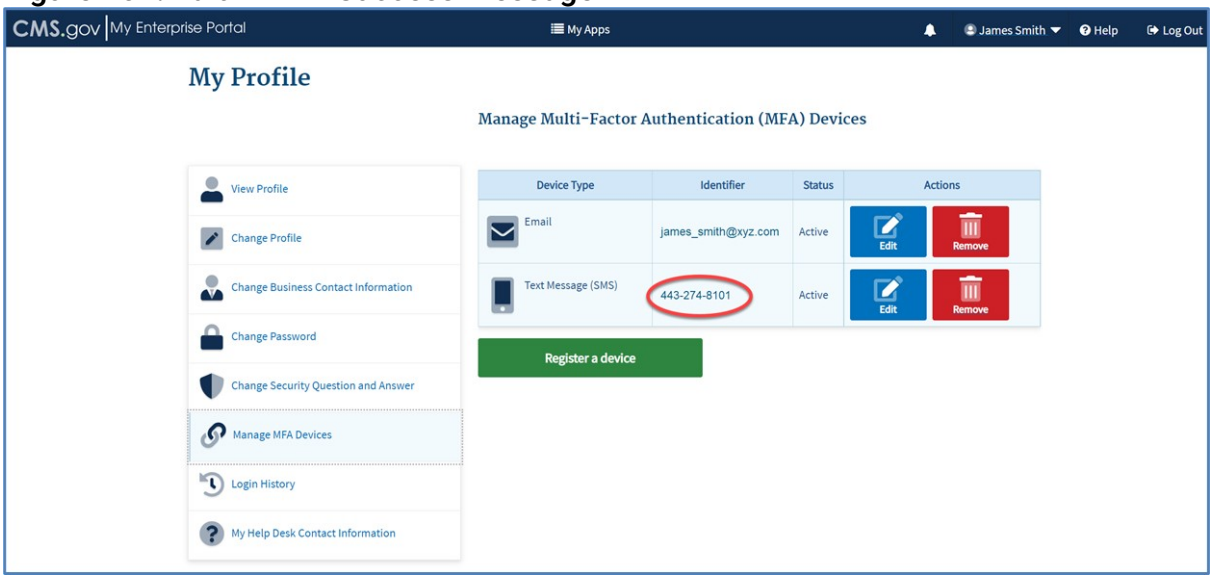

Figure 105: Edit MFA – Edited Device

Note

You will receive an email notification indicating that you successfully registered the MFA device.

8.6.8. Activating MFA Device

Note

Only Email, SMS or IVR MFA device in “Pending” status can be activated. A “Pending” state occurs when the user selects Cancel instead of entering the security code at the time of

registering the SMS or IVR device.

To activate a device for MFA, please follow each step listed below unless otherwise noted.

1. Navigate to the CMS Enterprise Portal public home page.

2. Login using your user ID and password.
   The CMS Enterprise Portal **My Portal** page is displayed, as shown in *Figure 59: My Portal Page – My Profile Drop-down*.

3. Select the down arrow icon that appears next to your name at the top of page. Then select **My Profile** from the drop-down list to continue.
   The **My Profile** page displays, as shown in *Figure 60: View Profile*.

4. Select **Manage MFA Devices** in the left pane, as shown in *Figure 71: Manage MFA Devices*.
   A list of registered MFA devices is displayed, as shown in *Figure 106: Registered MFA Devices*.

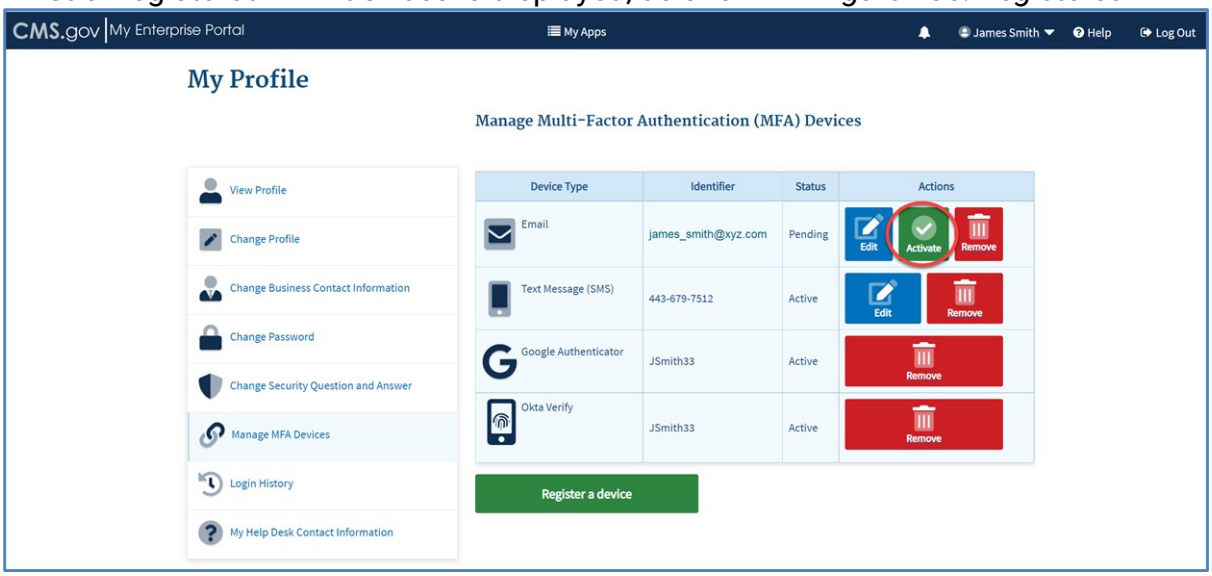

Figure 106: Registered MFA Devices

5. Click on **Activate** next to the registered device type you want to activate, as shown in *Figure 106: Registered MFA Devices*.
   The Activate modal dialog box displays, as shown in *Figure 107: Activate MFA – Sending Security Code*.

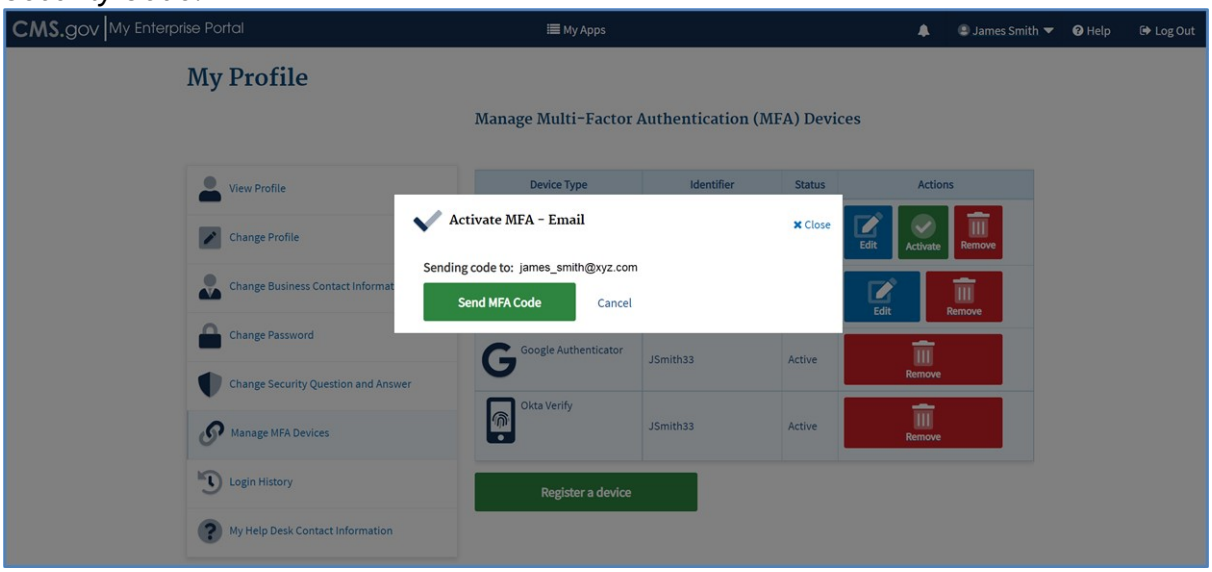

Figure 107: Activate MFA – Sending Security Code

6. Click **Send MFA Code**.
   You will receive confirmation that the MFA code has been sent to your MFA device, as shown

in *Figure 108: Activate MFA – Entering Security Code*.

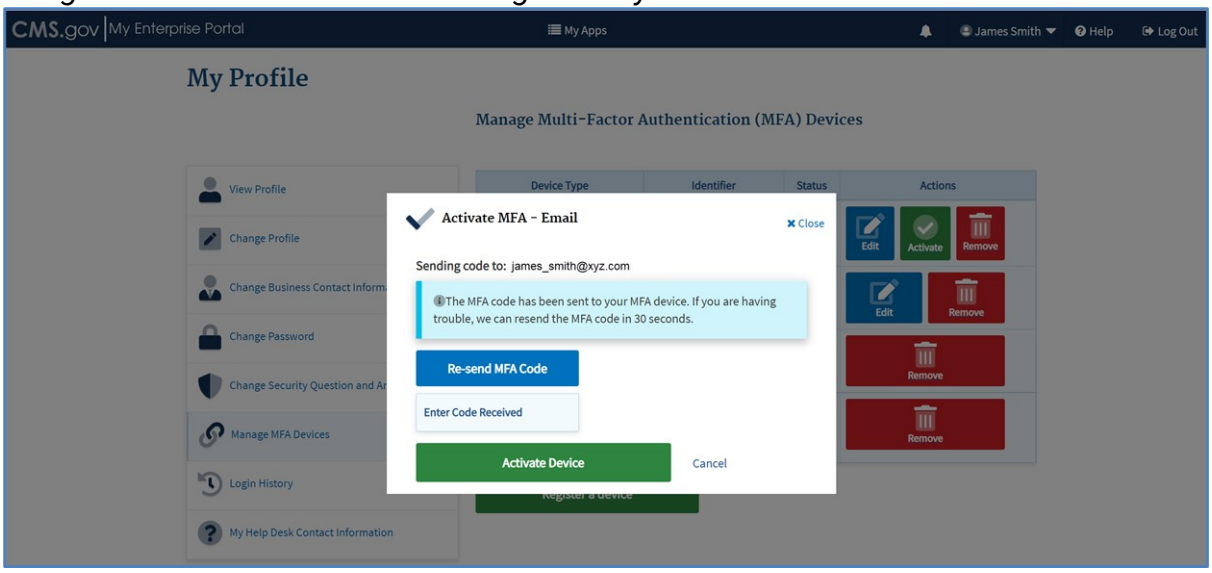

Figure 108: Activate MFA – Entering Security Code

7. Enter the security code you received in the **Enter Code Received** field. Then, click **Activate Device**.
   You will receive a confirmation that the changes to your profile were submitted successfully, as shown in *Figure 109: Activate MFA – Success Message*.

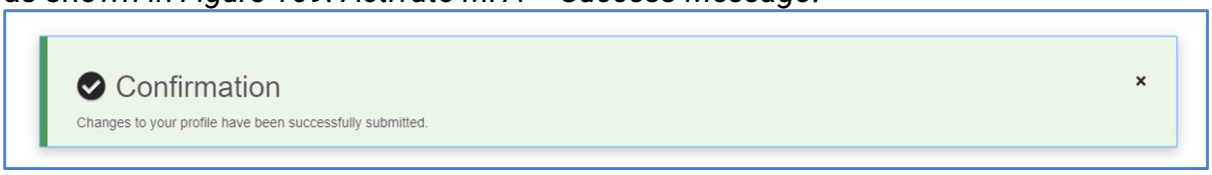

Figure 109: Activate MFA – Success Message

The selected device is activated and the **Activate** button will be removed from the View MFA Devices page, as shown in *Figure 110: Activate MFA – Activate Button Removed*.

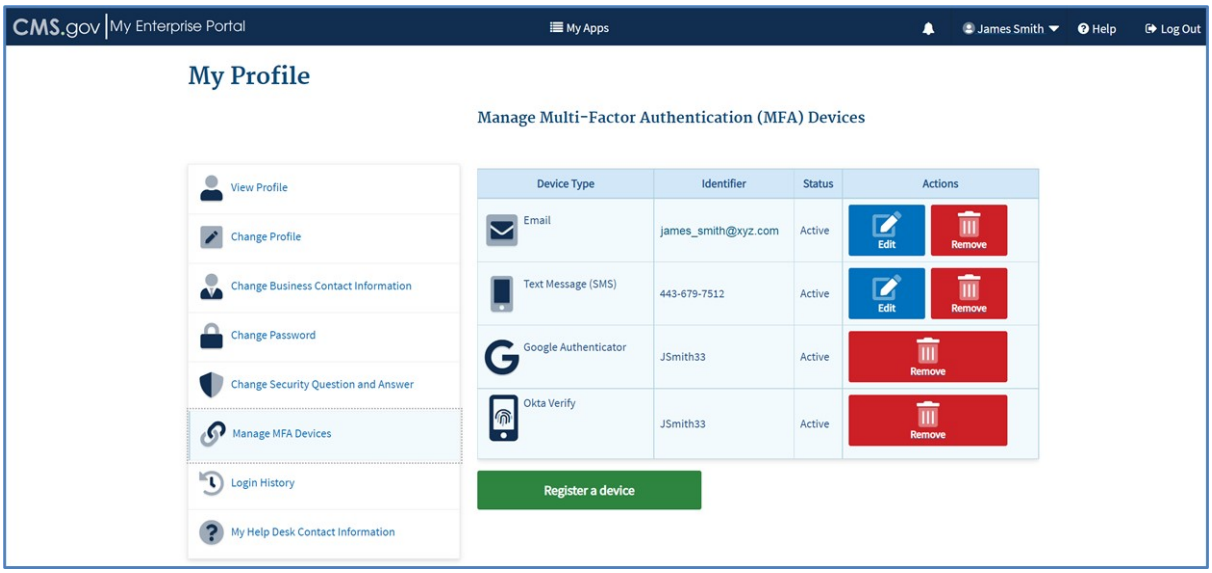

Figure 110: Activate MFA – Activate Button Removed

Note

You will receive an email notification indicating that you successfully registered the MFA device.

8.6.9. Removing MFA Device

To remove an MFA device, please follow each step listed below unless otherwise noted.

1. Navigate to the CMS Enterprise Portal public home page.

2. Login using your user ID and password.
   The CMS Enterprise Portal **My Portal** page is displayed, as shown in *Figure 59: My Portal Page – My Profile Drop-down*.

3. Select the down arrow icon that appears next to your name at the top of page. Then select **My Profile** from the drop-down list to continue.
   The **My Profile** page displays, as shown in *Figure 60: View Profile*.

4. Select **Manage MFA Devices** in the left pane, as shown in *Figure 71: Manage MFA Devices*.
   A list of registered MFA devices is displayed.

5. Click on **Remove** next to the registered device type you want to remove.

6. Click on **Confirm** in the modal dialog box, as shown in *Figure 111: Remove MFA Device Confirmation*.

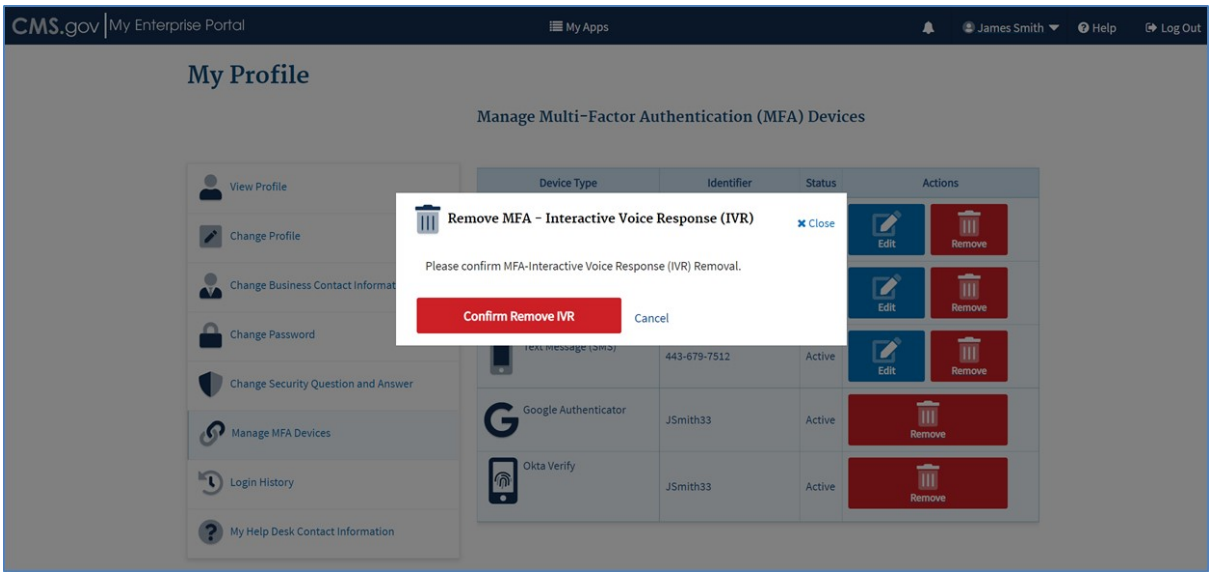

Figure 111: Remove MFA Device Confirmation

You will receive a confirmation that the changes to your profile were submitted successfully, as shown in *Figure 112: Remove MFA Device – Success Message*.

Figure 112: Remove MFA Device – Success Message

The selected device will be removed from the list of available devices.

Note

You will receive an email notification indicating that you successfully removed the MFA device.

8.7. Viewing Login History

The following are the instructions on how to use the 'Login History" feature to review you past successful and failed logins in order to identify suspicious activities with your account.

1. Navigate to the CMS Enterprise Portal public home page.

2. Login using your user ID and password.
   The CMS Enterprise Portal **My Portal** page is displayed, as shown in *Figure 59: My Portal Page – My Profile Drop-down*.

3. Select the down arrow icon that appears next to your name at the top of page. Then select **My Profile** from the drop-down list to continue.
   The View Profile page displays, as shown in *Figure 60: View Profile*.

4. Select **Login History** in the left pane, as shown in Figure 113: Login History.

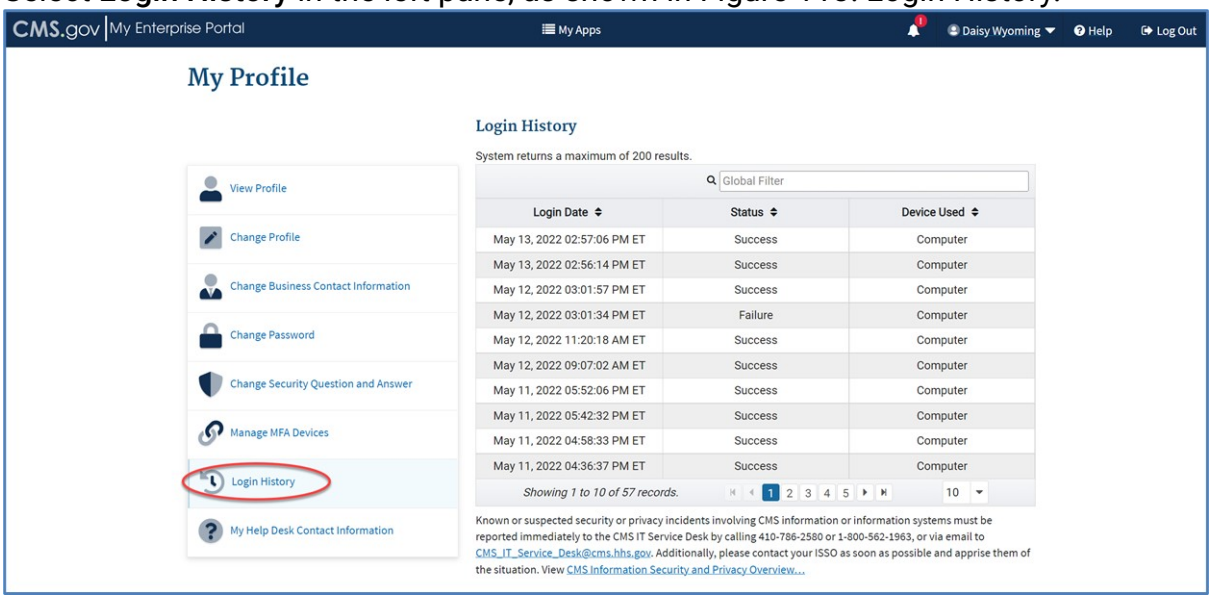

Figure 113: Login History

You can also get to the Login History page by selecting the **View Login History** link on the My Portal Landing page, as shown in *Figure 114: My Portal - Login History Link*.

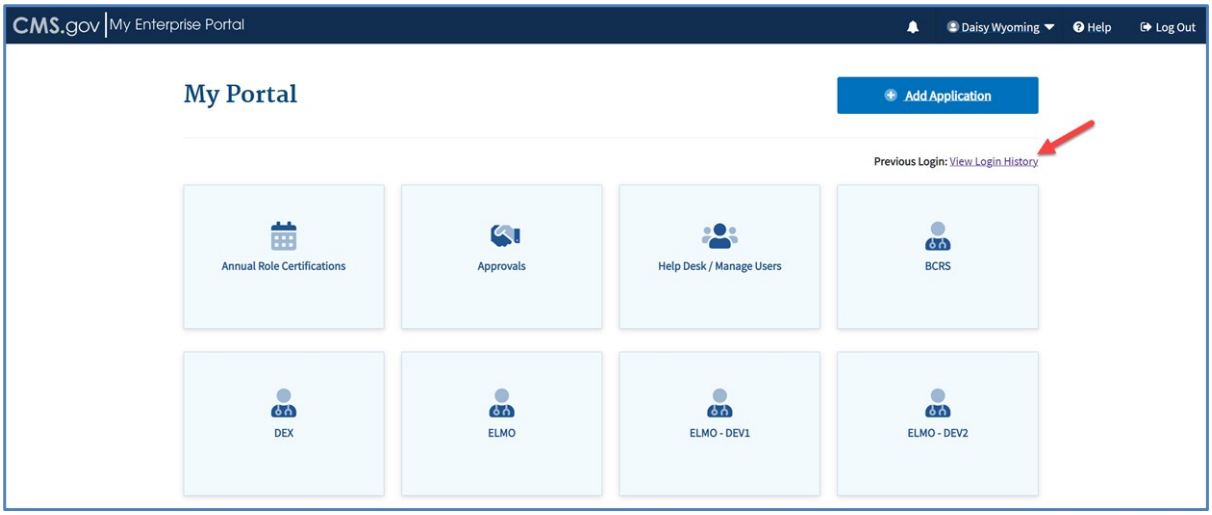

Figure 114: My Portal – Login History Link

8.8. Viewing My Help Desk Contact Information

The following are the instructions on how to view the My Help Desk Contact Information.

1. Navigate to the CMS Enterprise Portal public home page.

2. Login using your user ID and password.
   The CMS Enterprise Portal **My Portal** page is displayed, as shown in *Figure 59: My Portal Page – My Profile Drop-down*.

3. Select the down arrow icon that appears next to your name at the top of page. Then select **My Profile** from the drop-down list to continue.
   The View Profile page displays, as shown in *Figure 60: View Profile*.

4. Select **My Help Desk Contact Information** in the left pane, as shown in Figure 115: My Help Desk Contact Information.

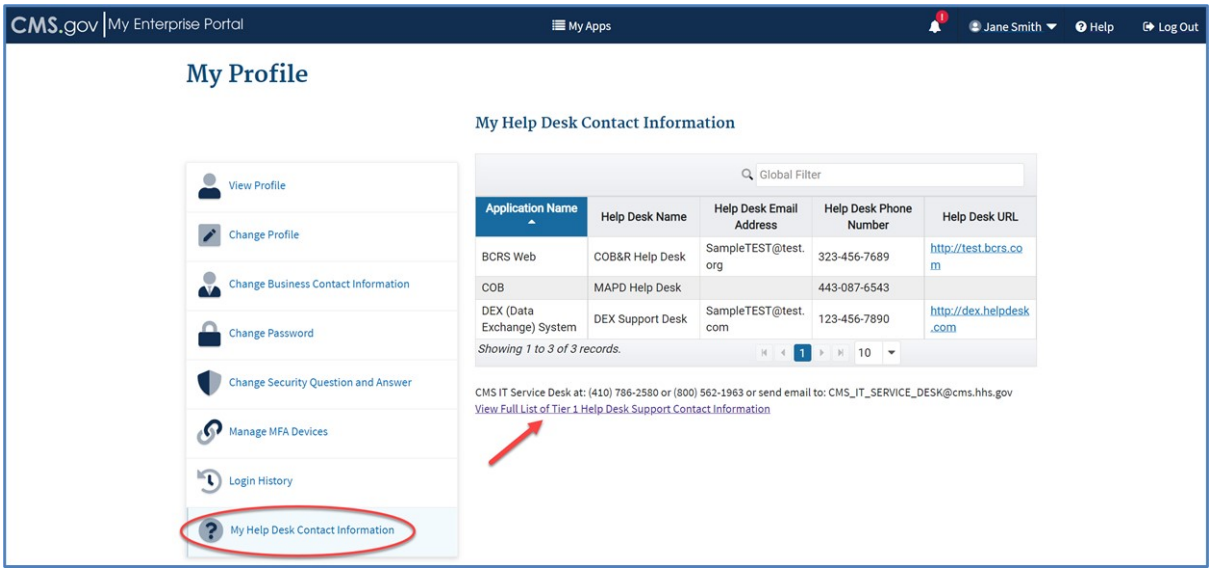

Figure 115: Login History

A paginated list of Help Desk contact information is displayed, as shown in *Figure 115: My Help Desk Contact Information*, for each application in which you have a role. The information displayed includes Application Name, Help Desk Name, Help Desk Email Address, Help Desk Phone Number, and Help Desk URL.This list can be sorted in the ascending or descending order of the Application Name. The Global Filter feature is also available and can be used to further refine the list if multiple rows are displayed. Clicking on the **View Full List of Tier 1 Help Desk Support Contact Information** link that appears in the message below the list allows you to view the Tier 1 Help Desk support information for all CMS applications.

9. Requesting Access to an Application

Applications hosted on the CMS Enterprise Portal may either be provisioned via the CMS Enterprise Portal system or via EUA. To access an application provisioned via CMS Enterprise Portal, users must request a role in that application from within the CMS Enterprise Portal system. To access an application provisioned via EUA, users must request the appropriate job codes from the EUA system. CMS Enterprise Portal users can only access or view the applications to which they have been granted access through the respective approved role request(s) or job code(s).

This section provides basic instructions on how to request access to an application and a Portal role or EUA job code.

Each application is different and may require you to enter or select information not indicated in the basic instructions provided in this section. The system prompts you to enter or select any additional information needed, based on the application and role you are requesting. In addition, the system will display help messages to assist you in completing your requests.

9.1. Add Application Button

Registered users can use the **Add Application** button or link to request access to a CMS Enterprise Portal application and a role within that application.

The **Add Application** button is available on the **My Portal** page, as shown in *Figure 116: Add Application Button on My Portal Page*.

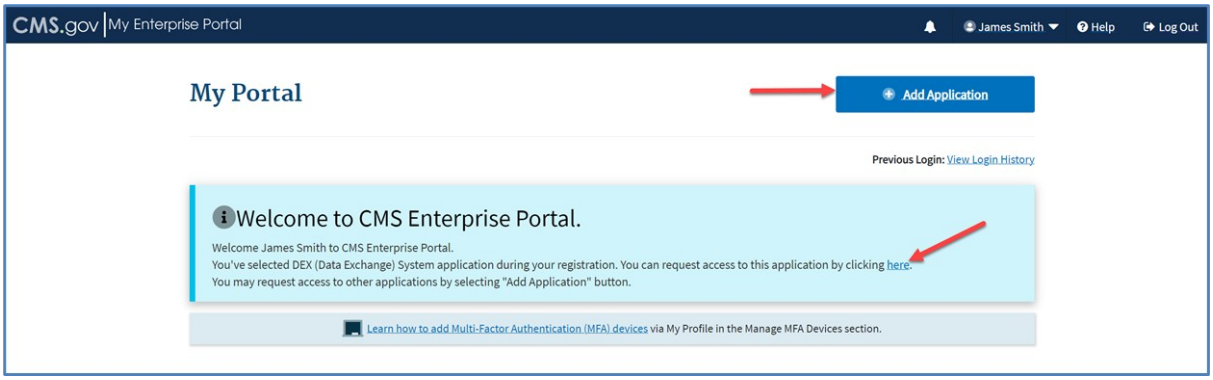

Figure 116: Add Application Button on My Portal Page

For the first-time users upon initial login, the **My Portal** page displays a Welcome message with a link to request access to the application that the user selected during registration, as shown in *Figure 116: Add Application Button on My Portal Page*.

The **Add Application** link is also present on the **My Access** page, as shown in *Figure 117: Add Application Link on My Access Page*.

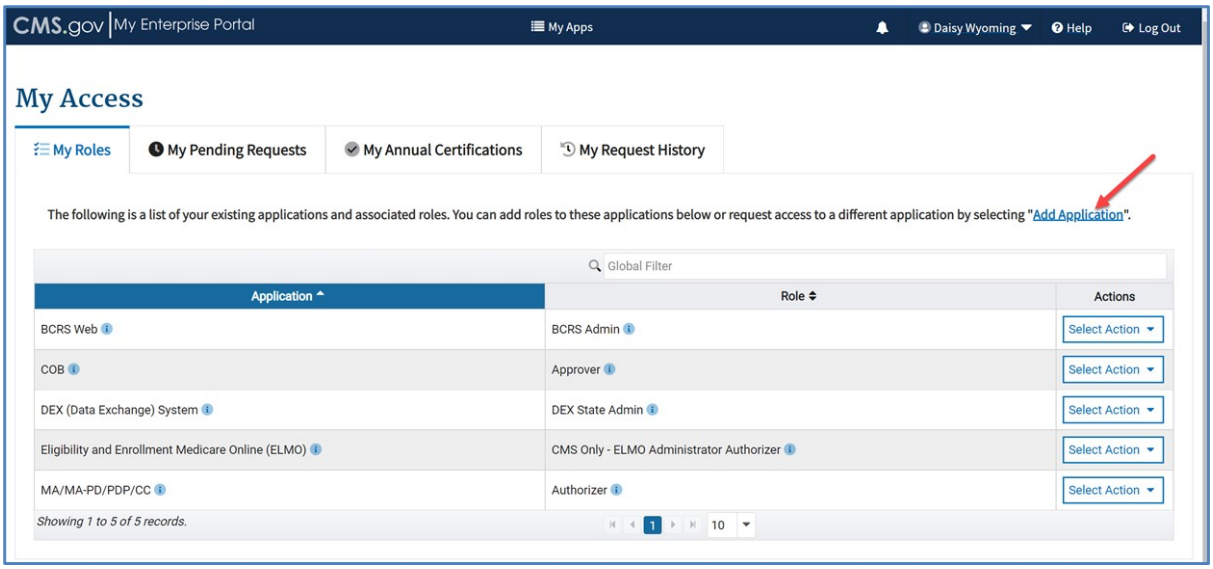

Figure 117: Add Application Link on My Access Page

Alternatively, the **Request Application Access** page can be accessed by clicking **My Apps** in the top navigation bar and then selecting **Add Application** under the **IDM** menu, as shown in *Figure 118: Accessing the Request Application Access Page via My Apps*.

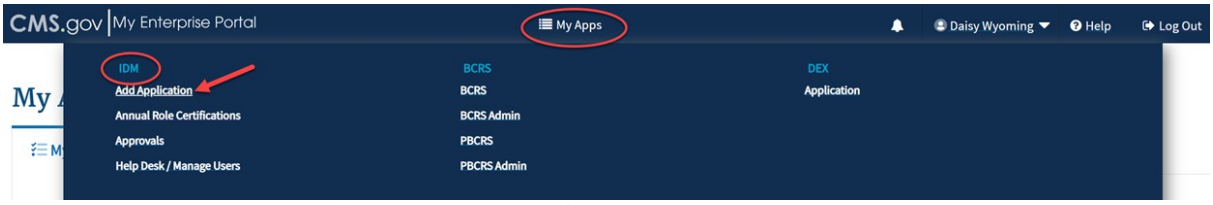

Figure 118: Accessing the Request Application Access Page via My Apps

Clicking the **Add Application** button or link takes you to the **Request Application Access** page, as shown in *Figure 119: Request Application Access Page*.

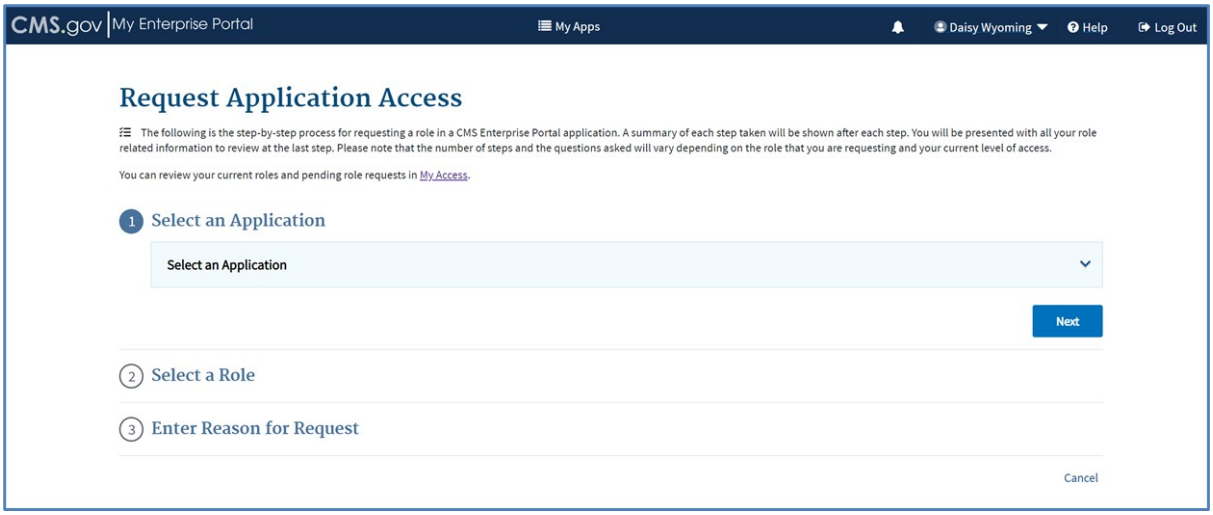

Figure 119: Request Application Access Page

9.2. My Access Page

The **My Access** page enables you to perform the following actions:

- Request access to any CMS application
- View a list of your existing applications and associated roles
- Add a role to an application you have access to

- Cancel a pending request
- Remove a role for an application you have access to
- View or modify role attributes
- View a list of pending role requests submitted for approval
- View a list of roles that require certification, have been certified or have been submitted for certification
- View all the past requests made for access to an application/role

The **My Access** page is accessed by selecting the **My Access** option from the name drop-down list in the top navigation bar, as shown in *Figure 120: Accessing the My Access Page via Name Drop-down*.

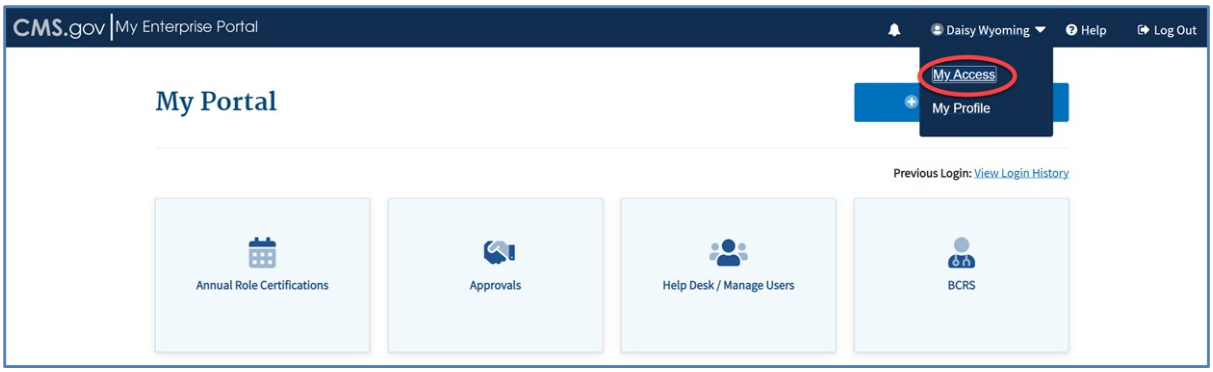

Figure 120: Accessing the My Access Page via Name Drop-down

The **My Access** page contains four tabs:

- **My Roles** – This default tab displays information for each application for which you have access including the existing roles you have been granted for the application, as shown in *Figure 121: My Roles Tab on My Access Page*.

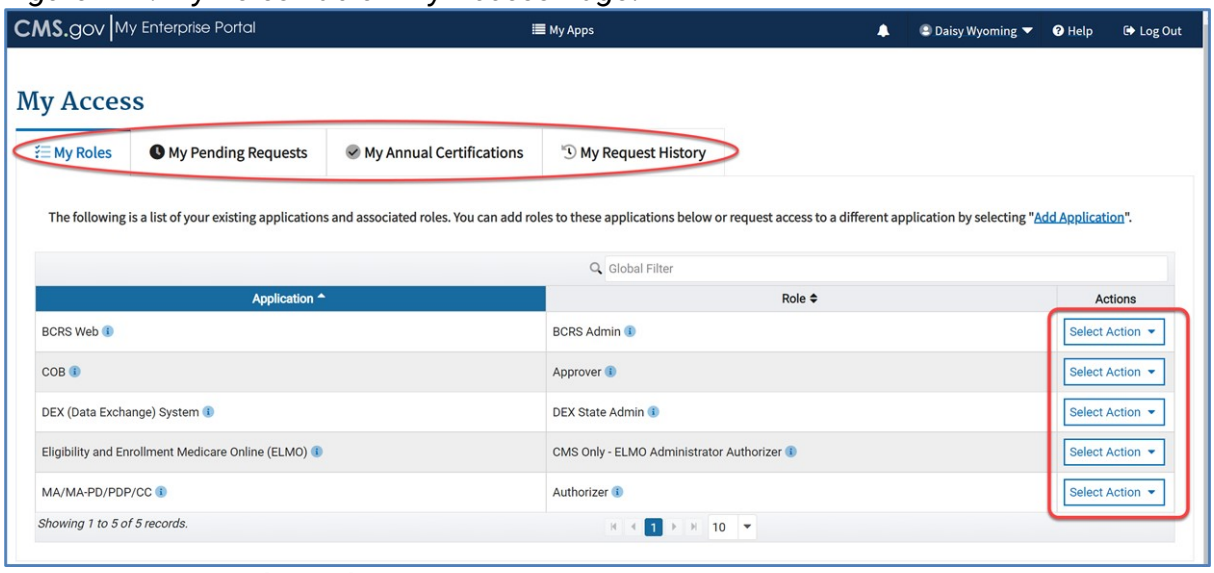

Figure 121: My Roles Tab on My Access Page

The **Select Action** drop-down, as shown in *Figure 121: My Roles Tab on My Access Page*, appears for each application for which you have access. You can select from the following options in the drop-down:

- Add Role – Directs you to the **Request Application Access** page to request an additional role for the application.
- Remove Role – Prompts you to confirm if you wish to remove the role from the application.
- View/Modify Role Details – Directs you to the **Role Details** page that displays additional role information with an option to modify this information, as shown in *Figure 122: Role Details*.

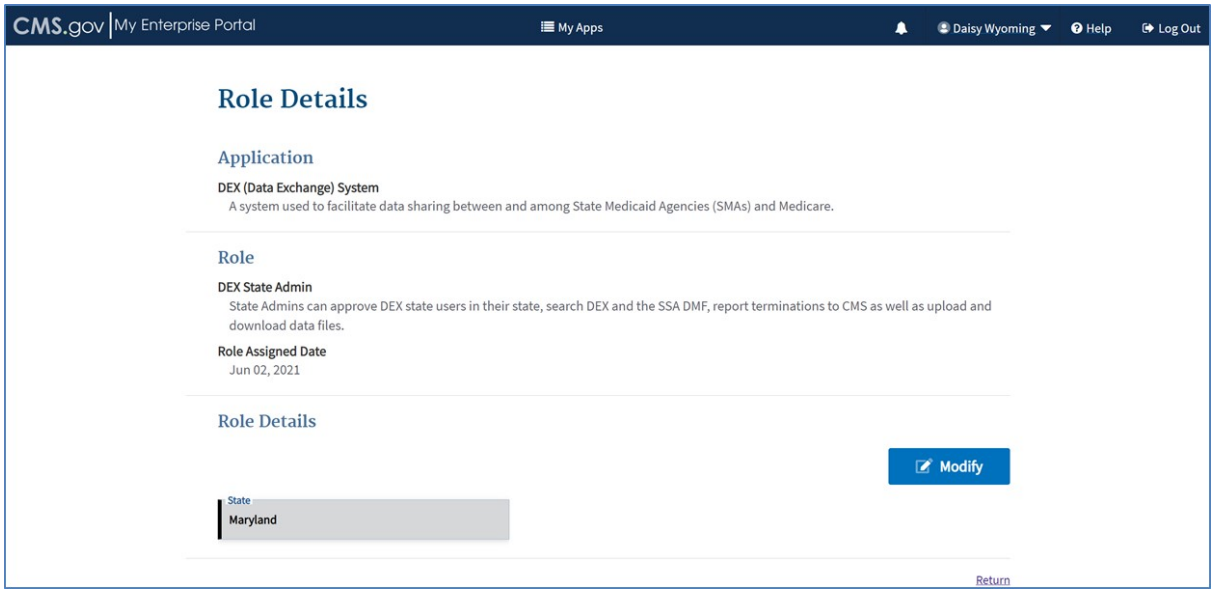

Figure 122: Role Details

- **My Pending Requests** – This tab lists the pending requests for application/role for which you have requested access. If you currently have pending requests, the page will display as shown in *Figure 123: My Pending Requests Tab on My Access Page*.

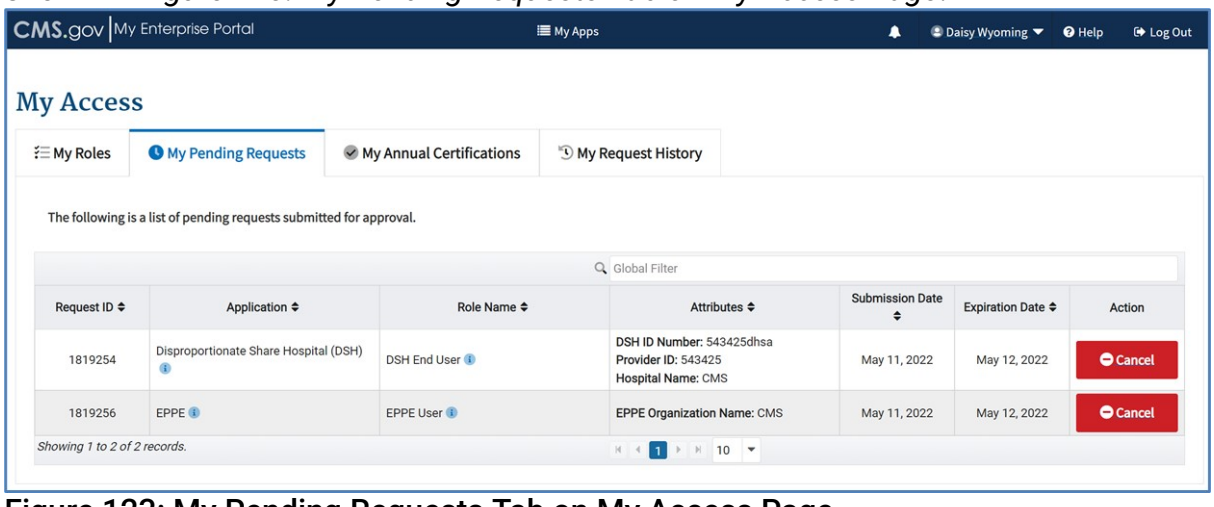

Figure 123: My Pending Requests Tab on My Access Page

- **My Annual Certifications** – This tab lists all the roles that you currently have access to that require certification, have been certified or have been submitted for certification, as shown in *Figure 124: My Annual Certifications Tab on My Access Page*.

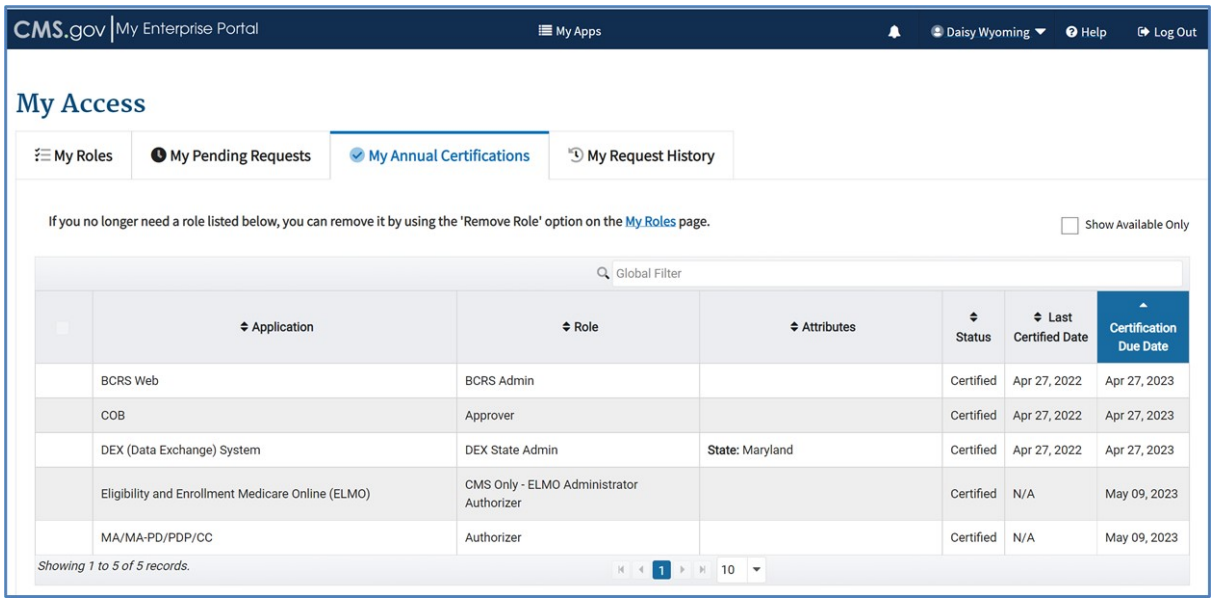

Figure 124: My Annual Certifications Tab on My Access Page

- **My Request History** – This tab lists all your requests for access to an application/role that have been approved, rejected, expired, revoked, or canceled, as shown in *Figure 125: My Request History Tab on My Access Page*.

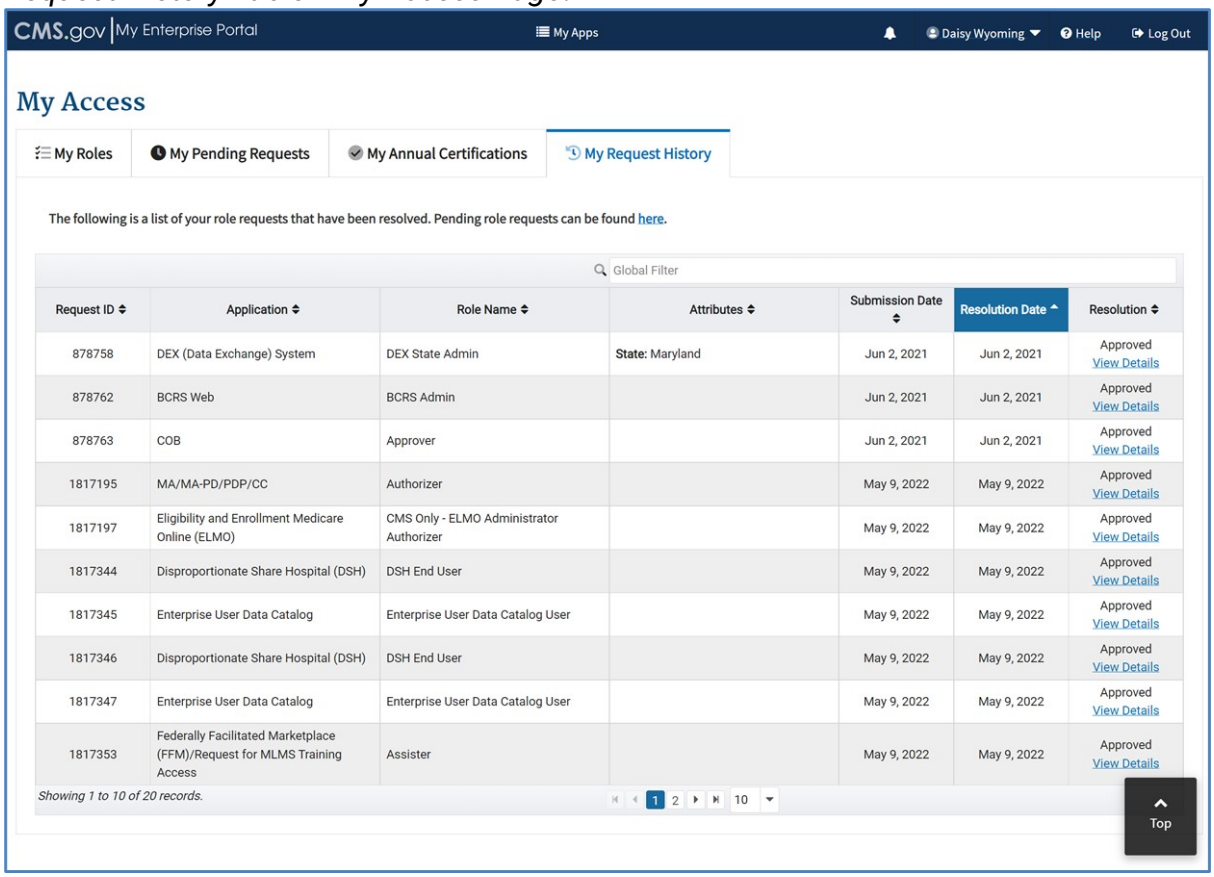

Figure 125: My Request History Tab on My Access Page

9.3. Requesting a Role

The following are the instructions on how to request a role in a CMS Enterprise Portal-provisioned application when you currently do not have any role in that application.

1. Navigate to the CMS Enterprise Portal public home page.

2. Login using your Portal user ID and password.

3. On the **My Portal** page, as shown in *Figure 116: Add Application Button on My Portal Page*, click the **Add Application** button.
   The **Request Application Access** page displays, as shown in *Figure 119: Request Application Access Page*.

4. Choose an application from the **Select an Application** drop-down list. For example, select **Eligibility and Enrollment Medicare Online (ELMO)**.
   Information about the selected application is displayed as shown in *Figure 126: Request Application Access – Selecting an Application*.
   Note

   You can click the **Help Desk Information** header to view how to contact the Help Desk for that application.

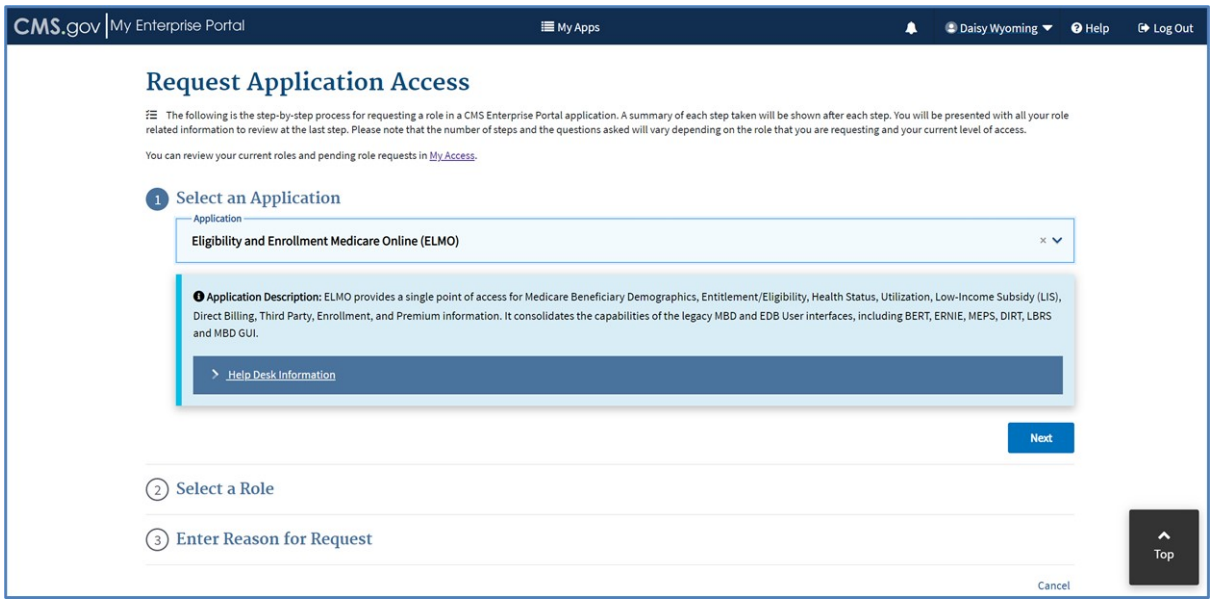

Figure 126: Request Application Access – Selecting an Application

5. Click **Next**.
   Step 1 of the Request Application Access is completed.

6. You may be asked to choose a Group, depending on the application selected. Next, choose a role from the **Select a Role** drop-down list, as shown in *Figure 127: Request Application Access – Selecting a Role*. For example, select **ELMO State Basic**.

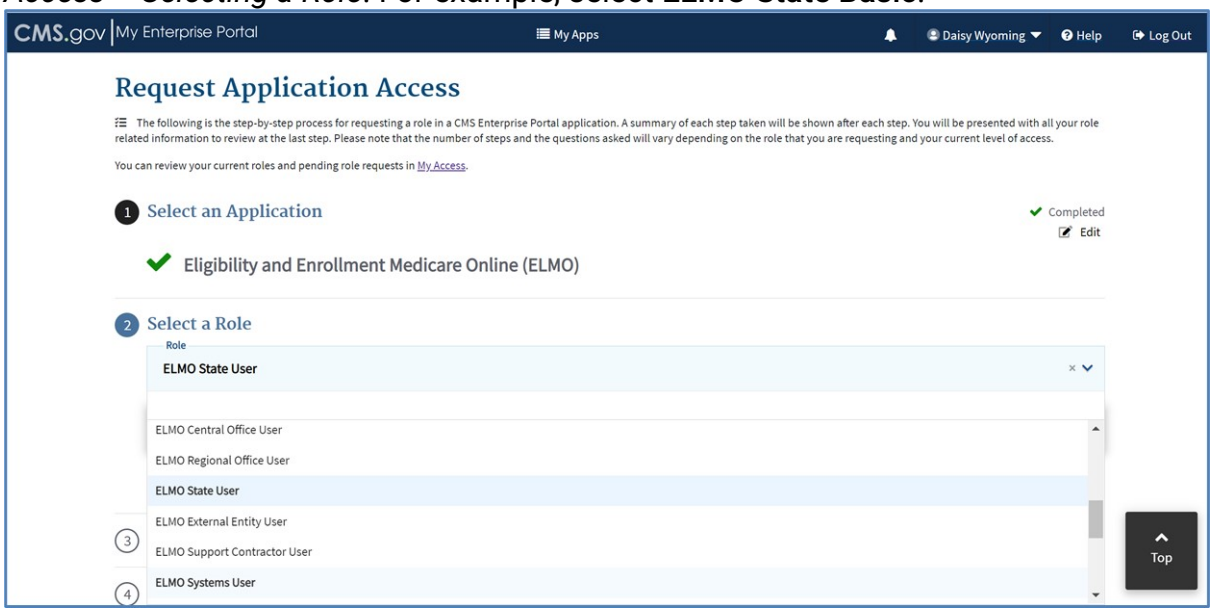

Figure 127: Request Application Access – Selecting a Role

The system may prompt you to enter or select any additional information needed, based on

the application and role you are requesting. For example, when the ELMO State Basic role is selected for the ELMO application, the system prompts you to enter the BCI and the Role Details, as shown in *Figure 128: Request Application Access – Additional Information*.

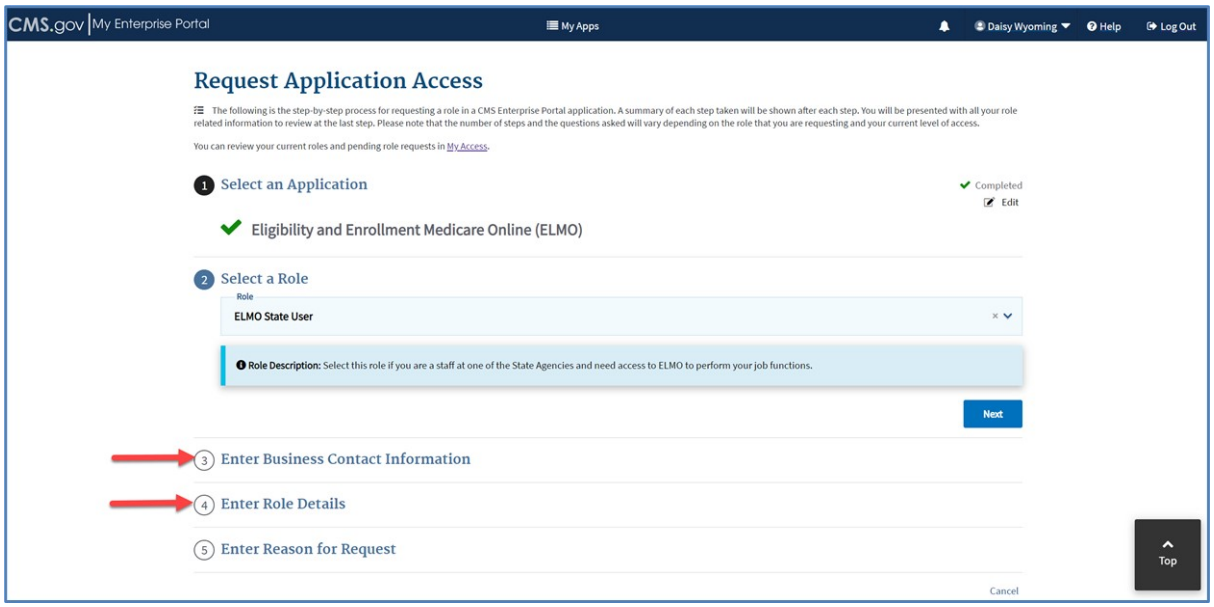

Figure 128: Request Application Access – Additional Information

7. Click **Next** to continue.

8. Provide the information requested in step 3, as shown in *Figure 129: Request Application Access – Enter BCI*. After all required information has been provided, click **Next** to continue.
   Note

   If you already provided the Business Contact Information via the **My Profile** page, this information will be auto populated.

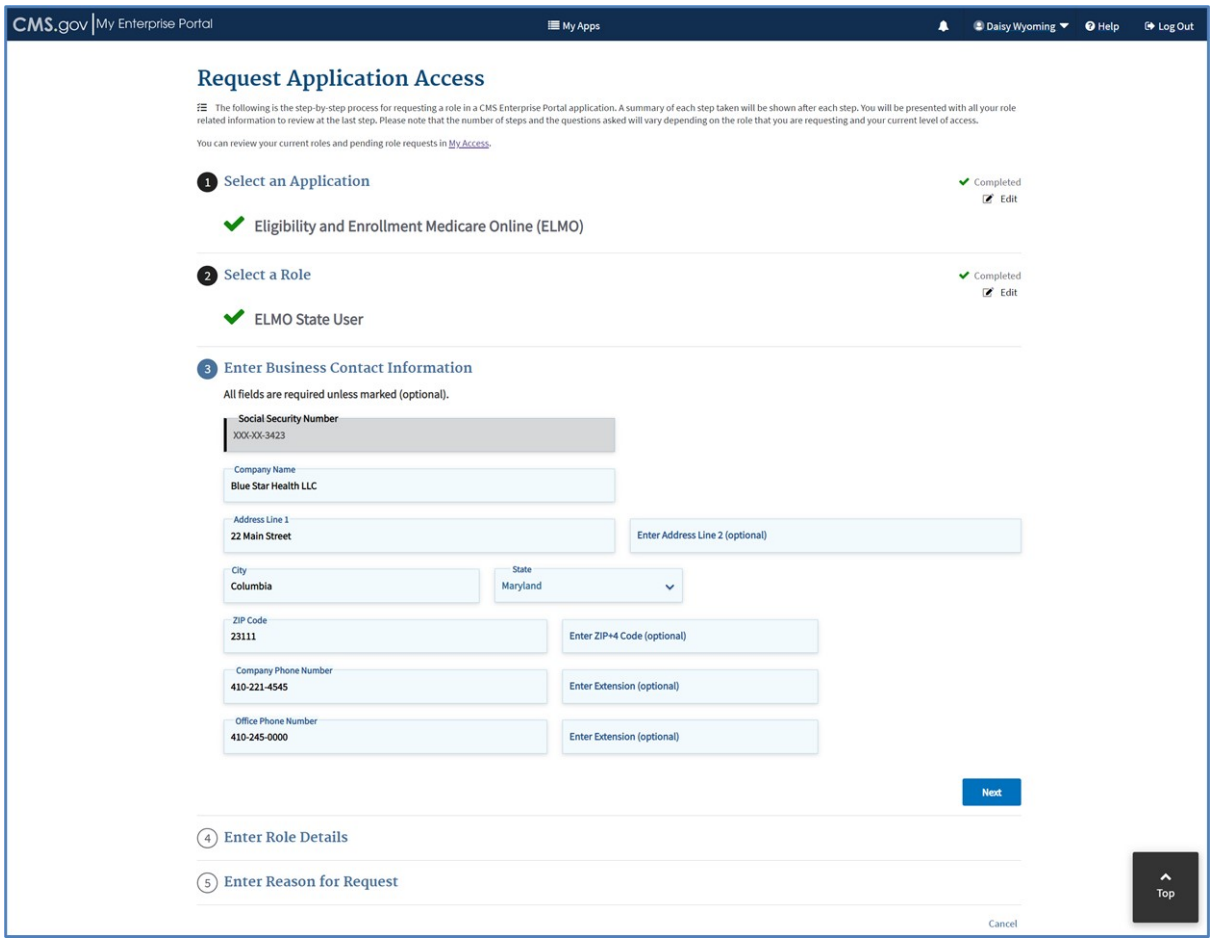

Figure 129: Request Application Access – Enter BCI

9. Provide the information, i.e. the role details, requested in step 4, as shown in *Figure 130: Requesting Application Access – Role Details*. The role details or role attributes are additional questions that some applications require you to answer at the time of role request. The answers to these questions help the Approver evaluate your role request. Sometimes, role attributes are used to identify the Approver for the role and route the role request to that Approver. After all required information has been provided, click **Next** to continue.

Note

Based on the role requested, you may or may not be required to enter the Role Details.

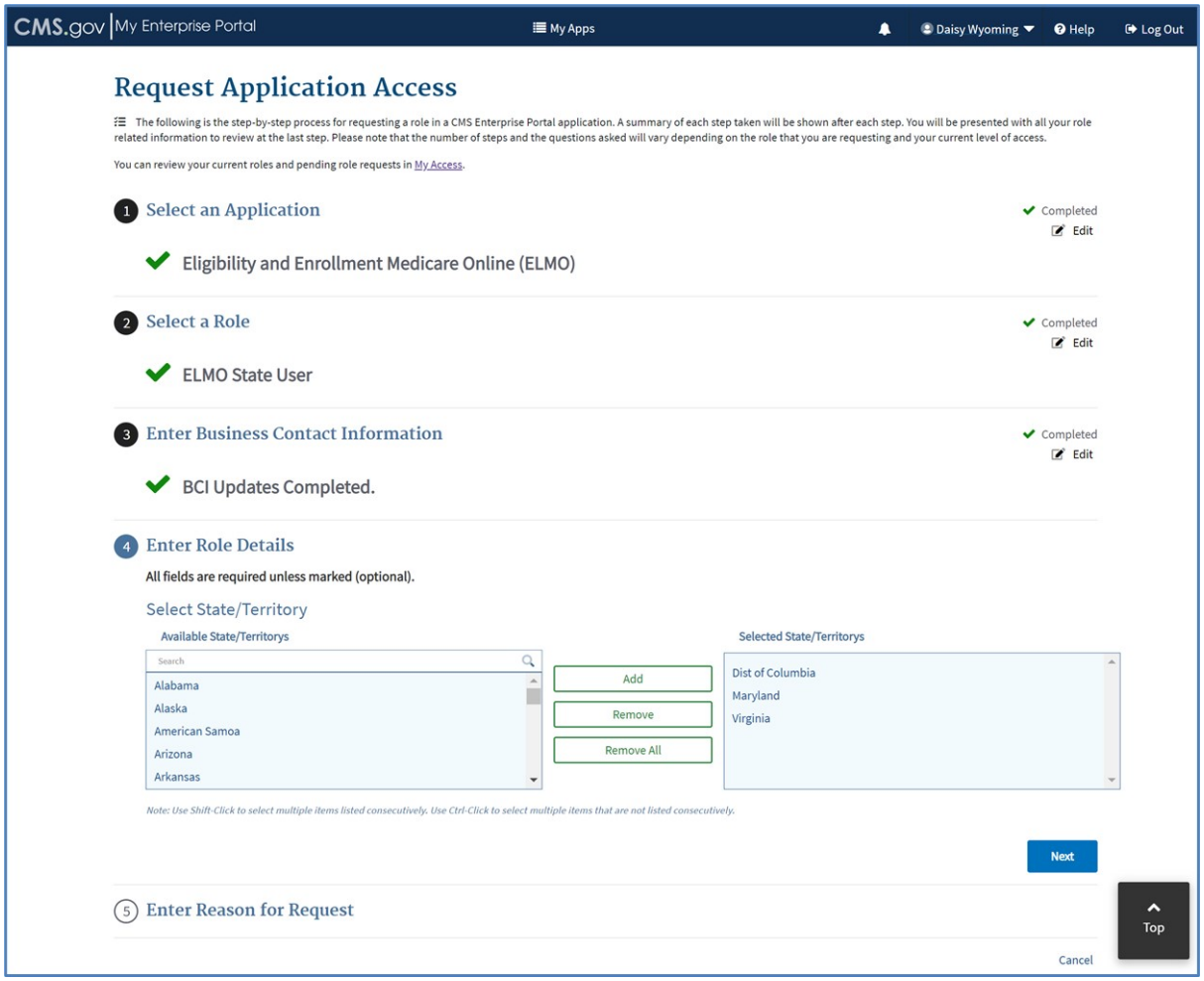

Figure 130: Requesting Application Access – Role Details

10. Provide the information requested in step 5, as shown in *Figure 131: Requesting Application Access – Reason for Request*.

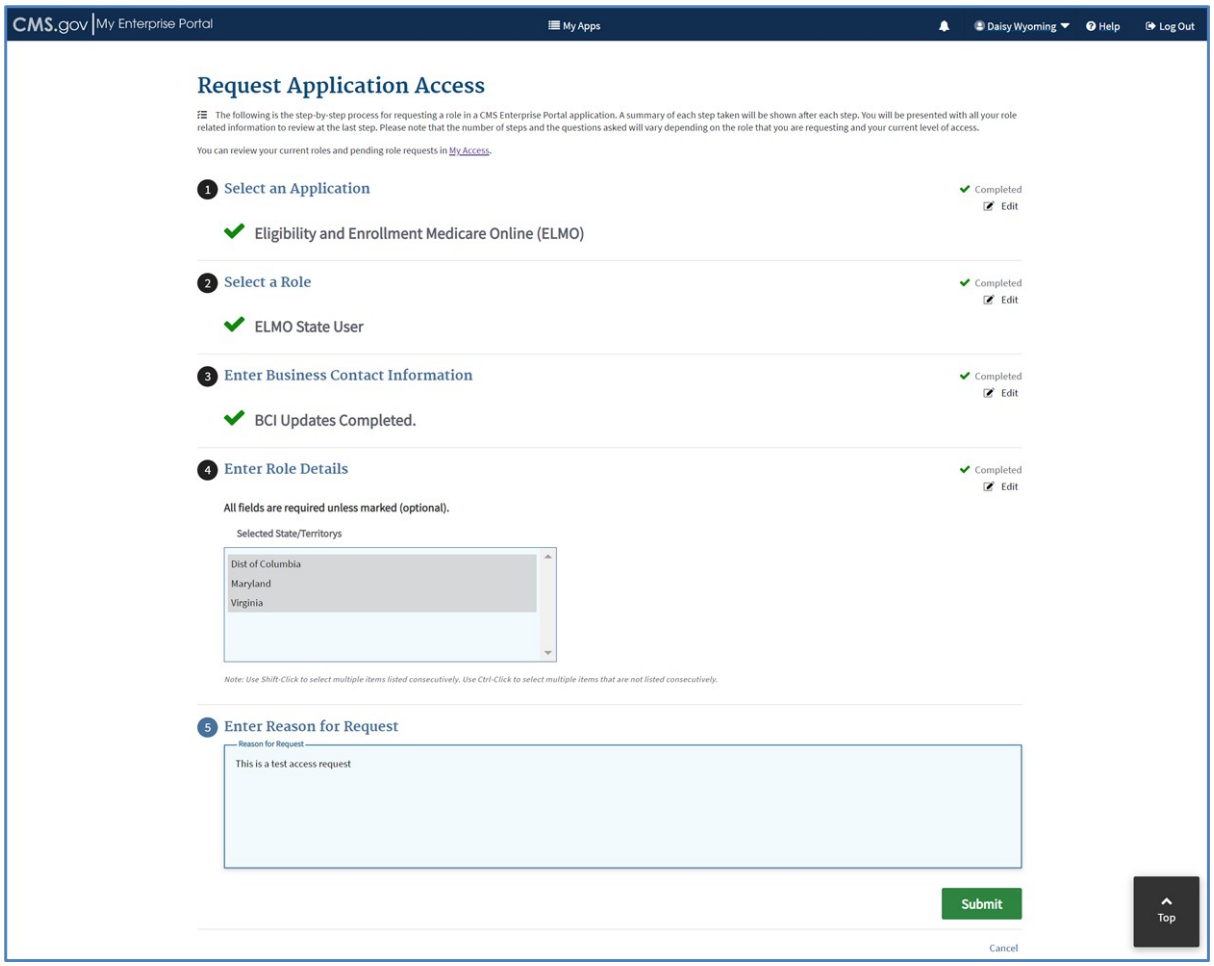

Figure 131: Requesting Application Access – Reason for Request

11. Click **Submit** to submit the request for approval. You will be prompted to confirm if you want to proceed.

12. Click **OK**.
    You will receive confirmation that the request was submitted successfully along with a tracking number for your request, as shown in *Figure 132: Request Application Access – Success Message*. You will see one or more request tracking number(s) on the **Request New Application Access Acknowledgement** page. You can use these tracking number(s) when contacting the approvers for help.

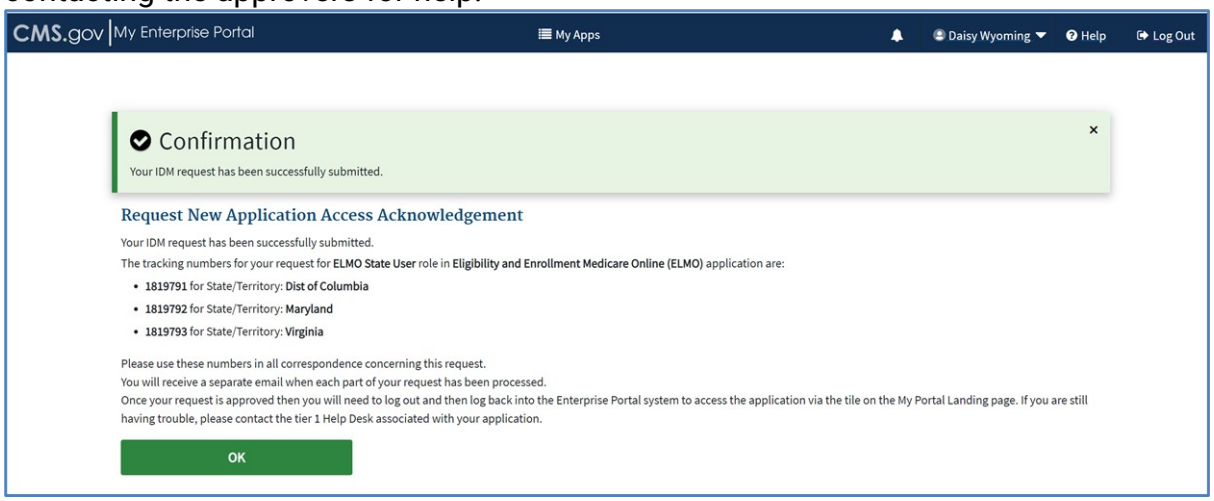

Figure 132: Request Application Access – Success Message

13. Click **OK**.
    You will be redirected to the **My Roles** page. Click the **My Pending Requests** tab. The request will display under the **My Pending Requests** tab, as shown in *Figure 133: Request Application Access – Pending Request*.

Note

You, as a Submitter, will receive an email notification with the request tracking number(s), while the Approver receives an email to take an action on the submitted request.

9.3.1. Determining User Identity and LOA

Depending on the role you requested and the information you provide, the system may take you to the Identity Verification page. The identity verification process is necessary for roles that require a higher level of security to access, but you are not at the correct Level of Assurance (LOA) that is required for the requested role. Identity verification is done by asking you questions based on your personal information.

Each role requires a specific LOA: LOA 1, LOA 2, or LOA 3. You will be assigned LOA 1 as soon as you register. To update or raise the LOA level, you go through the identity verification process.

Depending on your current LOA and the LOA required by the role you are requesting, you may or may not be required to go through the identity verification process.

There are three ways to complete the identity verification process:

- Remote Identity Proofing (RIDP) using the CMS Enterprise Portal and Experian's Identity Verification service.
- If you fail RIDP, then you go to the Experian Phone Proofing (with a review reference # obtained at the end of the failed RIDP process).
- If you subsequently fail Phone Proofing, you may go through the Manual Identity Proofing (IDP) procedure to update your LOA by contacting your Application Help Desk, who can manually raise the LOA after determining your identity.

Note

Manual IDP by the Application Help Desk is the last resort for IDP after you have failed RIDP and Phone Proofing. LOA level can be raised but cannot be lowered. Once LOA 3 is reached, no changes can be made to the LOA level. RIDP does not work if you have a foreign address associated with your account so Manual IDP is the only option.

9.3.2. Requesting a Role Requiring RIDP

The following are the instructions on how to request access to an application and role that requires RIDP.

1. On the **Request Application Access** page, choose an application from the **Select an Application** drop-down list. For example, select **Eligibility and Enrollment Medicare Online (ELMO)**.

2. Click **Next**.
   Step 1 of the Request Application Access is completed.

3. Choose a role from the **Select a Role** drop-down list. For example, select **ELMO Help Desk Users Administrator**.
   A message is displayed that the selected role requires additional level of identity verification, as shown in *Figure 134: Role Requiring RIDP*.

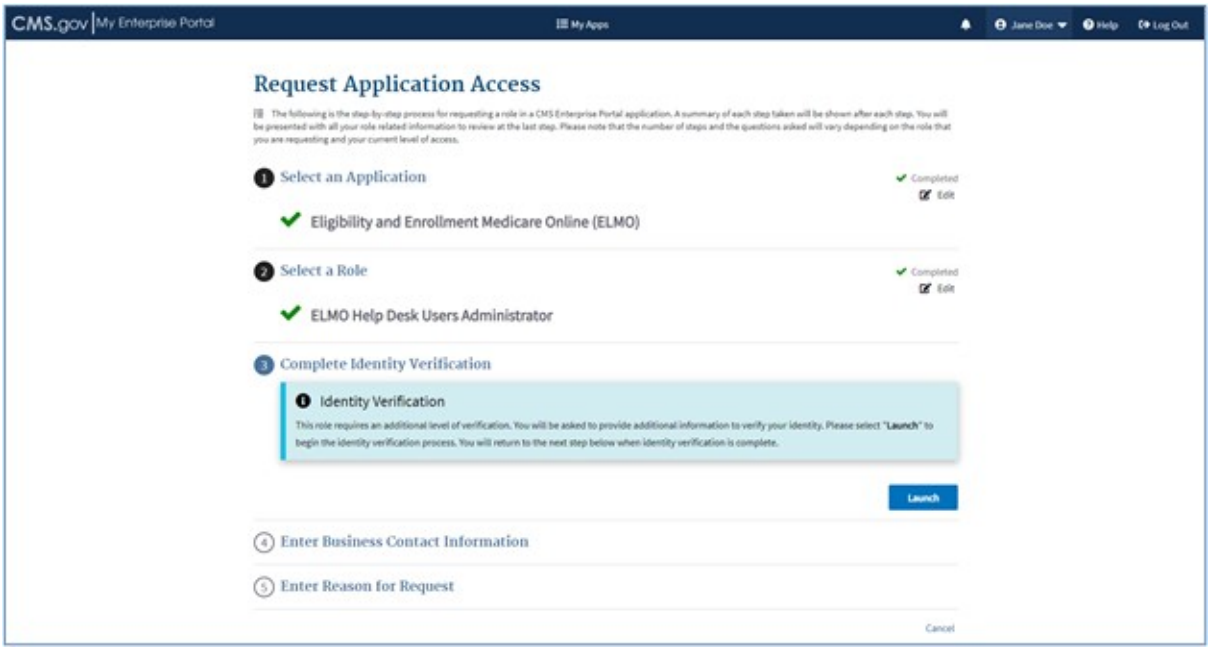

Figure 134: Role Requiring RIDP

4. Click **Launch** to begin the Identity Verification process.

   The **Step #1: Identity Verification Overview** page displays, as shown in *Figure 135: RIDP – Overview*.

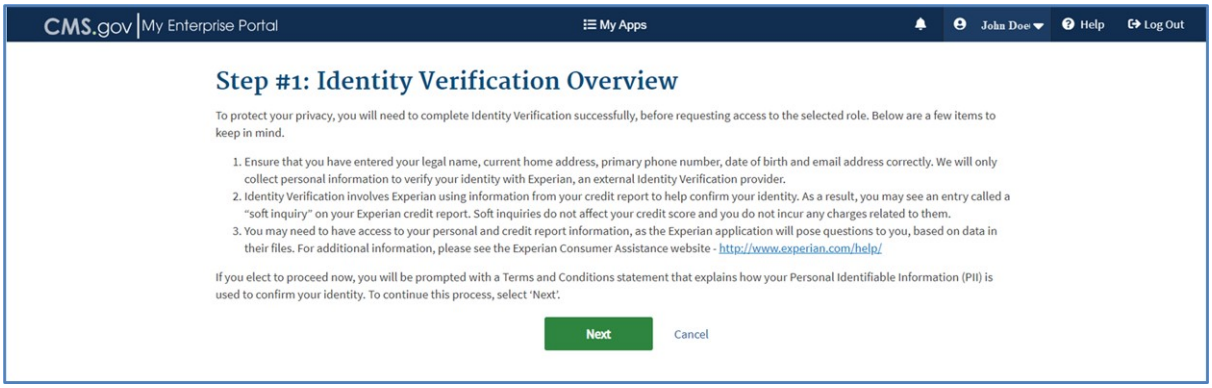

Figure 135: RIDP – Overview

5. Click **Next** to continue.

   The **Step #2: Accept Terms & Conditions** page displays, as shown in *Figure 136: RIDP – Terms and Conditions Information*.

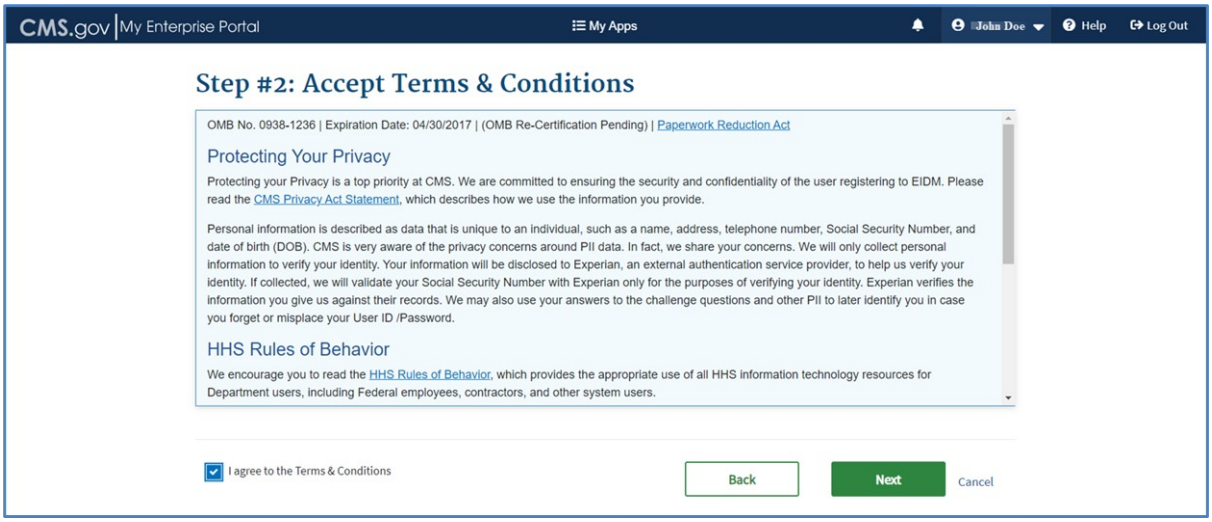

Figure 136: RIDP – Terms and Conditions Information

6. Read the **Terms and Conditions** information on this page and indicate your agreement by selecting the **I agree to the Terms and Conditions** checkbox. Click the **Next** button to continue.

   The **Step #3: Enter Your Information** page displays, as shown in *Figure 137: RIDP – Your Information Page*.

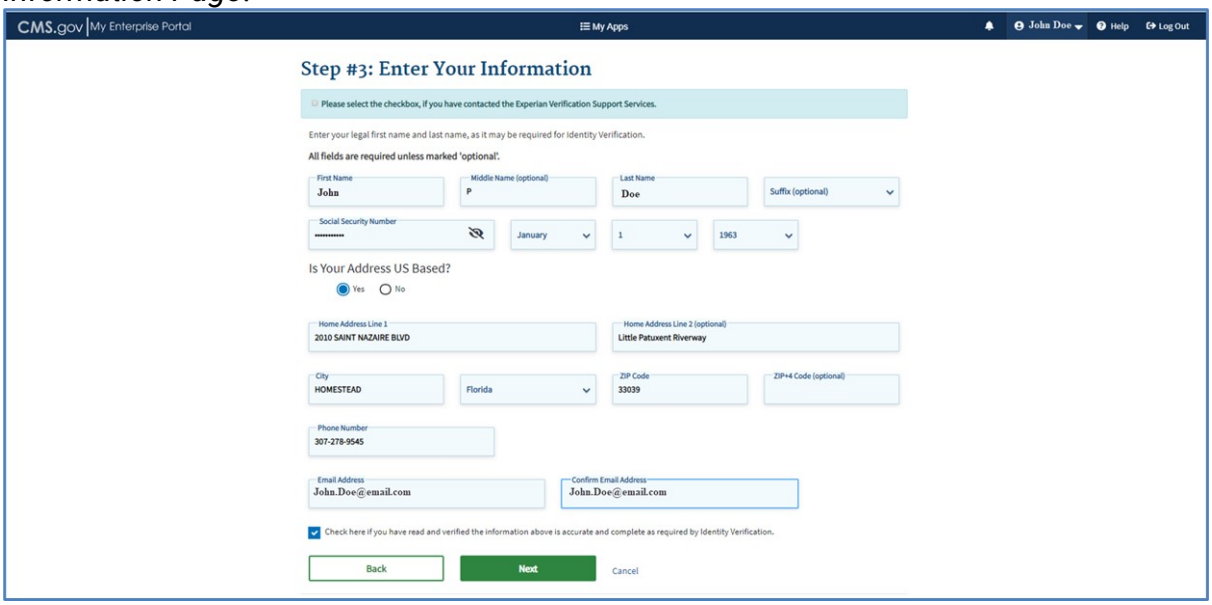

Figure 137: RIDP – Your Information Page

7. Enter your information into the required fields of the **Enter Your Information** page. Click **Next** to continue the identity verification process.
   The **Step #4: Verify Your Identity** page displays, as shown in *Figure 138: RIDP – Verify Identity*.

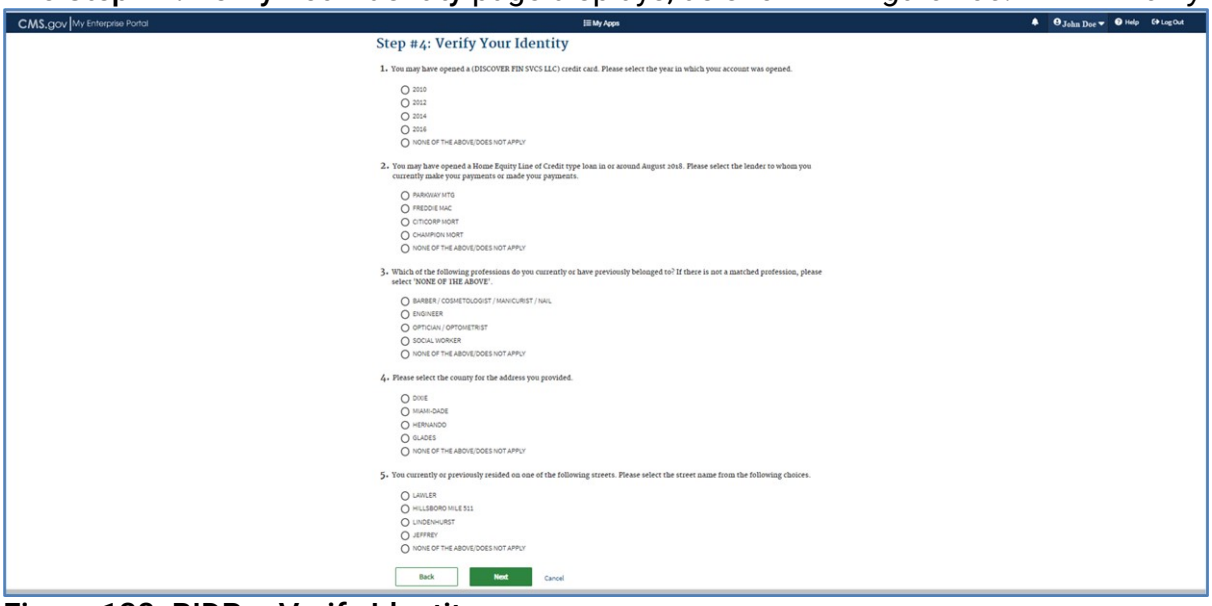

Figure 138: RIDP – Verify Identity

8. Provide an answer to each question and then click **Next** to continue. Click **Cancel** to terminate the request and return to the **My Access** page.
   If successful, a **confirmation** message is displayed, as shown in *Figure 139: RIDP – Confirmation Message*.

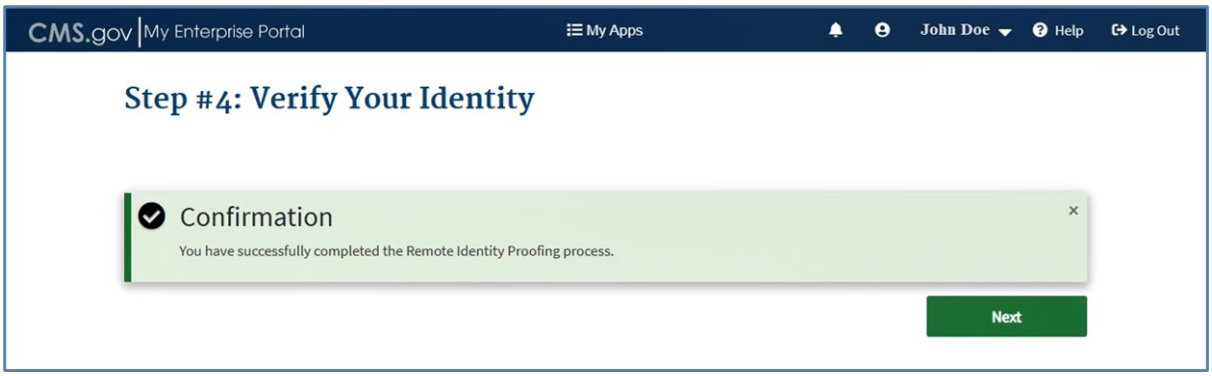

Figure 139: RIDP – Confirmation Message

RIDP is now complete.

9. Click **Next** to continue with the role request process.
   If RIDP is unsuccessful, you will get a review reference number and will be directed to call Experian to do Phone Proofing. If Phone Proofing does not work, then you can contact your Help Desk to go through the Manual IDP procedure to update your LOA.

9.4. Requesting an EUA Job Code

To access and view an EUA-provisioned application from within the CMS Enterprise Portal system, you will need to have an EUA CMS user ID and the approved Portal job code(s) for that application.

The following are the instructions on how to request access to job code(s) for accessing any EUA application hosted on the CMS Enterprise Portal system.

1. Navigate to the CMS Enterprise Portal public home page.

2. Login using your user ID and password.

3. On the **My Portal** page, as shown in *Figure 116: Add Application Button on My Portal Page*, click the **Add Application** button.
   The **Request Application Access** page displays, as shown in *Figure 140: Request Application Access Page*.

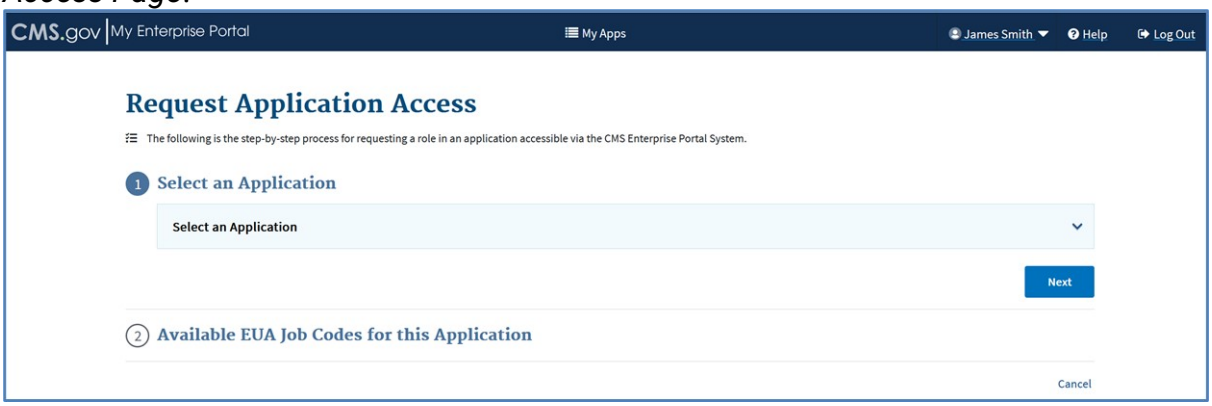

Figure 140: Request Application Access Page

4. Choose an application from the **Select an Application** drop-down list containing a list of EUA-provisoned applications. For example, select **Enterprise MicroStrategy Reports**.
   Information about the selected application is displayed as shown in *Figure 141: Request Application Access – Selecting an EUA Application*.
   Note

   You can click the **Help Desk Information** header to view how to contact the Help Desk for that

application.

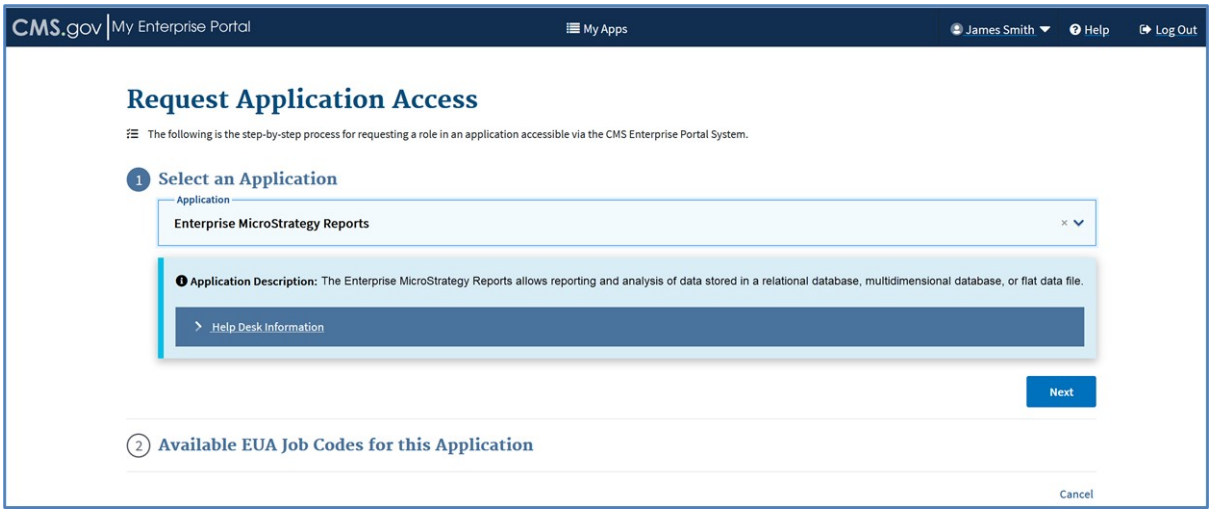

Figure 141: Request Application Access – Selecting an EUA Application

5. Click **Next**.
   Step 1 of the Request Application Access is completed and the system displays the available EUA job codes for the selected application and the instructions for how to request the required job code(s) from the EUA system in order to access and view the selected application from within the CMS Enterprise Portal system. Refer to *Figure 131: Listing of Available Job Codes for Selected EUA Application*.
   The list of job codes are returned as a paginated list, as shown in, *Figure 142: Listing of Available Job Codes for Selected EUA Application*, if there are multiple available job codes for the selected EUA application. This list can be sorted either by the job code or the description. The Global Filter feature is also available and can be used to further refine the list of job codes if multiple job codes are returned.
   To select a different EUA application and view the available job codes for that application, click the **Edit** button to the right of Step 1. Click **Cancel** at the bottom right of the page to return to the **My Portal** landing page. Upon clicking **Cancel**, the system will prompt you to confirm that you wish to exit the page.

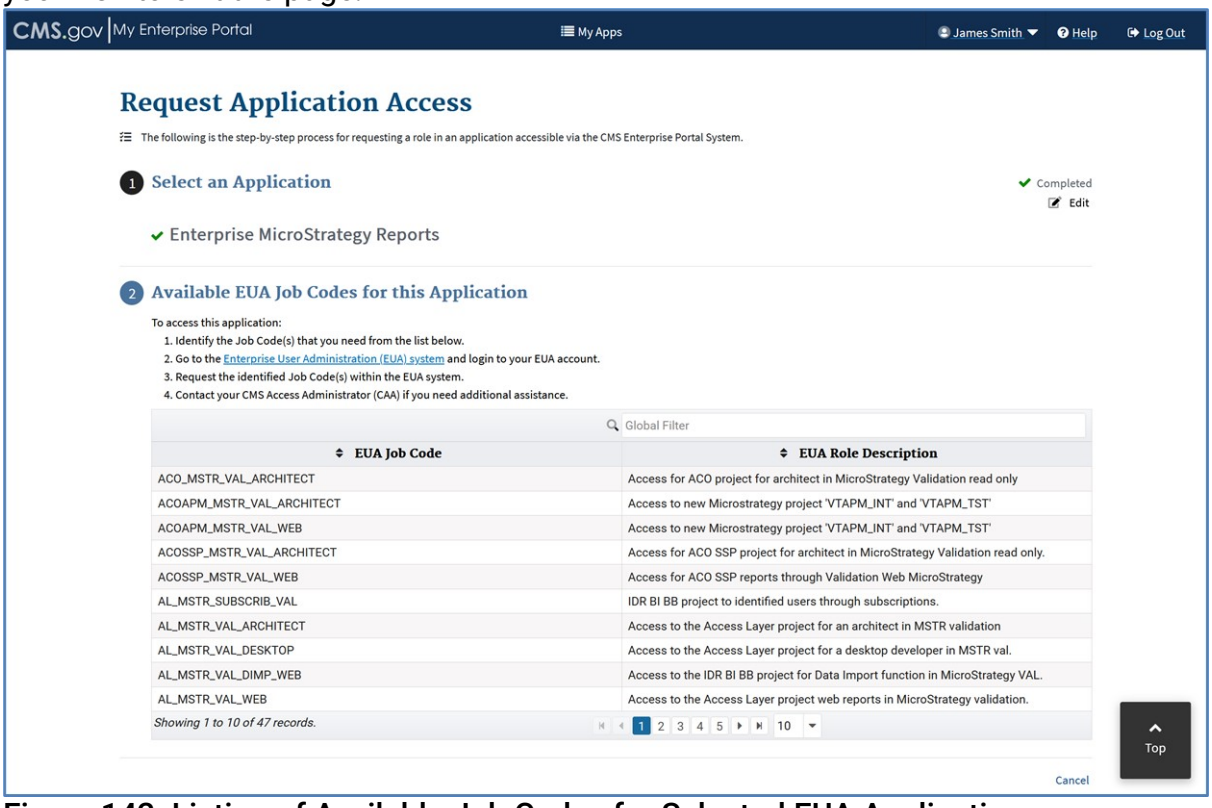

Figure 142: Listing of Available Job Codes for Selected EUA Application

9.5. Canceling a Pending Request

The following are the instructions on how to cancel a pending role request that was submitted for approval.

1. Navigate to the CMS Enterprise Portal public home page.

2. Login using your user ID and password.

3. On the **My Portal** page, select the **My Access** option from the name drop-down list in the top navigation bar, as shown in *Figure 120: Accessing the My Access Page via Name Drop-down*. The **My Roles** tab of the **My Access** page displays.

4. Click the **My Pending Requests** tab.
   The **My Pending Requests** tab displays with a list of pending requests submitted for approval, as shown in *Figure 143: List of Pending Requests*.

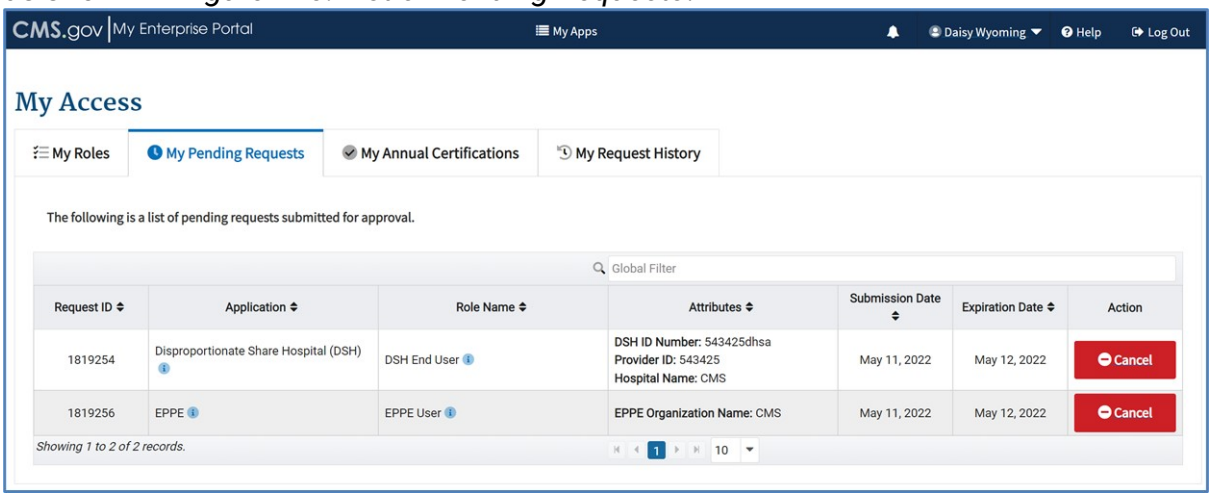

Figure 143: List of Pending Requests

5. Click the **Cancel** button next to the role request you want to cancel.

6. Click **OK** in the modal dialog box, as shown in *Figure 144: Cancel Pending Request – Confirmation*.

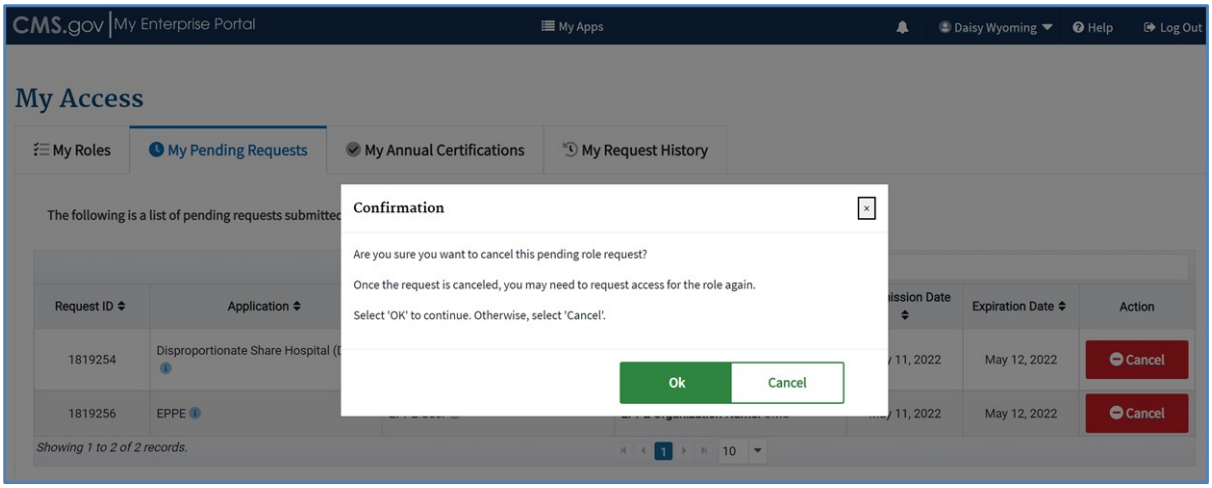

Figure 144: Cancel Pending Request – Confirmation

You will receive a confirmation that your pending role request has been canceled, as shown in *Figure 145: Cancel Pending Request – Success Message*.

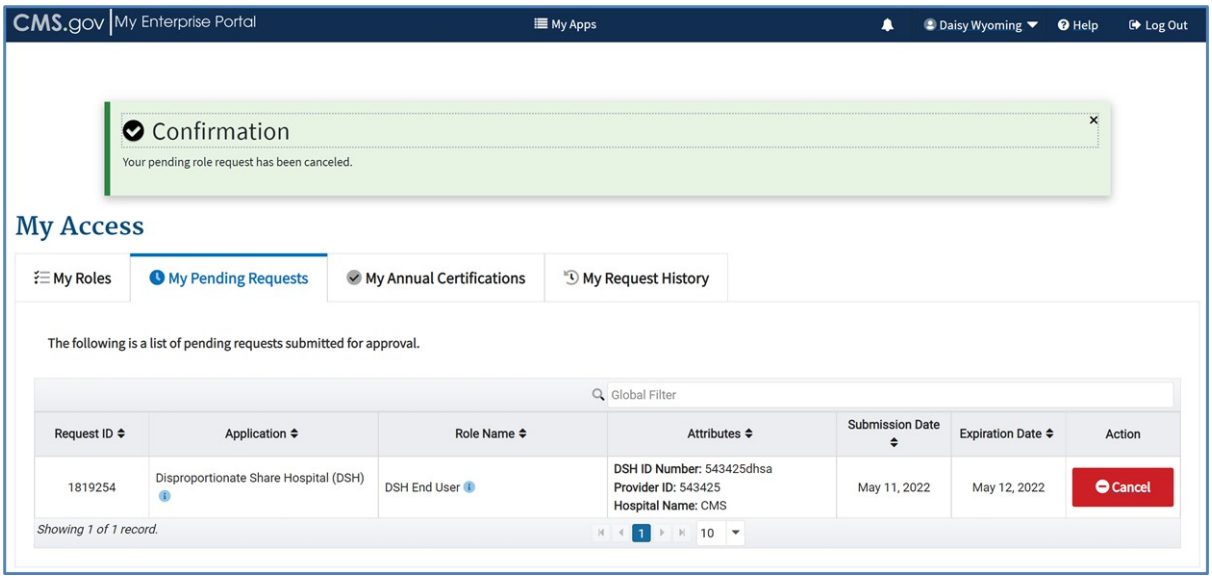

Figure 145: Cancel Pending Request – Success Message

Note

You will receive an email notification indicating that your pending role request was canceled.

9.6. Removing a Role

The following are the instructions on how to remove a role for an application you currently have access.

1. Navigate to the CMS Enterprise Portal public home page.

2. Login using your user ID and password.

3. On the **My Portal** page, select the **My Access** option from the name drop-down list in the top navigation bar, as shown in *Figure 120: Accessing the My Access Page via Name Drop-down*. The **My Roles** tab of the **My Access** page displays, as shown in *Figure 146: List of Existing Applications*.

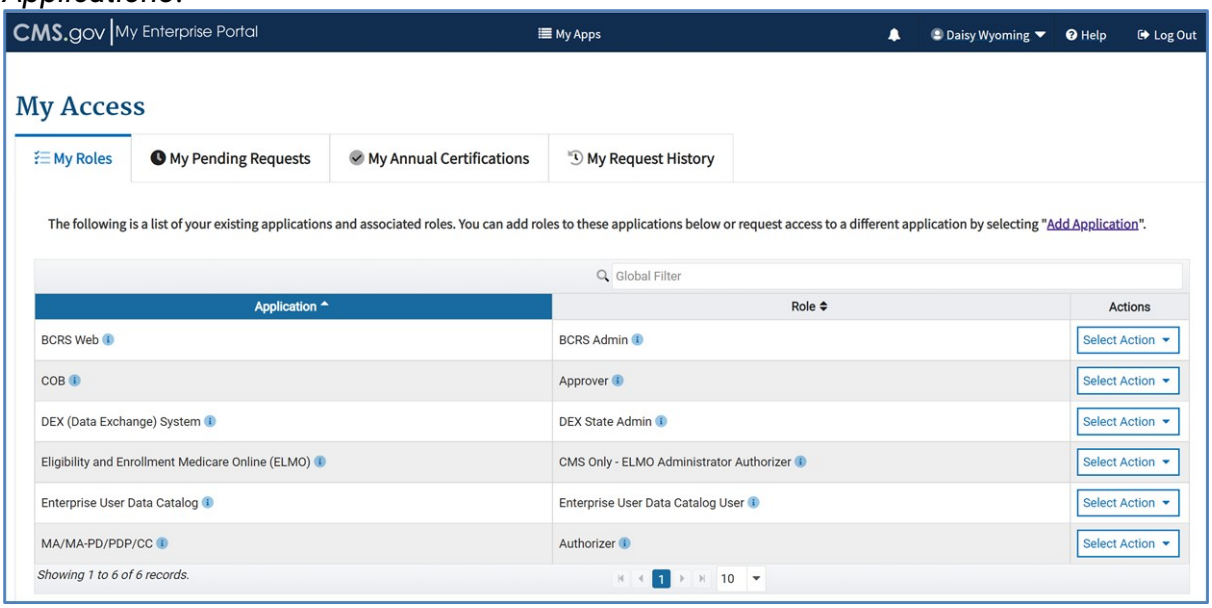

Figure 146: List of Existing Applications

4. Click the **Select Action** drop-down next to the application role you want to remove and then click the **Remove Role** option, as shown in *Figure 147: Selecting Remove Role Action*.

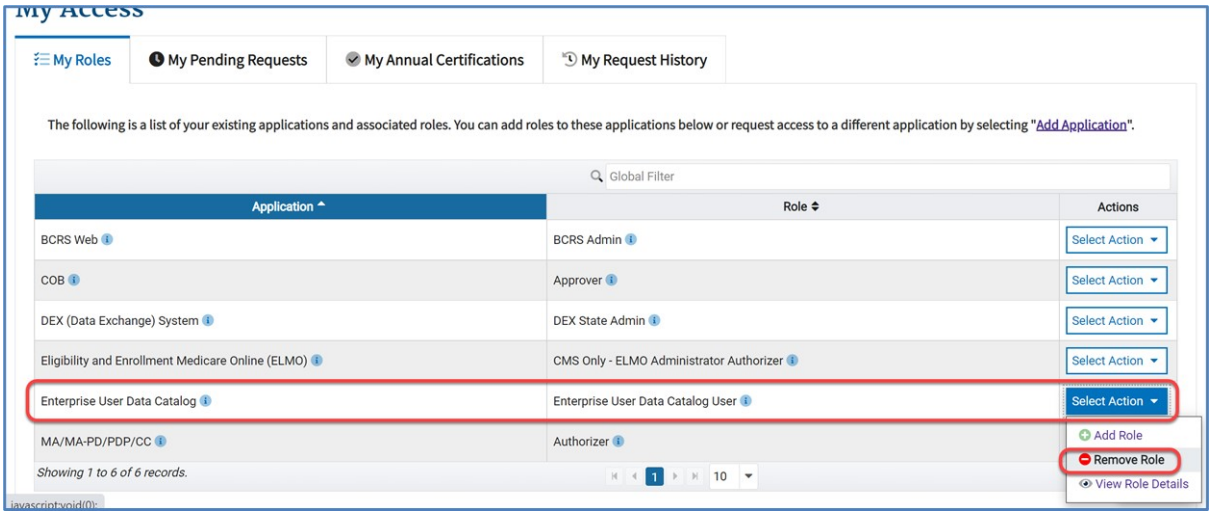

Figure 147: Selecting Remove Role Action

5. Click **OK** in the modal dialog box to confirm removal, as shown in *Figure 148: Remove Role – Confirmation*.

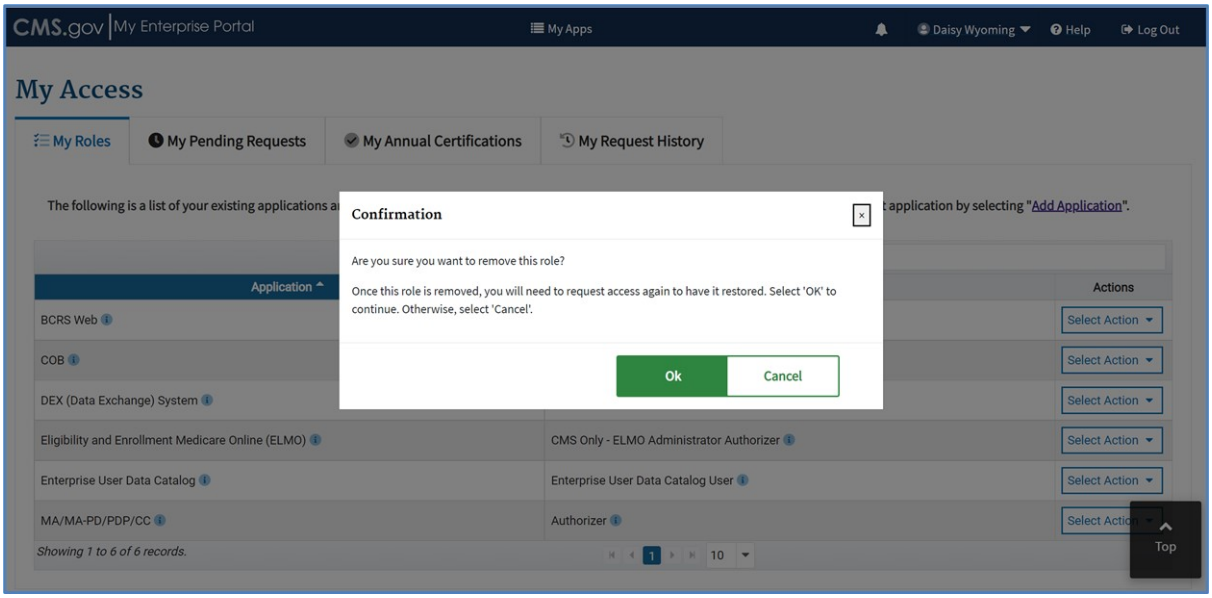

Figure 148: Remove Role – Confirmation

Note

You will see a warning if you are the last and only approver for a role you are requesting to remove. You will need to acknowledge the warning to remove the role completely.

A confirmation displays, as shown in *Figure 149: Remove Role – Success Message*.

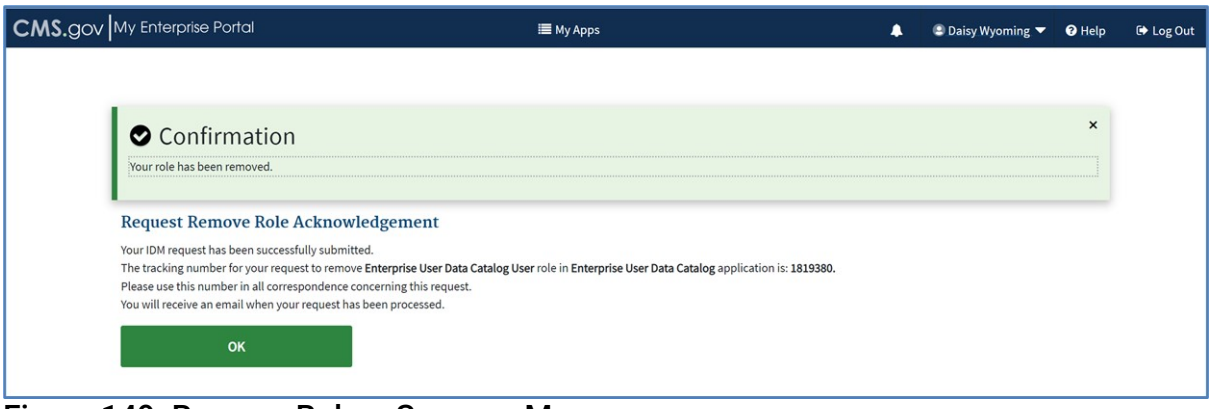

Figure 149: Remove Role – Success Message

Note

You will receive an email notification indicating that your role was removed.

6. Click **OK** to acknowledge and return to the **My Roles** tab.

9.7. Viewing/Modifying Role Details

The role details or role attributes are additional questions that some applications require you to answer at the time of role request. The answer to these questions help the Approver evaluate your role request. Sometimes, role attributes are used to identify the Approver for the role and route the role request to that Approver.

The following are the instructions on how to view role details for an application you currently have access.

1. Navigate to the CMS Enterprise Portal public home page.

2. Login using your user ID and password.

3. On the **My Portal** page, select the **My Access** option from the name drop-down list in the top navigation bar, as shown in *Figure 120: Accessing the My Access Page via Name Drop-down*. The **My Roles** tab of the **My Access** page displays, as shown in *Figure 146: List of Existing Applications*.

4. Click the **Select Action** drop-down next to the application role you want to view the details of and then click the **View Role Details** option, as shown in *Figure 150: Selecting View Role Details* Action.

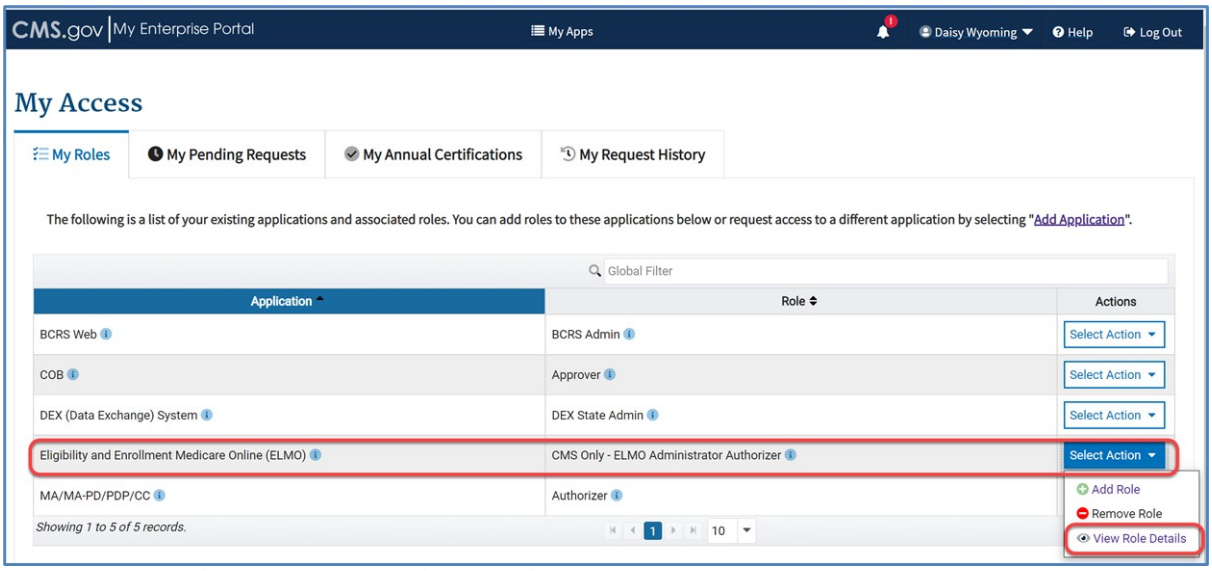

Figure 150 Selecting View Role Details Action

The **Role Details** page displays, as shown in *Figure 151: Role Details Page Without Details* or Attributes. There are no details or attributes associated with this role.

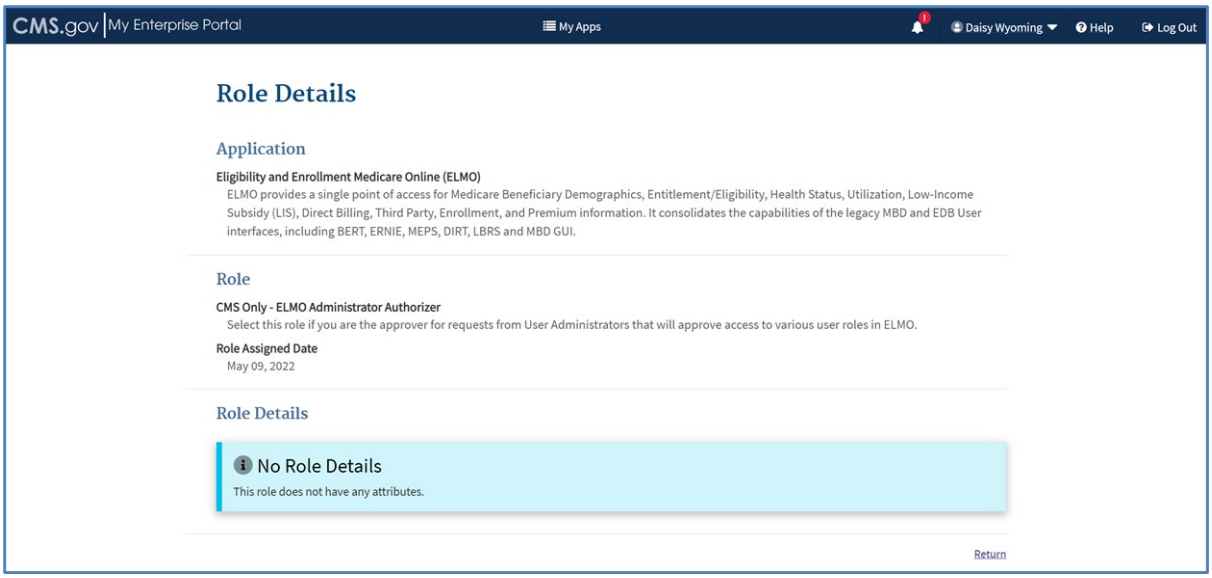

Figure 151: Role Details Page Without Details or Attributes

If, for example, during the role request process, the user was required to select state(s) under Role Details and the user selected one or more states, then the user will see a list of their role's states when viewing the **Role Details** page, as shown in *Figure 152: Role Details Page with Attributes – States*. The user, in this example, is associated with the listed states. On the **Role Details** page, the user also has the option to modify their role details, as applicable, for their role.

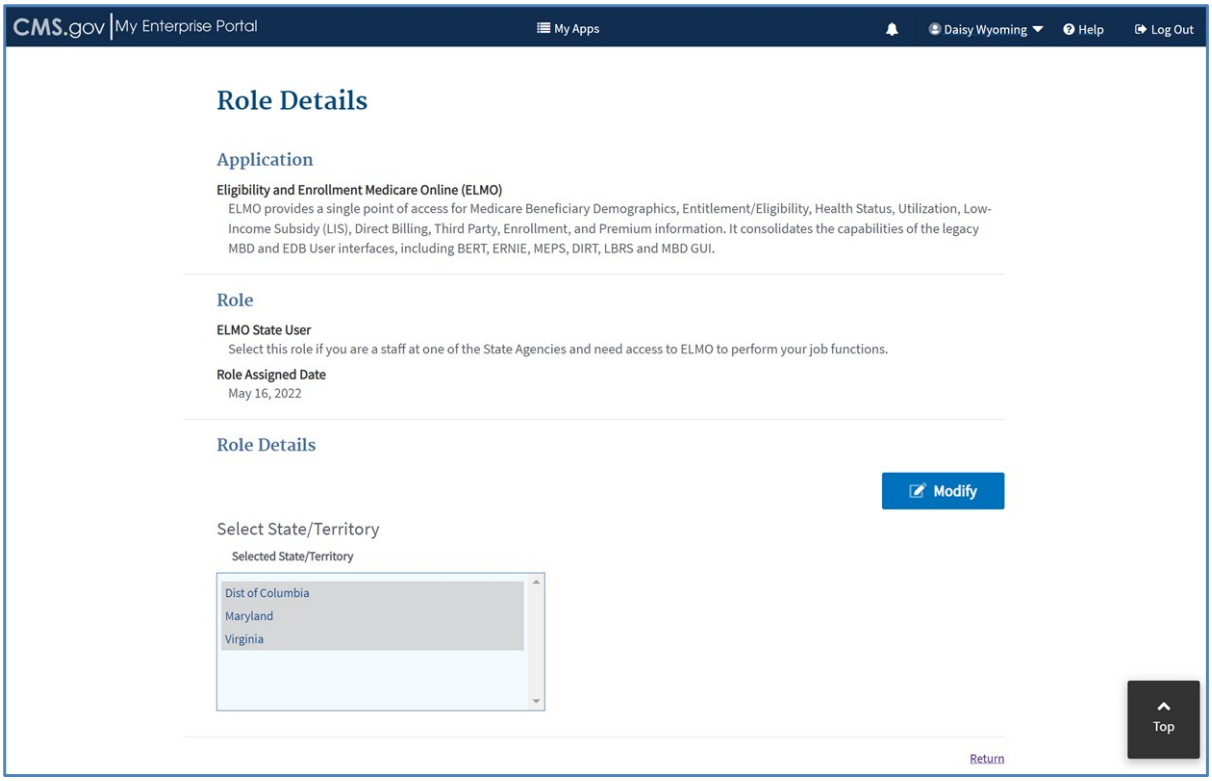

Figure 152: Role Details Page with Attributes – States

Upon selecting the **Modify** button the **Role Details** page, as shown in *Figure 153: Role Details Page with Attributes – Modify*, is Displayed and user can modify the details of a role.

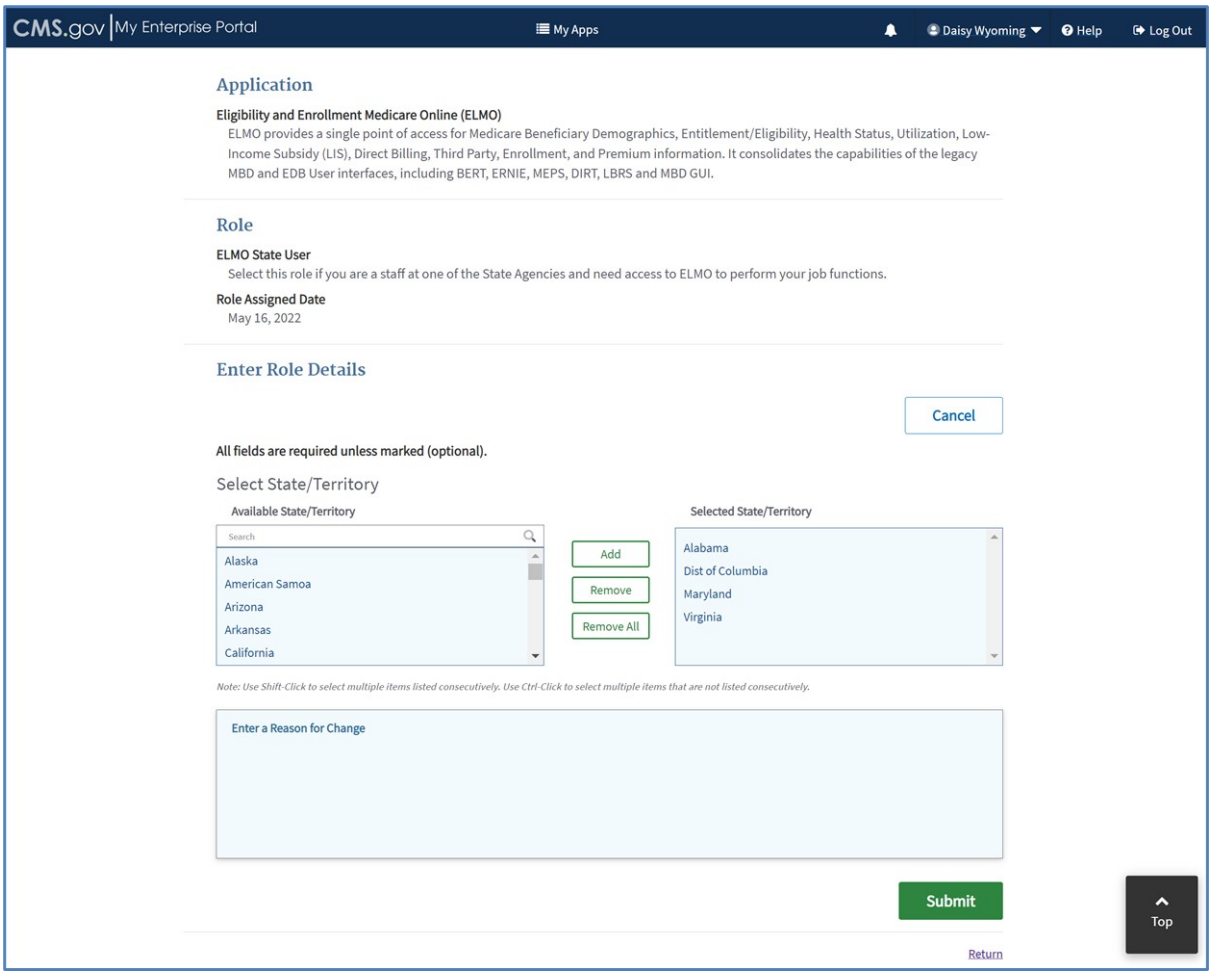

Figure 153: Role Details Page with Attributes – Modify

9.8. My Annual Certifications

CMS security guidelines require that the use of a role must be certified every year, or the role will automatically be removed from your profile. Annual Role Certification is the process of certifying your continued use of a role and is valid for one year.

While there is no action required on your part, you may want to notify your Approver of your desire to use a role for another year.

You can perform the following functions related to Annual Role Certifications in CMS Enterprise Portal:

- View a list of all the roles that you currently have access to that require certification, have been certified, or have submitted requests for certification
- Request certification of one or more roles

9.8.1. Viewing My Annual Certifications

The following are the instructions on how to view your annual certifications.

- Navigate to the CMS Enterprise Portal public home page.
- Login using your user ID and password.

- On the **My Portal** page, select the **My Access** option from the name drop-down list in the top navigation bar, as shown in *Figure 120: Accessing the My Access Page via Name Drop-down*. The **My Roles** tab of the **My Access** page displays as shown in *Figure 146: List Of Existing Applications*.

- Click the **My Annual Certifications** tab.
  The **My Annual Certifications page**, as shown in *Figure 154: Viewing My Annual Certifications*, displays a paginated list of all the roles that you currently have access to that are due for certification, have been certified, or have been submitted for certification, as indicated in the Status column. Any role that needs to be certified will show the status as “Certification Due”

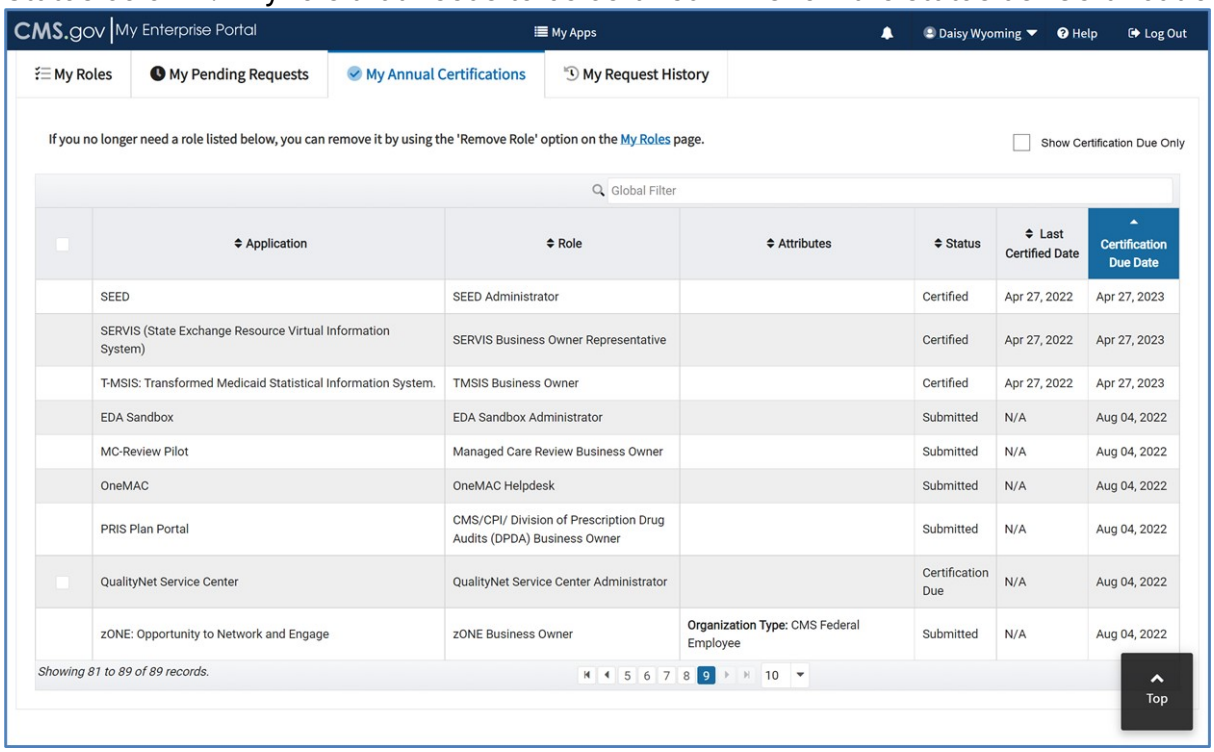

Figure 154: Viewing My Annual Certifications

By default, the **My Annual Certifications** page displays all your roles sorted in the descending order of Certification Due Date, such that the rows with certification due date closet to the current date are displayed first and the rows with dates farthest from the current date are displayed last. You can sort the list in ascending or descending order of any column (Application, Role, Attributes, Status, Last Certified Date, or Certification Due Date) by clicking on the arrow next to the column name. You can use the ‘Global Filter’ feature to filter the list of roles based on a text string, which will search on all the columns and the column data and display the results based on the entered text string. The checkbox for **Show Certification Due Only** is also present on the page which if selected, filters the list of roles to display only those roles that are due for certification.
Note that if you don’t have any annual role certifications, then a message is displayed on the page indicating this.

9.8.2. Requesting Annual Certifications

The following are the instructions on how to request your annual certifications.

- Navigate to the CMS Enterprise Portal public home page.

- Login using your user ID and password.

- On the **My Portal** page, select the **My Access** option from the name drop-down list in the top

navigation bar, as shown in *Figure 120: Accessing the My Access Page via Name Drop-down*. The **My Roles** tab of the **My Access** page displays as shown in *Figure 146: List Of Existing Applications*.

- Click the **My Annual Certifications** tab.
  The **My Annual Certifications page**, as shown in *Figure 124: My Annual Certifications Tab on My Access Page*.
- Select the checkbox for **Show Certification Due Only** to view only the roles that need to be certified, as shown in *Figure 155: Viewing Roles Due for Certification*.

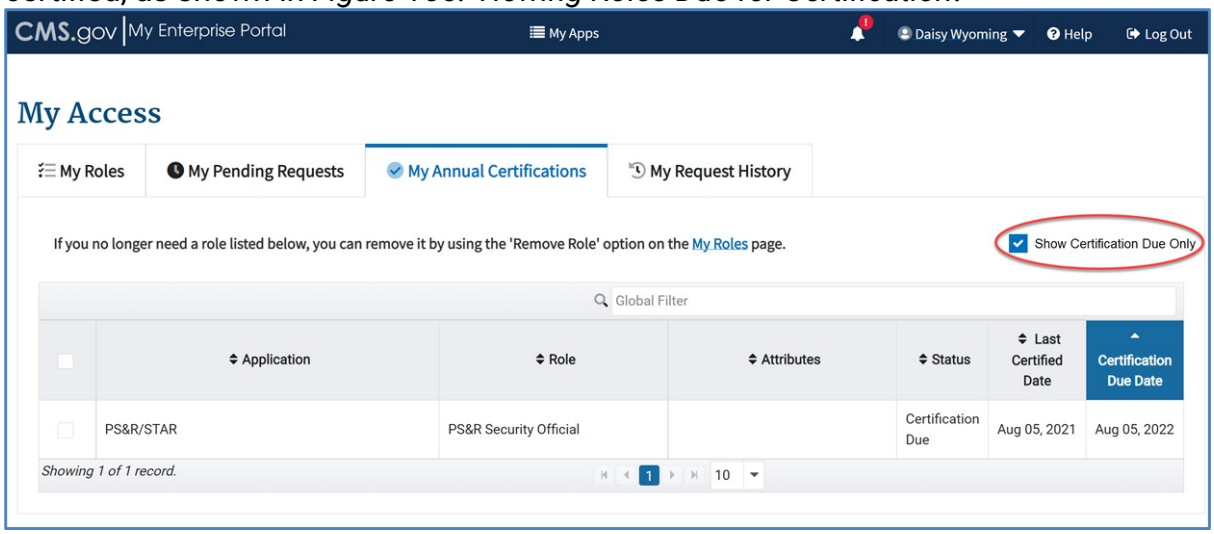

Figure 155: Viewing Roles Due for Certification

- Click on the checkboxes in the rows with the roles that you want to certify, as shown in *Figure 156: Selecting Roles to Certify*. Alternatively, click the **Select All** checkbox in the column header of the role list in order to select all the roles that require certification.

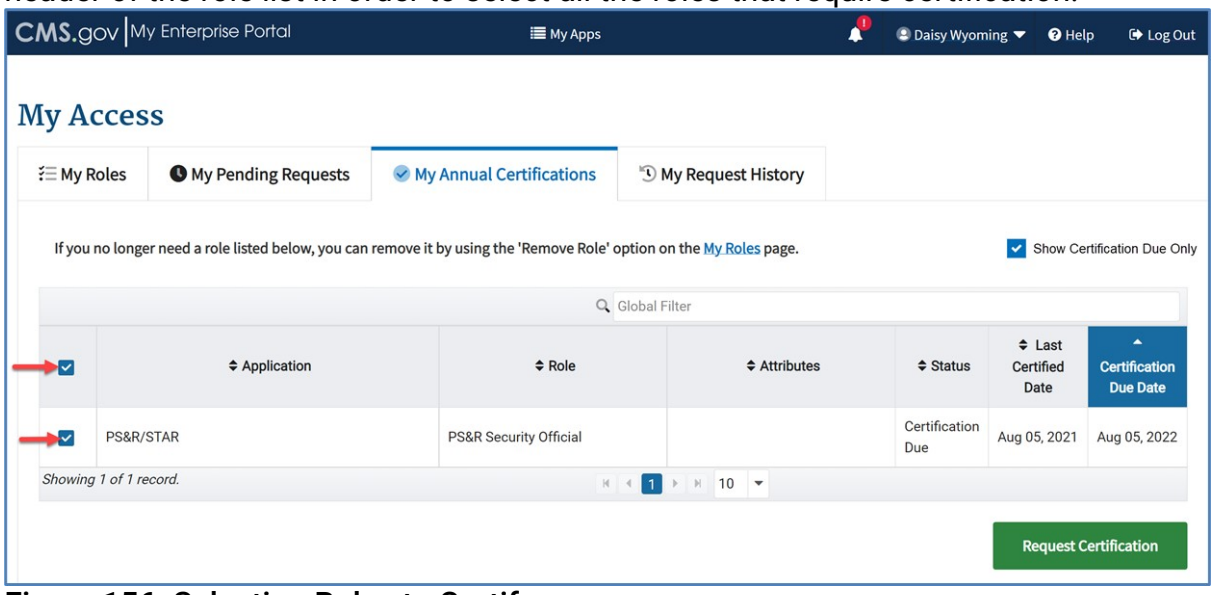

Figure 156: Selecting Roles to Certify

- Click the **Request Certification** button at the bottom of the page.
  A 'Confirmation of Certification Request' pop-up box appears, as shown in *Figure 157: Certification Request – Confirmation*, including the number of roles selected for certification and an optional textbox field to put in a reason for the request.

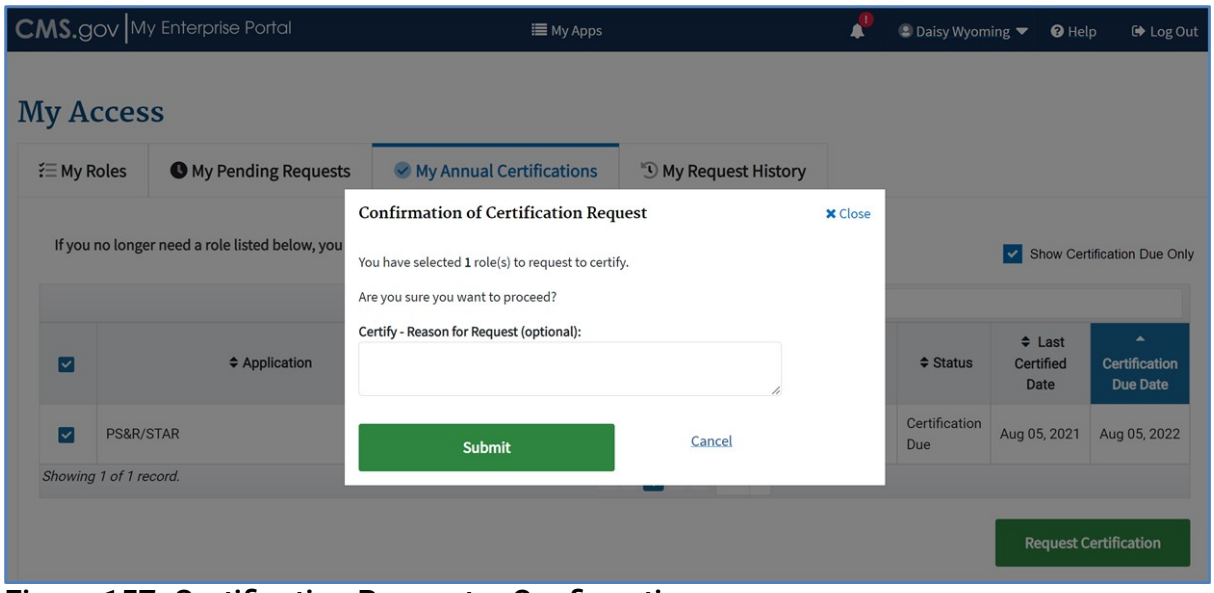

Figure 157: Certification Request – Confirmation

- You may enter a reason for requesting certification if applicable, and then click **Submit** to confirm your certification. Or click Cancel to cancel the certification and return to the **My Annual Certifications** page.
  Upon clicking **Submit**, you will see a confirmation message affirming the action taken, as shown in *Figure 158: Certification Request – Success Message*.

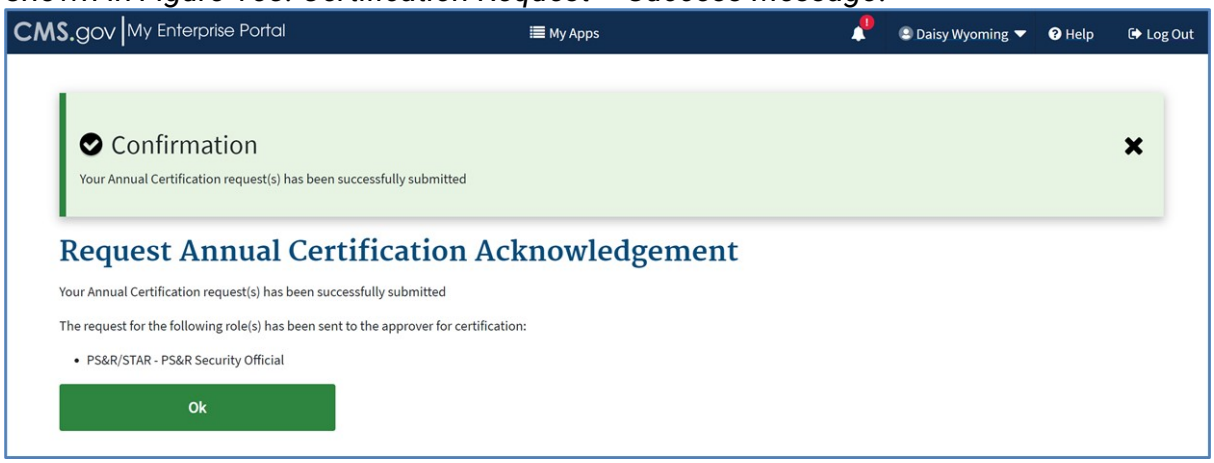

Figure 158: Certification Request – Confirmation

9.9. Viewing My Request History

The following are the instructions on how to view all your past requests for access to an application/role that have been approved, rejected, expired, revoked, or canceled.

1. Navigate to the CMS Enterprise Portal public home page.

2. Login using your user ID and password.

3. On the **My Portal** page, select the **My Access** option from the name drop-down list in the top navigation bar, as shown in *Figure 120: Accessing the My Access Page via Name Drop-down*.
   The **My Roles** tab of the **My Access** page displays, as shown in *Figure 146: List of Existing Applications*.

4. Click the **My Request History** tab.
   The **My Request History** page displays as shown in *Figure 159: Request History*, with a paginated list of all your request history items for access to an application/role that have been approved, rejected, expired, revoked, or canceled.

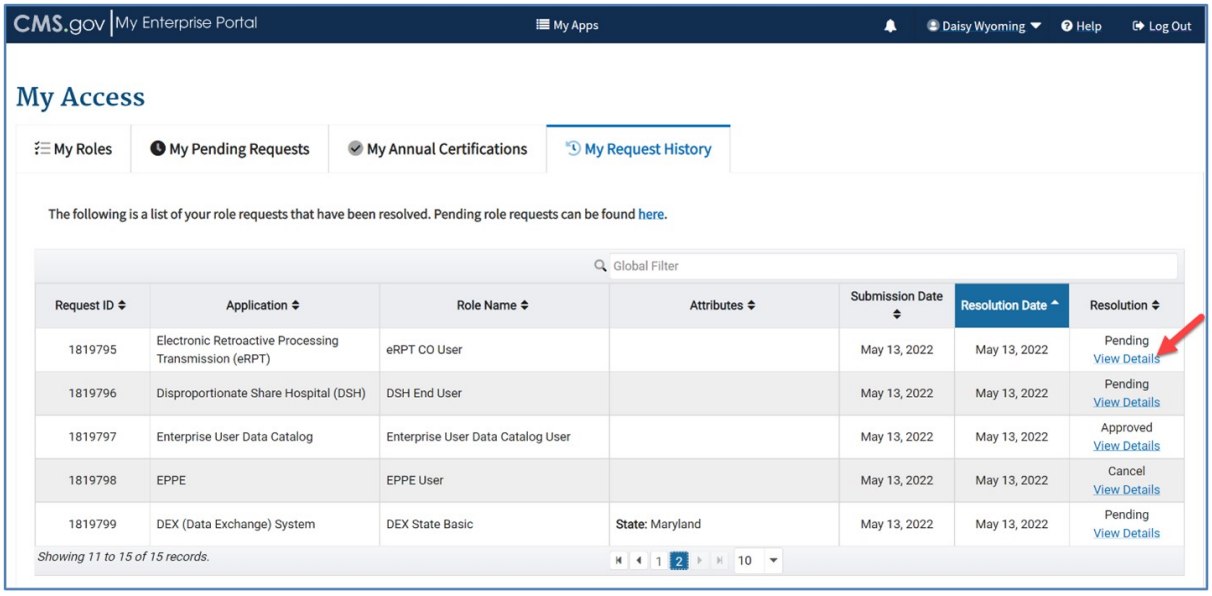

Figure 159: Request History

You can sort the request history list in the ascending or descending order of any column (Request ID, Application, Role Name, Attributes, Submission Date, Resolution Date, or Resolution) by clicking on the arrow next to the column name. You can also use the 'Global Filter' feature to filter the list of request history items based on a text string, which will search on all the columns and the column data and display the results based on the entered text string.

5. To view the details of any request history item, click the **View Details** link for that item under the Resolution column, as shown in *Figure 159: Request History*.
The details related to the selected request history item are displayed, as shown in *Figure 160: Details of a Request History Item*.

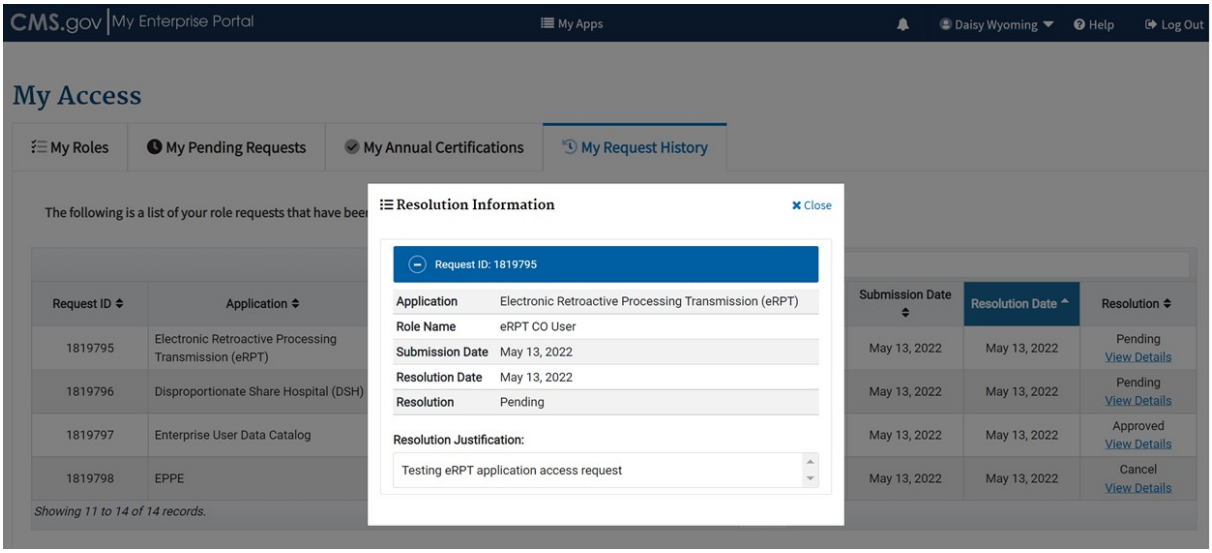

Figure 160: Details of a Request History Item

6. Click **Close** to return to the My Request History page.

10. Appendix: Acronyms

Table 1: Acronyms provides a literal translation of terms used in this document and related to the document.

Table 1: Acronyms

Acronym	Literal Translation
BCI	Business Contact Information
CHIP	Children's Health Insurance Program
CMS	Centers for Medicare & Medicaid Services
DDES	Division of Data Enterprise Services
HHS	Department of Health and Human Services
EDG	Enterprise Data Group
EIT	Electronic and Information Technology
EP (not regularly used)	Enterprise Portal; Portal (preferred)
EUA	Enterprise User Administration
GPO	Government Printing Office
HIPAA	Health Insurance Portability and Accountability Act
ID	Identifier
IDP	Identity Proofing
IE	Internet Explorer
IVR	Interactive Voice Response
LOA	Level of Assurance
MFA	Multi-Factor Authentication
OIT	Office of Information Technology
PHI	Personal Health Information
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIV	Personal Identity Verification
RIDP	Remote Identity Proofing
SMS	Short Message Service
UI	User Interface
VIP	Validation and ID Protection
VPN	Virtual Private Network