Centers for Medicare & Medicaid Services
CMS eXpedited Life Cycle (XLC)

CMS Identity Management User Guide

03/03/2021

1.   Introduction

The Centers for Medicare & Medicaid Services (CMS) is a federal agency that ensures health care coverage for more than 100 million Americans. CMS administers Medicare and provides funds and guidance for all of the 50 states in the nation, for their Medicaid programs and Children's Health Insurance Program (CHIP). CMS works together with the CMS community and organizations in delivering improved and better-coordinated care.

1.1   What is IDM?

CMS has established an Identity Management (IDM) system to provide our Business Partners with a means to apply for, obtain approval, and receive a single User ID they can use to access one or more CMS applications.

1.2   What You May Need Before You Begin

Prior to requesting access, you should have received instructions from your organization or CMS contact. The instructions should include application-specific information you may need to complete the request, such as:

- Social Security Number (SSN) / Taxpayer Identification Number (TIN)

- Legal Business Name (LBN) or Organization

- Application Name

- Application Role

- Other information specific to your application, for example, Contract Number, Gentran Mailbox, National Provider Identifier (NPI), Organization number.

- You will have to create a user ID and password of your choosing if you do not already have a user ID and password. EIDM allows you to create a User ID up to 74 characters. However, some applications have restrictions on the number of characters, and special characters, you can have in the User ID you create. Check with your CMS point of contact to identify restrictions for your application.

- Not every CMS application requires the same information, so it is important to get the specifics directly from your organization or CMS contact.

2. 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).
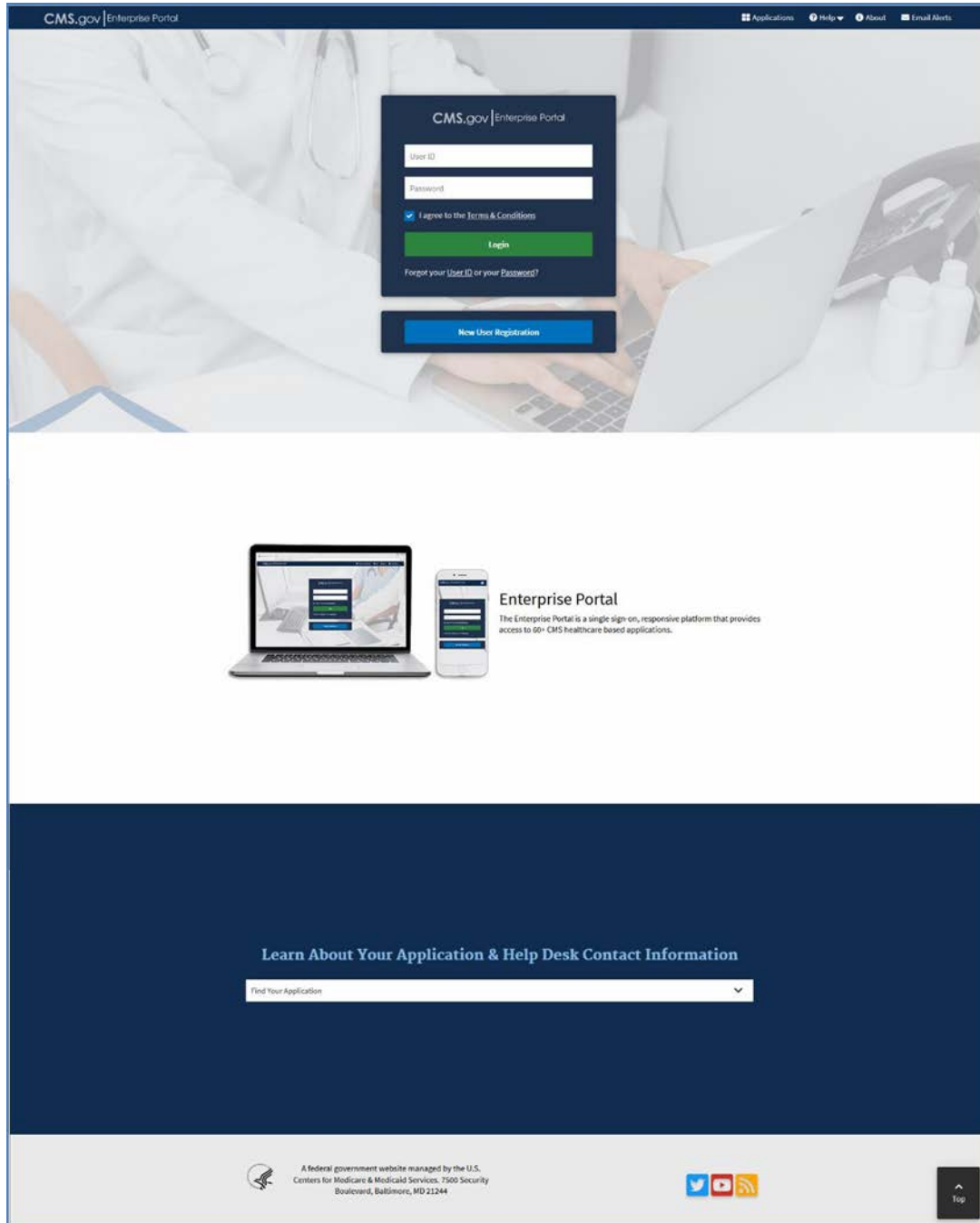

Figure 1: CMS Enterprise Portal Public Home Page

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

2.1   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 redirects users to a help page containing the answers to frequently asked questions.

- ***About link:*** Clicking this link displays information about CMS Enterprise Portal.

- ***Email Alerts link:*** CMS Enterprise Portal email alerts is a communication tool that allows Portal users to subscribe to notification lists, which deliver important and timely CMS information. Users can elect to receive CMS Enterprise Portal email alerts by clicking the Email Alerts link.

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).

2.2   Session Timeout

Session timeout occurs if users do not perform any action on the CMS Enterprise Portal site and remain idle for 15 minutes. When this happens, the session will automatically be terminated, and the user will be required to login again.

2.3   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.
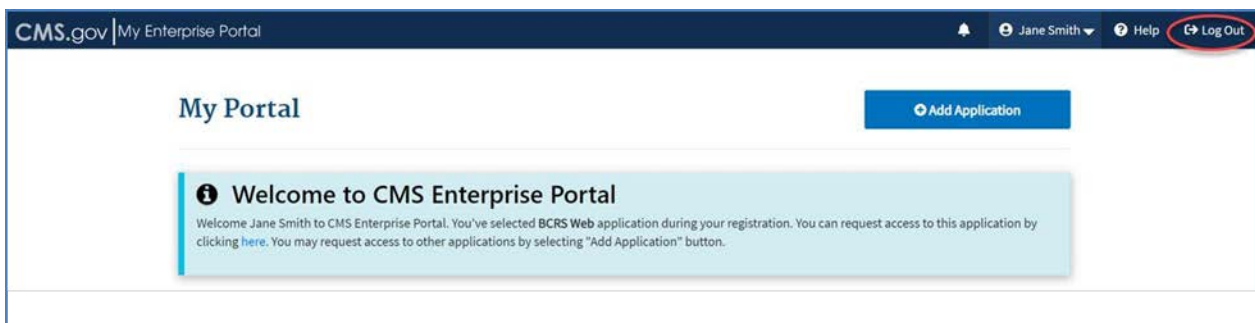

Figure 2: Logging Out of CMS Enterprise Portal

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*.
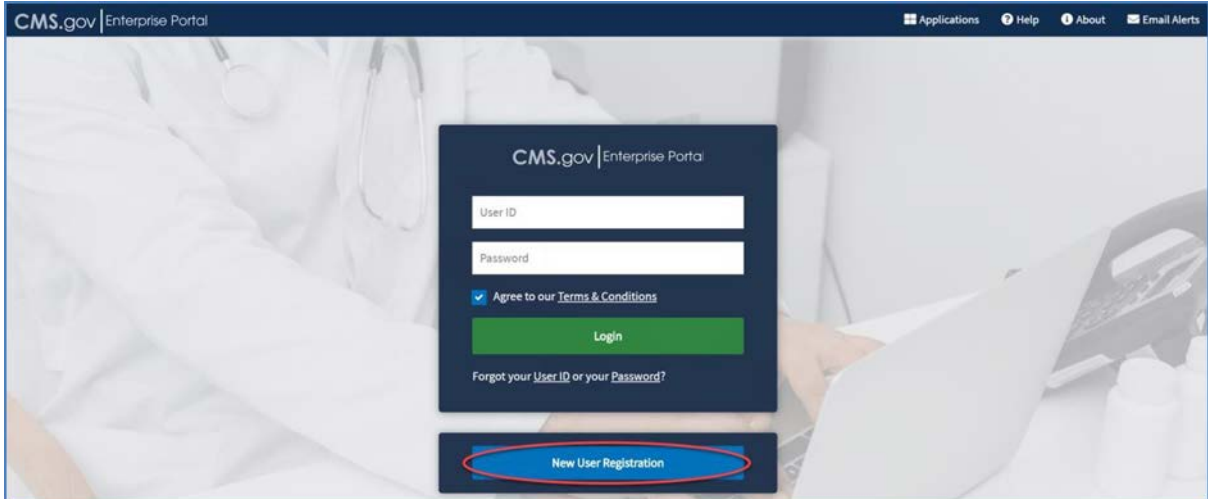

Figure 3: New User Registration Button on Public Home Page

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

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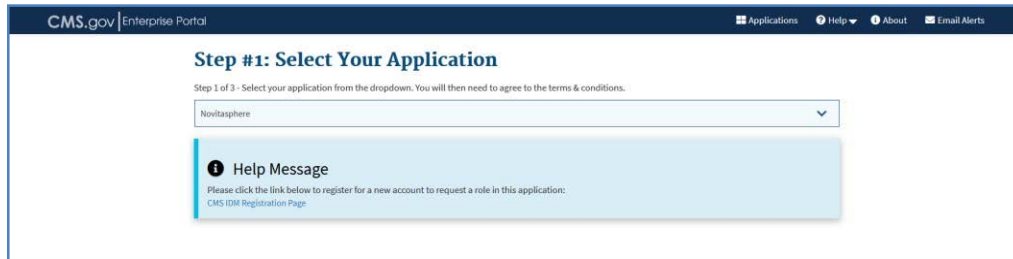
Figure 7: Help Message Displayed on Selecting IDM-Provisioned Application

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.*
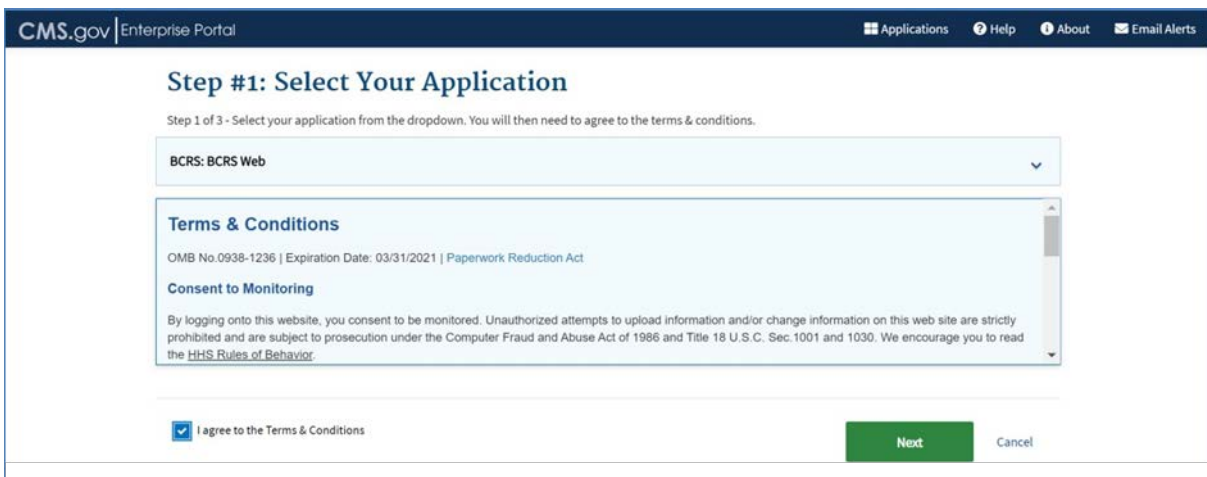
Figure 8: Agreeing to Terms and Conditions

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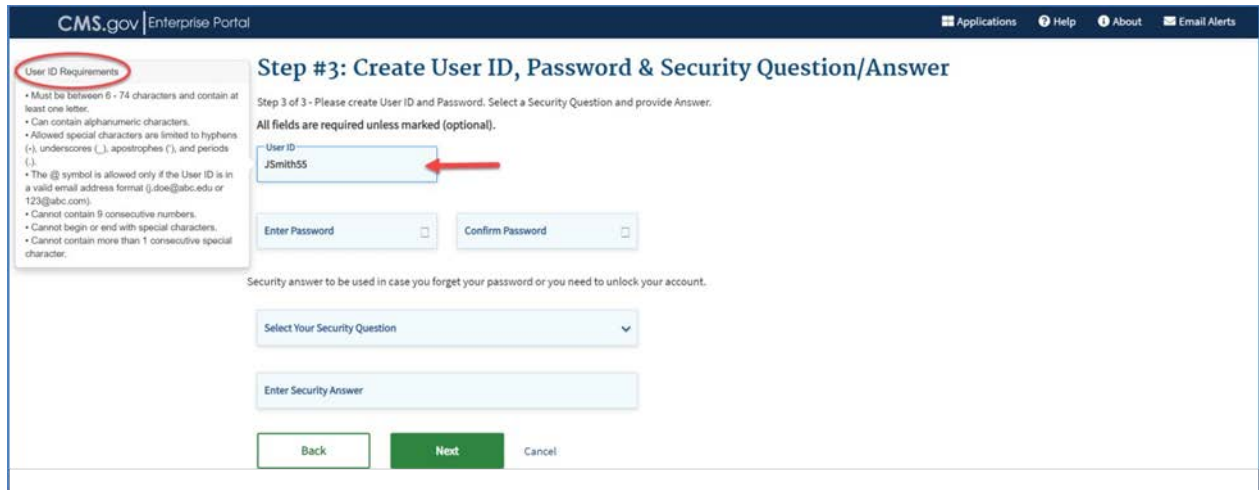
Figure 10: Step 2 of New User Registration - Register Your Information (Completed)

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 a 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 a 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 a tool tip, on what you are required to include in your security question and 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:* Email is automatically setup as the default MFA method (MFA device) once you successfully log in for the first time. 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*.
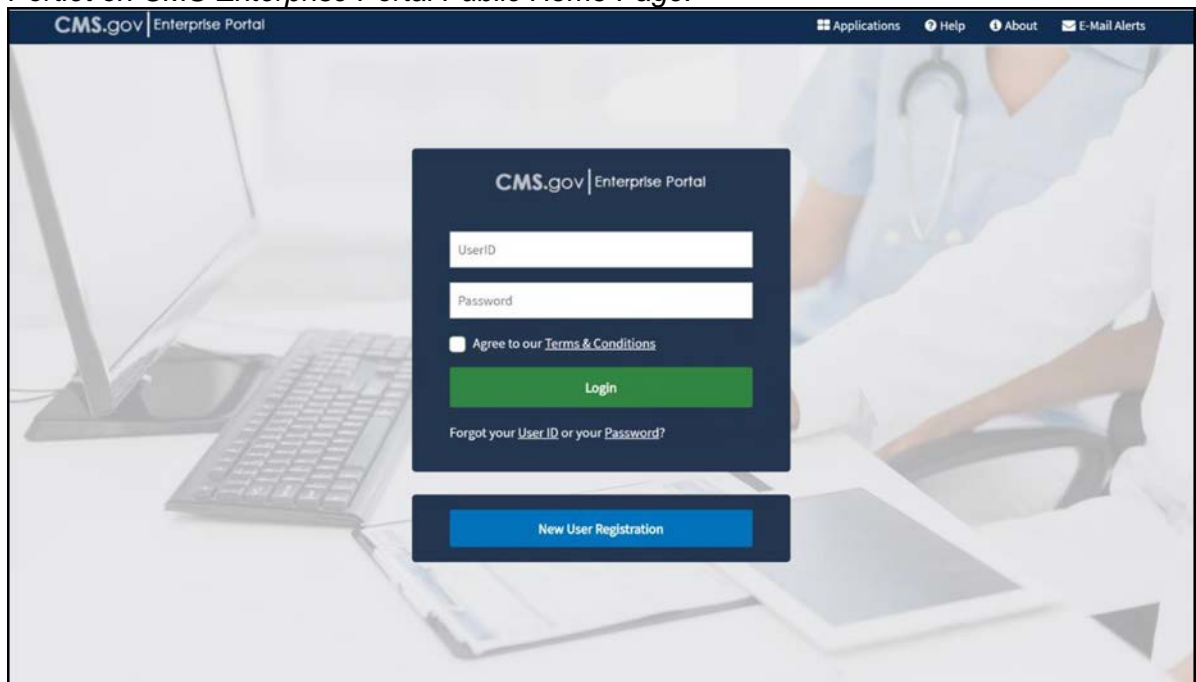

Figure 17: Login Portlet on CMS Enterprise Portal Public Home Page

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.*
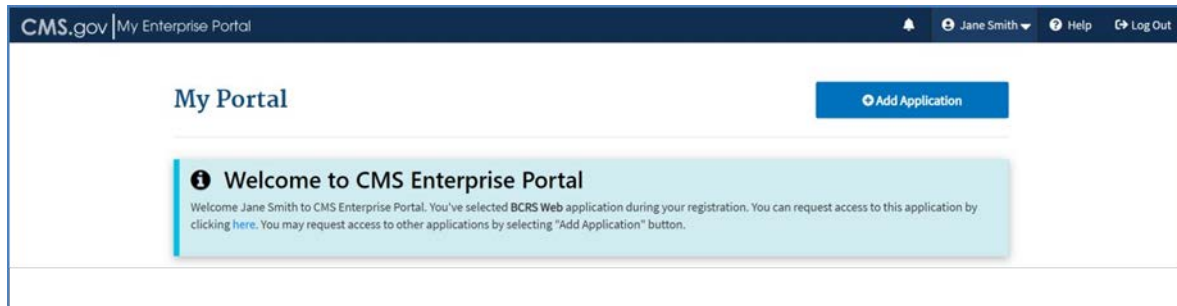

Figure 18: My Portal Page – First Login

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.*
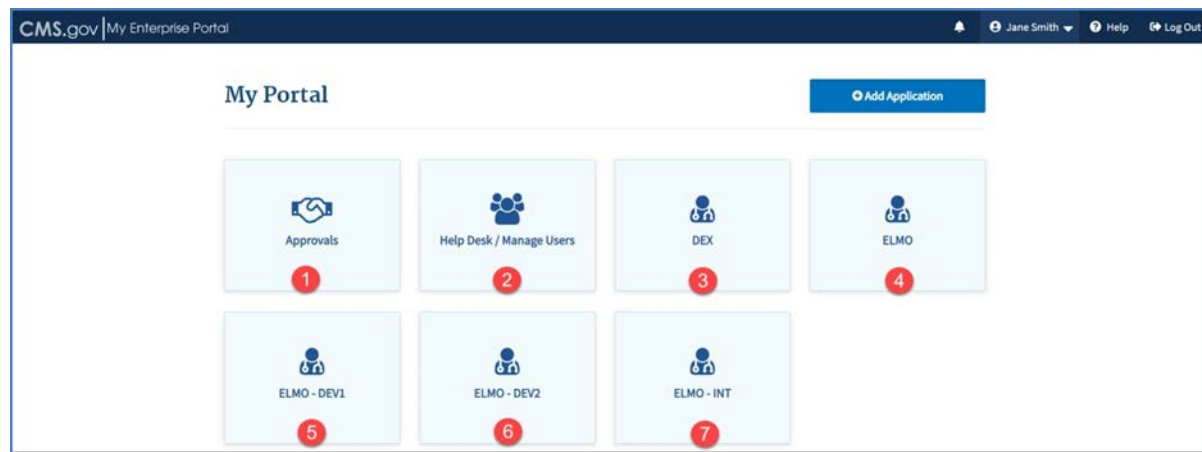

Figure 19: My Portal Page with Applications

The first tile (1) is **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 second tile (2) 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 Approvals and Help Desk/Manage Users functionality is provided in separate user guides.

The next five tiles (3-7) display the CMS applications to which you have access.

A single application role may give you access to multiple tiles for that application. In the example above, ELMO has four tiles while DEX has one tile.

4.2   User Login Using an MFA Device

4.2.1   Email

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

> *Note:* Email is automatically setup as the default MFA method (MFA device) once you successfully log in for the first time. 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 20: Login with MFA Device.* You will be presented with the MFA Devices that you have previously setup.
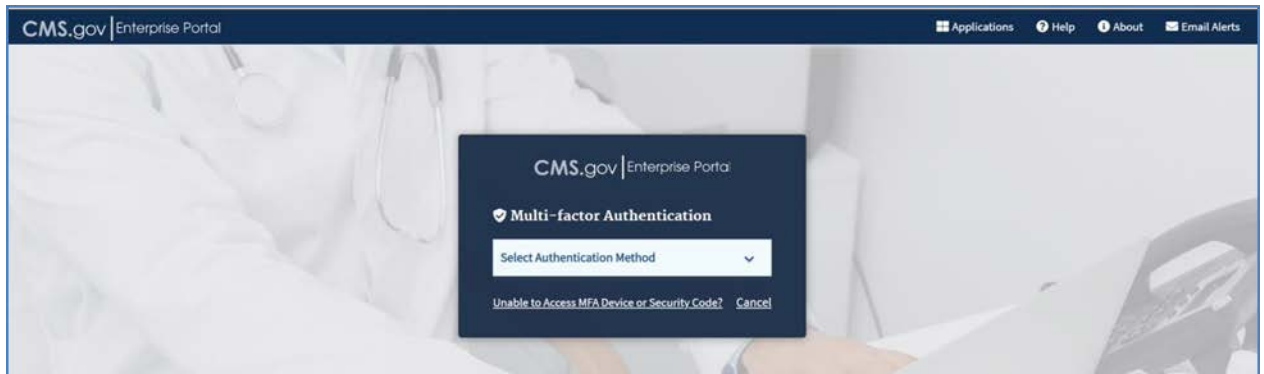

Figure 20: Login with MFA Device

5. Select **Email** as the Authentication Method.

Additional fields are displayed as shown in *Figure 21: Selecting Email Option as MFA Method.* See the MFA Device options described in the subsections *4.2.2* through *4.2.6*.
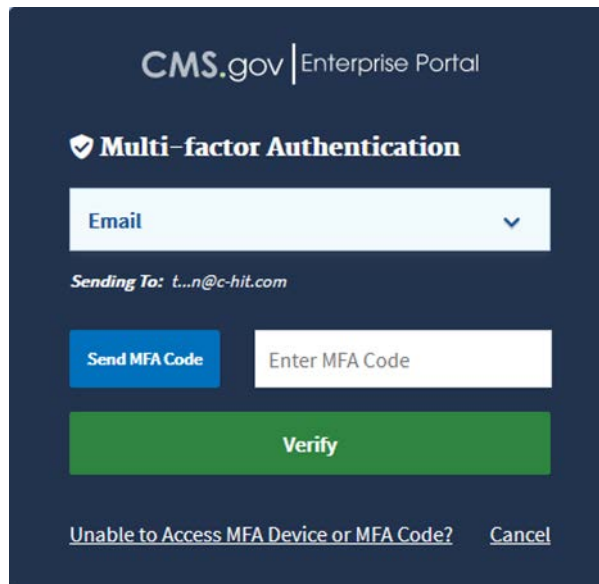

Figure 21: Selecting Email Option as MFA Method

6. Click **Send 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.*

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.

4.2.2   Text Message (SMS)

1. If you select **Text Message (SMS)**, the **Send MFA Code** button and **Enter MFA Code** fields display, as shown in *Figure 22: Selecting Text Message (SMS) Option as MFA Device.*

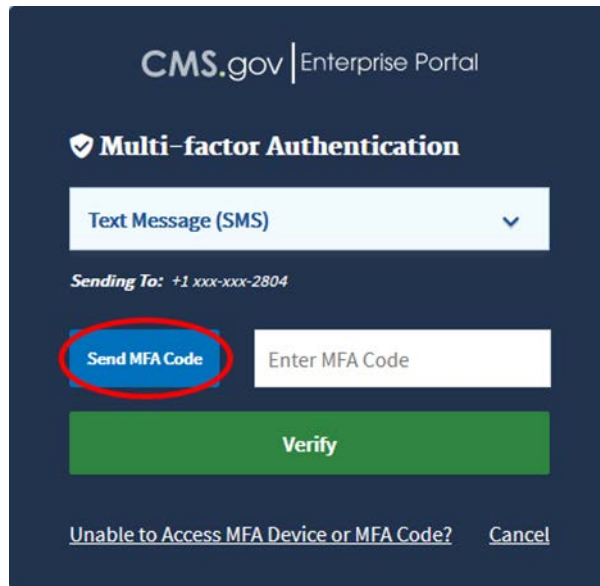2. Click **Send MFA Code** to have the code texted to your registered device.

Figure 22: Selecting Text Message (SMS) Option as MFA Device

3. Enter the MFA code from the text message and click **Verify**.

> ***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   Interactive Voice Response (IVR)

1. If you select **Interactive Voice Response (IVR)**, the **Send MFA Code** button and **Enter MFA Code** fields display, as shown in *Figure 23: Selecting IVR Option as MFA Device.*

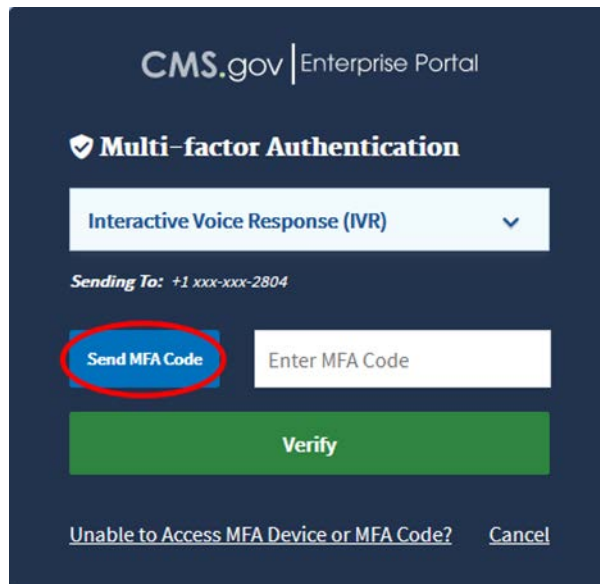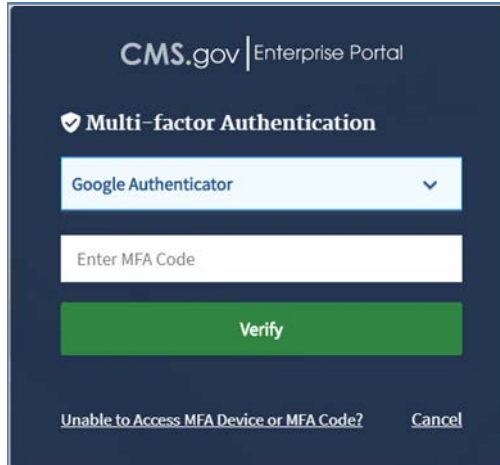2. Click **Send MFA Code** to have the code provided to you via phone call.

Figure 23: Selecting IVR Option as MFA Device

3. Enter the MFA code from the phone call and click **Verify**.

> ***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   Google Authenticator

1. If you select **Google Authenticator**, the **Enter MFA Code** field displays, as shown in *Figure 24: Selecting Google Authenticator Option as MFA Device*.

Figure 24: 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**.

> ***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   Okta Verify

1. If you select **Okta Verify**, the **Send Push** button and the **Enter Code Manually** link display, as shown in *Figure 25: Selecting Okta Verify Option as MFA Device*.
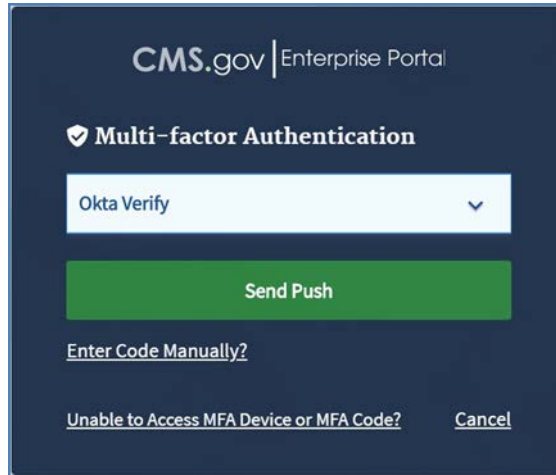

Figure 25: Selecting Okta Verify Option as MFA Device

Option 1: Send Push

2. Click the **Send Push** button to send a notification to your smart phone.

3. Check your smart phone for a pop-up notification from **Okta Verify**.

4. Tap the option to confirm that you are the one signing in.

Option 2: Enter Code Manually

2. Click the **Enter Code Manually** link.

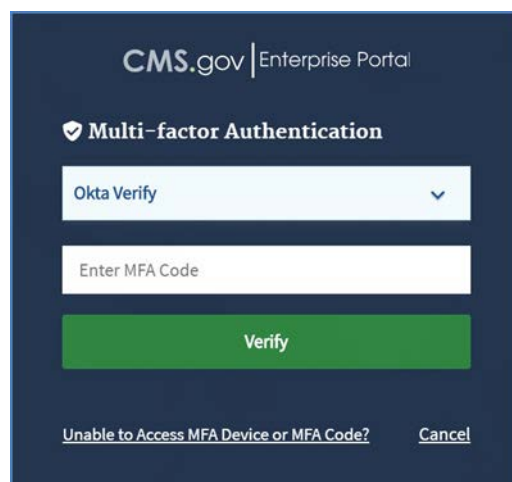The **Enter MFA Code** field displays, as shown in *Figure 26: Okta Verify Option – Enter Code Manually*.

Figure 26: Okta Verify Option – Enter Code Manually

3. Enter the security code from **Okta Verify** and click **Verify**.

4.2.6   YubiKey

1. If you select **YubiKey**, the **Code** field displays, as shown in *Figure 27: Selecting YubiKey Option as MFA Device.*
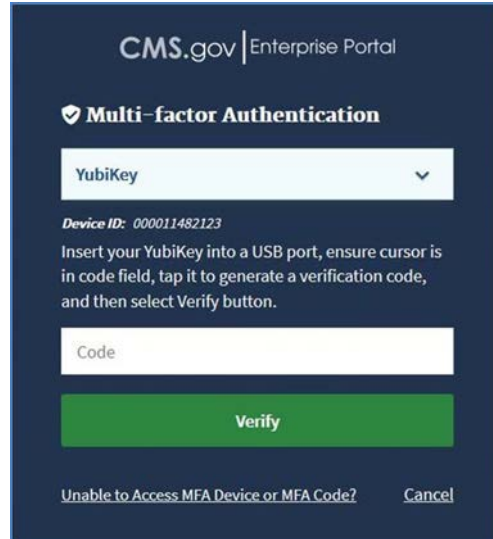

Figure 27: Selecting YubiKey Option as MFA Device

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 28: Code Field Populated with Security Code*.
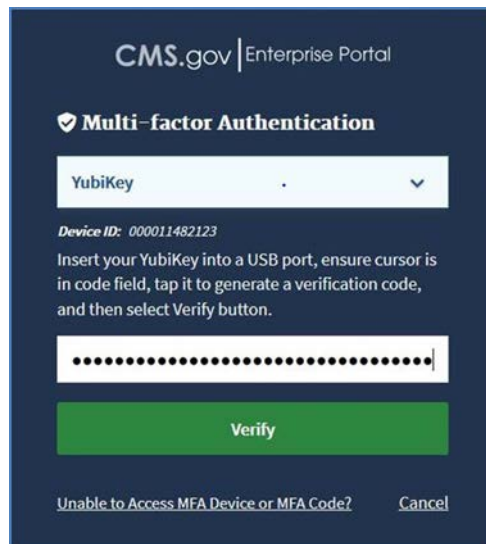

Figure 28: Code Field Populated with Security Code

3. Click **Verify**.

5. Requesting Access

This section provides basic instructions on how to request access to an application and a role.

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.

5.1 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.
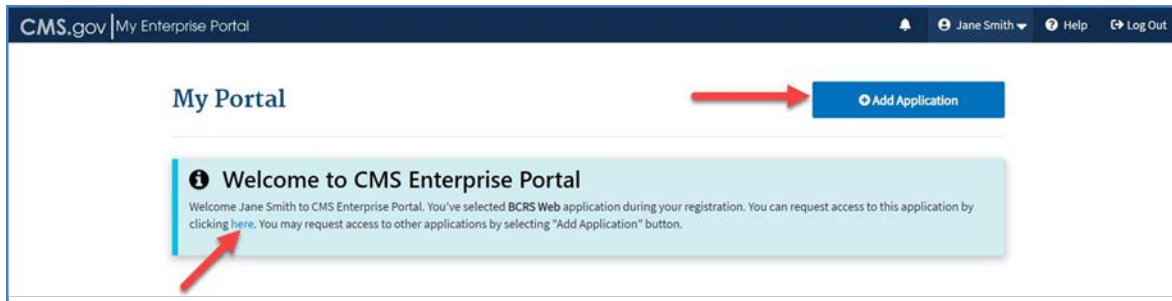

Figure 29: Add Application Button on My Portal Page

The **Add Application** button is available on the **My Portal** page, as shown in *Figure 29: 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 29: Add Application Button on My Portal Page*.
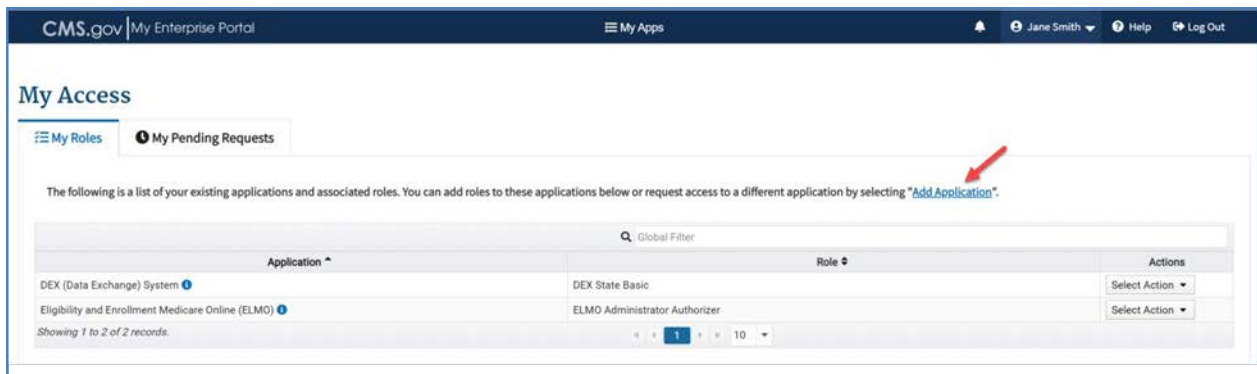

Figure 30: Add Application Link on My Access Page

The **Add Application** link is also present on the **My Access** page, as shown in *Figure 30: 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 31: Accessing the Request Application Access Page via My Apps.*
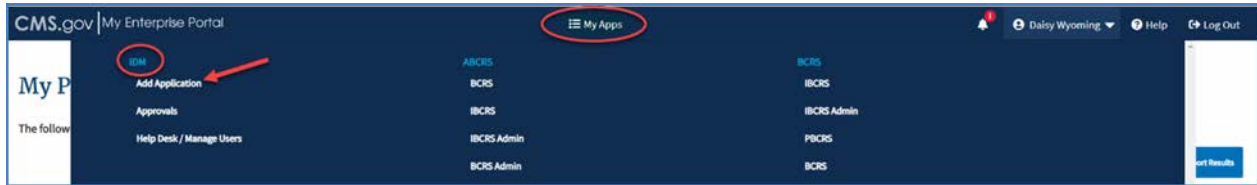

Figure 31: Accessing the Request Application Access Page via My Apps

Clicking the **Add Application** button or link takes you to the **Request Application Access** page, as shown in *Figure 32: Request Application Access Page*.
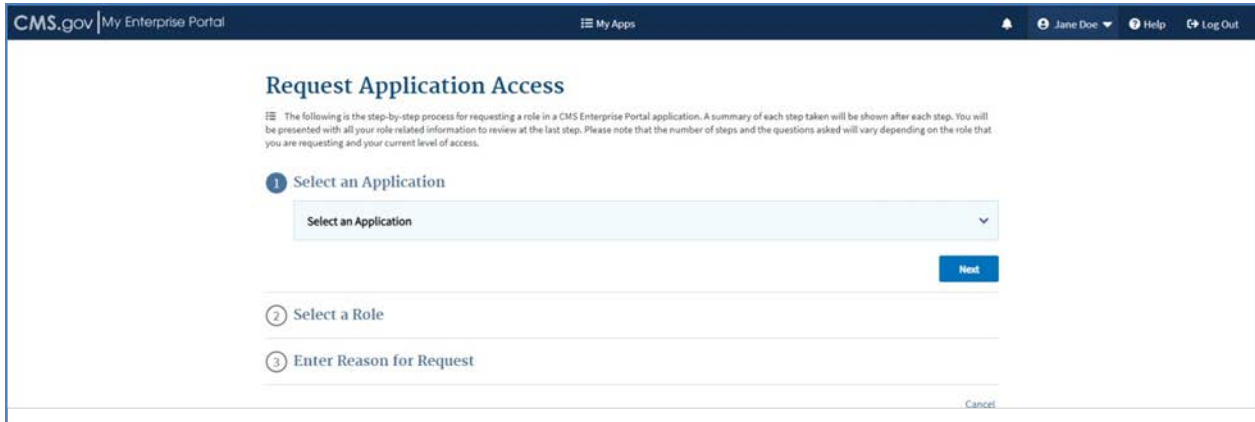
Figure 32: Request Application Access Page

5.2   My Access Page

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

5.2.1   Request access to any CMS application

5.2.2   View a list of your existing applications and associated roles

5.2.3   Add a role to an application you have access to

5.2.4   Remove a role for an application you have access to

5.2.5   View or modify role attributes

5.2.6   View a list of pending role requests submitted for approval

5.2.7   Cancel a pending request

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 33: Accessing the My Access Page via Name Drop-down*.
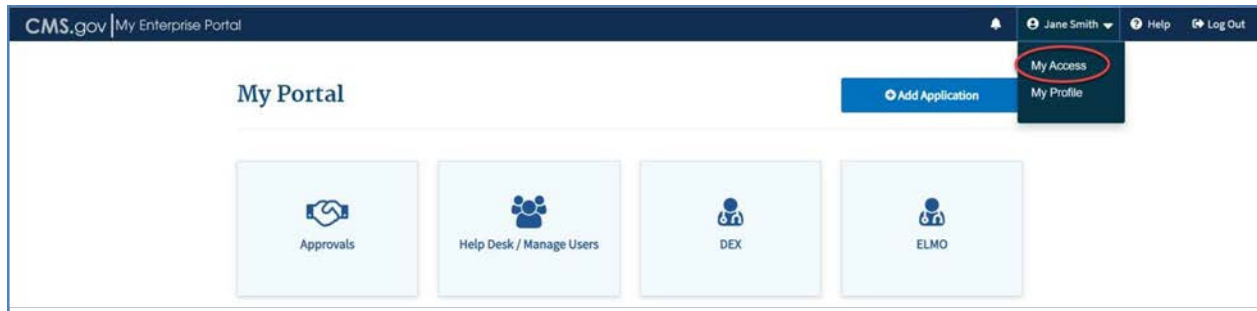
Figure 33: Accessing the My Access Page via Name Drop-down

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

5.2.8 **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 34: My Roles Tab on My Access Page*.
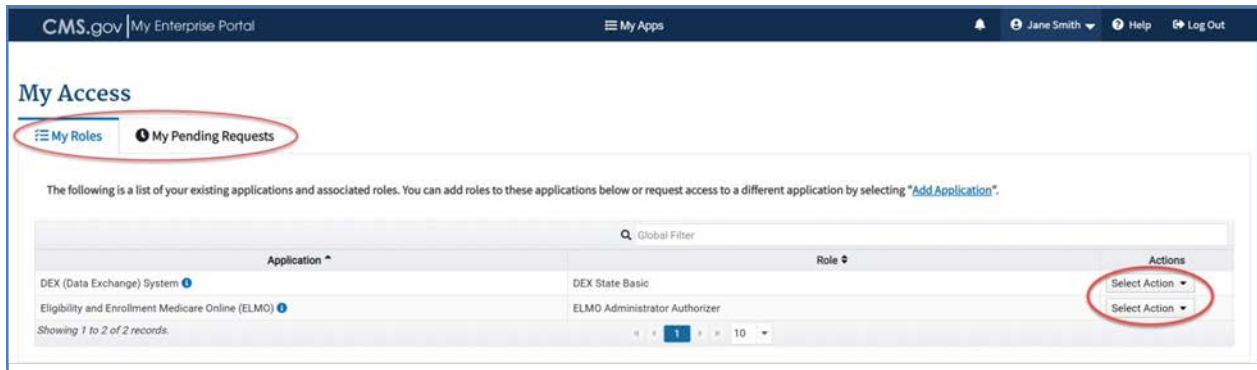

Figure 34: My Roles Tab on My Access Page

The **Select Action** drop-down, as shown in *Figure 34: 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:

5.2.9 Add Role – Directs you to the **Request Application Access** page to request an additional role for the application.

5.2.10 Remove Role – Prompts you to confirm if you wish to remove the role from the application.

5.3 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 35: Role Details*.
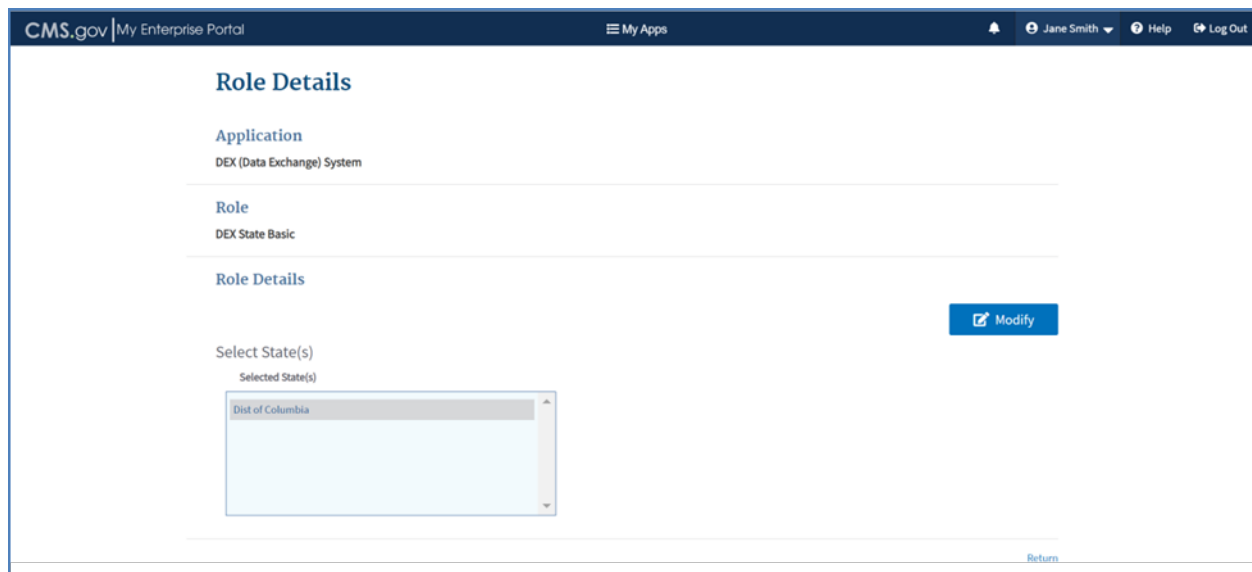
Figure 35: Role Details

5.3.1 **My Pending Requests** – This tab lists the pending requests for which you have requested access. If you currently have pending requests, the page will display as shown in *Figure 36: My Pending Requests Tab on My Access Page*.
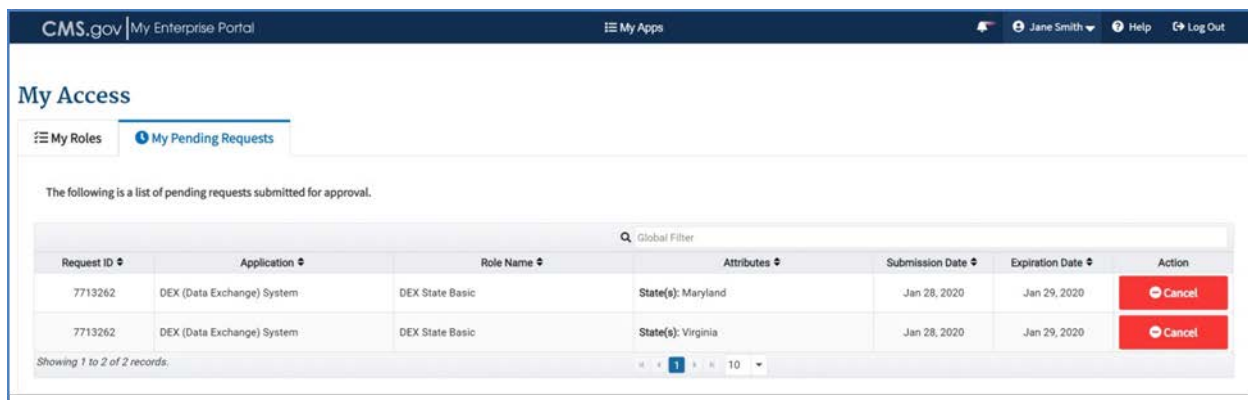

Figure 36: My Pending Requests Tab on My Access Page

5.4 Requesting a Role

The following are the instructions on how to request access to an application and role when you currently do not have a role in the application.

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 37: Add Application Button on My Portal Page*, click the **Add Application** button.

    The **Request Application Access** page displays, as shown in *Figure 37: Request Application Access Page*.

23

4. Choose an application from the **Select an Application** drop-down list. For example, select **DEX (Data Exchange) System**.

    Information about the selected application is displayed as shown in *Figure 37: 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.
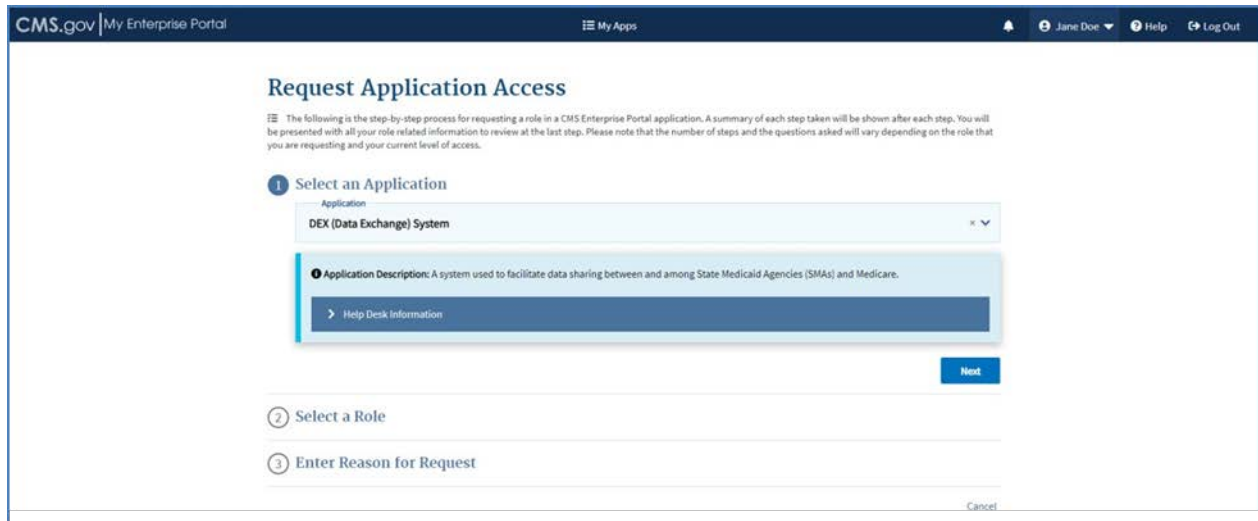
Figure 37: Request Application Access – Selecting an Application

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 38: Request Application Access – Selecting a Role*. For example, select **DEX State Basic**.
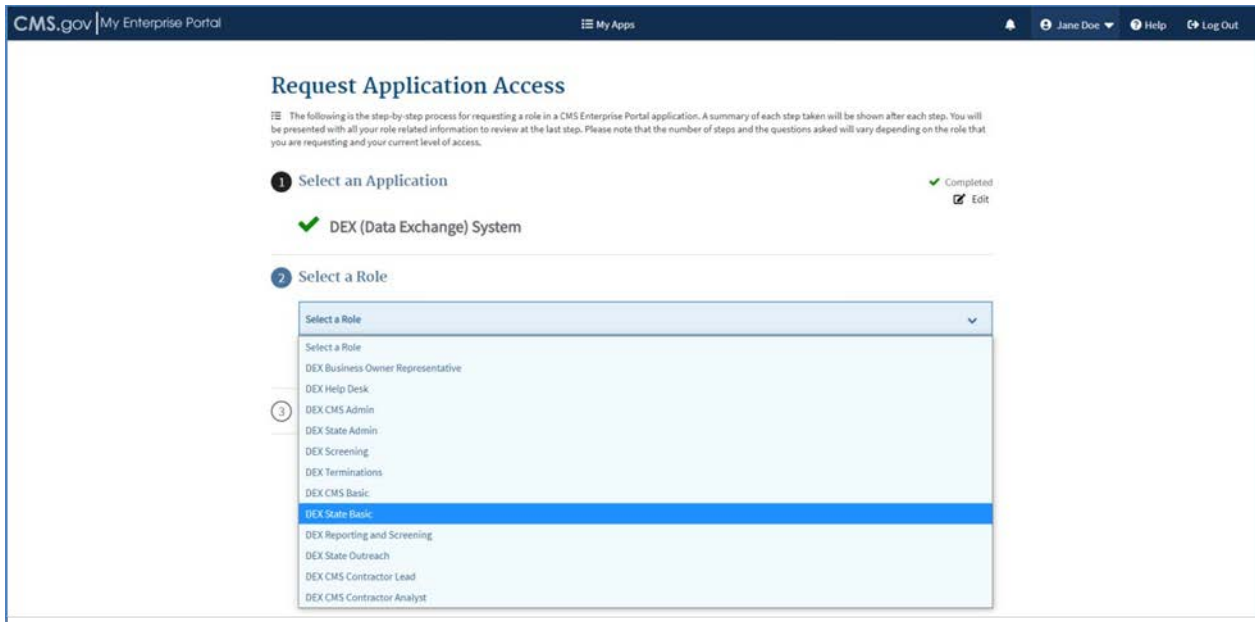
Figure 38: Request Application Access – Selecting a Role

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 DEX State Basic role is selected for the DEX application, the system prompts you to enter the BCI and the Role Details, as shown in *Figure 39: Request Application Access – Additional Information.*
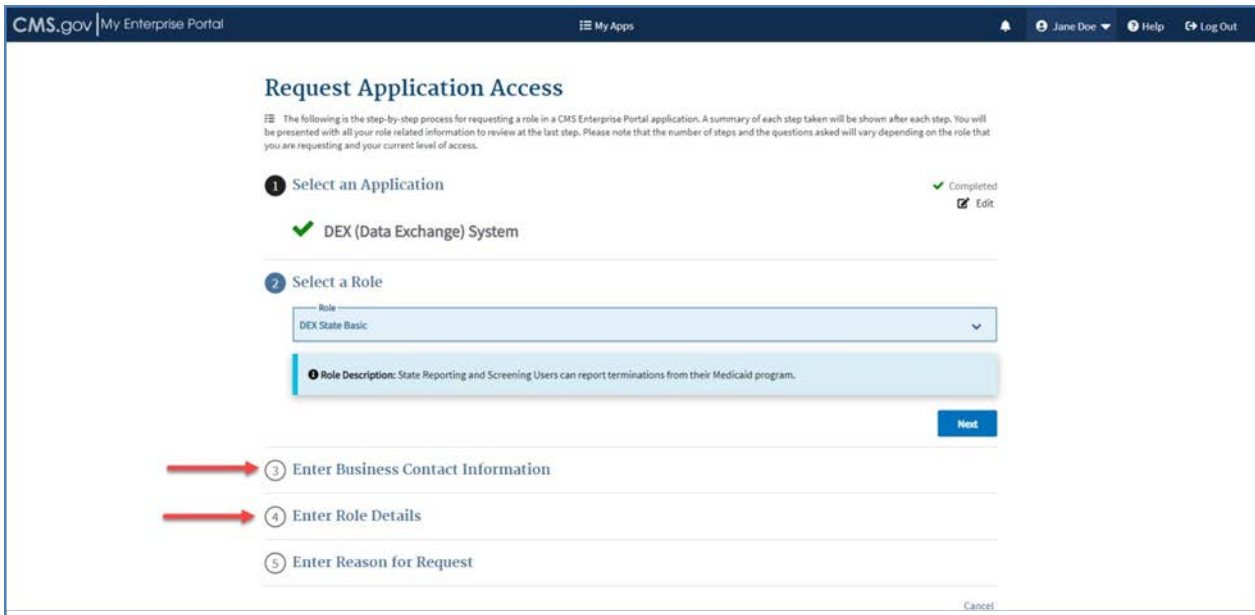
Figure 39: Request Application Access – Additional Information

7. Click **Next** to continue.

8. Provide the information requested in step 3, as shown in *Figure 40: 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 40: Request Application Access – Enter BCI

9. Provide the information, i.e. the role details, requested in step 4, as shown in *Figure 41: 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 41: Requesting Application Access – Role Details

10. Provide the information requested in step 5, as shown in *Figure 42: Requesting Application Access – Reason for Request.*

Figure 42: 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 43: 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.
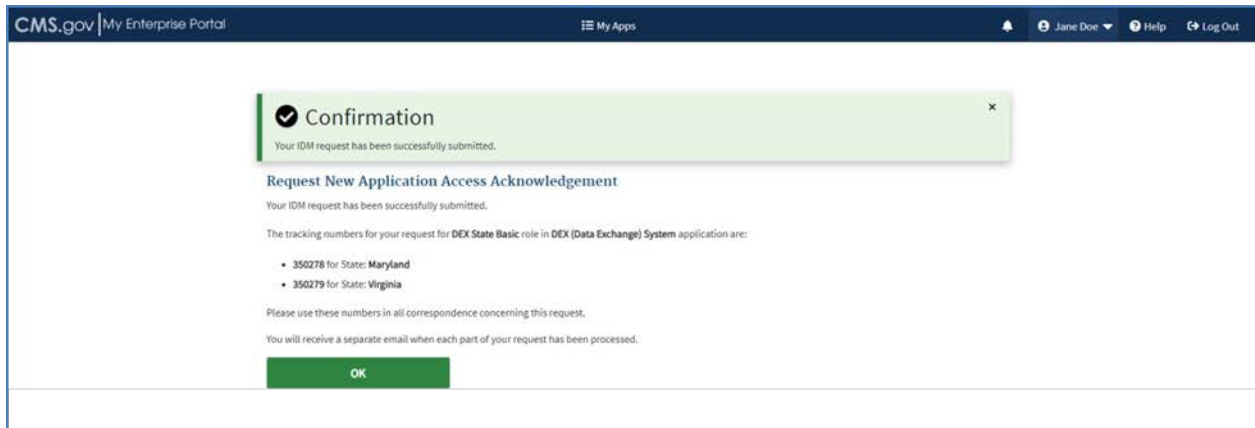

Figure 43: Request Application Access – Success Message

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 44: Request Application Access – Pending Request*.
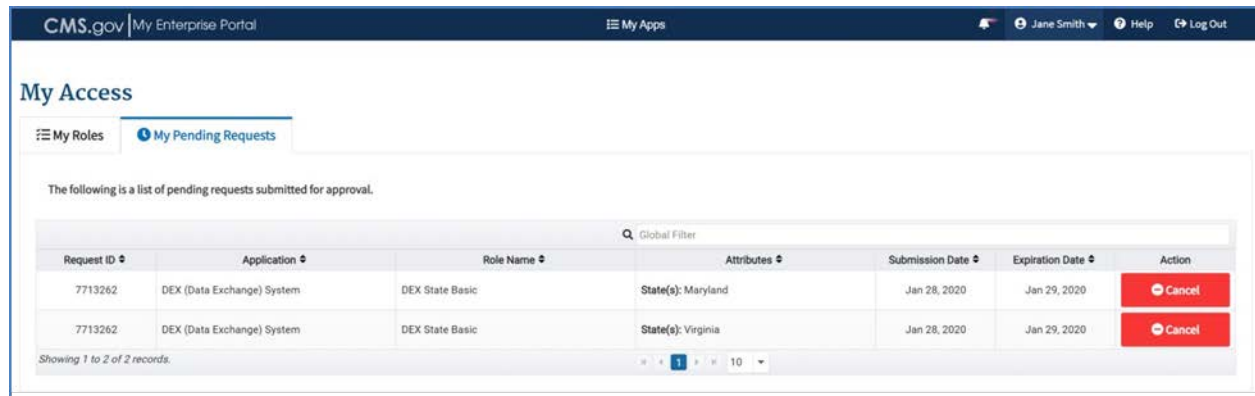

Figure 44: Request Application Access – Pending Request

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.

5.4.1 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:

> 5.4.1.1 Remote Identity Proofing (RIDP) using the CMS Enterprise Portal and Experian's Identity Verification service.
>
> 5.4.1.2 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).
>
> 5.4.1.3 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.

5.4.2 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 45: Role Requiring RIDP*.
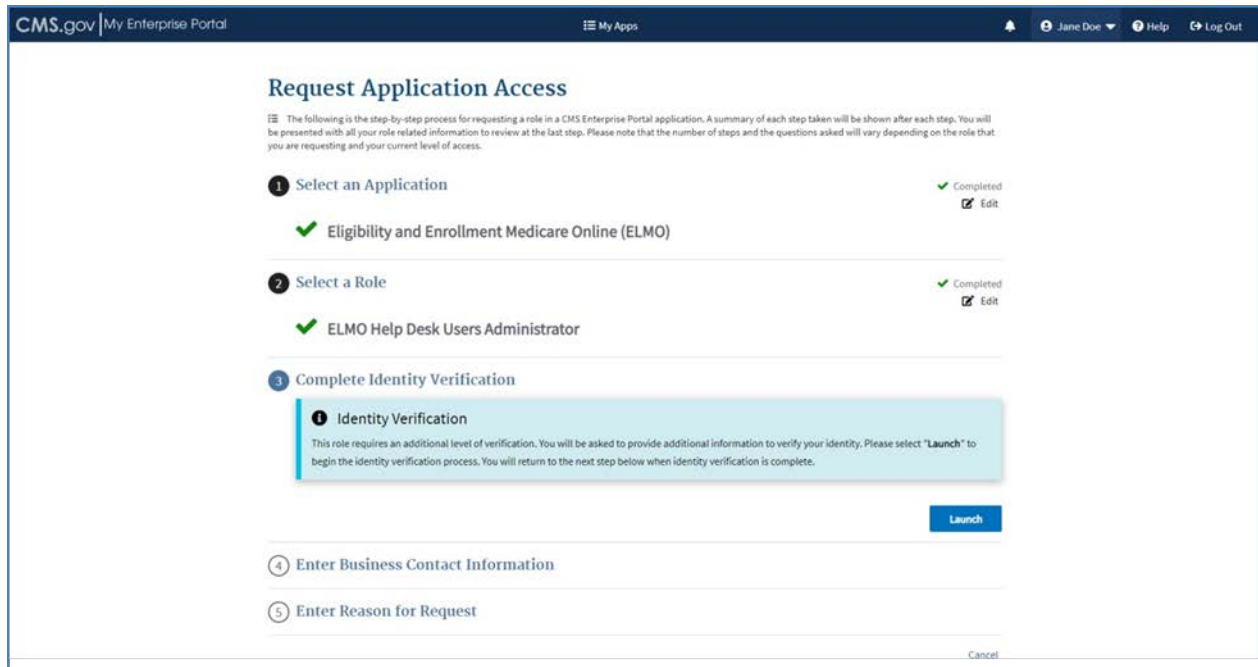

Figure 45: Role Requiring RIDP

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

The **Step #1: Identity Verification Overview** page displays, as shown in *Figure 46: RIDP – Overview.*

Figure 46: RIDP – Overview

5. Click **Next** to continue.

The **Step #2: Accept Terms & Conditions** page displays, as shown in *Figure 47: RIDP – Terms and Conditions Information.*

Figure 47: 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 48: RIDP – Your Information Page*.

Figure 48: 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 49: RIDP – Verify Identity*.

Figure 49: 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 50: RIDP – Confirmation Message*.
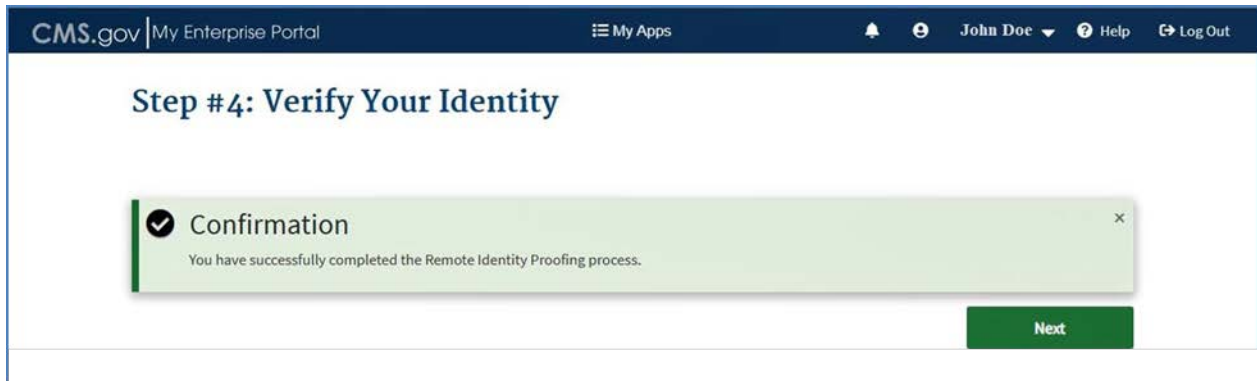

Figure 50: RIDP – Confirmation Message

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 complete 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