Centers for Medicare & Medicaid Services

CMS eXpedited Life Cycle (XLC)

CMS Enterprise Portal User Manual

Document Version 6.0

11/13/2017

Document Number: Enterprise_Portal_User_Manual_v6

Section 508 Compliant

Table of Contents

1. Introduction 1

2. Overview 2

2.1 Conventions 2
2.2 Cautions & Warnings 2

3. Getting Started 3

3.1 Set-up Considerations 3
3.2 User Access Considerations 3
3.2.1 EUA Process 3
3.2.2 EIDM Process 4
3.3 Accessing the System 4
3.4 Public Landing Page 6
3.5 Session Timeout 6
3.6 Exiting the System 6

4. Registering for CMS Enterprise Portal 8

5. Logging In 19

5.1 User Login Without a Registered MFA Device 19
5.2 User Login Using an MFA Device 22
5.2.1 Tablet/PC/Laptop 24
5.2.2 Text Message (SMS) 25
5.2.3 Interactive Voice Response (IVR) 26
5.2.4 Email 27
5.2.5 One Time Security Code 28

6. Forgot User ID 29

7. Forgot Password 31

8. Unlocking Account 34

9. User Profile 38

9.1 Viewing Your Profile 38
9.2 Changing Your Profile 39
9.3 Changing Your Password 43
9.4 Changing Your Challenge Questions 45
9.5 Registering Multi-Factor Authentication (MFA) 46
9.6 Removing MFA 54

10. Requesting Access 57

10.1 Application Access Catalog 57
10.2 Access Catalog Features 58

10.3 Requesting a Role 60

Appendix A: Record of Changes 65

Appendix B: Acronyms 66

Appendix C: Glossary 67

Appendix D: Referenced Documents 69

Appendix E: Approvals 70

List of Figures

Figure 1: CMS Enterprise Portal Public Landing Page 5

Figure 2: Logging Out of CMS Enterprise Portal 7

Figure 3: New User Registration Button on Landing Page 8

Figure 4: Step 1 of New User Registration – Choose Your Application 8

Figure 5: Terms & Conditions Information Displayed on Selecting EIDM-Provisioned Application 9

Figure 6: Help Message Displayed on Selecting EUA-Provisioned Application..... 9

Figure 7: Agreeing to Terms and Conditions 10

Figure 8: Step 2 of New User Registration - Register Your Information (Blank) ... 11

Figure 9: Step 2 of New User Registration - Register Your Information (Completed) 12

Figure 10: Step 3 of New User Registration – Create User ID, Password & Challenge Questions (Blank) 13

Figure 11: Step 3 of New User Registration – User ID Entered 14

Figure 12: Step 3 of New User Registration – Password Entered 15

Figure 13: Step 3 of New User Registration – Create User ID, Password & Challenge Questions (Completed) 16

Figure 14: New User Registration – Registration Summary 17

Figure 15: New User Registration – Confirmation 18

Figure 16: Login Portlet on CMS Enterprise Portal Public Landing Page 19

Figure 17: MFA Status Check 20

Figure 18: My Portal Page – First Login 20
Figure 19: My Portal Page with Apps 21
Figure 20: View Apps 21
Figure 21: Login with MFA Device 22
Figure 22: MFA Device Options 23
Figure 23: Selecting Tablet/PC/Laptop Option as MFA Device 24
Figure 24: VIP Access 24
Figure 25: Selecting Text Message (SMS) Option as MFA Device 25
Figure 26: Selecting IVR Option as MFA Device 26
Figure 27: Selecting Email Option as MFA Device 27
Figure 28: Selecting One Time Security Code Option as MFA Device 28
Figure 29: Forgot User ID Link 29
Figure 30: Forgot User ID – Blank Page 29
Figure 31: Invalid Data Error 30
Figure 32: Forgot User ID – Successful Confirmation 30
Figure 33: Forgot Password Link 31
Figure 34: Forgot Password – Enter User ID 31
Figure 35: Invalid Data Error 32
Figure 36: Forgot Password – Blank Form 32
Figure 37: Invalid Data Error 33
Figure 38: Forgot Password – Successful Confirmation 33
Figure 39: Incorrect Credentials Error Message 34
Figure 40: Account Locked Message 35
Figure 41: Correct User ID on Unlock Account Page 35
Figure 42: Incorrect User ID Error Message on Unlock Account Page 35
Figure 43: Unlock My Account – Challenge Questions 36
Figure 44: Challenge Questions – Invalid Data 36

Figure 45: Unlock Account – Successful Confirmation 37
Figure 46: My Portal Page – My Profile Drop-down 38
Figure 47: View My Profile 39
Figure 48: Change My Profile 40
Figure 49: Change Profile 41
Figure 50: Challenge Questions – Invalid Data 41
Figure 51: Change Profile Information 42
Figure 52: Update Profile – Successful Confirmation 42
Figure 53: Change Password 43
Figure 54: Password Guidelines Not Met 43
Figure 55: Change Password – Tool Tip 44
Figure 56: Password Requirements 44
Figure 57: Change Password – Successful Confirmation 45
Figure 58: Change Challenge Questions – Login 45
Figure 59: Change Challenge Questions – Update Information 46
Figure 60: Incorrect Credentials Error Message 46
Figure 61: Change Password – Successful Confirmation 46
Figure 62: Register MFA 48
Figure 63: Register MFA – Choose MFA Device 48
Figure 64: Register Phone/Tablet/PC/Laptop 49
Figure 65: VIP Access 50
Figure 66: Register MFA Device – Successful Confirmation 50
Figure 67: Register Text Message (SMS) 51
Figure 68: Register MFA Device – Successful Confirmation 51
Figure 69: Register Interactive Voice Response (IVR) 52
Figure 70: Register MFA Device – Successful Confirmation 53
Figure 71: Register E-mail 53

Figure 72: Register MFA Device – Successful Confirmation 54

Figure 73: Remove MFA 54

Figure 74: Remove MFA Device 55

Figure 75: Remove MFA Device – Successful Confirmation 55

Figure 76: Only One MFA Registered Device 56

Figure 77: Register New Device Error 56

Figure 78: Accessing the Application Catalog 57

Figure 79: Access Catalog Page 58

Figure 80: Features of Access Catalog 59

Figure 81: Searching for an Application 60

Figure 82: Requesting Access for an Application 61

Figure 83: Request New System Access Page 61

Figure 84: Identity Verification Page 61

Figure 85: Terms and Conditions Information 62

Figure 86: Your Information Page 62

Figure 87: Multi-Factor Authentication Information Page 63

Figure 88: Register Your Phone, Computer, or E-Mail Page 63

Figure 89: MFA Success Message 64

Figure 90: Request Acknowledgement Page 64

List of Tables

Table 1: Record of Changes 65

Table 2: Acronyms 66

Table 3: Glossary 67

Table 4: Referenced Documents 69

Table 5: Document Approval 70

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.

The CMS Enterprise Portal UI was originally designed in 2011. CMS Enterprise Portal has grown significantly since that time, adding content and features. The CMS Enterprise Portal UI is currently being redesigned to address the following goals:

- Simplify logon process
- Improve user experience
- Improve responsiveness
- Upgrade the CMS Enterprise Portal’s authentication mechanism, Enterprise Identity Management (EIDM)

This User Manual 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).

2. Overview

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 Enterprise Portal allows for a common gateway for applications, data query, analysis, and reporting needs for a variety of users. This flexible, convenient, and comprehensive access to data promotes activities across the CMS enterprise, and increases the overall return on investment in the modern CMS data environment.

2.1 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.

2.2 Cautions & Warnings

The following items should be considered prior to accessing CMS Enterprise Portal:

- CMS Enterprise Portal users are provisioned by the Enterprise User Administration (EUA) process and the Enterprise Identity Management (EIDM) process. Users must have their CMS identifier (ID) added to the relevant Portal job code or role (additional information is in *Section 3.2 - User Access Considerations)*.
- CMS screens are designed to be viewed at a minimum screen resolution of 1024 x 768. For optimal performance, screen resolution should be set to 1920 x 1080.
- Pop-up blockers must be disabled prior to attempting access to CMS Enterprise Portal.
- JavaScript must be enabled.

3. Getting Started

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

3.1 Set-up Considerations

CMS screens are designed to be viewed at a minimum screen resolution of 1024 x 768. For optimal performance, screen resolution should be set to 1920 x 1080. The following additional considerations optimize access to CMS Enterprise Portal:

- Disable pop-up blockers prior to accessing CMS Enterprise Portal.
- Use one of the following browsers with JavaScript enabled:
  - Internet Explorer (IE), version 11.0 or higher
  - Chrome (recommended for optimal performance)
  - Firefox
  - Safari

The only computer input device needed to access CMS Enterprise Portal is a keyboard; a mouse is not required, although it is recommended. For output devices, a monitor is required. A computer printer is also a required output device if a user wishes to print any portion of CMS Enterprise Portal.

3.2 User Access Considerations

CMS Enterprise Portal users are provisioned by the EUA process or the EIDM process, depending on the application(s) they will be accessing. These provisioning processes are described in *Section 3.2.1 - EUA Process* and *Section 3.2.2 - EIDM Process*. CMS Enterprise Portal users can only view the applications to which they have been granted access through the respective job code(s).

3.2.1 EUA Process

For applications provisioned via EUA, if a user does not have a 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 applications it hosts. If access is granted, the user will be notified by e-mail 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, click the link below, follow the log-in procedures, and click on the *Change My Password* link after signing in:

- 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.

3.2.2 EIDM Process

For applications provisioned via EIDM, if a user does not have a CMS user ID, they must register for a CMS account from the landing page of CMS Enterprise Portal by clicking on the *New User Registration* link. Detailed steps are in Section *4 - Registering for CMS Enterprise Portal.*

Note: CMS user IDs created using the EIDM process are a minimum of six and maximum of 74 characters in length.

Once an EIDM user is registered 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 Welcome drop-down menu displayed in the top navigation bar.

3.3 Accessing the System

To access CMS Enterprise Portal, open a browser window (refer to the list of approved browsers in Section *3.1 - 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 landing page, as shown in *Figure 1: CMS Enterprise Portal Public Landing* Page.

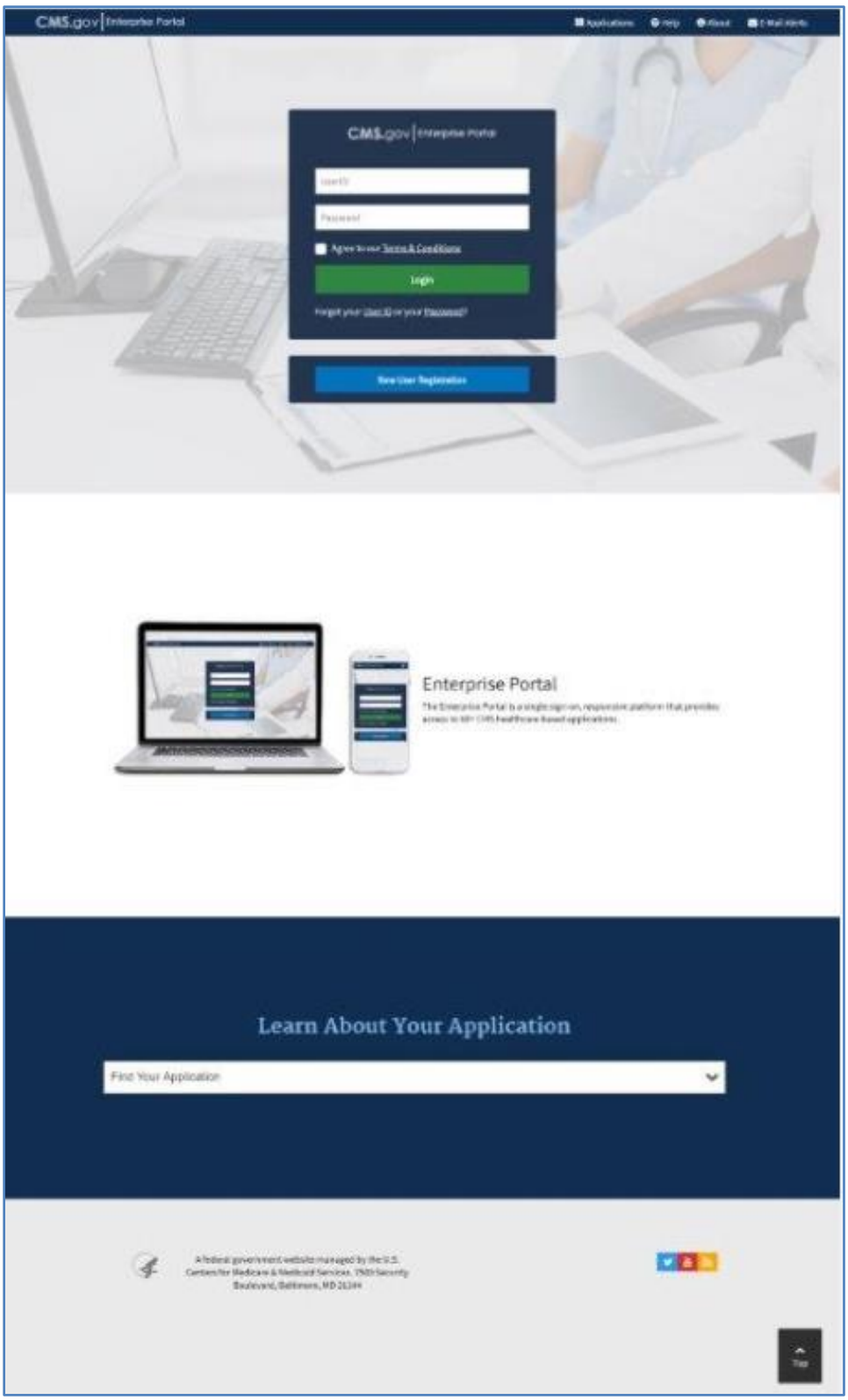

Figure 1: CMS Enterprise Portal Public Landing Page

3.4 Public Landing Page

The first page users will see when accessing CMS Enterprise Portal is the public landing page as shown in *Figure 1: CMS Enterprise Portal Public Landing* 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 landing page.
- ***Applications:*** Clicking this link allows users to select their application from a drop-down menu and view their application's helpdesk and support information.
- ***Help link:*** Clicking this link redirects users to a help page containing general help information.
- ***About link:*** Clicking this link displays information about CMS.
- ***E-Mail 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 E-Mail 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 landing page also provides the registration functionality for new users and login functionality for users who have already been authenticated.

3.5 Session Timeout

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

3.6 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 the user out and returns to the CMS Enterprise Portal public landing page.

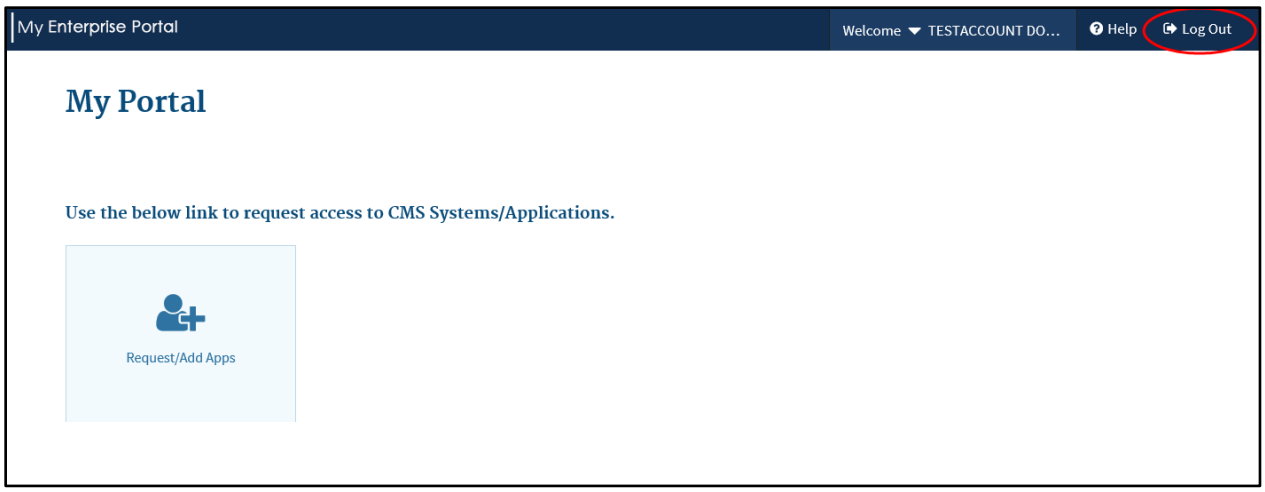

Figure 2: Logging Out of CMS Enterprise Portal

4. Registering for CMS Enterprise Portal

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

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

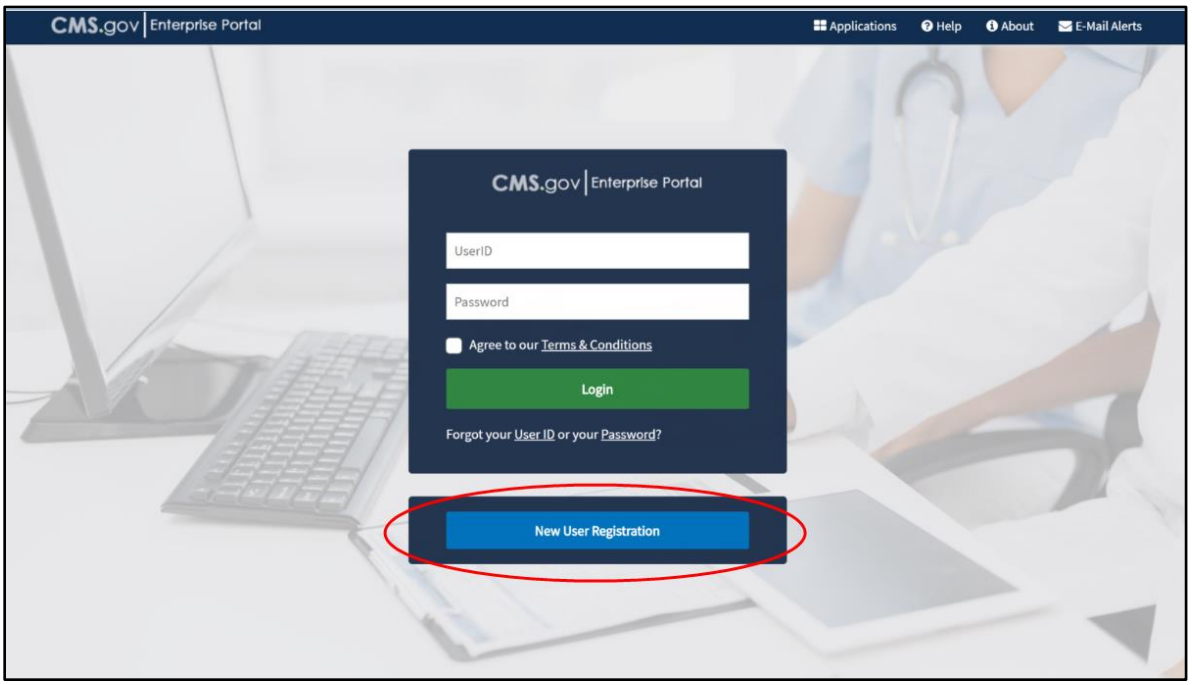

Figure 3: New User Registration Button on Landing Page

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

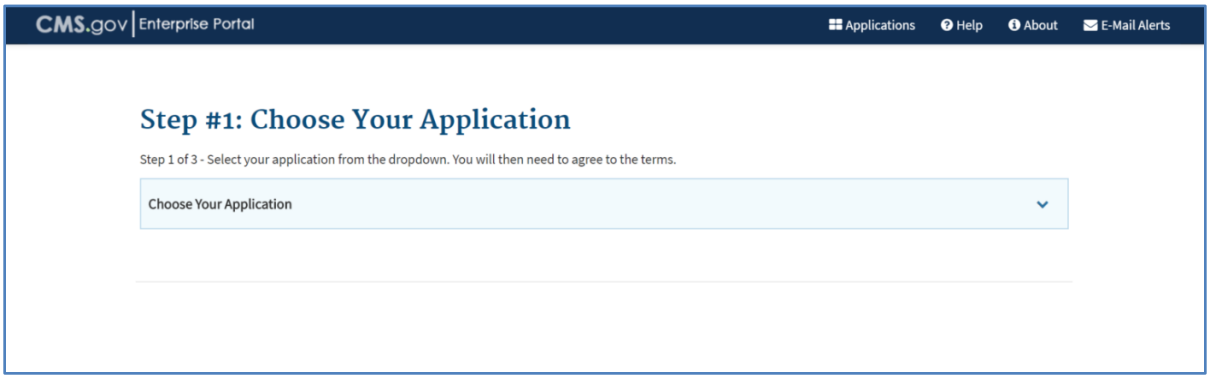

Figure 4: Step 1 of New User Registration – Choose Your Application

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

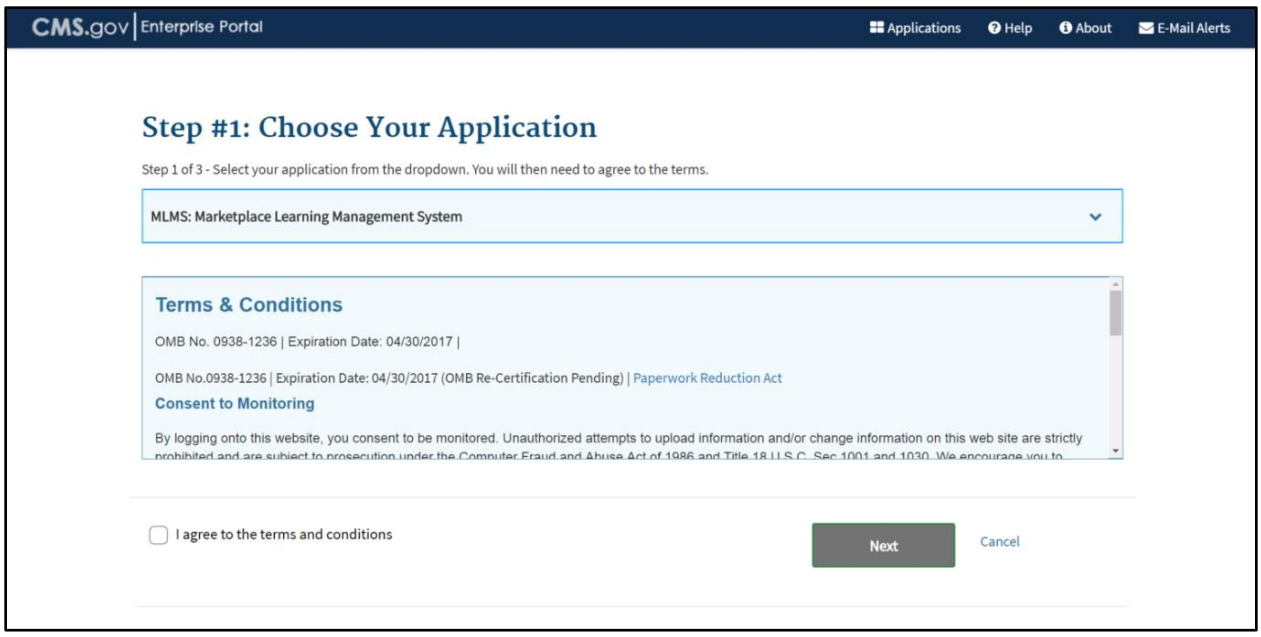

Figure 5: Terms & Conditions Information Displayed on Selecting EIDM-Provisioned Application

Note: Terms & Conditions are displayed only when an EIDM-provisioned application is selected from the **Choose 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*.

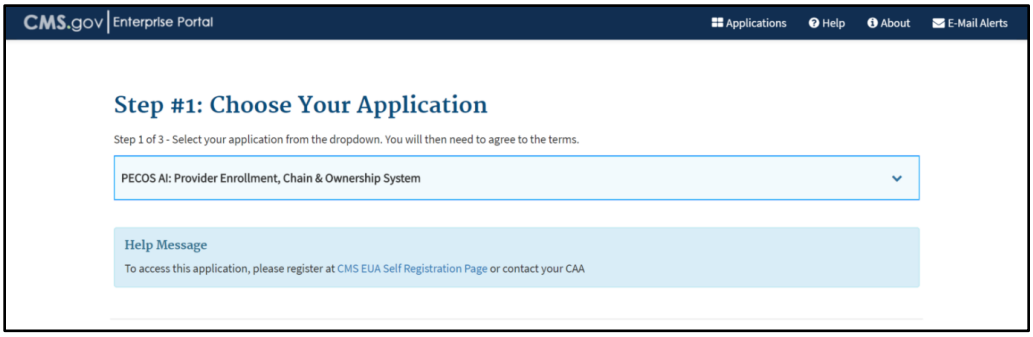

Figure 6: Help Message Displayed on Selecting EUA-Provisioned Application

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 7: Agreeing to Terms and Conditions.*

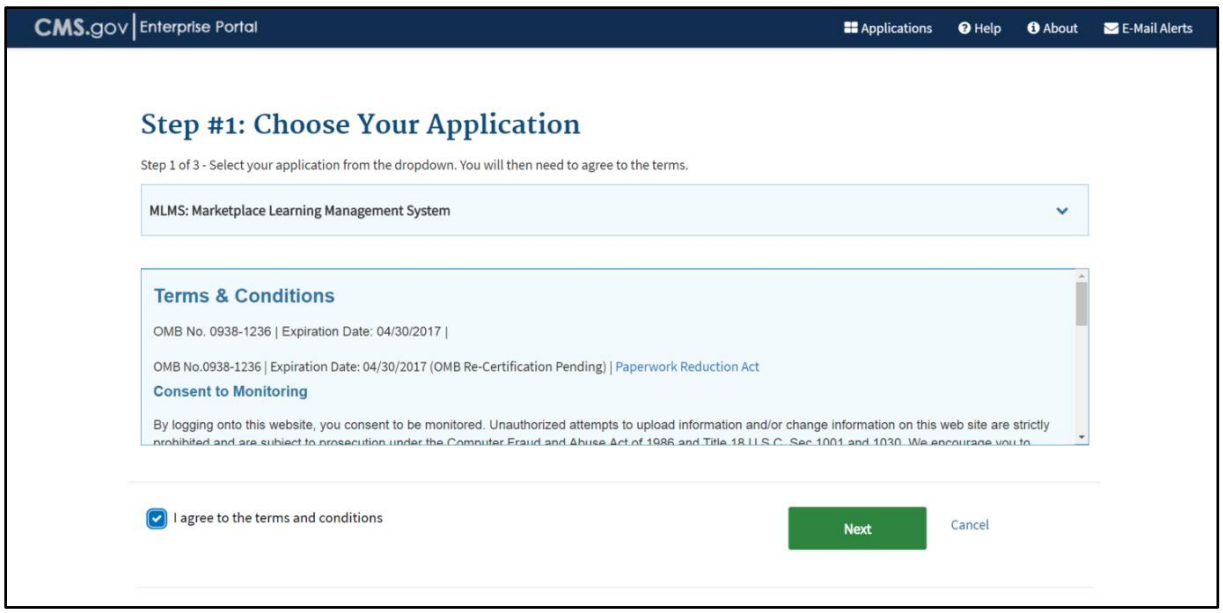

Figure 7: Agreeing to Terms and Conditions

The **Step #2: Register Your Information** page displays, as shown in *Figure 8: Step 2 of New User Registration - Register Your Information (Blank)*.

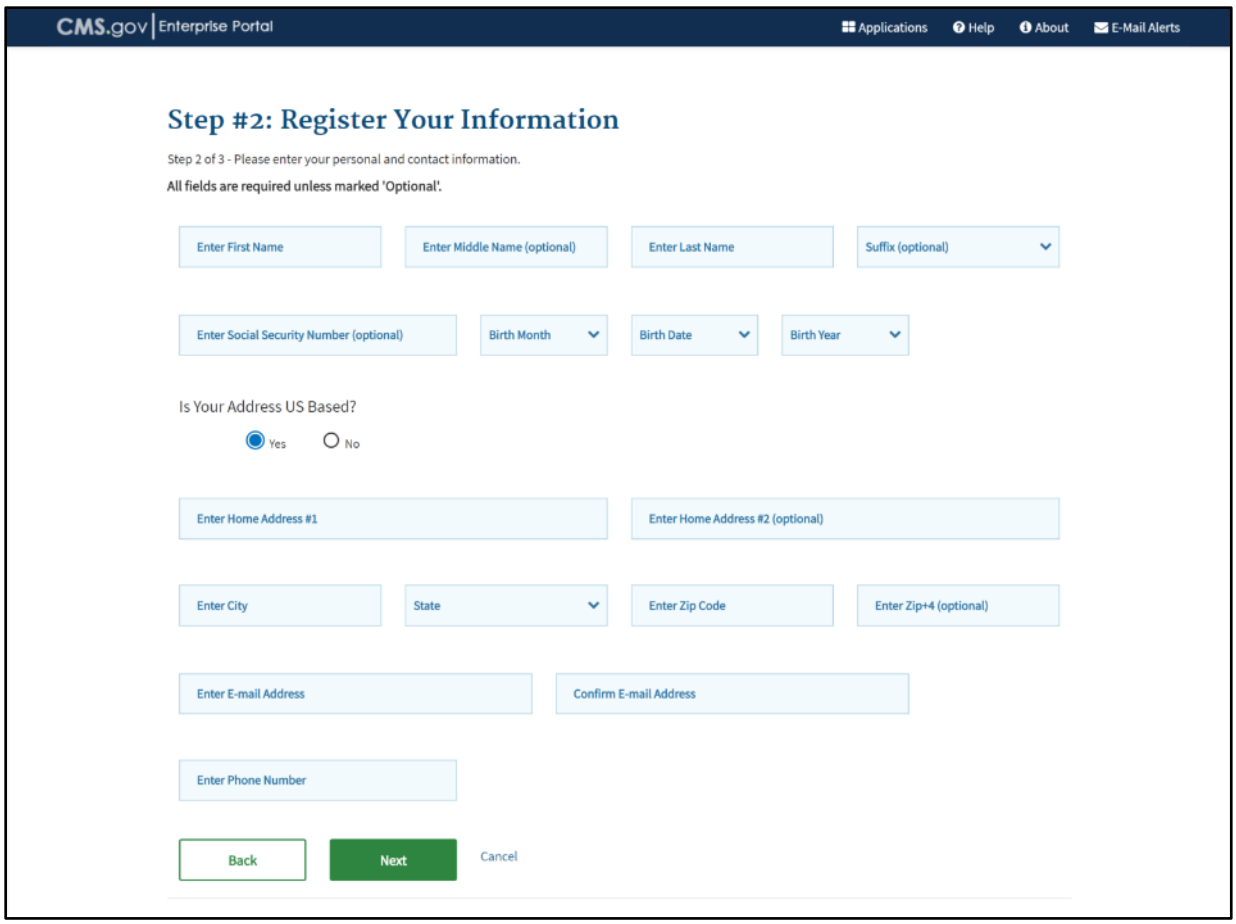

Figure 8: Step 2 of New User Registration - Register Your Information (Blank)

4. Provide the information requested on the **Step #2: Register Your Information** page, as shown in *Figure 9: 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.

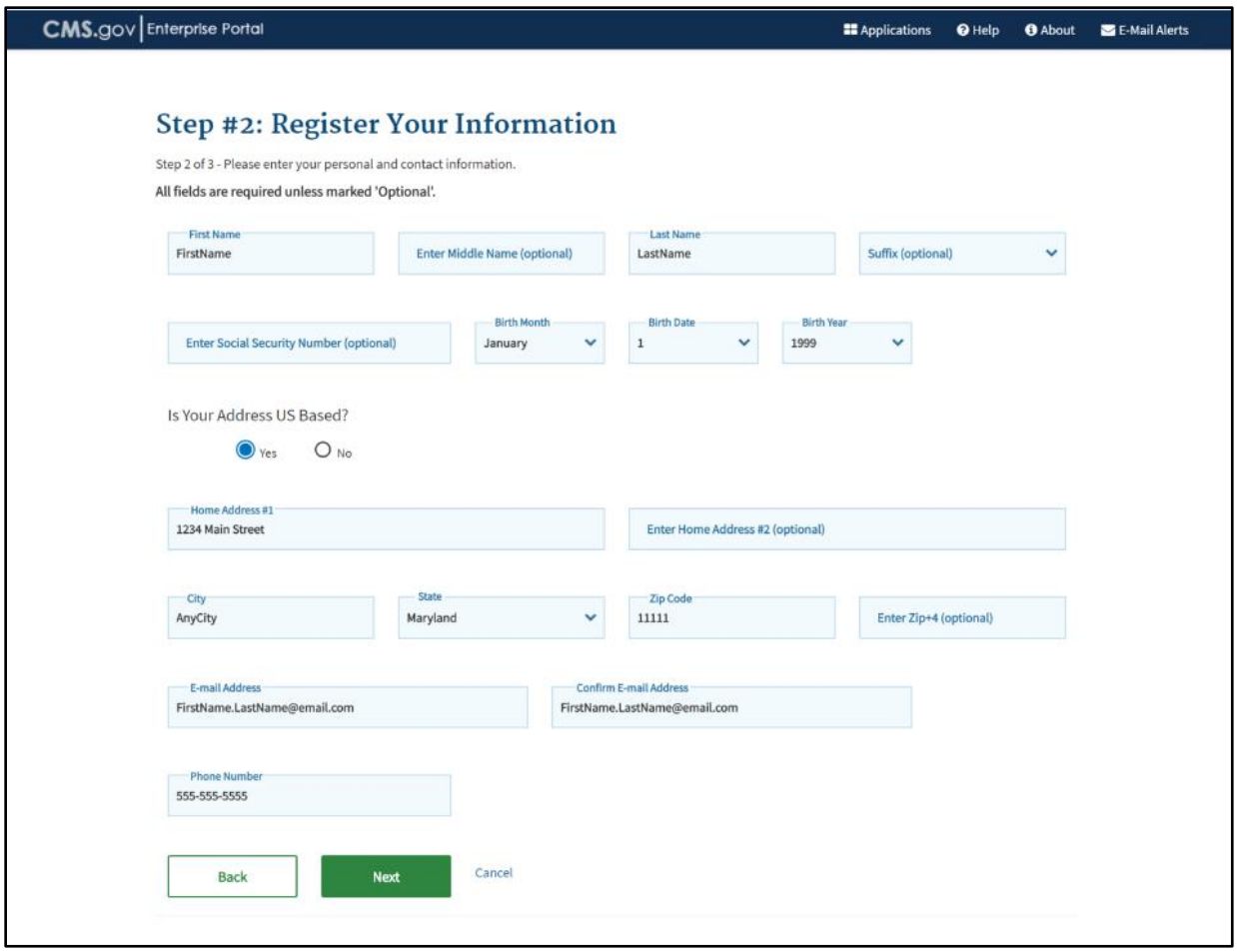

Figure 9: Step 2 of New User Registration - Register Your Information (Completed)

The **Step #3: Create User ID, Password & Challenge Questions** page displays, as shown in *Figure 10: Step 3 of New User Registration – Create User ID, Password & Challenge Questions (*Blank*).*

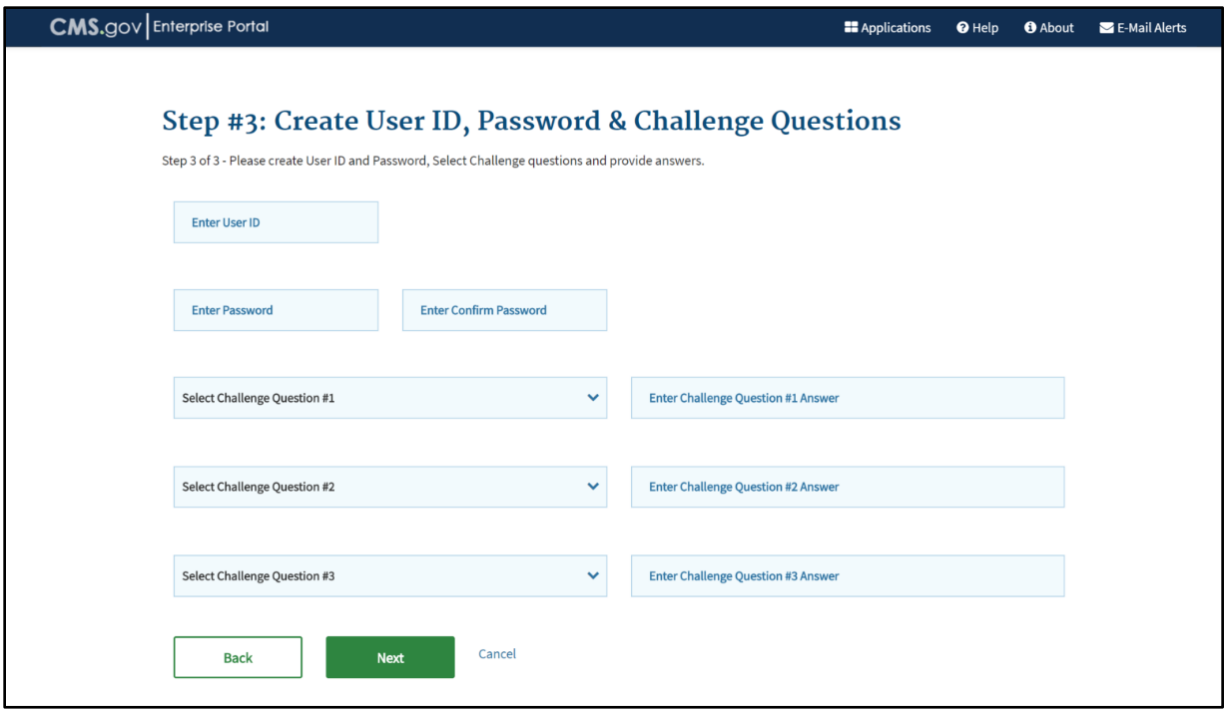

Figure 10: Step 3 of New User Registration – Create User ID, Password & Challenge Questions (Blank)

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 11: 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.

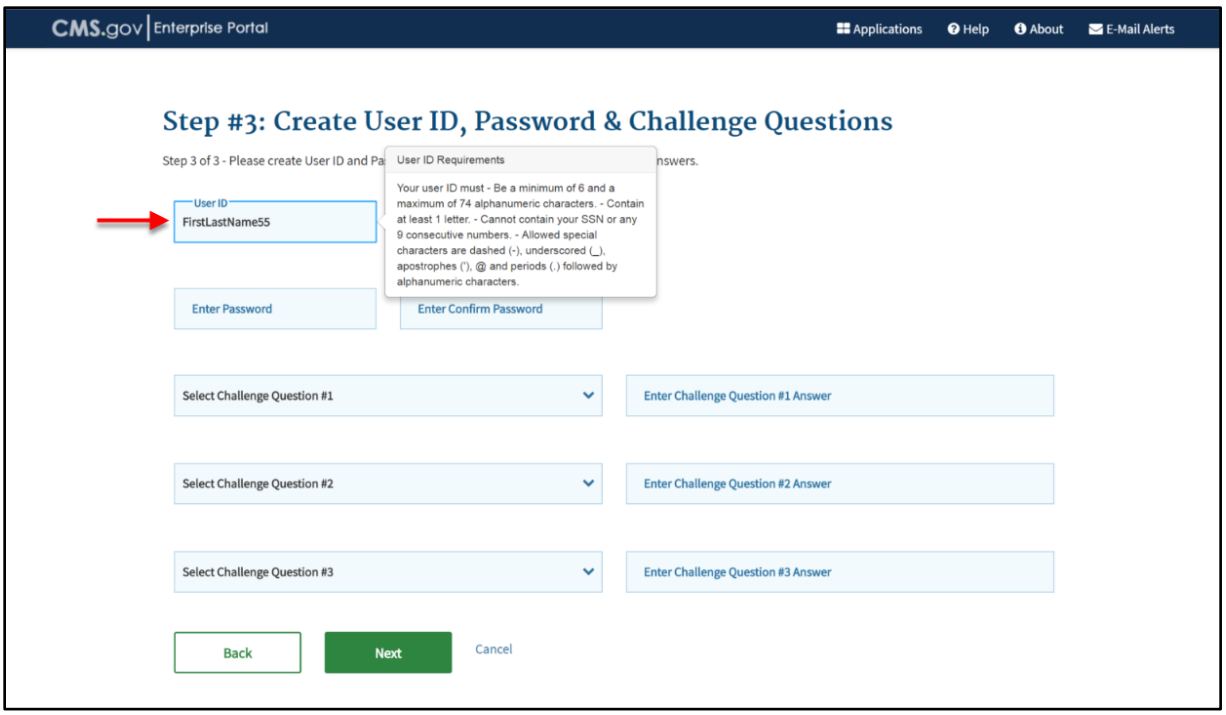

Figure 11: Step 3 of New User Registration – User ID Entered

6. Create and enter a password in the **Enter Password** field based on the requirements for creating a password, as shown in *Figure 12: 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.

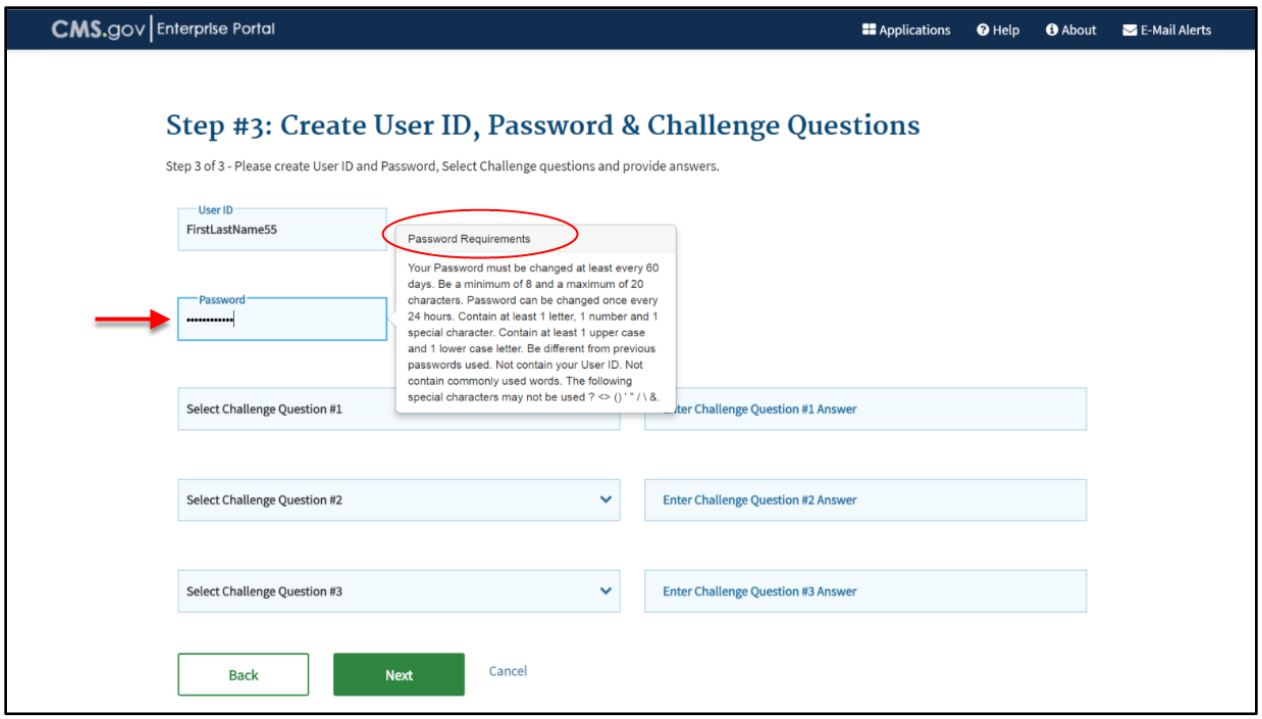

Figure 12: Step 3 of New User Registration – Password Entered

7. After entering the user ID and password, select a question in the **Select Challenge Question #1** drop-down list and enter the answer you want to be saved with the question, as shown in *Figure 13: Step 3 of New User Registration – Create User ID, Password & Challenge Questions (*Completed). Continue to select a question and enter an answer for Question #2 and Question #3. Click **Next** to complete the registration process.

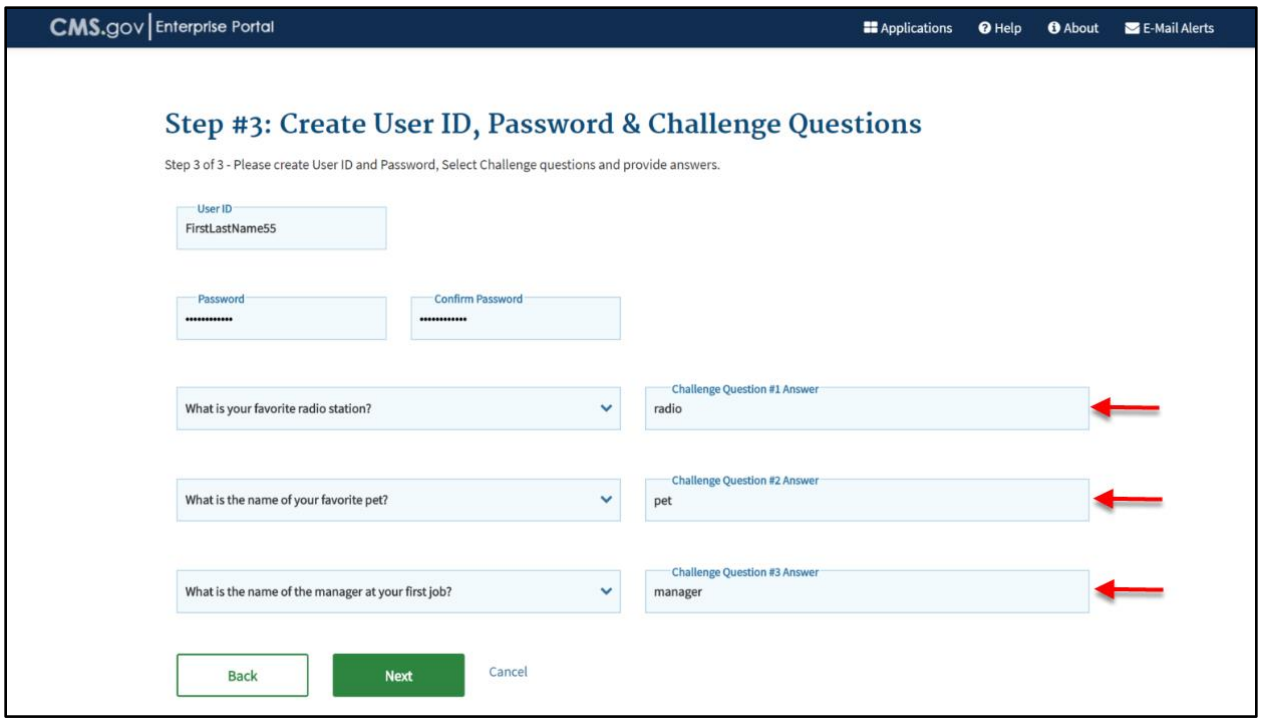

Figure 13: Step 3 of New User Registration – Create User ID, Password & Challenge Questions (Completed)

The **Registration Summary** page displays, as shown in *Figure 14: New User Registration – Registration Summary*.

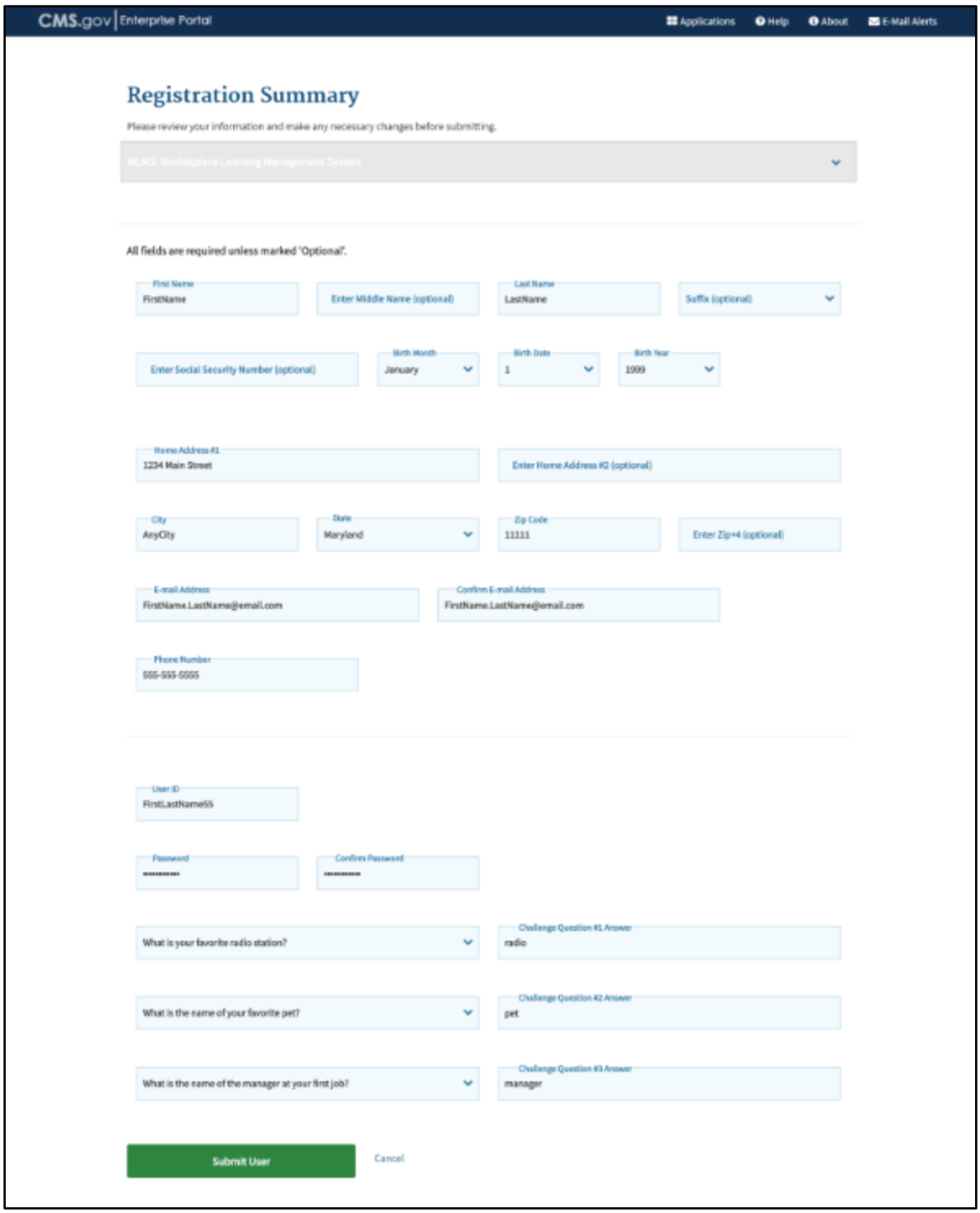

Figure 14: New User Registration – Registration Summary

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 an email with your user ID, as shown in *Figure 15: New User Registration – Confirmation.*

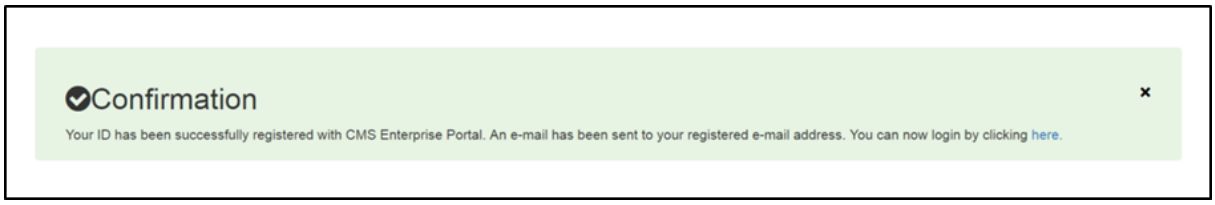

Figure 15: New User Registration – Confirmation

5. Logging In

5.1 User Login Without a Registered MFA Device

The instructions in this section demonstrate the login process for users who do not have Multi-Factor Authentication (MFA) configured in their profile.

1. Navigate to the CMS Enterprise Portal public landing page, as shown in *Figure 16: Login Portlet on CMS Enterprise Portal Public* Landing Page.

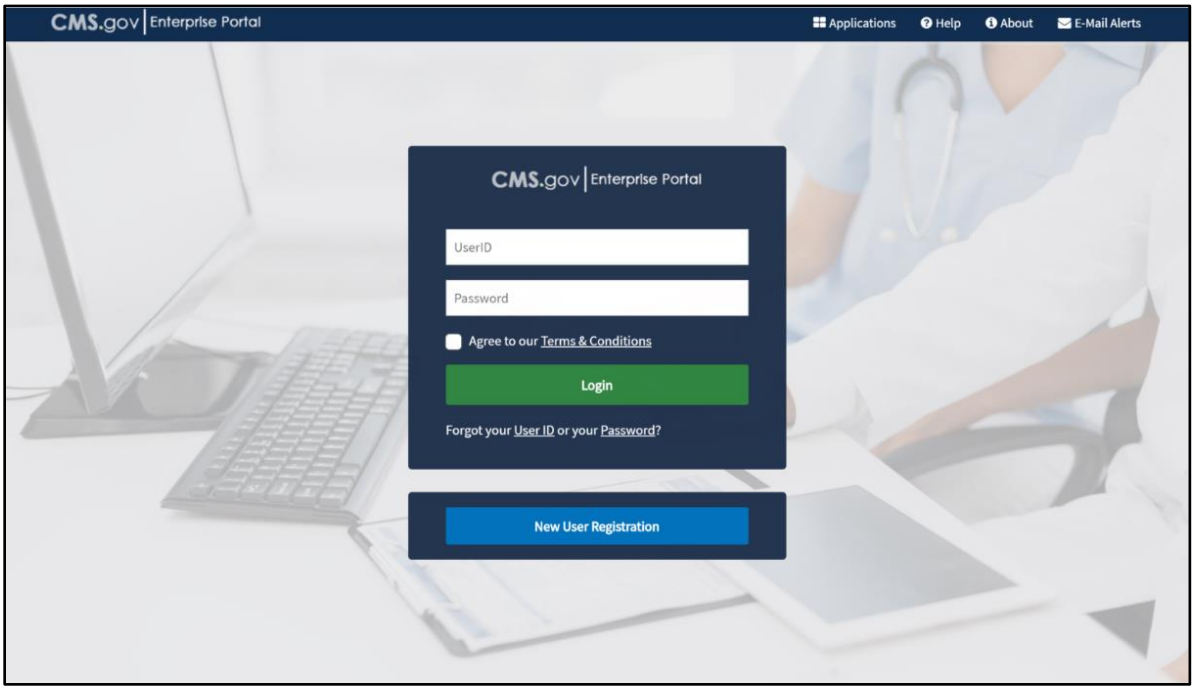

Figure 16: Login Portlet on CMS Enterprise Portal Public Landing Page

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**.

Note: If the process of checking your account's MFA status is delayed for any reason, you may see the pop-up message, as shown in *Figure 17: MFA Status Check*. Once the spinner stops, after a few seconds, close the pop-up window, and click **Login** again.

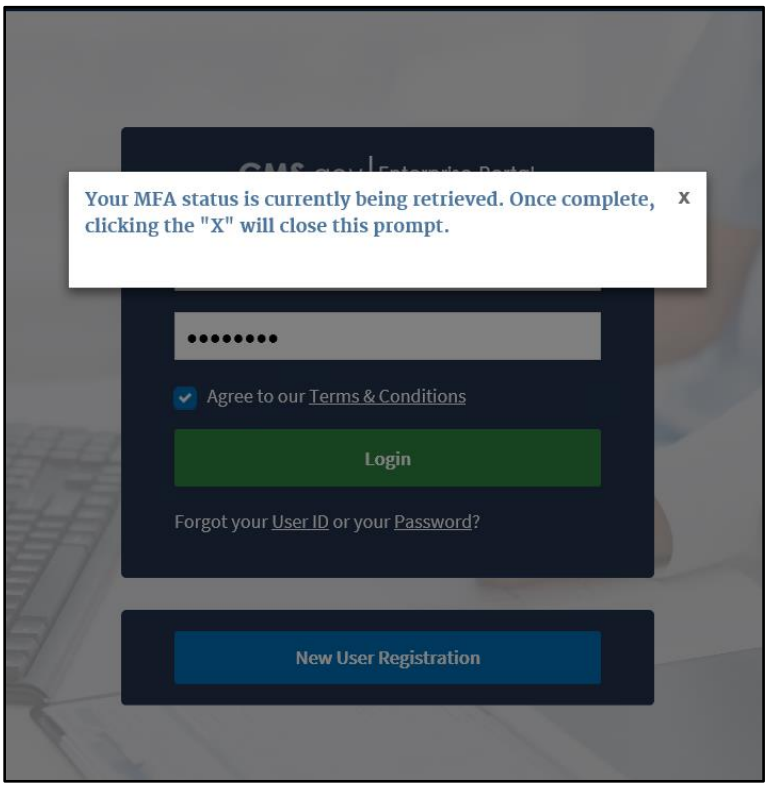

Figure 17: MFA Status Check

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

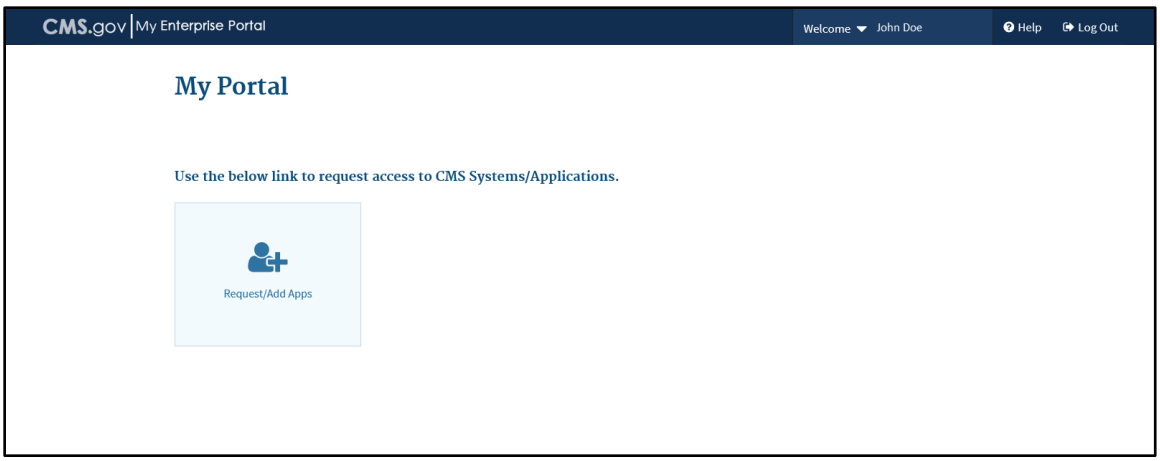

Figure 18: My Portal Page – First Login

7. For accounts that have access to CMS applications, the **My Portal** page displays 3-4 tiles (depending on how many CMS applications associated with your account), as shown in *Figure 19: My Portal Page with Apps.*

Figure 19: My Portal Page with Apps

The first two tiles (1 & 2) display two of the CMS applications you have access to; if you only have access to one application, only one application tile is displayed.

The third tile (3) is **View Apps**. Clicking this tile displays all of the remaining applications associated with your account, as shown in *Figure 20: View Apps*.

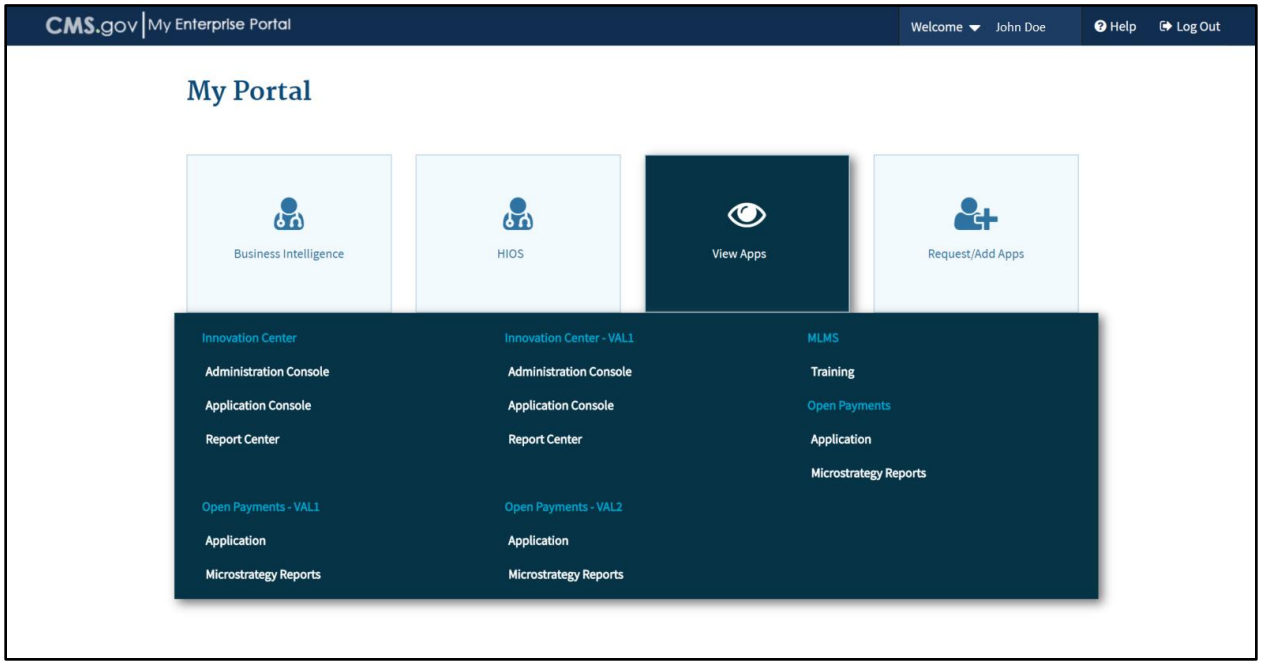

Figure 20: View Apps

The fourth tile (4) is **Request/Add Apps**. Clicking this tile takes you to the **Access Catalog** where you can request access to various CMS applications.

5.2 User Login Using an MFA Device

The following instructions demonstrate the login process for users who have MFA configured in their profile.

1. Navigate to the CMS Enterprise Portal public landing page.
2. Enter the CMS user ID in the **User ID** field.

   Upon entering a username that is configured with MFA, an additional **Choose MFA Device** field drop-down is displayed, as shown in *Figure 21: Login with MFA Device*.

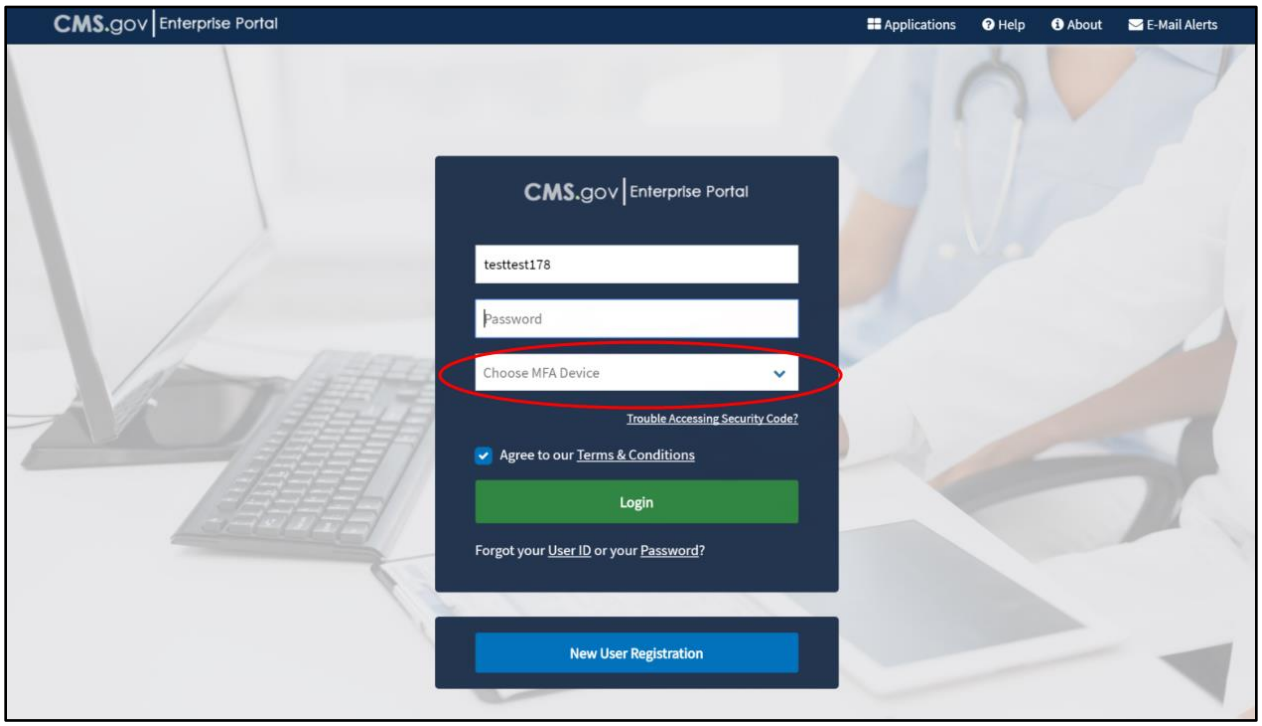

Figure 21: Login with MFA Device

3. Enter the CMS password in the **Password** field.
4. Expand the **Choose MFA Device drop-down** list, as shown in *Figure 22: MFA Device Options.*

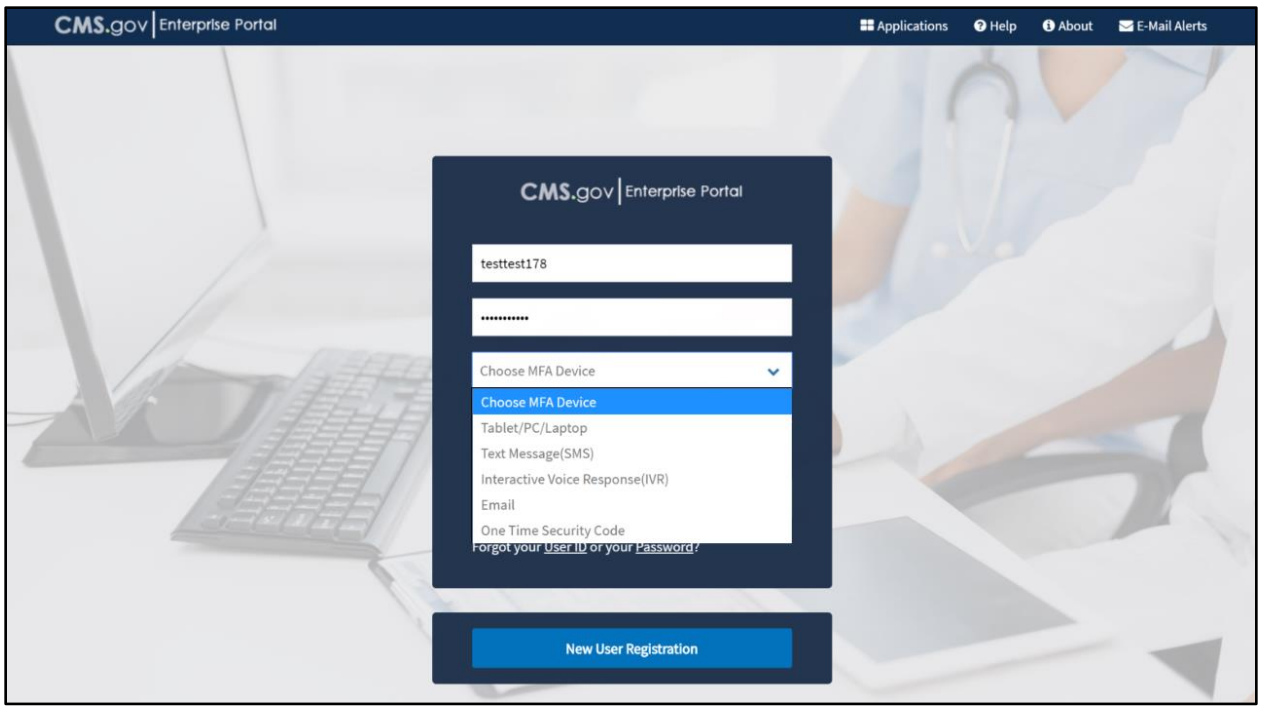

Figure 22: MFA Device Options

5. Select your MFA Device.

   Depending on your selection, additional fields are displayed. See the MFA Device options described in the subsections *5.2.1* through *5.2.5*.

6. Enter the security code and click **Login**.

   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 Apps.*

5.2.1 Tablet/PC/Laptop

1. If you select **Tablet/PC/Laptop**, the **Enter security code** field displays, as shown in *Figure 23: Selecting Tablet/PC/*Laptop.

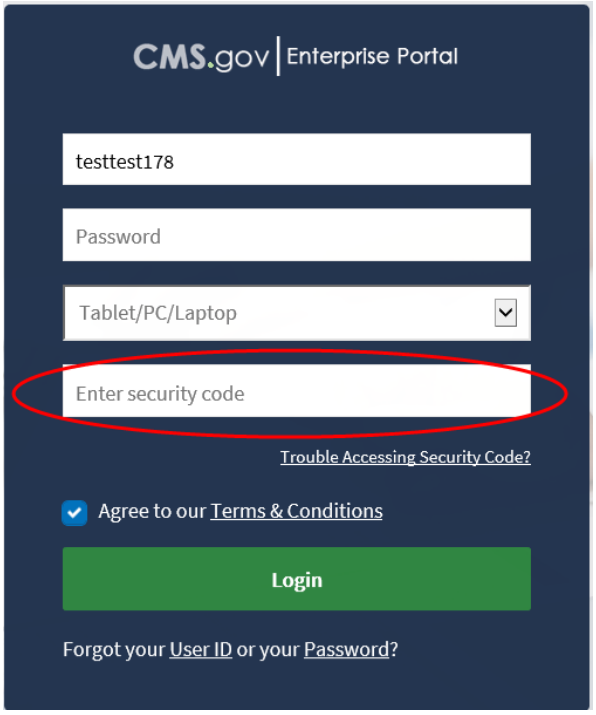

Figure 23: Selecting Tablet/PC/Laptop Option as MFA Device

2. Retrieve the security code from the VIP Access software, as shown in *Figure 24: VIP Access.*

Figure 24: VIP Access

3. Enter the security code and click **Login**.

5.2.2 Text Message (SMS)

1. If you select **Text Message (SMS)**, the **Send MFA Code** button and **Enter security code** field display, as shown in *Figure 25: Selecting Text Message (*SMS*).*
2. Click **Send MFA Code** to have the code texted to your device.

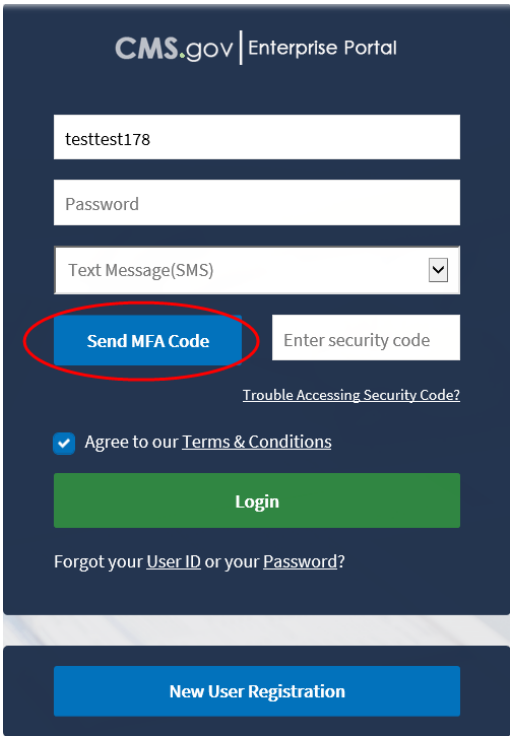

Figure 25: Selecting Text Message (SMS) Option as MFA Device

3. Enter the security code and click **Login**.

5.2.3 Interactive Voice Response (IVR)

1. If you select **Interactive Voice Response (IVR)**, the **Send MFA Code** button and **Enter security code** field display, as shown in *Figure 26: Selecting* IVR.
2. Click **Send MFA Code** to have the code provided to you via phone.

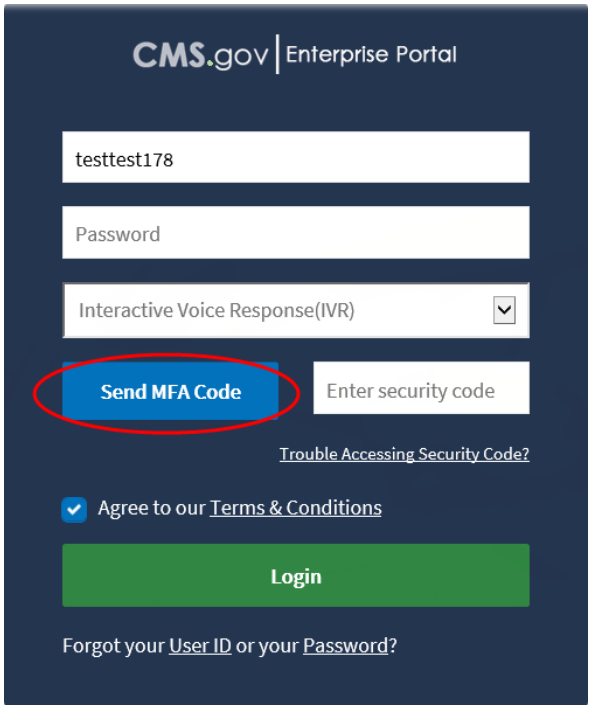

Figure 26: Selecting IVR Option as MFA Device

3. Enter the security code and click **Login**.

5.2.4 Email

1. If you select **Email**, the **Send MFA Code** button and **Enter security code** field display, as shown in *Figure 27: Selecting* Email.
2. Click **Send MFA Code** to have the code emailed to your registered email address.

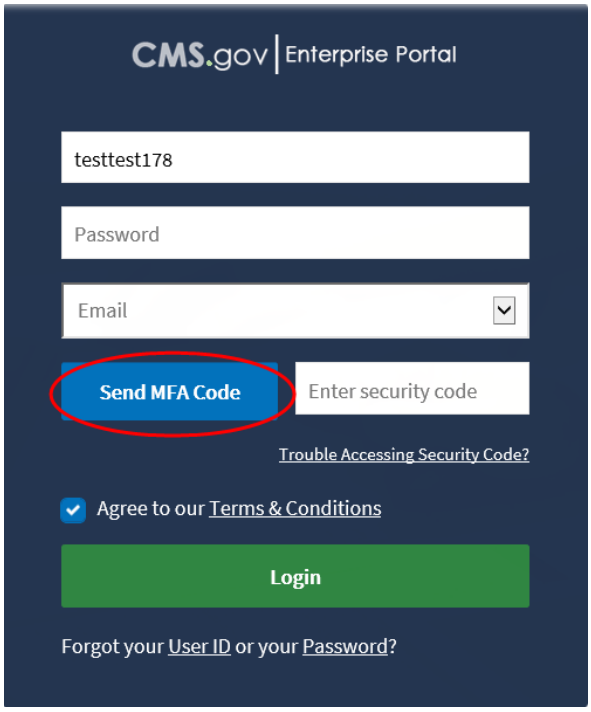

Figure 27: Selecting Email Option as MFA Device

3. Enter the security code and click **Login**.

5.2.5 One Time Security Code

1. If you select **One Time Security Code**, the **Enter one time security code** field displays, as shown in *Figure 28: Selecting One Time Security* Code.
2. Upon selecting this option, you will receive the security code either in an email sent to your registered e-mail address via the **Trouble Accessing Security Code?** link or by contacting your application's Help Desk.

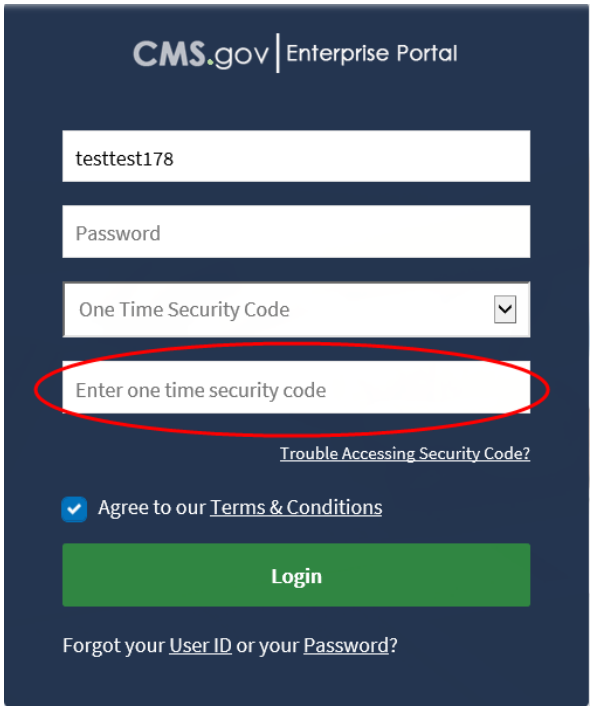

Figure 28: Selecting One Time Security Code Option as MFA Device

3. Enter the security code and click **Login**.

6. Forgot User ID

The instructions in this section demonstrate the 'Forget User ID' process for users who do not remember their registered user ID to login.

1. Navigate to the CMS Enterprise Portal public landing page, and click the **User ID** link, as shown in *Figure 29: Forgot User ID Link.*

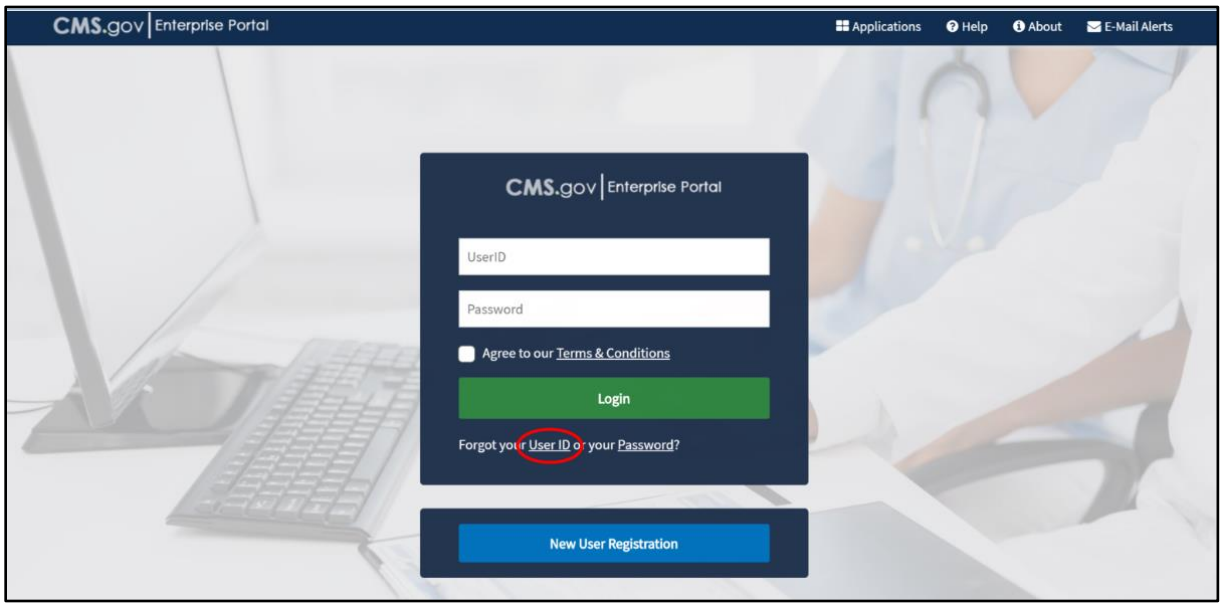

Figure 29: Forgot User ID Link

2. Enter the information shown in *Figure 30: Forgot User ID – Blank Page* and click **Submit.**

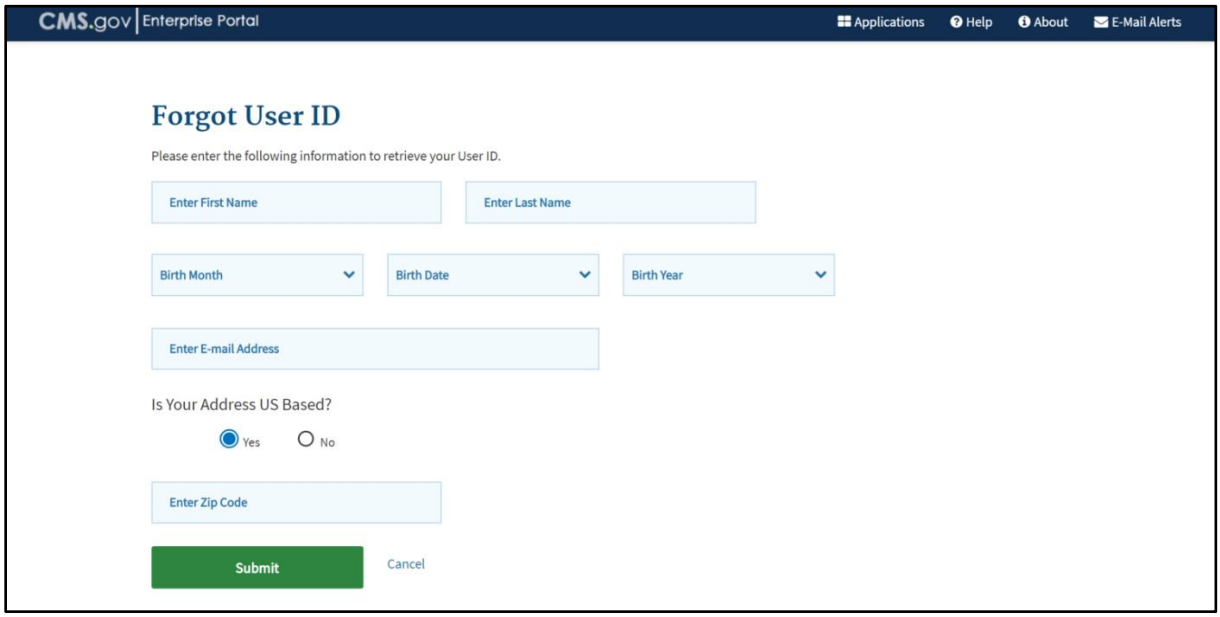

Figure 30: Forgot User ID – Blank Page

Note: An error will display if invalid data is entered, as shown in *Figure 31: Invalid Data Error*. You must re-enter the correct information and submit again.

Figure 31: Invalid Data Error

3. After successfully submitting your information, you will receive confirmation that your information has been successfully verified, as shown in *Figure 32: Forgot User ID – Successful Confirmation*.

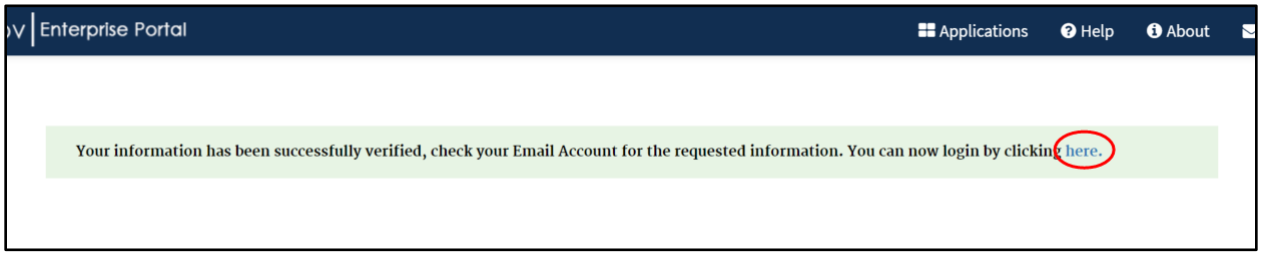

Figure 32: Forgot User ID – Successful Confirmation

Note: You will receive an e-mail notification that will contain your User ID. This e-mail will be sent to the e-mail address on your profile.

4. Click the link in the confirmation message, as shown in *Figure 32: Forgot User ID – Successful Confirmation*, to login with your user ID (retrieve from the e-mail notification).

7. Forgot Password

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

1. Navigate to the CMS Enterprise Portal public landing page, and click the **Password** link, as shown in *Figure 33: Forgot Password Link.*

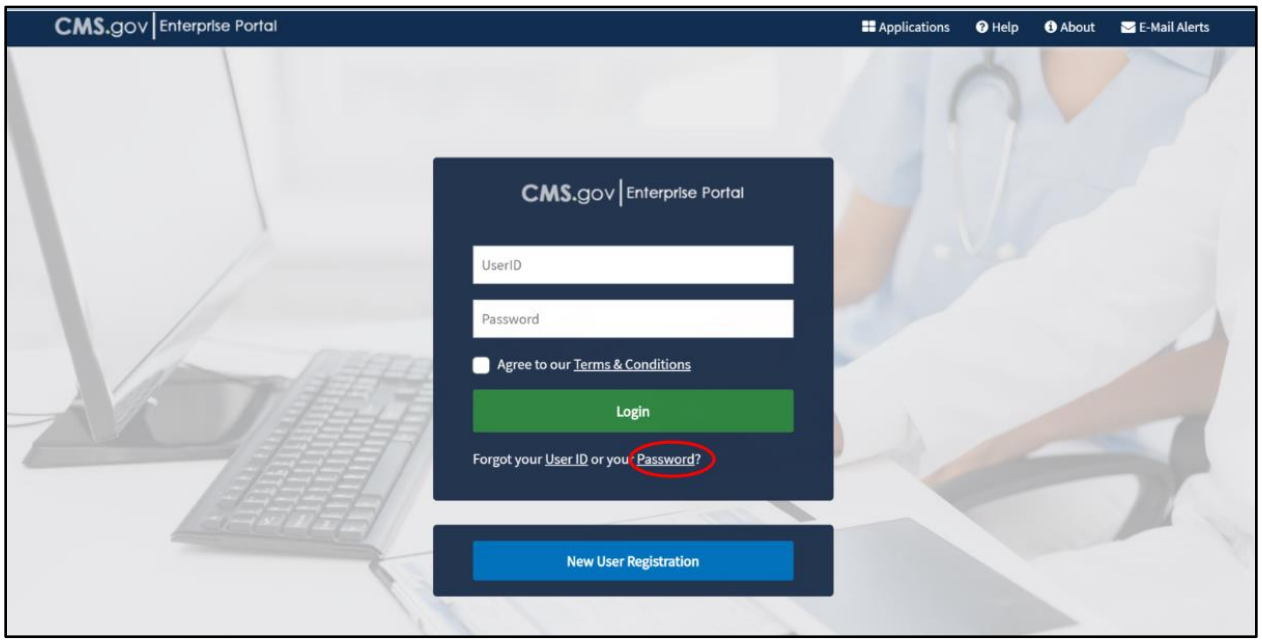

Figure 33: Forgot Password Link

2. Enter your user ID and click **Next**, as shown in *Figure 34: Forgot Password – Enter User ID.*

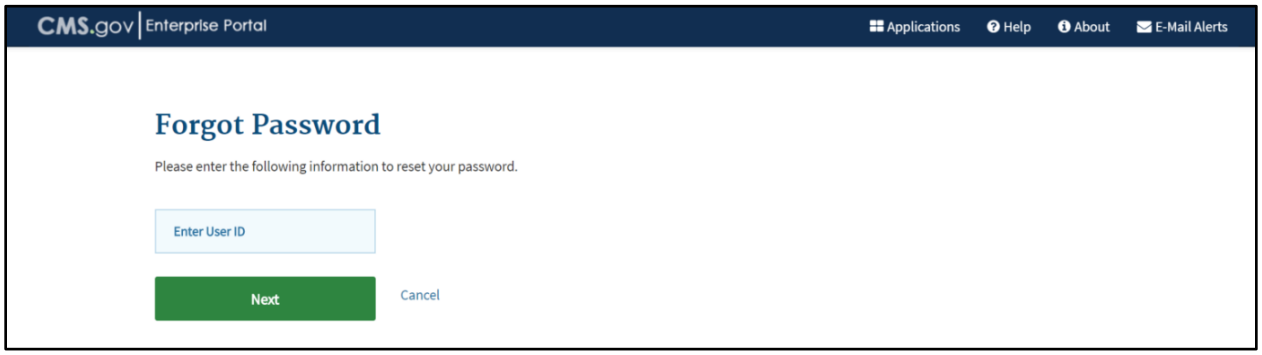

Figure 34: Forgot Password – Enter User ID

Note: An error is displayed if invalid data is entered, as shown in *Figure 35: Invalid Data Error.* You must re-enter the correct information and click **Next**.

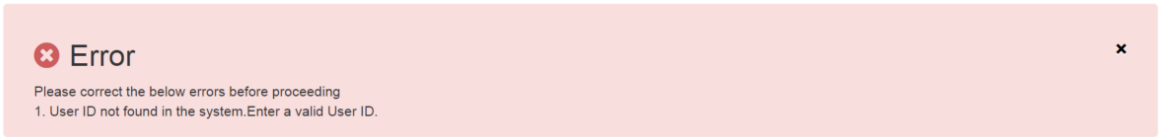

Figure 35: Invalid Data Error

3. Answer the challenge questions (your user ID will pre-populate). Enter a new password in the **Create New Password** field and again in the **Confirm New Password** field, as shown in *Figure 36: Forgot Password – Blank Form*. Then, click **Submit**.

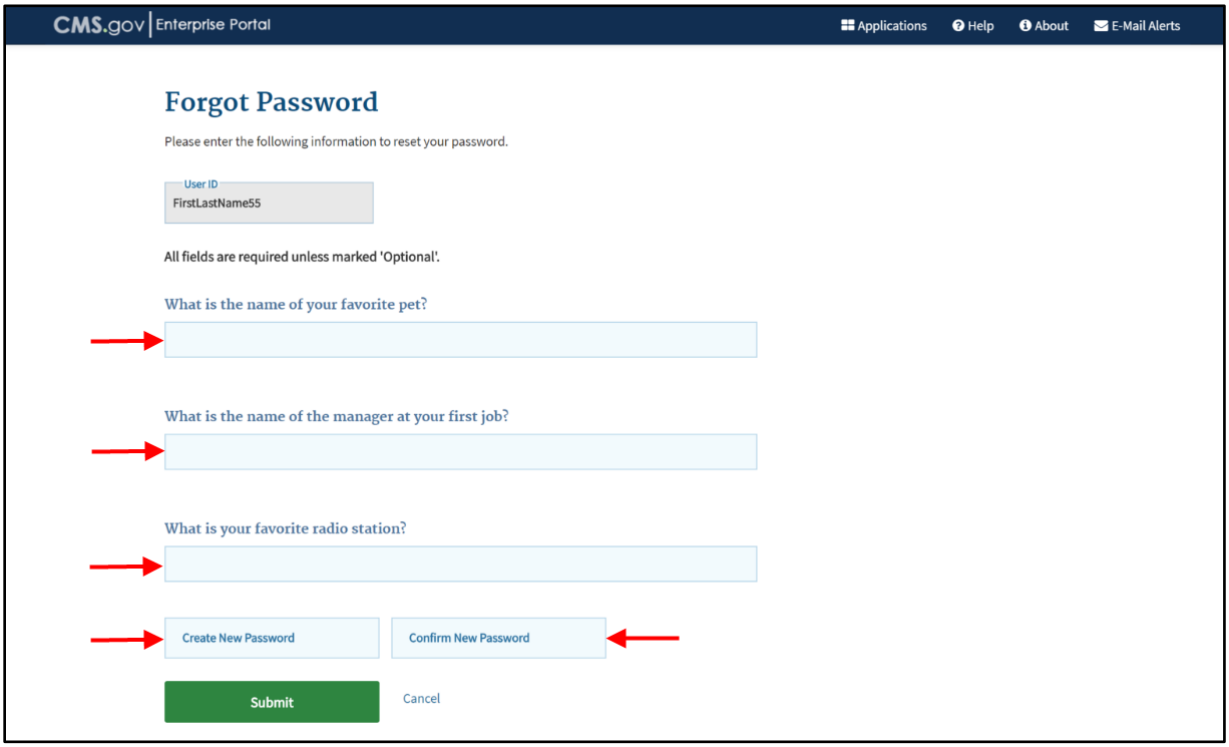

Figure 36: Forgot Password – Blank Form

Note: An error will display if invalid data is entered, as shown in *Figure 37: Invalid Data Error.* You must re-enter the correct information and click **Submit**.

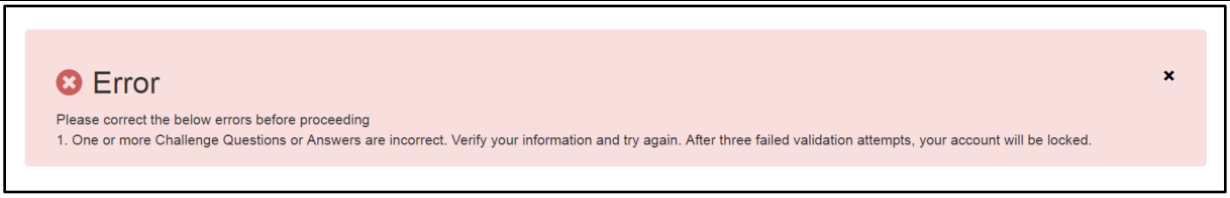

Figure 37: Invalid Data Error

4. After successfully submitting your information, you will receive confirmation that your information has been successfully verified, as shown in *Figure 38: Forgot Password – Successful Confirmation.*

Figure 38: Forgot Password – Successful Confirmation

Note: You will receive an e-mail notification indicating that you successfully changed your password.

8. 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, password and/or MFA security, an error occurs, as shown in *Figure 39: Incorrect Credentials Error Message.*

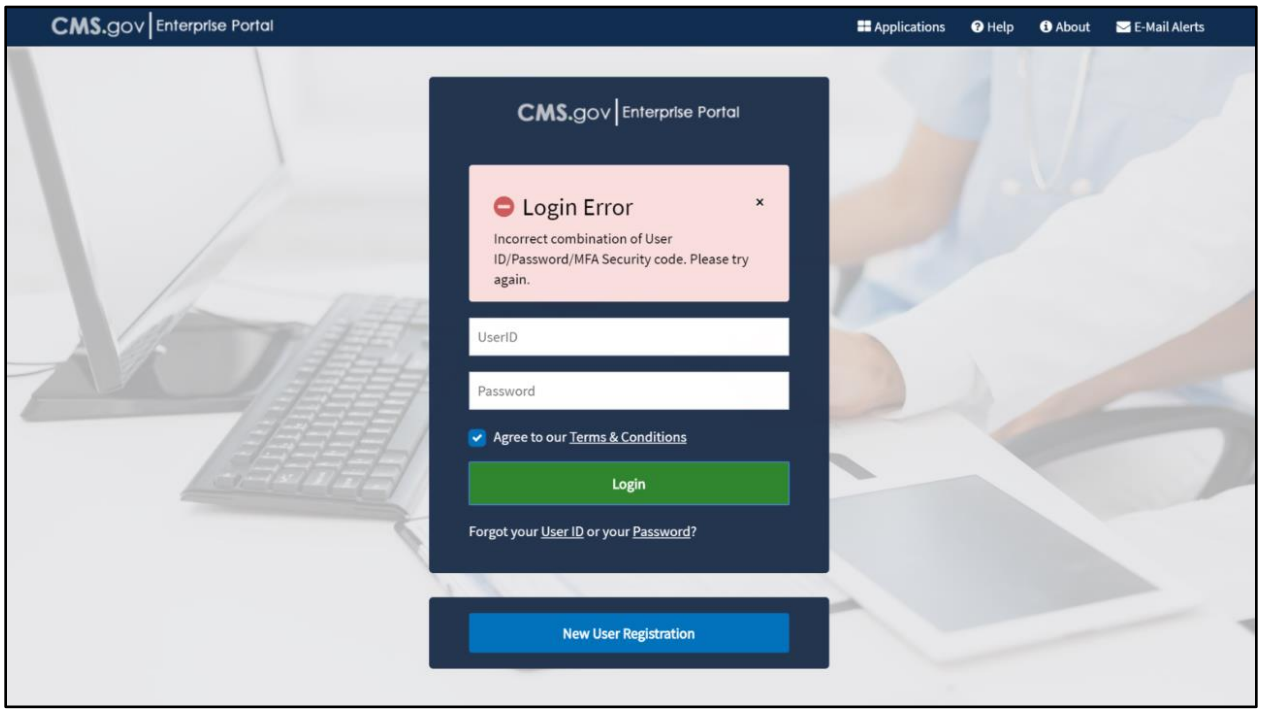

Figure 39: Incorrect Credentials Error Message

2. After entering an incorrect combination of user ID, password and/or MFA security code 3 times, your account locks, as shown in *Figure 40: Account Locked Message.*

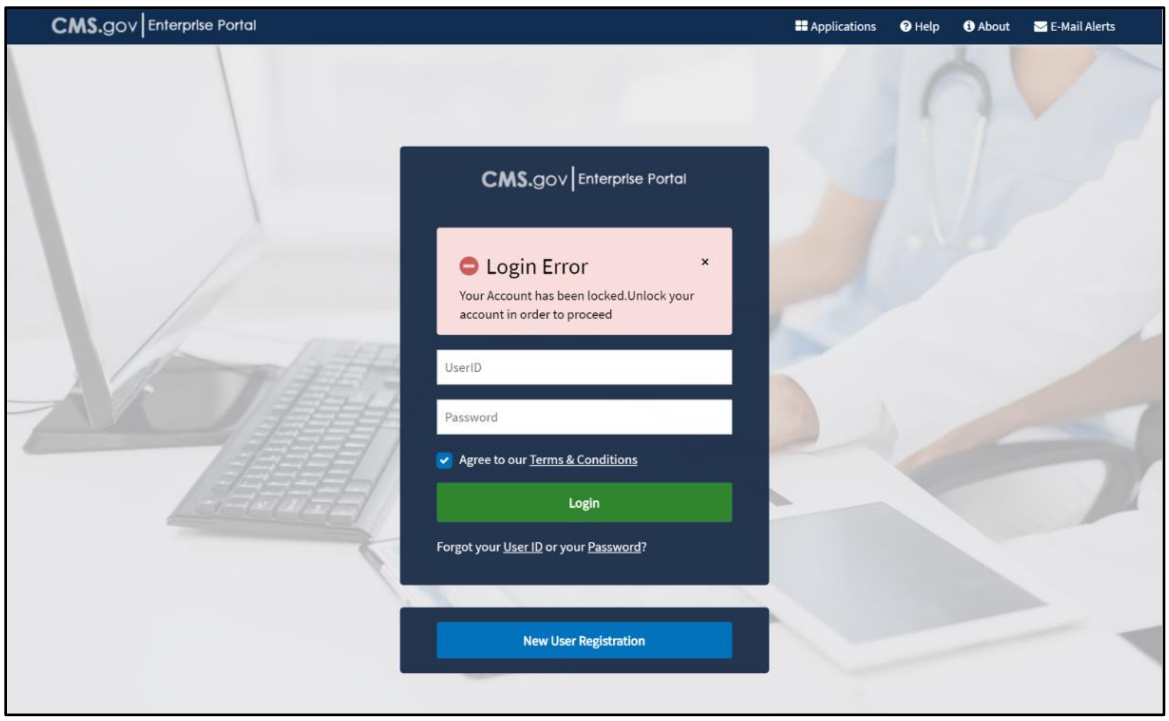

Figure 40: Account Locked Message

3. On the **Unlock My Account** page, enter your user ID and click **Next**, as shown in *Figure 41: Correct User ID on Unlock Account Page.*

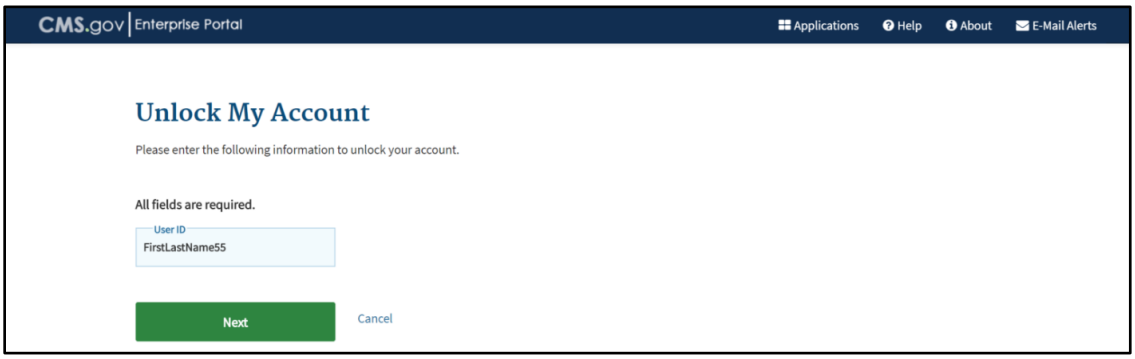

Figure 41: Correct User ID on Unlock Account Page

Note: If an incorrect user ID is entered, an error occurs, as shown in *Figure 42: Incorrect User ID Error Message on Unlock Account Page.*

Figure 42: Incorrect User ID Error Message on Unlock Account Page

4. Answer the challenge questions. Enter a new password in the **Create New Password** field and again in the **Confirm New Password** field, as shown in *Figure 43: Unlock My Account – Challenge Questions*. Then, click **Submit**.

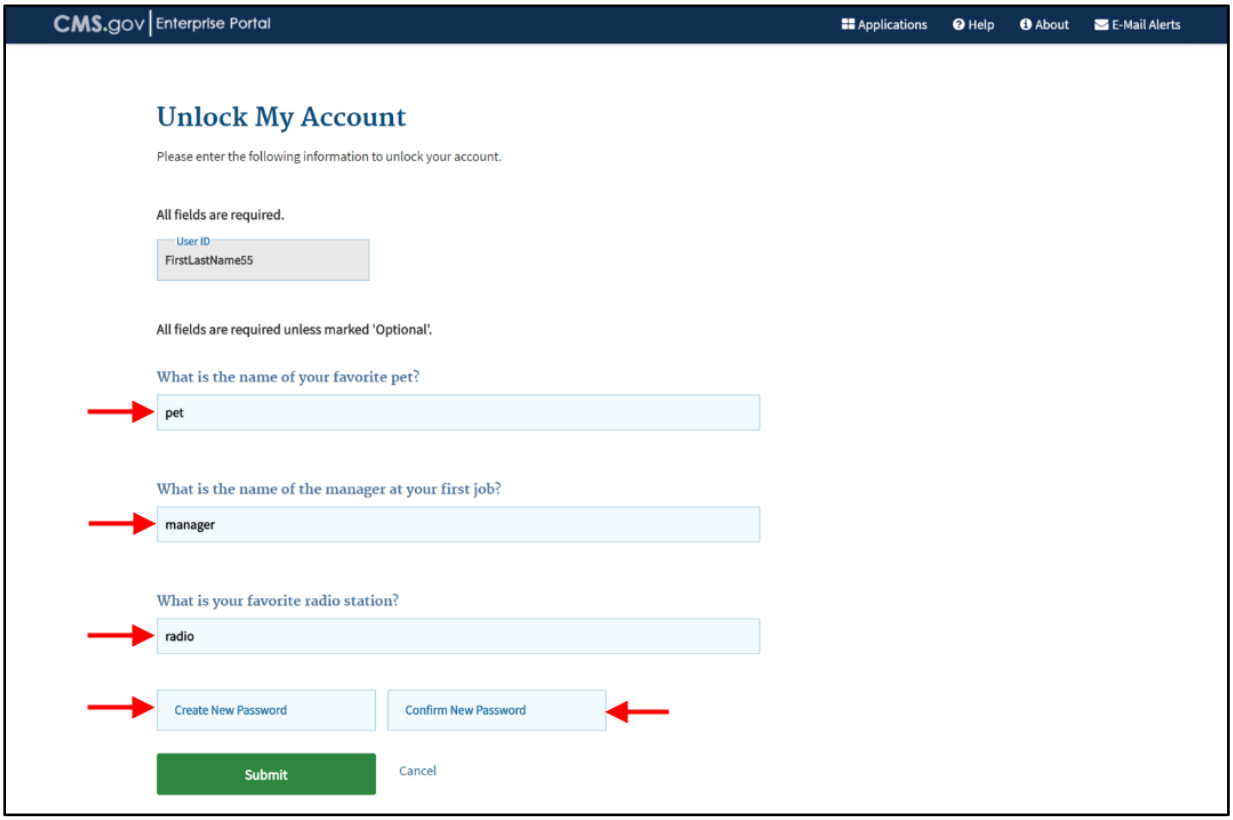

Figure 43: Unlock My Account – Challenge Questions

Note: If incorrect information is entered in the fields, an error occurs, as shown in *Figure 44: Challenge Questions – Invalid Data.* After 3 failed attempts, your account will be locked, and you will need to contact your application's Help Desk for assistance.

Figure 44: Challenge Questions – Invalid Data

5. After successfully submitting your information, you will receive confirmation that your account has been unlocked, as shown in *Figure 45: Unlock Account – Successful Confirmation.*

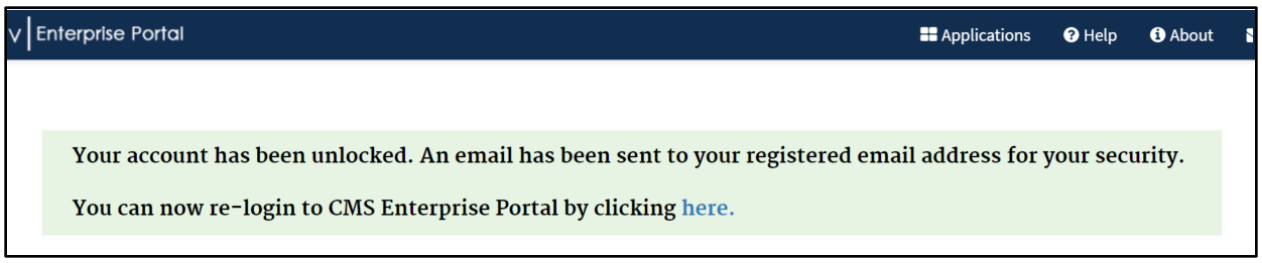

Figure 45: Unlock Account – Successful Confirmation

Note: You will receive an e-mail to your registered e-mail address indicating that your account has been unlocked.

9. User Profile

9.1 Viewing Your Profile

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

1. Navigate to the CMS Enterprise Portal public landing page.
2. Login using your user ID and password.

   The CMS Enterprise Portal **My Portal** page is displayed, as shown in *Figure 46: 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 46: My Portal Page – My Profile Drop-down

The **View My Profile** page displays, as shown in *Figure 47: View My Profile*.

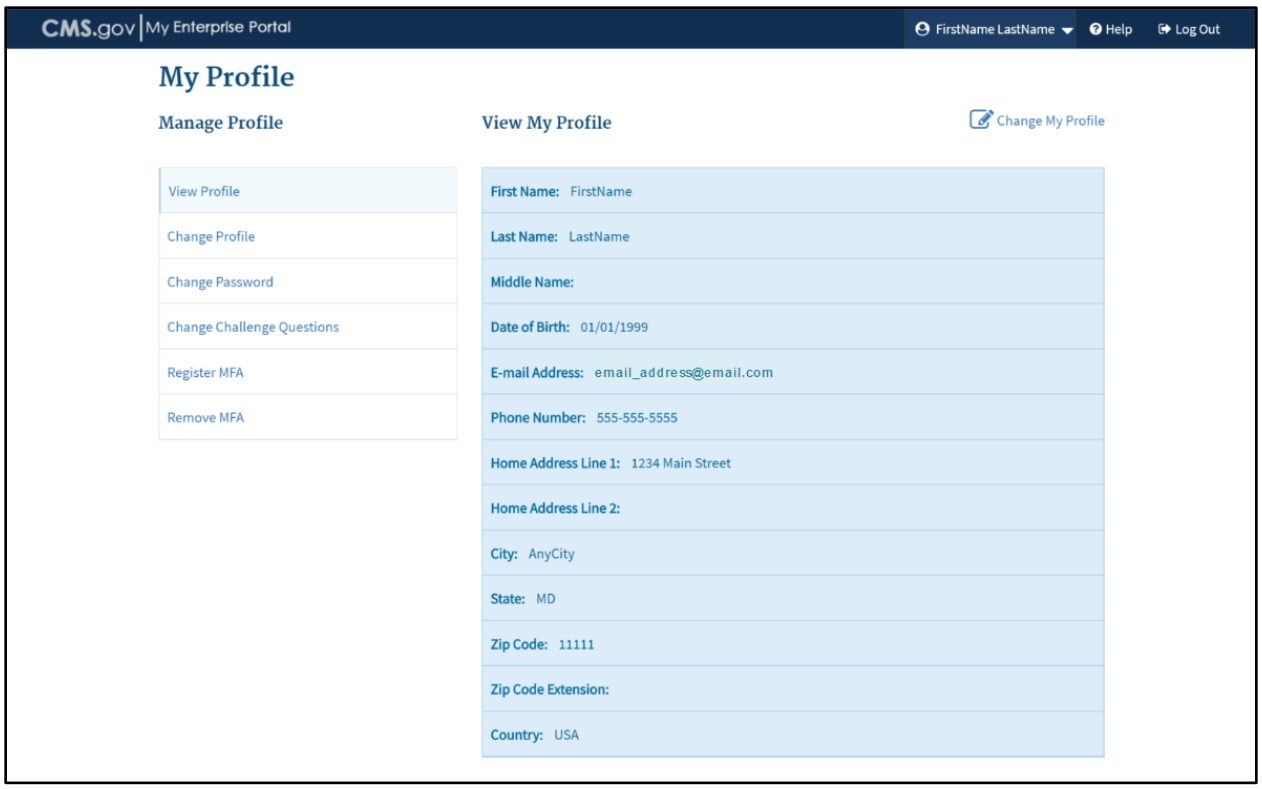

Figure 47: View My Profile

9.2 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 landing page.
2. Login using your user ID and password.

   The CMS Enterprise Portal **My Portal** page is displayed, as shown in *Figure 46: 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 My Profile** page displays, as shown in *Figure 47: View My Profile*.
4. Select **Change My Profile**, as shown in *Figure 48: Change My Profile*.

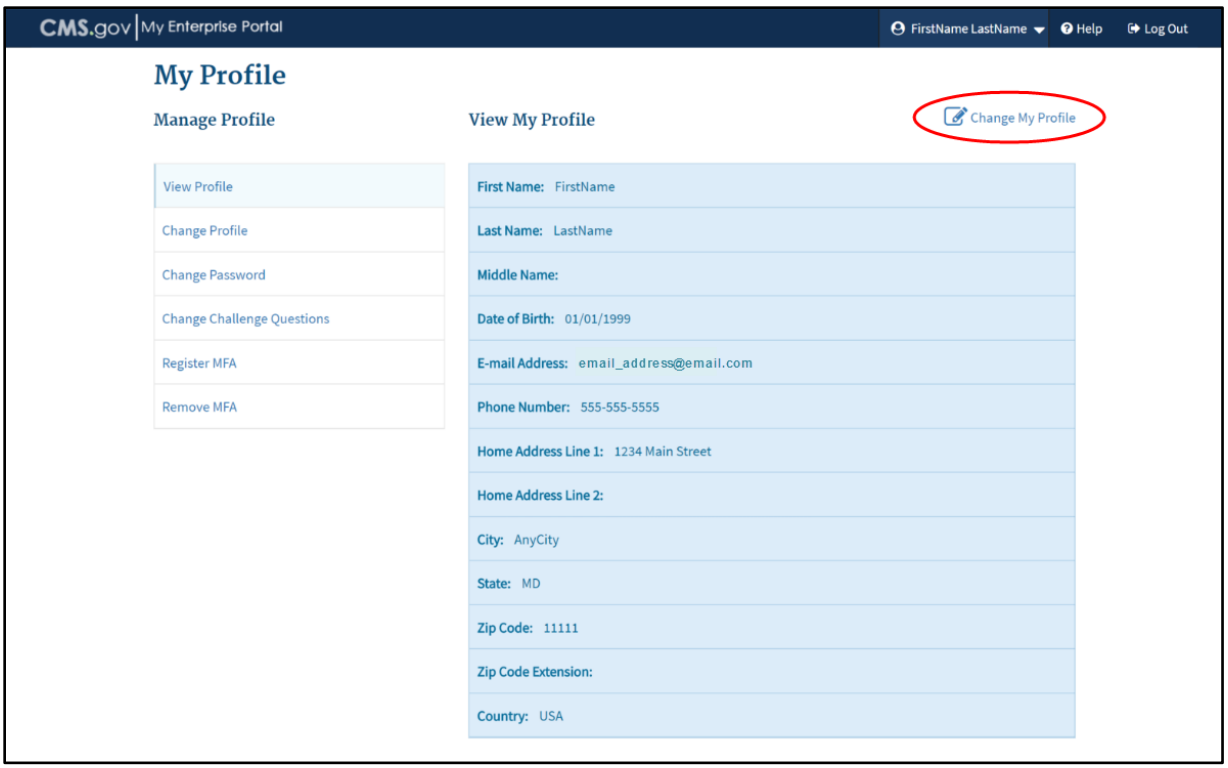

Figure 48: Change My Profile

The Change Profile page displays, as shown in *Figure 49: Change Profile*.

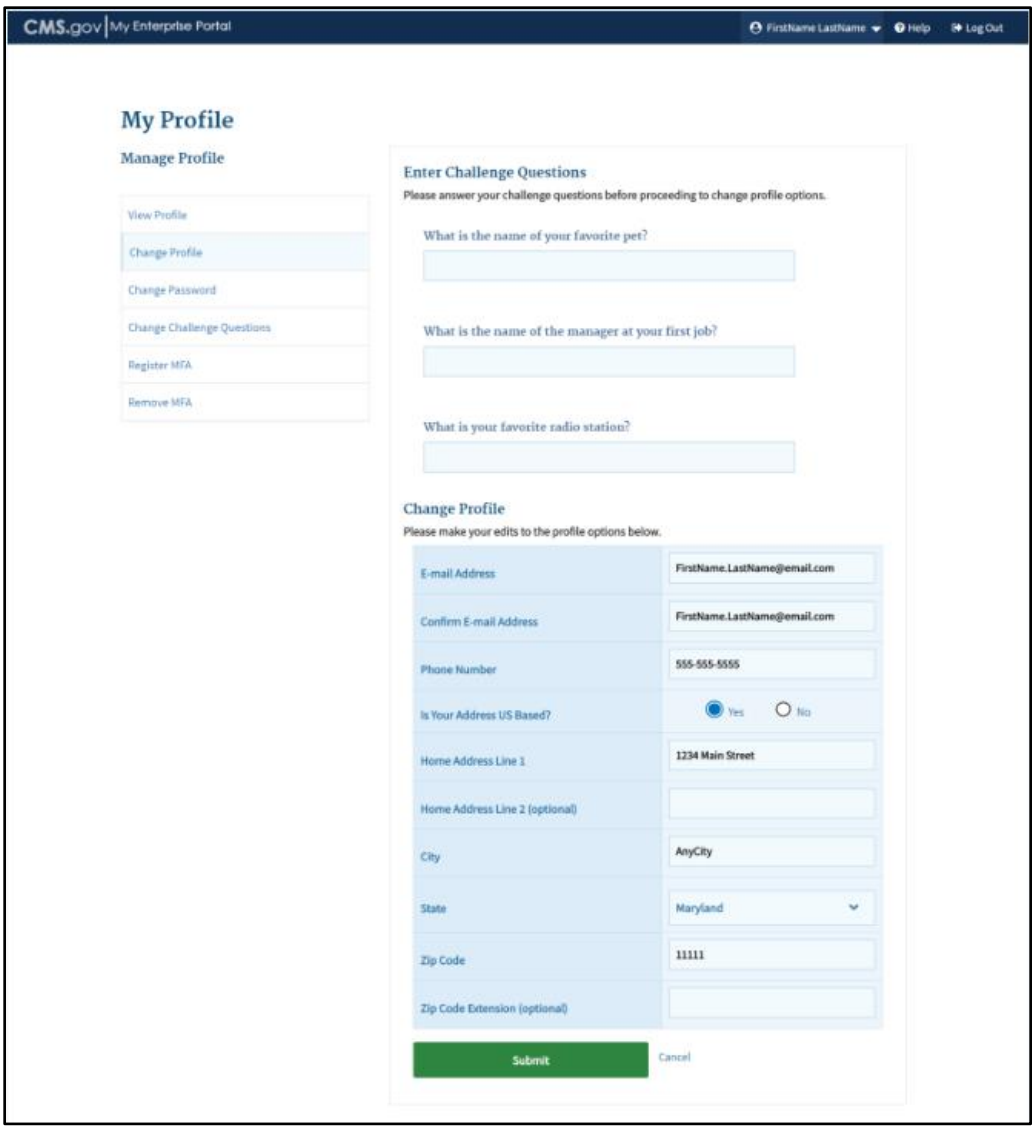

Figure 49: Change Profile

5. Answer the challenge questions before proceeding to change your profile options.

Note: If incorrect information is entered in the fields, an error occurs, as shown in *Figure 50: Challenge Questions – Invalid Data.* After 3 failed attempts, your account will be locked. For detailed steps on how to unlock your account, refer to Section *8 - Unlocking Account*.

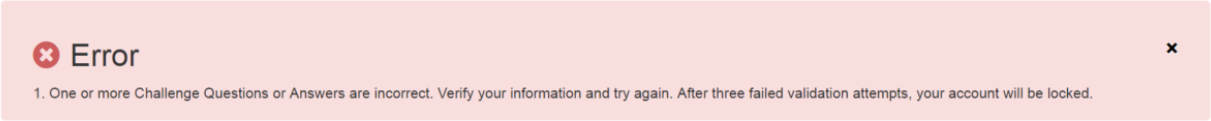

Figure 50: Challenge Questions – Invalid Data

6. Update the profile information, as needed, as shown in *Figure 51: Change Profile Information*, and click **Submit**.

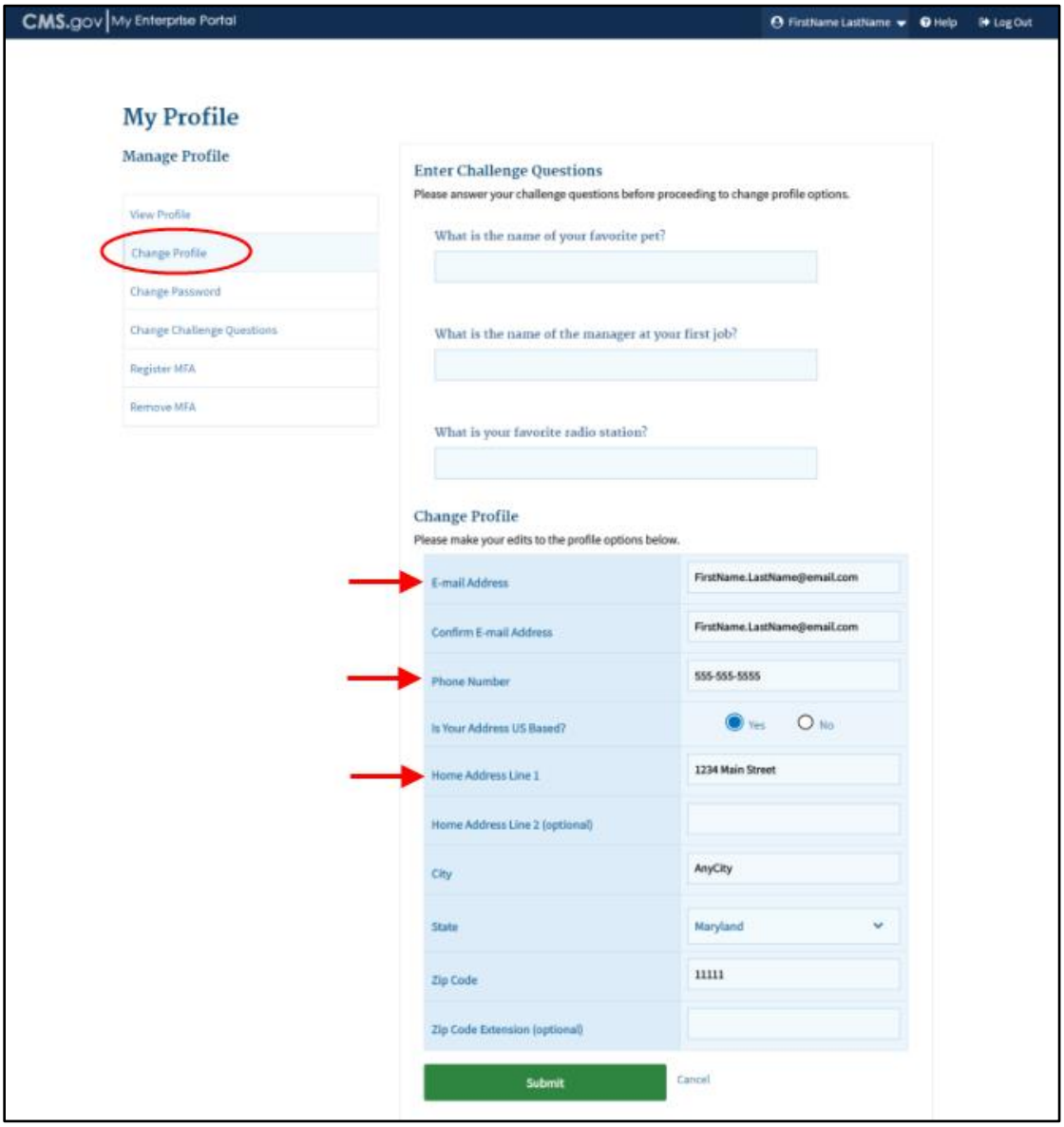

Figure 51: Change Profile Information

7. After submitting the updated information, you will receive confirmation that the changes to your profile were submitted successfully, as shown in *Figure 52: Update Profile – Successful Confirmation.*

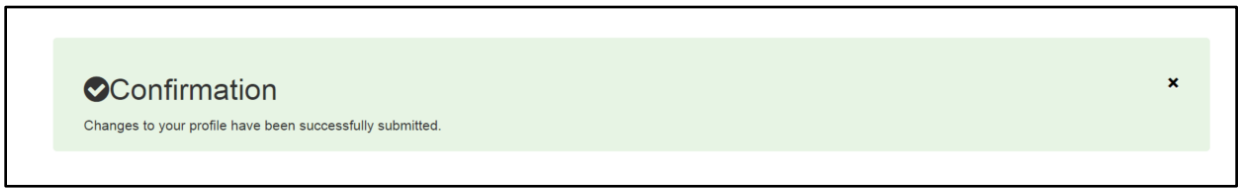

Figure 52: Update Profile – Successful Confirmation

9.3 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 landing page.
2. Login using your user ID and password.

   The CMS Enterprise Portal **My Portal** page is displayed, as shown in *Figure 46: 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 My Profile** page displays, as shown in *Figure 47: View My Profile.*
4. Select **Change Password**, as shown in *Figure 53: Change Password*.
5. Enter your old password in the **Enter Old Password** field.
6. Enter a new password in the **Enter New Password** field and again in the **Confirm New Password** field. Then, click **Submit**.

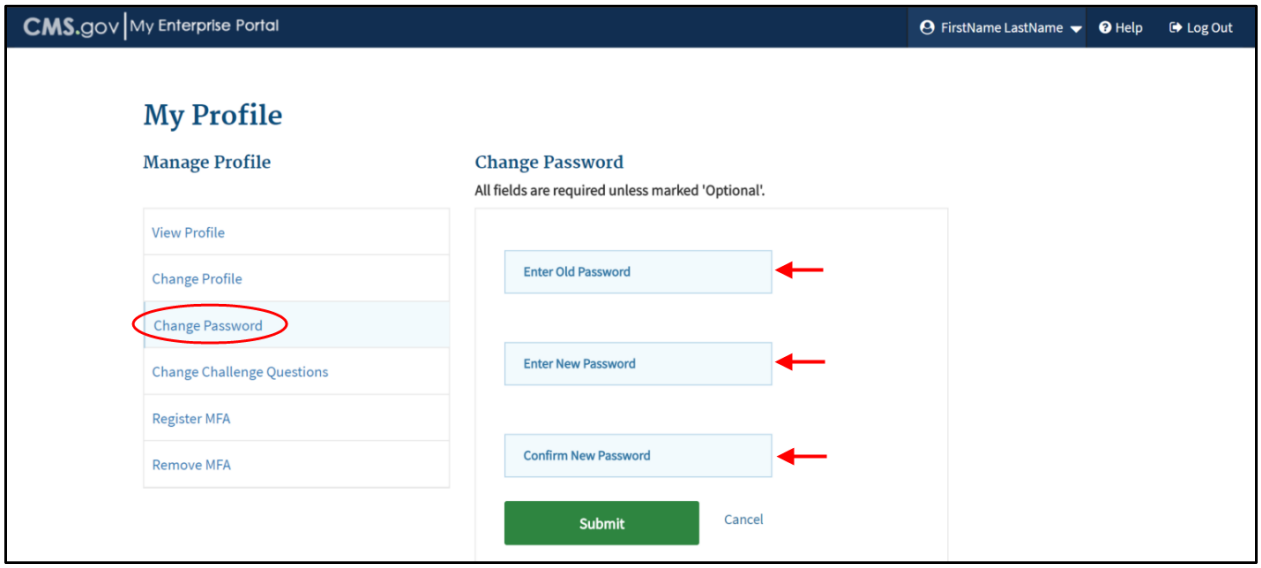

Figure 53: Change Password

Note: If the new password you enter is not compatible with the password guidelines, an error occurs, as shown in *Figure 54: Password Guidelines Not Met.*

Figure 54: Password Guidelines Not Met

A tool tip is enabled that provides the password requirements, as shown in *Figure 55: Change Password – Tool Tip.*

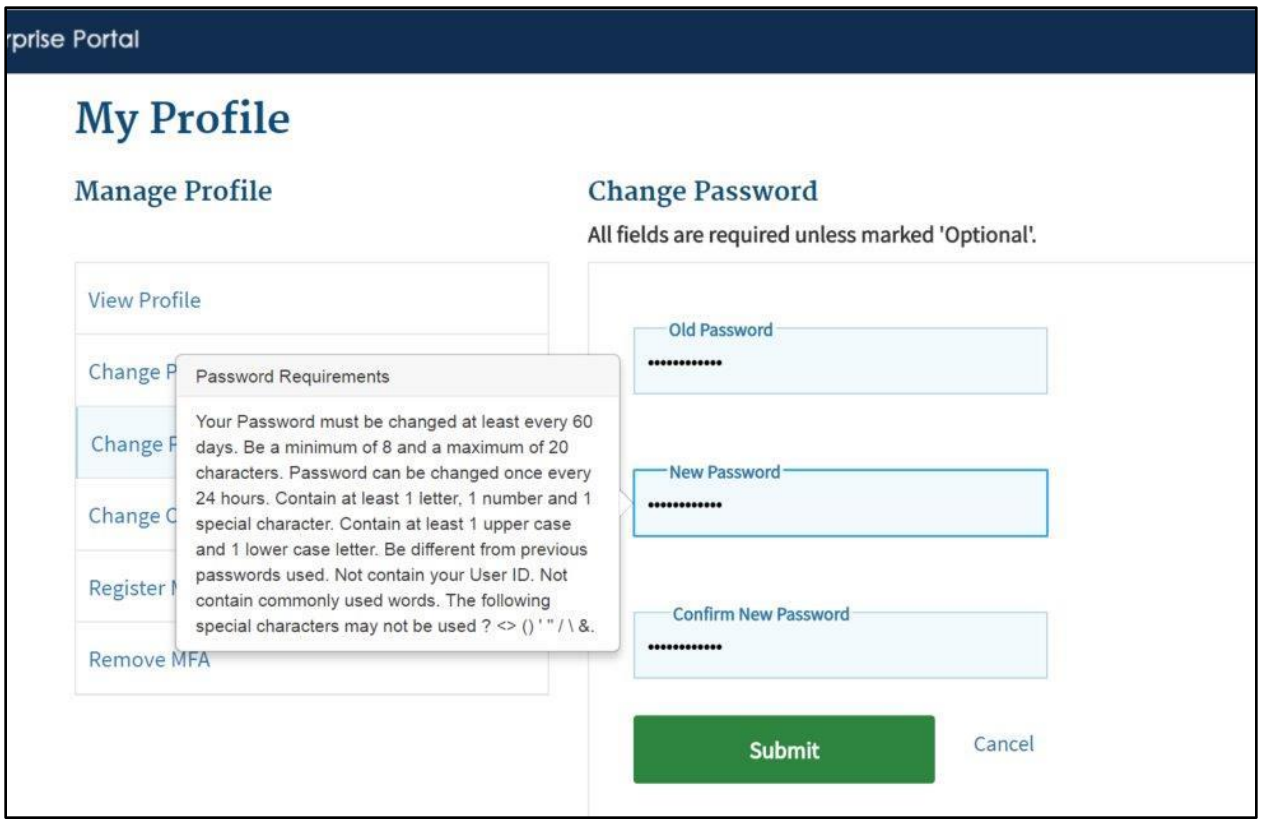

Figure 55: Change Password – Tool Tip

Or you may refer to *Figure 56: Password Requirements.*

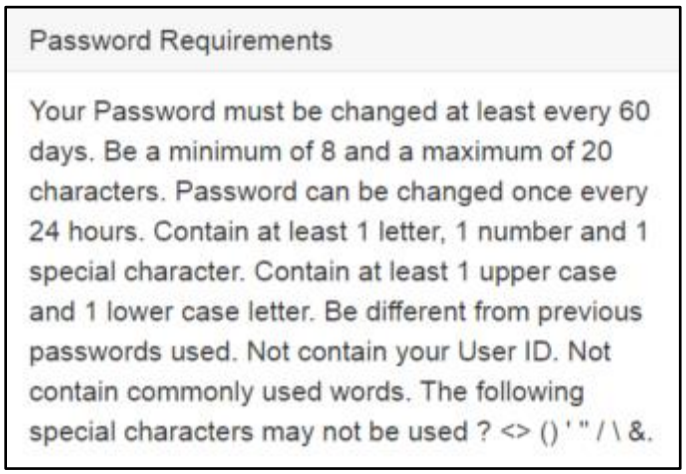

Figure 56: Password Requirements

7. After submitting the updated password information, you will receive confirmation that the changes to your profile were submitted successfully, as shown in *Figure 57: Change Password – Successful Confirmation.*

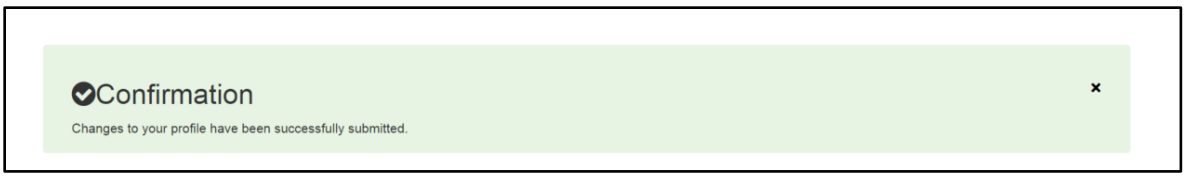

Figure 57: Change Password – Successful Confirmation

Note: You will receive an e-mail notification indicating that you successfully changed your password.

9.4 Changing Your Challenge Questions

The following are the instructions on how to use the 'Change Challenge Questions' feature to change your challenge questions and answers.

1. Navigate to the CMS Enterprise Portal public landing page.
2. Login using your user ID and password.

   The CMS Enterprise Portal **My Portal** page is displayed, as shown in *Figure 46: 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 47: View My Profile.*
4. Select **Change Challenge Questions** as shown in *Figure 58: Change Challenge Questions*.
5. Enter the user ID in the **Enter User ID** field.
6. Enter the password in the **Enter Password** field.
7. Click **Next**.

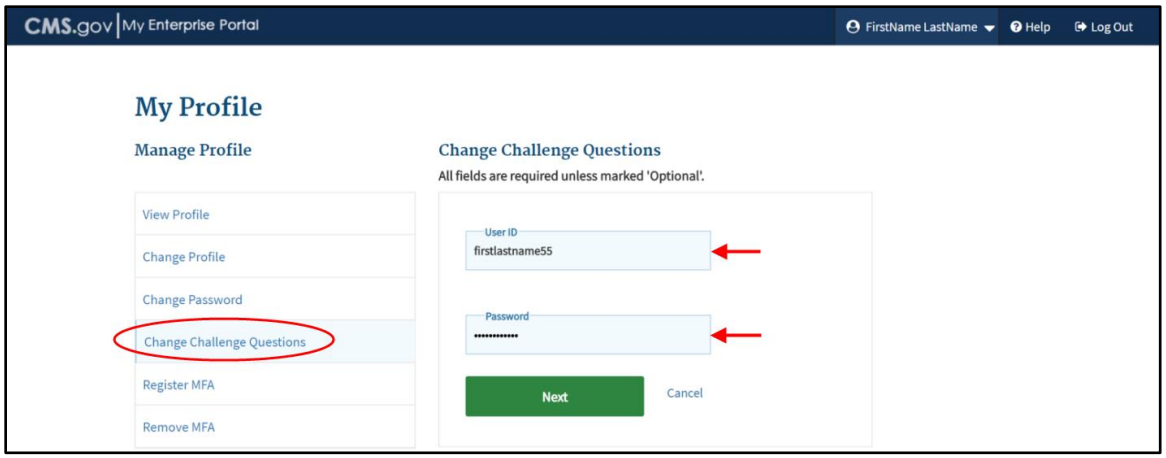

Figure 58: Change Challenge Questions – Login

8. Select a question and then provide an answer of your choosing. Continue until all three challenge questions have been selected and answered. Click **Submit**.

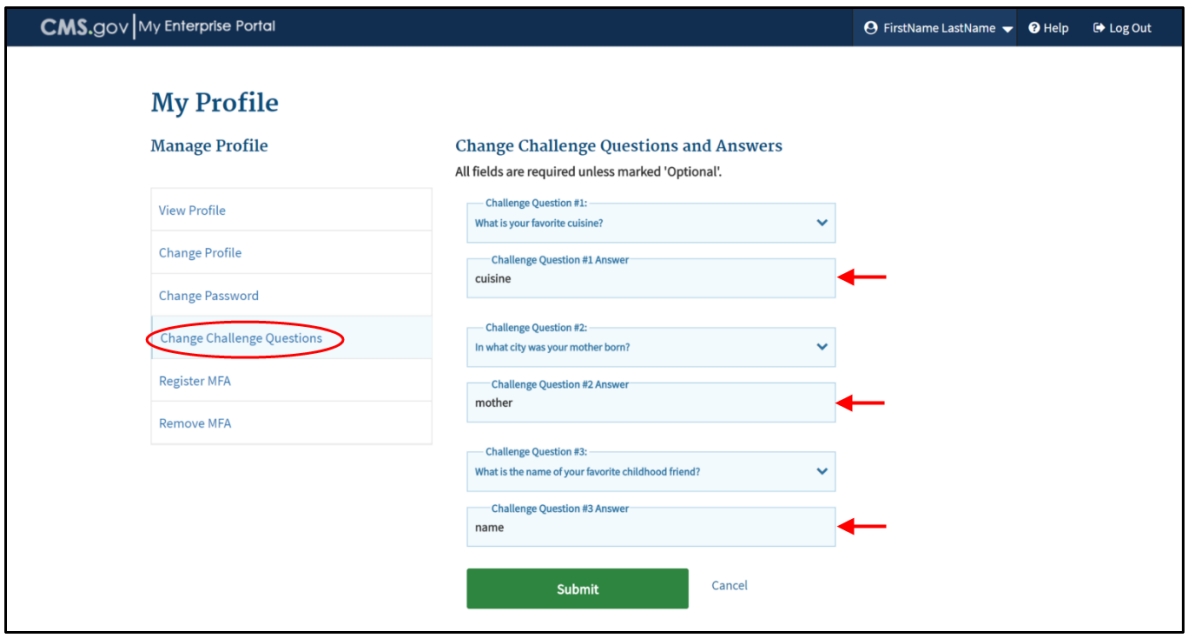

Figure 59: Change Challenge Questions – Update Information

Note: If an invalid combination of user ID and password was entered in the process of changing the challenge questions, an error occurs, as shown in *Figure 60: Incorrect Credentials Error Message.* After 3 failed attempts, your account will be locked. For detailed steps on how to unlock your account, refer to Section *8 - Unlocking Account*.

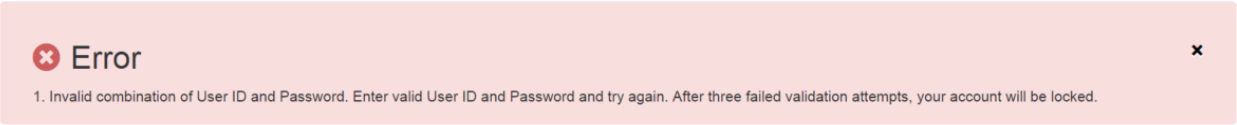

Figure 60: Incorrect Credentials Error Message

9. After submitting the updated information, you will receive confirmation that the changes to your profile were submitted successfully, as shown in *Figure 61: Change Password – Successful Confirmation*.

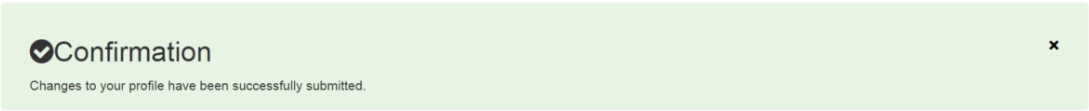

Figure 61: Change Password – Successful Confirmation

9.5 Registering 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 in with your User ID and Password.

Registered CMS portal users who wish to access a CMS MFA protected application are directed through the MFA registration process.

During the MFA registration process, the CMS EIDM system requires registration of a phone or computer to add an additional level of security to a user's account. The user is given five options from which to select, to complete the registration process:

- **Phone/Tablet/PC/Laptop**: Users can download VIP access software on their smart phone/tablet/computer. The user must enter the alphanumeric Credential ID that is generated by the VIP access client. The user then enters the Security Code generated by the VIP client.
- **Short Message Service (SMS)**: Users can use the SMS option to have their Security Code texted to their phone. The user must enter a valid phone number. The phone must be capable of receiving text messages. Carrier charges may apply.
- **Interactive Voice Response (IVR)**: The user can select the IVR option to receive a voice message containing their Security Code. The user must provide a valid phone number and (optional) phone extension.
- **E-mail**: Users can select the e-mail option to receive an e-mail containing the Security Code required at login. The e-mail address on the user's profile is used.

Notes:

• Delays in e-mail transmission, spam filters, and other issues outside the user's control can make this the least desirable option to receive a security code.

• Users can register more than one phone number for the SMS device type. Symantec will only use one number (the lowest number by area code) to send the Security Code.

• While the 'Security Code' for the VIP Access Software refreshes automatically every 30 seconds, the 'Security Code' for the 'E-mail' and 'One-Time Security Code' options expire in 30 minutes. The 'Security Code' for the other MFA device types expire in 10 minutes. If you are unable to enter the code within the allotted period, you must request a new one.

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

1. Navigate to the CMS Enterprise Portal public landing page.
2. The CMS Enterprise Portal **My Portal** page is displayed, as shown in *Figure 46: 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 47: View My Profile*.
4. Select **Register MFA**, as shown in *Figure 62: Register MFA*.

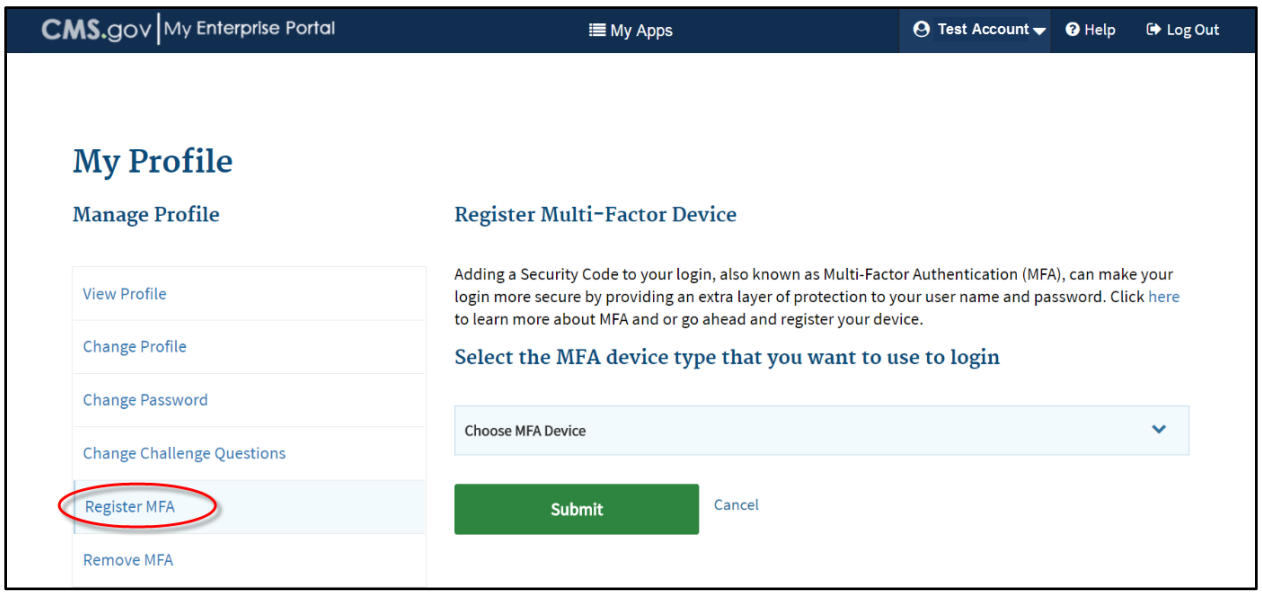

Figure 62: Register MFA

5. Expand the **Choose MFA Device** drop-down list, as shown in *Figure 63: Register MFA – Choose MFA Device.*

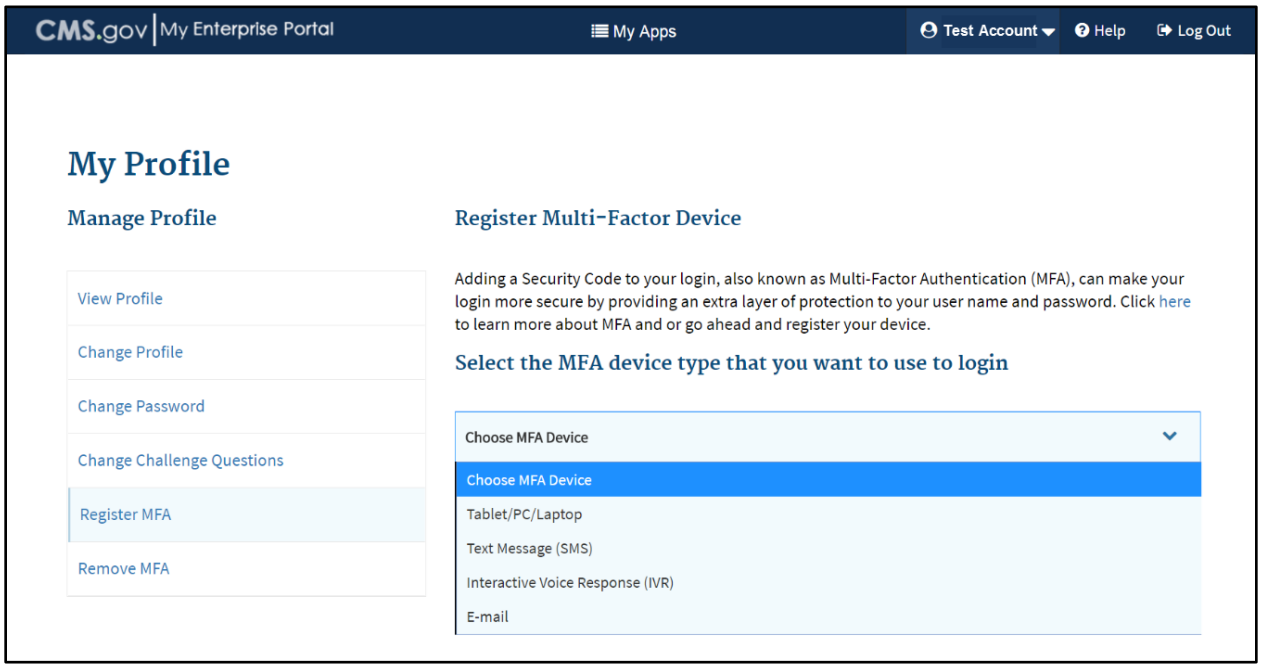

Figure 63: Register MFA – Choose MFA Device

6. Select your MFA Device.

   Specific directions are displayed depending on your selection. See the Register MFA Device options below.

Phone/Tablet/PC/Laptop

1. If you select **Phone/Tablet/PC/Laptop** as the MFA Device Type, read the information under the **Phone/Tablet/PC/Laptop** drop-down, as shown in *Figure 64: Register Phone/Tablet/PC/Laptop.*
2. Enter the alphanumeric code that displays under the field labeled **Credential ID** (on the VIP Access software (see *Figure 65: VIP Access*)) in the **Enter Credential ID** field. Enter a brief description (e.g., Laptop) in the field labeled **Enter MFA Device Description**. Then, click **Submit**.

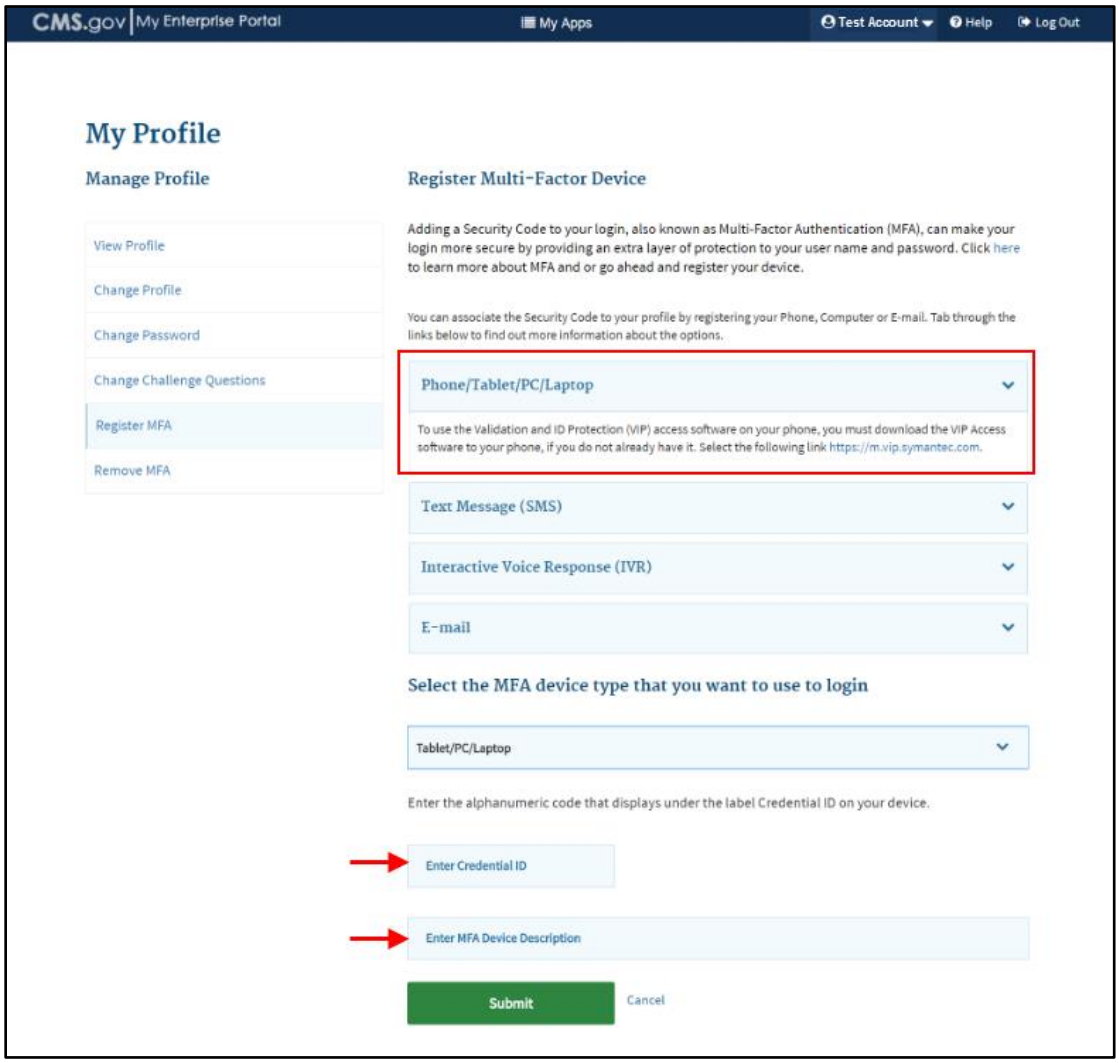

Figure 64: Register Phone/Tablet/PC/Laptop

Figure 65: VIP Access

3. After submitting the information, you will receive confirmation that the changes to your profile were submitted successfully, as shown in *Figure 66: Register MFA Device – Successful Confirmation.*

   Your registration of the MFA device is now complete.

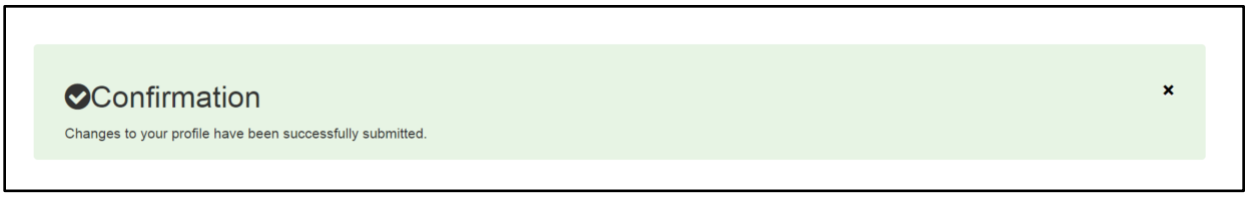

Figure 66: Register MFA Device – Successful Confirmation

Text Message (SMS)

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 67: Register Text Message (SMS).*
2. Enter the Phone Number that will be used to obtain the Security Code in the **Enter Phone Number** field. Enter a brief description (e.g., Text) in the field labeled **Enter MFA Device Description**. Then, click **Submit**.

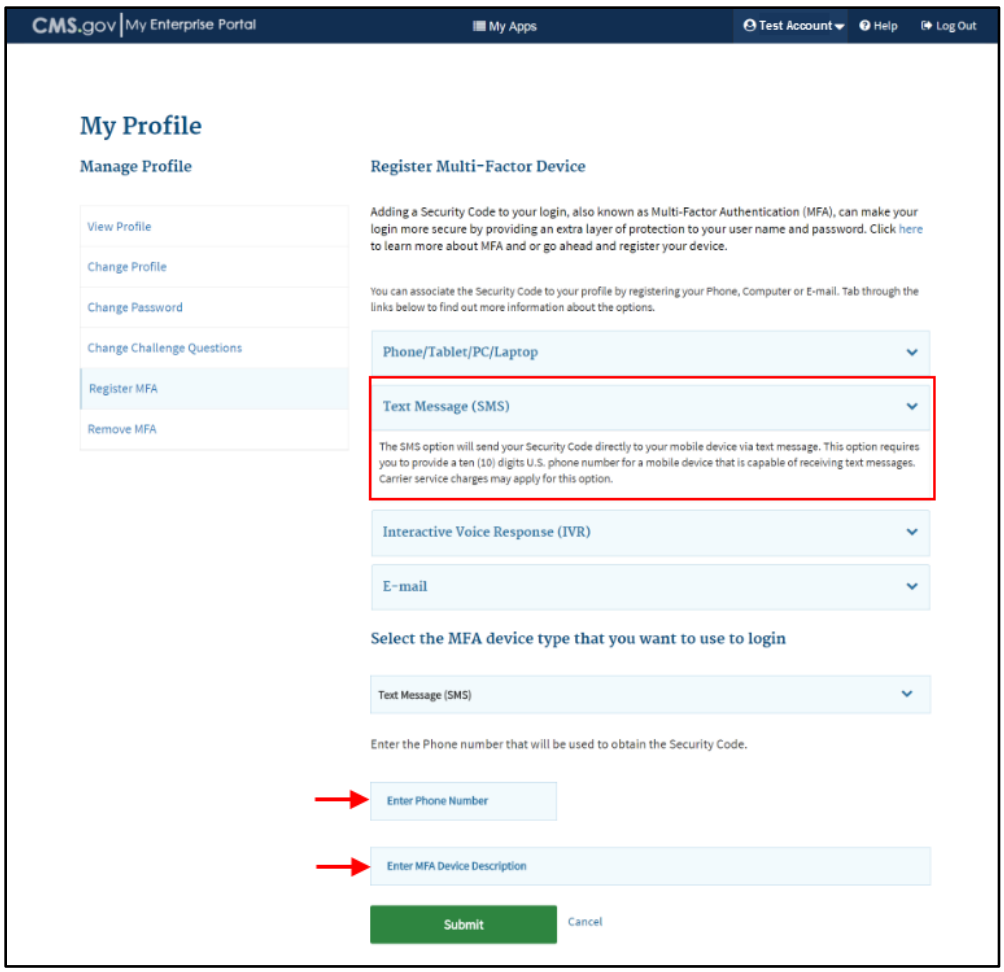

Figure 67: Register Text Message (SMS)

3. After submitting the information, you will receive confirmation that the changes to your profile were submitted successfully, as shown in *Figure 68: Register MFA Device – Successful Confirmation*.

   Your registration of the MFA device is now complete.

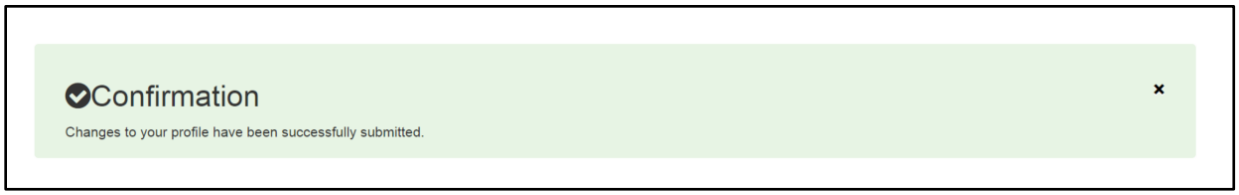

Figure 68: Register MFA Device – Successful Confirmation

Interactive Voice Response (IVR)

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 69: Register Interactive Voice Response (IVR).*
2. Enter the Phone Number and corresponding extension that will be used to obtain the Security Code in the **Enter Phone Number** field. Enter a brief description (e.g., IVR) in the field labeled **Enter MFA Device Description**. Then, click **Submit**.

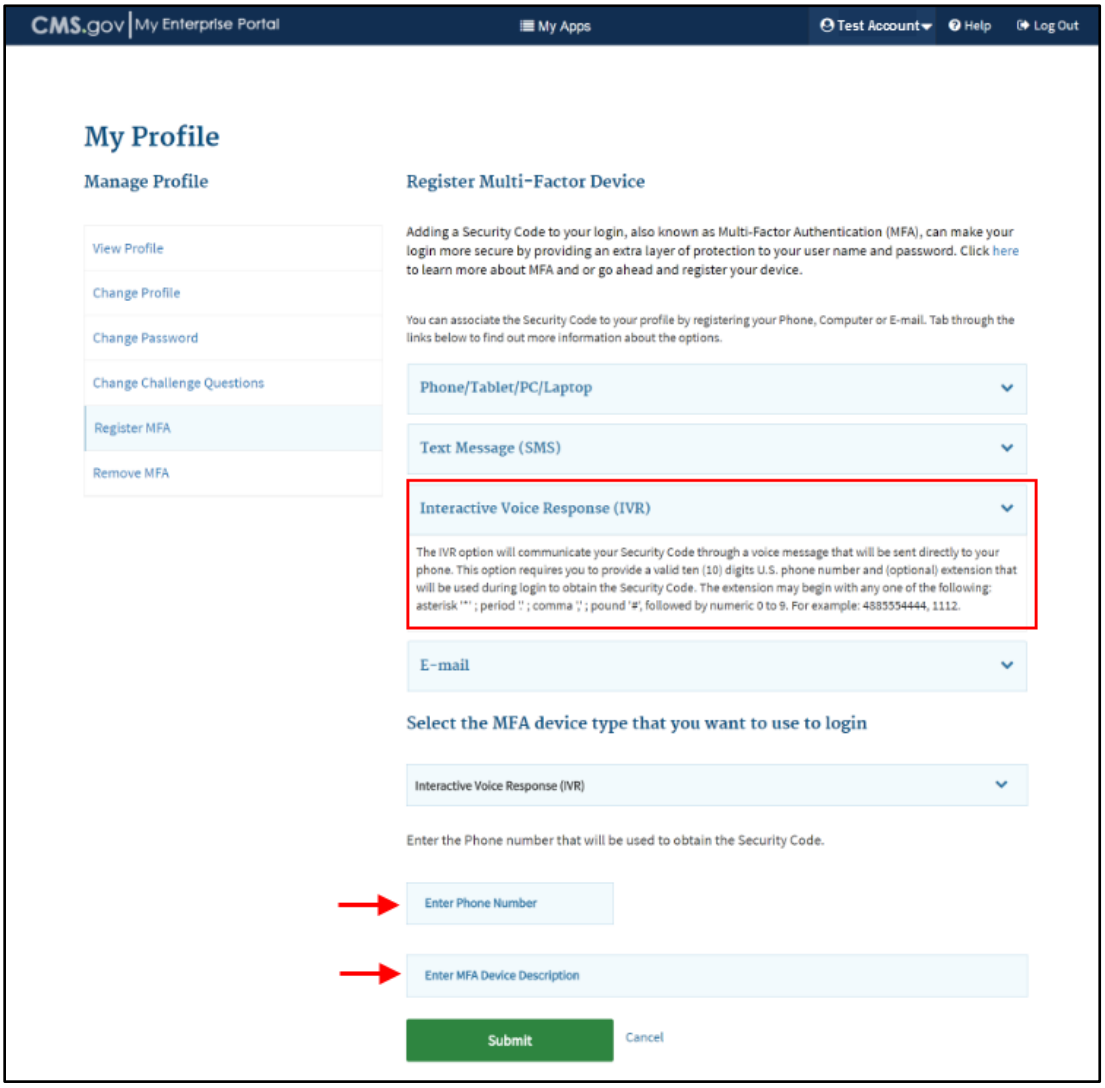

Figure 69: Register Interactive Voice Response (IVR)

3. After submitting the information, you will receive confirmation that the changes to your profile were submitted successfully, as shown in *Figure 70: Register MFA Device – Successful Confirmation.*

   Your registration of the MFA device is now complete.

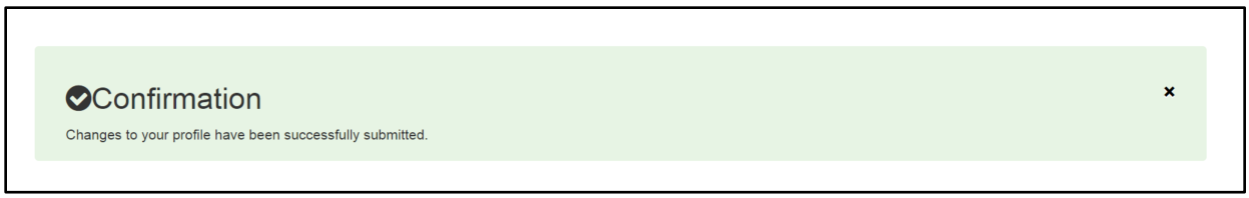

Figure 70: Register MFA Device – Successful Confirmation

E-mail

1. If you select **E-mail** as the MFA Device Type, read the information under the **E-mail** drop-down, as shown in *Figure 71: Register E-mail.*
2. The e-mail address on your profile will be automatically used to obtain the Security Code. Enter a brief description (e.g., e-mail) in the field labeled **Enter MFA Device Description**. Then, click **Submit.**

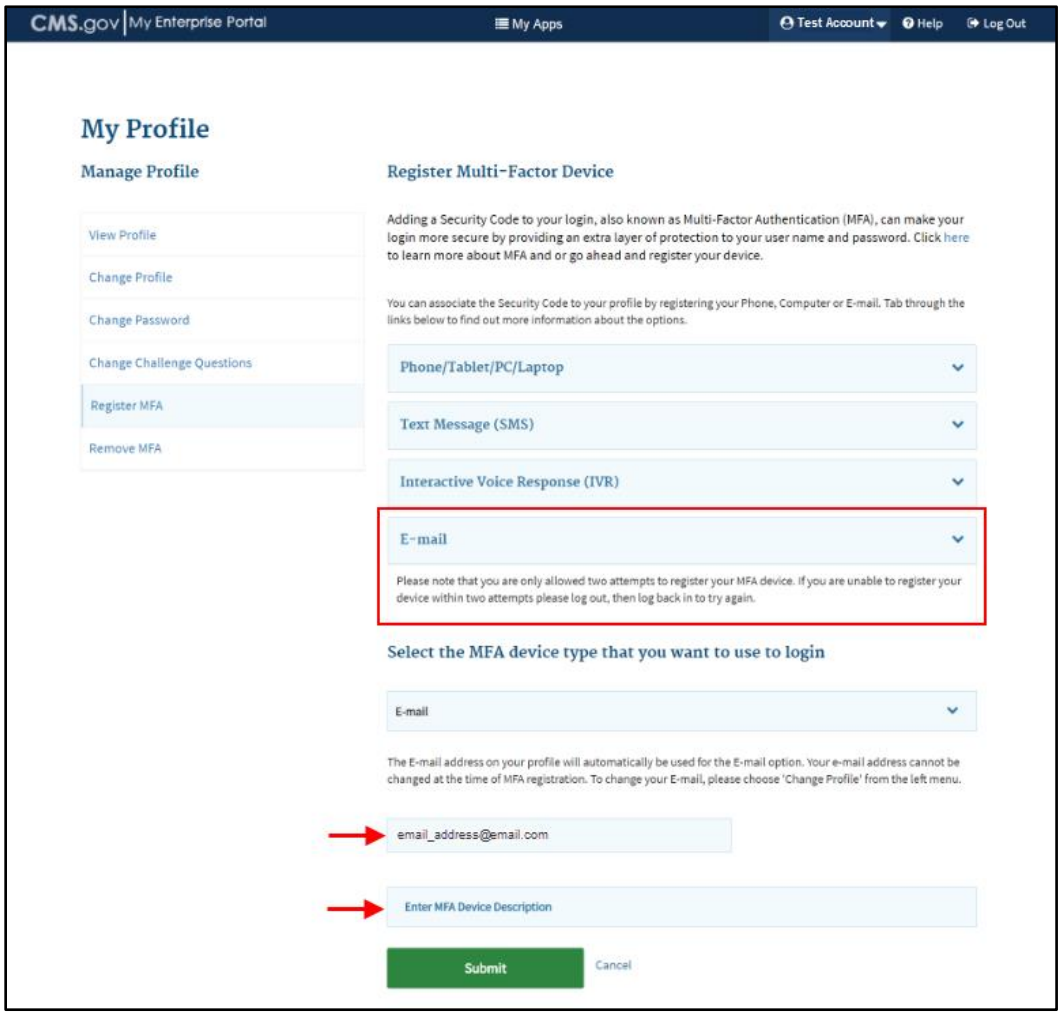

Figure 71: Register E-mail

Note: The e-mail address cannot be changed at the time of MFA device registration. It can only be changed using the 'Change E-Mail Address' option from the 'Change My Profile' menu.

3. After submitting the information, you will receive confirmation that the changes to your profile were submitted successfully, as shown in *Figure 72: Register MFA Device – Successful Confirmation*.

   Your registration of the MFA device is now complete.

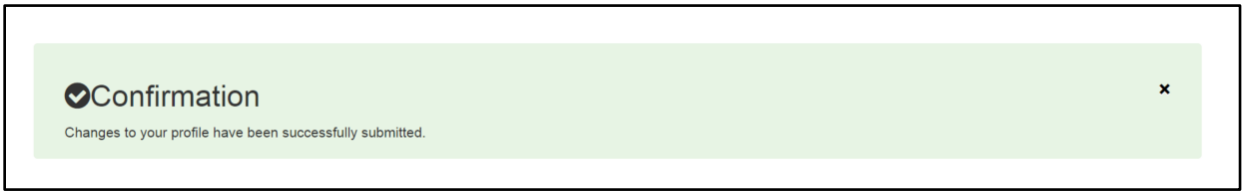

Figure 72: Register MFA Device – Successful Confirmation

9.6 Removing MFA

To remove a registered phone or computer, please follow each step listed below unless otherwise noted.

1. Navigate to the CMS Enterprise Portal public landing page.
2. The CMS Enterprise Portal **My Portal** page is displayed, as shown in *Figure 46: 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 47: View My Profile*.
4. Click **Remove MFA**, as shown in *Figure 73: Remove MFA*.

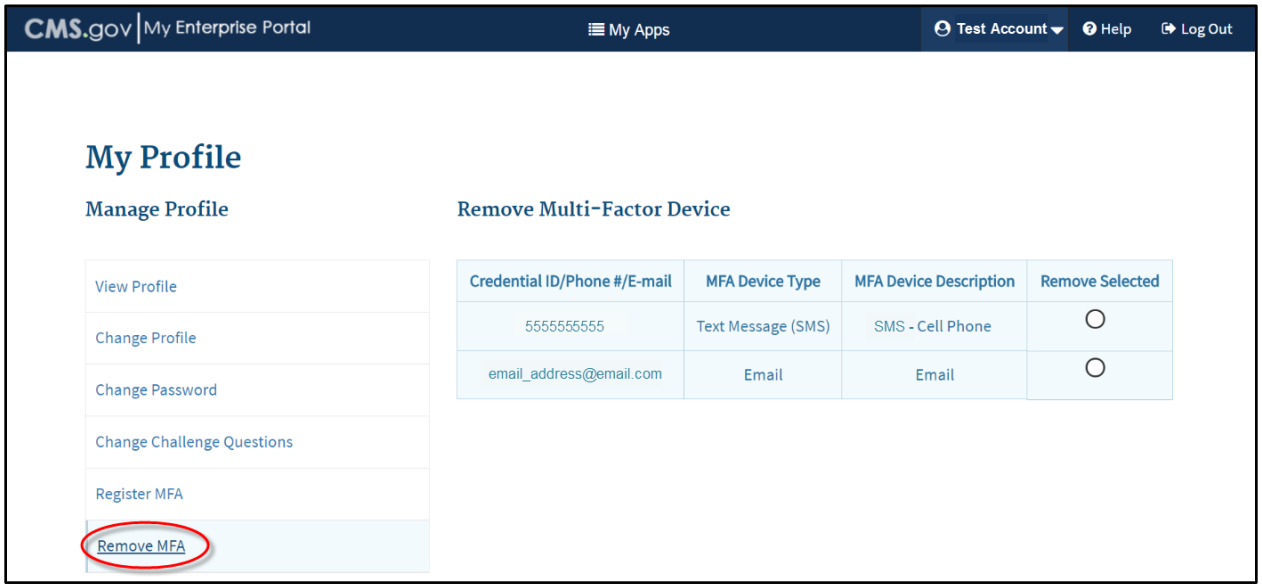

Figure 73: Remove MFA

5. Select the radio button next to the registered device you want to remove, as shown in *Figure 74: Remove MFA Device*.
6. Click the **Send Code** button to receive the security code on the selected MFA device.

7. Enter the security code received on the selected MFA device in the **Enter Security Code** field.

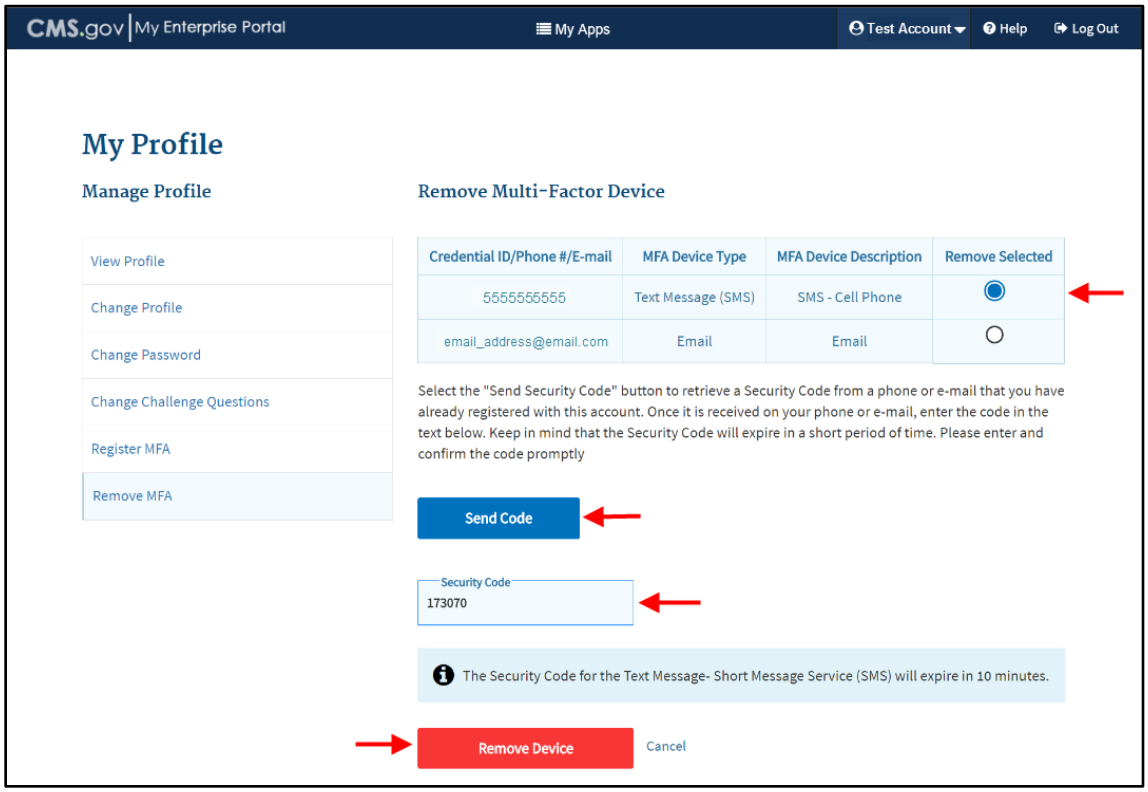

Figure 74: Remove MFA Device

8. Click **Remove Device**.

9. After submitting the information, you will receive confirmation that the changes to your profile were submitted successfully, as shown in *Figure 75: Remove MFA Device – Successful Confirmation.*

   Removal of the MFA device is now complete.

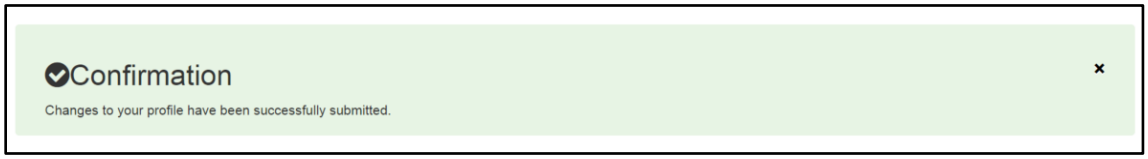

Figure 75: Remove MFA Device – Successful Confirmation

Note: Once MFA is enabled for the account, you must always have at least one MFA device registered.

If you attempt to remove the only MFA device registered, as shown in *Figure 76: Only One MFA Registered Device*, an error will occur, as shown in *Figure 77: Register New Device Error.*

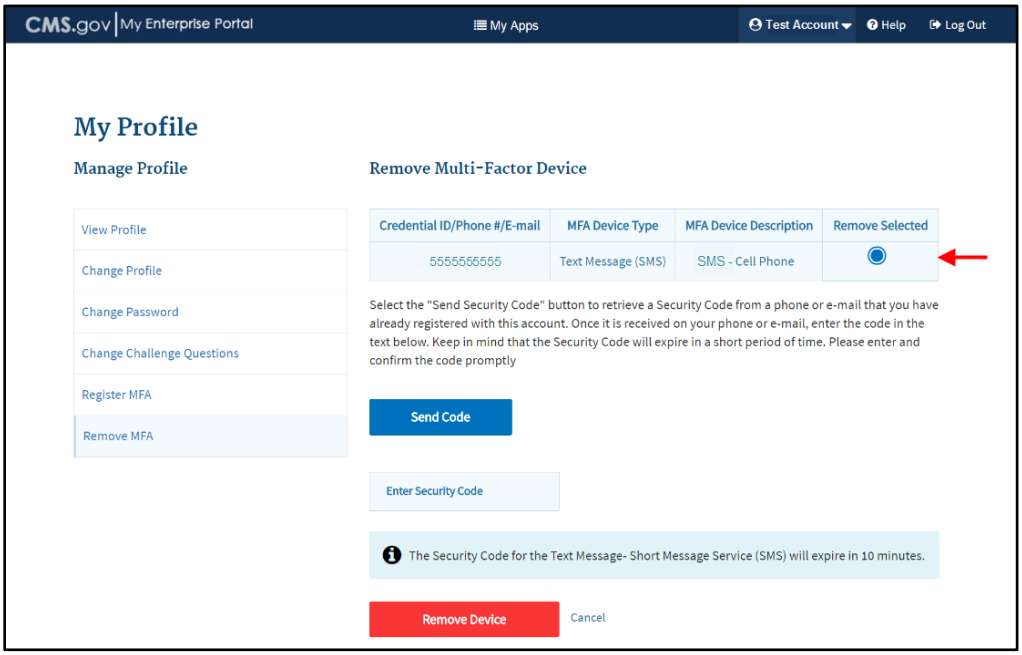

Figure 76: Only One MFA Registered Device

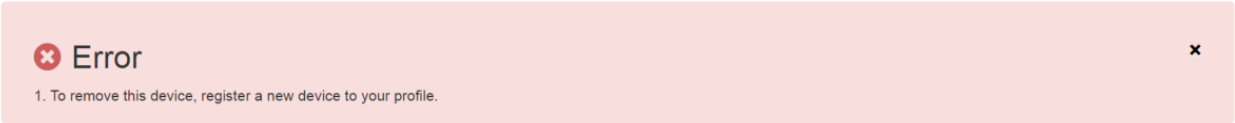

Figure 77: Register New Device Error

10. 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 User Manual. 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.

10.1 Application Access Catalog

Registered users can use the application **Access Catalog** to request access to CMS applications.

The catalog is accessed by selecting the **My Access** option from the Welcome drop-down list in the top navigation bar or by clicking the **Request/Add Apps** tile on the **My Portal** page, as shown in *Figure 78: Accessing the Application Catalog.*

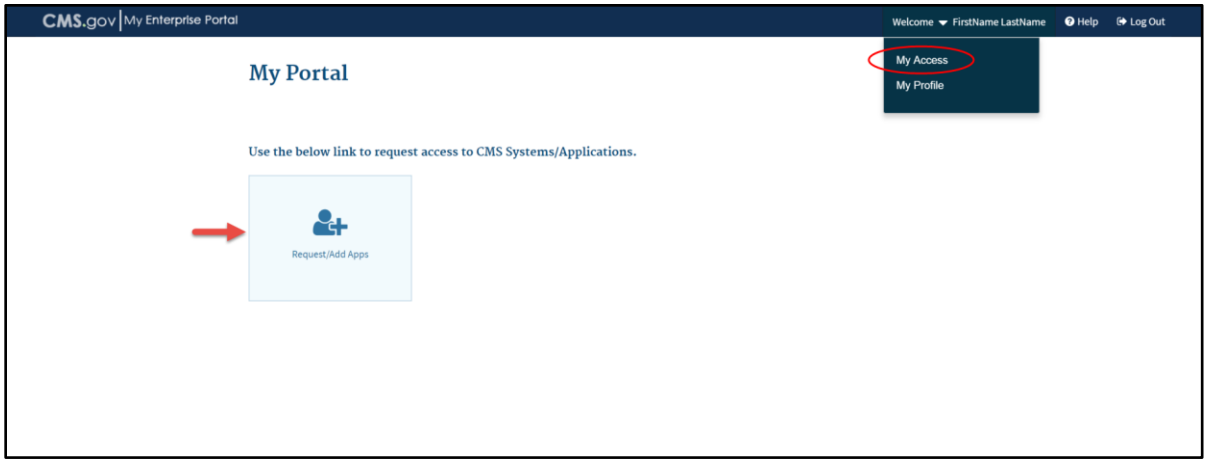

Figure 78: Accessing the Application Catalog

The application **Access Catalog** displays all the CMS applications that use EIDM services, as shown in *Figure 79: Access Catalog Page.*

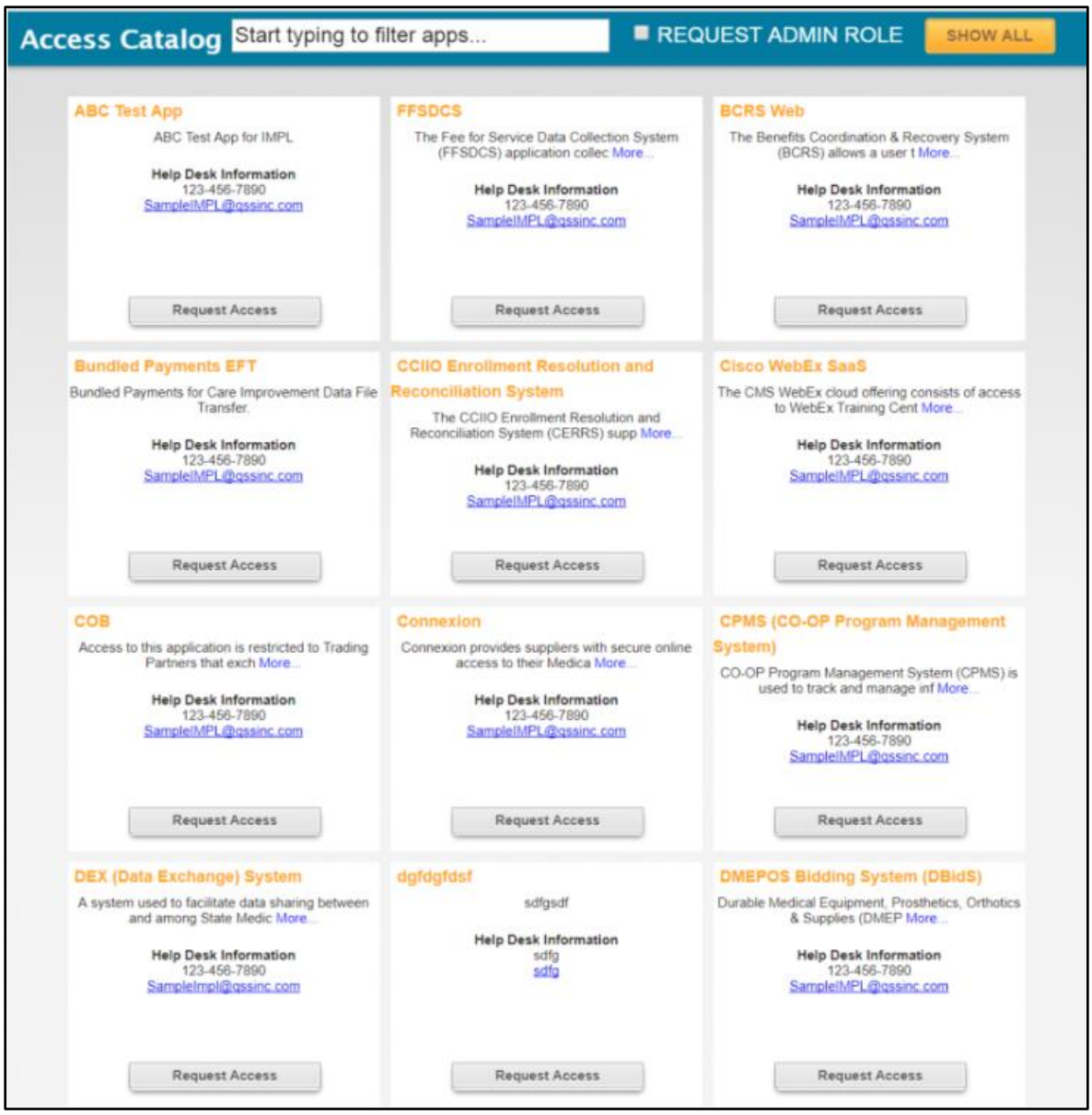

Figure 79: Access Catalog Page

10.2 Access Catalog Features

The features listed below refer to the numbered image shown in *Figure 80: Features of Access Catalog.*

1. **Request Access** – Request access to a particular application by clicking on the **Request Access** button on the application's tile.
2. **Search** – Search for a particular application by typing the name of the application in the search box on the **Access Catalog** title bar.
3. **My Access** – This panel displays information for each application for which the user has access including:
    a. Contact information for the application's Help Desk.

b. The existing roles the user has been granted for the application.

4. **Available Actions** – This panel appears for each application for which the user has access. The user can select from the following options:
   a. Add a Role – Directs the user to the **Request Additional Role** screen to request an additional role for the application.
   b. Remove a Role – Directs the user to the **View and Manage My Access** screen to remove a role from the application.
   c. Other Actions – Directs the user to the **View and Manage My Access** screen to select other options.
5. **My Pending Requests** – This section lists the pending requests for which the user has requested access.

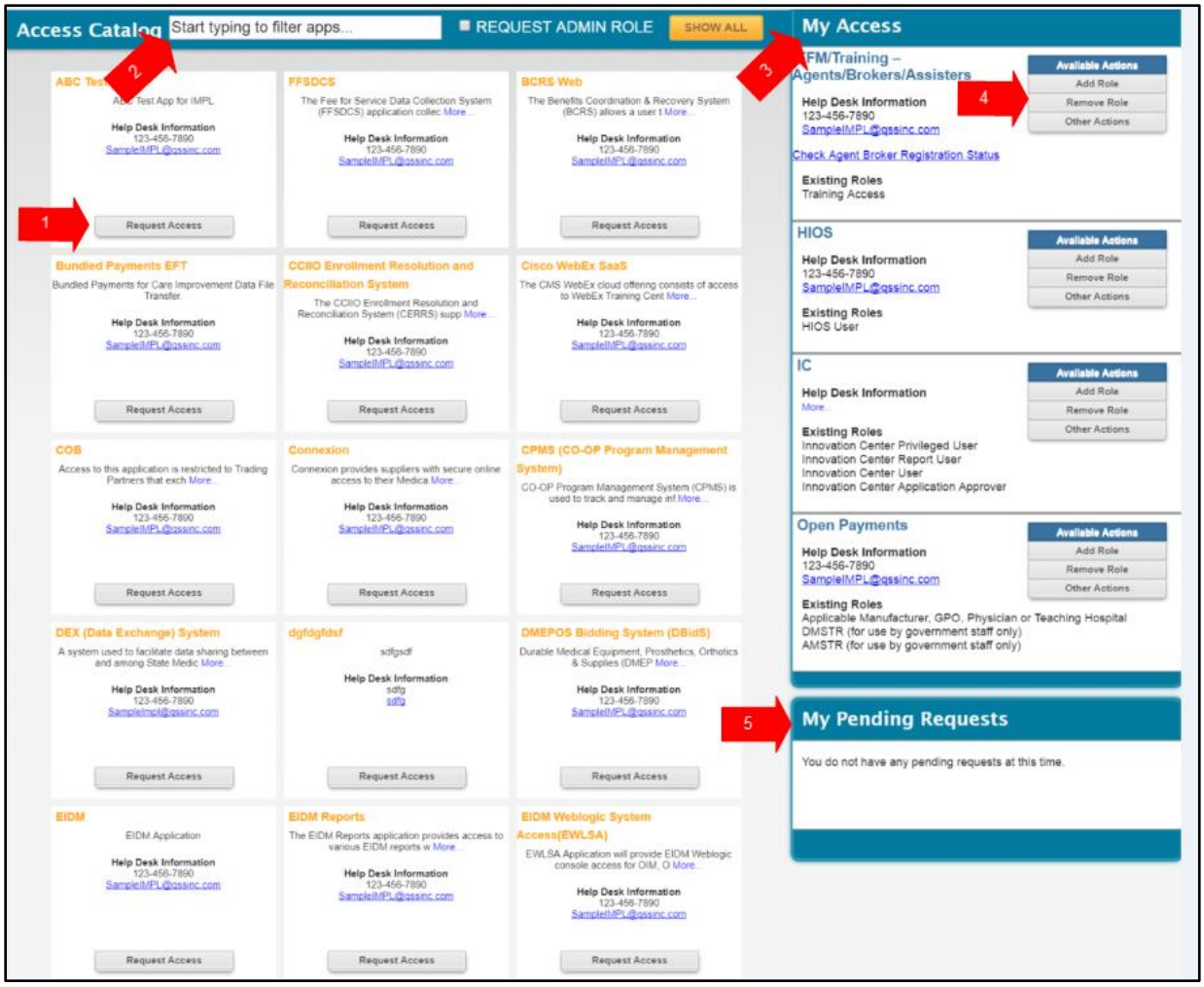

Figure 80: Features of Access Catalog

10.3 Requesting a Role

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

1. Navigate to the CMS Enterprise Portal public landing page.
2. Login using your user ID and password.
3. On the **My Portal** page, as shown in *Figure 78: Accessing the Application Catalog*, select the **My Access** option from the Welcome drop-down list in the top navigation bar. Alternatively, click **Request/Add Apps** to continue.
4. On the **Application Catalog** page, scroll down to locate the application you need. Alternatively, enter the first few letters of the application in the Search section and all of the applications beginning with those letters will display, as shown in *Figure 81: Searching for an Application.*

Note: If you currently have access to one or more applications, they display in the My Access panel. If you have pending requests, they display in the **My Pending Requests** panel.

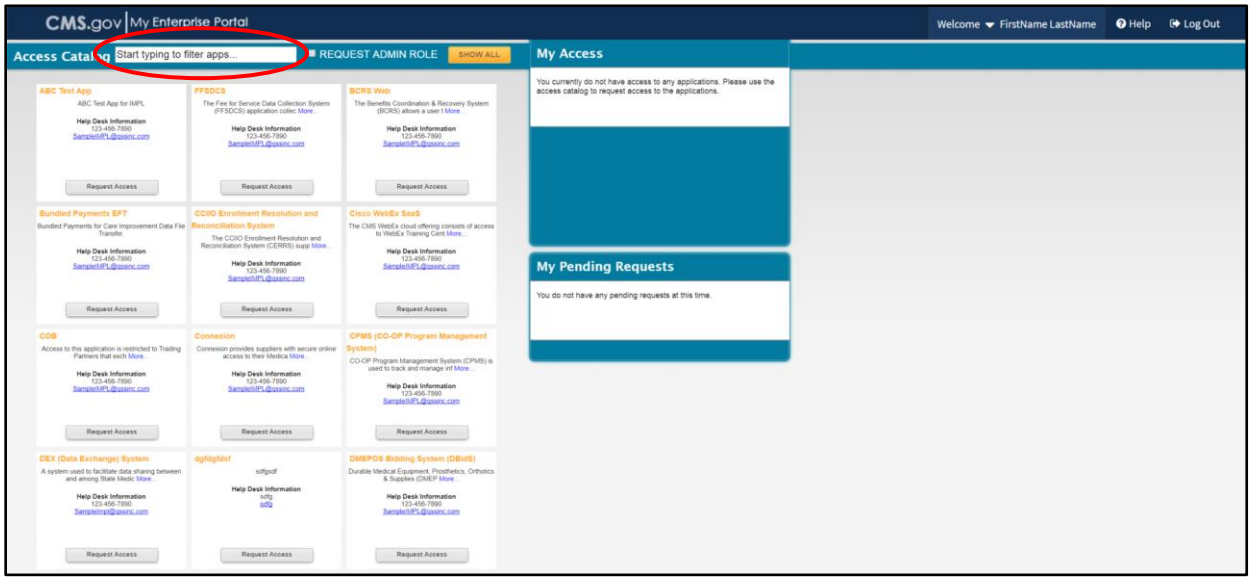

Figure 81: Searching for an Application

5. Click **Request Access** for the application you need, as shown in *Figure 82: Requesting Access for an Application.*

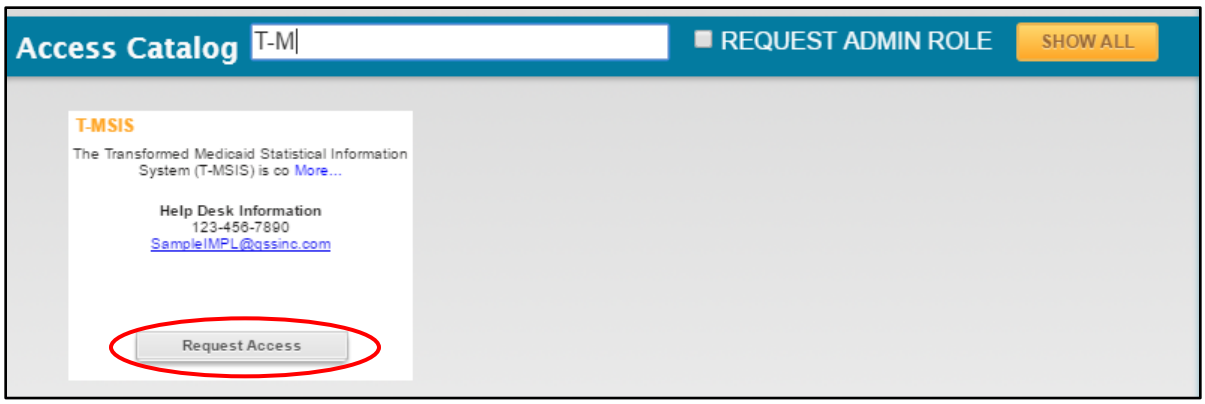

Figure 82: Requesting Access for an Application

The **Request New System Access** page displays, as shown in *Figure 83: Request New System Access Page.*

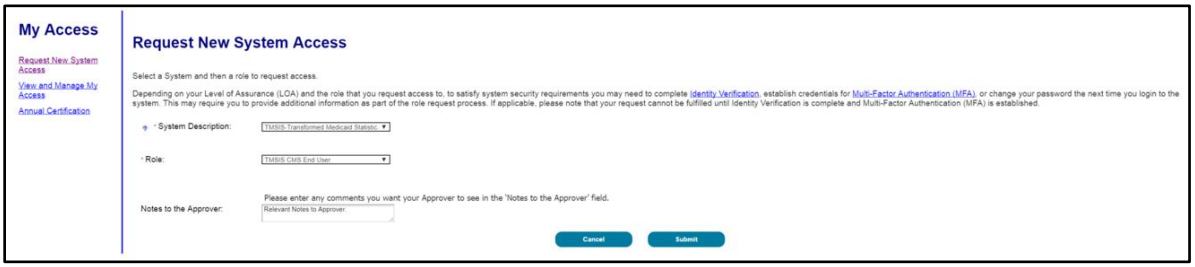

Figure 83: Request New System Access Page

6. Click **Submit** to submit the request for approval.

   If you select a role that requires identity verification, the Identify Verification page is displays as shown in *Figure 84: Identity Verification Page*. Follow steps 6 through 12 to complete the Identity Verification process.

   If you select an application and role that does not require identity verification, skip to step 12.

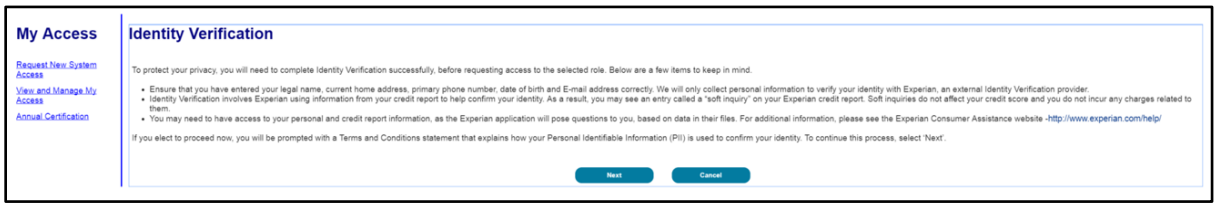

Figure 84: Identity Verification Page

Note: Depending on the role and the information you provide, the system may take you to the Identity Verification page. The Identity Verification process, also known as Remote Identity Proofing (RIDP), is necessary for roles that require a higher level of security to access. Identity Verification is done by asking you questions based on your personal information.

7. Click **Next** to begin the Identity Verification process.

8. Read the **Terms and Conditions** information on this screen and indicate your agreement by selecting the **I agree to the terms and conditions** checkbox. Click the **Next** button to continue, as shown in *Figure 85: Terms and Conditions Information.*

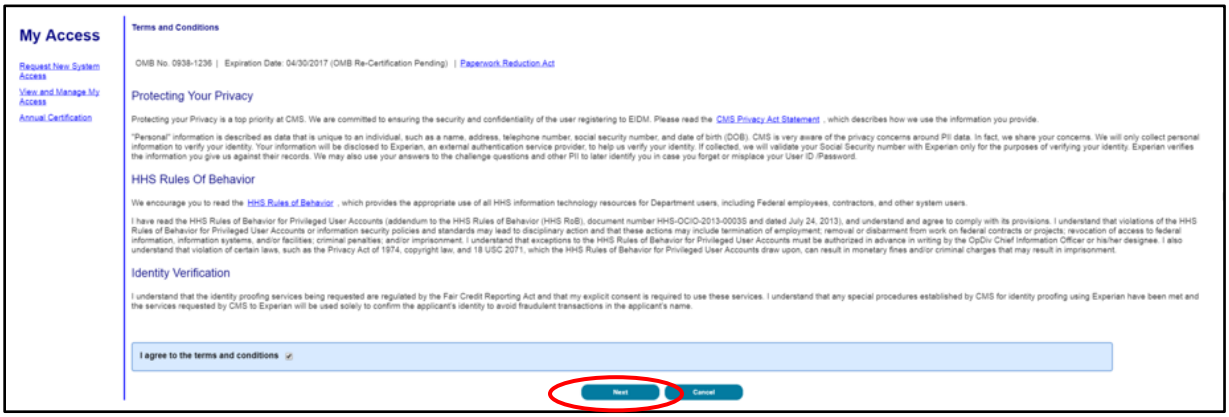

Figure 85: Terms and Conditions Information

9. Enter your information into the required fields of the **Your Information** page. Click **Next** to continue the Identity Verification process, as shown in *Figure 86: Your Information Page*.

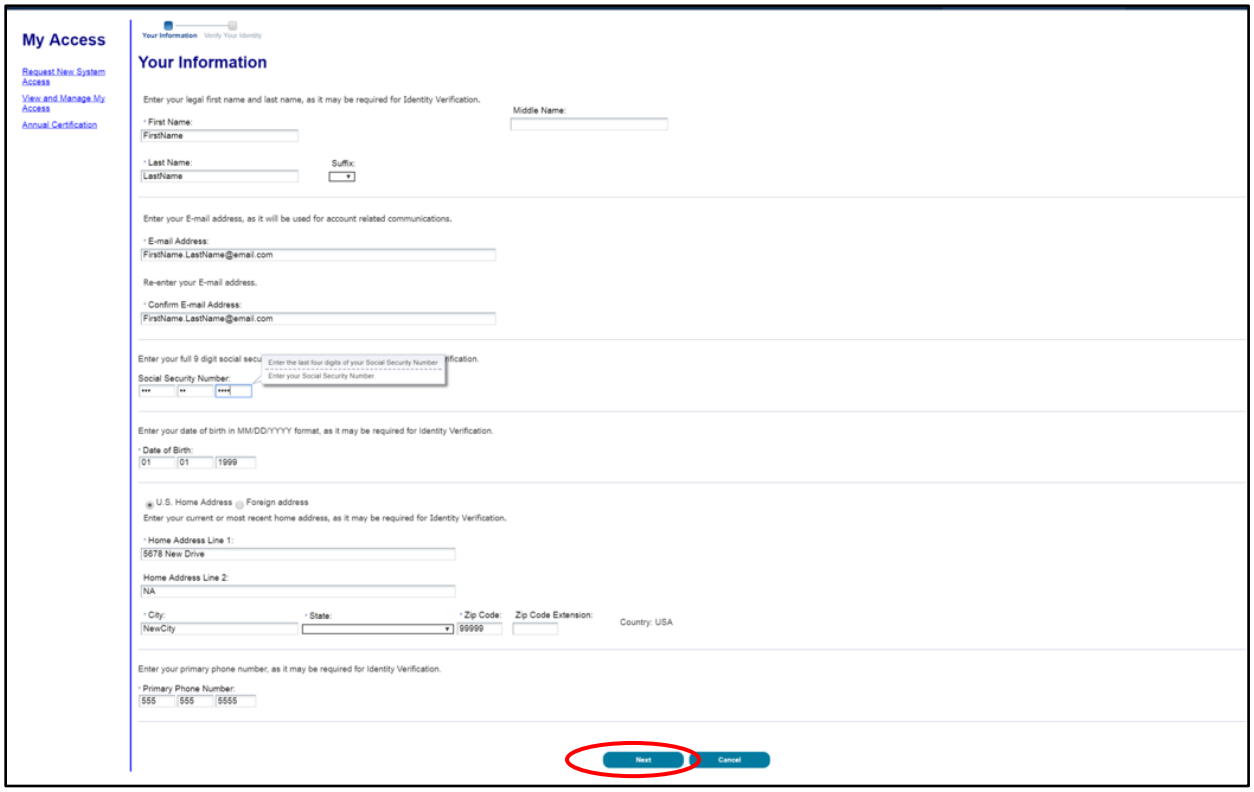

Figure 86: Your Information Page

10. If you select a CMS MFA-protected application, the Multi-Factor Authentication Information page is displayed, as shown in *Figure 87: Multi-Factor Authentication Information Page*. Click **Next** to begin the MFA Registration process.

Figure 87: Multi-Factor Authentication Information Page

Note: Multi-Factor Authentication (MFA) is a security mechanism that is implemented to provide an extra layer of security such as a security code, when logging in with your User ID and Password. Registered CMS Enterprise Portal users who wish to access a CMS MFA-protected application are directed through the MFA registration process. During the MFA registration process, the CMS EIDM system requires registration of a phone or computer to add an additional level of security to a user's account. The user is given four options from which to select, to complete the registration process: 1. Phone/Tablet/PC/Laptop, 2. SMS, 3. IVR, and 4. E-mail.

11. To make your account more secure, you are directed to the **Register Your Phone, Computer, or E-Mail** page, as shown in *Figure 88: Register Your Phone, Computer, or E-Mail Page*. Select the device type you wish to register from the **MFA Device Type** drop-down list and enter the other required information.

    For more details on how to register an MFA device, refer to the *Section 9.5 - Registering Multi-Factor Authentication (MFA).*

Figure 88: Register Your Phone, Computer, or E-Mail Page

12. After submitting the registration, a message that you have successfully registered your device is displayed, as shown in *Figure 89: MFA Success Message*. Click **OK** to continue.

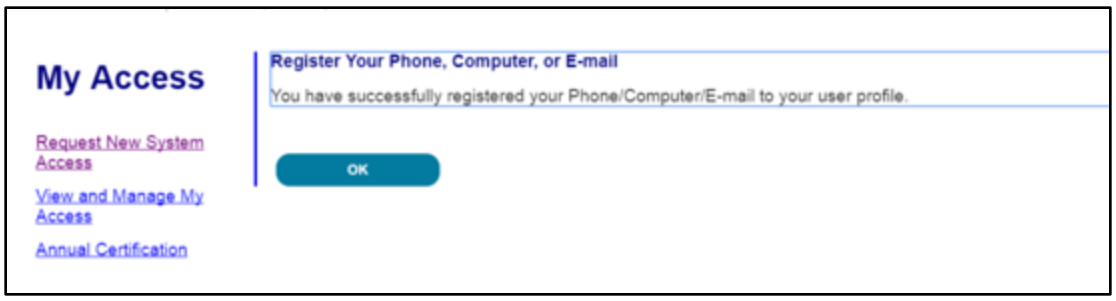

Figure 89: MFA Success Message

13. The **Request Acknowledgement** message is displayed, as shown in *Figure 90: Request Acknowledgement Page*. Click the **OK** button to exit the screen and return to the **View and Manage My Access** page.

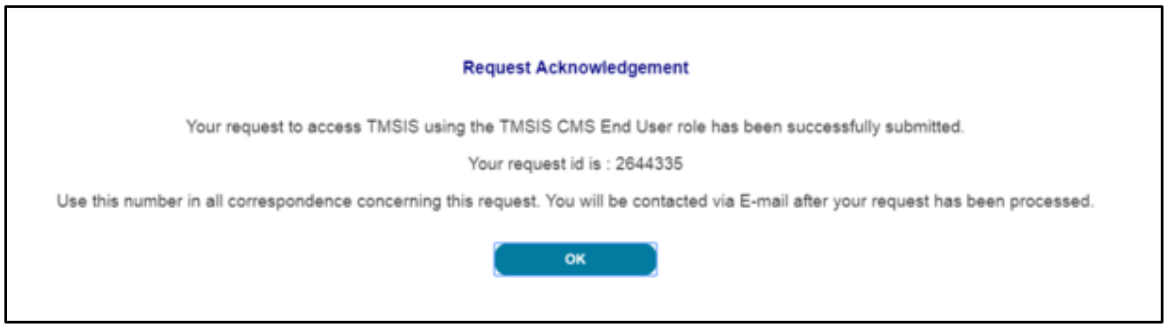

Figure 90: Request Acknowledgement Page

Appendix A: Record of Changes

Table 1: Record of Changes lists the changes that have been made in this document over time.

Table 1: Record of Changes

Version Number	Date	Author/Owner	Description of Change
1.0	10/31/2017	CSRA/Maricom	EP_UIRedesign_UserManual_v1_D Initial draft version
2.0	11/1/2017	CSRA/Maricom	EP_UIRedesign_UserManual_v2 Edited entire document for consistency of writing and formatting styles Updated Appendices B, C, D and E
3.0	11/7/2017	CSRA/Maricom	EP_UIRedesign_UserManual_v3 Addressed feedback from CMS team
4.0	11/8/2017	CSRA/Maricom	Enterprise_Portal_User_Manual_v4 Changed document number Made minor edits per CMS' request
5.0	11/9/2017	CSRA/Maricom	Enterprise_Portal_User_Manual_v5 Addressed findings from internal QA review
6.0	11/14/2017	CSRA/Maricom	Enterprise_Portal_User_Manual_v6 Replaced all instances of 'security questions' with 'challenge questions'as the terms had been interchangeably used Replaced images for the following figures due to UI changes: Figures 1, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 17, 21, 22, 30, 32, 34, 36, 38, 39, 40, 41, 43, 45, 47, 48, 49, 51, 53, 55, 58, 59, 62, 63, 64, 67, 69, 71, 73, 74, and 76

Appendix B: Acronyms

Table 2: Acronyms provides a literal translation of terms used in this document and related to the document.

Table 2: Acronyms

Acronym	Literal Translation
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
EIDM	Enterprise Identity Management
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
IE	Internet Explorer
IVR	Interactive Voice Response
MFA	Multi-Factor Authentication
OIT	Office of Information Technology
PHI	Personal Health Information
PII	Personally Identifiable Information
RIDP	Remote Identity Proofing
SMS	Short Message Service
UI	User Interface
VIP	Validation and ID Protection
VPN	Virtual Private Network
XLC	Expedited Life Cycle

Appendix C: Glossary

Table 3: Glossary defines the terms used in this document and related to the document.

Table 3: Glossary

Term	Definition
Centers for Medicare & Medicaid Services	A Federal agency within the United States HHS that administers the Medicare program and works in partnership with state governments to administer Medicaid, the State CHIP, and health insurance portability standards.
Department of Health and Human Services	A Cabinet department of the United States government with the goal of protecting the health of all Americans and providing essential human services.
Enterprise Identity Management	A CMS Enterprise shared service that will assign single identity to individuals and organizations to use to access CMS business applications, verify sufficient information to establish an individual's right to a claimed identity, assign credentials to the individual, and check those credentials during the user log in.
Enterprise User Administration	A system that CMS uses to manage enterprise user IDs and passwords. It provides centralized administration of user IDs on the entire enterprise including the mainframe systems, mid-tier devices such as Advanced Interactive Executive or Sun systems, network operating systems such as Netware or Windows, and database platforms such as Oracle, Sybase, and Microsoft SQL. The system utilizes online data to automate the approval process for access requests, and provides logging and auditing support.
Expedited Life Cycle	A streamlined development life cycle model, created by CMS, to guide and coordinate IT Projects.
Government Printing Office	An agency of the legislative branch that provides printing and binding services for Congress and the departments and establishments of the Federal government.
Identifier	A unique identifying set of characters assigned to a person or persons to ensure privacy and security on a computer system or network.
Multi-Factor Authentication	An approach to authentication which requires the presentation of two or more of the three authentication factors: a knowledge factor ("something the user knows"), a possession factor ("something the user has"), and an inherence factor ("something the user is").
Office of Information Technology	CMS governance role that serves as the Deputy to the CMS' Chief Information Officer and is responsible for providing implementation services and operational support for CMS component-specific information technology needs and enterprise-wide services. Plans, organizes, and coordinates the activities required to maintain an agency-wide information resources management program.

Term	Definition
Personal Health Information	Under HIPAA, any information about health status, provision of health care, or payment for health care that may link to a specific individual. The interpretation of this is broad and includes any part of a patient's medical record or payment history. PHI is also referred to as Protected Health Information.
Personally Identifiable Information	Information that identifies or describes an individual, including but not limited to name, address, telephone number, social security number, credit card number, and personal characteristics that make the individual's identity easily discoverable.
Remote Identity Proofing	An Enterprise Identity Management shared service that validates users of CMS network through a series of steps in order to grant access to an application.
Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d)	The section of the Federal law governing accessibility for disabled persons to the full range of electronic and information technologies (EIT) in the Federal sector, whenever agencies develop, procure, maintain, or use such EIT.
User Manual	A technical communication document that assists people using a particular system.
Virtual Private Network	A network set up for use by a limited number of individuals, such as employees of a company, operating over a large area. The network typically uses encryption to keep information secure.

Appendix D: Referenced Documents

Table 4: Referenced Documents lists the documents and standards that are applicable to the development of this document.

Table 4: Referenced Documents

Document Name	Document Location and/or URL	Issuance Date
CMS User Manual (UM) Template This document is a template with instructions for building a CMS UM.	Version 2.1 https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/XLC/Downloads/UserManual.docx	02/02/2015
Department of Health and Human Services (HHS) Section 508 These standards establish HHS Section 508 compliancy requirements that impact this document.	http://www.hhs.gov/web/508/	N/A
U.S. Government Printing Office (GPO) Style Manual The GPO is an agency of the legislative branch that provides printing and binding services for Congress and the departments and establishments of the Federal government.	http://www.gpo.gov/fdsys/pkg/GPO-STYLEMANUAL-2008/content-detail.html 30th Edition	09/16/2008

Appendix E: Approvals

The undersigned acknowledge that they have reviewed the User Manual and agree with the information presented within this document. Changes to this User Manual will be coordinated with, and approved by, the undersigned, or their designated representatives.

Table 5: Document Approval

Document Approved By	Date Approved
Name: Paul Benning, Government Task Leader and Records Officer, EDG	Date:
Name: Julia Fultz, Division Director, CMS/OIT/EDG/DDES	Date:
Name: Glenn Radcliffe, Technical Lead, CMS/OIT/EDG/DDES	Date:
Name: Ken Harvey, Program Manager, CSRA/Maricom	Date:
Name: Srinivasu Togari, Technical Manager, CSRA/Maricom	Date:
Name: Jennifer Jacobson, Quality Assurance Lead, CSRA/Maricom	Date: