Office of Hearings Case and Document Management System ("OH CDMS")

External Registration and User Access Manual

Version 2.0

February 21, 2021

CENTERS FOR MEDICARE & MEDICAID SERVICES

Table of Contents

List of Figures iii

List of Tables v

1. Introduction 1

1.1 Office of Hearings Case and Document Management System 1

1.2 CMS Salesforce Enterprise Integration Portal 1

1.3 CMS Identity Management System 1

1.4 Cautions & Warnings 2

1.4.1 Use of CMS IDM Accounts Are Reserved For Account Owner 2

1.4.2 CMS SEI Portal Differs From CMS IDM Portal 2

1.4.3 Account Identity Verification 2

1.4.4 Multi-Factor Authentication 2

1.4.5 Session Timeout 3

1.4.6 Password Timeframes 3

1.4.7 Annual Certification 3

1.5 Accessibility Standards 3

2. Getting Started 4

2.1 Computer Set-Up Considerations 4

2.2 User Access Considerations 4

3. Access CMS SEI Portal Sign In Page 5

4. Register for Secure CMS IDM Account 6

4.1 Personal Information 7

4.2 Contact Information 9

4.3 Credentials Information 10

4.4 Registration Confirmation 11

5. Request Access to Salesforce Application 12

5.1 Application Selection – Salesforce 13

5.2 Role Selection – Salesforce User 14

5.3 Remote Identity Proofing 15

5.3.1 RIDP Quick Tips 19
5.3.2 Manual Identity Proofing 20
5.4 Business Contact Information 21
5.5 Role Request Review 22

6. Access the Salesforce App Store 24
6.1 OH CDMS Application 27

7. Request OH CDMS Community User Role 30

8. Launch OH CDMS 34

9. Support 37
9.1 IDM Self Service 37
9.1.1 Contact Information Updates 38
9.1.2 MFA Options 38
9.1.3 CMS SEI Reference Materials for Other Self Service Activities 40
9.2 OH CDMS Help Desk 40

Appendix A: Acronyms 41

Appendix B: Record of Changes 42

List of Figures

Figure 1: CMS SEI Portal Sign In Page 5
Figure 2: CMS SEI Portal Sign In Page – New User Registration Button 6
Figure 3: CMS IDM Account – Information Status Bar 6
Figure 4: Sample Personal Information 7
Figure 5: CMS IDM Terms and Conditions 8
Figure 6: Sample Contact Information 9
Figure 7: Sample Credentials Information 10
Figure 8: Registration Confirmation Message 11
Figure 9: CMS SEI Portal Sign In Page 12
Figure 10: Access Denied Message 12
Figure 11: CMS IDM Self Service Landing Page 13
Figure 12: Select Application by Filtering 13
Figure 13: Select Application by Using Scroll Bar 14
Figure 14: Select Role – Salesforce User 14
Figure 15: Remote Identity Proofing Page 15
Figure 16: RIDP Terms and Conditions 16
Figure 17: RIDP Information Review 17
Figure 18: Sample RIDP Questions 18
Figure 19: Sample Business Contact Information 21
Figure 20: Role Request Review 22
Figure 21: Role Request Confirmation 22
Figure 22: Sample IDM Acknowledgement Email 23
Figure 23: Sample IDM Approval Email 23
Figure 24: CMS SEI Portal Sign In Page 24
Figure 25: Verification Code Request Page 24
Figure 26: Sample Verification Code Email 25
Figure 27: Verification Code Entry 26
Figure 28: CMS SEI App Launcher Page 26

Figure 29: CMS SEI App Store Page with OH CDMS Tile....27
Figure 30: CMS App Listing for OH CDMS – Application Details....28
Figure 31: CMS SEI App Store Page with Pop-Up Message....28
Figure 32: CMS App Listing for OH CDMS – Access Status Message....29
Figure 33: CMS App Listing for OH CDMS – Help Desk Information....29
Figure 34: Sample OH CDMS Community Registration Page....30
Figure 35: OH CDMS Requester Organization Type Drop-Down Menu....31
Figure 36: OH CDMS Hearing Officer Petitioner Type Drop-Down Menu....31
Figure 37: OH CDMS Organization Information Field....32
Figure 38: OH CDMS Community Registration Page – New Organization Fields....32
Figure 39: OH CDMS Community Registration Conformation....33
Figure 40: CMS SEI App Launcher page with Approved Apps....34
Figure 41: OH CDMS Community Rules of Behavior....35
Figure 42: OH CDMS Landing Page....36
Figure 43: CMS SEI App Launcher Page with Approved Apps and Avatar Options....37
Figure 44: CMS IDM Self Service Options....37
Figure 45: IDM Self Service – My Profile....38
Figure 46: Verification Code Request Page with Multiple MFA Options....39
Figure 47: Verification Code Request Page with Multiple MFA Options – Drop-Down Menu....39
Figure 48: CMS SEI Reference Materials....40

List of Tables

Table 1: Acronyms 41
Table 2: Record of Changes 42

1. Introduction

This user manual provides step-by-step instructions for new external users requesting access to the Office of Hearings Case and Document Management System ("OH CDMS") application through the Centers of Medicare & Medicaid Services (“CMS”) Salesforce Enterprise Integration (“SEI”) Portal.

1.1 Office of Hearings Case and Document Management System

The Office of Hearings Case and Document Management System (“OH CDMS”) is a web-based portal for parties to enter and maintain their cases and to correspond with the Office of Hearings ("OH"). OH supports three distinct administrative hearing functions:

- The **Provider Reimbursement Review Board** ("PRRB"): provider appeals of cost report audits and other final determinations per 42 C.F.R. § 405, Subpart R;
- The **Medicare Geographic Classification Review Board** ("MGCRB"): hospital applications to request geographic redesignation to an alternative payment area per 42 C.F.R. § 412, Subpart L; and
- The **CMS Hearing Officer**: diverse range of matters brought by healthcare institutions, insurance issuers, state Medicaid plans, organ procurement organizations, and other entities per various regulatory authorities.

Access to the various modules is granted as needed based on role. Access to specific cases is limited to the parties of each case and their representatives.

1.2 CMS Salesforce Enterprise Integration Portal

The CMS Salesforce Enterprise Integration (“SEI”) Portal (https://sei.cms.gov) is a single point of entry to numerous CMS applications on the Salesforce platform. The portal supports users’ role-based access and personalization to present each user with only relevant content and applications (e.g., OH CDMS). Registration is a multi-step process to obtain secure access to both the portal itself and to the specific application.

1.3 CMS Identity Management System

CMS created the Identity Management (“IDM”) System to provide Business Partners with a means to request and obtain a single User ID which they can use to access one or more CMS applications, including the Salesforce applications available through the SEI Portal. The IDM System uses a cloud-based distributed architecture that supports the needs of both legacy and new applications while providing an improved user experience on desktop and laptop computers as well as tablet and smartphone mobile devices.

CMS IDM governs access to CMS systems by managing the creation of user IDs and passwords, multi-factor authentication (“MFA”), and the assignment of roles within CMS applications. CMS IDM also supports end users to manage their profile and perform self-service functions such as recovering a forgotten user ID, resetting a forgotten or expired password, and unlocking an account.

1.4 Cautions & Warnings

1.4.1 Use of CMS IDM Accounts Are Reserved For Account Owner

The use of CMS IDM accounts are reserved for the account owner, meaning each individual user must create and use their own account within CMS IDM. Once created, these credentials serve as your electronic signature within the Agency. You will be held responsible for the consequences of unauthorized or illegal transactions.

Users that breach CMS IDM's Terms & Conditions may have their account suspended and/or realize adverse action up to and including legal prosecution. Examples of user agreement violations include users sharing their account with another individual or using screen scraping software. In such cases, the application's Tier 1 Help Desk, the individual responsible for approving the user's application role, or the CMS appointed Business Owner of the application will request that the user's account be suspended. Please note that users, through no fault of their own, may also be suspended if their identity has been stolen and their account is at risk of being accessed fraudulently.

Regardless of culpability, once an account has been suspended the user will lose access to CMS IDM, as well as all CMS applications that are accessed through CMS IDM. Only CMS IDM Tier 2 personnel can unsuspend an account. Users will be unsuspended once the reason for suspension has been fully mitigated.

1.4.2 CMS SEI Portal Differs From CMS IDM Portal

The CMS SEI Portal (https://sei.cms.gov) is specific to CMS Salesforce applications. The CMS IDM Portal (https://idm.cms.gov) is used to access other non-Salesforce applications, such as DSH or PS&R. Note that both portals require the establishment of a shared CMS IDM account (see Section 4). Also, the two Portal Sign In pages are very similar in their user interface; however, OH CDMS may only be accessed by logging in through the CMS SEI Portal.

1.4.3 Account Identity Verification

CMS uses Experian as the external authentication service provider for the identity verification process. Experian uses information from your credit report solely to help confirm your identity to avoid fraudulent access or transactions in your name. As a result, you may see an entry called a "soft inquiry" on your Experian credit report. Soft inquiries do not affect your credit score and do not incur any charges related to them. You may need access to your personal and credit report information as the Experian application will pose questions to you based on historical data in Experian's files. For additional information, please see the Experian Consumer Assistance website at http://www.experian.com/help.

1.4.4 Multi-Factor Authentication

Multi-Factor Authentication ("MFA") is a security mechanism that is implemented to provide an extra layer of security, through the use of a unique security code, in addition to the entry of a User ID and Password. Since OH CDMS is an MFA-protected application, the CMS IDM system requires registration of a phone or computer to obtain the necessary security code.

Multi-factor authentication defaults to the Email option upon initial set up. At each login, users will be prompted to obtain a current security code via email. The security code for the email option expires in 30 minutes. If you are unable to enter the code within the allotted period, you must request a new code.

Upon logging in to the CMS SEI Portal successfully, users will be able to add any of the other MFA options through a profile update within the IDM Self Service menu (see Section 9.1). Note that the email option cannot be removed, and it is the only option that will always remain on the profile. However, it is recommended that users select an additional MFA option in case email is experiencing a temporary delay.

1.4.5 Session Timeout

Session timeout occurs if a user does not perform any action within the CMS SEI Portal or OH CDMS for 30 minutes. A session pop-up message is displayed shortly before expiration allowing the user to stay logged in. If no activity by the end of the 30-minute timeframe, the session will automatically be terminated.

1.4.6 Password Timeframes

Your password must be changed at least every 60 days to remain an active user within the CMS SEI Portal and its associated systems and applications. Passwords can be changed only once every 24 hours.

1.4.7 Annual Certification

CMS security guidelines require an annual certification of a user's role. Annual Certification is typically performed in the same manner as the original role approval process used by Business Owners, their representatives, authorizers, Help Desks, or other approvers. If the continued use of a role is not approved, then the role will be removed from your profile.

1.5 Accessibility Standards

CMS is committed to making its electronic and information technologies accessible to people with disabilities. We strive to meet or exceed the requirements of Section 508 of the Rehabilitation Act (29 U.S.C. § 794d), as amended in 1998.

If any content or use of any features in the CMS SEI Portal cannot be accessed due to a disability, please contact our Section 508 Team via email at 508Feedback@cms.hhs.gov.

For more information on CMS Accessibility and Compliance with Section 508, see the CMS Accessibility & Nondiscrimination for Individuals with Disabilities Notice.

2. Getting Started

2.1 Computer 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 SEI Portal:

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

2.2 User Access Considerations

Six distinct steps are required to obtain access to OH CDMS:

1. Access the CMS SEI Portal Sign In page via https://sei.cms.gov. Section 3
2. Register for secure CMS IDM account. Section 4
3. Request access to Salesforce. Section 5
4. Access the Salesforce App Store. Section 6
5. Request OH CDMS communuty user role. Section 7
6. Launch OH CDMS. Section 8

3. Access CMS SEI Portal Sign In Page

Navigate to the CMS SEI Portal at https://sei.cms.gov. The CMS SEI Portal Sign In page is displayed.

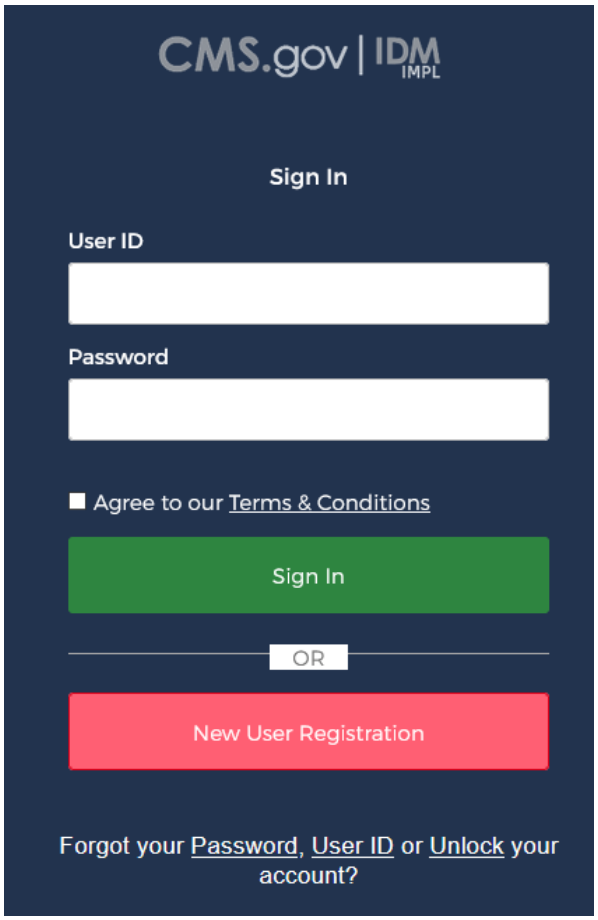


Figure 1: CMS SEI Portal Sign In Page

4. Register for Secure CMS IDM Account

If you have an existing CMS IDM account from another application, go to Section 5: Request Access to Salesforce Application.

1. To establish a new CMS IDM account, select the **New User Registration** button.

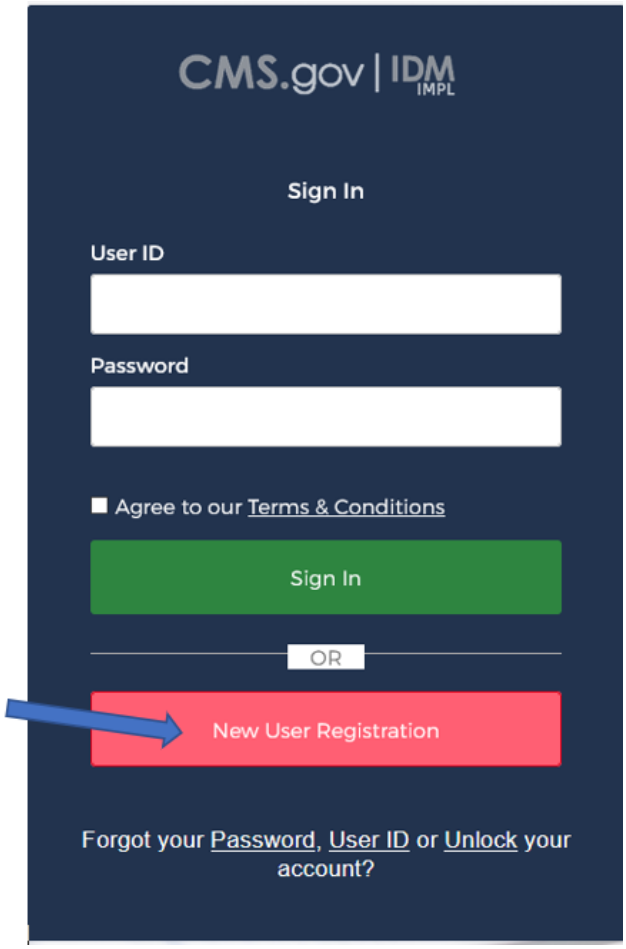


Figure 2: CMS SEI Portal Sign In Page – New User Registration Button

2. After clicking on the **New User Registration** button, you will see a status bar that indicates the three stages of information gathering: Personal, Contact, and Credentials. You must complete each section to fully establish your new user account.

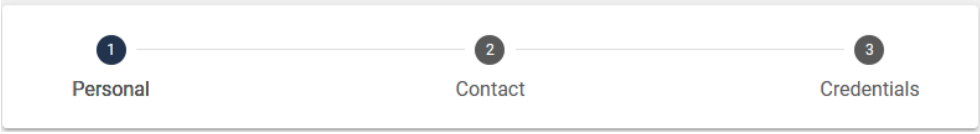


Figure 3: CMS IDM Account – Information Status Bar

Note: You may select **Cancel** at any time to exit out of the registration process. If you cancel, then any changes entered will not be saved.

4.1 Personal Information

1. Provide the personal information requested on the page. All fields are required and must be completed unless marked “Optional.”
    - First Name
    - Middle Name (Optional)
    - Last Name
    - Suffix (Optional)
    - Date of Birth
    - Email Address
    - Confirm Email

    Note: The Email Address and Confirm Email Address must match. Also, ensure that the email address is valid because the CMS IDM System uses email to communicate with users for many reasons including sign in, security, and self-service.

2. Select the **View Terms & Conditions** button. Read the page regarding Privacy, HHS Rules of Behavior, and Identity Verification. Select the **Close Terms & Conditions** button to return to the Personal information page.

3. Click the checkbox to acknowledge agreement with the terms and conditions, then select the **Next** button to continue.

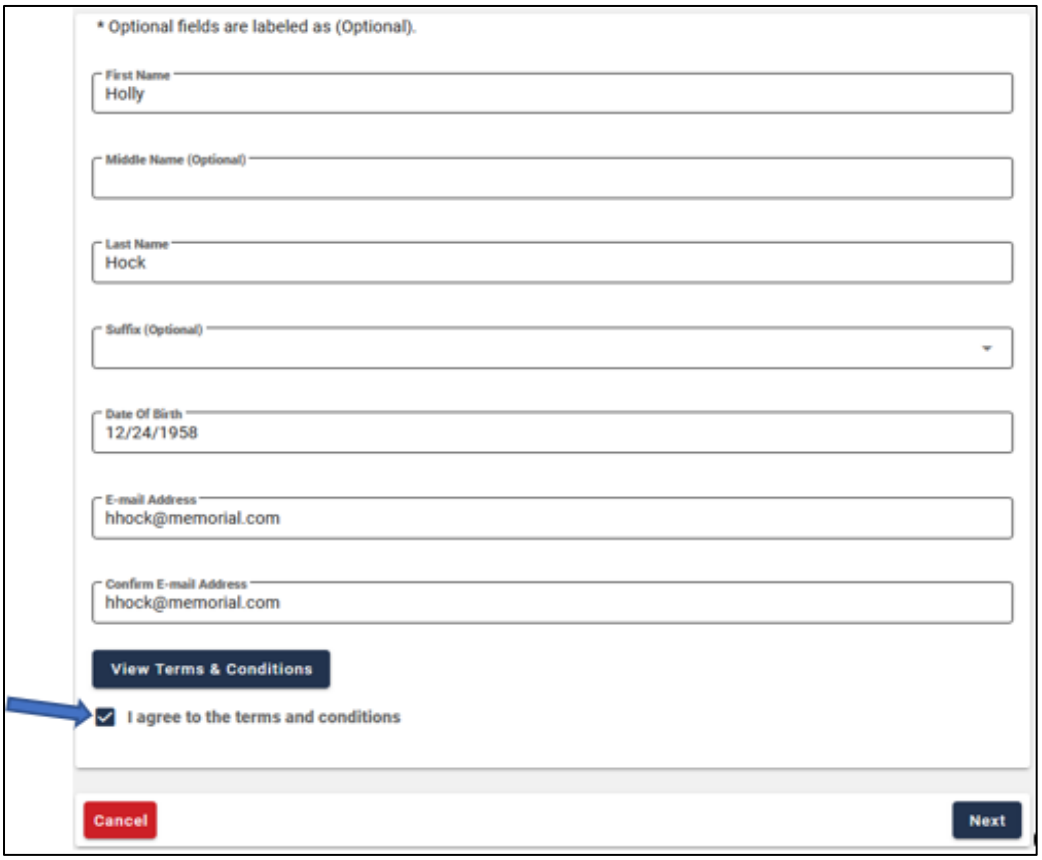


Figure 4: Sample Personal Information

Terms and Conditions

OMB No. 0938-1236 | Expiration Date: 04/30/2017 (OMB Re-Certification Pending) | Paperwork Reduction Act

Protecting Your Privacy CMS Privacy Act Statement

Protecting your Privacy is a top priority at CMS. We are committed to ensuring the security and confidentiality of the user registering to EIDM. Please read the CMS Privacy Act Statement which describes how we use the information you provide.

Personal information is described as data that is unique to an individual, such as a name, address, telephone number, Social Security Number, and date of birth (DOB). CMS is very aware of the privacy concerns around PII data. In fact, we share your concerns. We will only collect personal information to verify your identity. Your information will be disclosed to Experian, an external authentication service provider, to help us verify your identity. If collected, we will validate your Social Security Number with Experian only for the purposes of verifying your identity. Experian verifies the information you give us against their records. We may also use your answers to the challenge questions and other PII to later identify you in case you forget or misplace your User ID /Password.

HHS Rules of Behavior HHS Rules of Behavior

We encourage you to read the HHS Rules of Behavior, which provides the appropriate use of all HHS information technology resources for Department users, including Federal employees, contractors, and other system users.

I have read the HHS Rules of Behavior for Privileged User Accounts (addendum to the HHS Rules of Behavior (HHS RoB), document number HHS-OCIO-2013-0003S and dated July 24, 2013), and understand and agree to comply with its provisions. I understand that violations of the HHS Rules of Behavior for Privileged User Accounts or information security policies and standards may lead to disciplinary action and that these actions may include termination of employment; removal or disbarment from work on federal contracts or projects; revocation of access to federal information, information systems, and/or facilities; criminal penalties; and/or imprisonment. I understand that exceptions to the HHS Rules of Behavior for Privileged User Accounts must be authorized in advance in writing by the OpDiv Chief Information Officer or his/her designee. I also understand that violation of certain laws, such as the Privacy Act of 1974, copyright law, and 18 USC 2071, which the HHS Rules of Behavior for Privileged User Accounts draw upon, can result in monetary fines and/or criminal charges that may result in imprisonment.

Identity Verification

I understand that the identity proofing services being requested are regulated by the Fair Credit Reporting Act and that my explicit consent is required to use these services. I understand that any special procedures established by CMS for identity proofing using Experian have been met and the services requested by CMS to Experian will be used solely to confirm the applicant's identity to avoid fraudulent transactions in the applicant's name.

Close Terms & Conditions

Figure 5: CMS IDM Terms and Conditions

4.2 Contact Information

1. Provide the personal contact information requested on the page. All fields are required and must be completed unless marked “Optional.” Note that business contact inormation will be requested at a later step.

2. Select whether US Address or Foreign Address. US Addresses include those in the 50 U.S. states, the District of Columbia, and U.S. territories.

3. Enter Home Address, City, State, Zip Code, and Phone Number

4. Select the **Next** button to continue.

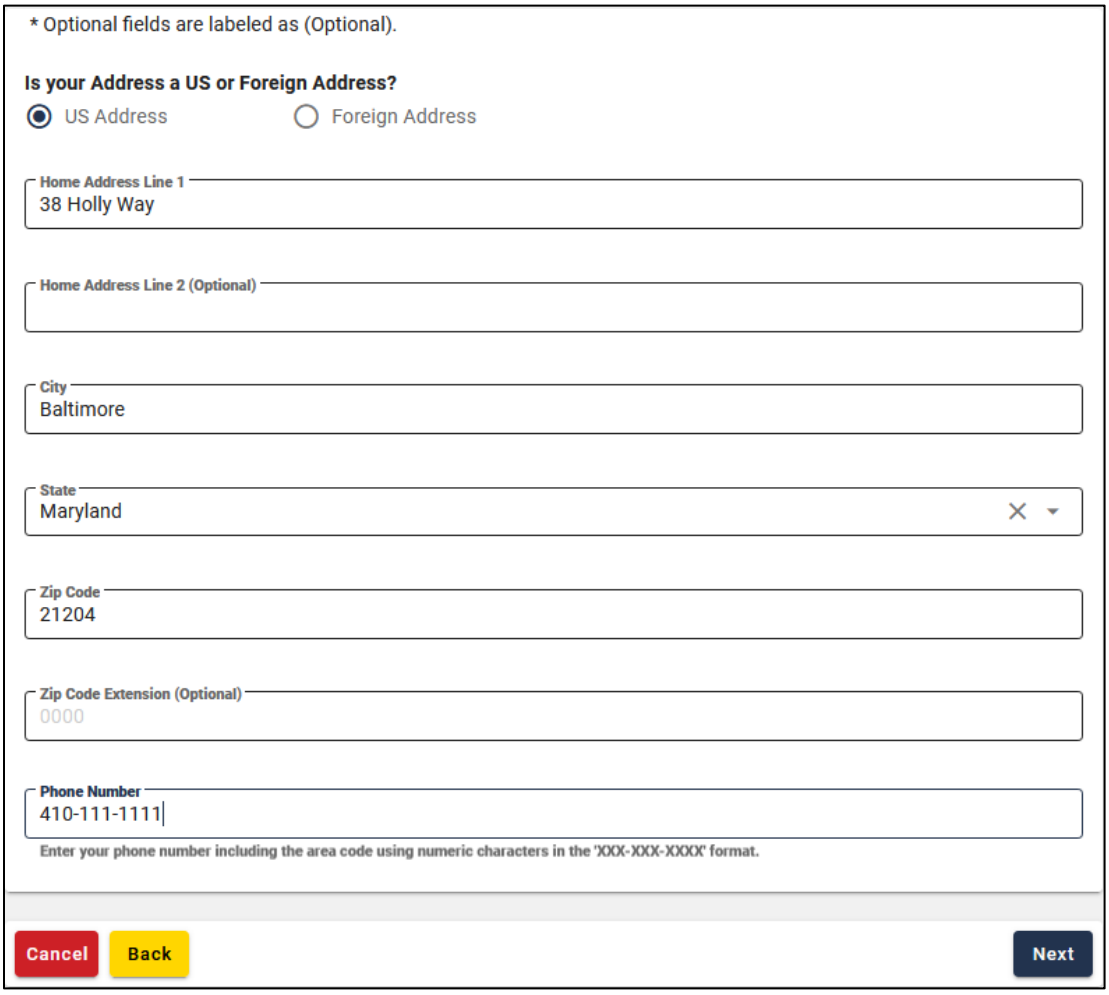


Figure 6: Sample Contact Information

4.3 Credentials Information

1. Provide the credentials information requested on the page. All fields are required and must be completed unless marked “Optional.”

2. Enter the desired User ID.

3. Enter the desired Password and Confirm Password. The Password and Confirm Password must match.

   CMS Password Guidelines:

   - Passwords must be at least 8 characters in length.
   - Passwords must include an uppercase letter.
   - Passwords must include a lowercase letter.
   - Passwords must include a number (0 - 9).
   - Passwords must include one of one special character.
   - Passwords must not contain a space.
   - Passwords must not be one of the user’s last 24 passwords.
   - Passwords must not contain parts of the user’s First Name, Last Name, or User ID.
   - 24 hours must have elapsed since the last password change.

4. Select a Security Question from the list.

5. Type the security question answer into the Answer dialog box.

6. Select the **Submit** button to continue.

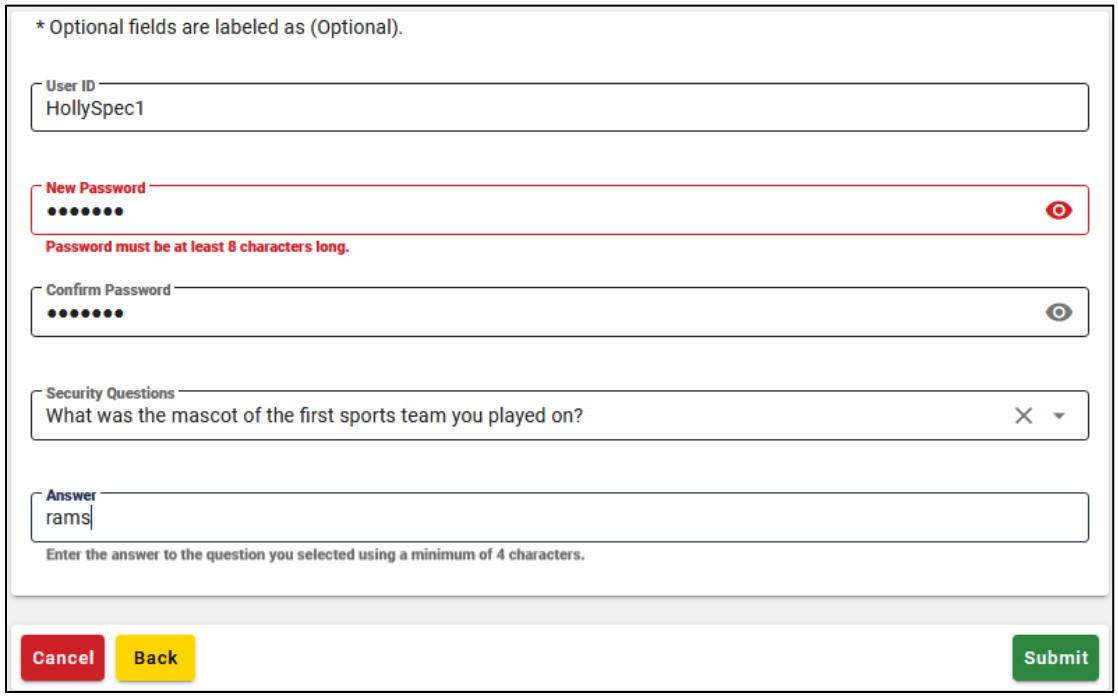


Figure 7: Sample Credentials Information

4.4 Registration Confirmation

1. Upon submission, the system will display a confirmation message that indicates the account was successfully created. Select the **Return** button to continue.

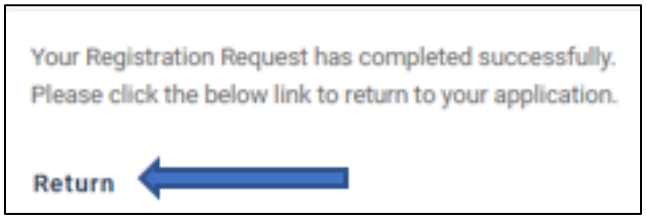


Figure 8: Registration Confirmation Message

2. The screen refreshes and the System Sign-In window appears.

5. Request Access to Salesforce Application

1. Sign in using the newly established credentials. Enter your valid User ID and Password and check the box to Agree to our Terms & Conditions. Select the **Sign In** button.

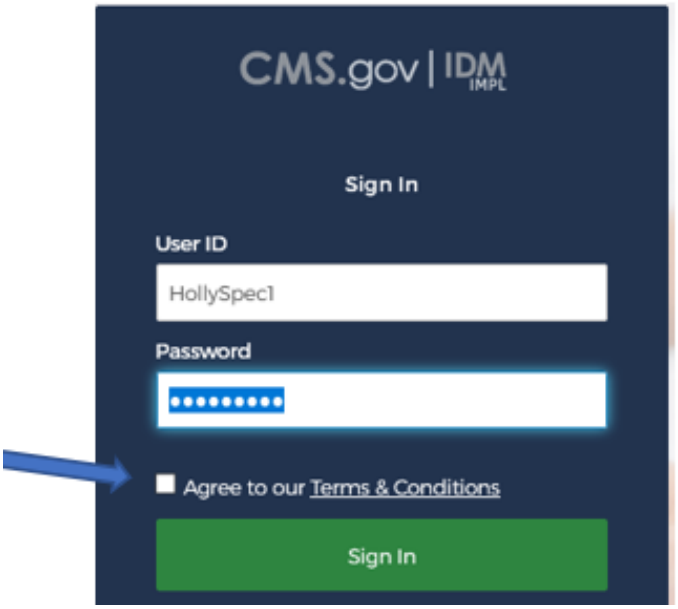


Figure 9: CMS SEI Portal Sign In Page

2. Upon login, you will initially be directed to an Access Denied window. Select the **Click here to request access to IDM** link as displayed on the screen below.

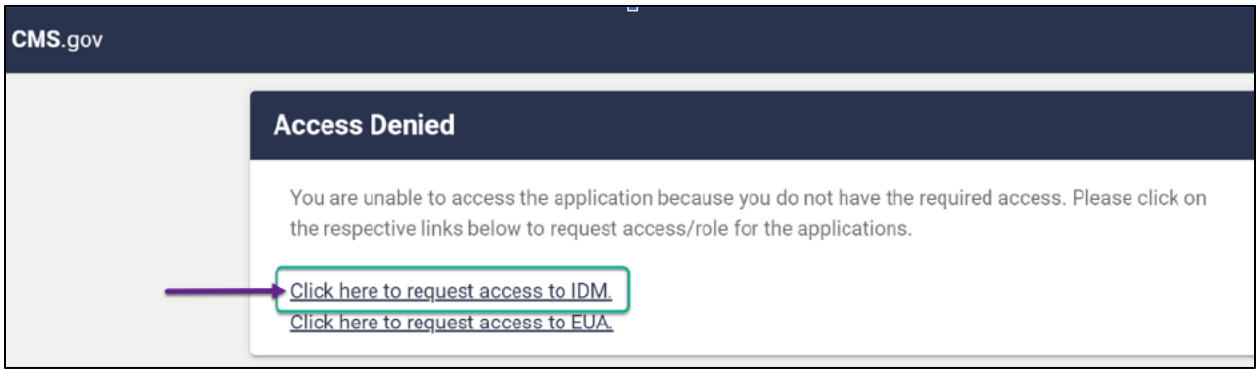


Figure 10: Access Denied Message

3. The self-service page will be displayed with four tiles.
    - My Profile
    - Role Request
    - Manage My Roles
    - My Requests

4. Select the **Role Request** tile.

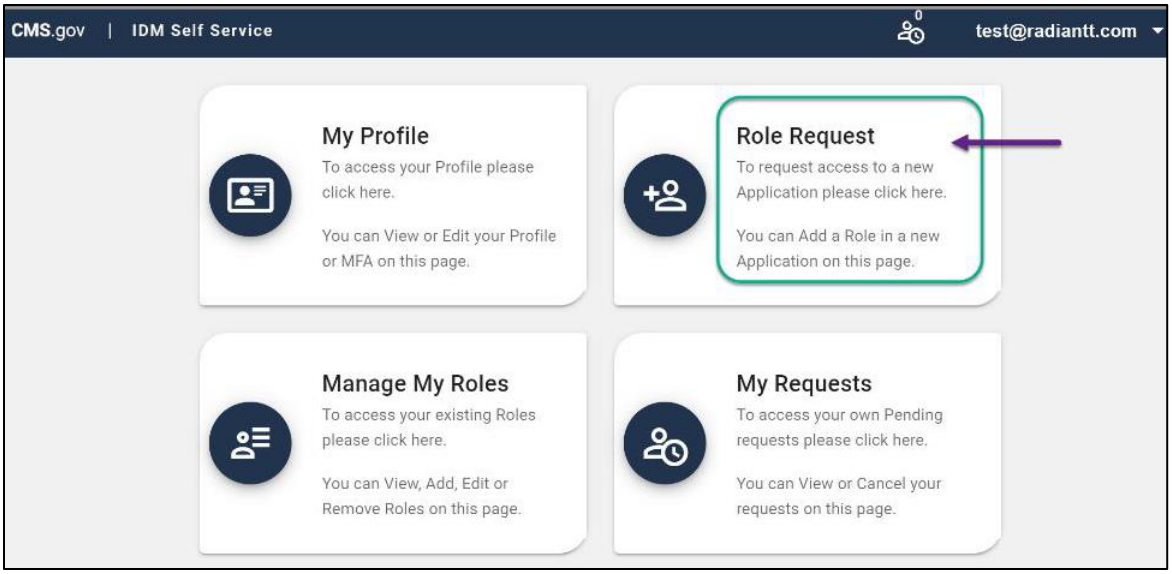


Figure 11: CMS IDM Self Service Landing Page

5.1 Application Selection – Salesforce

1. The **Role Request** page contains a drop-down list with a variety of CMS applications. There are two methods to select an application from the list.

    a. By filtering: Begin entering "**Sa**" in the **Select an Application** box.

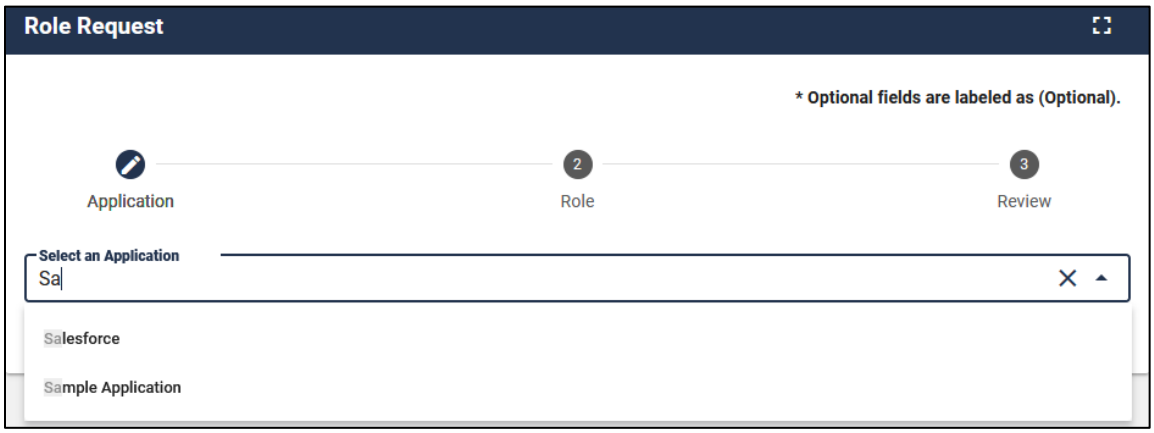


Figure 12: Select Application by Filtering

b. By using the scoll bar: Scroll down through the list until you see **Salesforce**.

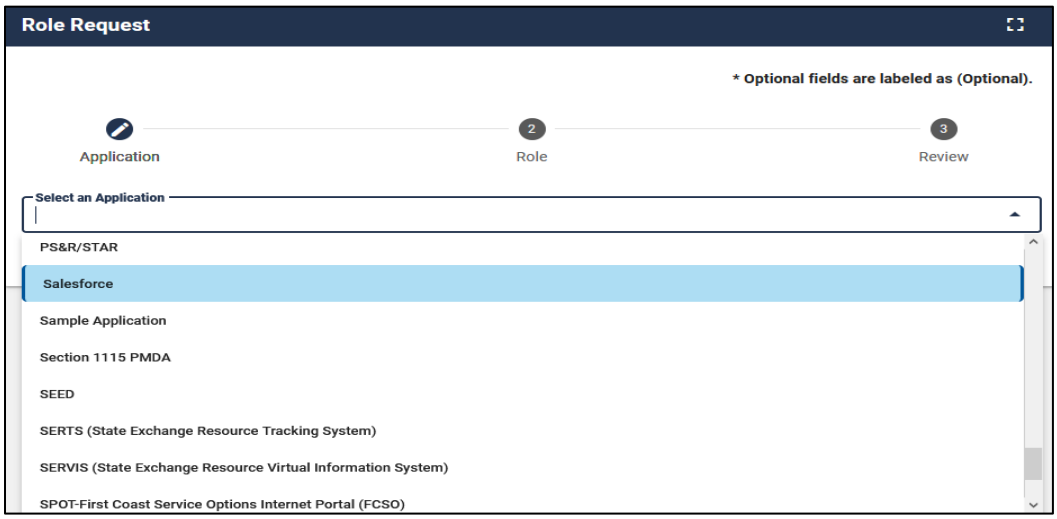


Figure 13: Select Application by Using Scroll Bar

2. Select **Salesforce** from the list.

5.2 Role Selection – Salesforce User

1. Select the **Salesforce user** role as displayed below. The other roles are for internal users to perform administrative and help desk functions.

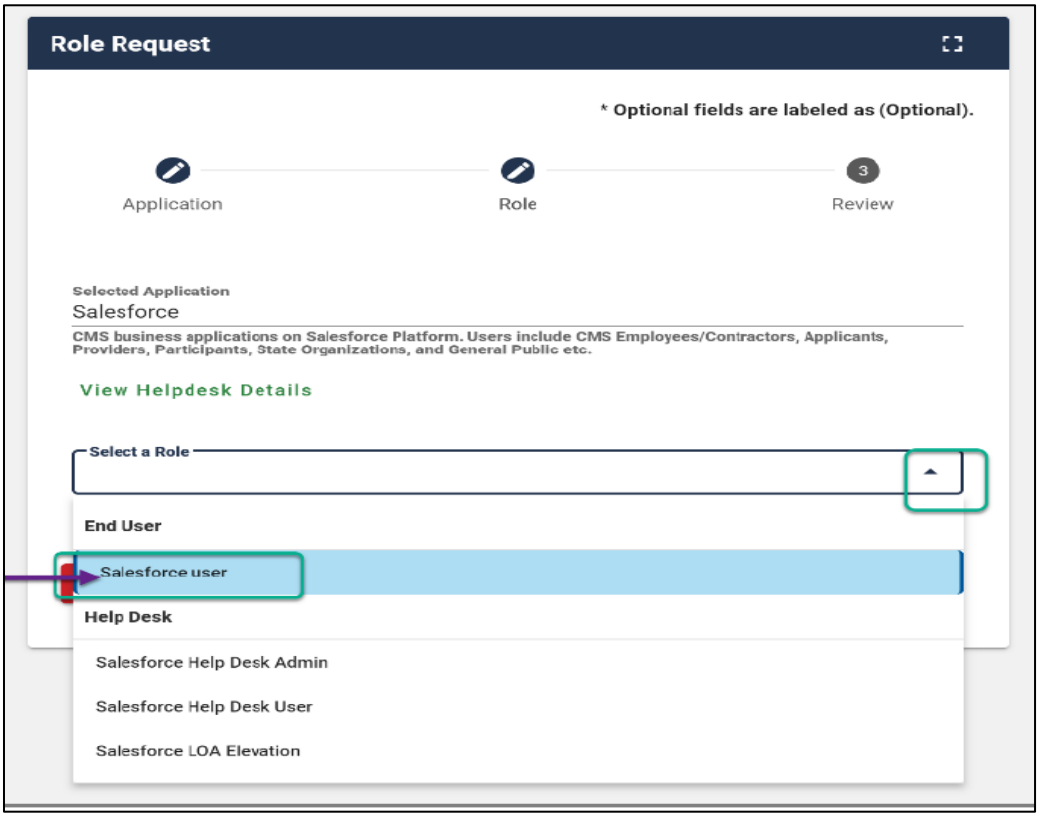


Figure 14: Select Role – Salesforce User

5.3 Remote Identity Proofing

1. Review the **Remote Identity Proofing** ("RIDP") background information. This process is used to verify user's identity and is done by asking relevant questions based on your personal and financial history. CMS uses Experian as the external authentication service provider

2. Select the **View Terms & Conditions** link to open the Terms & Conditions page. After reading, select the **Back** button to return to the RIDP page.

3. Select the **I agree to the Terms & Conditions** checkbox and select the **Next** button to continue.

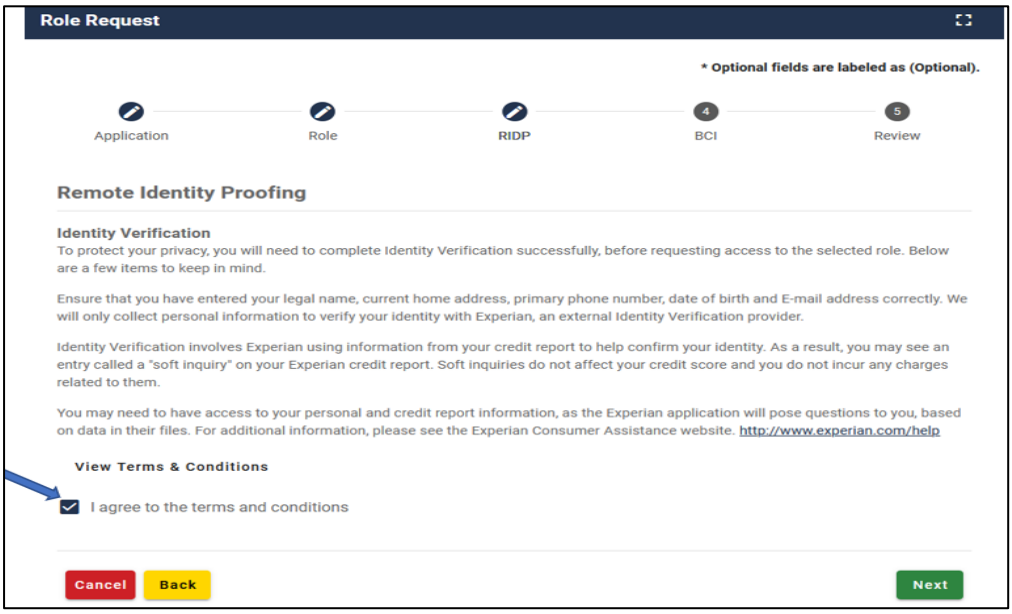


Figure 15: Remote Identity Proofing Page

Role Request

*** Optional fields are labeled as (Optional).**

Application | Role | RIDP | 4 BCI | 5 Review

Remote Identity Proofing

Terms and Conditions

OMB No. 0938-1236 | Expiration Date: 04/30/2017 (OMB Re-Certification Pending) | Paperwork Reduction Act

Protecting Your Privacy CMS Privacy Act Statement

Protecting your Privacy is a top priority at CMS. We are committed to ensuring the security and confidentiality of the user registering to EIDM. Please read the CMS Privacy Act Statement which describes how we use the information you provide.

Personal information is described as data that is unique to an individual, such as a name, address, telephone number, Social Security Number, and date of birth (DOB). CMS is very aware of the privacy concerns around PII data. In fact, we share your concerns. We will only collect personal information to verify your identity. Your information will be disclosed to Experian, an external authentication service provider, to help us verify your identity. If collected, we will validate your Social Security Number with Experian only for the purposes of verifying your identity. Experian verifies the information you give us against their records. We may also use your answers to the challenge questions and other PII to later identify you in case you forget or misplace your User ID /Password.

HHS Rules of Behavior HHS Rules of Behavior

We encourage you to read the HHS Rules of Behavior, which provides the appropriate use of all HHS information technology resources for Department users, including Federal employees, contractors, and other system users.

I have read the HHS Rules of Behavior for Privileged User Accounts (addendum to the HHS Rules of Behavior (HHS RoB), document number HHS-OCIO-2013-0003S and dated July 24, 2013), and understand and agree to comply with its provisions. I understand that violations of the HHS Rules of Behavior for Privileged User Accounts or information security policies and standards may lead to disciplinary action and that these actions may include termination of employment; removal or disbarment from work on federal contracts or projects; revocation of access to federal information, information systems, and/or facilities; criminal penalties; and/or imprisonment. I understand that exceptions to the HHS Rules of Behavior for Privileged User Accounts must be authorized in advance in writing by the OpDiv Chief Information Officer or his/her designee. I also understand that violation of certain laws, such as the Privacy Act of 1974, copyright law, and 18 USC 2071, which the HHS Rules of Behavior for Privileged User Accounts draw upon, can result in monetary fines and/or criminal charges that may result in imprisonment.

Identity Verification

I understand that the identity proofing services being requested are regulated by the Fair Credit Reporting Act and that my explicit consent is required to use these services. I understand that any special procedures established by CMS for identity proofing using Experian have been met and the services requested by CMS to Experian will be used solely to confirm the applicant's identity to avoid fraudulent transactions in the applicant's name.

Back

Figure 16: RIDP Terms and Conditions

4. The **Role Request** form is displayed. The user's previously entered personal and contact information is populated for confirmation.

5. Complete all remaining fields unless marked as optional, including Social Security Number and Confirm Email Address.

6. After all required information has been completed, select the **Next** button to continue.

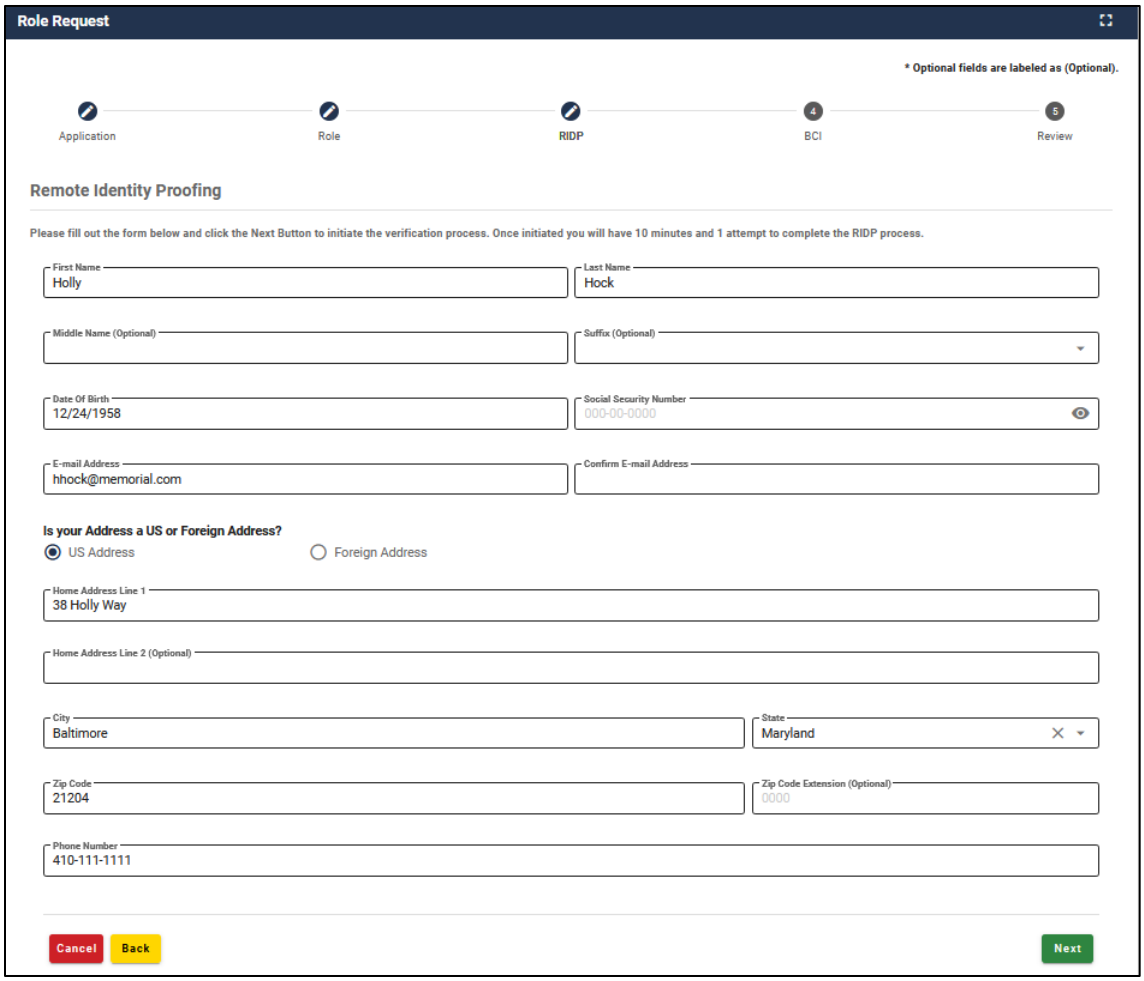


Figure 17: RIDP Information Review

7. the **Verify Identity** page is displayed. You are required to answer five questions about information that may be in your personal or financial records. Select the **Next** button to submit the request.

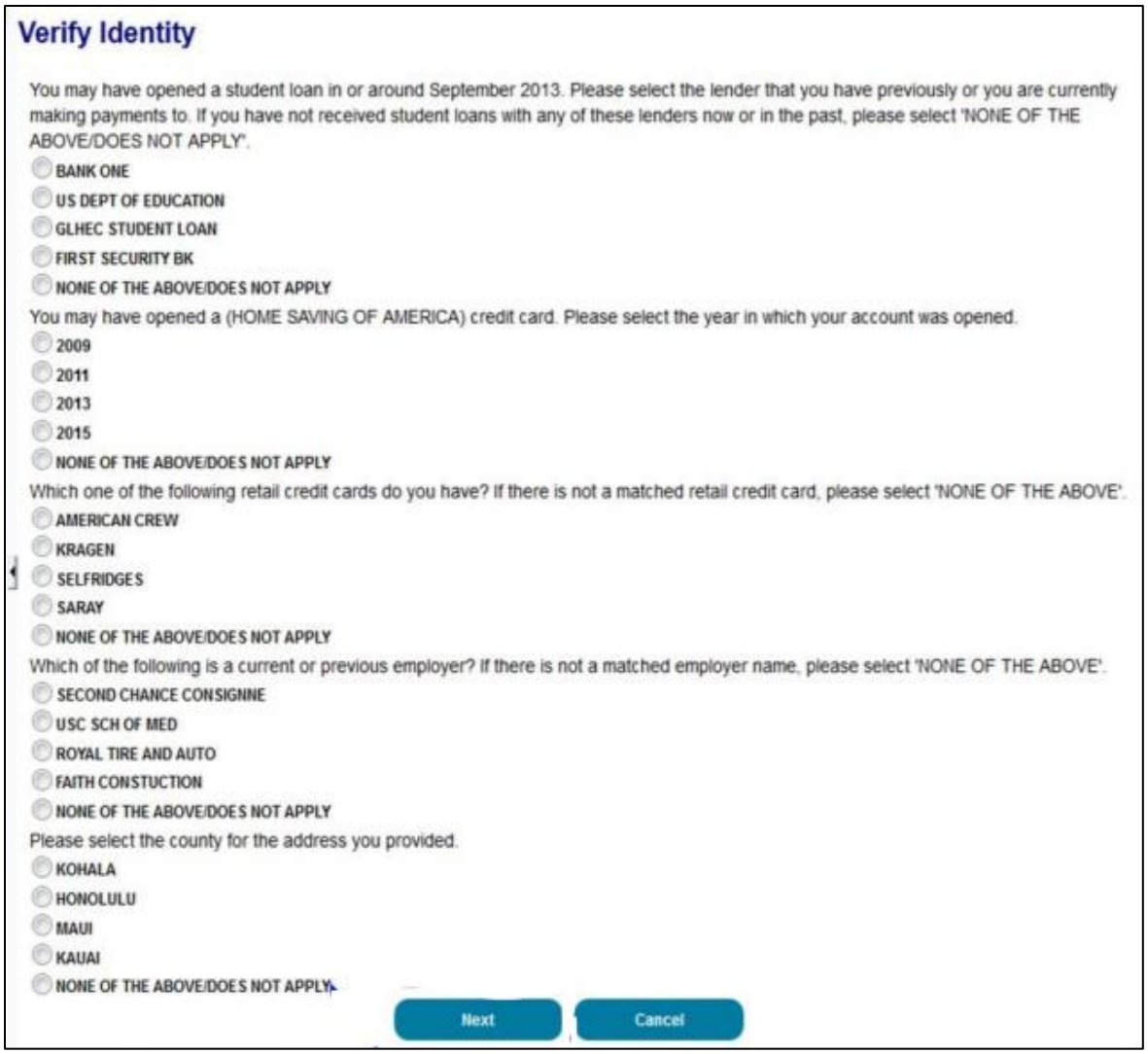


Figure 18: Sample RIDP Questions

5.3.1 RIDP Quick Tips

Provided below are RIDP quick tips for success and additional guidance regarding some of the challenges users may encounter while attempting to complete RIDP online.

During the RIDP process, you will be asked to provide a set of core credentials, which include:

Full Legal Name

- ✓ You must use your full legal name as listed on your Driver's License or financial account information.
- ✓ Your surname must match the surname Experian has for you on file.
- ✓ Do not use nicknames.
- ✓ If you have a two-part name, enter the second part in the middle name field. (*i.e.*, Billy Bob would have Billy in the first name field and Bob in the middle name field).

Social Security Number

- ✓ Ensure that Social Security Number field is filled in correctly. Users can review and edit these fields prior to sending the information to Experian.

Current Residential Address

- ✓ Ensure your personal/residential/home address is used:
  - Where you receive financial statements (i.e., Credit cards and/or utility bills).
  - Consistently used for billing purposes.
  - Associated with your credit report.
- ✓ Do not use your business address.
- ✓ If you have a recent change in address, try to identity proof with a prior address.
- ✓ Do not enter any extraneous symbols in the address field. If you want to confirm the correct format, visit USPS Look up a Zip Code.

Date of Birth

- ✓ Ensure that the Date of Birth field is entered accurately. Users can review and edit this field prior to sending the information to Experian.

Personal Phone Number

- ✓ Enter a personal landline phone number (if you have one).
- ✓ A cell phone can be used, but a residential landline is preferred.

Users may attempt online RIDP six times in an 18-hour period. If a user continues to encounter problems with RIDP, the IDM system will prompt the user to contact Experian Support Services via phone to resolve any issues. The Experian Identity Verification Service will use the individual's core credentials to locate personal information in Experian and generate a set of questions, referred to as "Out-of-Wallet" questions. Experian will attempt to verify the

individual's identity to the appropriate level of assurance with the information provided. Upon successful completion of RIDP phone proofing with Experian, the user can proceed with the IDM registration.

Out-of-Wallet Questions

- ✓ You will be asked a series of questions regarding your personal financial transactions/information.
- ✓ Try to collect all necessary information before attempting the session.
- ✓ Download a free copy of your credit report at Annual Credit Report.

Consent

- ✓ You will be asked to provide consent to verify your identity information from your credit report.
- ✓ The information is used only for purposes of identity proofing – "you are who you say you are."
- ✓ The consent of using the information does post as a soft inquiry on your credit report. The soft inquiry is visible only to you.
- ✓ The consent/inquiry does not affect your credit score.

Exclusions

- ✓ If you have a Victim's Statement or a blocked or frozen file, you will NOT be able to complete the identity proofing process online. After attempting online, you will be directed to call Experian's Consumer Services at **1-866-578-5409** to have the alert temporarily lifted so that you can attempt the identity proofing process.
- ✓ If you are listed as deceased on the Social Security Administration's (SSA) Death Master File, you will NOT be able to complete the identity proofing process online. You may contact the SSA at **1-800-269-0271**. They will be able to make sure that your information is being reported correctly.
- ✓ Telephone based proofing can only be used one time. If the user fails phone proofing, Experian will not be able to assist users who call back with the same reference number or call a different Experian call center phone number.

5.3.2 Manual Identity Proofing

If users are unable to complete the RIDP process online or with assistance from Experian's Consumer Services, contact the Help Desk for an alternative Manual Identity Proofing ("MIDP") process. See Help Desk at Section 9.2.

5.4 Business Contact Information

1. Provide the business contact information ("BCI") requested on the page. All fields are required and must be completed unless marked "Optional."

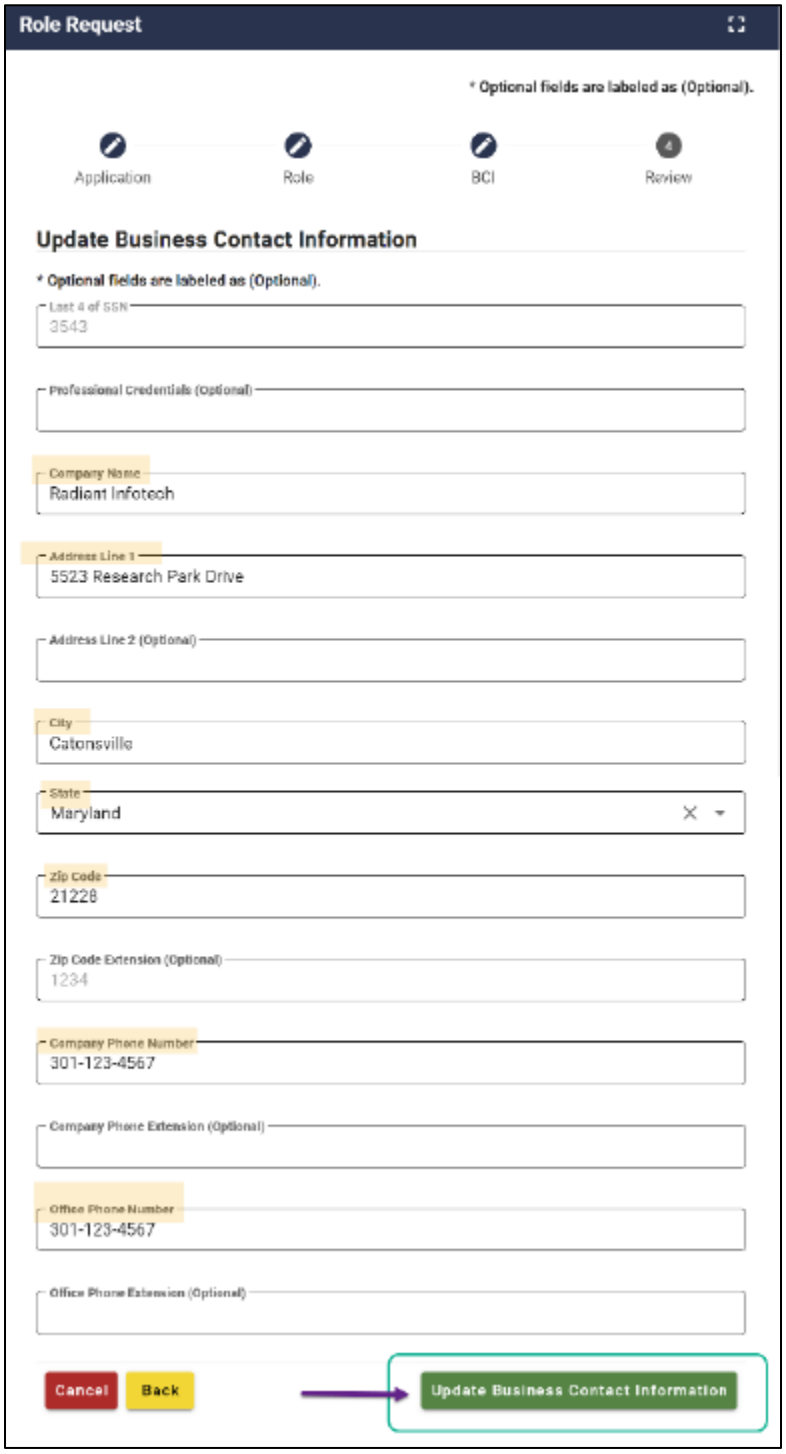


Figure 19: Sample Business Contact Information

2. Once Business Contact Information is complete, select the **Update Business Contact Information** button to continue.

5.5 Role Request Review

1. A **Review** page will be displayed. Provide a brief explanation in the **Reason for Request** field. The Salesforce application should be identified as OH CDMS.

2. Select the **Submit Role Request** button to continue.

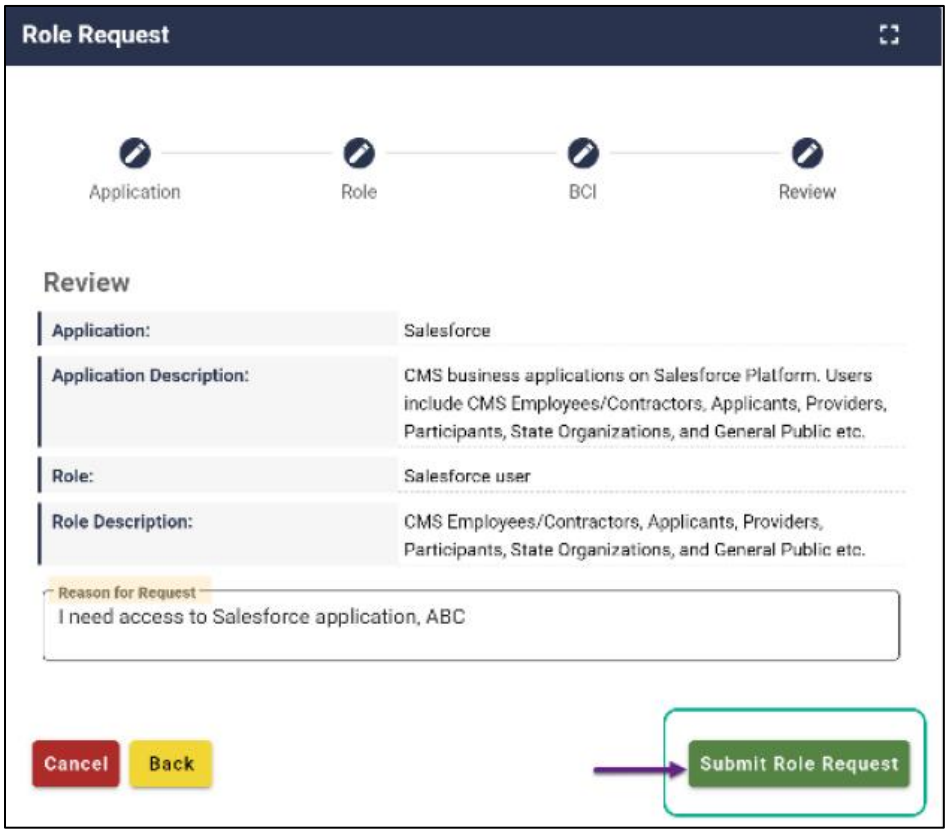


Figure 20: Role Request Review

3. A system message confirming your role request as a Salesforce user is displayed with an auto-generated Request ID. Select the **Back to Home** button to continue.

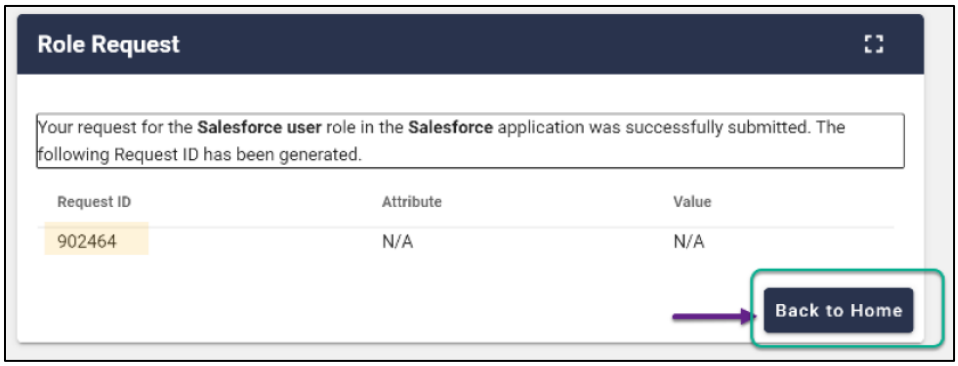
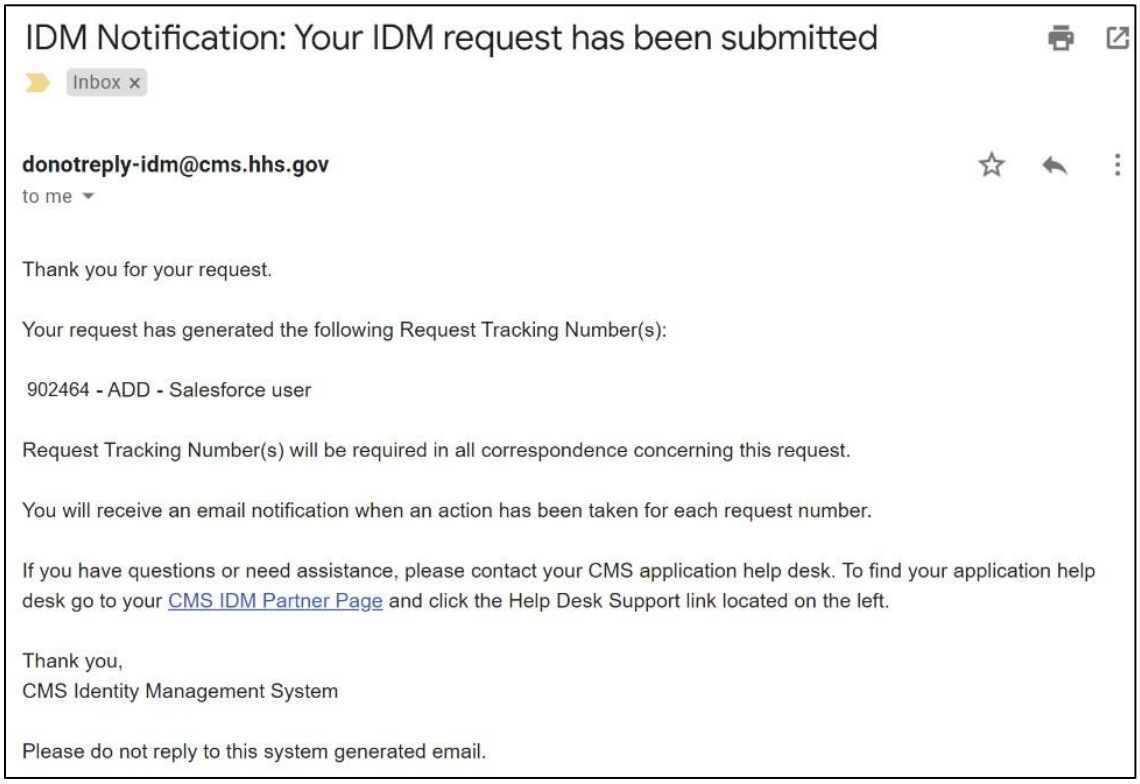


Figure 21: Role Request Confirmation

4. You will receive an email confirmation for the submitted request and upon approval of your role request.



IDM Notification: Your IDM request has been submitted

Inbox ×

donotreply-idm@cms.hhs.gov
to me

Thank you for your request.

Your request has generated the following Request Tracking Number(s):

902464 - ADD - Salesforce user

Request Tracking Number(s) will be required in all correspondence concerning this request.

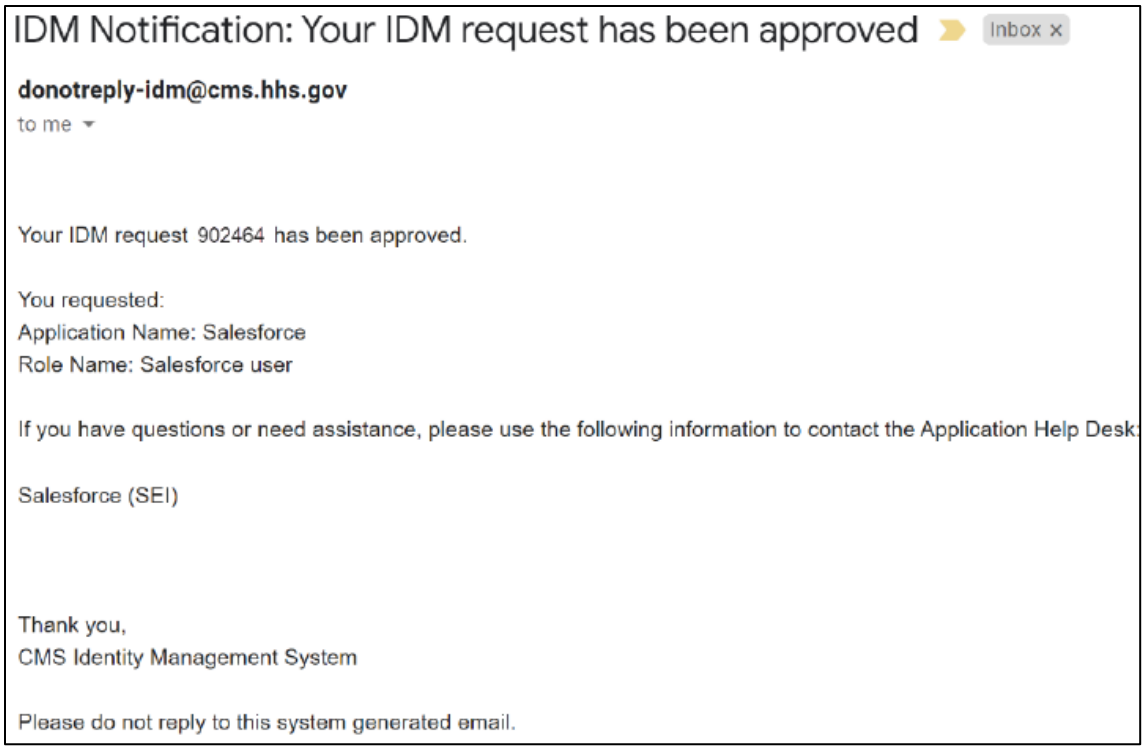
You will receive an email notification when an action has been taken for each request number.

If you have questions or need assistance, please contact your CMS application help desk. To find your application help desk go to your CMS IDM Partner Page and click the Help Desk Support link located on the left.

Thank you,
CMS Identity Management System

Please do not reply to this system generated email.

Figure 22: Sample IDM Acknowledgement Email



IDM Notification: Your IDM request has been approved Inbox ×

donotreply-idm@cms.hhs.gov
to me

Your IDM request 902464 has been approved.

You requested:
Application Name: Salesforce
Role Name: Salesforce user

If you have questions or need assistance, please use the following information to contact the Application Help Desk:

Salesforce (SEI)

Thank you,
CMS Identity Management System

Please do not reply to this system generated email.

Figure 23: Sample IDM Approval Email

6. Access the Salesforce App Store

Upon approval of the Salesforce User role request, the user will be able to access the App Store from the CMS SEI Portal. The App Store provides a list of available CMS Salesforce applications.

1. Log in to the CMS SEI Portal, making sure to select the check box to agree to terms & conditions.

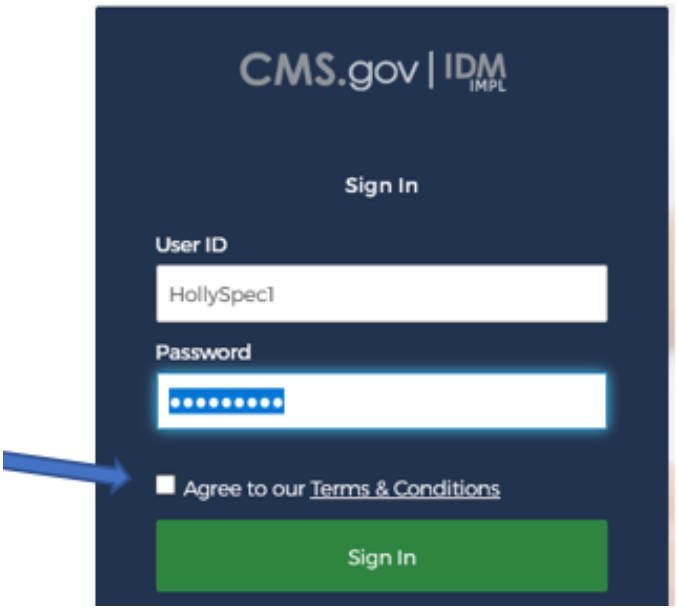


Figure 24: CMS SEI Portal Sign In Page

2. The system requires a verification code. Click the **Send me the code** button to have a verification code generated.

Figure 25: Verification Code Request Page

Note: Multi-factor authentication defaults to the Email option upon initial set up. To change the option, you will need to use the IDM Self Service component of the portal (see Section 9.1). Once you update your MFA Device for more than one option, all devices set up will be displayed in a drop-down list.

3. Open the email received.

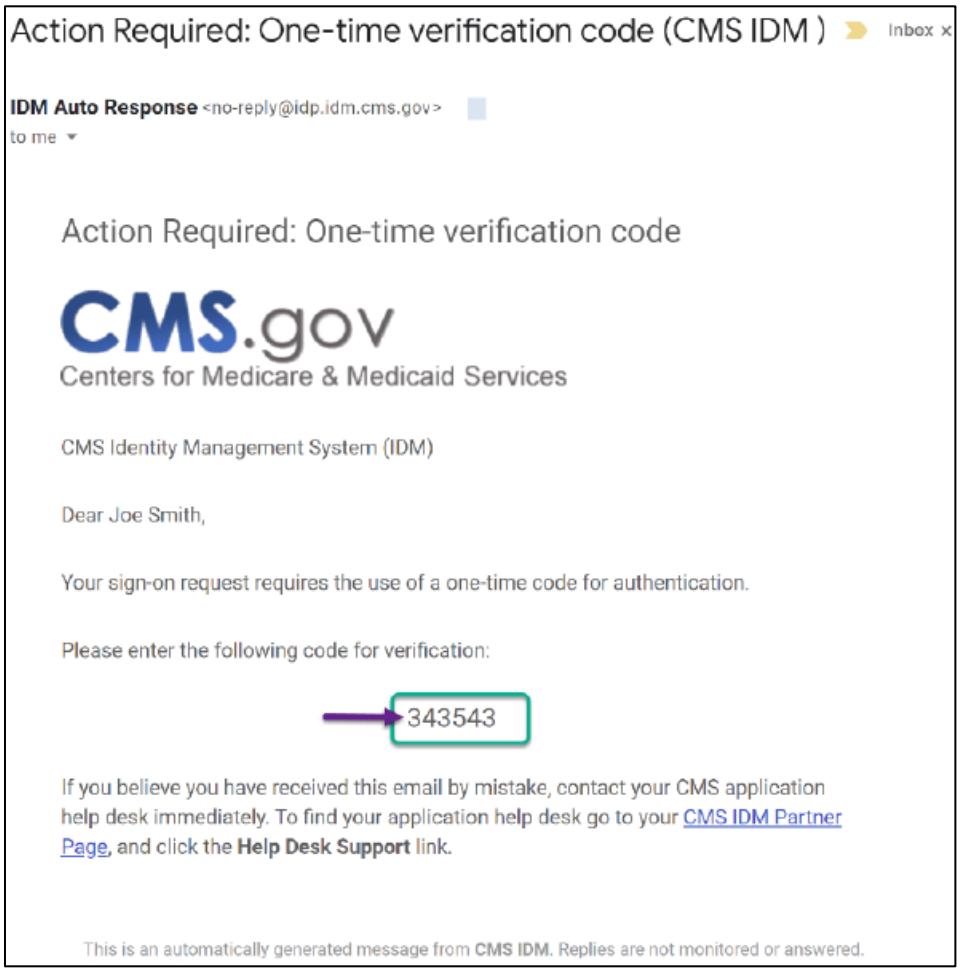


Figure 26: Sample Verification Code Email

4. Enter the 6-digit code from the email into the **Verification code** box and select the **Verify** button.

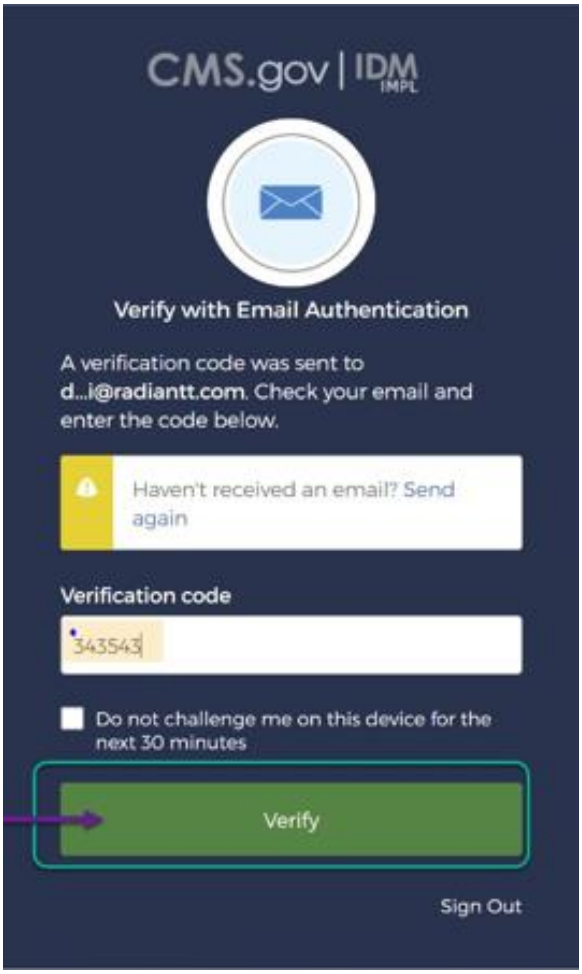


Figure 27: Verification Code Entry

5. The **App Launcher** page is displayed. No applications will be listed here until a selection is made.

6. Click on the **App Store** button to view the available CMS Salesforce applications.

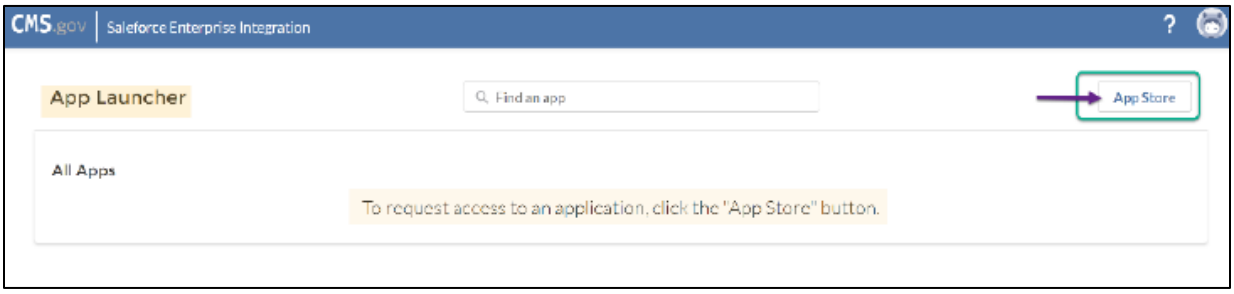


Figure 28: CMS SEI App Launcher Page

6.1 OH CDMS Application

1. Click on the **OH CDMS** tile.

   Note: If the OH CDMS tile is not located in the All Apps listing as shown in the image below, users can locate the tile by: (1) typing "**OH**" into the **Find an app** field; (2) selecting the **CHAMP (OHI)** filter in the Categries menu on the left; or (3) scrolling through the menu of applications.

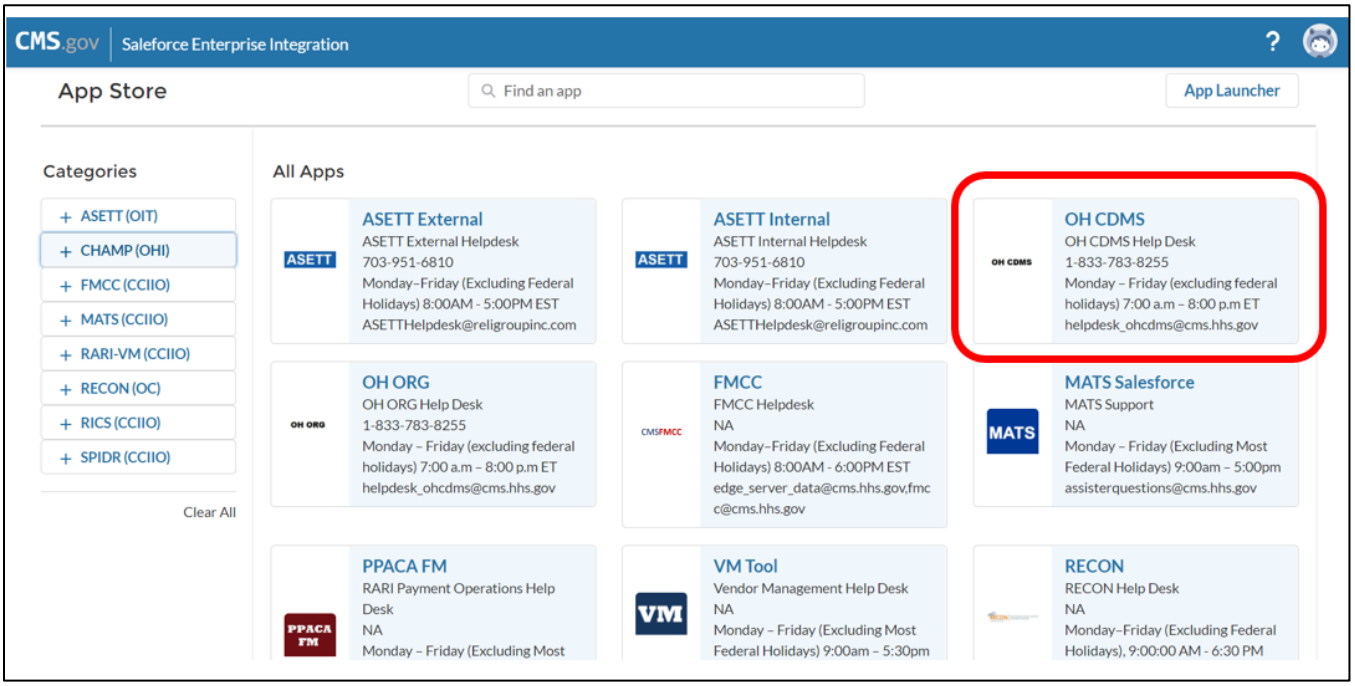


Figure 29: CMS SEI App Store Page with OH CDMS Tile

2. The **CMS App Listing** page is displayed for the OH CDMS Application. In the **Comments** field, enter a brief reason why you are requesting access to OH CDMS and select the **Send Request** button.

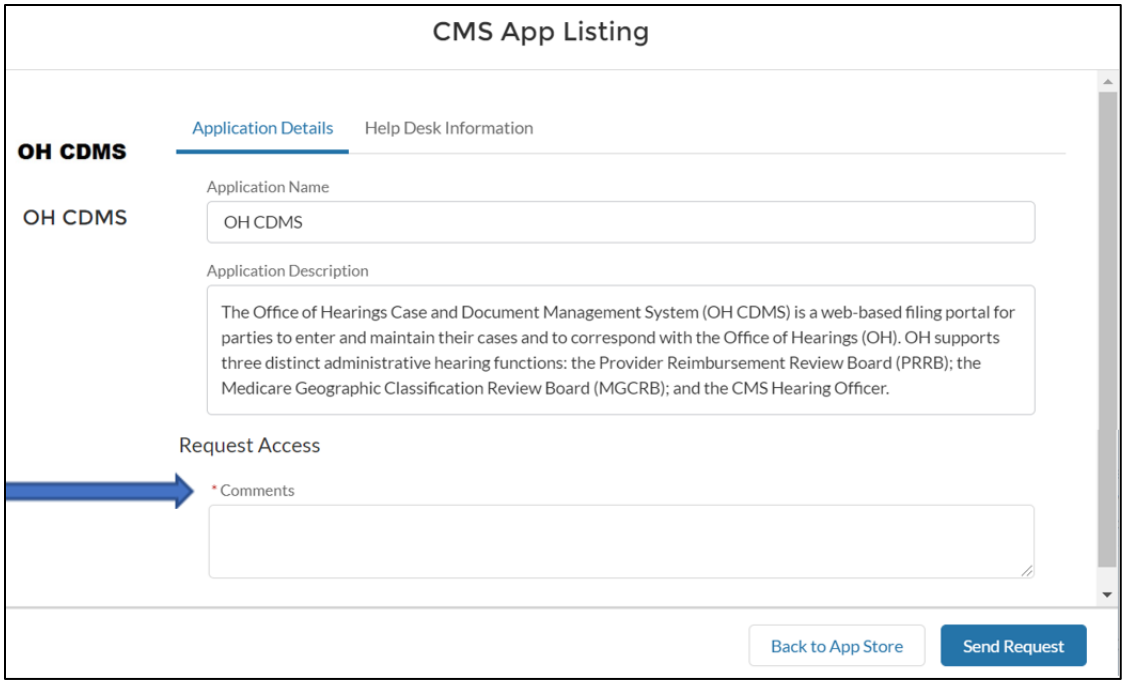


Figure 30: CMS App Listing for OH CDMS – Application Details

3. A confirmation message is displayed letting the user know that the access request has been submitted for review. A Request Confirmation Number is also auto-generated. Click on the X in the box to close the message.

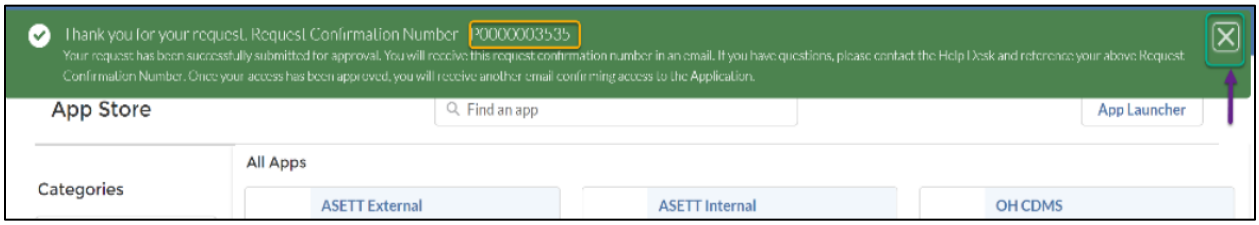


Figure 31: CMS SEI App Store Page with Pop-Up Message

4. The CMS App Listing opens displaying information about the access request status. Note that the Send Request button is no longer available after the request is submitted for review to the Component Org. If the user wants to inquire about the request or has a question, you may contact the **Application Help Desk**. Information for the Help Desk is available in the second tab of the same window.

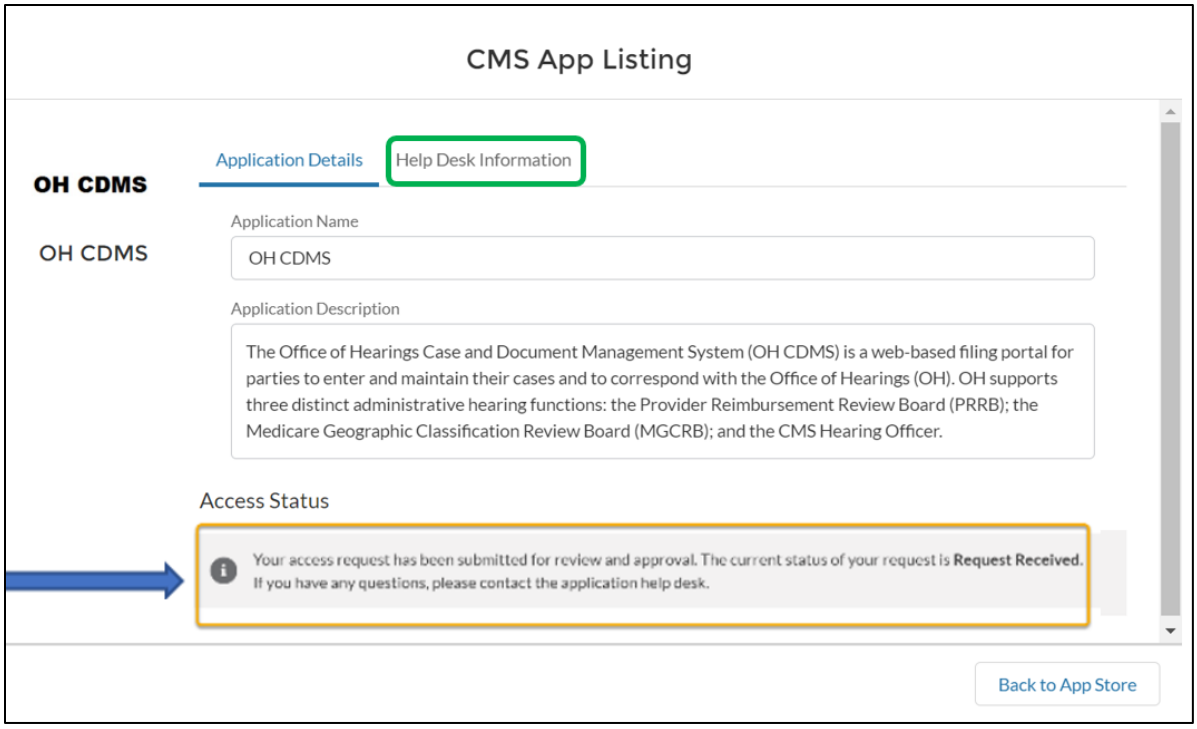


Figure 32: CMS App Listing for OH CDMS – Access Status Message

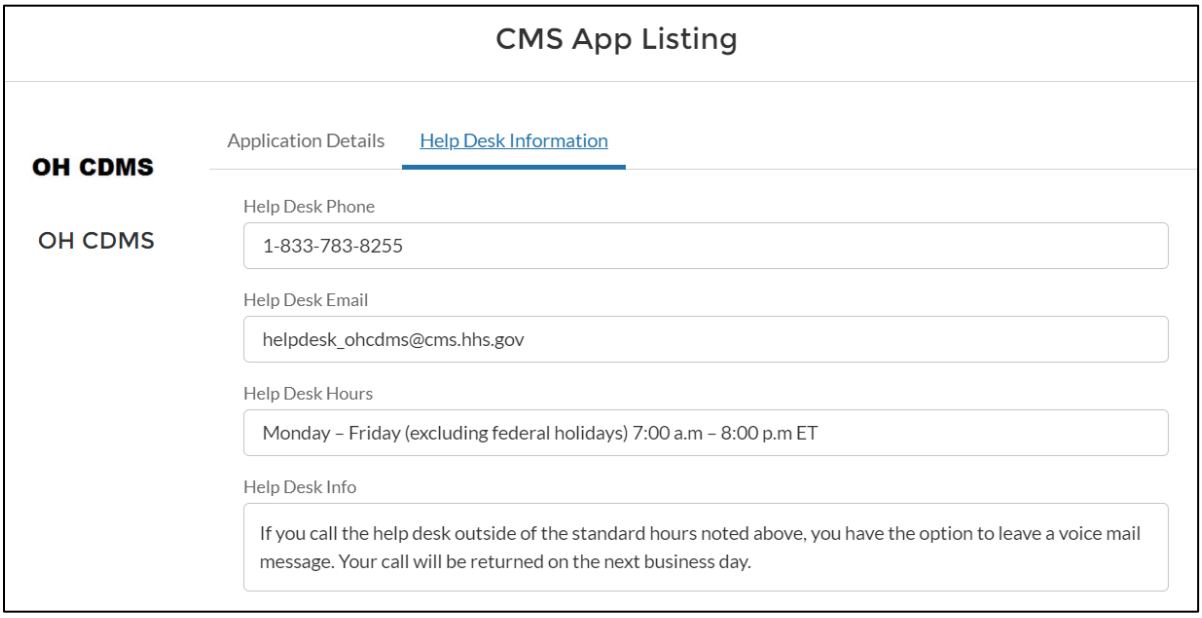


Figure 33: CMS App Listing for OH CDMS – Help Desk Information

7. Request OH CDMS Community User Role

Upon successfully completing the request for the OH CDMS App from the Salesforce App Store, the OH CDMS Community Registration page is displayed.

1. Enter text into the fields and make selections from drop-down menus as requested. This information is specific to OH CDMS and is the manner with which the PRRB, MGCRB, and/or CMS Hearing Officer will correspond with you regarding your cases.

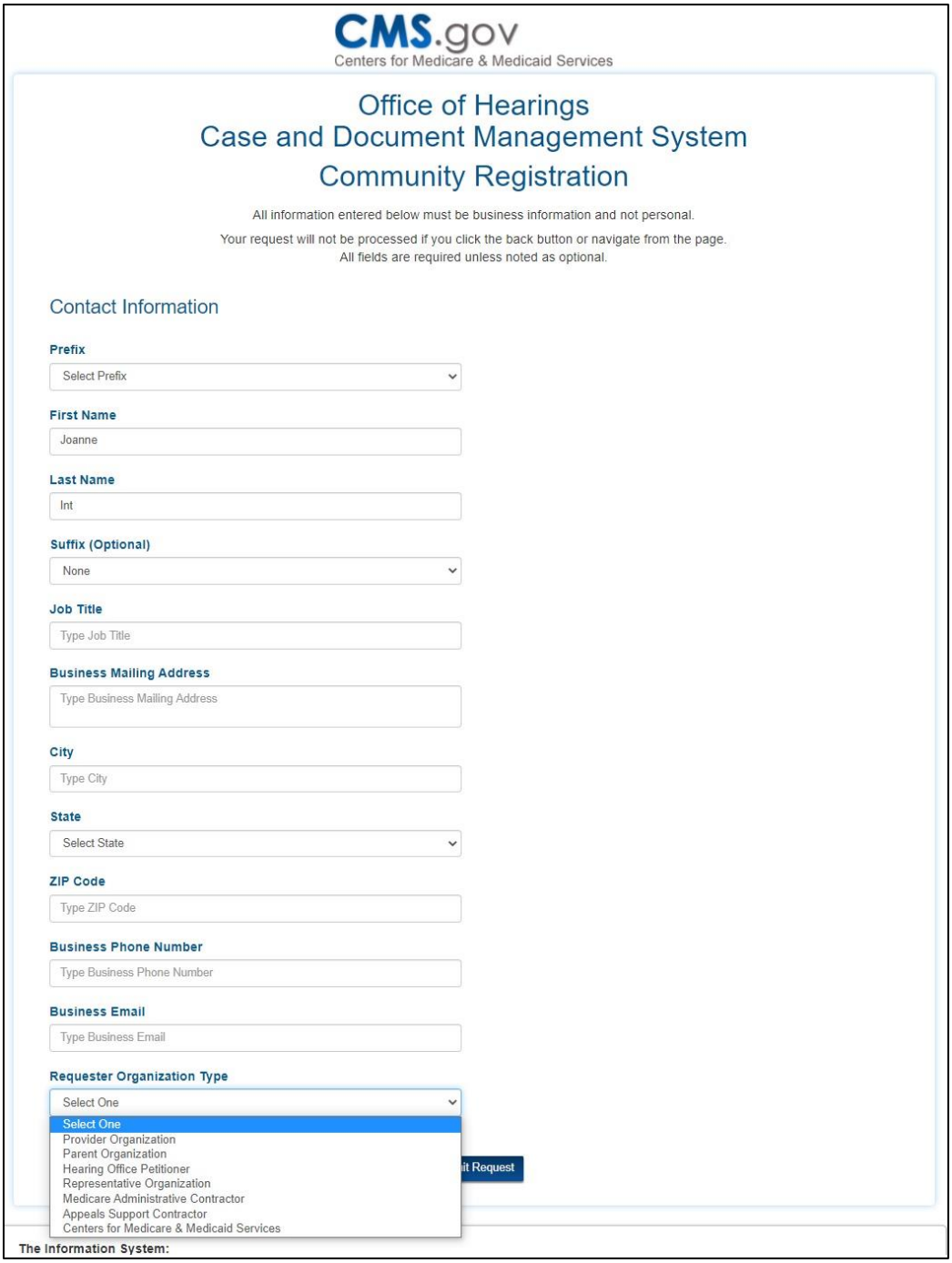


Figure 34: Sample OH CDMS Community Registration Page

2. Select the desired user role from the **Requester Organization Type** drop-down menu.

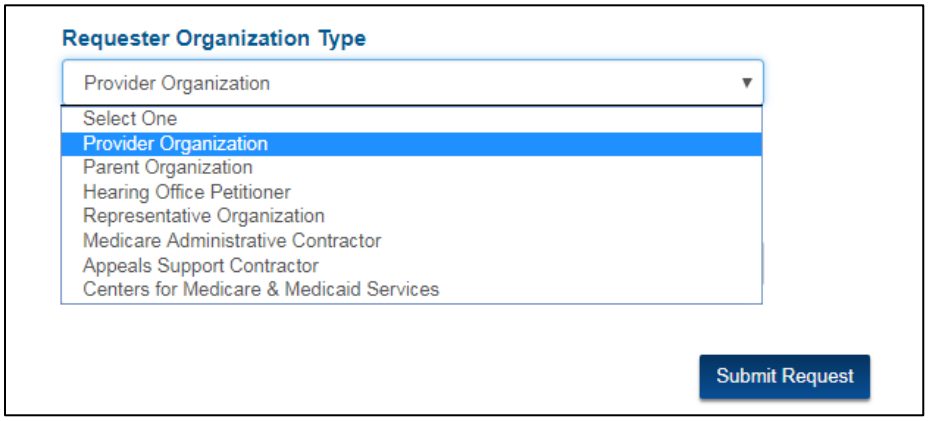


Figure 35: OH CDMS Requester Organization Type Drop-Down Menu

a. If you select Hearing Officer Petitioner from the **Requester Organization Type** drop-down menu, then an additional field is displayed to select the **Hearing Office Petitioner Type**. Select from the second drop-down menu and then the **Organization Information** section will be displayed.

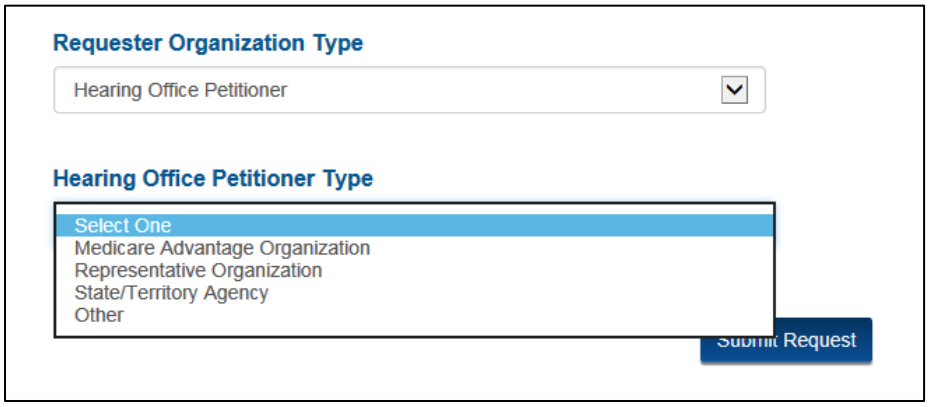


Figure 36: OH CDMS Hearing Officer Petitioner Type Drop-Down Menu

b. If you select any other organization type from the drop-down list, then the **Organization Information** section will automatically be displayed.

3. Start typing your organization's name or in the resulting organization information field. When at least two numbers or letters have been entered, the field will present a predictive text drop-down list. The volume of entries on the list will decrease as more characters are entered. You must select the appropriate organization entry from the predictive list to complete the field.

   Note: It is preferred to search by number if the organization type has a unique identiier, such as a provider number. It will narrow the predictive list more quickly and avoid potential errors due to similarities in names to other organizations or diffferences between the search term and the organization name as loaded in OH CDMS.

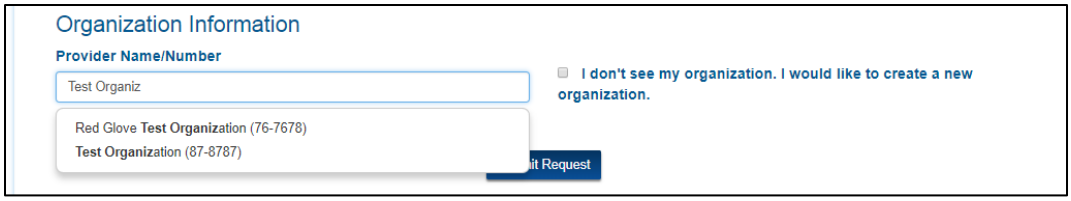


Figure 37: OH CDMS Organization Information Field

4. If your organization does not exist in the system, select the checkbox that says "I don't see my organization. I would like to create a new organization." Additional fields are displayed. Enter text as requested.

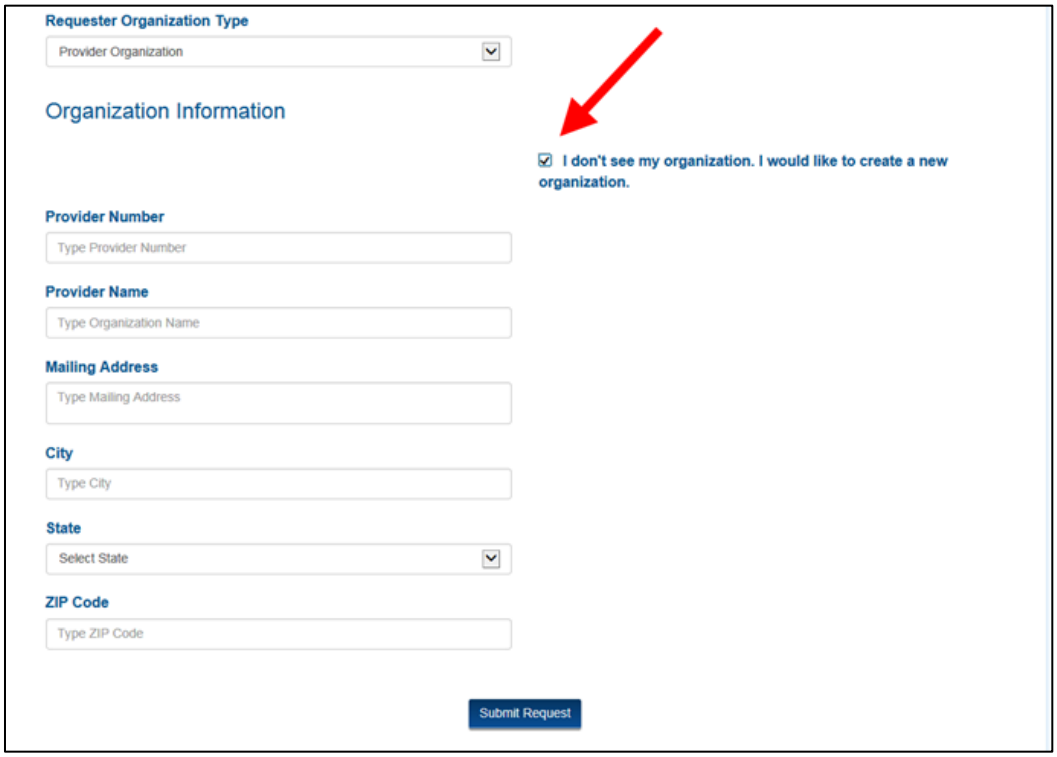


Figure 38: OH CDMS Community Registration Page – New Organization Fields

Note: Government entities and contractors cannot create new organizations from the registration page. You must select from the established organizations or contact the OH CDMS help desk.

5. Once you have completed all the fields and made selections from the drop-down menus, select the **Submit Request** button. The Application Request Confirmation is displayed with an auo-generated confirmation number.

Figure 39: OH CDMS Community Registration Conformation

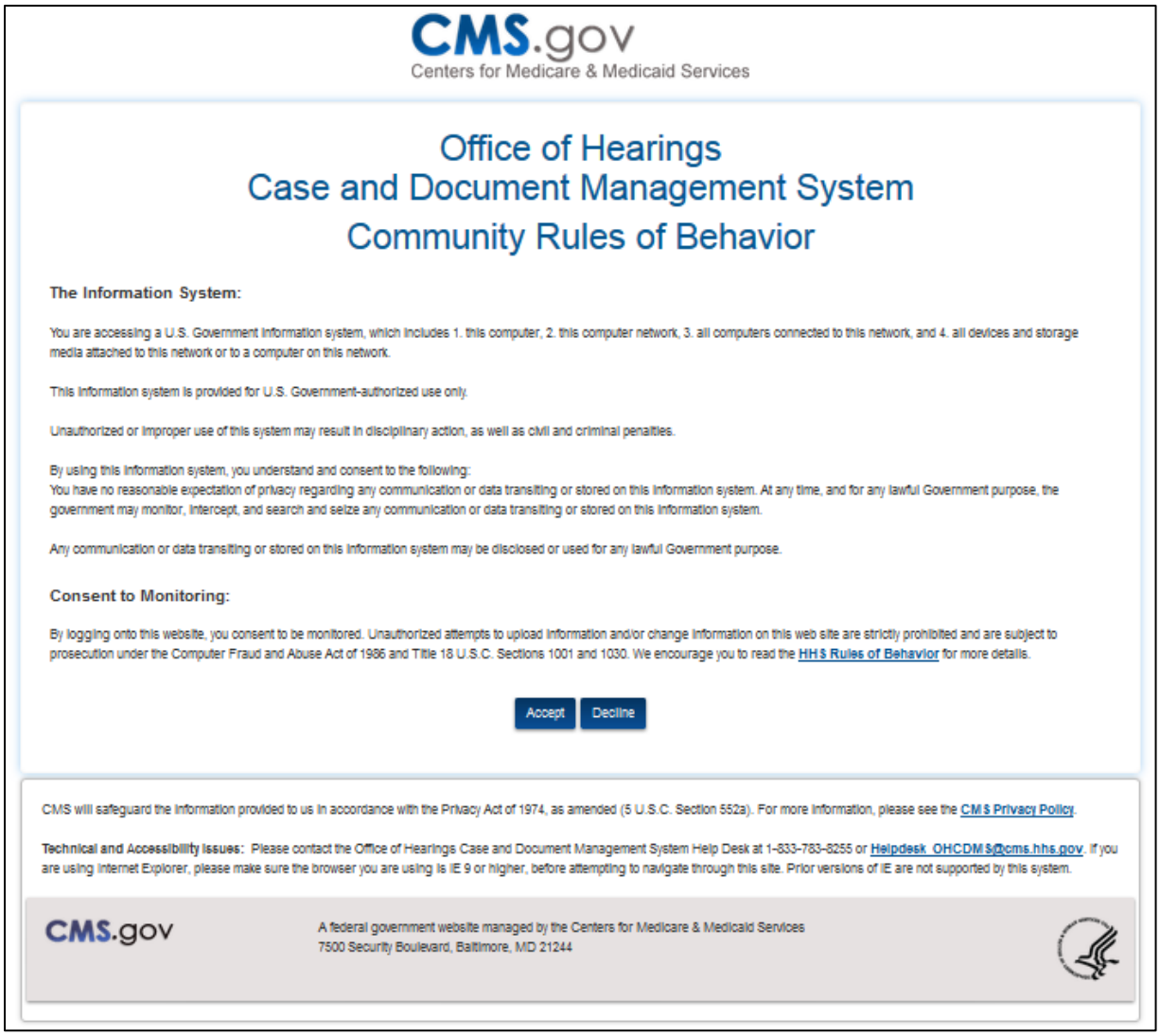
6. An email will be issued indicating approval or denial of the OH CDMS request. Further action may not be taken until OH CDMS approval is granted.

8. Launch OH CDMS

1. Navigate to the CMS SEI portal using https://sei.cms.gov.
2. Enter User ID and Password. Check the box agreeing to terms and conditions. Select the **Sign In** button.
3. Request an MFA Security Code. Enter the 6-digit code into the Verification code box and select the **Verify** button.
4. The **App Launcher** page is displayed. Select the **OH CDMS** tile to open the application.

Figure 40: CMS SEI App Launcher page with Approved Apps

5. The **OH CDMS Community Rules of Behavior** page is displayed. Review the disclosures and select the **Accept** button to proceed to the OH CDMS Landing Page.



CMS.gov
Centers for Medicare & Medicaid Services

Office of Hearings
Case and Document Management System
Community Rules of Behavior

The Information System:

You are accessing a U.S. Government information system, which includes 1. this computer, 2. this computer network, 3. all computers connected to this network, and 4. all devices and storage media attached to this network or to a computer on this network.

This information system is provided for U.S. Government-authorized use only.

Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties.

By using this information system, you understand and consent to the following:
You have no reasonable expectation of privacy regarding any communication or data transiting or stored on this information system. At any time, and for any lawful Government purpose, the government may monitor, intercept, and search and seize any communication or data transiting or stored on this information system.

Any communication or data transiting or stored on this information system may be disclosed or used for any lawful Government purpose.

Consent to Monitoring:

By logging onto this website, you consent to be monitored. Unauthorized attempts to upload information and/or change information on this web site are strictly prohibited and are subject to prosecution under the Computer Fraud and Abuse Act of 1986 and Title 18 U.S.C. Sections 1001 and 1030. We encourage you to read the HHS Rules of Behavior for more details.

Accept Decline

CMS will safeguard the information provided to us in accordance with the Privacy Act of 1974, as amended (5 U.S.C. Section 552a). For more information, please see the CMS Privacy Policy.

Technical and Accessibility Issues: Please contact the Office of Hearings Case and Document Management System Help Desk at 1-833-783-8255 or Helpdesk_OHCDMS@cms.hhs.gov. If you are using Internet Explorer, please make sure the browser you are using is IE 9 or higher, before attempting to navigate through this site. Prior versions of IE are not supported by this system.

CMS.gov
A federal government website managed by the Centers for Medicare & Medicaid Services
7500 Security Boulevard, Baltimore, MD 21244

Figure 41: OH CDMS Community Rules of Behavior

6. The **OH CDMS Landing Page** is displayed. The view may have one or more of the tiles noted below based on your role.

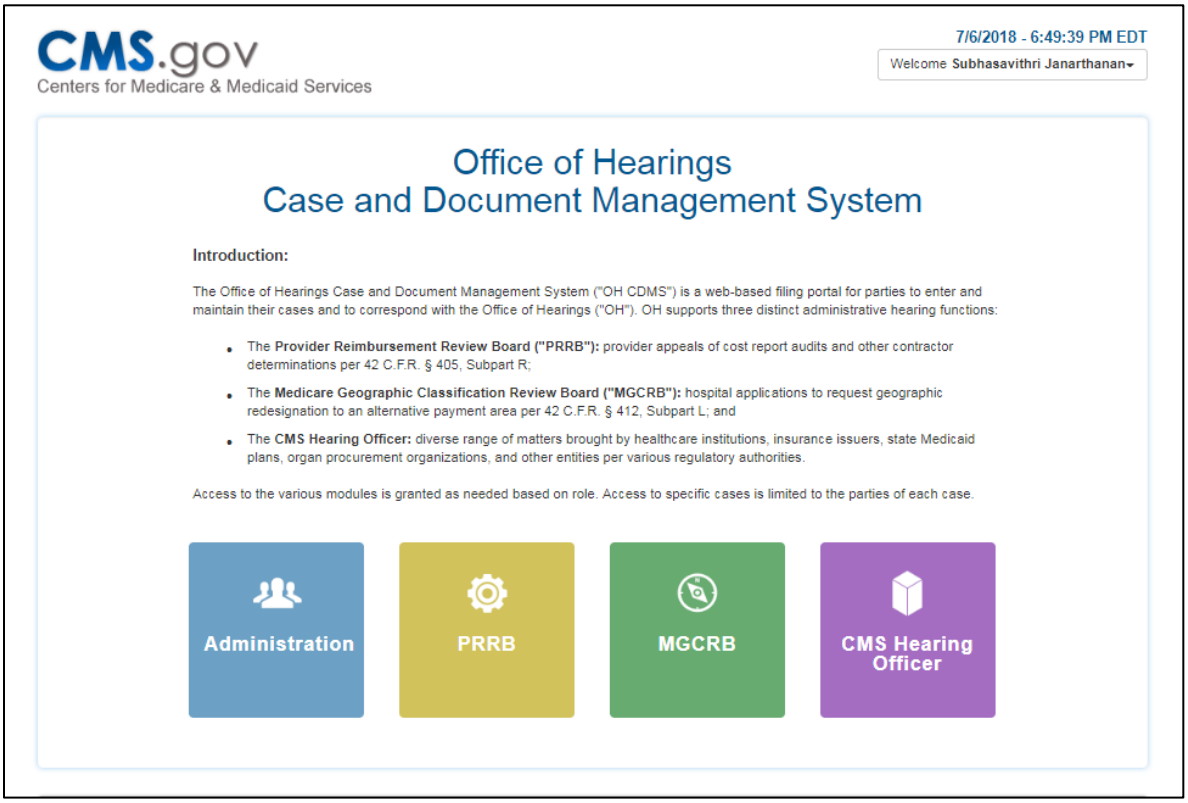


Figure 42: OH CDMS Landing Page

7. For further information about a specific module, please reference the associated External User Manuals from the PRRB, MGCRB, and CMS Hearing Officer websites:

   » https://www.cms.gov/Regulations-and-Guidance/Review-Boards/PRRBReview/Electronic-Filing;

   » https://www.cms.gov/Regulations-and-Guidance/Review-Boards/MGCRB/Electronic-Filing;

   » https://www.cms.gov/regulations-guidance/CMS-Hearing-Officer/Electronic-Filing.

9. Support

9.1 IDM Self Service

From the CMS SEI App Launcher page, users will see all applications for which they are approved and may click on the tile to enter the application. On the right side of the menu bar, users have access to several options in the avatar drop-down menu, including Profile information, IDM Self Service, and Log Out.

Figure 43: CMS SEI App Launcher Page with Approved Apps and Avatar Options

Click on the **IDM Self Service** link from the drop down menu to navigate to the IDM Self Service landing page.

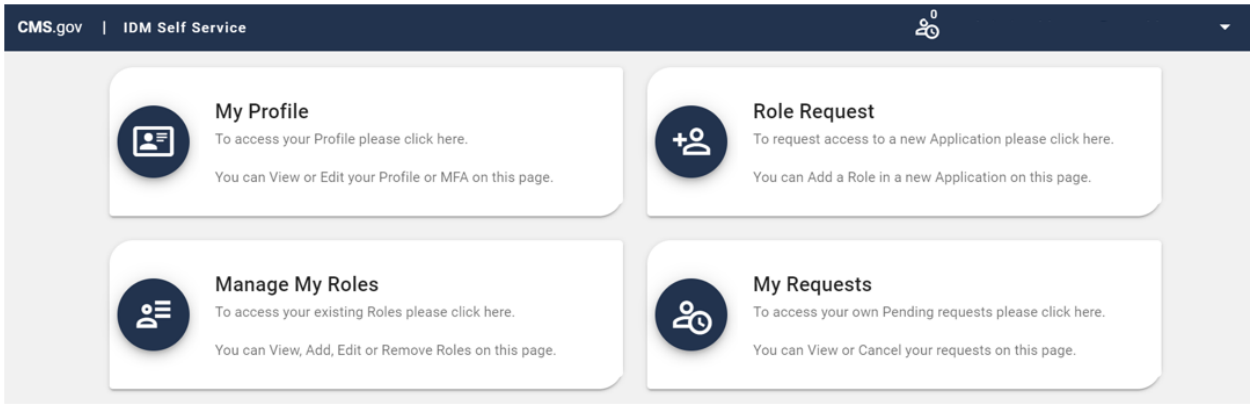


Figure 44: CMS IDM Self Service Options

Click on the **My Profile** tile. The links available in the left menu identify the components that can be reviewed and/or updated, including personal and contact information, password, security question and answer, and MFA options.

Figure 45: IDM Self Service – My Profile

9.1.1 Contact Information Updates

Any profile changes made from CMS IDM Self Service page will affect the shared CMS IDM account only. If you have changes that are applicable to user or organization contact information as reported within OH CDMS, you must contact the OH CDMS Help Desk (see Section 9.2).

9.1.2 MFA Options

Multi-factor authentication will default to the Email option upon initial set up, but users will have the following MFA options that may also be added to their profile.

a. Short Message Service (SMS) – The SMS option will send the security code directly to the user's mobile device via a text message. This option requires the users to provide a ten-digit U.S. phone number for a mobile device that is capable of receiving text messages. A carrier service charge may apply for this option.

b. Interactive Voice Response (IVR) – The IVR option will communicate the security code through a voice message that will be sent directly to your phone. This option requires the users to provide a valid 10-digit U.S. phone number (and, if needed, an extension).

c. Google Authenticator – Google Authenticator is an application for the smart phone that generates security codes. Supported phones include iPhone, Android Phone, and Blackberry. The users will need to download this application on their smartphone to be able to use this option.

d. Okta Verify – Okta Verify is an application for the smart phone that produces push notifications allowing users to verify their identity with a single tap on the

device, without the need to type a security code. Supported phones include iPhone, Android Phone, and Windows Phone. The users will need to download this application on their smartphone to be able to use this option.

Once additional MFA options are added to the user's profile, a drop-down menu of these options is available on the Verification Code Request page. The last MFA method used will remain the default option until another method is chosen.

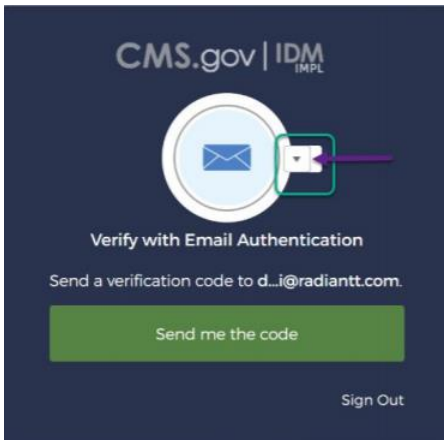


Figure 46: Verification Code Request Page with Multiple MFA Options

Figure 47: Verification Code Request Page with Multiple MFA Options – Drop-Down Menu

9.1.3 CMS SEI Reference Materials for Other Self Service Activities

Reference materials are available on the CMS SEI portal using the "**?**" icon to assist with any other CMS IDM self-service activities.

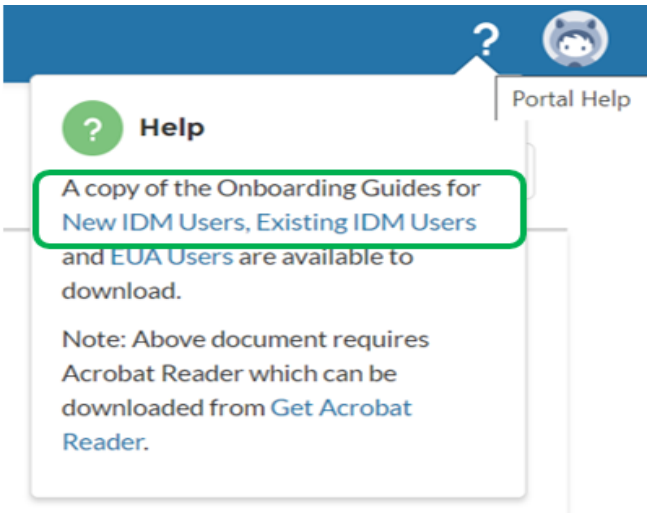


Figure 48: CMS SEI Reference Materials

9.2 OH CDMS Help Desk

For any technical system issues, please contact the OH CDMS Help Desk at 1-833-783-8255 or email helpdesk_ohcdms@cms.hhs.gov. The hours of operation are Monday – Friday (excluding federal holidays) from 7:00 a.m. to 8:00 p.m. Eastern Time.

Appendix A: Acronyms

Acronym	Term
BCI	Business Contact Information
CMS	Centers for Medicare & Medicaid Services
IDM	Identity Management
MFA	Multi-factor Authentication
MGCRB	Medicare Geographic Classification Review Board
MIDP	Manual Identity Proofing
OH	Office of Hearings
OH CDMS	Office of Hearings Case and Document Management System
PRRB	Provider Reimbursement Review Board
RIDP	Remote Identity Proofing
SEI	Salesforce Enterprise Integration

Table 1: Acronyms

Appendix B: Record of Changes

Version Number	Date	Description of Change
1.0	07/09/2018	Initial manual issuance for release of OH CDMS application through the CMS Enterprise Portal
2.0	02/21/2021	Full manual revision to identify changes to the CMS Identity Management process, registration procedures, and access to the OH CDMS application via the new Salesforce Enterprise Integration Portal.

Table 2: Record of Changes