



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

Enterprise Identity Management (EIDM) Frequently Asked Questions

Version 0.2 Final

06/10/2016

Document Number: EIDM FAQs-R14.2016.06

Contract Number: HHSM-500-2007-00024I

Table of Contents

A.	General Information:	3
B.	Personal Information:	4
C.	Identity Verification:	6
D.	Request Application Access Using the Access Catalog:	9
E.	Add/Remove a Role or Application:	9
F.	Multifactor Authentication (MFA):	11
G.	Annual Certification:	16
H.	Section 508:	19
I.	Record of Changes	20

The most frequently asked questions (FAQ) by EIDM users are listed below:

A. General Information:

1. What is CMS EIDM?

EIDM is the acronym for CMS' Enterprise Identity Management system which includes Registration, Authentication, Authorization Assistance, and Identity Lifecycle Management (IDLM) Services.

2. What does EIDM have to do with the CMS Enterprise Portal?

EIDM is integrated with the CMS Enterprise Portal and provides a way for users to register and receive a single User ID/Password on the CMS Enterprise Portal, which they can use to access multiple CMS applications.

3. What is a CMS EIDM user account?

An EIDM account ensures that only authorized/registered users can access protected information and systems through the CMS Enterprise Portal.

4. Who is eligible to have a CMS EIDM user account?

All US residents who are over 18 years of age and have a current or previous valid US residential address are eligible to have a CMS EIDM user account.

5. I am new to CMS Enterprise Portal. How do I create my user account?

Once you are on the CMS Enterprise portal landing page, select the 'New User Registration' link. You are required to enter some personal information and choose a desired User ID/Password following the guidelines provided. Once the details have been successfully updated in EIDM, the system will display a message confirming the creation of the user account.

6. How should I enter my name if I have two first names, for example Mary Kate?

EIDM requires users to enter the first part of the name in the first name field and the second part of the name in the middle name field. For example, Mary Kate would be entered as First Name: Mary, Middle Name: Kate.

7. How should I enter my name if I only have one name, like Prince?

EIDM requires users to enter your mono-name in both the first name and last name field. For example, Prince would be entered as First Name: Prince, Last Name: Prince.

B. Personal Information:

8. What personal information am I required to provide in order to register for my user account?

You must provide your legal name, current home address, primary phone number, and E-mail address. You must enter your first and last name as they appear in legal documents, such as your driver's license or passport. If you have a suffix included in your name (such as Sr., Jr., II, etc.), make sure you select it from the suffix field exactly as it appears on legal documents.

9. Why should I submit personal information to create a user account and how safe is it?

EIDM collects personal information to uniquely identify users when registering with the system. We may also use your answers to the challenge questions and other Personal Identifiable Information (PII) to later identify you in case you forget or misplace your User ID/Password. For security level information please visit:

[Centers for Medicare & Medicaid Services \(CMS\) Website Privacy Policy](#)

10. Can I register for an EIDM user account with a foreign address and an international phone number?

Yes, EIDM allows users to register with a foreign address and an international phone number. At a minimum, foreign addresses must include the following information:

1. House number, street name, and country; and
2. An international phone number that must start with the country code, followed by the area code, and the primary phone number.

11. Can I change my foreign address to a U.S. address, and vice versa?

Yes, EIDM allows users to change their address from a foreign address to a U.S. address, and vice versa. Use the 'Change Address' link under the 'My Profile' menu to change your address.

12. What will you do with my Personal Identifiable Information (PII)?

EIDM uses an external authentication service provider, [Experian](#), to verify your identity based on the information you provide. Experian verifies your information against its records to successfully identify you. CMS provides, on public-facing websites, their Terms & Conditions of how your information will be handled when registering for a CMS EIDM user account.

13. How many days do I have to confirm my EIDM account?

EIDM requires users to confirm their account between 30 and 180 days. Accounts are confirmed by selecting the link provided to the user in their account confirmation E-mail. If the user fails to confirm their account, then the link and the account will expire.

14. How can I update my personal information?

You can update your personal information by selecting 'My Profile' from the dropdown menu at the top right hand corner of the CMS Portal home page. You will then be directed to the 'View My Profile' page, where you can change your personal information by selecting the links on the right side of the page. You may be requested to answer challenge questions based on the changes you make.

15. Where can I find information regarding who has the right to request a Social Security Number (SSN)?

Federal law mandates that State departments of motor vehicles, tax authorities, welfare offices, and other governmental agencies request your SSN as proof that you are who you claim to be. However, the Privacy Act of 1974 requires that any government agency requesting your SSN provide details on how this information will be used, and what law or authority requires its use.

For information on who has the right to request your SSN please select the following link:

[Who Can Lawfully Request My Social Security Number?](#)

The Privacy Act can be read at the following link:

[The Privacy Act of 1974](#)

16. I already provided my personal information during registration to setup an EIDM user account. Why do I have to provide it again to access certain applications?

When you have selected an application or role that requires a higher level of security, you are required to complete Identity Verification. In most cases, you may need to provide a few more details (i.e. SSN, Date of Birth) to be able to request access to the selected application or role.

17. Will my Social Security Number (SSN) be shared with any federal or private agency?

Your SSN will be used for verification purposes only. EIDM does not share your SSN with any other federal or private agency.

18. How often do I need to update my password?

EIDM requires that users update their password at least once between 60 days and 24 months depending on the user role community. Once your password expires, you will be prompted to enter your new password. You can use the 'Change Password' self-service feature located on the 'My Profile' page. To use this feature, you must sign into the CMS Portal and select the 'My Profile' link from the dropdown menu at the top right hand corner of the CMS Portal home page. You must click the 'Change Password' link on the 'My Profile' page to change your Password.

19. How often can I reuse my password?

EIDM allows your password to be reused between 1 and 12 generations depending on the user role community.

C. Identity Verification:**20. What is Identity Verification?**

Identity Verification is the process of providing sufficient information (e.g., identity history, credentials, or documents) to a service provider for the purpose of proving that an individual is who he/she claims to be. Individuals requesting electronic access to CMS protected information or systems must be identity proofed prior to being given access.

21. Why does Experian require my personal information?

Experian uses your personal information to verify your identity against your personal information record.

22. Does verifying my identity by Experian affect my credit score?

No, this kind of inquiries is known as a "soft inquiry". Soft inquiries do not affect your credit score, and there are no charges related to them. Soft inquiries are displayed in the consumer version of the credit profile, which is neither viewable nor reported to lenders. If you order a credit report from Experian, you will see an entry of inquiry by the Centers for Medicare & Medicaid Services with CMS' address on the date the request was made.

23. Will I be required to go through Identity Verification after changing my address from foreign address to U.S. home address and vice versa?

No, you will not be required to re-do Identity Verification if you already have a role that previously required your identity to be verified.

24. What if I have problems completing Identity Verification? Is there an Experian Help Desk?

Yes, Experian Verification Support Services is a dedicated call center for individuals who have failed the online Remote Identity Proofing (RIDP) process while attempting to obtain a CMS EIDM user account. If you fail online RIDP, EIDM will generate a reference code and the Experian Verification Support Services contact information will be provided on the screen for further action.

25. What happens if the Experian Help Desk cannot verify my identity?

If your identity cannot be verified, even with assistance from the Experian Help Desk, you will need to contact your application specific Help Desk to go through a document based proofing process. If your Application Help Desk cannot verify your identity, your access to CMS applications that require a higher level of security will be restricted.

26. Why am I not able to change my User ID?

The User ID identifies you uniquely to EIDM; therefore, you cannot change your User ID.

27. Can I use the same credentials for different applications?

Yes, you may use the same credentials to access different applications. Once you have logged into the CMS Portal home page, you can request access to other applications.

28. When I try to login I get an error message “Incorrect combination of User ID or Password. Please try again. If you need further assistance, you may use the “Forgot User ID” or the “Forgot Password” link to help you.” What should I do?

Please check the user ID and password that you entered. An incorrect combination of these will result in such an error message.

29. When I try to login I get an error message “Incorrect combination of User ID, Password or Security Code. Please try again. If you need further assistance, you may use the “Forgot User ID” or “Forgot Password” links to help you. For issues with the Security Code, you may use the “Unable to Access Security Code?” link or contact your Application Help Desk.” What should I do?

Please check the user ID, password and Security Code that you entered. An incorrect combination of these will result in such an error message.

30. When I try to login, I am prompted to enter a Security Code. What do I do if I don't have a Multi-Factor Authentication (MFA) device registered to my account or am having issues retrieving a Security Code?

For issues with logging in with a Security Code you may use the following options:

1. If you do not have an MFA device registered to your account, you may use the “Register MFA Device” link on the Password and Security Code page for assistance.
2. If you are unable to retrieve a Security Code from your registered MFA device or do not have your device available, you may use the “Unable to Access Security Code?” link on the Password and Security Code page for assistance.
3. If you have trouble using the “Register MFA Device” or “Unable to Access Security Code?” links, you may contact your Application Help Desk for assistance.

For more information about MFA, please refer to the Multifactor Authentication (MFA) section below.

31. When I try to login, I get the error message stating “Your account is disabled. Contact the Help Desk to enable your account.” Why does this happen?

A user’s account can be disabled by Application Help Desks or by EIDM Administrators for possible reasons that are linked to security violations or fraud detection. In order to enable your disabled account, you are required to contact the Application Help Desk.

32. When I try to login, I get the error message stating “Your account has been locked. Please try again later.” Why did this happen and how can I get my account unlocked?

After three unsuccessful attempts to login, your account will be locked. Your account will be unlocked after 60 minutes have elapsed since your third consecutive failed authentication attempt. After the 60 minutes have passed, you will be required to enter valid credentials associated to your user account to unlock the account. If you are unable to unlock your account, you may call your Application Help Desk for assistance.

33. When I try to login, I am directed to the ‘Unlock My Account’ view. Why is this and how do I unlock my account?

EIDM locks your user account if no account activity is reported for 60 days. When you login after 60 days the system will display the ‘Unlock my Account’ view; enter your User ID and correctly answer all challenge questions on the next page; enter your old password and then a new password in the input fields of ‘New Password’ and ‘Confirm New Password’ to unlock your account.

34. What are challenge questions and why do I need to select and answer them when setting up my account?

EIDM uses challenge questions for security purposes to verify your account. When you register your account, you will need to select three different questions and provide an answer for each question. You will be asked to answer the challenge questions in the future if you forget your password, change your address, change your phone number, or to unlock

your account. Correct responses to the challenge questions will enable EIDM to confirm your account.

D. Request Application Access Using the Access Catalog:

35. I am trying to request access to an application. Why can't I see my application in the Access Catalog?

There are two options for finding an application in the Access Catalog:

1. Type the name of the application in the search window of the Access Catalog toolbar. The application will be displayed.

Note: Applications are listed by their acronym, not their full name. You must use the acronym of the application to search.

2. Use the inner scroll bar and scroll down through the catalog to find a specific application.

E. Add/Remove a Role or Application:

36. How do I request access to applications now that I have an EIDM account?

After setting up your EIDM account, you must request access to the applications that you previously used. This is a one-time setup process per application. Select the 'My Access' link located on the CMS Portal home page, then click the 'Request New Application Access' link. Follow the on-screen instructions. Once your request has been approved, a link to the application will appear on your 'My Home' page.

37. How long does it take to get approved for an access to a requested application or a role?

It can take up to 30 days to be granted access to an application or role. After 30 days, your request will expire. In the unlikely event that this happens, please contact the respective Application Help Desk.

38. How do I add another role to an application to which I already have access?

After you have access to an application role, you can request access to additional roles by selecting the 'My Access' link and then selecting the 'Add a Role' link next to the desired application on the 'View and Manage My Applications' view. You will be required to select a new role, as well as possibly to provide additional information before submitting your request. For some applications, you may receive immediate approval based on the

information entered. Depending on your Level of Assurance (LOA) and the role that you request access to, to satisfy system security requirements you may need to complete Identity Verification, establish credentials for Multi-Factor Authentication (MFA), or change your password the next time you login to the system. This may require you to provide additional information as part of the role request process. If applicable, please note that your request cannot be fulfilled until Identity Verification is complete and Multi-Factor Authentication (MFA) is established.

39. How do I remove a role that I no longer need?

Select the 'My Access' link and then select the 'Remove a Role' link next to the desired application on the 'View and Manage My Applications' view. Next, select the 'Remove' link next to the role that you want to remove. The system will ask you to confirm that you want to remove the role. You can cancel the request or continue by selecting 'Submit'. If you are a user with approval authority you may not be able to remove your approval role if you are the only approver for your end users. In cases like this you must contact the Application Help Desk for further assistance.

40. How do I cancel a pending role request?

Select the 'My Access' link and then select the desired Request ID under the 'My Pending Requests' section. Next, select the 'Cancel' link next to the pending role request you want to cancel and follow the instructions on your screen.

41. Why am I being asked to associate my role to an organization?

An organization is a particular provider, practice group, or other entity that may exist for a particular application in EIDM. Applications that require a role to be associated to an organization do so with the assumption that the user is representing or acting on behalf of that organization.

42. As a provider can I create a new organization or associate with an existing organization?

Yes, providers can create a new organization or they can associate with an existing organization when requesting a role for your application.

Note: This is applicable only for applications that have a provider related structure.

F. Multifactor Authentication (MFA):

43. What is Multi-Factor Authentication (MFA)?

MFA is a type of login (authentication) that, in addition to a user ID and password, requires another “factor” such as a Security Code. To comply with CMS policy, most users will need to establish a second login “factor” commensurate with the level of access requested. CMS uses Symantec’s Validation and Identity Protection (VIP) service to add a second layer of protection for your online identity. Symantec provides validation and identity protection through computer, phone, and E-mail.

44. How do we use MFA?

You will be asked to enter your user ID, password, and an additional Security Code that is generated by Symantec VIP software to gain access to your application. The Security Code can be generated by:

- A free Symantec application that can be downloaded to your desktop or smartphone;
- A Short Message Service (SMS) or Interactive Voice Response (IVR) once you have registered your phone in your application; or
- By E-mail.

The “Where can I get the MFA software?” section below provides the necessary information to install the Symantec application on your desktop or smartphone.

45. How do I get an MFA device?

Your application will prompt you to register an MFA device when you request access to protected information and you have not already registered an MFA device with the application. You will be given a choice of MFA Security Code delivery methods. The primary MFA Security Code delivery method is to download software and install it on your computer or a mobile device. Alternatively, if you require special support, you can set up SMS or IVR to deliver your MFA Security Code. Details on where to get the MFA software are described below.

46. Where can I get the MFA software?

You will need MFA software if you choose to receive your MFA Security Code on a computer, laptop, or mobile device. You will be required to download the MFA software from Symantec and install it on your device of choice.

To download the desktop software for Windows or Mac, navigate to <https://idprotect.vip.symantec.com/desktop/home.v> and follow the instructions.

If using an iPhone, Android, Blackberry, or other mobile device, use your device to navigate to <https://m.vip.symantec.com/home.v> and follow the instructions.

SMS, IVR, and E-mail options do not require a software download.

47. When I click on an application, I am redirected to the Multi-Factor Authentication (MFA) login screen. What is this?

The MFA login screen is displayed when you attempt to access an MFA-protected application. If you have an MFA device, you will be able to access the application. If you do not have an MFA device, then you will have to register for MFA using either your phone or computer.

48. What are the types of devices I can register with for my Multi-Factor Authentication (MFA)?

You can add one or more of the following devices as your MFA device:

- Smartphone, Computer, or Tablet – By downloading the Symantec VIP access application;
- Interactive Voice Response (IVR) – By registering with a U.S. phone number;
- Short Message Services (SMS) – By registering with a U.S. phone number; and
- E-mail – By registering with a valid E-mail address (the E-mail address associated with your profile will be used).

49. How do I register my Multi-Factor Authentication (MFA) device (phone, computer, or E-mail) to my EIDM user account?

Once you successfully complete the Identity Verification process, EIDM will display the 'Register your Phone, Computer, or E-mail' page depending on the application role being requested. Alternatively, you can register for MFA by selecting the 'Register your Phone, Computer, or E-mail' link under 'My Profile'.

Your device can be registered for MFA in one of five ways:

1. Download VIP access software on your phone – Enter the alphanumeric Credential ID generated by the VIP access client. Then enter the Security Code generated by the VIP client.
2. Download VIP access software on your computer – Enter the alphanumeric Credential ID generated by the VIP access client. Then enter the Security Code generated by the VIP client.
3. Text Message Short Message Service (SMS) – Use this option to have the Security Code texted to your phone. You must enter a valid phone number and your phone must be capable of receiving text messages. Carrier charges may apply.

4. Interactive Voice Response (IVR) – Use this option to receive a Voice Message containing the Security Code. You must provide a valid phone number and (optional) extension that will be used during login to obtain the Security Code. The extension may begin with any one of the following: asterisks '*'; period '.'; comma ','; pound '#', followed by numeric 0 to 9. For example: 4885554444, 1112.
 - * (asterisk) Used by some phone systems to access extension;
 - . (period) Creates a delay of approximately 5 seconds;
 - , (comma) Creates a short delay of approximately 2 seconds;
 - # (pound) Used by some phone systems to access an extension; and
 - A comma may be used if you are unsure of the special character supported by your company's phone system.
5. E-mail – You can also opt to use the E-mail in your profile to receive a Security Code when logging into a secure application.

50. How do I register for MFA if I receive an error when installing the software on my computer?

If you are having trouble downloading and installing the MFA software on your desktop or laptop, it is possibly due to your company's IT policy that disables users from installing any software on company-provided machines. Check with your company's IT department for assistance. If your company does not allow you to install MFA software, one alternative is to use a mobile device that you control, or you can also use a voice call to obtain the Security Code. You can refer to other instructions in this FAQ document for information on cell phone installation and IVR usage.

51. I cannot use the desktop MFA software or the mobile phone MFA software. What should I do?

Your application allows you to set up a voice or SMS delivery method for your Security Code that does not require an MFA software download. You can register a phone number and select SMS or IVR. Then your application can register your phone number and delivery method with Symantec. After your MFA is activated, when you login to your application you will receive either a phone call or text message that contains your Security Code, depending on the delivery method you selected.

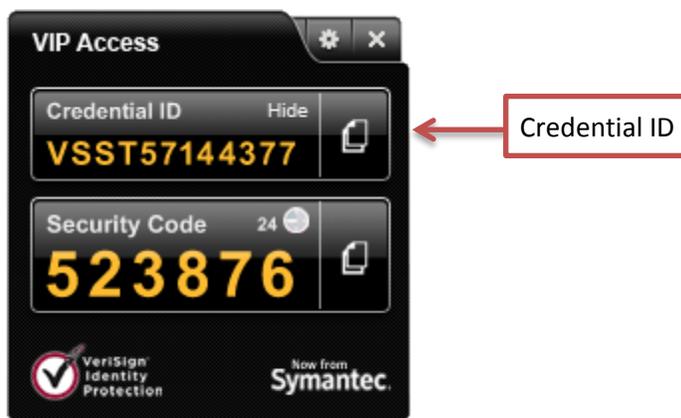
The SMS and IVR Security Codes expire within 10 minutes of when they are sent, so please make sure you provide a phone number that will be accessible to you during your typical work hours. For example, do not use a residential phone number if you will normally login from your place of employment. E-mail Security Codes expire within 30 minutes of when they are sent.

52. I cannot download Symantec VIP on my mobile phone. What should I do?

If your mobile phone is company-provided, your IT department may have locked down your device and disallowed users from loading applications. Check with your IT department to see if you have the required permissions to download an application to your mobile phone. Some companies allow the download of applications on their mobile phones but only over Wi-Fi networks. If this is the case, connect your mobile phone to a Wi-Fi network to download Symantec VIP by typing <https://m.vip.symantec.com/home.v> in the mobile phone browser.

53. I am being asked to type a Credential ID. Where do I find the Credential ID?

The Credential ID is the 12-digit alpha-numeric number on the top of the soft token that was downloaded to your device from Symantec. The Credential ID begins with four letters and ends with eight numbers. In the example below, the token displays the credential ID as VSST57144377.



54. What is a Security Code?

A Security Code is a six-digit numeric code that appears under the label 'Security Code' on your MFA device. This Security Code is mapped to your user ID and is used as a second-factor authentication to confirm your identity.

55. Do I need to use my Multi-Factor Authentication (MFA) device every time I login? How do I know if I need MFA?

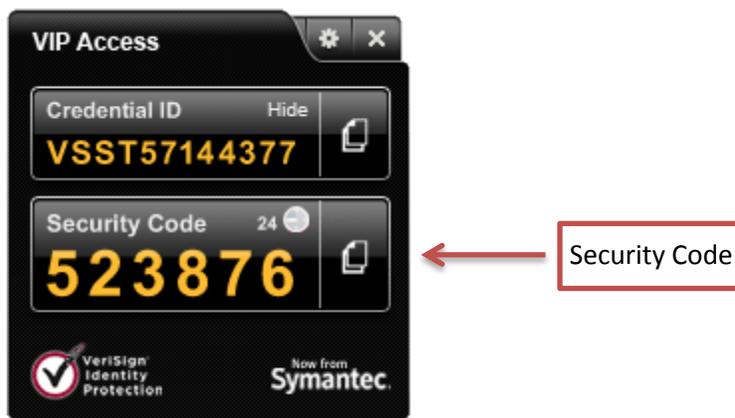
MFA is required for specific applications that require a higher Level of Assurance (LOA). Not all applications require MFA for users. This is decided on the basis of application access that a user has. For example, a user has access to App1 and App2. App1 requires MFA and App2 does not. The user will have to login using Multi-Factor Authentication (MFA) (i.e. the user ID, password, and Security Code).

56. Can I access multiple applications if I'm Multi-Factor Authenticated (MFA)?

Once you have been multi-factor authenticated (i.e. “logged in”) into your application, if you do not log out of the system, you can access other protected CMS Applications that require MFA without having to be authenticated again with an MFA Security Code. If you log out of the system, when you log back in, you will be asked to present your MFA Security Code when accessing your CMS Application.

57. How do I use my Multi-Factor Authentication (MFA) device to log into my CMS EIDM user account?

When you log into your application, the system will display the MFA login screen. You will be required to enter your user ID, password, and the MFA Security Code. If you have registered an MFA device, enter your user ID, password, and the Security Code that is displayed on your MFA device.



For your protection, an MFA device automatically generates a new Security Code each time it counts down from a 30-second timer.

If you have registered an MFA SMS or IVR device, when you log into your application, the system will send you a Security Code via text message or voice call to the number you registered in EIDM.

For your protection a Security Code sent via SMS or IVR counts down from a 10-minute timer. The Security Code sent via E-mail counts down from a 30-minute timer.

58. How do I add additional Multi-Factor Authentication (MFA) devices to my CMS EIDM user account?

You can register up to five MFA devices to your user account. Additional MFA devices can be added to your account after you have been prompted by your application to set up the first MFA device. The “Register your Phone, Computer, or E-mail” link on the “My Profile”

page will appear once you have successfully set up your first MFA device. You can click on the link and add additional MFA devices to your user account.

59. Will I be charged cell phone time each time I use Symantec VIP MFA on my mobile device?

It depends on what delivery method you use. The Symantec VIP MFA software is free. Once the Symantec VIP MFA application is downloaded and installed on the phone it does not utilize any cell time to generate the six-digit security code. Cell or network traffic is used to download the application to one's mobile device. There are no recurring charges associated with the use of either software option. If you choose not to use the software option and select SMS or IVR, carrier charges may apply.

60. I lost all my Multi-Factor Authentication (MFA) devices linked to my EIDM user account. How do I deactivate the linked devices and link new devices to my user account?

Your Application Help Desk should be able to assist you in removing/deactivating the registered devices and registering new devices to your user account.

61. What should I do if I lock my MFA device?

You must contact your Application Help Desk to unlock the registered MFA device.

62. If my Credential ID is copied or stolen, can someone else access my CMS EIDM User account?

No. A Credential ID cannot be used to access an EIDM user account.

G. Annual Certification:

63. What does it mean when my account is inactive?

A CMS Portal account is inactive when a user has not logged into either their application or the CMS Portal for 60 days or more.

64. What does it mean when my account is locked?

A user's account is locked following 60 days of inactivity. The user is prevented from logging into any application. To unlock an account the user must: login to the CMS Portal, answer their challenge questions, and reset their password; or call the Application Help Desk.

65. What does it mean when my account is deleted?

When a user's CMS Portal account does not have a role in any application and has been inactive for more than 360 days it will be deleted. The user's account may no longer be used for any purpose and the user may register again to create a new account.

66. What is an Account Review?

Users wishing to acquire a role in their application must first register for a CMS Portal account. Account Reviews are conducted every six months to check for the presence of at least one application role in a user's account. If an account does not have any application roles associated to it and has been inactive for more than 180 days, it will fail. If the account has been inactive for more than 360 days, it will be deleted.

67. Is there anything I need to do for Account Reviews?

If you have an application role associated to your account then no action is required on your part. If you do not have an application role associated to your account and have been inactive for more than 180 days, you will receive an E-mail with instructions on how to proceed.

68. I got an E-mail that my account failed an Account Review. What should I do next?

If you no longer require an account in the CMS Portal, no further action is required on your part. If you wish to continue using your account, please follow the instructions in the E-mail describing how to proceed.

69. I got an E-mail that my account was deleted as part of an Account Review. What should I do to get my account back?

If your account was deleted as part of Account Review, you must create a new account. Please go to the CMS Portal and follow the on screen instructions to create a new account.

70. What is a Role?

A Role is the name (e.g. Submitter or Representative) given to a set of privileges and permissions that an individual may perform within an application or other computer resource. Users must submit a role request which should be approved and then the role will be added to the user's profile. Use of a role is typically granted for one year by an application Business Owner, their representatives, authorizers, Help Desk personnel or other approver. Each year, continued use of a role must be approved or the role will be removed from the user's profile. This annual re-approval is known as Annual Certification.

71. What is Annual Certification?

CMS security guidelines require that each year, the use of a role must be approved or the role will be removed from the user's profile. Annual Certification is the process of approving

a user's continued use of a role and is valid for one year. 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 the user's profile and an E-mail will be sent notifying the user that their role has been removed.

72. What is an Annual Certification due date?

The Annual Certification due date is the date that a role is due to be certified. This is normally one year after the last Annual Certification.

73. How often does my role need to be certified?

Your role needs to be certified once a year. It is your approver's responsibility to certify your role and usually requires no action on your part.

74. What do I need to do to have my role certified?

It is your approver's responsibility to certify your role and usually requires no action on your part. If your role failed Annual Certification, an E-mail will be sent to you with more information.

75. I got an E-mail that my role was removed because it failed Annual Certification. How do I get my role back?

If you still need access to the role that was removed, you must request the role again. Please follow the instructions provided in the E-mail.

76. I am an approver who is responsible for approving role requests. What do I need to do for Annual Certification?

As an approver for role requests, you will be responsible for certifying users' roles by the certification due date. An 'Annual Certification' link can be found where you usually go to approve user role requests. On that page you will be able to search, review, certify, or revoke the certifications for users under your authority. If no action is taken by the certification due date, the role will be removed.

77. I am an approver and I received an E-mail informing me that I have roles pending Annual Certification. What do I need to do?

As an approver for users' role requests, you are also responsible for certifying those roles annually. 30 days before a role's certification due date, you will receive an E-mail providing a count of user roles that are due for certification within the next 30 days, 15 days, 7 days, and 1 day. If no action is taken by the certification due date, the role will be removed.

78. If my role is automatically approved, do I need to take any action for Annual Certification?

If your role requests are automatically approved, they will also be automatically certified. Some automatically approved roles require the information provided, when the role was first requested, to be validated against a trusted resource. As part of Annual Certification, this information will need to be revalidated. If the validation is successful, your role will be certified automatically and no action is required on your part. If the validation fails, CMS.gov will send you an E-mail notifying you that validation failed and describing how to correct the error before the certification due date for your role.

79. Why can't I see all my users' roles in the Pending Certification View Page?

The Pending Certification View Page shows a maximum of 250 roles that you are responsible for certifying in the next 30 days. If you have more than 250 roles to certify in the next 30 days or wish to see roles due for certification past the next 30 days, you must use the Search feature.

80. I am searching for roles that I need to certify but don't see any results after selecting the Search button. Why is my search not displaying any results?

The most likely reason is that your search did not match any existing role certifications. The search will also not return any results if there are more than 250 certifications found for your specific search criteria. Please ensure that you narrow down your search so that no more than 250 certifications will be found from your search request.

H. Section 508:

81. What is Section 508?

Section 508 is a federal law that requires agencies to provide people with disabilities equal access to electronic information and data comparable to those who do not have disabilities, unless doing so would impose an undue burden on the agency. The Section 508 standards are the technical requirements and criteria used to determine whether the agency is meeting the requirements of this law.

82. How do I access EIDM in 508 Accessibility Mode?

EIDM users can use the 'Screen Reader Mode' link that is located on the 'My Profile' page to turn the accessibility mode on or off. The 'Accessibility Settings' link is also located on the 'My Profile' page. To use either of these features, you must sign into the CMS Portal and select the 'My Profile' link from the dropdown menu at the top right hand corner of the CMS Portal home page.

I. Record of Changes

Version Number	Date	Author/Owner	Description of Change
0.1	06/01/2016	QSSI	Initial draft.
0.2	06/10/2016	QSSI	Updated to address comments from CMS and made final.