CMS Enterprise User Administration (EUA)
Job Code Profile Questionnaire

Purpose: This form is used to request the creation of an EUA Job Code. All IT infrastructure (servers) and application access is granted based on Job Codes, thereby enabling the complete automation of the approval process to grant, change or rescind access to these resources. This request form should be completed by the Application Owner of the resources. Use the "IT Support" icon from the CMS desktop to submit this completed form to the EUA Team. Use a new form for each new Job Code that you wish to have created.

IT Support Icon Instructions: To submit a request, select the "IT Support icon" from the desktop, logon on and then select the "CREATE" button, from the "REQUEST DETAILS" menu, scroll down to and select "REQUEST TO CREATE A NEW PROFILE/JOB CODE" from the "SERVICE REQUEST" entries. From the "ADD ATTACHMENT" section, select "ATTACHMENT 1" and then click the "ADD" button, fill in the attachment name or browse to find the name and location of where you have save this completed form, and then select OK. Click on the "SUBMIT REQUEST" button. Refer to the *CMS EUA Users Guide* http://www.cms.hhs.gov/InformationSecurity/Downloads/EUA_User_Guide.pdf for additional information on the "IT Support Icon".

Job Code Name: Please enter the name that you would like your users to request from their CMS Access Administrator (CAA). This name cannot contain spaces and is normally based on the 3-letter acronym defined by APCSS, if applicable and must be unique to all other Job Codes. (see current list https://www.cms.hhs.gov/cbt/downloads/jobcodes.htm).

ISSO_Office/Center_level

Detail Job Description: Please enter the full name of the application and a detailed description (no more then 80 characters) of the application that will be displayed to the CAA.

Information System Security Officer (ISSO) Office/Center level

Application Owner: Please provide the names and UserID's of the at least two individuals that will approve access to your application/data. Application/Data Owners are responsible for maintaining the validity and integrity of the application's data. The owner must be a Federal Employee and at least a Division level manager.

Cyndy Anderson A2PA Dick Lyman MH33

Application Maintainer: The Application Owner listed above must be the 1st line supervisor of the application maintainer listed in this section. Please provide the names and UserID's of individuals that must be notified upon access being granted or removed to your application. The email address of a distribution list or resource mailbox could also be used. Application Maintainers are the individual or group who is responsible for maintaining the application. They complete any work that cannot be completed by EUA such as granting access within an application.

Sharon Kavanagh K127 Bill Pollak MJ20

Connect to RACF Group: (for mainframe applications only) Please provide the name of the group or groups where the accounts should be added as unique members. The access that the groups have will dictate what the users will be able to do within the Platform. The group should be used by the backend platform or application for access management.

n/a

Profile Type: (for mainframe applications only) Indicate if the access fits into one of the categories specified. This information is used to execute special actions when access is granted. Remote Access will cause an email of remote access instructions to be sent. RACF TSO will indicate within RACF the TSO access status. CICS will indicate that the profile will create CICS accounts as needed. If the profile does not fit any of the categories, then this can be left blank.

n/a

Platform Type: Please provide the type of operating system or database for which access is being granted. CMS.Local indicates that the user will log on directly to the CMS domain. HCFA.Gov indicates that the user may or may not logon directly to the network. UNIX indicates that the access will be granted to specific servers. LDAP indicates that the user may or may not log onto the network directly. Oracle, MSSQL and Sybase are the database types that are serviced by EUA.

none

Account Default Group: If necessary, please provide a default group for the account. This group will grant the user basic level of rights. For most managed systems, the default is best. This should only be changed for special circumstances.

none

Additional Account Requirements: Please indicate if there are any other details about the account that should be set during account creation. This could include special home folder information or other details about the account.

This is a job code in name only to replace a paper based process for issuing appointment orders for individuals who are being appointed as ISSOs.

Additional Information: Please provide additional information about what access will be granted, how the access will be used and a general description of what the application does. This information will be provided to 1st Approvers so that they may better understand the system accesses that their users have requested, especially during annual UserID certification and it will greater insight for the EUA staff to understand how to best meet your application needs.

This is so that an annual process to reconfirm ISSOs for auditing purposes.