Public and Indian Housing (PIH)
Real Estate Assessment Center (REAC)
Inventory Management System (IMS)
PIC Maintenance Module
Security Administration sub Module

U.S. Department of Housing and Urban Development (HUD)

Prepared by: Quality Software Services, Inc.
Shiva Information Technology Services
# TABLE OF CONTENTS

## 1.0 PIC Maintenance ........................................................................................................... 1-1

## 1.1 Security Administration .............................................................................................. 1-2

1.1.1 Security ....................................................................................................................... 1-2
  1.1.1.1 Displaying Users in the System ............................................................................. 1-4
  1.1.1.2 Searching for existing system users ...................................................................... 1-4
  1.1.1.3 Adding New Users .............................................................................................. 1-5
  1.1.1.4 Modifying and Deleting User Information ............................................................. 1-7
  1.1.1.5 Removing All Roles ............................................................................................. 1-8
  1.1.1.6 Copying Bulk User Data ...................................................................................... 1-9
  1.1.1.7 Security Details .................................................................................................... 1-10
  1.1.1.8 Modify user organization .................................................................................... 1-11

1.1.2 Role Maintenance ........................................................................................................ 1-11

1.1.3 Access Reports ............................................................................................................. 1-13
  1.1.3.1 Displaying User Security Access ......................................................................... 1-13
  1.1.3.2 Generating Privacy Act Data Access Report ......................................................... 1-15
  1.1.3.3 Searching for users globally ................................................................................ 1-17
  1.1.3.4 Viewing User Access by sub Module ................................................................. 1-18

1.1.4 Activity Reports ........................................................................................................... 1-19
  1.1.4.1 Querying User Activity ....................................................................................... 1-20
  1.1.4.2 Viewing New User Reports ................................................................................. 1-21
  1.1.4.3 Viewing Improper Logoff Reports ...................................................................... 1-23
  1.1.4.4 Displaying User Account Usage Reports ............................................................. 1-26

1.1.5 User Certification ......................................................................................................... 1-27
  1.1.5.1 Certifying the Users in the System .................................................................... 1-28
1.0 PIC MAINTENANCE
1.0 PIC MAINTENANCE

The PIC Maintenance module allows the user to maintain certain functions throughout the system. It allows all IMS users to maintain their own personal and contact information by using the User Profile sub module. The Reference sub module is accessible only for Super users. It allows Super users to maintain certain variables in the system, change PIC headlines, maintain PIC email functionality and geographic region data. Only super users can access the Reference sub module. For all other user types, the sub module will not be visible. The Security Administration sub module allows Security Coordinators of different levels to maintain access privileges of various user types and user profiles, view access reports and recertify users so that they could access the system throughout the certification period.
1.1 SECURITY ADMINISTRATION

The Security Administration sub module is a function in the IMS system that allows authorized users to assign, delete or modify access privileges of all users in the PIC system.

The Security Administration sub module consists of five tabs:

- The Security List tab allows the HUD users to add new user accounts to PIC, view and modify existing user accounts, and also delete user accounts.
- The Role Maintenance tab allows the HUD users to view the Role Details and security actions relevant to the system users.
- The Access Reports tab generates reports that list information related to a user’s PIC System access.
- The Activity Reports tab generates reports that list PIC system user activity information.
- The User Certification tab allows HUD users to manage user certifications and re-certifications at the Division and Field Office organizational level.

1.1.1 Security

The hierarchy of users in the IMS system is depicted below. At each user level some users are given administration rights like User management, User certification and recertification and access management etc.

For example, a HUD Security Administrator can certify other users at the Division level, Field Office level and HA level in the system.

The IMS System distinguishes between a Security Administrator/Coordinator and a system user by displaying a % symbol beside the user id. For Example, in Error! Reference source not found., the user M00510 is a user type with Administration rights and M00520 is a user type without any administration rights.
Figure 1: The Security tab displaying users with administration rights.
1.1.1.1 Displaying Users in the System

The Security List sub tab of the Security tab allows the user to access the list of users based on the selected search criteria. Then, the user can select the desired user profile and modify the access privileges.

The Select View list allows users to access the list of users grouped by organization (Field Office user, PHA user, TARC user, etc.) Once the user selects the desired user group in the Select View list by clicking the Select button, a list of user details records are displayed. Also, users under a particular HQ Division belonging to a HUB and appropriate Field Offices can be selected and displayed by the system (see Figure 2).

1.1.1.2 Searching for existing system users

The User Search section of the page allows the user to search for a user profile based on the User ID or Last name of the user. To search for a user based on the user ID, the user must select the User ID option, enter the desired user ID in the Enter Search Text box, and then click Search. To search for a user based on the last name, the user must select the Last Name option, enter the desired user ID in the Enter Search Text box, and then click Search.

The Security List section of the page displays the list of users that matched the search criteria. A user can search other users of the system based on their status. The statuses can be categorized into Active, Inactive or the user can select the All option to view users of both statuses. Active users are users who are allowed to access the system currently. Inactive users are users who have a profile in the system; however, they currently cannot access the system until their profile is set to Active again. The user can select the desired user status in the Select User Status list (See Figure 3).
## 1.0 PIC Maintenance

### 1.1.1.3 Adding New Users

If the user clicks the **Add New User** link (see Figure 3), then the program will display the **Security Details** sub tab with all the controls active allowing the user to enter details of a new user profile. The mandatory controls are marked with an asterisk (*). After the user enters all the required details, the user can click **Create New User** to save the current user profile in the system, or **Cancel** to abort the action (see Figure 4).

When the user selects a user profile, the **Security Summary** sub tab of the **Security** tab is displayed. Depending upon the user type of the user profile different links can show up in the Security Summary.
page. For example, a HUD User can have privileges to add new user. A Guest User may not have such privileges (see Figure 5).

The Security tab displays the following sub tabs:

- The Security List sub tab
- The Security Summary sub tab
- The Bulk Copy sub tab
- The Security Details sub tab
- The Modify User Organization sub tab

The IMS System manages the application access and privileges through a Role Based Security. A role is a set of privileges given to the system user specifying what security actions are allowed. The Security Summary sub tab allows a HUD user to:

- Modify the User Information
- Delete a User from the system
- Remove the Roles assigned to a system user.

Security Summary page displays the user roles based on the selected module and sub module of the system. The user can select the desired module in the Module Name list and the appropriate sub module in the Sub Module Name list. In the View Role list, the user can select one of the available roles to view. The program will display available roles for the selected sub module.

Specific roles are assigned to users for every sub module and entity. For example, if a user needs a read-only access to data for PHA 1, they will not be able to view data for PHA 2. Also, if a user needs high access level (for example, Hub, or Field Office), the user will be able to access all smaller entities that are linked to the entity to which the user has granted the access level. For example, if a user has approval access level to Field Office in New York, the user will have the same access privileges for all the PHAs that report to this Field Office.
### 1.1.1.4 Modifying and Deleting User Information

The **Modify User Info** link in the **Security Summary** sub tab allows the user to modify user information (see Figure 5). Upon clicking the link, the **Security Details** page is displayed. Here, the user can modify various details relevant to the user in the **User Details** section. The mandatory controls are marked with an asterisk (*) (see Figure 6). The user can click the **Submit User Info** button to submit the necessary changes in the system.

![Figure 6: The Security Details page of Security tab](image)

To delete a user profile from the system, a user can click the **Delete User** link in the **Security Summary** sub tab. The **Security Details** page is refreshed displaying a message for the user to confirm permanent deletion of a user profile from the system (see Figure 7).
**1.0 PIC Maintenance**

**Figure 7: Deleting a user from the system**

### 1.1.1.5 Removing All Roles

User can remove all the roles assigned to a system user by clicking the **Remove All Roles** button in the Security Summary sub tab. The Security Summary page is refreshed and a confirmation message is displayed to the user. To permanently remove all the assigned roles, user must click the **Remove All Assigned Roles** button (see Figure 8).

![Figure 8: The Security Summary sub tab of the Security Tab.](image)

When user tries to delete all the assigned roles, all other roles except the User Profile Role is not removed (see Figure 9).

![Figure 9: The Security Summary sub tab of the Security Administration sub module.](image)
1.1.1.6 Copying Bulk User Data

The Bulk Copy page allows the user to copy the access privileges from one user to one or more other users (see Figure 10). It eliminates the extra work required to create access profile for every user of the system. Instead, user can create the access profile for one user and then copy the access privileges to other users of the same function within the program.

To copy the access profile, the user must select the appropriate level in the Bulk Copy option list. This list consists of three options: Module Level, Sub Module Level and User Level.
1.0 PIC Maintenance

The User Level option allows copying the entire user access profile to the selected staff. For example, in the above figure upon clicking the Copy button, the access profile of selected user ID (HHTC01) is copied to user HHTC00 (see Figure 11). The Security Summary sub tab along with a message Successfully Copied Roles is displayed.

The Module Level option of the Bulk Copy Option list allows copying the access profile for a specific module to the selected staff. The Sub Module Level allows copying the access profile for a specific sub module to the selected users. The user can select the desired module in the Module Name list, and the sub module in the Sub Module list. Then, the user must select the staff members to copy the access profile to using the controls in the Resources section. To select the staff members, the user must move the desired users from the Available Staff box to the Copy to Selected Staff box. To copy the access profile after all the users have been selected, the user must click Copy (see Figure 11).

1.1.1.7 Security Details

The Security Details sub tab allows the user to modify the user information. The boxes marked with an asterisk (*) require a mandatory entry by the user (see Figure 12). User can click Submit User Info to submit the changes in the system.
1.0 PIC Maintenance

1.1.1.8 Modify user organization

The Modify User Organization sub tab of the Security tab is a read-only page for the HUD user. User can view the user and organization details in this page (see Figure 13).

![Figure 12: The Security Details Page of the Security Tab.](image)

![Figure 13: The Modify User Organization page of the Security tab.](image)

1.1.2 Role Maintenance

The IMS system manages the application access and privileges through the role based security system. A user can access only the functionality allowed by the roles assigned.
A role can be defined as a set of security actions that can be assigned to users of the system. The Role Maintenance tab of the Security Administration sub module allows HUD user to view the roles assigned to a user type in the system (see Figure 14).

Roles can be searched at module and sub module level. The Module Name, Sub Module Name and User Type controls allow user to select the user type at a module and sub module level.

The Role Search section of the page provides the controls to refine the role search based on the sub module and user type selected. To search by a role name, the Role Name option can be selected and to search by the user who created the role, Creation User option can be selected. The appropriate search text must be entered in the Enter Search Text box.

Using the controls in the User Module List section, the user can view existing roles for a user type. The Role Name column displays the role names as links. The user can click the role name to access the existing role and view the role details. Roles can be categorized as global or local. The local role is only accessible to the user who created it. This role can be assigned to user profiles only by the user who created it. The global roles can be viewed and assigned to user profiles by all authorized users in the IMS system. The table also contains the name of the user who created the role in the Creation User column. The user can sort the existing roles in the table by Role Name, Role Description, G/L (global or local), and Creation User by clicking the appropriate column heading.

A sample role details page is displayed below. It displays the user type at the module and sub module level and also displays the Role Details and the assigned Security Actions for the desired user type (see Figure 15).
1.1.3 Access Reports

IMS System has a functionality to run reports which display user’s security actions. The roles assigned to the users at each module and sub module level can be viewed by the user. The Access Reports page generates reports displaying the access information of each user at the level desired.

1.1.3.1 Displaying User Security Access

The User Security Access sub tab displays a list of roles and actions for a particular user grouped by sub module and at what organizational level these roles are valid (see Figure 16).
The users at a particular level in an organization can be selected using the Select View list. Further users can be narrowed down to a particular office in the HQ Office list by clicking the Select button.

From the user’s list that is displayed with the Select View option, existing users can be searched by either choosing the User ID or Last Name option. The desired search text can be entered in the Enter Search Text box which could be either user ID or last name depending on the option chosen above.

Users can also be searched by status or ID type by selecting an appropriate option in the Select Status list or Select ID Type list. A user can have three statuses: Active, Inactive or All. An active user is one who is currently active in the system; an inactive user is one who has a user profile but is currently inactive in the system. The Select ID Type list is currently no longer functional.

Reports are generated for each user by clicking the desired user ID in the Security List section. The generated User Security Report consists of description of the roles and user’s accesses at the module and sub module level (see Figure 17).
1.0 PIC Maintenance

Figure 17: A Sample User Security Report

The User Security Report consists of

- User Identification section identifying the user in the system.
- User Roles section defining the roles at module and sub module level.
- User Actions section defining the User security actions at the module and sub module level.

1.1.3.2 Generating Privacy Act Data Access Report

The Privacy Act Data Access Report displays the number of times a particular system user accesses the data that is protected by the Privacy Act during one session. These reports are displayed in the Privacy Act Access sub tab of the Access Reports tab of the Security Administration sub module (see Figure 18). The user has to accept the terms and conditions under Privacy Act to access certain data types in IMS. If not, the system will not display the privacy data.
To generate a privacy access report users at the appropriate organization level have to be selected using the *Select View* control. The *Data Filters* section allows the user to select the system users within a desired timeframe. Either one of the predefined options (e.g. *Last one week*, *Last one month*, *Last three months*), or *Custom Dates* option can be selected. To enter custom dates, the user must select the *Custom Dates* option in the *Report Period* list and then enter the actual dates in the *From* and *To* boxes. The dates must be entered in the following format: MM/DD/YYYY. Then, the user must select the desired user type for the program to display. The available options are *HUD User*, *HA User*, *Guest User*, and the *Super User*. The *Tribe/TDHE User* user type is obsolete. If the user selects the *All* option, then the program will display all available user types.

The *Display Filters for Privacy Act Access Report* section of the page allows the user to select how the program will display the report data. The *No of rows to display* list allows the user to select the number of records that the program will display on every report page. Depending on this selection, the report might be several pages or one page if the user selects the *Display all Rows* option. The *Sort report data by* list allows the user to select how the program will sort the records in the report. At this point, the user can sort the records by user name, user ID, and user type. If the user selects the *ASP Page* option, the program will sort the records based on the pages that contained the privacy data accessed by the user. The *Privacy Act Response* option allows the user to sort the records based on the selection that the user made when accessing the IMS system. The *Privacy Act Response Time* option allows the user to sort the records based on the time that the users responded to the Privacy Act Notice when logging in IMS. The *Access Count* option allows the user to sort the records based on the number of times the users accessed privacy data during one session. The *Session Logon/Logoff Timestamp* options allow the user to sort the records based on the time that the user logged in or logged out of IMS. The records can be sorted in
ascending or descending order. To generate a report based on the selection criteria entered by the user, click **Generate Report**. A sample Privacy Act Data Access Report is generated as below (see Figure 19).

![Privacy Act Data Access Report](image)

**1.0 PIC Maintenance**

1.1.3.3 Searching for users globally

The IMS system users can be searched by organization level or globally. The global search of an existing system user can be done in the **Global User Search** sub tab of the **Access Reports** tab (see Figure 20).
1.0 PIC Maintenance

Users can be either searched by user ID or by user first and last name. When searching for users using user ID, the appropriate user ID of the users can be entered in the User-ID(s) box. When the Search Users button in the Search by User ID(s) section is clicked system starts searching the user ID, irrespective of the organization level. Multiple user IDs separated by comma (,) can be entered to search for multiple users. A separate report window is generated displaying the user type, full name, organization and the status of user. For example, when searching for user ID HPIC22 a Global user Search Report is generated (see Figure 21).

To search the users by first or last name at least the first three characters or all the characters of the name can be entered in the Search By First And/Or Last name section of the Global User Search sub tab. For example, to search for the user Test, the text can be entered to generate the desired report.

1.1.3.4 Viewing User Access by sub Module

User can view the accesses of other users of the system at sub module level. This is achieved through the User Access By Sub module page of the Access Reports tab. Reports generated contain role details at the sub module level for users at a particular level in the organization. The Data Filters section allows user to choose the desired sub module to print the report (see Figure 22).
1.0 PIC Maintenance

The generated report displays the list of users at that sub module level, their log on time and their account expiry dates (see Figure 23).

1.1.4 Activity Reports

The IMS System generates reports based on a user’s activity in the system. Users at an organization level can be selected through the Select View list of the page (see Figure 24).
1.1.4.1 Querying User Activity

Existing users can be searched either by user ID or last name by selecting the appropriate option. To perform this search, the user must enter text in the **Enter Search Text** box of the **User Search** section. Users can also be selected based on their status or ID type.

The **Activity Period** section of the **User Activity Query** sub tab enables a user to display user activities within the specified time frame. Dates can be entered in the **From** box and the **To** box to narrow down the user search.

To display user activities of a single user, the respective user ID can be selected in the **User ID** column of the **Security List** section.
The User Activity Information report displays the following information (see Figure 25):

- The **Login** details of a user
- The **Operating System** used
- The **Date** an activity was reported
- Other details, such as web server name, browser version and client IP address, etc

The user can view the report, print the report by clicking the **Print** button, or download the report data in the Excel format by clicking the **Download in Excel** button.

### 1.1.4.2 Viewing New User Reports

IMS system allows users to run reports that display information about new user profiles created in the system. The **New Users** sub tab of the **Activity Reports** tab of the **Security Administration** sub module allows users to view details when a new user was created and given access to the system, and the user’s account expiration details (see Figure 26).
The New Users report can be generated by selecting the organization level in the Select View list of the New Users sub tab. Users are first narrowed down to a Field Office and then to further narrow the search criteria, users can use the options in the Data Filters for New Users Report section. The Data Filters for New Users Report section allows the user to select all the new users who were created within certain time period. The Report Period list allows the user to select the report time frame. The user can either select one of the predefined options (e.g. Last one week, Last one month, Last three months), or select custom dates. To enter custom dates, the user must select the Custom Dates option in the Report Period list and then enter the actual dates in the From and To boxes. The dates must be entered in the following format: MM/DD/YYYY. Then, the user must select the desired user type for the program to display. The available options are HUD User, HA User, Guest User, and the Super User. The Tribe/TDHE User user type is obsolete. If the user selects the All option, then the program will display all available user types.

The Display Filters for New Users Report section allows user to set the way the program will display the report. The No of rows to display list allows the user to select the number of rows to be displayed per page. The Sort report data by list allows the user to select how the program will sort the records in the report. At this point, the user can sort the records by user name, user ID, user type, user creation date/time, account expiry date and creation user ID (user ID of the user who created those profiles). To run a report based on the user search criteria, click on Generate Report button.

A sample report is displayed in Figure 27.
1.0 PIC Maintenance

1.1.4.3 Viewing Improper Logoff Reports

The Improper Logoff sub tab of the Activity Reports tab allows users to run a report displaying all the IMS system users who have been logged out of the system due to various reasons (see Figure 28).
The system users are narrowed down to the Field Office level in the Select View section and Data Filters and Display Filters are applied to narrow the search criteria by timeframe and number of rows to display per page (See Figure 28).

The Improper Logoff report can be run by selecting the organization level in the Select View list of the Improper Logoff sub tab. Users are first narrowed down to a Field Office and then to further narrow the search criteria, users can use the options in the Data Filters for Improper Logoff Report section. The Data Filters for Improper Logoff Report section allows the user to select all the new users who were created within certain time period. The Report Period list allows the user to select the report time frame. The user can either select one of the predefined options (e.g. Last one week, Last one month, Last three months), or select custom dates. To enter custom dates, the user must select the Custom Dates option in the Report Period list and then enter the actual dates in the From and To boxes. The dates must be entered in the following format: MM/DD/YYYY. Then, the user must select the desired user type for the program to display. The available options are HUD User, HA User, Guest User, and the Super User. The Tribe/TDHE User user type is obsolete. If the user selects the All option, then the program will display all available user types.

The Display Filters for Improper Logoff Report section allows user to set the way the program will display the report. The No of rows to display list allows the user to select the number of rows to be displayed per page. The Sort report data by list allows the user to select a sorting criterion for the user records while generating a report.

At this point, the user can sort the records by user name, user ID, user type. The OS Type and Version option allows the user to generate a report where the selection criterion is the type of the operating system.
(for example, Windows/Unix, etc) and the OS version (for example, XP/7 for Windows operating system). With the **Browser Type and Version** a user can sort the user records based on the browser type and version used to log in to the system (or example, Internet Explorer 7/Firefox, etc). The **Log on and Log off Date and Time** allows the user to sort the user records based on the time when the user logged in and logged out of the system. The **Account Expiry Date** option allows user to sort the user records based on when a user’s account will expire or has expired. The **Error Description** option of the **Sort report data by** list allows the user to sort the user records based on the error description (the error that caused improper logoff).

To run a report based on the user search criteria, click on **Generate Report** button (see Figure 29).

Several reasons that contribute to the improper logoff may include (see Figure 29):
- Users are trying to log in again without logging out of the system properly previously.
- User is logged out of the system due to a period of inactivity.
- System Processing failed (For example, Query Failed)

To view the report based on the search criteria entered, click on the **Generate Report** button. A sample Improper Logoff Report is displayed below (see Figure 29).

---

**Improper Logoff Report**

<table>
<thead>
<tr>
<th>#</th>
<th>User Name (First Name, Last Name)</th>
<th>User ID</th>
<th>OS type and version</th>
<th>Browser type and version</th>
<th>Login date &amp; Time</th>
<th>Logoff date &amp; Time</th>
<th>Account Expiry</th>
<th>Error Description</th>
</tr>
</thead>
</table>

*Figure 29: The Improper Logoff Report of the Security Administration sub module*
### 1.1.4.4 Displaying User Account Usage Reports

The User Account Usage sub tab of the Activity Reports tab allows users to run a report displaying users who are inactive in the system (see Figure 30).

![User Account Usage sub tab of the Activity Reports tab](image)

**Figure 30: The User Account Usage sub tab of the Activity Reports tab**

The users can be selected at a Field Office level in the Select View list of the User Account Usage sub tab. Then, users can use the Data Filters for User Account Usage Report section to narrow the search criteria.

To run the User Account Usage Report after making the appropriate selections, user must click the Generate Report button (see Figure 30). A sample User Account Usage report is displayed below (see Figure 31).
1.1.5 User Certification

The IMS system allows Security Administrator to set up roles and actions for users at various levels in the user hierarchy.
1.0 PIC Maintenance

The User Certification tab allows users to accomplish the certification. Following, are the steps that need to be performed by the users to initialize the recertification, email notification process and setting up the roles and actions for users at different levels in the user hierarchy.

- The first step is to initialize the security roles and to assign actions. To certify a user, the Security Coordinator should have the appropriate security actions added to the existing roles or new roles based on the user types. The actions will be added to the appropriate Security Coordinator role so that the Security Coordinators/Administrators at a particular level can certify ALL the users below that level. For Example, the Division Security Administrators/Coordinators can certify all users below that level, i.e Division Users, FO Security Administrators, FO Users, HA Security Administrators and HA Users.
- The Security Coordinators cannot certify themselves or any other security coordinators at their level.
- The user must create security roles and assign actions. New Security Coordinator roles are created for Super users with appropriate actions to certify other users. This will enable each Security Coordinator to certify the users under their level.

Super Users will be certified by the PIH-REAC Security Coordinator.

1.1.5.1 Certifying the Users in the System

The User Certification tab displays the search criteria selected in the Security tab of the Security Administration module. Thus, in order to make changes to the Select View list in the User Certification tab, the Security Administrator has to navigate to the Security tab and make appropriate changes (see Figure 32).

![Figure 32: Setting the users view in the organization](image)

Changes made in Select View section in the Security tab are now reflected in the Select View list of the User Certification tab. In the User Certification tab, the Select Action control allows the Security...
Administrator to select the desired users and certify them. A **Certify Selected Users** button is displayed at the bottom of the **User Certification** tab (see Figure 33).

![Figure 33: The User certification Page of the Security Administration Sub module](image)

To certify the user, the **Certify** check box has to be checked and when the **Certify Selected Users** button is clicked a message is displayed asking the user to confirm the selection (see Figure 34).

![Figure 34: Message Certifying the Users](image)

Upon clicking the **OK** button, the user/users are certified (see Figure 35).
Figure 35: Page Displaying Successful certification of users