



# HUD USER MANUAL

*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

---

# TABLE OF CONTENTS

<b>1.0</b>	<b><i>PIC Maintenance</i></b> .....	<b><i>1-1</i></b>
<b>1.1</b>	<b>Security Administration</b> .....	<b>1-2</b>
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

---

# 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.



## 1.0 PIC Maintenance

---

### 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.



## 1.0 PIC Maintenance

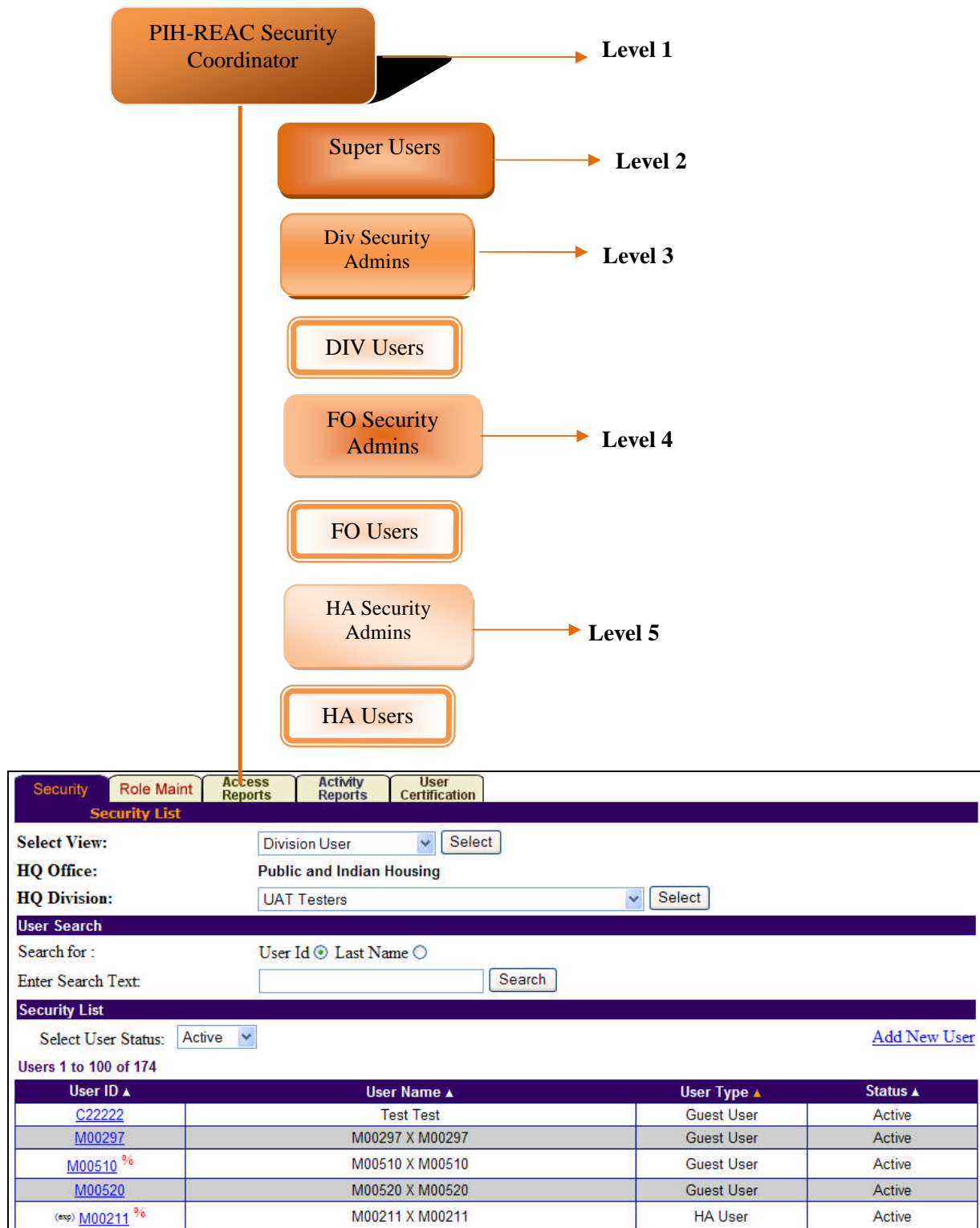


Figure 1: The Security tab displaying users with administration rights.



## 1.0 PIC Maintenance

### 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

User ID	User Name	User Type	Status
M64374	zrsgmbx mlhmzs	HA User	Active
M65801	bzq z bvmvmxn	HA User	Active
MAF058	zlyw h volx	HA User	Active
(exp) MAJ895	vvgloizsx vhrhzm	HA User	Active
MAL148	bxczgh mvhol	HA User	Active

Figure 2: The Security page of the Security Administration sub module

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

User ID ▲	User Name ▲	User Type ▲	Status ▲
C22222	Test Test	Guest User	Active

Figure 3: The Select User Status drop down menu

### 1.1.1.3 Adding New Users

**New user Details**

User Type: \* -- Select User Type --

User Id: \*

First Name: \*

Middle Initial:

Last Name: \*

Email Address: \*

Confirm Email Address: \*

Effective Start Date: \* 5/11/2010 (mm/dd/yyyy)

Expiration Date: \* 5/11/2011 (mm/dd/yyyy)

User Status: \* Active

Comments:

Cancel Create New User

Figure 4: Adding New User functionality

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





## 1.0 PIC Maintenance

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

Role	Level	Entity
Use User Profile	Division User	User Name

Figure 5: The Security Summary sub tab of the Security Administration sub module

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.



## 1.0 PIC Maintenance

### 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.

<b>Security</b>	<b>Role Maint</b>	<b>Access Reports</b>	<b>Activity Reports</b>	<b>User Certification</b>
<b>Security Details</b>				
HQ Office:	Public and Indian Housing			
HQ Division:	UAT Testers			
<b>User Details</b>				
User Id:	M00513			
User Type:	HA User			
First Name:*	<input type="text" value="M00513"/>			
Middle Initial:	<input type="text" value="X"/>			
Last Name:*	<input type="text" value="M00513"/>			
Email Address:*	<input type="text" value="asd@sdsf.com"/>			
Confirm Email Address:*	<input type="text" value="asd@sdsf.com"/>			
Effective Start Date:*	<input type="text" value="10/28/2009"/> (mm/dd/yyyy)			
Expiration Date:*	<input type="text" value="02/02/2011"/> (mm/dd/yyyy)			
User Status:*	<input type="text" value="Active"/>			
Comments:	<input type="text"/>			
		<input type="button" value="Cancel"/> <input type="button" value="Submit User Info"/>		

Figure 6: The Security Details page of Security tab

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).

<b>Security</b>	<b>Role Maint</b>	<b>Access Reports</b>	<b>Activity Reports</b>	<b>User Certification</b>
<b>Security List</b>	<b>Security Summary</b>	<b>Bulk Copy</b>	<b>Security Details</b>	<b>Modify User Organization</b>
HQ Division:	Public and Indian Housing			
HQ Office:	PO Field Operations			
Hub:	2HNYC New York City Hub			
Field Office:	2APH NEW YORK CITY HUB OFFICE			
<b>User Details</b>				
User ID:	H02291			
User Name:	LUIGI D'ANCONA			
User Type:	HUD User			
Are you sure you want to permanently delete this user?				
		<input type="button" value="Delete"/> <input type="button" value="Cancel"/>		



## 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).

The screenshot shows the 'Security Summary' sub tab of the 'Security' tab. The 'User Details' section displays: User ID: M00513, User Name: M00513 X M00513, and User Type: HA User. A confirmation dialog is shown with the text: 'Are you sure you want to remove all roles assigned to this user?'. Below this text is a 'Please note:' section with three bullet points: 'User profile role will not be removed.', 'Existing user roles will be archived prior to removal.', and 'If you wish to view the roles assigned to the selected user please generate corresponding Security Access Report ("Access Reports" business function tab).'. The 'Remove All Assigned Roles' button is highlighted with a red box, and a 'Cancel' button is also visible.

Figure 8: The Security Summary sub tab of the Security Tab.

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

The screenshot shows the 'Security Summary' sub tab of the 'Security' tab. The 'User Details' section displays: UserID: M00513, User Name: M00513 X M00513, and User Type: HA User. The 'User Summary' section displays: Module Name: PIC Maintenance (dropdown), Sub Module Name: User Profile (dropdown), and View Role: Use User Profile (dropdown). A confirmation message is displayed in a green box: 'All roles assigned to the user: M00513 (M00513 X M00513) have been archived and removed (with the exception of User Profile role).'. Below this message is a 'Remove All Roles' button. The 'Records 1 to 1 of 1' section displays a table with the following data:

Role	Level	Entity
Use User Profile	Division User	User Name

The 'Pages' section displays: Pages 1.

Figure 9: The Security Summary sub tab of the Security Administration sub module.



## 1.0 PIC Maintenance

### 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.

The screenshot displays the 'Bulk Copy' sub-tab within the 'Security Administration' module. The top navigation bar includes tabs for 'Security', 'Role Maint', 'Access Reports', 'Activity Reports', and 'User Certification'. The 'Bulk Copy' tab is active, showing a 'Security Summary' section with fields for 'User ID' (H05848), 'User Name' (mvvosgzp ofvp), and 'User Type' (HUD User). Below this is a 'Select Choice' section with three dropdown menus: 'BulkCopy Option' (set to 'Sub-Module Level'), 'Module Name' (set to 'Housing Inventory'), and 'Sub Module Name' (with options 'Housing Agency', 'Development', and 'Inventory Removals'). The 'Resources' section at the bottom features two lists: 'Available Staff' (listing names and IDs like Estep, Charles E(H01426)) and 'Copy to Selected Staff' (an empty list). Navigation arrows (> and <) are between the lists, and a 'Copy' button is at the bottom right.

Figure 10: The Bulk Copy sub tab of the Security Administration Sub module.

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

LOGOFF HUD HOME PIH HOME Q & A SEARCH / INDEX E-MAIL WASS MAIN

Security Role Maint Access Reports Activity Reports User Certification

Security List Security Summary Bulk Copy Security Details Modify User Organization

User ID: HHTC00  
User Name: HHTC00 X HHTC00  
User Type: Super User

Select Choice

BulkCopy Option: User Level

Resources

Available Staff:

- HHTC00, HHTC00 X(HHTC00)
- HPIC04(HMAPS2)
- HPIC04(HMAPS3)
- HPIC04(HMAPS4)
- HPIC04(HMAPS7)
- HPIC04(HMAPS9)
- HPIC04(HPIC01)
- HPIC04(HPIC02)
- HPIC04(HPIC03)
- HPIC04(HPIC06)

Copy to Selected Staff:

- HHTC01(HHTC01)

Copy

Figure 11: Copying the bulk user data.

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

<b>Security</b>	<b>Role Maint</b>	<b>Access Reports</b>	<b>Activity Reports</b>	<b>User Certification</b>
<b>Security Details</b>				
HQ Office:	Public and Indian Housing			
HQ Division:	UAT Testers			
<b>User Details</b>				
User Id:	M00513			
User Type:	HA User			
First Name:*	<input type="text" value="M00513"/>			
Middle Initial:	<input type="text" value="X"/>			
Last Name:*	<input type="text" value="M00513"/>			
Email Address:*	<input type="text" value="asd@sdsf.com"/>			
Confirm Email Address:*	<input type="text" value="asd@sdsf.com"/>			
Effective Start Date:*	<input type="text" value="10/28/2009"/> (mm/dd/yyyy)			
Expiration Date:*	<input type="text" value="02/02/2011"/> (mm/dd/yyyy)			
User Status:*	<input type="text" value="Active"/>			
Comments:	<input type="text"/>			
		<input type="button" value="Cancel"/> <input type="button" value="Submit User Info"/>		

Figure 12: The Security Details Page of the Security Tab.

### 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).

<b>Security</b>	<b>Role Maint</b>	<b>Access Reports</b>	<b>Activity Reports</b>	<b>User Certification</b>
<b>Security List</b>	<b>Security Summary</b>	<b>Bulk Copy</b>	<b>Security Details</b>	<b>Modify User Organization</b>
User ID:	M00513			
User Name:	M00513 X M00513			
User Type:	HA User			
<b>Change User Organization</b>				
Security: HQ Division				
<b>Field Names</b>		<b>Key Value</b>		
HQ Office		Public and Indian Housing		
HQ Division		<input type="text" value="UAT Testers"/>		
<p style="color: red;">This is a read only page.</p>				

Figure 13: The Modify User Organization page of the Security tab.

### 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.





## 1.0 PIC Maintenance

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).

Role Name ▲	Role Description ▲	G/L ▲	Creation User ▲	Role Group
<a href="#">Edit HA Role</a>	This role is allow to view and edit Housing Authority Information	Global	hxdoshi	WASS
<a href="#">Read Only Role</a>	This role is allow to view Housing Authority Information in detail	Global	hxdoshi	WASS
<a href="#">Submit HA Role</a>	Read, edit HA details and view the Development and Building Mapping Reports	Global	H01608	WASS

Figure 14: The Role Maintenance tab of the Security Administration sub module

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).



## 1.0 PIC Maintenance

Security	Role Maint	Access Reports	Activity Reports	User Certification
<b>Role List</b>				
Module Name:	Housing Inventory			
Sub Module Name:	Housing Agency			
User Type:	HA			
<b>Role Details</b>				
Role Name:	Edit HA Role			
Role Description:	This role is allow to view and edit Housing Authority Information			
Role Group:	WASS			
<b>Assigned Actions</b>				
<b>Housing Authority</b>				
<ul style="list-style-type: none"><li>• ReadHAList</li><li>• ReadHADetails</li><li>• ReadSearchHAList</li><li>• ReadHADetails</li><li>• ModifyHADetails</li><li>• ReadHAContactDetails</li><li>• ReadHAAddress</li><li>• CreateHAAddress</li></ul>				

Figure 15: The Role List page of the Role Maintenance tab.

### 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).





## 1.0 PIC Maintenance

Security	Role Maint	Access Reports	Activity Reports	User Certification
<b>User Security Access</b>				
<b>Select View:</b> Division User <input type="button" value="Select"/>				
<b>HQ Division:</b> Public and Indian Housing				
<b>HQ Office:</b> UAT Testers <input type="button" value="Select"/>				
<b>User Search</b>				
Search for: User Id <input checked="" type="radio"/> Last Name <input type="radio"/>				
Enter Search Text: <input type="text"/>				
Select Status: ALL <input type="button" value="v"/>				
Select ID Type: ALL <input type="button" value="v"/>				
<input type="button" value="Search"/>				
<b>Security List</b>				
Users 1 to 50 of 167				
User ID▲	User Name▲	User Type▲	ID Type	Status▲
C22222	Test Test	Guest User	User	Active
HHTC00 %	HHTC00 X HHTC00	Super User	User	Active
HHTC01 %	HHTC01 X HHTC01	Super User	User	Active
HHTC03 %	HHTC03 X HHTC03	Super User	User	Active
HHTC04 %	HHTC04 X HHTC04	Super User	User	Active
HHTC05 %	HHTC05 X HHTC05	Super User	User	Active
HHTC06 %	HHTC06 X HHTC06	Super User	User	Active
HHTC07 %	HHTC07 X HHTC07	Super User	User	Active
HHTC08 %	HHTC08 X HHTC08	Super User	User	Active
HHTC09 %	HHTC09 X HHTC09	Super User	User	Active
HHTC10 %	HHTC10 X HHTC10	Super User	User	Active
HHTC11 %	HHTC11 X HHTC11	Super User	User	Active

Figure 16: The Access Reports tab of the Security Administration sub module

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

### User Security Report

User Identification			
User-id:	C22222	Name (last, first):	Test, Test
Telephone Number:		E-Mail:	test@hud.gov
User Type:	Guest User	User Status:	active
Creation Date :	12/07/2009	Account End Date:	12/07/2010

User Roles				
Module	Sub Module	Role	Level	Entity
PIC Maintenance	User Profile	Use User Profile	Division User	Test, Test
Housing Inventory	Development	Read Only - Privacy	Field Office	SIPH MILWAUKEE PROGRAM CENTER
Housing Inventory	Development	Read Only - Privacy	Field Office	SKPH MINNEAPOLIS HUB OFFICE

### User Actions

PIC Maintenance >> User Profile:

Update User Profile

Housing Inventory >> Development:

Development List View	View	View 1999 Unit Counts Info	View Address Information
View Approval Reports	View Bldg Inventory List	View Building	View Building Information
View Building Reports	View Contact Information	View Data Transfer Page	View Dev Inventory List
View Development Information	View Development List	View Exception List	View Geo Coded Addr Report

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.



## 1.0 PIC Maintenance

Security	Role Maint	Access Reports	Activity Reports	User Certification
User Security Access		Privacy Act Access		Global User Search
User Access by Submodule				
Select View:	HA User <input type="button" value="Select"/>			
HQ Office:	Public and Indian Housing			
HQ Division:	PO Field Operations <input type="button" value="Select"/>			
Hub:	10HSEA Seattle Hub <input type="button" value="Select"/>			
Field Office:	OAPH SEATTLE HUB OFFICE <input type="button" value="Select"/>			
Field Office HA:	AK001 AHFC <input type="button" value="Select"/>			
<b>Data Filters for Privacy Act Access Report</b>				
Report Period:	Custom Dates (From and To dates required) <input type="button" value="Select"/>			
From:	3/16/2010 (mm/dd/yyyy)			
To:	3/31/2010 (mm/dd/yyyy)			
User Types:	ALL <input type="button" value="Select"/>			
<b>Display Filters for Privacy Act Access Report</b>				
No of rows to display:	50 Rows per page <input type="button" value="Select"/>			
Sort report data by:	User Name <input type="button" value="Select"/> in Descending order. <input type="button" value="Select"/>			
<input type="button" value="Generate Report"/>				

Figure 18: The Privacy Act Access page of the Security Administration sub module

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





## 1.0 PIC Maintenance

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).

pic

Privacy Act Data Access Report


[Download in Excel](#)


[Print](#)

HQ Division: **Public and Indian Housing**  
 HQ Office: **PO Field Operations**  
 Hub: **2HNYC New York City Hub**  
 Field Office: **2APH NEW YORK CITY HUB OFFICE**

Report Period: **1/4/2009 to 1/19/2010**  
 Report generation Date: **Tuesday, January 19, 2010 2:15:47 PM**

Users who have attempted to access the Privacy Act data from 1/4/2009 to 1/19/2010

Records 1 - 50 of 457 ([View All](#))

<< Prev page [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) Next Page >>

#	▼ User Name (First, Middle, Last)	User ID	User Type	ASP Page	Privacy Act Response(Y or N)	Privacy Act Response Time	Access Count	Session Logon Timestamp	Session Logoff Timestamp
1	zrsgmbx.n.gstrmpxn	H07614	HUD User	DAP household Search (DAPSearchHousehold.asp)	Y	1/30/2009 2:33:28 PM	4	1/30/2009 2:33:21 PM	1/30/2009 2:37:55 PM
2	zrsgmbx.n.gstrmpxn	H07614	HUD User	DAP household Search (DAPSearchHousehold.asp)	Y	1/30/2009 2:38:07 PM	3	1/30/2009 2:38:02 PM	1/30/2009 3:23:57 PM
3	zrsgmbx.n.gstrmpxn	H07614	HUD User	MTCS Search Page(mtcsearch.asp)	Y	2/25/2009 2:08:49 PM	1	2/25/2009 2:06:10 PM	2/25/2009 6:09:29 PM
4	zrsgmbx.n.gstrmpxn	H07614	HUD User	DAP household Search (DAPSearchHousehold.asp)	Y	2/1/2009 3:16:15 PM	5	2/1/2009 3:15:58 PM	2/1/2009 4:03:31 PM
5	zrsgmbx.n.gstrmpxn	H07614	HUD User	DAP household Search (DAPSearchHousehold.asp)	Y	2/1/2009 4:40:57 PM	8	2/1/2009 4:40:48 PM	2/1/2009 5:39:22 PM
6	zrsgmbx.n.gstrmpxn	H07614	HUD User	DAP household Search (DAPSearchHousehold.asp)	Y	2/1/2009 9:35:07 PM	1	2/1/2009 9:34:56 PM	2/1/2009 10:20:31 PM
7	zrsgmbx.n.gstrmpxn	H07614	HUD User	DAP household Search (DAPSearchHousehold.asp)	Y	2/2/2009 10:54:48 AM	26	2/2/2009 10:54:29 AM	2/2/2009 12:52:29 PM
8	zrsgmbx.n.gstrmpxn	H07614	HUD User	DAP household Search (DAPSearchHousehold.asp)	Y	2/2/2009 2:19:13 PM	48	2/2/2009 2:19:01 PM	2/2/2009 4:44:29 PM

Figure 19: A Sample Privacy Act Data Access Report

### 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

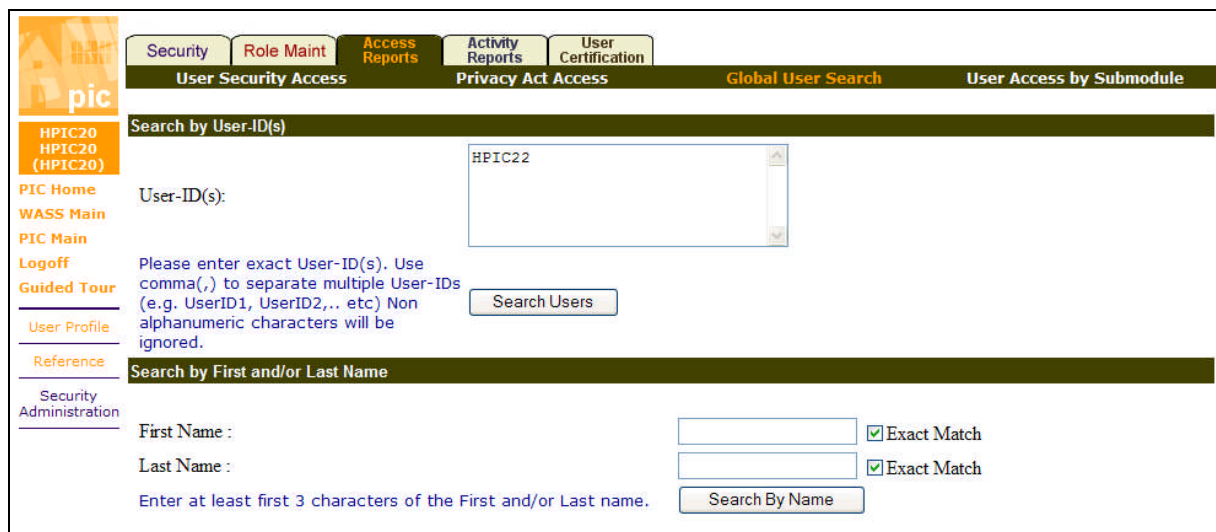
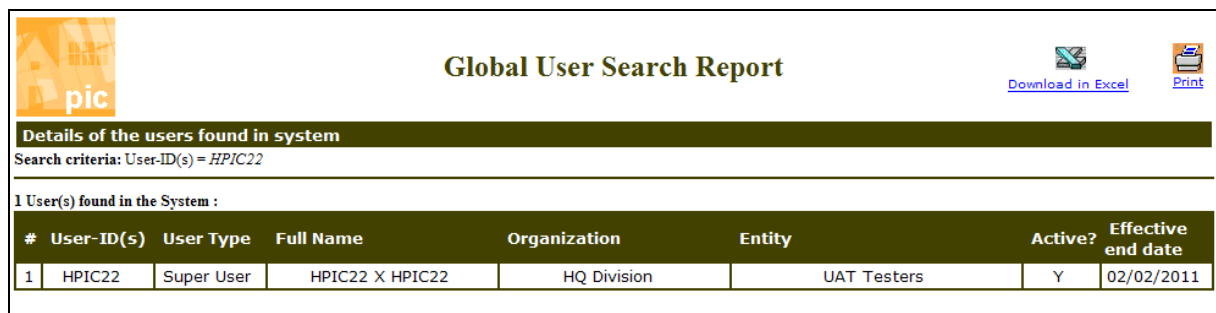


Figure 20: Global User Search page of the Access Reports tab

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).



#	User-ID(s)	User Type	Full Name	Organization	Entity	Active?	Effective end date
1	HPIC22	Super User	HPIC22 X HPIC22	HQ Division	UAT Testers	Y	02/02/2011

Figure 21: A Sample Global User Search Report

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

**pic**

Security Role Maint Access Reports Activity Reports User Certification

User Security Access Privacy Act Access Global User Search User Access by Submodule

Select View: Division User Select

HQ Office: Public and Indian Housing

HQ Division: UAT Testers Select

Data Filters for User Access by Submodule Report

User Types: ALL Select

Select Status: ALL Select

Select Submodule: User Profile Select

Display Filters for User Access by Submodule Report

No of rows to display: 50 Rows per page Select

Sort report data by: User ID Select in Descending order. Select

Generate Report

Figure 22: The User Access By Submodule Page

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).

**pic**

User Access By Submodule Report

Download in Excel Print

HQ Office: Public and Indian Housing

HQ Division: UAT Testers

SubModule Name: User Profile

Report generation Date: Tuesday, April 06, 2010 11:26:46 AM

List of users with access rights to selected submodule.

Records 1 - 37 of 37 << Prev page 1 Next Page >>

User Name (First, Middle, Last)	User ID	User Type	Account Expiry	Logon Date/Time	Created By	User Status
M00509 X M00509	M00509	HA User	02 Feb 2011	2010-04-02 10:27:03.917	UAT5.9	Active
		Role Name			Role Level	
		Use User Profile			Division User	
M00508 X M00508	M00508	HA User	02 Feb 2011	2009-11-20 14:21:21.187	UAT5.9	Active
		Role Name			Role Level	
		Use User Profile			Division User	
M00507 X M00507	M00507	HA User	02 Feb 2011	2009-12-15 10:18:19.373	UAT5.9	Active
		Role Name			Role Level	
		Use User Profile			Division User	

Figure 23: A Sample User Access By Submodule Report

### 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).



## 1.0 PIC Maintenance

<b>Security</b>	<b>Role Maint</b>	<b>Access Reports</b>	<b>Activity Reports</b>	<b>User Certification</b>
<b>User Activity Query</b>		<b>New Users</b>		<b>Improper Logoff</b>
<b>User Account Usage</b>				
Select View:		Division User <input type="button" value="Select"/>		
HQ Office:		Public and Indian Housing		
HQ Division:		UAT Testers <input type="button" value="Select"/>		
<b>User Search</b>				
Search for:		User ID <input checked="" type="radio"/> Last Name <input type="radio"/>		
Enter Search Text:		<input type="text"/>		
Select Status:		ALL <input type="button" value="v"/>		
Select ID Type:		ALL <input type="button" value="v"/>		
<input type="button" value="Search"/>				
<b>Activity Period</b>				
From:		3/13/2010		
To:		4/13/2010		
<b>Security List</b>				
Users 1 to 50 of 174				
<b>User ID▲</b>	<b>User Name▲</b>	<b>User Type▲</b>	<b>ID Type</b>	<b>Status▲</b>
<a href="#">C22222</a>	Test Test	Guest User	User	Active

Figure 24: A User Activity Query page

### 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.





## 1.0 PIC Maintenance

### User Activity Information

Selected View: **Division User**  
HQ Office: **Public and Indian Housing**  
HQ Division: **UAT Testers**  
Report Start Date: **3/6/2010** Report End Date: **4/6/2010**

---

First Name: **HPIC22**  
Last Name: **HPIC22**  
Middle Initial: **X**  
Phone Number:  
Phone Number  
Extn:  
E-Mail Address: **asd@sdsf.com**

  Download in Excel. Print Page.

*Activity Report*

#### Summary Report

Total Connect Time	Total Number of Logins	Average Connect Time
4:19:49	12	0:21:39

#### Detailed Report

Sr No.	Date	Operating System	Browser Name/Version	Client IP Address	Web Server Name	Activity Status	Login Begin	Login End	Total Time Logged On
1	04/05/2010 17:10:21	Windows XP	Internet Explorer 7.0	10.210.43.57	HLANNWT002	ABNRML	04/05/2010 17:10:21	04/05/2010 17:31:24	0:21:3
2	04/05/2010 16:57:21	Windows XP	Internet Explorer 7.0	10.210.43.57	HLANNWT002	ABNRML	04/05/2010 16:57:21	04/05/2010 17:10:03	0:12:42

Figure 25: A Sample User Activity Information Report

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).





## 1.0 PIC Maintenance

The screenshot shows the 'New Users' sub tab of the 'Security Administration' sub module. The interface includes a top navigation bar with tabs: Security, Role Maint, Access Reports, Activity Reports, and User Certification. Below this, there are four main sections: 'User Activity Query', 'New Users', 'Improper Logoff', and 'User Account Usage'. The 'New Users' section is active and contains the following fields:

- Select View:** A dropdown menu set to 'Field Office User' with a 'Select' button.
- HQ Office:** A text field containing 'Public and Indian Housing'.
- HQ Division:** A dropdown menu set to 'PO Field Operations' with a 'Select' button.
- Hub:** A dropdown menu set to '10HSEA Seattle Hub' with a 'Select' button.
- Field Office:** A dropdown menu set to 'OAPH SEATTLE HUB OFFICE' with a 'Select' button.

Below these fields is the 'Data Filters for New Users Report' section, which includes:

- Report Period:** A dropdown menu set to 'Custom Dates (From and To dates required)'.
- From:** A text field containing '3/17/2010' with a '(mm/dd/yyyy)' placeholder.
- To:** A text field containing '4/1/2010' with a '(mm/dd/yyyy)' placeholder.
- User Types:** A dropdown menu set to 'ALL'.

Below the data filters is the 'Display Filters for New Users Report' section, which includes:

- No of rows to display:** A dropdown menu set to '50 Rows per page'.
- Sort report data by:** A dropdown menu set to 'User creation Date/Time' and a secondary dropdown set to 'in Descending order'.

A red box highlights the 'Generate Report' button located at the bottom right of the form.

Figure 26: The New users sub tab of the Security Administration sub module


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



### New Users Report

[Download in Excel](#)[Print](#)

---

HQ Office:

Public and Indian Housing

HQ Division:

PO Field Operations

Hub:

10HSEA Seattle Hub

Field Office:

0APH SEATTLE HUB OFFICE

---

Report Period:

3/22/2008 to 4/6/2010

Report generation Date:

Tuesday, April 06, 2010 10:14:10 AM

New users created between 3/22/2008 and 4/6/2010

Users 1 - 3 of 3

<< Prev page 1 Next Page >>

#	User Name (First, Middle, Last)	User ID	User Type	Creation Date/Time	Account Expiry	Created By
1	mzbi pvixxovm	H45310	HUD User	Oct 17 2008 1:01PM	17 Oct 2012	H01801
2	mvrs nlw	H44848	HUD User	Aug 22 2008 1:17PM	22 Aug 2012	H01801
3	wizsxri y oozd	H23743	HUD User	Jun 9 2008 2:06PM	09 Jun 2012	H01801

Users 1 - 3 of 3

<< Prev page 1 Next Page >>

Figure 27: A Sample New users Report

### 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).



## 1.0 PIC Maintenance

The screenshot displays the 'Improper Logoff' sub-tab within the 'Security Administration' module. The interface includes a sidebar with navigation links and a main content area with several tabs. The 'Improper Logoff' tab is selected, showing a 'Select View' dropdown set to 'Field Office User'. Below this, there are filters for 'HQ Office' (Public and Indian Housing), 'HQ Division' (PO Field Operations), 'Hub' (10HSEA Seattle Hub), and 'Field Office' (OAPH SEATTLE HUB OFFICE). The 'Data Filters for Improper Logoff Report' section includes a 'Report Period' dropdown set to 'Custom Dates (From and To dates required)', with 'From' and 'To' date fields set to '3/22/2010' and '4/6/2010' respectively. The 'User Types' dropdown is set to 'ALL'. The 'Display Filters for Improper Logoff Report' section shows 'No of rows to display' set to '50 Rows per page' and 'Sort report data by' set to 'User Name' in 'Descending order'. A 'Generate Report' button is located at the bottom right of the form.

Figure 28: The Improper Logoff sub tab of the Security Administration sub module

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



## 1.0 PIC Maintenance

(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

[Download in Excel](#)

[Print](#)

HQ Office: **Public and Indian Housing**

HQ Division: **UAT Testers**

Report Period: **3/18/2010 to 4/2/2010**

Report generation Date: **Friday, April 02, 2010 10:41:37 AM**

**Improper logoff's during 3/18/2010 and 4/2/2010**

**Records 1 - 50 of 291** ([View All](#))

<< [Prev page](#) **1** [2](#) [3](#) [4](#) [5](#) [6](#) [Next Page](#) >>

#	▼ User Name (First, Middle, Last)	User ID	User Type	OS type and version	Browser type and version	Logon date & time	Logoff date & time	Account Expiry	Error Description
1	P X G	HPIC12	Super User	Windows XP	Internet Explorer 7.0	3/18/2010 3:39:45 PM	3/22/2010 11:38:06 AM	2/2/2011	7084- User logged-on again without logging out
2	P X G	HPIC12	Super User	Windows XP	Internet Explorer 7.0	3/22/2010 11:38:06 AM	3/22/2010 11:58:22 AM	2/2/2011	7083- Automatic logoff due to timeout
3	P X G	HPIC12	Super User	Windows XP	Internet Explorer 7.0	3/22/2010 2:06:21 PM	3/22/2010 2:27:12 PM	2/2/2011	7083- Automatic logoff due to timeout
4	P X G	HPIC12	Super User	Windows XP	Internet Explorer 7.0	3/22/2010 2:15:01 PM	3/22/2010 2:35:03 PM	2/2/2011	7083- Automatic logoff due to timeout
5	P X G	HPIC12	Super User	Windows XP	Internet Explorer 7.0	3/22/2010 3:34:19 PM	3/22/2010 3:56:10 PM	2/2/2011	7083- Automatic logoff due to timeout
6	P X G	HPIC12	Super User	Windows XP	Internet Explorer 7.0	3/24/2010 5:41:46 AM	3/24/2010 6:03:10 AM	2/2/2011	7083- Automatic logoff due to timeout
7	P X G	HPIC12	Super User	Windows XP	Internet Explorer 7.0	3/24/2010 6:10:03 AM	3/24/2010 6:35:18 AM	2/2/2011	7083- Automatic logoff due to timeout
8	P X G	HPIC12	Super User	Windows XP	Internet Explorer 7.0	3/24/2010 6:25:05 AM	3/24/2010 7:01:20 AM	2/2/2011	7083- Automatic logoff due to timeout
9	P X G	HPIC12	Super User	Windows XP	Internet Explorer 7.0	3/24/2010 11:42:07 AM	3/24/2010 11:42:15 AM	2/2/2011	9504- Query Failed

Figure 29: The Improper Logoff Report of the Security Administration sub module



## 1.0 PIC Maintenance

### 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).

Security Role Maint Access Reports **Activity Reports** User Certification

User Activity Query New Users Improper Logoff **User Account Usage**

Select View: Field Office User Select

HQ Office: Public and Indian Housing

HQ Division: PO Field Operations Select

Hub: 10HSEA Seattle Hub Select

Field Office: OAPH SEATTLE HUB OFFICE Select

Data Filters for User Account Usage Report

User Inactivity Period: Last one week

User Types: Last one week

Select Status: Last one month  
Last three months  
Last six months  
Last one year

Display Filters for User Account Usage Report

No of rows to display: Since beginning of this month  
Since beginning of this Year

Sort report data by: User Name in Descending order

Generate Report

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).




## 1.0 PIC Maintenance



# User Account Usage Report

  
[Download in Excel](#)

  
[Print](#)

HQ Office:Public and Indian Housing

HQ Division:UAT Testers

Report Period:3/26/2010 to 4/2/2010

Report generation Date:Friday, April 02, 2010 12:05:58 PM

List of users who didn't access the system in last one week (3/26/2010 - 4/2/2010).

Records 1 - 50 of 652 (View All) << Prev page 1 2 3 4 5 6 7 8 9 10 11 12 13 14 Next Page >>

▼ User Name (First, Middle, Last)	User ID	User Type	Last Logon Date/Time	Account Expiry Date	User Status
M00508 X M00508	M00508	HA User	2009-11-20 14:21:21.187	02 Feb 2011	Active
	Role Name			Role Level	
	Add New HOH - WASS			HQ Office	
	AMP Change - WASS			HQ Office	
	AMP Change-Local-RH			HQ Office	
	DIS HA Role - WASS			HQ Office	
	Edit Demo-Dispo			HQ Office	
	Edit Development			HQ Office	
	Edit HA Role			HQ Office	
	Edit non-KD Inv - W			HQ Office	
	Edit SEMAP Role			HQ Office	
	Eligibility1			HQ Office	
	Eligibility2			HQ Office	
	HA Certifier - W			HQ Office	
	HA Coordinator			HQ Office	
	HA Recert Sec Adm -			HQ Office	
	Modify Details-WASS			HQ Office	

Figure 31: A Sample User Account Usage Report

### 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).

**Security** | **Role Maint** | **Access Reports** | **Activity Reports** | **User Certification**

**Security List** | **Security Summary** | **Bulk Copy** | **Security Details** | **Modify User Organization**

Select View:

HQ Office:

HQ Division:

**User Search**

Search for : ☐ User Id ☐ Last Name

Enter Search Text:

**Security List**

Select User Status:  [Add New User](#)

Users 1 to 100 of 174

User ID ▲	User Name ▲	User Type ▲	Status ▲
<a href="#">C22222</a>	Test Test	Guest User	Active
<a href="#">H99999</a>	Pawani X G	Super User	Active
(exp) <a href="#">HHTC01</a> %	HHTC01 X HHTC01	Super User	Active
(exp) <a href="#">HHTC04</a> %	HHTC04 X HHTC04	Super User	Active

Figure 32: Setting the users view in the organization

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



## 1.0 PIC Maintenance

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).

#	Certify	User Id	User Name
1	<input type="checkbox"/>	C22222	Test Test
2	<input type="checkbox"/>	HMAPSQ	Testing Testing
3	<input type="checkbox"/>	M00297	M00297 X M00297
4	<input type="checkbox"/>	M00513	M00513 X M00513
5	<input type="checkbox"/>	M00520	M00520 X M00520

Figure 33: The User certification Page of the Security Administration Sub module

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).

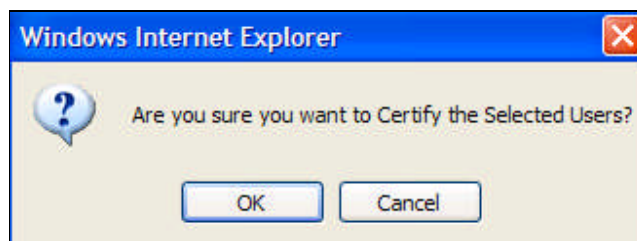


Figure 34: Message Certifying the Users

Upon clicking the **OK** button, the user/users are certified (see Figure 35).





## 1.0 PIC Maintenance

Security

Role Maint

Access Reports

Activity Reports

User Certification

**User Certification**

Select View: Division User

HQ Office: Public and Indian Housing

HQ Division: UAT Testers

Select Action: Certify Super users

User list filter: All Users

Select Users for Certification

Selected users have been successfully certified!

Showing user records: 101 To 115 of 115

#	Certify	User Id	User Name
101	<input checked="" type="checkbox"/>	HPIC03	HPIC03 X HPIC03
102	<input type="checkbox"/>	HPIC06	HPIC06 X HPIC06
103	<input type="checkbox"/>	HPIC09	HPIC09 X HPIC09

Figure 35: Page Displaying Successful certification of users