



# HOUSING AUTHORITY 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 .....	1-3
1.1.1.1	Displaying Users in the System.....	1-3
1.1.1.2	Searching for existing system users .....	1-4
1.1.1.3	Adding New Users .....	1-6
1.1.1.4	Modifying User Information .....	1-7
1.1.1.5	Modifying Special Privileges for a user .....	1-8
1.1.1.6	Removing All Existing Roles For a User .....	1-9
1.1.1.7	Security Details .....	1-10
1.1.1.8	Modify user organization .....	1-10
1.1.2	Role Maintenance .....	1-10
1.1.3	Access Reports.....	1-12
1.1.3.1	Displaying User Security Access .....	1-12
1.1.3.2	Generating Privacy Act Data Access Report.....	1-14
1.1.3.3	Searching for users globally .....	1-16
1.1.3.4	Viewing User Access by sub Module .....	1-17
1.1.4	Activity Reports.....	1-19
1.1.4.1	Querying User Activity .....	1-20
1.1.4.2	Viewing New User Reports.....	1-22
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

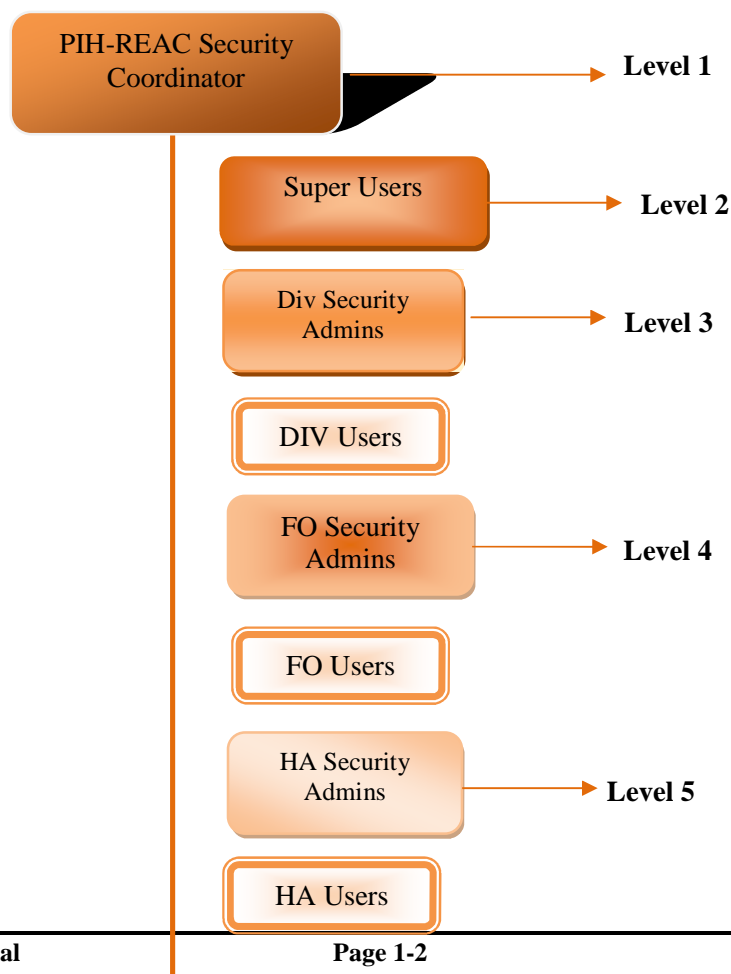
### 1.1 SECURITY ADMINISTRATION

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 HA users to add new user accounts to PIC, view and modify user information and remove all the roles associated to a user type.
- The **Role Maintenance** tab allows the HA users to view the roles assigned to a user at a module and sub module level. The system will display this tab only if the user has sufficient access privileges.
- 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 HA users to manage user certifications and re-certifications of other HA users in the system.

The hierarchy of the users in the IMS System is displayed below.





## 1.0 PIC Maintenance

Each user level has a user Security Administrator and user of the system. Security Administrators are system users with special administration rights like User management, User certification and recertification and access management etc.

For example, a HA Security Administrator can certify other HA users 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 Figure 1, the user M00510 is a user type with Administration rights and M00520 is a user type without any administration rights.

User ID ▲	User Name ▲	User Type ▲	Status ▲
<a href="#">C22222</a>	Test Test	Guest User	Active
<a href="#">M00297</a>	M00297 X M00297	Guest User	Active
<a href="#">M00510 %</a>	M00510 X M00510	Guest User	Active
<a href="#">M00520</a>	M00520 X M00520	Guest User	Active
<a href="#">(exp) M00211 %</a>	M00211 X M00211	HA User	Active

Figure 1: Distinguishing Security Administrators and other users of the system.

### 1.1.1 Security

#### 1.1.1.1 Displaying Users in the System

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

The **Select View** list allows coordinators to access the list of users grouped by organization (Field Office user, PHA user, TARC user, etc.) Once the coordinator 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).



## 1.0 PIC Maintenance

### 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 bvmimrxn	HA User	Active
MAF058	ziyww h volx	HA User	Active
(exp) MAI895	vggloizsx vhrhzm	HA User	Active
MAL148	bxzgh mvhol	HA User	Active

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

The **User Search** section of the page allows the coordinator 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 coordinator 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 coordinator 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 coordinator 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).

User ID	User Name	User Type	Status
(exp) M64374	zrsgmbx mlhmzs	HA User	Active
M65801	bzq z bvmimrxn	HA User	Active
MAF058	ziyww h volx	HA User	Active
(exp) MAI895	vggloizsx vhrhzm	HA User	Active



## 1.0 PIC Maintenance

Figure 3: The Select User Status drop down menu

When the coordinator 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 HA Security Administrator can have privileges to modify role. A Guest User may not have such privileges (see Figure 4).

The **Security** tab displays the following sub tabs.

- The **Security List** sub tab
- The **Security Summary** sub tab
- The **Security Details** sub tab
- The **Modify User Organization** sub tab

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

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

UserID: HHTC05  
User Name: HHTC05 X HHTC05  
User Type: Super User

[Modify User Info](#)  
[Modify Special Privilege](#)  
[Modify User Type](#)

**User Summary**

Module Name: PIC Maintenance [Select]  
Sub Module Name: User Profile [Select]

View Role: Use User Profile [Select]

[Remove All Role](#)

Records 1 to 1 of 1

Role	Level	Entity
Use User Profile	Division User	HHTC05

Pages 1

Figure 4: 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 HA Coordinator to modify user information and remove roles for a particular user of the system. It displays the user roles based on the selected module and sub module of the system. The HA 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

### 1.1.1.3 Adding New Users

The screenshot shows a web application interface for adding a new user. At the top, there are tabs: Security, Role Maint, Access Reports, Activity Reports, and User Certification. The 'Security' tab is selected, and the sub-tab is 'Security Details'. Below this, there are fields for 'HQ Division' (Public and Indian Housing) and 'HQ Office' (UAT Testers). The main section is titled 'New user Details' and contains several input fields. The 'User Type' field is a dropdown menu currently showing '-- Select User Type --'. The 'User Id' field is a text box. The 'First Name', 'Middle Initial', and 'Last Name' fields are text boxes. The 'Email Address' and 'Confirm Email Address' fields are text boxes. The 'Effective Start Date' and 'Expiration Date' fields are date pickers showing 5/11/2010 and 5/11/2011 respectively, with a format hint '(mm/dd/yyyy)'. The 'User Status' field is a dropdown menu showing 'Active'. The 'Comments' field is a large text area. At the bottom right, there are two buttons: 'Cancel' and 'Create New User'. The 'Create New User' button is highlighted with a red box.

Figure 5: 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 5).

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 4).

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



## 1.0 PIC Maintenance

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

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

UserID: M00513 [Modify User Info](#) [Delete User](#)

User Name: M00513 X M00513

User Type: HA User

**User Summary**

Module Name: PIC Maintenance

Sub Module Name: User Profile

View Role: Use User Profile  [Remove All Roles](#)

Records 1 to 1 of 1

Role	Level	Entity
Use User Profile	Division User	User Name

Pages 1

Figure 6: 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.

### 1.1.1.4 Modifying User Information

The **Modify User Info** link in the **Security Summary** sub tab allows the coordinator to modify user information (see Figure 4). Upon clicking the link, the **Security Details** page is displayed. Here, the coordinator can modify various details relevant to the user in the **User Details** section. The mandatory controls are marked with an asterisk (\*). The user type of the user can be modified using the **Modify** link (See Figure 7).



## 1.0 PIC Maintenance

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

**Security Details**

HQ Division: Public and Indian Housing  
HQ Office: UAT Testers

**User Details**

User Id: HHTC03  
User Type: Super User [Modify]  
First Name: HHTC03  
Middle Initial: X  
Last Name: HHTC03  
Email Address: asd@sdsf.com  
Confirm Email Address: asd@sdsf.com  
Effective Start Date: 10/28/2009 (mm/dd/yyyy)  
Expiration Date: 02/02/2010 (mm/dd/yyyy)  
User Status: Active  
Comments:  
[Cancel] [Submit User Info]

Figure 7: The Security Details page of Security tab

Upon clicking the **Modify** link, the **Security Details** sub tab gets refreshed and displays a **User Details** section where the coordinator can add comments specifying the reason for changing the user type. Once the **Submit User Type Change** button is clicked (see Figure 8), the necessary changes are saved. To navigate back to the Security Summary tab user can click the **Cancel** button.

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

**Security Details**

HQ Division: Public and Indian Housing  
HQ Office: UAT Testers

**User Details**

User Id: HHTC03  
User Type: Super User  
Name: HHTC03 X HHTC03  
Comments:  
Please note : All the roles assigned to the selected user will be removed as a result of user type change.  
[Cancel] [Submit User Type Change]

Figure 8: The Security Details page of the Security Tab

### 1.1.1.5 Modifying Special Privileges for a user

The **Security Summary** sub tab consists of a functionality to modify the special privileges for a user. This means the selected user can view the private data like SSN in the system. The **View Unmasked Privacy Data** box must be checked and the **Save Special Privileges** button must be clicked to give the user system-wide special privileges (see Figure 9). The **Back To User Security Summary** link allows user to navigate back to the Security Summary page of the sub module.



## 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

UserID: HHTC00  
User Name: HHTC00 X HHTC00  
User Type: Super User

Special Systemwide Privileges

☒ View Unmasked Privacy Data.

Cancel Save Special privileges

<< Back to User Security Summary

Figure 9: Giving Special System-wide Privileges to the user

### 1.1.1.6 Removing All Existing Roles For a User

The Security Summary sub tab of the Security Administration sub module allows the administrator to remove all the roles assigned to a system user. The **Remove All Roles** in figure 3 allows user to perform the removal actions. When user clicks this link, the Security Summary page gets refreshed and coordinator can click the **Remove All Assigned Roles** button

Security Role Maint Access Reports Activity Reports User Certification

Security List Security Summary Security Details Modify User Organization

HQ Office: Public and Indian Housing  
HQ Division: UAT Testers

User Details

User ID: HHTC05  
User Name: HHTC05 X HHTC05  
User Type: Super User

Are you sure you want to remove all roles assigned to this user?

Remove All Assigned Roles Cancel

Please note:

- User profile role will not be removed.
- Existing user roles will be archived prior to removal.
- If you wish to view the roles assigned to the selected user please generate corresponding Security Access Report ("Access Reports" business function tab).

Figure 10: Removing roles for a system user.



## 1.0 PIC Maintenance

### 1.1.1.7 Security Details

The screenshot shows the 'Security Details' page for user HHTC04. The page has a purple header with tabs: Security, Role Maint, Access Reports, Activity Reports, and User Certification. The 'Security' tab is selected. Below the header, the page is divided into sections: 'Security Details' (HQ Office: Public and Indian Housing, HQ Division: UAT Testers) and 'User Details' (User Id: HHTC04, User Type: Super User with a [Modify] link, First Name: HHTC04, Middle Initial: X, Last Name: HHTC04, Email Address: asd@sdsf.com, Confirm Email Address: asd@sdsf.com, Effective Start Date: 10/28/2009, Expiration Date: 02/02/2010, User Status: Active, and a Comments text area). At the bottom are 'Cancel' and 'Submit User Info' buttons.

Figure 11: 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 HA Security Administrator (see Figure 12). No actions can be performed by the administrator in this page.

The screenshot shows the 'Modify User Organization' page for user HHTC01. The page has a purple header with tabs: Security, Role Maint, Access Reports, Activity Reports, and User Certification. The 'Security' tab is selected. Below the header, the page is divided into sections: 'Security List' (User ID: HHTC01, User Name: HHTC01 X HHTC01, User Type: Super User), 'Security Summary', 'Security Details', and 'Modify User Organization'. The 'Modify User Organization' section has a 'Change User Organization' sub-section with a table showing 'Field Names' and 'Key Value'. The table has two rows: 'HQT Office' with value 'Public and Indian Housing' and 'HQT Division' with value 'PCF OAFBC, Section 8 Financial Management Center'. At the bottom, a red box contains the text 'This is a read only page.'

Figure 12: Copying one user profile to another profile

## 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 coordinator to view the roles of the system users (see Figure 13).

Role Name ▲	Role Description ▲	G/L ▲	Creation User ▲
<a href="#">Read Only Role</a>	HA Guest User (WASS) This role allows guest user to view Housing Authority information in detail.	Global	hxdoshi

Figure 13: The Role Maintenance tab of the Security Administration sub module

Roles for a system user can be view at module and sub module level. The **Module Name**, **Sub Module Name** and **User Type** controls allow user to create roles for 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.

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 (See Figure 13).

To view the role details and actions associated to a user, click the name of the role in the **Role Name** column. The **Role Details** section allows the user to view a description of the role as it would display in the **Role Description**. The security actions associated with a user are displayed in the **Assigned Actions** section of the Role List sub tab (see Figure 14).



## 1.0 PIC Maintenance

Security	<b>Role Maint</b>	Access Reports	Activity Reports	User Certification
<b>Role List</b>				
Module Name:		Housing Inventory		
Sub Module Name:		Housing Agency		
User Type:		GUEST		
<b>Role Details</b>				
Role Name:		Read Only Role		
Role Description:		HA Guest User (WASS) This role allows guest user to view Housing Authority information in detail.		
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>• ReadHAContactDetails</li><li>• ReadHAAddress</li><li>• ReadHAInventory</li><li>• ReadHAPerformance</li><li>• ReadHAFunding</li></ul>				

Figure 14: Assigning Roles to a user in the system

To navigate back to the role list display, administrator can click on the **Role List** sub 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 15).



## 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="Select"/>				
Select ID Type: ALL <input type="button" value="Select"/>				
<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 15: 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 16).



## 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 16: 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.

(See Figure 16)

### 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 17). 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 17: 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 coordinator to select how the program will display the report data. The **No of rows to display** list allows the coordinator to select the number of records that the program will display on every 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 coordinator to sort the records based on the selection that was made when accessing the IMS system. The **Privacy Act Response Time** option allows the coordinator 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 coordinator 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 coordinator to sort the records based on the time that the user logged in or





## 1.0 PIC Maintenance

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 18).



# Privacy Act Data Access Report


[Download in Excel](#)


[Print](#)

HQ Division:

HQ Office:

Hub:

Field Office:

Public and Indian Housing

PO Field Operations

2HNYC New York City Hub

2APH NEW YORK CITY HUB OFFICE

Report Period:

Report generation Date:

1/4/2009 to 1/19/2010

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 gstmpxn	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 gstmpxn	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 gstmpxn	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 gstmpxn	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 gstmpxn	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 gstmpxn	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 gstmpxn	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 gstmpxn	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 18: 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 19).

## 1.0 PIC Maintenance

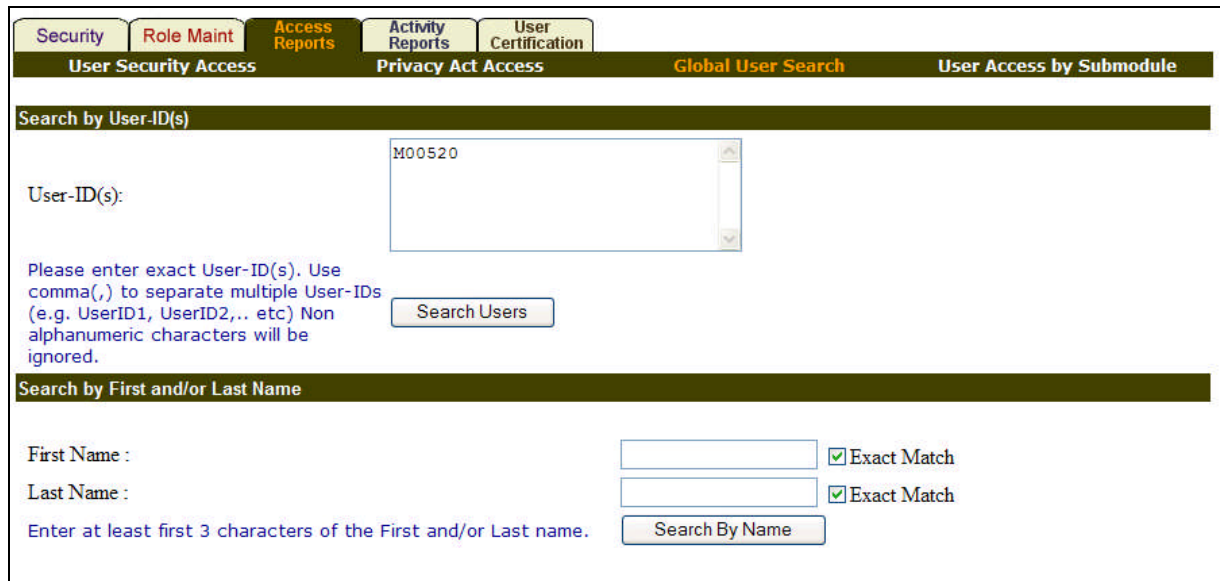
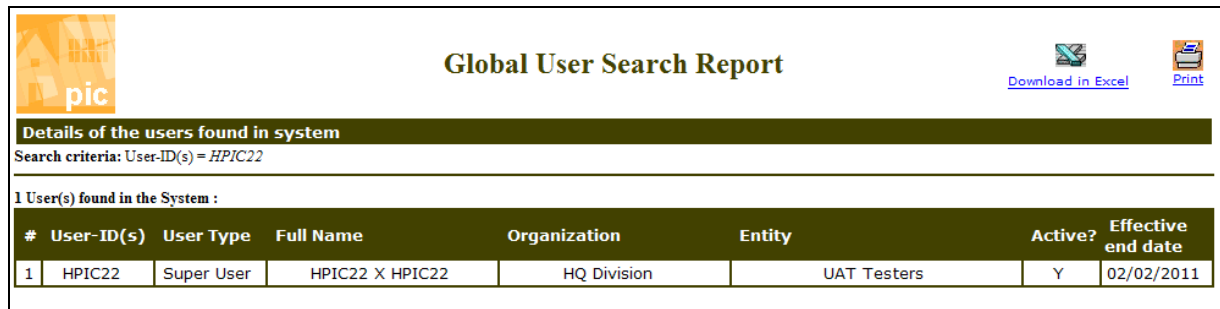


Figure 19: Global User Search page of the Access Reports tab

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 20).



#	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 20: 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

HA Security Administrator 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 21).



## 1.0 PIC Maintenance


Security	Role Maint	Access Reports	Activity Reports	User Certification
User Security Access		Privacy Act Access		Global User Search
<b>User Access by Submodule</b>				
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:	0CPH ALASKA COMMUNITY SERVICE CENTER <input type="button" value="Select"/>			
Field Office HA:	AK001 AHFC			
<b>Data Filters for User Access by Submodule Report</b>				
User Types:	HA User <input type="button" value="Select"/>			
Select Status:	ALL <input type="button" value="Select"/>			
Select Submodule:	User Profile <input type="button" value="Select"/>			
<b>Display Filters for User Access by Submodule Report</b>				
No of rows to display:	50 Rows per page <input type="button" value="Select"/>			
Sort report data by:	User ID <input type="button" value="Select"/> in Descending order. <input type="button" value="Select"/>			
<input type="button" value="Generate Report"/>				

Figure 21: 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 22).



## 1.0 PIC Maintenance



### User Access By Submodule Report

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

---

HQ Office: Public and Indian Housing  
HQ Division: PO Field Operations  
Hub: 10HSEA Seattle Hub  
Field Office: OCPH ALASKA COMMUNITY SERVICE CENTER  
Field Office HA: AK001 AHFC

---

SubModule Name: User Profile  
Report generation Date: Monday, April 12, 2010 10:26:54 AM

---

List of users with access rights to selected submodule.

Records 1 - 25 of 25 << Prev page 1 Next Page >>

User Name (First, Middle, Last)	User ID	User Type	Account Expiry	Logon Date/Time	Created By	User Status
ziyvw mzsgz	MZ2189	HA User	20 Jun 2010	2008-09-19 11:53:08.140	M59111	Inactive
		Role Name		Role Level		
		Use User Profile		HA User		
mzhfh vmlsxn-hwmlnnrh	MW2857	HA User	31 Jan 2010	2008-01-30 13:10:41.890	M59111	Active
		Role Name		Role Level		
		Use User Profile		HA User		
vrofq bvori	MV9576	HA User	29 Feb 2008	2008-02-07 21:08:59.577	saayers	Inactive
		Role Name		Role Level		
		Use User Profile		HA User		
zmzrw vwfsu	MV0318	HA User	16 Jun 2007	2006-07-21 18:37:43.827	saayers	Inactive
		Role Name		Role Level		
		Use User Profile		HA User		
biltvit wlld	MU9289	HA User	01 Jun 2010	2009-05-22 17:12:30.500	smolmste	Active
		Role Name		Role Level		

Figure 22: 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 23).



## 1.0 PIC Maintenance

Security	Role Maint	Access Reports	Activity Reports	User Certification
<b>User Activity Query</b>				
New Users				
Improper Logoff				
User Account Usage				
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: OCPH ALASKA COMMUNITY SERVICE CENTER <input type="button" value="Select"/>				
Field Office HA: AK001 AHFC				
<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: 3/12/2010				
To: 4/12/2010				
<b>Security List</b>				
Users 1 to 45 of 45				
<b>User ID▲</b>	<b>User Name▲</b>	<b>User Type▲</b>	<b>ID Type</b>	<b>Status▲</b>
M64374	zrsgmbx mlhmzs	HA User	User	Active

Figure 23: 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

Selected View:	<b>HA User</b>	
HQ Office:	<b>Public and Indian Housing</b>	
HQ Division:	<b>PO Field Operations</b>	
Hub:	<b>10HSEA Seattle Hub</b>	
Field Office:	<b>0CPH ALASKA COMMUNITY SERVICE CENTER</b>	
Field Office HA:	<b>AK001 AHFC</b>	
Report Start Date:	<b>3/12/2005</b>	Report End Date: <b>4/12/2010</b>

First Name:	<b>bzq</b>
Last Name:	<b>bvmivmrnxn</b>
Middle Initial:	<b>z</b>
Phone Number:	
Phone Number Extn:	
E-Mail Address:	<b>hf.pz.vgzgh.xusz@mivmrnxnq</b>



Download in Excel. Print Page.

*Activity Report*

**Summary Report**

Total Connect Time	Total Number of Logins	Average Connect Time
0:25:7	1	0:25:7

**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	09/28/2007 20:50:47	Windows XP	Internet Explorer 6.0	205.159.28.1	HLANNWP004	ABNRML	09/28/2007 20:50:47	09/28/2007 21:15:54	0:25:7

Figure 24: A Sample User Activity Information Report

The User Activity Information report displays the following information (See Figure 24):

- 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.



## 1.0 PIC Maintenance

### 1.1.4.2 Viewing New User Reports

IMS system allows coordinators 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 coordinators to view details when a new user was created and given access to the system, and the user's account expiration details (see Figure 25).

The screenshot displays the 'New Users' sub-tab within the 'Security Administration' module. The interface features a top navigation bar with tabs for 'Security', 'Role Maint', 'Access Reports', 'Activity Reports', and 'User Certification'. The 'Activity Reports' tab is selected, and the 'New Users' sub-tab is active. Below the navigation bar, there are several sections for filtering and generating reports. The 'Select View' section includes a dropdown menu set to 'Field Office User' and a 'Select' button. The 'HQ Office' field is set to 'Public and Indian Housing'. The 'HQ Division' dropdown is set to 'PO Field Operations' with a 'Select' button. The 'Hub' dropdown is set to '10HSEA Seattle Hub' with a 'Select' button. The 'Field Office' dropdown is set to 'OAPH SEATTLE HUB OFFICE' with a 'Select' button. Below these fields is the 'Data Filters for New Users Report' section, which includes a 'Report Period' dropdown set to 'Custom Dates (From and To dates required)', 'From' and 'To' date boxes (3/17/2010 and 4/1/2010), and a 'User Types' dropdown set to 'ALL'. At the bottom is the 'Display Filters for New Users Report' section, which includes a 'No of rows to display' dropdown set to '50 Rows per page' and a 'Sort report data by' dropdown set to 'User creation Date/Time' with a secondary dropdown set to 'in Descending order'. A 'Generate Report' button is located at the bottom right of the form, highlighted with a red border.

Figure 25: 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 coordinator 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 coordinator 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 coordinator 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 coordinator 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 **All** option is selected by the coordinator, then the program will display all available user types.

The **Display Filters for New Users Report** section allows coordinator to set the way the program will display the report. The **No of rows to display** list allows coordinator to select the number of rows to be displayed per page. With the **Sort report data by** list coordinator can select how the program will sort the records in the report. At this point, the coordinator 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



## 1.0 PIC Maintenance

those profiles). To run a report based on the user search criteria, click on **Generate Report** button (See Figure 25).

A sample report is displayed in Figure 26.

#	User Name (First, Middle, Last)	User ID	User Type	Creation Date/Time	Account Expiry	Created By
1	mzbi pvizxovm	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

Figure 26: 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 27).



## 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 fields for 'HQ Office' (Public and Indian Housing), 'HQ Division' (PO Field Operations), 'Hub' (10HSEA Seattle Hub), and 'Field Office' (OAPH SEATTLE HUB OFFICE). A 'Data Filters for Improper Logoff Report' section includes a 'Report Period' dropdown set to 'Custom Dates', 'From' and 'To' date fields (3/22/2010 and 4/6/2010), and a 'User Types' dropdown set to 'ALL'. A 'Display Filters for Improper Logoff Report' section includes a 'No of rows to display' dropdown set to '50 Rows per page' and a 'Sort report data by' dropdown set to 'User Name' with a secondary dropdown set to 'in Descending order'. A 'Generate Report' button is located at the bottom right.

Figure 27: 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 27).

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 coordinator to select all the new users who were created within certain time period. The **Report Period** list allows the coordinator to select the report time frame. The coordinator can select either 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 **Custom Dates** option in the **Report Period** list can be selected and then actual dates can be entered in the **From** and **To** boxes. The dates must be entered in the following format: MM/DD/YYYY. Then, the desired user type can be selected. 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 coordinator to set the way the program will display the report. The **No of rows to display** list allows the coordinator to select the number of rows to be displayed per page. The **Sort report data by** list helps in selecting a sorting criterion for the user records while generating a report.

At this point, the coordinator 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



## 1.0 PIC Maintenance

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** the user records can be sorted 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 coordinator 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 coordinator 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 coordinator 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 27).

Several reasons that contribute to the improper logoff may include (see Figure 28):

- 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.

## 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 28: 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 Security coordinators to run a report displaying users who are inactive in the system (see Figure 29).

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

Display Filters for User Account Usage Report

No of rows to display: Since beginning of this month

Sort report data by: User Name in Descending order

Generate Report

Figure 29: 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, coordinators 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, the security coordinator must click the **Generate Report** button (see Figure 29).



## 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 30: A Sample User Account Usage Report

### 1.1.5 User Certification

The IMS system allows HA Security Administrator/Coordinator to set up roles and actions for HA users in the user hierarchy.



## 1.0 PIC Maintenance

The **User Certification** tab allows HA Security Coordinators to accomplish the certification (see Figure 32). It displays the HUB and Field Office Housing Authority details. The **Select Action** section of the tab displays a list which allows HA administrator to certify other HA Security administrators and HA users.

### 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 31).

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

**Security List**

Select View: HA User

HQ Office: Public and Indian Housing

HQ Division: PO Field Operations

Hub: 3HPIT Pittsburgh Hub

Field Office: 3EPH PITTSBURGH HUB OFFICE

Field Office HA: PA001 Pittsburgh HA

**User Search**

Search for : User Id ☒ Last Name ☐

Enter Search Text:

**Security List**

Select User Status: Active

Users 1 to 36 of 36

User ID ▲	User Name ▲	User Type ▲	Status ▲
<a href="#">M59236</a> %	biizo d pmzsh	HA User	Active
<a href="#">MA2384</a> %	ovzsxm bvozvsh	HA User	Active
<a href="#">MAQ080</a>	riivg o wo	HA User	Active
(exp) <a href="#">MAU915</a>	bxmzm nlgzvsx	HA User	Active
<a href="#">MAU920</a>	zbmlg mizvs	HA User	Active

Figure 31: 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 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 32).



## 1.0 PIC Maintenance

#	Certify	User Id	User Name
1	<input checked="" type="checkbox"/>	M59236	biizo d pmzsh
2	<input type="checkbox"/>	MA2384	ovzsxm bvozvsh
3	<input type="checkbox"/>	MM8222	ivsgzvs hvmrzt
4	<input type="checkbox"/>	MV7155	biizo wlvox xn

Figure 32: 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 33).

#	Certify	User Id	User Name
1	<input checked="" type="checkbox"/>	M59236	biizo d pmzsh
2	<input type="checkbox"/>	MA2384	ovzsxm bvozvsh
3	<input checked="" type="checkbox"/>	MM8222	ivsgzvs hvmrzt
4	<input type="checkbox"/>	MV7155	biizo wlvox xn

Figure 33: Message Certifying the Users

Upon clicking the **OK** button, the user/users are certified (see Figure 34).



## 1.0 PIC Maintenance

Security

Role Maint

Access Reports

Activity Reports

User Certification

User Certification

Select View: FO HA User  
HQ Office: Public and Indian Housing  
HQ Division: PO Field Operations  
Hub: 3HPIT Pittsburgh Hub  
Field Office: 3EPH PITTSBURGH HUB OFFICE  
Field Office HA: PA001 Pittsburgh HA

Select Action: Certify HA Security Administrators Select...

User list filter: All Users Refresh

Select Users for Certification

Selected users have been successfully certified!

Showing user records: 1 To 4 of 4

#	Certify	User Id	User Name
1	✓	M59236	büzo d pmzsh
2	☐	MA2384	ovzsxm bvozvsh
3	✓	MM8222	ivsgzvs hvmrzt
4	☐	MV7155	büzo wlvox xn

☐ Select all users on this page

Certify Selected Users

Figure 34: Page Displaying Successful certification of users