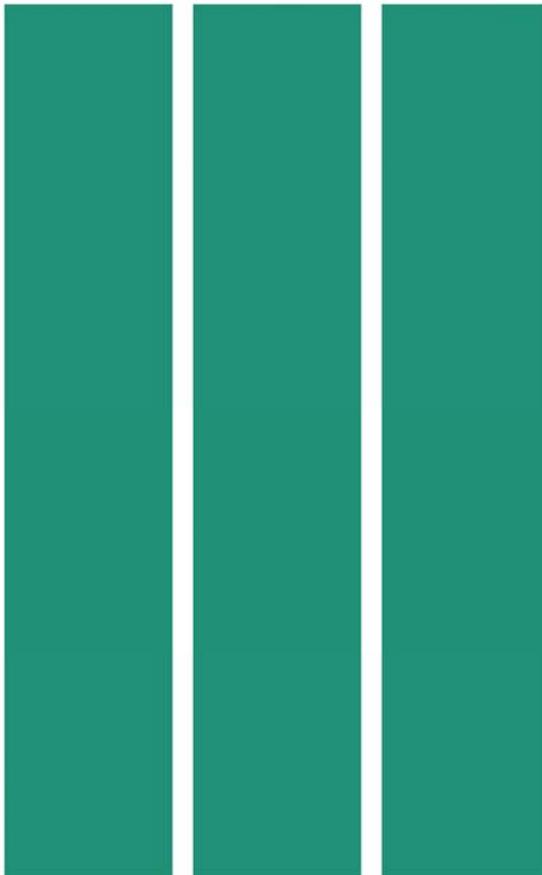


PIH Information Center

HUD PIC

Security Administration

Business
Partners



User Manual
March 2006

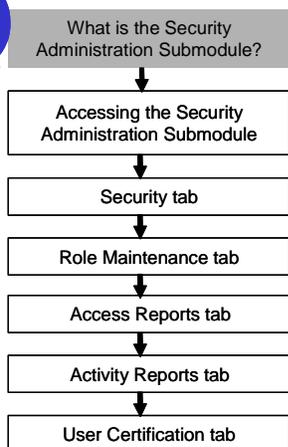
Contents

1.	What is the Security Administration Submodule?.....	1-1
	Security Administration submodule overview.....	1-1
	User manual objectives.....	1-2
	User manual audience.....	1-2
	Acknowledgements.....	1-2
	Entering information in the Security Administration submodule...	1-3
	Security Coordinator principles and guidelines.....	1-4
2.	Accessing the Security Administration Submodule	2-1
	Overview.....	2-1
	Accessing the PIC system with a PIC ID.....	2-2
	Accessing the PIC system through WASS	2-4
	Navigating to the Security Administration submodule.....	2-7
3.	Security tab.....	3-1
	Searching for an existing user.....	3-1
	Inserting a WASS user ID into the PIC system	3-2
	Assigning access rights to a new or existing user.....	3-6
	Copying access rights to a user or group of users.....	3-10
	Modifying a user profile	3-12
	Removing access rights from a user	3-14
	Deactivating a user.....	3-16
	Deleting a user	3-17
4.	Role Maintenance tab	4-1
5.	Access Reports tab	5-1
	Access Reports tab overview	5-1
	Guidelines for using the Access Reports tab	5-2
	Navigating to the Access Reports tab	5-4
	Generating a User Security Access report	5-5
	Generating a Privacy Act Access report	5-8
	Generating a Global User Search report	5-11
	Generating a User Access by Submodule report	5-14
6.	Activity Reports tab	6-1
	Activity Reports tab overview	6-1
	Guidelines for using the Activity Reports tab.....	6-2
	Navigating to the Activity Reports tab	6-4
	Generating a User Activity Query report.....	6-5
	Generating a New Users report.....	6-8
	Generating an Improper Logoff report	6-11
	Generating a User Account Usage report	6-14
7.	User Certification tab	7-1

Appendix A: Password security.....A-1
Appendix B: Security concepts and best practices.....B-1
Appendix C: HUD system user responsibilities.....C-1
Appendix D: Role list and descriptions.....D-1
Appendix E: Acronym list.....E-1
Appendix F: Sample PIC access authorization forms.....F-1

The Security Administration Submodule

1. What is the Security Administration Submodule?



This section discusses the following topics:

- *Security Administration submodule overview* on page 1-1
- *User manual objectives* on page 1-2
- *User manual audience* on page 1-2
- *Acknowledgements* on page 1-2
- *Entering information in the Security Administration submodule* on page 1-3
- *Security Coordinator principles and guidelines* on page 1-4

Security Administration submodule overview

The **Security Administration** submodule is a tool on the Public and Indian Housing Information Center (PIC) system that allows authorized users to manage end-user access to the PIC system.

The Security Administration submodule consists of the tabs described below.

- **Security**
Perform tasks such as add new users to the PIC system, assign access rights, and deactivate PIC user accounts.
The Security tab is discussed in section 3.
- **Role Maintenance**
Revise existing PIC submodule roles or create new roles.
The Role Maintenance tab is discussed in section 4.
Note: The tab is used by authorized United States Department of Housing and Urban Development (HUD) employees only. The tab is displayed if you have access rights to it.
- **Access Reports**
Generate reports that list information related to a user's PIC system access.
The Access Reports tab and its reports are discussed in section 5.
- **Activity Reports**
Generate reports that list PIC system user activity information.
The Activity Reports tab and its reports are discussed in section 6.
- **User Certification**
Manage user certifications and re-certifications.
The User Certification tab is discussed in section 7.

User manual objectives

In this manual, you will learn to:

- Access the submodule.
- Use the submodule to complete security-related tasks.
- Use the submodule to generate security-related reports.

The manual contains appendices that discuss the following:

- Password security
- Security concepts and best practices
- HUD computer system end-user responsibilities
- List of submodule roles and their descriptions
- Acronyms used in this manual
- Sample PIC Access Authorization Forms

User manual audience

This manual is primarily intended for the Housing Authority (HA) employee who manages access to the PIC system for the end users at that HA. In this manual, this person is referred to as the **Security Coordinator**.

Note: Some HAs are larger than others and may have several persons or a department, such as an Information Technology (IT) department, dedicated to managing access to the PIC system.

HUD employees and HUD contractors may refer to the manual and its appendices as necessary.

Acknowledgements

The following HUD employees assisted in the creation of the Security Administration Submodule User Manual:

- Robert Harmon
- Timothy Still
- Emily Bridge
- Wendalyn Hovendick
- Susan Tindera
- Hitesh Doshi
- Patsy Stringer

Their professional attention to detail, teamwork, and specialized knowledge enhanced the value and clarity of this manual.

Entering information in the Security Administration submodule

There are four methods available for entering information in the Security Administration submodule:

- Drop-down menus
- Radio buttons
- Check boxes
- Text fields

Drop-down menus

The drop-down menu is the most common method for entering information. Select the drop-down menu and then select the desired option (see Figure 1-1 for an example).

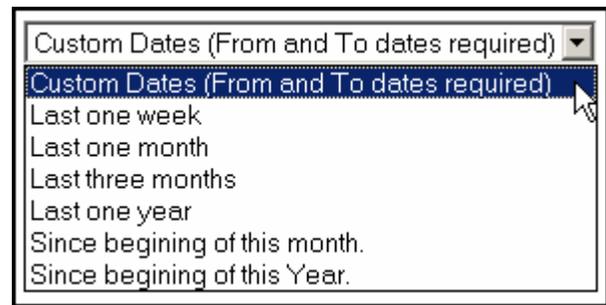


Figure 1-1: Using a drop-down menu

Radio buttons

The radio button is a less common method for selecting information. Select the button next to the desired option to make a selection (see Figure 1-2 for an example).

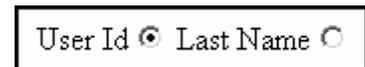


Figure 1-2: Using a radio button

Check boxes

The check box is another less common method for selecting information. Select the box next to the desired option (see Figure 1-3 for an example).



Figure 1-3: Using a check box

Text fields

Click inside a text field to type information, such as names, dates, and e-mail addresses (see Figure 1-4 for an example).

A screenshot of a web form showing a text input field. The label "Email Address:" is on the left, and the text "user@domainname.com" is entered in the field.

Figure 1-4: Using a text field

Sorting data

Some data tables in the Security Administration submodule can be sorted by selecting a column heading in the data table; the data is displayed in ascending alphabetical order according to the selected column heading. For example, select **User ID** to sort by user ID (see Figure 1-5).

Note: If you sort by user name, the user names are displayed in ascending alphabetical order by last name.

A screenshot of a web application interface titled "Security List". It features two dropdown menus: "Select ID Type:" set to "ALL" and "Select Status:" set to "Active". A link "Insert New WASS User" is on the right. Below the filters, it says "Users 1 to 41 of 41". A table with five columns is shown: "User ID", "User Name", "User Type", "ID Type", and "Status". Each column header has a small upward-pointing triangle, indicating that the table is sorted by "User ID".

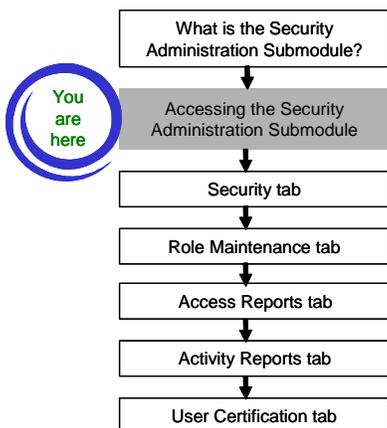
Figure 1-5: Sorting data in the Security Administration submodule

Security Coordinator principles and guidelines

The Security Coordinator's primary function is to manage HA end-user access to the PIC system. In order to achieve optimal security when managing PIC access, the Security Coordinator must keep the following principles and guidelines in mind:

- Security is authentication (proving your identity) and authorization (what information is a user allowed to access).
- Balance access and protection; give users just enough access to complete job-related tasks as directed by HA management in writing; keep the written security authorization in a secure location. Refer to appendix F for sample PIC Access Authorization Forms.
- Most users do not need maximum access rights. Only assign maximum access rights to users who need them to complete job-related tasks.
- Identify a knowledgeable and trusted Security Coordinator backup; assign full access rights to the backup so he or she can assume the responsibilities of the Security Coordinator in the Security Coordinator's absence.
- Store PIC logon information in a sealed envelope and store the envelope in a secure location; make sure the envelope is accessible to senior staff in the Security Coordinator's absence.
- Do not share Security Coordinator user IDs.

2. Accessing the Security Administration Submodule



This section discusses the following topics:

- *Overview* on page 2-1
- *Accessing the PIC system with a PIC ID* on page 2-2
- *Accessing the PIC system through WASS* on page 2-4
- *Navigating to the Security Administration submodule* on page 2-7

Overview

In 2002, HUD created a Web Access Security Subsystem (WASS), a secure, single access point to all HUD computer systems. The transition to WASS for some systems, such as PIC, is in progress. HUD expects the transition to WASS for the PIC system to be complete during mid to late 2006.

Until the transition to WASS for the PIC system is complete, users may continue to use their PIC IDs to access the PIC system. HUD will notify users when the transition to WASS is complete and when PIC IDs are no longer supported.

Because the exact completion date for the transition is unknown, this section explains how to access the PIC system with a PIC ID and how to access the PIC system through WASS.

Accessing the PIC system with a PIC ID

Follow these steps to use a PIC ID to access the PIC system:

Step	Action/Result
<p>1. Type pic.hud.gov in your Web browser's address field and press ENTER.</p> <p>Typing pic.hud.gov redirects you to the PIC home page located at http://www.hud.gov/offices/pih/systems/pic/.</p>	<p>The PIC home page appears (see Figure 2-1).</p> <p>Tip: Add the home page to your Web browser's list of bookmarks or favorite sites so you can easily access the page in the future.</p>
<p>2. Select Logon to PIC in the middle of the page or at the left of the page.</p>	

The screenshot shows the PIH Information Center (PIC) home page. At the top, there's a red header with the HUD logo and 'Public and Indian Housing'. Below the header, the page title is 'PIH Information Center (PIC)'. The main content area is divided into several sections: a description of the PIC, a list of sub-modules, a 'Quick Access' section with a 'Logon to the PIC System' button, and a 'What's New' section with a list of recent updates. A left sidebar contains navigation links for various categories like 'Public and Indian Housing', 'Online systems', 'HUD news', 'Homes', 'Communities', 'Working with HUD', 'Resources', 'Tools', 'Webcasts', 'Mailing lists', 'Contact us', and 'Help'. There are also links for 'En español', 'Text only', and 'Search/index' in the top right corner.

Figure 2-1: PIC home page

Step	Action/Result
3. Type your user ID and password on the PIC Logon page (see Figure 2-2).	
4. Select Logon to PIC or press the ENTER key.	The PIC Main page appears (see Figure 2-3).

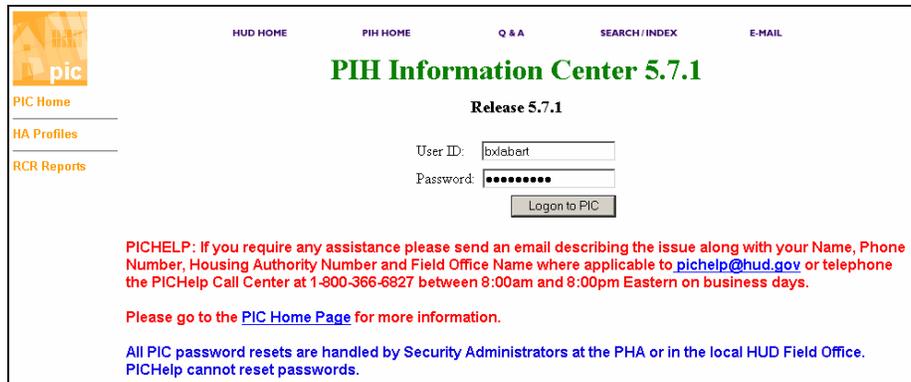


Figure 2-2: PIC Logon page

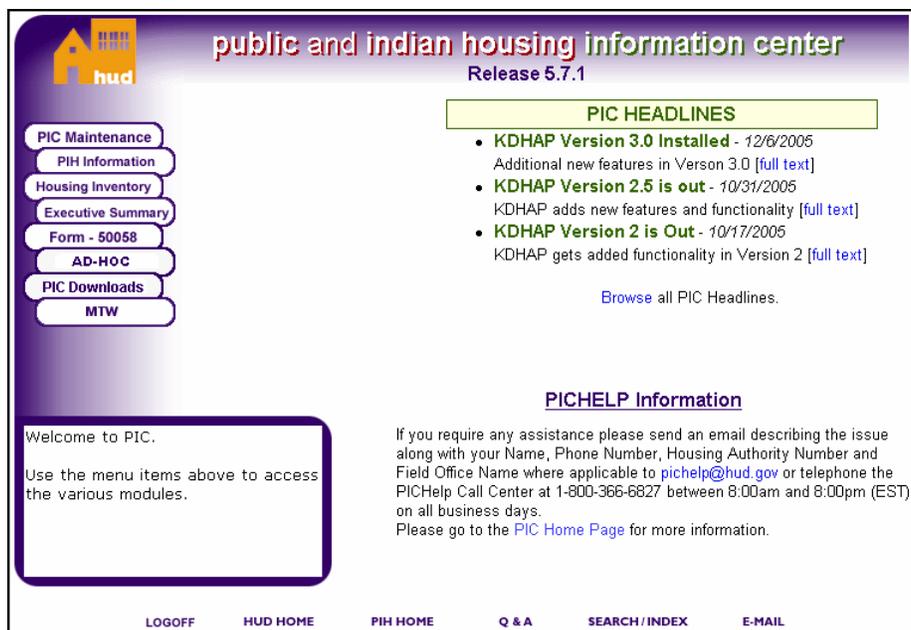


Figure 2-3: PIC Main page

Accessing the PIC system through WASS

Users must follow these steps to access the PIC system through WASS once the transition to WASS for the PIC system is complete and PIC IDs are no longer supported:

Step	Action/Result
<p>1. Type pic.hud.gov in your Web browser's address field and press ENTER.</p> <p>Typing pic.hud.gov redirects you to the PIC home page located at http://www.hud.gov/offices/pih/systems/pic/.</p>	<p>The PIC home page appears (see Figure 2-4).</p> <p>Tip: Add the home page to your Web browser's list of bookmarks or favorite sites so you can easily access the page in the future.</p>

Homes & Communities
U.S. Department of Housing and Urban Development

Public and Indian Housing

En español | Text only | Search/index

PIH Information Center (PIC)

What is the PIH Information Center (PIC)?

The PIH Information Center (PIC) allows Housing Authorities (HAs) to electronically submit information to HUD.

- Logon to WASS (HA User)
- Logon to WASS (HUD User)
- Logon to PIC
- Logon to PICTEST
- Online registration for new WASS ID
- System requirements
- Technical support (Job Aids & Help)
- Form-50058
- Resident Characteristics Report
- HA Profiles
- PIC Demo-Dispo
- HUD's Hurricane Katrina resource page
- Katrina Disaster Housing Assistance Program (KDHAP) Application - User Guide

Sub-Modules

PIC consists of the following modules and sub-modules:

- 1. PIC Maintenance**
 - User Profile
 - Security Administration
- 2. PIH Information**

Information by State

- Esta página en español
- Print version
- Email this to a friend

Quick Access

If you already have a User ID and Password, use the link below to logon into the PIC system:

[Logon to the PIC System](#)

What's New

- Dec. 6, 2005 - KDHAP Version 3.0 in PICTEST
- Dec. 2, 2005 - PIC now works with newer browsers
- Nov. 22, 2005 - 9/30 SENAP Certifications due 11/29
- Nov. 10, 2005 - Known bug in Delinquency Report
- Oct. 31, 2005 - KDHAP Version 2.5 is Out
- Oct. 6, 2005 - KDHAP added to PICTEST
- Oct. 3, 2005 - JUMP is a PICHelp online support system...

Figure 2-4: PIC home page

Step	Action/Result
2. Select Logon to WASS (HA User) in the middle of the page. Note: HUD users must select Logon to WASS (HUD User) .	The WASS Logon page appears (see Figure 2-5).
3. Type your WASS ID in the User ID field. Note: Make sure to capitalize the letters of your ID.	
4. Type your password in the Password field.	
5. Select Login .	The WASS Main Menu page appears (see Figure 2-6 on page 2-6).

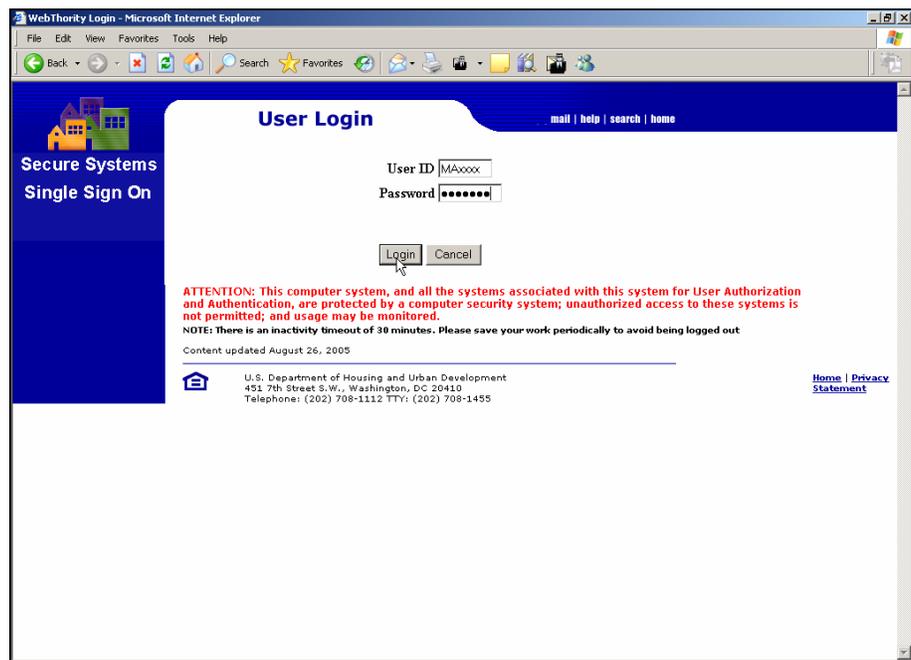


Figure 2-5: Accessing the PIC system through WASS

Step	Action/Result
6. Select PIH Information Center (circled in Figure 2-6).	The PIC Main page appears (see Figure 2-7).

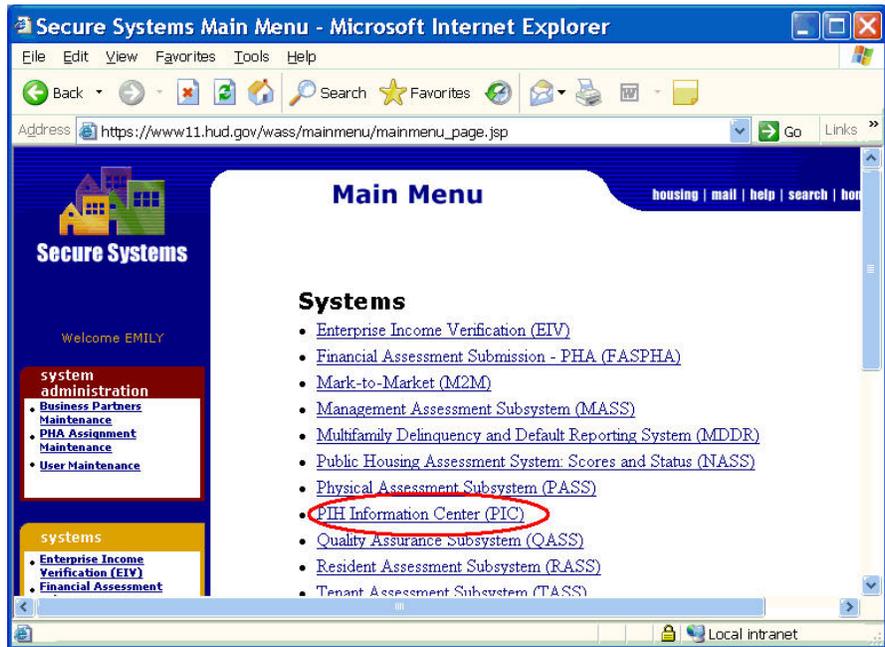


Figure 2-6: WASS Main Menu page

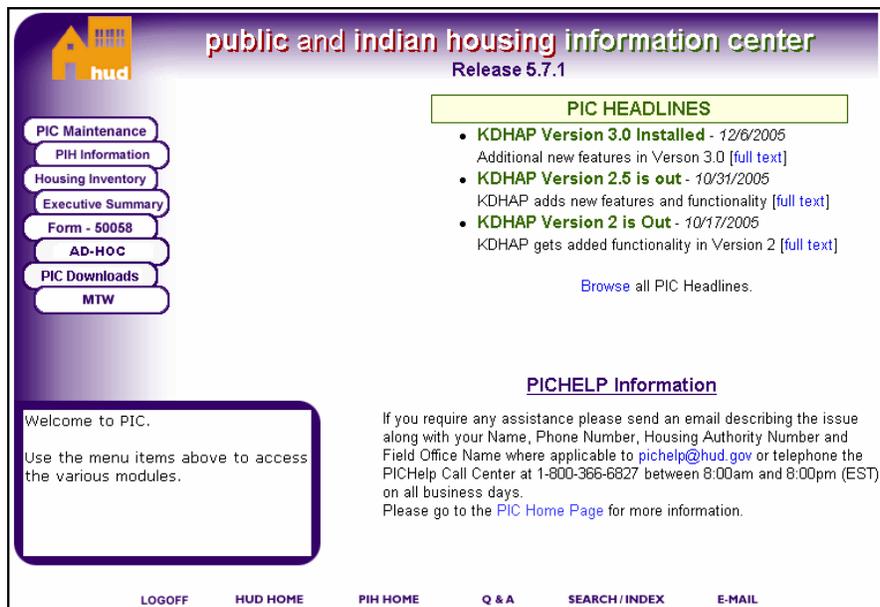


Figure 2-7: PIC Main page

Navigating to the Security Administration submodule

Follow these steps to access the Security Administration submodule:

Step	Action/Result
1. Move your mouse cursor over the PIC Maintenance button.	<p>Two submodules are displayed (see Figure 2-8):</p> <ul style="list-style-type: none"> • User Profile • Security Administration <p>Note: Your access to the other modules and submodules depends on the access rights assigned to you.</p>
2. Select Security Administration .	<p>The Privacy Act Statement and Compliance Notice may appear (see Figure 2-9). The notice appears when you first try to access content protected by the Privacy Act.</p> <p>Note: The notice does not appear if you previously accepted the statement to access other content protected by the Privacy Act.</p>

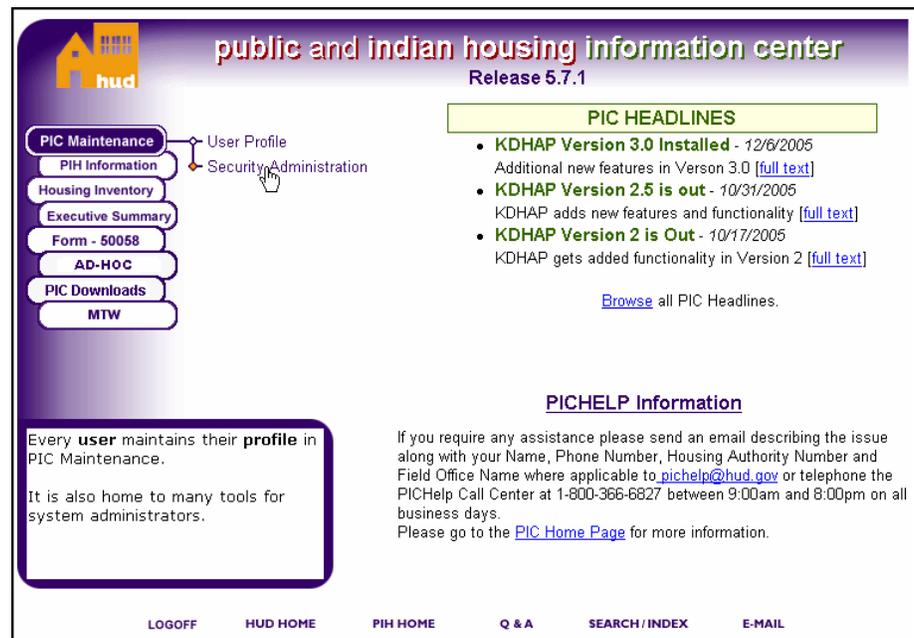


Figure 2-8: Navigating to the Security Administration submodule

Privacy Act Statement and Compliance Notice

Welcome Brian Labarta! 2/7/2006 10:23:05 AM

IMPORTANT: Please read the following carefully.

Legal Warning
 Misuse of Federal Information through the HUD Secure Connection web site falls under the provisions of Title 18, United States Code, Section 1030. This law specifies penalties for exceeding authorized access, alterations, damage, or destruction of information residing on Federal Computers.

Privacy Statement
 Information contained in this system is subject to the Privacy Act of 1974 (5 U.S.C. 552a, as amended). Personal information contained in this system may be used only by authorized persons in the conduct of official business. Any individual responsible for unauthorized disclosure or misuse of personal information will be prosecuted to the maximum extent possible under law.

Warning Notice
 The PIH Information Center (PIC) System supports Internet Explorer version 5.0 and above. Other browsers may not be compatible with this system.
 Your compliance is requested because you may have access rights to certain parts of PIC system which are covered by the Privacy Act. You may choose to decline and can still access the parts of the PIC system not covered by the Privacy Act as per your access privileges. All attempts to access the information (covered by Privacy act) will be logged into the PIC database irrespective of compliance status.

Figure 2-9: Privacy Act Statement and Compliance Notice

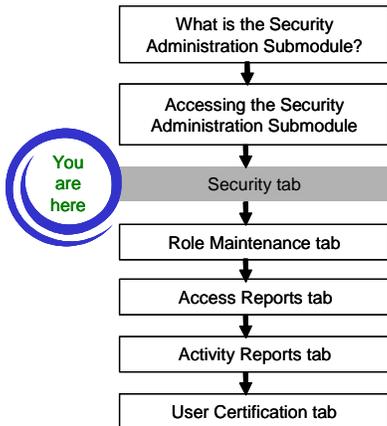
Step	Action/Result
3. Review the Privacy Act Statement and Compliance Notice (if applicable).	
4. Select Agree to comply with the statement (if applicable). Note: You cannot access the Security Administration submodule if you select Decline ; however, you can access PIC data not protected by the Privacy Act. Your access rights determine which sections of the system you may access.	The Security tab appears (see Figure 2-10).

The screenshot shows the 'Security List' interface. At the top, there are navigation tabs: Security, Role Maint, Access Reports, Activity Reports, and User Certification. Below the tabs, there are search and filter options. The 'Field Office HA' dropdown is set to 'MD001 ANNAPOLIS HOUSING AUTHORITY'. The 'Search for:' section has 'User ID' and 'Last Name' options. Below this, there are 'Select ID Type' (set to 'ALL') and 'Select Status' (set to 'Active') dropdowns. At the bottom, there is a table with the following data:

User ID	User Name	User Type	ID Type	Status
atuser	Another Test User	HA User	User	Active
bxiabart01	Brian Labarta	HA User	User	Active

Figure 2-10: Security tab

3. Security tab



The Security tab is the primary tab used to perform security-related tasks. This section discusses how to use the Security tab to perform the following tasks:

- *Searching for an existing user* on page 3-1
- *Inserting a WASS user ID into the PIC system* on page 3-2
- *Assigning access rights to a new or existing user* on page 3-6
- *Copying access rights to a user or group of users* on page 3-10
- *Modifying a user profile* on page 3-12
- *Removing access rights from a user* on page 3-14
- *Deactivating a user* on page 3-16
- *Deleting a user* on page 3-17

Searching for an existing user

The easiest way to locate a user is to review the Security List at the bottom of the Security tab (see Figure 3-1). The Security List displays the following information for each user associated with the HA:

- User ID
- User name
- User type
- ID type
- Status

User ID	User Name	User Type	ID Type	Status
MXXXXX	Sara Test User	HA User	User	Active
MXXXXX	Bill Test User	HA User	User	Active

Figure 3-1: Security tab and Security List

Note: By default, Security List information appears in ascending alphabetical order by user ID. Select a column heading to sort the Security List by that heading. For example, select **User Name** to sort the list in ascending alphabetical order by user name; the names sort by last name.

If necessary, you can search for a user by ID or last name. Refer to Figure 3-2 for an example and follow these steps:

Step	Action/Result
1. Select the Security tab if you are currently on another tab or page in the submodule. Note: If you just accessed the submodule, continue with step 2 because the Security tab is the default tab displayed after accessing the submodule.	
2. Select the User ID or Last Name radio button.	
3. Type all or part of the user's ID or last name in the Enter Search Text field.	
4. Select Search .	Results that match the information entered are displayed in the Security List.

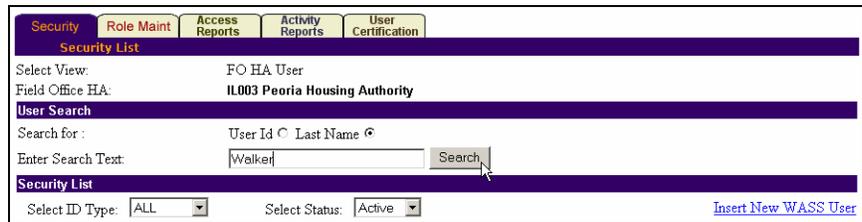


Figure 3-2: Searching for a user by ID or last name

Inserting a WASS user ID into the PIC system

These events must have occurred in the order listed before you can insert a WASS user ID into the PIC system:

1. The user successfully registered for a WASS ID.
2. The WASS (Real Estate Assessment Center (REAC) Secure Systems) Coordinator assigned a PIC access role to the WASS ID.

Note: Assigning the PIC access role to a WASS ID allows the user to see the PIC system option on the WASS Main Menu page. Assigning PIC module and submodule access rights is discussed in *Assigning access rights to a new or existing user* on page 3-6.

Follow these steps to insert a WASS user ID into the PIC system:

Step	Action/Result
1. Navigate to the Security Administration submodule.	
2. Select the Security tab.	
3. Select Insert New WASS User in the Security List section of the page (see Figure 3-3).	The Security Details page appears (see Figure 3-4). You must provide information for drop-down menus and fields marked with a blue asterisk (*).

Figure 3-3: Accessing the Security Details page

Figure 3-4: Using the Security Details page to add a new user

Step	Action/Result
4. Type the user's WASS ID in the WASS User ID field.	Make sure to capitalize the letters of the ID.
5. Type the user's first name in the First Name field.	
6. Type the user's middle name in the Middle Name field.	
7. Type the user's last name in the Last Name field.	
8. Select the type of user you are adding from the User Type drop-down menu.	
9. Type the user's e-mail address in the Email Address field.	Make sure to use a valid e-mail address because the user will receive important e-mail updates, such as re-certification e-mails, at the address provided.
10. Confirm the e-mail address is correct by re-typing it in the Confirm Email Address field.	
11. Type the account activation date in the Effective From Date field. Note: This is typically the date on which the user is added to the PIC system.	
12. Type the account expiration date in the Expiration Date field. Note: You can change the date at any time. Follow the steps in <i>Modifying a user profile</i> on page 3-12 to change the date.	If you do not know the exact expiration date, use your best judgment when choosing a date. For example, choose one year from the date on which the account is created for an HA employee on a six-month contract. You may use an expiration date of five years from the account creation date if you are still uncertain of which date to choose.
13. Select the Yes active indicator.	

Step	Action/Result
14. Type comments regarding the user's account in the User Status Comments field. Note: You are not required to type comments in the User Status Comments field.	
15. Review the information entered in steps 4–14 to make sure it is correct.	
16. Select Save .	<p>The Security Summary page appears, indicating the user successfully was added to the system (see Figure 3-5).</p> <p>Continue with step 3 in <i>Assigning access rights to a new or existing user</i> to assign access rights to the user.</p> <p>Or, repeat steps 2–16 to add more users.</p>

The screenshot displays the 'Security Summary' page. At the top, there are navigation tabs: Security, Role Maint, Access Reports, Activity Reports, and User Certification. The 'Security Summary' tab is active. Below the tabs, there are links for 'Security List', 'Security Summary', 'Bulk Copy', 'Security Details', and 'Modify User Organization'. The user information is as follows:

- UserID: MXXXX1
- User Name: Bill PIC User
- User Type: HA User

There are also links for 'Modify User' and 'Delete User'. Below this is the 'User Summary' section with dropdown menus for 'Module Name' (PIC Maintenance) and 'Sub Module Name' (User Profile). A table for 'Template Name' and 'Template Description' shows 'No Templates Defined.' Below that is a 'View Role' dropdown set to 'Use User Profile'. At the bottom, a table shows 'Records 1 to 1 of 1' with the following data:

Role	Level	Entity
Use User Profile	FO HA User	User, Bill P

At the very bottom, it says 'Pages 1'.

Figure 3-5: Security Summary page

Assigning access rights to a new or existing user

Typically, there are four types of access roles that can be assigned to a user: read-only, edit, submit, and approve; however, not all the roles are available for every submodule.

The read-only, edit, and submit roles are typically assigned to HA users; the approve role is for HUD use only.

Follow the steps below to assign access rights to a new or existing user. Remember to assign access rights as authorized in writing by HA management. Refer to appendix F for sample authorization forms.

Step	Action/Result
1. Follow the steps in <i>Searching for an existing user</i> on page 3-1 to locate the user.	
2. Select the User ID hyperlink.	The user's Security Summary page is displayed (see Figure 3-6).
3. Select the module you want to give the user access to from the Module Name drop-down menu. Note: A module may have more than one submodule.	Wait for the page to refresh before continuing with step 4.
4. Select Sub Module Name and select the submodule to which you want to give the user access (see Figure 3-6).	Wait for the page to refresh before continuing with step 5.
5. Select Add Role . Note: The Add Role link does not appear until you select a module and submodule.	The Security Summary page refreshes. Role details and security details for the selected submodule are displayed.

The screenshot shows the 'Security Summary' page for user MXXXX1. The user's name is 'Bill PIC User' and they are an 'HA User'. The 'Module Name' is 'MTCS' and the 'Sub Module Name' is 'Reports'. A dropdown menu is open for the 'Sub Module Name', showing options: Reports, Submission, Viewer, Reports, and Tenant ID Management. The 'Add Role' link is visible. Below the dropdown, there is a table with columns: Remove, Template Name, Template Description. The table is currently empty, with the message 'No Templates Defined.' displayed. Below the table, there is a 'View Role' section with a table with columns: Remove, Role, Level, Entity. This table is also empty, with the message 'No Roles Defined.' displayed.

Figure 3-6: Assigning access rights: selecting a submodule

Step	Action/Result
<p>6. Select the appropriate role from the Roles drop-down menu (see Figure 3-7 for an example).</p> <p>Note: Select View Actions to view actions the user can complete for the selected role.</p>	<p>A description of the role appears in the Role Description field.</p> <p>Refer to appendix D for a complete list of access roles and their descriptions.</p>
<p>7. Select a security level from the Security drop-down menu.</p> <p>Note: <i>Field Office HA</i> is typically the default setting for HA users.</p>	<p>Depending on your access level, other drop-down menus may appear.</p>

The screenshot displays the 'Security Summary' tab in the PIC Security Administration interface. At the top, there are navigation tabs: Security, Role Maint, Access Reports, Activity Reports, and User Certification. Below these are sub-tabs: Security List, Security Summary (active), Bulk Copy, Security Details, and Modify User Organization. The main content area shows user information: User ID: MXXXX1, User Name: Bill PIC User, User Type: HA User, Module Name: MTCS, and Sub Module Name: Reports. Under the 'Role/Data Details' section, the 'Roles' dropdown is set to 'Read Only Privacy' with a 'View Actions' button next to it. The 'Role Description' is 'Privacy data'. The 'Security' dropdown is set to 'HQ Division'. Below this is a table with two columns: 'Field Names' and 'Key Value'. The table contains one row: 'HQ Division' in the 'Field Names' column and 'Public and Indian Housing' in the 'Key Value' column. At the bottom right of the table area is a checkbox labeled 'Select/Deselect All'. A 'Save' button is located at the bottom right of the entire form.

Figure 3-7: Assigning access rights: selecting a role

Step	Action/Result
8. Select the hub for the user's field office and HA from the Hub drop-down menu (if applicable).	
9. Select the appropriate field office for the user's HA from the Field Office drop-down menu (if applicable).	
10. Select the user's HA from the Field Office HA list.	

Security Administration Interface - Security Summary

User ID: MXXXX1
 User Name: Bill PIC User
 User Type: HA User
 Module Name: MTCS
 Sub Module Name: Reports

Role/Data Details

Roles: Read Only Privacy [View Actions]

Role Description: Read Only Privacy data

Security: Field Office HA

Field Names	Key Value
HQ Division	Public and Indian Housing
HQ Office	PO Field Operations
Hub	3HBLT Baltimore Hub
Field Office	3GPH WASHINGTON, DC PROGRAM CENTER

Field Office HA

- DC001 D.C HOUSING AUTHORITY
- DC101 KENILWORTH PARKSIDE PMC
- DC880 Community Connections
- MD004 MONTGOMERY CO HOUSING AUTHORITY**
- MD007 ROCKVILLE HOUSING AUTHORITY
- MD011 GLENARDEN HOUSING AUTHORITY
- MD015 PRINCE GEORGES COUNTY HOUSING AUTHORITY
- MD017 COLLEGE PARK HOUSING AUTHORITY
- MD902 MD DEPT HSG COMMUNITY DEVELOPM
- VA004 ALEXANDRIA REDEVELOPMENT & H/A

Select/Deselect All

Save

Figure 3-8: Assigning access rights: selecting the user's security level

Step	Action/Result
11. Select Save at the bottom of the page.	<p>The user's Security Summary page appears (see Figure 3-9). The role is displayed in the table at the bottom of the page.</p> <p>Tip: Follow the steps in <i>Generating a User Security Access report</i> on page 5-5 to view a detailed summary of the user's current access rights.</p> <p>Repeat steps 3–11 to add more roles to the user's ID.</p>

Security	Role Maint	Access Reports	Activity Reports	User Certification
Security List	Security Summary	Bulk Copy	Security Details	Modify User Organization
UserID:	MXXXX1	Modify User Delete User		
User Name:	Bill PIC User			
User Type:	HA User			
User Summary				
Module Name:	MTCS	Copy Rights To Users		
Sub Module Name:	Reports	Add Template		
<input type="checkbox"/> Remove	Template Name	Template Description		
No Templates Defined.				
View Role:	Read Only Privacy	Add Role		
Records 1 to 1 of 1				
<input type="checkbox"/> Remove	Role	Level	Entity	
<input type="checkbox"/>	Read Only Privacy	Field Office HA	MD004 MONTGOMERY CO HOUSING AUTHORITY	
<input type="checkbox"/> Select/DeSelect All				<input type="button" value="Remove Role"/>
Pages				1

Figure 3-9: Security Summary page showing newly assigned role

Copying access rights to a user or group of users

Security Coordinators can use the bulk copy feature to copy access rights from one user to another user or group of users. Copying access rights eliminates the need to assign access rights to one user at a time.

Follow these steps to use the bulk copy feature to assign access rights:

Step	Action/Result
1. Follow the steps in <i>Searching for an existing user</i> on page 3-1 to locate the user from whom the access rights will be copied.	
2. Select the User ID hyperlink.	The user's Security Summary page is displayed.
3. Select Bulk Copy (circled in Figure 3-10).	The Bulk Copy page appears (see Figure 3-11).

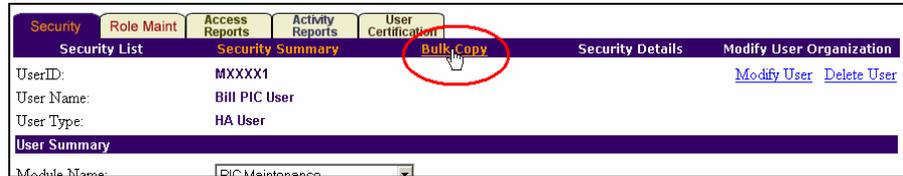


Figure 3-10: Accessing the Bulk Copy page

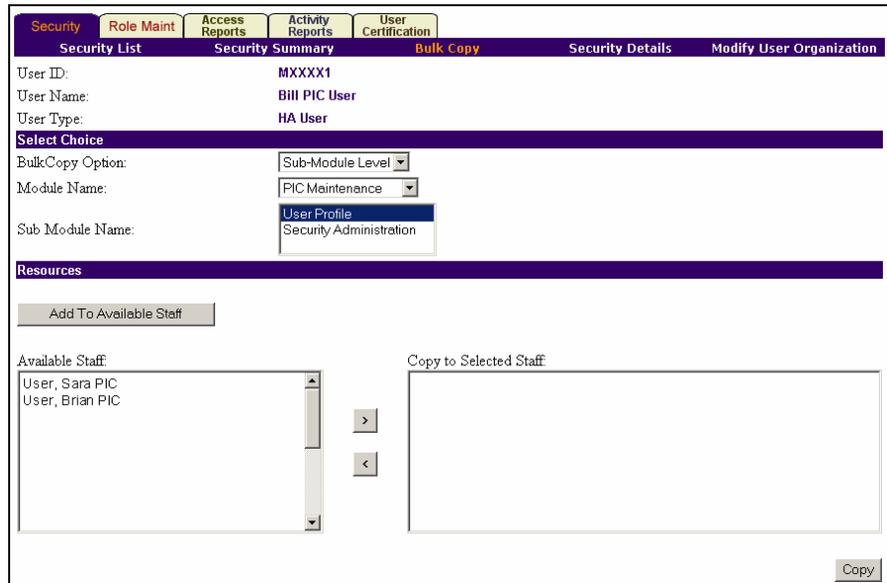


Figure 3-11: Bulk Copy page

Step	Action/Result
<p>4. Select the level at which you want to copy the access rights from the Bulk Copy Option drop-down menu:</p> <ul style="list-style-type: none"> • <i>Sub-Module Level</i> • <i>Module Level</i> • <i>User Level</i> <p>Note: Wait for the page to refresh before continuing.</p>	<p><i>Sub-Module Level</i> copies access rights for a submodule only. You must select the module from the Module Name drop-down menu and the submodule from the Sub Module Name field (see Figure 3-12 for an example).</p> <p><i>Module Level</i> copies access rights for a module and all of its submodules. You must select the module from the Module Name list.</p> <p><i>User Level</i> copies all the user's access rights.</p>
<p>5. Select the user to whom you want to copy the access rights from the Available Staff list.</p>	<p>Press and hold the CTRL key to select more than one user.</p>
<p>6. Select the right arrow to add the user or users to the Copy to Selected Staff list.</p> <p>Select a user in the Copy to Selected Staff list and then select the left arrow to move the user back to the Available Staff list.</p>	
<p>7. Select Copy.</p>	

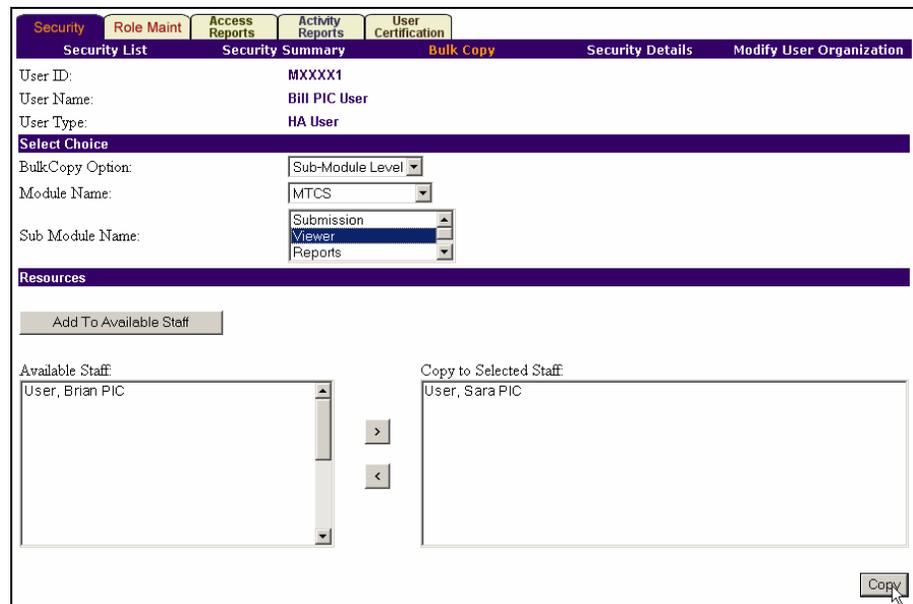


Figure 3-12: Copying access rights to a user or group of users

Modifying a user profile

Occasionally, a Security Coordinator may need to modify a user's profile for reasons such as updating an e-mail address or updating the user's account expiration date.

Follow these steps to modify a user profile:

Step	Action/Result
1. Follow the steps in <i>Searching for an existing user</i> on page 3-1 to locate the user.	
2. Select the User ID hyperlink.	The user's Security Summary page appears.
3. Click Modify User at the right of the page under Modify User Organization (see Figure 3-13).	The user's Security Details page appears (see Figure 3-14).

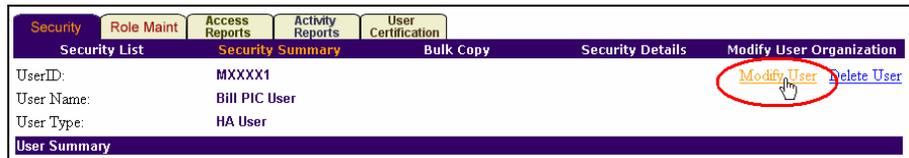


Figure 3-13: Accessing a user's Security Details page

The screenshot shows the Security Details page for user MXXXX1. The navigation bar is the same as in Figure 3-13. The main content area displays the following information:

- Field Office HA: IL003 Peoria Housing Authority
- User Details:
 - WASS User ID: MXXXX1
 - First Name: Bill
 - Middle Name: PIC
 - Last Name: User
 - User Type: HA User
 - Email Address: bill@domain.gov
 - Confirm Email Address: bill@domain.gov
 - Effective From Date: 02/15/2006
 - Expiration Date: 02/15/2007
 - Active Indicator: Yes No
 - User Status Comments: (empty text area)
- Save button

Figure 3-14: Security Details page

Step	Action/Result
4. Type or select the changes to the user's profile.	
5. Type the reason for modifying the user's profile in the User Status Comments field.	
6. Select Save .	The Security Summary page appears after the changes have been saved.

Removing access rights from a user

Removing access rights from a user involves removing one or more access roles from the user's ID.

Follow these steps to remove access rights from a user:

Step	Action/Result
1. Follow the steps in <i>Searching for an existing user</i> on page 3-1 to locate the user.	
2. Select the User ID hyperlink.	The user's Security Summary page appears.
3. Select the module for which the role will be removed from the Module Name drop-down menu.	Wait for the page to refresh before continuing with step 4.
4. Select the appropriate submodule from the Sub Module Name drop-down menu (see Figure 3-15).	Wait for the page to refresh before continuing with step 5.

The screenshot displays the 'Security Summary' page for user MXXXX1. The user's name is 'Bill PIC User' and their type is 'HA User'. Under the 'User Summary' section, the 'Module Name' is 'MTCS' and the 'Sub Module Name' is 'Submission'. A dropdown menu for 'Sub Module Name' is open, showing options: 'Submission', 'Viewer', 'Reports', and 'Tenant ID Management'. The 'Viewer' option is selected. Below the dropdown, there is a 'Remove' button and a 'Template Description' field. The page also shows 'No Templates Defined.' and 'View Role:' with an 'Add Role' link.

Figure 3-15: Removing an access role from a module and submodule

Step	Action/Result
5. Select the role you want to remove from the View Role drop-down menu. It will show only those roles linked to the selected submodule (see Figure 3-16).	
6. Select the check box next to the role to be removed (circled in Figure 3-16).	
7. Select Remove Role .	
8. Select OK on the pop-up that appears to confirm you want to delete the role (see Figure 3-17).	
9. Repeat steps 3–8 to remove additional roles.	

The screenshot shows a web application interface for security administration. At the top, there are tabs for 'Security', 'Role Maint', 'Access Reports', 'Activity Reports', and 'User Certification'. Below these are sub-tabs: 'Security List', 'Security Summary', 'Bulk Copy', 'Security Details', and 'Modify User Organization'. The main content area displays user information: User ID: MXXXX1, User Name: Bill PIC User, User Type: HA User. There are links for 'Modify User' and 'Delete User'. Below this is a 'User Summary' section with 'Module Name' set to 'MTCS' and 'Sub Module Name' set to 'Viewer'. There are links for 'Copy Rights To Users' and 'Add Template'. A table with columns 'Remove', 'Template Name', and 'Template Description' shows 'No Templates Defined.'. Below that is a 'View Role' dropdown menu with 'Submit Role' selected. There are links for 'Add Role' and 'Remove Role'. At the bottom, a table with columns 'Remove', 'Role', 'Level', and 'Entity' is shown. The 'Remove' column has a checked checkbox circled in red. The 'Role' column contains 'Submit Role', 'Level' contains 'Field Office HA', and 'Entity' contains 'MD004 MONTGOMERY CO HOUSING AUTHORITY'. There is a 'Select/Deselect All' checkbox and a 'Remove Role' button.

Figure 3-16: Selecting a role for deletion



Figure 3-17: Confirming the deletion of an access role

Deactivating a user

You may need to deactivate a user's account if a user's employment contract expires and is not renewed, a user resigns or retires, or a user no longer needs access to the PIC system.

Follow these steps to deactivate a user's account:

Step	Action/Result
1. Follow the steps in <i>Searching for an existing user</i> on page 3-1 to locate the user.	
2. Select the User ID hyperlink.	The user's Security Summary page appears.
3. Select Modify User .	The user's Security Details page appears (see Figure 3-18).
4. Type an account expiration date in the Expiration Date field.	In the example shown in Figure 3-18, the date in the Expiration Date field was updated to reflect the last day of employment for an HA employee.
5. Select the No radio button next to Active indicator . Note: The user does not appear in the Security List after you select the No radio button and click Save .	
6. Type the reason for deactivating the account in the User Status Comments field (if applicable).	Note: You are not required to provide a reason for deactivating the user's account.
7. Select Save .	

The screenshot shows the 'Modify User' form for a user named 'User' with WASS User ID 'MA1234'. The form includes fields for personal information, contact details, and account settings. The 'Expiration Date' is set to 01/25/2006, and the 'Active Indicator' is set to 'No'. The 'User Status Comments' field contains a note about the user's employment ending on 01/24/2006. A 'Save' button is located at the bottom right of the form.

Figure 3-18: Deactivating a user

Deleting a user

Follow the steps below to delete a user from the PIC system. You may need to delete a user if you incorrectly entered the user's WASS ID or if you selected the wrong user type for the user's account.

Note: HA Security Coordinators can delete users for their HA only. A HUD Field Office Security Coordinator can delete users for their Field Office and HA users in their Field Office's jurisdiction.

Step	Action/Result
1. Follow the steps in <i>Searching for an existing user</i> on page 3-1 to locate the user.	
2. Select the User ID hyperlink.	The user's Security Summary page appears.
3. Select Delete User (circled in Figure 3-19).	The user's Security Details page appears.
4. Select Delete to confirm you want to delete the user permanently (see Figure 3-20).	The Security List appears. A message appears indicating that the user was deleted successfully.

The screenshot shows the 'Security Summary' page for a user with ID MA1234. The user's name is 'Example User' and they are an 'HA User'. The page includes a 'User Summary' section with dropdown menus for 'Module Name' (PIC Maintenance) and 'Sub Module Name' (User Profile). Below this is a table for 'Template Name' and 'Template Description', which is currently empty with the message 'No Templates Defined.' At the bottom, there is a table with one record: 'Use User Profile' with level 'FO HA User' and entity 'User, Example'. The 'Delete User' link is circled in red.

Figure 3-19: Deleting a user

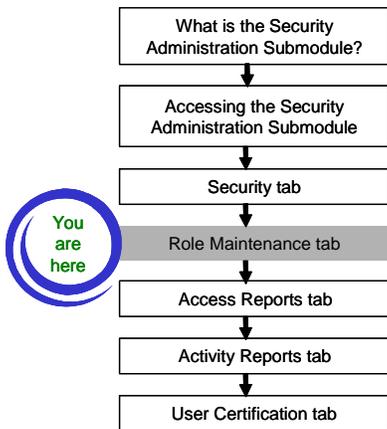
The screenshot shows the 'Security Details' page for the same user. At the bottom, a confirmation dialog is displayed: 'Are you sure you want to permanently delete this user?' with 'Delete' and 'Cancel' buttons. A mouse cursor is pointing at the 'Delete' button.

Figure 3-20: Confirming the deletion of a user

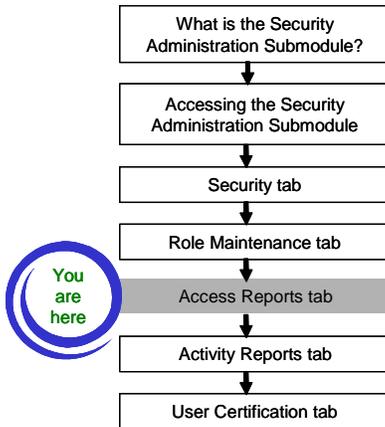
4. Role Maintenance tab

The Role Maintenance tab is visible to qualified HUD headquarters employees only. Qualified HUD employees can use the tab to revise existing submodule roles or to create new roles.

Note: The information in this section is for reference purposes only.



5. Access Reports tab



This section discusses the following topics:

- *Access Reports tab overview* on page 5-1
- *Guidelines for using the Access Reports tab* on page 5-2
- *Navigating to the Access Reports tab* on page 5-4
- *Generating a User Security Access report* on page 5-5
- *Generating a Privacy Act Access report* on page 5-8
- *Generating a Global User Search report* on page 5-11
- *Generating a User Access by Submodule report* on page 5-14

Access Reports tab overview

The Access Reports tab has four sub-tabs that can help generate access-related reports. A description of the reports follows.

- **User Security Access**
The report provides a detailed view of a user's access rights.
The report lists user identification information, modules and sub-modules to which a user has access, and the actions a user can complete for each submodule.
- **Privacy Act Access**
The report lists users who tried to access data protected by the Privacy Act.
Refer to appendix B for more information on the Privacy Act.
- **Global User Search**
Use this feature to search for a PIC user at another HA or HUD Field Office.
- **User Access by Submodule**
The report lists users who have access to a specific submodule.

Guidelines for using the Access Reports tab

Disabling pop-up blockers

The reports discussed in this section are displayed in separate windows. Pop-up blocking software may prevent the reports from generating or displaying properly. Because there are many pop-up blocking tools, this manual does not explain how to disable pop-up blockers. Refer to your pop-up blocker's Help files for detailed instructions on how to disable it.

For information on system requirements and recommended settings for using the PIC system, go to <http://www.hud.gov/offices/pih/systems/pic/sr/>.

Tip: If you use Internet Explorer to generate a report, press and hold the CTRL key immediately before selecting the **Generate Report** button to disable the pop-up blocker temporarily. Make sure to hold the key down while the report is generating.

Navigating between report pages

Some reports may contain more than one page of information. To view another page of information, select the numbered link for that page or select **Next Page**; select **Prev page** to return to the previous page of information (see Figure 5-1).

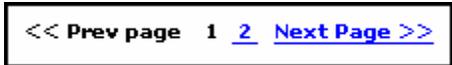


Figure 5-1: Navigating between report pages

Some reports allow you to view the entire report on a single report page. If you see **View All** on a report page, you can select it to view the entire report on a single page (see Figure 5-2 for an example).

The screenshot shows a report titled "New Users Report" with a "pic" logo on the left and "Download in Excel" and "Print" icons on the right. The report details include:

- HQ Division: **Public and Indian Housing**
- HQ Office: **PO Field Operations**
- Hub: **5HCHI Chicago Hub**
- Field Office: **5APH CHICAGO HUB OFFICE**
- Field Office HA: **IL003 Peoria Housing Authority**
- Report Period: **1/2/2004 to 2/17/2006**
- Report generation Date: **Friday, February 17, 2006 1:33:00 PM**

Below this is a summary line: "New users created between 1/2/2004 and 2/17/2006". A navigation bar shows "Users 1 - 25 of 2 (View All)" with the "View All" link circled in red. To the right of the navigation bar are the same navigation controls as in Figure 5-1: "<< Prev page 1 2 Next Page >>".

#	User Name (Last, Middle, First)	User ID	User Type	Creation Date/Time	Account Expiry	Created By
1	Bill PIC User	MXXXXX1	HA User	Feb 16 2006 10:50AM	17 Feb 2006	MXXXXXX

Figure 5-2: Viewing an entire report on a single page

Choosing a report output option

All of the reports discussed in this section can be printed or downloaded to a Microsoft Excel™ spreadsheet.

Click the icon for the desired output option (see Figure 5-3).



Figure 5-3: Choosing a report output option

Closing report windows

When closing a report window, make sure to select the “x” in the report window (see Figure 5-4) and not the “x” in the main window. You must re-login to the PIC system if you mistakenly close the main PIC window.

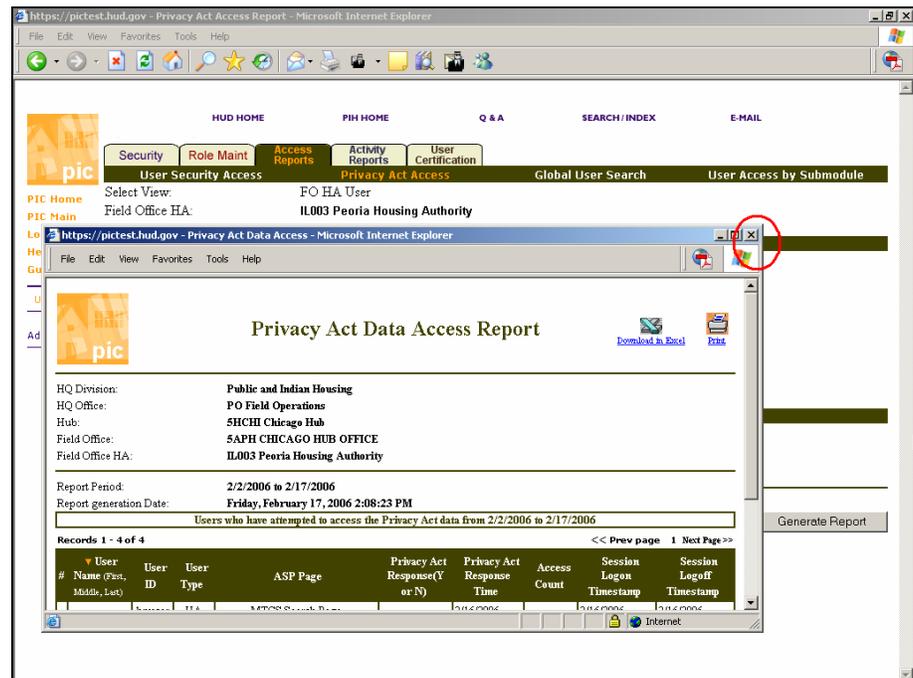


Figure 5-4: Closing a report window

Navigating to the Access Reports tab

Follow these steps to navigate to the Access Reports tab:

Step	Action/Result
1. Log on to the PIC system.	
2. Move the cursor over the PIC Maintenance button.	
3. Select the Security Administration hyperlink.	
4. Select the Access Reports tab (see Figure 5-5).	

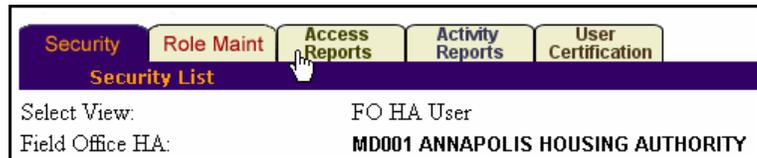


Figure 5-5: Navigating to the Access Reports tab

Generating a User Security Access report

The User Security Access report provides a detailed view of a user's access rights. It also lists the actions a user can perform for each submodule to which the user has access.

Follow these steps to generate a User Security Access report:

Step	Action/Result
1. Select the Access Reports tab.	The User Security Access report page is the default page displayed (see Figure 5-6).
2. Locate the user in the Security List at the bottom of the page.	
3. If necessary, narrow the list of users by following these steps: <ol style="list-style-type: none"> Select the User ID or Last Name radio button; then type all or part of the ID or last name in the Enter Search Text field. Or, Select a user ID status from the Select Status drop-down menu. Or, Select an ID type from the Select ID Type drop-down menu. Select Search. 	
4. Select the user ID hyperlink to generate the report.	

Figure 5-6: User Security Access report page

Information listed in a User Security Access report

A User Security Access report lists information in three tables. A sample report is shown in Figure 5-7. The following pages describe the report tables.

User Security Report				
 				
User Identification				
User-id:	MXXXXX1	Name (last, first):	User, Bill	
Telephone Number:		E-Mail:	bill@domain.gov	
User Type:	HA User	User Status:	active	
Creation Date :	02/15/2006	Account End Date:	02/15/2007	
User Roles				
Module	Sub Module	Role	Level	Entity
PIC Maintenance	User Profile	Use User Profile	FO HA User	User, Bill P
Housing Inventory	Housing Authority	Edit Role	Field Office HA	MD004 MONTGOMERY CO HOUSING AUTHORITY
Housing Inventory	Development	Submit Role	Field Office HA	MD004 MONTGOMERY CO HOUSING AUTHORITY
MTCS	Submission	Submit Role	Field Office HA	MD004 MONTGOMERY CO HOUSING AUTHORITY
MTCS	Viewer	Read Only Privacy	Field Office HA	MD004 MONTGOMERY CO HOUSING AUTHORITY
MTCS	Viewer	Submit Role	Field Office HA	MD004 MONTGOMERY CO HOUSING AUTHORITY
MTCS	Reports	Read Only Privacy	Field Office HA	MD004 MONTGOMERY CO HOUSING AUTHORITY
User Actions				
PIC Maintenance >> User Profile:				
Update User Profile				
Housing Inventory >> Housing Authority:				
Create HA	CreateHAAddress	CreateHAContact	ModifyHAAddress	
ModifyHAContactAddress	ModifyHAContactDetails	ModifyHADetails	ModifyOccupancyForm	
Read Development Summary	Read HA Report	Read HA Summary	ReadHAAddress	
ReadHAContactAddress	ReadHAContactDetails	ReadHAContactList	ReadHADetails	
ReadHAFunding	ReadHAHistoryDetails	ReadHAHistoryList	ReadHAInventory	
ReadHAList	ReadHAPerformance	ReadHAStaffList	ReadHATempOffice	
ReadOccupancyForm	ReadOccupancyReport	ReadSearchHAList		
Housing Inventory >> Development:				
Add New Contact	Add Units	AMP Assignment - Building	B&U Cert. Submit	
B&U Certification	Copy Unit Info	Delete Unit	Development List View	
Download Unit Template	Edit Building	Edit Building Information	Edit Contact Information	
Edit Development	Edit review status	Edit Unit Info	Edits the submission comments	
Occupancy Read-Only	Review Development	Search Units	Submit HA	
Submit HA Info	Upload Unit Template	View	View Address Information	
View AMP Assignment	View AMP Assignment Report	View AMP Assignment Report 2	View Building	
View Building Information	View Building Reports	View Contact Information	View Data Transfer Page	
View Development Information	View Development List	View Exception List	View Geo Coded Addr Report	
View HA RASS Report	View Submission page	View Unit Details	View Unit Information	
View Unit Reports	View Vac/Occ Report			
MTCS >> Submission:				
Report View	Upload File	Upload Page View		
MTCS >> Viewer:				
Assets View	FSS General View	FSS View	FSS/W/W Service View	
HA Query Report View	Household Action View	Household Agency View	Household Background View	
Household Unit View	Income View	Iss/Exp Voucher Details	Iss/Exp Vouchers List	
Manufactured Home View	Members View	Online EOP Insert	Rent Calculation View	
Rent Expected Income View	Rent TTP view	Search View	Transaction Report View	
VO Iss/Exp Report View	W/W View			
MTCS >> Reports:				
Budget Rel. Avgs Report View	Changes In Income Report View	Deconcentration Report View	Delinquency Report View	
EOP Report View	FSS Report View	Income Report View	KMI Report View	
Late HQS Report View	Late Reexam Report View	Mob & Portability Report View	New Adm Report View	
Newly leased Units Report View	RCR Report View	Rent & Rent Burden Report View	Rent Discrepancy Report View	
Semap Report View				

Figure 5-7: Sample User Security Access report

Table	Information Presented
User Identification	<p>The User Identification table lists the following information:</p> <ul style="list-style-type: none"> • User ID • Name • Telephone number • E-mail address • User type • User status • Creation date (date on which the user's account was created) • Account end date (date on which the user's account expires)
User Roles	<p>The User Roles table lists the following information:</p> <ul style="list-style-type: none"> • Module • Submodule • Role • Level • Entity (typically, the HA to which the user belongs)
User Actions	<p>The User Actions table lists the actions a user can take for each submodule.</p> <p>Refer to appendix D for a complete list of access roles and their descriptions.</p>

Generating a Privacy Act Access report

The Privacy Act Access report lists PIC pages protected by the Privacy Act that a user tried to access. The report indicates whether or not the user accepted the Privacy Act statement.

Note: Refer to appendix B for more information on the Privacy Act.

Follow these steps to generate a Privacy Act Access report:

Step	Action/Result
1. Select the Access Reports tab.	The User Security Access report page is the default page displayed.
2. Select Privacy Act Access (see Figure 5-8).	The Privacy Act Access report page appears (Figure 5-9).

The screenshot shows a web application interface with a navigation bar at the top containing 'Security', 'Role Maint', 'Access Reports', 'Activity Reports', and 'User Certification'. The 'Activity Reports' tab is active, and 'Privacy Act Access' is highlighted. Below the navigation bar, there are options for 'Select View' (FO HA User) and 'Field Office HA' (IL003 Peoria Housing Authority). A 'User Search' section includes a search box, a 'Search' button, and dropdown menus for 'Select Status' and 'Select ID Type', both set to 'ALL'. Below this is a 'Security List' section with a table header: 'User ID', 'User Name', 'User Type', 'ID Type', and 'Status'. The first row of the table shows 'awebb', 'Andrea Webb', 'Guest User', 'User', and 'Inactive'.

Figure 5-8: Accessing the Privacy Act Access report page

The screenshot shows the same web application interface as Figure 5-8, but with the 'Privacy Act Access' report page fully loaded. The 'Data Filters for Privacy Act Access Report' section is visible, featuring a 'Report Period' dropdown menu set to 'Custom Dates (From and To dates required)'. Below this are 'From' and 'To' date pickers, both set to 2/2/2006 and 2/17/2006. The 'User Types' dropdown is set to 'ALL'. The 'Display Filters for Privacy Act Access 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' in 'Descending order'. A 'Generate Report' button is located at the bottom right of the page.

Figure 5-9: Privacy Act Access report page

Step	Action/Result
3. Enter the report data filters: <ol style="list-style-type: none"> a. Select a pre-defined report range from the Report Period drop-down menu; or, use the <i>Custom Dates</i> default and type dates in the From and To fields. b. Select the user type from the User Types drop-down menu. 	
4. Enter the report display filters: <ol style="list-style-type: none"> a. Select the number of rows you want to display per page from the No of rows to display drop-down menu. b. Select how you want to sort the report data from the Sort report data by drop-down menu; then select the order in which you want the data displayed from the adjacent drop-down menu. 	
5. Select Generate Report .	

Information listed in a Privacy Act Access report

The Privacy Act Access report consists of a report header and one table that lists report data. A sample report is shown in Figure 5-10.

pic		Privacy Act Data Access Report							
HQ Division:	Public and Indian Housing								
HQ Office:	P O Field Operations								
Hub:	3HBLT Baltimore Hub								
Field Office:	3BPH BALTIMORE HUB OFFICE								
Field Office HA:	MD001 ANNAPOLIS HOUSING AUTHORITY								
Report Period:	1/10/2006 to 1/25/2006								
Report generation Date:	Wednesday, January 25, 2006 11:47:58 AM								
Users who have attempted to access the Privacy Act data from 1/10/2006 to 1/25/2006									
Records 1 - 13 of 13		<< Prev page 1 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	Taniana D.		Guest	FEM/ Katrina Search		1/10/2006		1/10/2006	1/10/2006

Figure 5-10: Sample Privacy Act Access report

The report header may contain the following information:

- Headquarters (HQ) division
- HQ office
- Hub
- Field office
- Field office HA
- Report period
- Report generation date

The following information is listed in the report table:

- User name
- User ID
- User type
- Active Server Page (ASP)
- Privacy Act Response (“Y” indicates the user accepted the Privacy Act Statement and Compliance Notice; “N” indicates the user rejected it)
- Privacy Act response time (the date and time the notice was accepted or rejected)
- Access count (the number of times a page containing data protected by the Privacy Act was accessed)
- Session logon timestamp (the date and time the user logged on to the PIC system)
- Session logoff timestamp (the date and time the user logged off the PIC system)

Generating a Global User Search report

Follow these steps to search for a PIC user at another HA or HUD Field Office:

Step	Action/Result
1. Select the Access Reports tab.	The User Security Access report page is the default page displayed.
2. Select Global User Search (circled in Figure 5-11).	The Global User Search report page appears (see Figure 5-12).

The screenshot shows a navigation menu with the following tabs: Security, Role Maint, Access Reports, Activity Reports, and User Certification. Below these are sub-tabs: User Security Access, Privacy Act Access, Global User Search (circled in red), and User Access by Submodule. The page content includes: Select View: FO HA User; Field Office HA: IL003 Peoria Housing Authority; Search for: User Id Last Name; Enter Search Text: [input field]; Select Status: ALL; Select ID Type: ALL; Search button; Security List; Users 1 to 50 of 51; and a table header with columns: User ID, User Name, User Type, ID Type, Status.

Figure 5-11: Accessing the Global User Search report page

The screenshot shows the search interface with the following sections: Search by User-ID(s) with a text input field and a Search Users button; a note: "Please enter exact User-ID(s). Use comma(,) to separate multiple User-IDs (e.g. UserID1, UserID2,.. etc) Non alphanumeric characters will be ignored."; Search by First and/or Last Name with input fields for First Name and Last Name, checkboxes for Exact Match, and a Search By Name button. A note below the name fields says: "Enter at least first 3 characters of the First and/or Last name."

Figure 5-12: Global User Search report page

Step	Action/Result
<p>3. Determine if you want to search by user ID or by name.</p> <ul style="list-style-type: none"> To search by user ID, type the user ID in the User-ID(s) field and select Search Users (see Figure 5-13). <p>Note: You must separate multiple user IDs with commas.</p> <ul style="list-style-type: none"> To search by name, type all or part of the first name in the First Name field; or, type all or part of the last name in the Last Name field; then select Search By Name (see Figure 5-14 on page 5-13). <p>Note: You must type at least the first three characters of the first name or last name.</p>	<p>Tip: When searching by name, clear the Exact Match check box to increase the number of search results.</p>

The screenshot shows a web application interface with a navigation bar at the top containing tabs for Security, Role Maint, Access Reports, Activity Reports, and User Certification. Below the navigation bar, there are several menu items: User Security Access, Privacy Act Access, Global User Search (highlighted), and User Access by Submodule. The main content area is divided into two sections. The first section, titled "Search by User-ID(s)", features a text input field containing "MXXXXX, MXXXX1" and a "Search Users" button. Below this field is a blue instruction: "Please enter exact User-ID(s). Use comma(,) to separate multiple User-IDs (e.g. UserID1, UserID2,.. etc) Non alphanumeric characters will be ignored." The second section, titled "Search by First and/or Last Name", contains two text input fields for "First Name" and "Last Name", each followed by a checked "Exact Match" checkbox and a "Search By Name" button. A note below these fields states: "Enter at least first 3 characters of the First and/or Last name."

Figure 5-13: Searching for a user by user ID

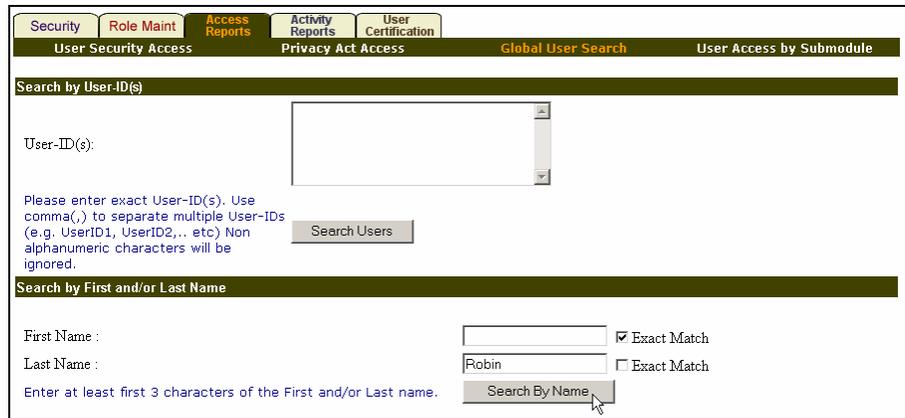
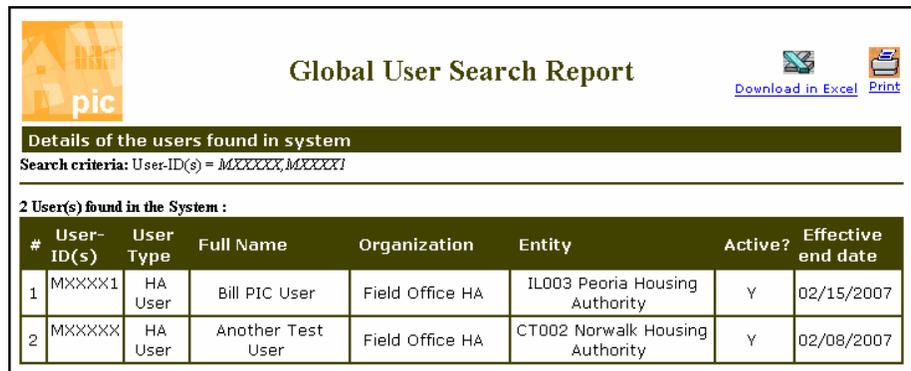


Figure 5-14: Searching for a user by name

Information listed in a Global User Search report

The Global User Search report contains a header and one table listing report data. A sample Global User Search report is shown in Figure 5-15.



#	User-ID(s)	User Type	Full Name	Organization	Entity	Active?	Effective end date
1	MXXXXX1	HA User	Bill PIC User	Field Office HA	IL003 Peoria Housing Authority	Y	02/15/2007
2	MXXXXXX	HA User	Another Test User	Field Office HA	CT002 Norwalk Housing Authority	Y	02/08/2007

Figure 5-15: Sample Global User Search report

The report header lists the user IDs entered when generating the report.

The following information is listed in the report table:

- User ID
- User type
- Full name of the user
- Organization to which the user belongs (common values that may appear in this column include Field Office HA, Field Office, and HQ Office)
- Entity (typically, the name of the organization)
- Whether or not the user ID is active (“Y” indicates an active ID; “N” indicates an inactive ID)
- Effective end date (account expiration date)

Generating a User Access by Submodule report

The User Access by Submodule report lists users who have access to a particular submodule.

Follow these steps to generate a User Access by Submodule report:

Step	Action/Result
1. Select the Access Reports tab.	The User Security Access report page is the default page displayed.
2. Select User Access by Submodule (circled in Figure 5-16).	The User Access by Submodule report page appears (see Figure 5-17).

The screenshot shows a web application interface with a top navigation bar containing tabs: Security, Role Maint, Access Reports, Activity Reports, and User Certification. Below the navigation bar, there are several menu items: User Security Access, Privacy Act Access, Global User Search, and User Access by Submodule. The 'User Access by Submodule' tab is circled in red. Below the navigation bar, there is a 'Select View' dropdown set to 'FO HA User' and a 'Field Office HA' dropdown set to 'IL003 Peoria Housing Authority'. A 'User Search' section includes a search box, a 'Search' button, and dropdowns for 'Select Status' (set to 'ALL') and 'Select ID Type' (set to 'ALL'). Below the search section is a 'Security List' header and a table with columns: User ID, User Name, User Type, ID Type, and Status.

Figure 5-16: Accessing the User Access by Submodule report page

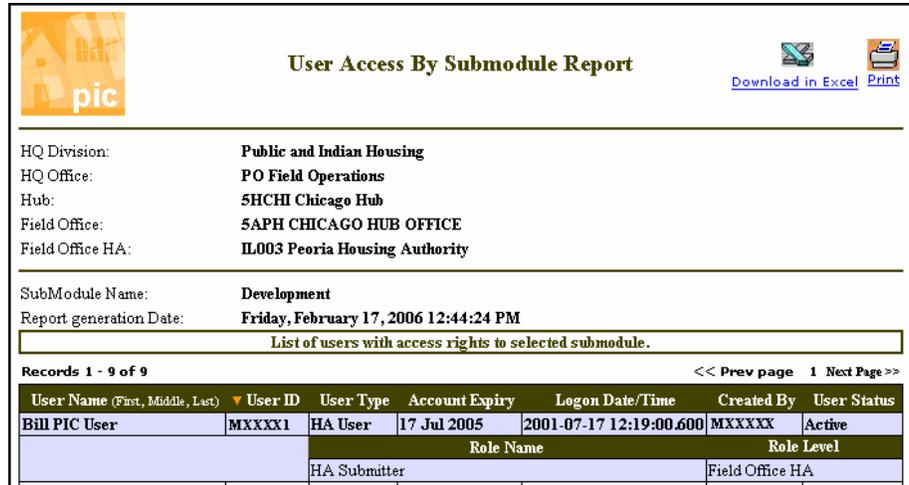
The screenshot shows the 'User Access by Submodule' report page. It features a 'Data Filters for User Access by Submodule Report' section with dropdowns for 'User Types' (set to 'ALL'), 'Select Status' (set to 'ALL'), and 'Select Submodule' (set to 'User Profile'). Below this is a 'Display Filters for User Access by Submodule Report' section with dropdowns for 'No of rows to display' (set to '50 Rows per page') and 'Sort report data by' (set to 'User Name' and 'in Descending order'). A 'Generate Report' button is located at the bottom right of the page.

Figure 5-17: User Access by Submodule report page

Step	Action/Result
3. Enter the report data filters: <ol style="list-style-type: none"> a. Select the user type from the User Types drop-down menu. b. Select the status of the user's account from the Select Status drop-down menu. c. Select the submodule from the Select Submodule drop-down menu. 	
4. Enter the report display filters: <ol style="list-style-type: none"> d. Select the number of rows you want displayed on each page from the No of rows to display drop-down menu. e. Select how you want the report data sorted from the Sort report data by drop-down menu; then select the order in which you want the data displayed from the adjacent drop-down menu. 	
5. Select Generate Report .	

Information listed in a User Access by Submodule report

The User Access by Submodule report contains a report header and one table listing report data. A sample User Access by Submodule report is shown in Figure 5-18.



The screenshot shows a report titled "User Access By Submodule Report" with a "pic" logo. It includes report details such as HQ Division (Public and Indian Housing), HQ Office (PO Field Operations), Hub (5HCHI Chicago Hub), Field Office (5APH CHICAGO HUB OFFICE), and Field Office HA (IL003 Peoria Housing Authority). The SubModule Name is Development, and the Report generation Date is Friday, February 17, 2006 12:44:24 PM. Below this is a table listing users with access rights to the selected submodule. The table has columns for User Name, User ID, User Type, Account Expiry, Logon Date/Time, Created By, and User Status. The first row shows "Bill PIC User" with User ID "MXXXX1", User Type "HA User", Account Expiry "17 Jul 2005", Logon Date/Time "2001-07-17 12:19:00.600", Created By "MXXXXX", and User Status "Active". Below this is a table with columns for Role Name and Role Level, showing "HA Submitter" and "Field Office HA".

User Name (First, Middle, Last)	User ID	User Type	Account Expiry	Logon Date/Time	Created By	User Status
Bill PIC User	MXXXX1	HA User	17 Jul 2005	2001-07-17 12:19:00.600	MXXXXX	Active

Role Name	Role Level
HA Submitter	Field Office HA

Figure 5-18: Sample User Access by Submodule report

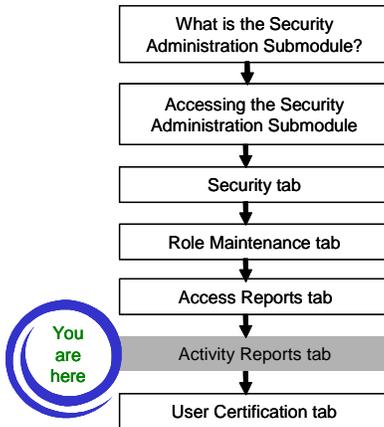
The report header may contain the following information:

- HQ division
- HQ office
- Hub
- Field office
- Field office HA
- Submodule name
- Report generation date

The following information is listed in the report table:

- User name
- User ID
- User type
- Logon date and time
- Created by (the user ID of the Security Coordinator who created the account)
- User status (the status of the user's account—active or inactive)
- Role name
- Role level

6. Activity Reports tab



This section discusses the following topics:

- *Activity Reports tab overview* on page 6-1
- *Guidelines for using the Activity Reports tab* on page 6-2
- *Navigating to the Activity Reports tab* on page 6-4
- *Generating a User Activity Query report* on page 6-5
- *Generating a New Users report* on page 6-8
- *Generating an Improper Logoff report* on page 6-11
- *Generating a User Account Usage report* on page 6-14

Activity Reports tab overview

The Activity Reports tab has four sub-tabs that can help generate activity-related reports. A description of the reports follows.

- **User Activity Query**
The report provides detailed user activity information, including the number of times a user logged on to the system, the average time connected, the total time connected, and the operating system and browser of the computer used to access the system.
- **New Users**
The report lists users added to the system during a specified time frame.
- **Improper Logoff**
The report provides detailed information about connections to the PIC system terminated by an action other than selecting **Logoff**.
The report lists information such as user names and descriptions for why connections were terminated.
- **User Account Usage**
The report lists users who have not accessed the system within a specified time frame.

Guidelines for using the Activity Reports tab

Disabling pop-up blockers

The reports discussed in this section are displayed in separate windows. Pop-up blocking software may prevent the reports from generating or displaying properly. Because there are many pop-up blocking tools, this manual does not explain how to disable pop-up blockers. Refer to your pop-up blocker's Help files for detailed instructions on how to disable it.

For information on system requirements and recommended settings for using the PIC system, go to <http://www.hud.gov/offices/pih/systems/pic/sr/>.

Tip: If you use Internet Explorer to generate a report, press and hold the CTRL key immediately before selecting the **Generate Report** button to disable the pop-up blocker temporarily. Make sure to hold the key down while the report generates.

Navigating between report pages

Some reports may contain more than one page of information. To view another page of information, select the numbered link for that page or select **Next Page**; select **Prev page** to return to the previous page of information (see Figure 6-1).

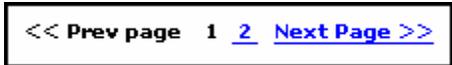
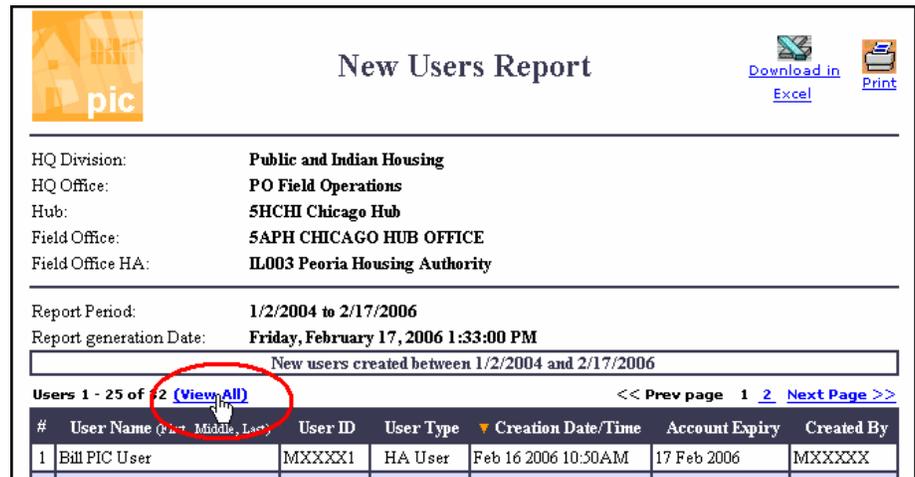


Figure 6-1: Navigating between report pages

Some reports allow you to view the entire report on a single report page. If you see **View All** on a report page, you can select it to view the entire report on a single page (see Figure 6-2).



New Users Report

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

HQ Division: **Public and Indian Housing**
HQ Office: **PO Field Operations**
Hub: **5HCHI Chicago Hub**
Field Office: **5APH CHICAGO HUB OFFICE**
Field Office HA: **IL003 Peoria Housing Authority**

Report Period: **1/2/2004 to 2/17/2006**
Report generation Date: **Friday, February 17, 2006 1:33:00 PM**

New users created between 1/2/2004 and 2/17/2006

Users 1 - 25 of 2 **(View All)** << Prev page 1 2 Next Page >>

#	User Name (Last, Middle, Last)	User ID	User Type	Creation Date/Time	Account Expiry	Created By
1	Bill PIC User	MXXXXX1	HA User	Feb 16 2006 10:50AM	17 Feb 2006	MXXXXXX

Figure 6-2: Viewing an entire report on a single page

Choosing a report output option

All of the reports discussed in this section can be printed or downloaded to a Microsoft Excel™ spreadsheet.

Select the icon for the desired output option (see Figure 6-3).



Figure 6-3: Choosing a report output option

Closing report windows

When closing a report window, make sure to select the “x” in the report window (circled in Figure 6-4) and not the “x” in the main window. You must re-logout to the PIC system if you mistakenly close the main PIC window.

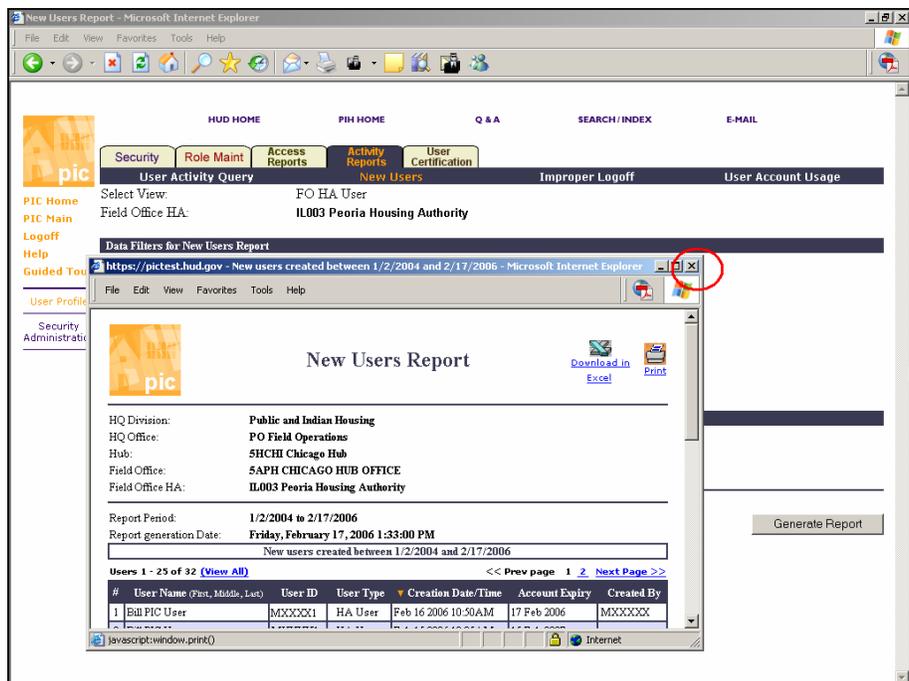


Figure 6-4: Closing a report window

Navigating to the Activity Reports tab

Follow these steps to navigate to the Activity Reports tab:

Step	Action/Result
1. Log on to the PIC system.	
2. Move the cursor over the PIC Maintenance button.	
3. Select the Security Administration hyperlink.	
4. Select the Activity Reports tab (see Figure 6-5).	

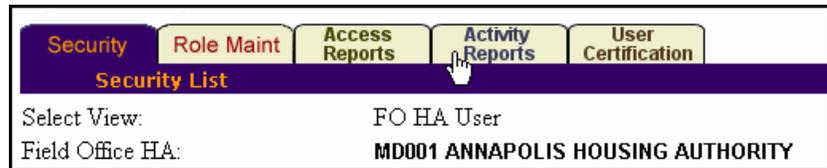


Figure 6-5: Navigating to the Activity Reports tab

Generating a User Activity Query report

The User Activity Query report lists detailed information regarding how and when a user accesses the PIC system.

Follow these steps to generate a User Activity Query report:

Step	Action/Result
1. Select the Activity Reports tab.	The User Activity Query report page is the default page displayed (see Figure 6-6).
2. Locate the user in the Security List at the bottom of the page.	
3. In the Activity Period section of the page, type the report start date in the From field and type the report end date in the To field.	
4. Select the User ID hyperlink to generate the report.	

Figure 6-6: User Activity Query report page

Information listed in a User Activity Query report

The User Activity Query report contains a report header and two tables that list report data. A sample User Activity Query report is shown in Figure 6-7.

User Activity Information										
Selected View:	FO HA User									
HQ Division:	Public and Indian Housing									
HQ Office:	PO Field Operations									
Hub:	5HCHI Chicago Hub									
Field Office:	5APH CHICAGO HUB OFFICE									
Field Office HA:	IL003 Peoria Housing Authority									
Report Start Date:	1/16/2006							Report End Date:	2/16/2006	
First Name:	Bill									
Last Name:	User									
Middle Initial:	PIC									
Phone Number:	2405551212									
Phone Number Extn:										
E-Mail Address:	billuser@domain.gov									
<i>Activity Report</i>										
Summary Report										
Total Connect Time			Total Number of Logins			Average Connect Time				
0:3:85			3			0:0:88				
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	02/16/2006 10:59:39	Windows NT	Microsoft Internet Explorer 6.0	xx.xxx.xx.xxx	HLANNWT001	CRRNT	02/16/2006 10:59:39	*	*	
2	02/16/2006 10:58:46	Windows NT	Microsoft Internet Explorer 6.0	xx.xxx.xx.xxx	HLANNWT001	LOGOFF	02/16/2006 10:58:46	02/16/2006 10:59:18	0:0:32	
3	02/16/2006 10:54:53	Windows NT	Microsoft Internet Explorer 6.0	xx.xxx.xx.xxx	HLANNWT003	ABNRML	02/16/2006 10:54:53	02/16/2006 10:58:46	0:3:53	
* Insufficient Data.										
** Session Timed out.										
1 - 3 of 3										

Figure 6-7: Sample User Activity Query report

The report header consists of two sections. The first section may contain the following information:

- HQ division
- HQ office
- Hub
- Field office
- Field office HA
- Report start date
- Report end date

The second section of the report header contains the following user-specific information:

- First name
- Last name
- Middle Initial
- Phone number
- Phone number extension
- E-mail address

A description of the report tables and the information they contain follows.

Table	Information Presented
Summary Report	The Summary Report table lists the following information: <ul style="list-style-type: none">• Total time connected• Total number of logins• Average time connected
Detailed Report	The Detailed Report table lists the following information: <ul style="list-style-type: none">• Date• Operating system• Browser name and version• Client IP address• Web server name• Activity status• Login begin• Login end• Total time logged on

Generating a New Users report

The New Users report lists new users added to the system for a specified date range.

Follow these steps to generate a New Users report:

Step	Action/Result
1. Select the Activity Reports tab.	The User Activity Query report page is the default page displayed.
2. Select New Users (circled in Figure 6-8).	The New Users report page appears (see Figure 6-9).

The screenshot shows the 'User Activity Query' report page. At the top, there are tabs for 'Security', 'Role Maint', 'Access Reports', 'Activity Reports', and 'User Certification'. The 'Activity Reports' tab is active, and the 'New Users' option is circled in red. Below the tabs, there are sections for 'User Search' and 'Activity Period'. The 'User Search' section includes a search for 'User Id' or 'Last Name', an 'Enter Search Text' field, and dropdown menus for 'Select Status' (ALL) and 'Select ID Type' (ALL). The 'Activity Period' section includes 'From' and 'To' date fields with values 12/26/2005 and 1/26/2006 respectively. Below these sections is a 'Security List' header and a table with columns for 'User ID', 'User Name', 'User Type', 'ID Type', and 'Status'.

Figure 6-8: Accessing the New Users report page

The screenshot shows the 'New Users' report page. At the top, there are tabs for 'Security', 'Role Maint', 'Access Reports', 'Activity Reports', and 'User Certification'. The 'Activity Reports' tab is active, and the 'New Users' option is selected. Below the tabs, there are sections for 'Data Filters for New Users Report' and 'Display Filters for New Users Report'. The 'Data Filters' section includes a 'Report Period' dropdown set to 'Custom Dates (From and To dates required)', 'From' and 'To' date fields with values 1/11/2006 and 1/26/2006 respectively, and a 'User Types' dropdown set to 'ALL'. The 'Display Filters' section includes 'No of rows to display' set to '50 Rows per page' and 'Sort report data by' set to 'User creation Date/Time' in 'Descending order'. A 'Generate Report' button is located at the bottom right.

Figure 6-9: New Users report page

Step	Action/Result
3. Enter the report data filters: <ol style="list-style-type: none"> a. Select a pre-defined report range from the Report Period drop-down menu; or, use the <i>Custom Dates</i> default and type dates in the From and To fields. b. Select the user type from the User Types drop-down menu. 	
4. Enter the report display filters: <ol style="list-style-type: none"> a. Select the number of rows you want to display per page from the No of rows to display drop-down menu. b. Select how you want the report data sorted from the Sort report data by drop-down menu; then select the order in which you want the data displayed from the adjacent drop-down menu. 	
5. Select Generate Report .	

Information listed in a New Users report

The New Users report contains a report header and one table listing report data. A sample New Users report is shown in Figure 6-10.

#	User Name (First, Middle, Last)	User ID	User Type	Creation Date/Time	Account Expiry	Created By
1	Sara PIC User	MXXXXX9	HA User	Feb 16 2006 10:50AM	17 Feb 2006	MXXXXXX
2	Bill PIC User	MXXXXX1	HA User	Feb 15 2006 10:35AM	15 Feb 2007	MXXXXXX

Figure 6-10: Sample New Users report

The report header contains the following information:

- HQ division
- HQ office
- Hub
- Field office
- Field office HA
- Report period
- Report generation date

The report table contains the following information:

- User name
- User ID
- User type
- Creation date and time (date and time the user was added to the system)
- Account expiry (account expiration date)
- Created by (user ID of the Security Coordinator who created the account)

Generating an Improper Logoff report

The Improper Logoff report lists detailed information about connections to the PIC system terminated by an action other than selecting **Logoff**.

Follow these steps to generate an Improper Logoff report:

Step	Action/Result
1. Select the Activity Reports tab.	The User Activity Query report page is the default page displayed.
2. Select Improper Logoff (circled in Figure 6-11).	The Improper Logoff report page appears (see Figure 6-12).

The screenshot shows the 'User Activity Query' report page. At the top, there are navigation tabs: Security, Role Maint, Access Reports, Activity Reports, and User Certification. The 'Activity Reports' tab is active, and the 'Improper Logoff' option is highlighted with a red circle. Below the tabs, the page displays 'Select View: FO HA User' and 'Field Office HA: MD001 ANNAPOLIS HOUSING AUTHORITY'. There are sections for 'User Search' and 'Activity Period' with various input fields and dropdown menus. At the bottom, a 'Security List' table is partially visible with columns for User ID, User Name, User Type, ID Type, and Status.

Figure 6-11: Accessing the Improper Logoff report page

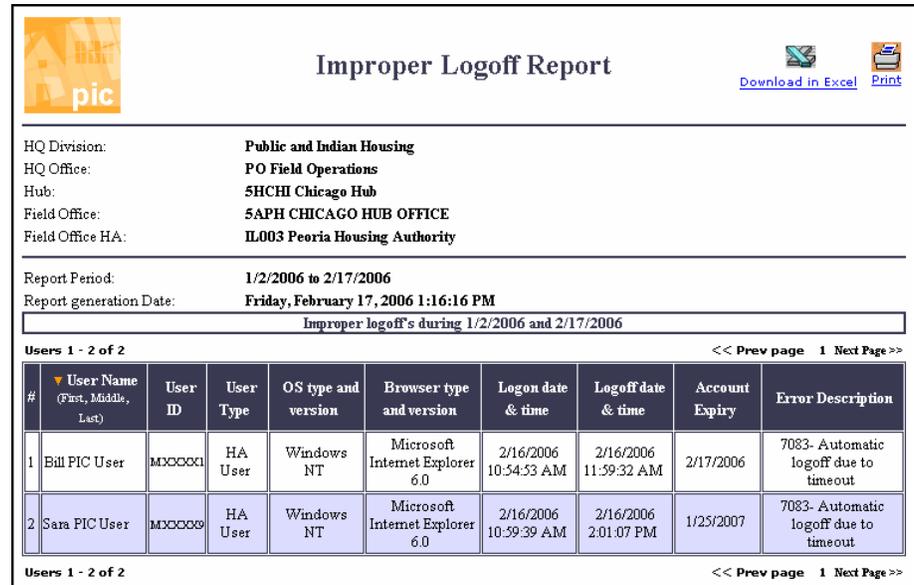
The screenshot shows the 'Improper Logoff' report page. At the top, the 'Improper Logoff' tab is selected. The page displays 'Select View: FO HA User' and 'Field Office HA: MD001 ANNAPOLIS HOUSING AUTHORITY'. Below this, there are two filter sections: 'Data Filters for Improper Logoff Report' and 'Display Filters for Improper Logoff Report'. The 'Data Filters' section includes a 'Report Period' dropdown set to 'Custom Dates (From and To dates required)', with 'From' and 'To' date fields set to 1/11/2006 and 1/26/2006 respectively. The 'User Types' dropdown is set to 'ALL'. The 'Display Filters' 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 6-12: Improper Logoff report page

Step	Action/Result
3. Enter the report data filters: <ol style="list-style-type: none"> a. Select a pre-defined report range from the Report Period drop-down menu; or, use the <i>Custom Dates</i> default and type dates in the From and To fields. b. Select the user type from the User Types drop-down menu. 	
4. Enter the report display filters: <ol style="list-style-type: none"> a. Select the number of rows you want displayed on each page from the No of rows to display drop-down menu. b. Select how you want the report data sorted from the Sort report data by drop-down menu; then select the order in which you want the data displayed from the adjacent drop-down menu. 	
5. Select Generate Report .	

Information listed in an Improper Logoff report

The Improper Logoff report contains a report header and one table listing report data. A sample Improper Logoff report is shown in Figure 6-13.



The screenshot shows a report titled "Improper Logoff Report" with a PIC logo on the left and "Download in Excel" and "Print" links on the right. The report header contains the following information:

HQ Division: **Public and Indian Housing**
HQ Office: **PO Field Operations**
Hub: **SHCHI Chicago Hub**
Field Office: **5APH CHICAGO HUB OFFICE**
Field Office HA: **IL003 Peoria Housing Authority**

Report Period: **1/2/2006 to 2/17/2006**
Report generation Date: **Friday, February 17, 2006 1:16:16 PM**

Improper logoffs during 1/2/2006 and 2/17/2006

Users 1 - 2 of 2 << Prev page 1 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	Bill PIC User	MXXXXX1	HA User	Windows NT	Microsoft Internet Explorer 6.0	2/16/2006 10:54:53 AM	2/16/2006 11:59:32 AM	2/17/2006	7083- Automatic logoff due to timeout
2	Sara PIC User	MXXXXX9	HA User	Windows NT	Microsoft Internet Explorer 6.0	2/16/2006 10:59:39 AM	2/16/2006 2:01:07 PM	1/25/2007	7083- Automatic logoff due to timeout

Users 1 - 2 of 2 << Prev page 1 Next Page >>

Figure 6-13: Sample Improper Logoff report

The report header contains the following information:

- HQ division
- HQ office
- Hub
- Field office
- Field office HA
- Report period
- Report generation date

The report table contains the following information:

- User name
- User ID
- User type
- Operating System (OS) type and version
- Browser type and version
- Logon date and time
- Logoff date and time
- Account expiry (account expiration date)
- Error description (explanation of why the connection to the PIC system was terminated)

Generating a User Account Usage report

The User Account Usage report lists users who have not accessed the system within a specified time frame.

Follow these steps to generate a User Account Usage report:

Step	Action/Result
1. Select the Activity Reports tab.	The User Activity Query report page is the default page displayed.
2. Select User Account Usage (circled in Figure 6-14).	The User Account Usage report page appears (see Figure 6-15).

The screenshot shows a web application interface with a top navigation bar containing tabs: Security, Role Maint, Access Reports, Activity Reports, and User Certification. Below the navigation bar, there are several menu items: User Activity Query, New Users, Improper Logoff, and User Account Usage. The 'User Account Usage' menu item is circled in red. Below the navigation bar, there are fields for 'Select View' (FO HA User) and 'Field Office HA' (MD001 ANNAPOLIS HOUSING AUTHORITY). There is also a 'User Search' section with a search box and dropdown menus for 'Select Status' and 'Select ID Type'. Below that is an 'Activity Period' section with 'From' and 'To' date fields. At the bottom, there is a 'Security List' section showing a table of users.

Figure 6-14: Accessing the User Account Usage report page

The screenshot shows the 'User Account Usage' report page. The top navigation bar is the same as in Figure 6-14. Below the navigation bar, there are fields for 'Select View' (FO HA User) and 'Field Office HA' (MD001 ANNAPOLIS HOUSING AUTHORITY). Below that is a 'Data Filters for User Account Usage Report' section with dropdown menus for 'User Inactivity Period' (Last one week), 'User Types' (ALL), and 'Select Status' (ALL). Below that is a 'Display Filters for User Account Usage Report' section with dropdown menus for 'No of rows to display' (50 Rows per page) and 'Sort report data by' (User Name in Descending order). At the bottom right, there is a 'Generate Report' button.

Figure 6-15: User Account Usage report page

Step	Action/Result
3. Enter the report data filters: <ol style="list-style-type: none"> a. Select a pre-defined date range from the User Inactivity Period drop-down menu. b. Select the user type from the User Types drop-down menu. c. Select a user ID status from the Select Status drop-down menu. 	
4. Enter the report display filters: <ol style="list-style-type: none"> a. Select the number of rows you want displayed per page from the No of rows to display drop-down menu. b. Select how you want the report data sorted from the Sort report data by drop-down menu; then select the order in which you want the data displayed from the adjacent drop-down menu. 	
5. Select Generate Report .	

Information listed in a User Account Usage report

The User Account Usage report contains a report header and one table listing report data. A sample User Account Usage report is shown in Figure 6-16.

User Name (First, Middle, Last)	User ID	User Type	Last Logon Date/Time	Account Expiry Date	User Status
Jane PIC User	MXXXXX	HA User	2001-07-17 12:19:00.600	17 Jul 2005	Active

Figure 6-16: Sample User Account Usage report

The report header may contain the following information:

- HQ division
- HQ office
- Hub
- Field office
- Field office HA
- Report period
- Report generation date

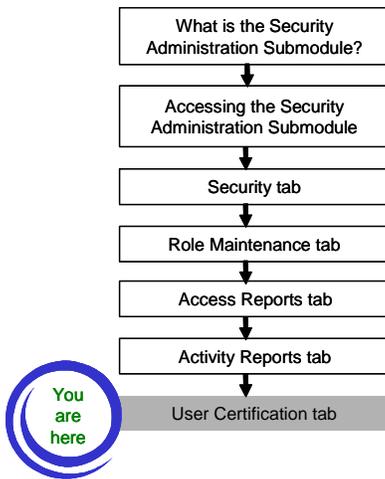
The report table contains the following information:

- User name
- User ID
- User type
- Last logon date and time
- Account expiry date (account expiration date)
- User status
- Role name
- Role level

7. User Certification tab

The User Certification tab is under development and will not be available for use until mid to late 2006. The User Certification tab will be used to manage user certifications and re-certifications.

This section of the user manual will be updated when development of the User Certification tab is complete.



Appendix A

Password Security

Password Security

This appendix discusses the following topics:

- Choosing a strong password
- Protecting your password

Choosing a strong password

A password is a secret sequence of characters that verifies a user's identity and authorizes access to a computer system.

Passwords are the first level of security for the Public and Indian Housing Information Center (PIC) system.

PIC system security can be compromised if users commit any of the following errors:

- Select easily guessed passwords
- Share passwords
- Write their passwords down
- Use system or application default passwords
- Fail to protect their passwords
- Fail to change their passwords

PIC system users must make sure to choose strong passwords. Users must follow these guidelines when choosing a strong password:

- Use a mix of lower and upper case letters, numbers, and non-words; for example, 175uPdOwn or fLoOpEr29.
- Do not use obvious passwords, such as birthdays, names of family members, names of pets, or the name of your home town.
- If you are required to select a secret question and provide an answer to that question, do not select an obvious question.

Protecting your password

PIC system users are responsible for protecting their passwords. Users must follow these guidelines to protect their passwords:

- Do not share user IDs or passwords.
Think of a password as a personal identification number (PIN) for your bank automated teller machine (ATM) card. Would you openly share it with someone?
- Do not write your password on a piece of paper and leave it on your desk or in your desk drawer.
- If you must make a note of your password, keep the paper with you at all times or lock it in a location for which only you have the key.
- Do not use the same password for multiple accounts.
- Do not recycle the same passwords too often.
- Change your passwords regularly; three months is the recommended interval for changing passwords.
Note: The PIC system prompts users to change passwords every 60 days.
- Change your password immediately if you think it has been compromised.

Appendix B

Security Concepts and Best Practices

Security Concepts and Best Practices

This appendix discusses the following topics:

- Privacy Act of 1974 and the PIC system
- Security best practices

Privacy Act of 1974 and the PIC system

The Privacy Act of 1974 was created to guard against the misuse of personal information in the possession of Federal agencies, such as the United States Department of Housing and Urban Development (HUD).

The following personal information is protected by the Privacy Act:

- Home address
- Phone numbers
- Medical history
- Social Security information
- Identification codes; for example, user IDs
- Biographical history
- Criminal history
- Educational history
- Employment history
- Terms of employment
- Income-related information

Because many sections of the HUD PIC system contain personal information, those sections are protected by the Privacy Act. Users are required to accept a Privacy Act Statement and Compliance Notice (see Figure B-1) in order to access protected information.

Note: Violators of the Privacy Act may be charged with a misdemeanor and fined up to \$5,000 per violation.

Privacy Act Statement and Compliance Notice

Welcome Brian Labarta! 1/27/2006 10:59:44 AM

IMPORTANT: Please read the following carefully.

Legal Warning

Misuse of Federal Information through the HUD Secure Connection web site falls under the provisions of Title 18, United States Code, Section 1030. This law specifies penalties for exceeding authorized access, alterations, damage, or destruction of information residing on Federal Computers.

Privacy Statement

Information contained in this system is subject to the Privacy Act of 1974 (5 U.S.C. 552a, as amended). Personal information contained in this system may be used only by authorized persons in the conduct of official business. Any individual responsible for unauthorized disclosure or misuse of personal information will be prosecuted to the maximum extent possible under law.

Warning Notice

The PIH Information Center (PIC) System supports Internet Explorer version 5.0 and above. Other browsers may not be compatible with this system.

Your compliance is requested because you may have access rights to certain parts of PIC system which are covered by the Privacy Act. You may choose to decline and can still access the parts of the PIC system not covered by the Privacy Act as per your access privileges. All attempts to access the information (covered by Privacy act) will be logged into the PIC database irrespective of compliance status.

Figure B-1: Privacy Act Statement and Compliance Notice

Security best practices

Computer users can minimize the risk of inadvertently disclosing data protected by the Privacy Act by following the guidelines below. The guidelines address several security areas, including physical security, computer security, data protection, and data disposal.

- Be aware of your work environment.
- Make sure others are not able to easily view your computer monitor.
- Managers should restrict access to computer rooms.
- Place important items in desk drawers and lock the drawers if you must leave your work area.
- Maintain files of all source documents entered in the PIC system; lock the files in a safe place.
- Log off or lock your computer if you leave your work area.
- Remove diskettes and CD-ROMs from your computer and lock them in a safe place when you are done using them.
- Remove Universal Serial Bus (USB) flash drives from your computer; keep them with you at all times or lock them in a safe place.
- Do not discard hard copies of sensitive information in a waste basket; you must shred or burn hard copies of sensitive information.
- Delete data from diskettes.
- Delete data from USB flash drives.
- Remove sensitive information from computer hard drives if they are sent out for maintenance.

Appendix C

HUD System User Responsibilities

HUD System User Responsibilities

This appendix discusses the following topics:

- User responsibilities
- Examples of inappropriate use and misuse of HUD systems

User responsibilities

One person alone cannot protect an organization from information security threats. All users should take the time to learn about information security to help maintain a safe and secure work environment. The most valuable asset of an organization in combating information security threats is the eyes and ears of its many computer users.

Users are responsible for everything that takes place in their workspace as well as activities performed on their desktop computer or laptop computer.

The following responsibilities apply to internal users (HUD employees) and external users (for example, HA users and guest users) of HUD computer systems. The responsibilities may also apply to users of HA computer systems.

- Safeguard information contained in HUD's computer systems from unauthorized or inadvertent modification, disclosure, destruction, denial of service, and use. Your organization's systems, networks, and internal Web sites are for official use and authorized purposes and are subject to monitoring and security testing.
- Report known or suspected incidents immediately.
- Comply with organizational safeguards, policies, and procedures to prevent unauthorized access to computer systems.
- Comply with the terms of software licenses and only use licensed and authorized software. Do not install single-license software on shared hard drives or servers.
- Recognize the accountability assigned to a User ID and password. Each user must have a unique access to systems as the User IDs identify an individual's actions on work systems and on the Internet. Individual user activity may be recorded and reviewed.
- Use authorized virus scanning software on the workstation or PC.
- Know the source before using diskettes or downloading files. Scan files for viruses before opening them.
- Know your data and properly protect all data inputs and outputs according to their sensitivity and value. Label sensitive media and ensure that sensitive information is removed from hard disks that are disposed of or sent out for maintenance.
- Do not use shared drives to relay sensitive information unless that information is password-protected and the folder within the shared drive has access set up only for those who are authorized to work with the data.

- Use e-mail for official business, and ensure that e-mail messages are professional and accurately state your organization's policies and positions.
- Do not send sensitive information over the Internet unless it has been encrypted. See your ISSO for assistance with encryption.
- Do not generate or distribute offensive or inappropriate e-mail messages, images, or sound files.
- Do not open unsolicited or suspicious e-mail messages or their attachments; do not forward chain mail.
- Limit distribution of e-mail to only those who need to receive it.
- Ask your supervisor or your local IT security point of contact, if you have any questions about your security responsibilities.

Examples of inappropriate use or misuse of HUD systems

The following examples of inappropriate use or misuse of HUD computer systems apply to internal users (HUD employees) and external users (for example, HA users and guest users) of HUD computer systems:

- Any personal use that could cause congestion, delay, or disruption of service to any Government system or equipment. For example, continuous data streams, video, sound, or other large file attachments that degrade performance of HUD's network.
- Using HUD systems as a staging ground or platform to gain unauthorized access to other systems.
- Creating, copying, sending, or forwarding chain letters or other unauthorized mass mailings regardless of the subject matter.
- Participating in activities that are illegal, inappropriate, or offensive to coworkers or the public. Such activities include hate speech, or material that ridicules others on the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation.
- Creating, downloading, viewing, storing, copying, or transmitting of sexually explicit or sexually-oriented materials or materials related to gambling, illegal weapons, terrorist activities, and any illegal or prohibited activities.
- Using HUD IT assets for commercial purposes or in support of "for profit" activities or in support of other outside employment or business activity (for example, consulting for pay, sales or administration of business transactions, sale of goods or services).
- Using HUD resources to engage in any outside fund-raising activity, endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity.
- Posting HUD information to external newsgroups, bulletin boards, or other public forums without authorization. This includes any use that could create the perception that the communication was made in one's official capacity as a HUD employee (unless appropriate approval has been obtained), or uses that are at odds with the HUD's mission or positions.
- Without authorization, acquiring, using, reproducing, transmitting, or distributing any controlled information including computer software and data that includes private information; copyrighted, trademarked, or material with other intellectual property rights beyond fair use; proprietary data; or export-controlled software or data.

Appendix D
Role List and Descriptions

Role Descriptions

This appendix lists roles and role descriptions for United States Department of Housing and Urban Development (HUD) users, Housing Authority (HA) users, and guest users of the PIC system.

The roles listed in the table below are limited to the Web Access Security Subsystem (WASS) user group only.

Module	Submodule	Role Name	Role Description	Type of User
PIH Maintenance	User Profile	<i>User Profile</i>	Edit user information and change passwords.	All users
	Security Administration	<i>Security Coordinator</i>	Perform security administration tasks. Note: Role is currently under development.	HA User
		<i>Recertify HA Security Admins</i>	Re-certify HA Security Admins and view reports.	HA User
		<i>HA Certifier</i>	Certify HA users on a quarterly basis.	HA User
		<i>Sec Coord</i>	View, edit, and create users.	HUD User
		<i>Read Only</i>	View security reports and data.	HUD User
		<i>Read Only</i>	View security reports and data.	Guest
PIH Information	SEMAP	<i>Read Only - SEMAP</i>	View information in SEMAP.	HA User
		<i>Edit SEMAP Role</i>	View and edit information in SEMAP.	HA User
		<i>Submit SEMAP Role</i>	Create, view, edit, and submit information in SEMAP.	HA User
		<i>Read only SEMAP</i>	View information in SEMAP.	HUD User
		<i>Edit SEMAP Role</i>	View and edit information in SEMAP; view reports.	HUD User
		<i>Approve SEMAP</i>	View, edit, and approve SEMAP profiles and comments; view reports.	HUD User
		<i>HQ SEMAP Appeal</i>	Approve or reject HQ level appeals.	HUD User
		<i>Read Only - Semap</i>	View information in SEMAP.	Guest

Module	Submodule	Role Name	Role Description	Type of User
PIH Information	Risk Assessment (HUD only)	<i>Read Only Role</i>	View Risk Assessment data, comments, and reports.	HUD User
		<i>Edit Risk Assessment</i>	View and edit Risk Assessment data and comments; view reports.	HUD User
		<i>Approve R.A. Data</i>	View, edit, and approve Risk Assessment data and comments; view reports.	HUD User
		<i>Read Only Role</i>	View Risk Assessment data.	Guest
Housing Inventory	Housing Authority	<i>Read Only Role</i>	View housing authority information, including Occupancy report.	HA User
		<i>Edit HA Role</i>	View and edit housing authority information, including Occupancy report.	HA User
		<i>Submit HA Role</i>	View, edit, and submit housing authority information, including Occupancy report.	HA User
		<i>Read Only Role</i>	View information in Housing Authority.	HUD User
		<i>HA Exec Approve</i>	View, edit, and approve information in Housing Authority.	HUD User
		<i>Read Only Role</i>	View Housing Authority information, including Occupancy report.	Guest
	Development	<i>Read Only - Privacy</i>	View all building and unit data.	HA User
		<i>Edit Development</i>	View and edit all building, unit, and AMP data.	HA User
		<i>Submit Development</i>	View, edit, and submit all building, unit, and AMP data.	HA User
		<i>Read Only - Privacy</i>	View all building and unit data.	HUD User
		<i>Edit Development</i>	View and edit all building, unit, and AMP data.	HUD User
		<i>HUD Approve</i>	View, edit, submit, and approve all building, unit, and AMP data.	HUD User
		<i>Read Only - Privacy</i>	View all building, unit, and AMP data.	Guest

Module	Submodule	Role Name	Role Description	Type of User
Housing Inventory	Demolition & Disposition	<i>Read Only Role</i>	View Demolition and Disposition data.	HA User
		<i>Edit Demo Dispo</i>	View and edit Demolition and Disposition applications.	HA User
		<i>Submit Demo Dispo</i>	View, edit, and submit Demolition and Disposition applications.	HA User
		<i>Read Only Role</i>	View Demolition and Disposition data.	HUD User
		<i>Edit Demo Dispo</i>	View and edit Demolition and Disposition applications.	HUD User
		<i>Approve DD-FO</i>	View Demolition and Disposition data; approve removal transactions.	HUD User
		<i>SAC Staff</i>	SAC staff members can create and view applications; add attachments or comments to applications.	HUD (SAC) User
		<i>SAC Mgt</i>	SAC Management (Director/Deputy Director) can approve and disapprove applications.	HUD (SAC) User
		<i>Read Only Role</i>	View Demolition and Disposition data.	Guest
Executive Summary	Executive Summary	<i>Read Only Role</i>	View housing authority summary information.	HA User
		<i>Exec Read Only</i>	View housing authority summary information.	HUD User
		<i>Read Only Role</i>	View housing authority summary information.	Guest
MTCS (Form-50058)	Submission	<i>Read Only Role</i>	View upload file error reports.	HA User
		<i>Submit Form-50058</i>	Submit files and view error reports.	HA User
		<i>Read Only Role</i>	View upload file error reports.	HUD User
		<i>Submit Form-50058</i>	Submit files with PHA permission and view error reports.	HUD User
		<i>Read Only Role</i>	View upload file error reports.	Guest

Module	Submodule	Role Name	Role Description	Type of User
MTCS (Form-50058)	Viewer	<i>Read Only Role</i>	View all sections of Form-50058 and reports, including privacy act data.	HA User
		<i>Submit EOP Role</i>	View all sections of Form-50058 and reports including privacy act data; submit online End of Participation (EOPs).	HA User
		<i>Read Only Role</i>	View all sections of Form-50058 and reports, including privacy act data.	HUD User
		<i>Read Only Role</i>	View all sections of Form-50058 and reports, including privacy act data.	Guest
	Reports	<i>Read Only Role</i>	View Form-50058 Reports with privacy act data.	HA User
		<i>Read Only Role</i>	View Form-50058 Reports with privacy act data.	HUD User
		<i>Read Only Role</i>	View Form-50058 Reports with privacy act data.	Guest
	Tenant ID Management	<i>Read Only - Privacy</i>	View Tenant ID Management reports.	HA User
		<i>Submit Role</i>	Generate and replace AID information; view Tenant ID Management reports.	HA User
		<i>Validate SSN-AID</i>	Generate and replace AID information; view Tenant ID Management reports. Note: This role may have further capabilities at a later time.	HA User
		<i>Read Only - Privacy</i>	View Tenant ID Management reports.	HUD User
		<i>Read Only - Privacy</i>	View Tenant ID Management reports.	Guest
ADHOC	MTCS	<i>Read Only Role</i>	Generate and view an Ad Hoc Report containing Form-50058 data.	HA User
		<i>Read Only Role</i>	Generate and view an Ad Hoc Report containing Form-50058 data.	HUD User
		<i>Read Only Role</i>	Generate and view an Ad Hoc Report containing Form-50058 data.	Guest

Module	Submodule	Role Name	Role Description	Type of User
PIC Downloads	Building and Unit	<i>Read Only Role</i>	View ticket numbers and status for requested building or unit files.	HA User
		<i>Submit Role</i>	Request and download files containing building or unit data.	HA User
		<i>Read Only Role</i>	View ticket numbers and status for requested building or unit files.	HUD User
		<i>Download B&U Data</i>	Request and download files containing building or unit data.	HUD User
		<i>Read Only Role</i>	View ticket numbers and status for requested building or unit files.	Guest
MTW (Moving To Work)	Data Collection	<i>Submit</i>	Submit data files.	HA User
		<i>Read Only</i>	View ticket numbers and status for submitted files.	HUD User
	Viewer	Roles are currently under development.		

Appendix E

Acronym List

Acronym List

This appendix defines acronyms used in this manual and explains how to access a comprehensive list of HUD terms and acronyms on the HUD Web site.

Refer to the following table for a list of acronyms used in this manual.

Acronym	Definition
AMP	Asset Management Project
ASP	Active Server Page
HA	Housing Authority
HQ	Headquarters
HUD	United States Department of Housing and Urban Development
ID	Identification
IP	Internet Protocol
IT	Information Technology
OS	Operating System
PC	Personal Computer
PIH	Public and Indian Housing
PIC	Public and Indian Housing Information Center
REAC	Real Estate Assessment Center
WASS	Web Access Security Subsystem

Go to <http://www.hud.gov/about/acronyms.cfm> to view a comprehensive list of commonly used HUD terms and acronyms.

Appendix F
PIC Access Authorization Forms

PIC Access Authorization Forms

This appendix contains sample PIC Access Authorization Forms. Security Coordinators use the forms to assign PIC system access rights.

A sample authorization form for HA users is shown in Figure F-1. A sample authorization form for HUD users is shown in Figure F-2 on page F-2.



Public and Indian Housing Information Center (PIC)
PHA Access Authorization Form

(Please Print or Type)

HOUSING AUTHORITY NAME: _____ HA CODE: _____

Program Type: Low Rent (PH) Section 8 Combined

USER DETAILS

New User Delete Role Add Role Terminate User

AUTHORIZED USER'S NAME (First, MI & Last): _____ WASS USER ID (Mxxxxx): _____

EMAIL ADDRESS: _____ OFFICE PHONE NUMBER: _____

CHECK EACH MODULE, SUB-MODULE, AND ROLE REQUESTED

MODULE	SUB-MODULE	ROLE (SELECT ONE ONLY)
<input type="checkbox"/> PIC Maintenance	<input type="checkbox"/> User Profile <input type="checkbox"/> Security Administration	Use User Profile (<i>automatic access</i>) <input type="checkbox"/> Read-Only <input type="checkbox"/> Security Coordinator
<input type="checkbox"/> PIH Information	<input type="checkbox"/> SEMAP (Section 8 only)	<input type="checkbox"/> Read-Only <input type="checkbox"/> Edit <input type="checkbox"/> Submit
<input type="checkbox"/> Housing Inventory	<input type="checkbox"/> Housing Authority <input type="checkbox"/> Development (PH only) <input type="checkbox"/> Demo-Dispo (PH only)	<input type="checkbox"/> Read-Only <input type="checkbox"/> Edit <input type="checkbox"/> Submit <input type="checkbox"/> Read-Only Privacy <input type="checkbox"/> Edit <input type="checkbox"/> Submit <input type="checkbox"/> Read-Only <input type="checkbox"/> Edit <input type="checkbox"/> Submit
<input type="checkbox"/> Executive Summary	<input type="checkbox"/> HA Executive Summary	<input type="checkbox"/> Read-Only
<input type="checkbox"/> Form-50058 (MTCS)	<input type="checkbox"/> Submission <input type="checkbox"/> Viewer <input type="checkbox"/> Reports <input type="checkbox"/> Alt ID Generator	<input type="checkbox"/> Read-Only <input type="checkbox"/> Submit <input type="checkbox"/> Read-Only <input type="checkbox"/> Submit <input type="checkbox"/> Read-Only <input type="checkbox"/> Read-Only Privacy <input type="checkbox"/> Submit <input type="checkbox"/> Validate SSN-AID
<input type="checkbox"/> AD-HOC	<input type="checkbox"/> MTCS	<input type="checkbox"/> Read-Only
<input type="checkbox"/> PIC Downloads	<input type="checkbox"/> Building and Unit (PH only)	<input type="checkbox"/> Read-Only <input type="checkbox"/> Submit
<input type="checkbox"/> MTW	<input type="checkbox"/> Data Collection	<input type="checkbox"/> MTW Data Upload

I authorize the above person access as indicated above to the PIH Information Center (PIC).

Executive Director's Name (Print) _____

Executive Director's Signature _____ Date: _____

File in Security Control File	March 2005	Designed by Kansas City Hub
-------------------------------	------------	-----------------------------

Figure F-1: Sample PIC Access Authorization Form for HA users



Public and Indian Housing Information Center (PIC) HUD Access Authorization Form

(Please Print or Type)

AUTHORIZED USER'S NAME *(First, MI & Last)*: _____ USER ID *(Hxxxxx)*: _____

EMAIL ADDRESS: _____ OFFICE PHONE NUMBER: _____

USER DETAILS

New User Delete Role Add Role Terminate User

CHECK EACH MODULE, SUB-MODULE, AND ROLE REQUESTED

MODULE	SUB-MODULE	ROLE
<input type="checkbox"/> PIC Maintenance	<input type="checkbox"/> User Profile <input type="checkbox"/> Security Administration	Use User Profile <i>(automatic access)</i> <input type="checkbox"/> Read-Only <input type="checkbox"/> HA Security Admin
<input type="checkbox"/> PIH Information	<input type="checkbox"/> SEMAP <i>(Section 8 only)</i> <input type="checkbox"/> Risk Assessment	<input type="checkbox"/> Read-Only <input type="checkbox"/> Edit <input type="checkbox"/> Approve <input type="checkbox"/> Read-Only <input type="checkbox"/> Edit <input type="checkbox"/> Approve
<input type="checkbox"/> Housing Inventory	<input type="checkbox"/> Housing Authority <input type="checkbox"/> Development <input type="checkbox"/> Demo-Dispo	<input type="checkbox"/> Read-Only <input type="checkbox"/> Approve <input type="checkbox"/> Read-Only Privacy <input type="checkbox"/> Edit <input type="checkbox"/> Approve <input type="checkbox"/> Read-Only <input type="checkbox"/> Edit <input type="checkbox"/> Submit
<input type="checkbox"/> Executive Summary	<input type="checkbox"/> HA Executive Summary	<input type="checkbox"/> Read-Only
<input type="checkbox"/> Management Reports	<input type="checkbox"/> RDS	<input type="checkbox"/> Read-Only
<input type="checkbox"/> Form-50058 (MTCS)	<input type="checkbox"/> Submission <input type="checkbox"/> Viewer <input type="checkbox"/> Reports <input type="checkbox"/> Alt ID Generator	<input type="checkbox"/> Read-Only <input type="checkbox"/> Submit <input type="checkbox"/> Read-Only <input type="checkbox"/> Read-Only <input type="checkbox"/> Read-Only Privacy
<input type="checkbox"/> AD-HOC	<input type="checkbox"/> MTCS	<input type="checkbox"/> Read-Only
<input type="checkbox"/> PIC Downloads	<input type="checkbox"/> Building and Unit	<input type="checkbox"/> Read-Only
<input type="checkbox"/> MTW	<input type="checkbox"/> Data Collection	<input type="checkbox"/> MTW Data Upload

I authorize the above person access as indicated above to the PIH Information Center (PIC).

FO Director's Name (Print) _____

FO Director's Signature _____ Date: _____

File in Security Control File March 2005 Designed by Kansas City Hub

Figure F-2: Sample PIC Access Authorization Form for HUD users