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).

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).

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).
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).

![Email Address: user@domainname.com](image)

*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.

![Security List](image)

*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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action/Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Type <code>pic.hud.gov</code> in your Web browser’s address field and press ENTER. Typing <code>pic.hud.gov</code> redirects you to the PIC home page located at <a href="http://www.hud.gov/offices/pih/systems/pic/">http://www.hud.gov/offices/pih/systems/pic/</a>. The PIC home page appears (see Figure 2-1). <strong>Tip:</strong> 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.</td>
</tr>
<tr>
<td>2.</td>
<td>Select Logon to PIC in the middle of the page or at the left of the page.</td>
</tr>
</tbody>
</table>

![Figure 2-1: PIC home page](image)

**Home and Indian Housing**

**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 PIHTEST
  - Online registration for new WASS ID
  - System requirements
  - Technical support (Helpdesk & Help)
  - Forms: S9950
  - Resident Characteristics Report
  - HA Profiles
  - PIH Online- dispute
  - HUD’s Hurricane Katrina resource page
  - Extra Character Housing Assistance Program (EDHAP) Application - User Guide

**Sub-Modules**

PIC consists of the following modules and sub-modules:

1. PIC Maintenance
2. User Profile
3. Security Administration
4. PIH Information

---

**Quick Access**

- Dec. 6, 2005 - KDHAP Version 1.0 in PIHTEST
- Dec. 7, 2005 - PIC now works with version browsers
- Nov. 22, 2005 - 9/10 Release Certification due 11/24
- Nov. 15, 2005 - Known bug in Discrepancy Report
- Oct. 31, 2005 - KDHAP Version 2.50 Out
- Oct. 8, 2005 - KDHAP added to PIHTEST
- Oct. 1, 2005 - JUMP is a PIC help online support system...
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).
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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action/Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Type <strong>pic.hud.gov</strong> in your Web browser’s address field and press ENTER. Typing <strong>pic.hud.gov</strong> redirects you to the PIC home page located at <a href="http://www.hud.gov/offices/pih/systems/pic/">http://www.hud.gov/offices/pih/systems/pic/</a>. The PIC home page appears (see Figure 2-4). <strong>Tip:</strong> 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.</td>
</tr>
<tr>
<td>Step</td>
<td>Action/Result</td>
</tr>
<tr>
<td>------</td>
<td>---------------</td>
</tr>
</tbody>
</table>
| 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*
6. Select **PIH Information Center** (circled in Figure 2-6).  
The PIC Main page appears (see Figure 2-7).
Navigating to the Security Administration submodule

Follow these steps to access the Security Administration submodule:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action/Result</th>
</tr>
</thead>
</table>
| 1.   | Move your mouse cursor over the **PIC Maintenance** button. Two submodules are displayed (see Figure 2-8):  
- User Profile  
- Security Administration  
**Note:** Your access to the other modules and submodules depends on the access rights assigned to you. |
| 2.   | Select **Security Administration**. 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.  
**Note:** The notice does not appear if you previously accepted the statement to access other content protected by the Privacy Act. |
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.
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

![Figure 3-1: Security tab and Security List](image)

**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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action/Result</th>
</tr>
</thead>
</table>
| 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](image)

**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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action/Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Navigate to the Security Administration submodule.</td>
</tr>
<tr>
<td>2.</td>
<td>Select the Security tab.</td>
</tr>
<tr>
<td>3.</td>
<td>Select <strong>Insert New WASS User</strong> 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 (*).</td>
</tr>
</tbody>
</table>

![Figure 3-3: Accessing the Security Details page](image)

![Figure 3-4: Using the Security Details page to add a new user](image)
<table>
<thead>
<tr>
<th>Step</th>
<th>Action/Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.</td>
<td>Type the user’s WASS ID in the <strong>WASS User ID</strong> field. Make sure to capitalize the letters of the ID.</td>
</tr>
<tr>
<td>5.</td>
<td>Type the user’s first name in the <strong>First Name</strong> field.</td>
</tr>
<tr>
<td>6.</td>
<td>Type the user’s middle name in the <strong>Middle Name</strong> field.</td>
</tr>
<tr>
<td>7.</td>
<td>Type the user’s last name in the <strong>Last Name</strong> field.</td>
</tr>
<tr>
<td>8.</td>
<td>Select the type of user you are adding from the <strong>User Type</strong> drop-down menu.</td>
</tr>
<tr>
<td>9.</td>
<td>Type the user’s e-mail address in the <strong>Email Address</strong> 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.</td>
</tr>
<tr>
<td>10.</td>
<td>Confirm the e-mail address is correct by re-typing it in the <strong>Confirm Email Address</strong> field.</td>
</tr>
<tr>
<td>11.</td>
<td>Type the account activation date in the <strong>Effective From Date</strong> field. <strong>Note</strong>: This is typically the date on which the user is added to the PIC system.</td>
</tr>
<tr>
<td>12.</td>
<td>Type the account expiration date in the <strong>Expiration Date</strong> field. <strong>Note</strong>: You can change the date at any time. Follow the steps in <em>Modifying a user profile</em> 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.</td>
</tr>
<tr>
<td>13.</td>
<td>Select the <strong>Yes</strong> active indicator.</td>
</tr>
</tbody>
</table>
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**. The Security Summary page appears, indicating the user successfully was added to the system (see Figure 3-5).

Continued with step 3 in *Assigning access rights to a new or existing user* to assign access rights to the user.

Or, repeat steps 2–16 to add more users.

---

![Security Summary page](image)

*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.

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

![Figure 3-6: Assigning access rights: selecting a submodule](image-url)
6. Select the appropriate role from the **Roles** drop-down menu (see Figure 3-7 for an example).

**Note:** Select **View Actions** to view actions the user can complete for the selected role.

A description of the role appears in the **Role Description** field.

Refer to appendix D for a complete list of access roles and their descriptions.

7. Select a security level from the **Security** drop-down menu.

**Note:** Field Office HA is typically the default setting for HA users.

Depending on your access level, other drop-down menus may appear.

---

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

---

**Figure 3-8: Assigning access rights: selecting the user’s security level**
<table>
<thead>
<tr>
<th>Step</th>
<th>Action/Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>11. Select <strong>Save</strong> at the bottom of the page.</td>
<td>The user’s Security Summary page appears (see Figure 3-9). The role is displayed in the table at the bottom of the page. <strong>Tip:</strong> Follow the steps in <em>Generating a User Security Access report</em> on page 5-5 to view a detailed summary of the user’s current access rights. Repeat steps 3–11 to add more roles to the user’s ID.</td>
</tr>
</tbody>
</table>

![Security Summary page showing newly assigned role](image)
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:

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

*Figure 3-10: Accessing the Bulk Copy page*

*Figure 3-11: Bulk Copy page*
4. Select the level at which you want to copy the access rights from the **Bulk Copy Option** drop-down menu:
   - **Sub-Module Level**
   - **Module Level**
   - **User Level**

   **Note:** Wait for the page to refresh before continuing.

5. Select the user to whom you want to copy the access rights from the **Available Staff** list.

6. Select the right arrow to add the user or users to the **Copy to Selected Staff** list.

   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.

7. Select **Copy**.

---

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

- **Sub-Module Level** 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).

- **Module Level** copies access rights for a module and all of its submodules. You must select the module from the **Module Name** list.

- **User Level** copies all the user’s access rights.

Press and hold the CTRL key to select more than one user.
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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action/Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Follow the steps in <em>Searching for an existing user</em> on page 3-1 to locate the user.</td>
</tr>
<tr>
<td>2.</td>
<td>Select the User ID hyperlink. The user’s Security Summary page appears.</td>
</tr>
<tr>
<td>3.</td>
<td>Click <strong>Modify User</strong> 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).</td>
</tr>
<tr>
<td>Step</td>
<td>Action/Result</td>
</tr>
<tr>
<td>------</td>
<td>---------------</td>
</tr>
<tr>
<td>4.</td>
<td>Type or select the changes to the user’s profile.</td>
</tr>
<tr>
<td>5.</td>
<td>Type the reason for modifying the user’s profile in the <strong>User Status Comments</strong> field.</td>
</tr>
<tr>
<td>6.</td>
<td>Select <strong>Save</strong>. The Security Summary page appears after the changes have been saved.</td>
</tr>
</tbody>
</table>
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:

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

![Figure 3-15: Removing an access role from a module and submodule](image-url)

---

**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.

![Figure 3-16: Selecting a role for deletion](image)

![Figure 3-17: Confirming the deletion of an access role](image)
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:

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

![Figure 3-18: Deactivating a user](image-url)
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.

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

![Figure 3-19: Deleting a user](image)

![Figure 3-20: Confirming the deletion of a user](image)
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.
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](image)

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).

![Figure 5-2: Viewing an entire report on a single page](image)
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](image)

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-logon to the PIC system if you mistakenly close the main PIC window.

![Figure 5-4: Closing a report window](image)
Navigating to the Access Reports tab

Follow these steps to navigate to the Access Reports tab:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action/Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Log on to the PIC system.</td>
</tr>
<tr>
<td>2.</td>
<td>Move the cursor over the <strong>PIC Maintenance</strong> button.</td>
</tr>
<tr>
<td>3.</td>
<td>Select the <strong>Security Administration</strong> hyperlink.</td>
</tr>
<tr>
<td>4.</td>
<td>Select the Access Reports tab (see Figure 5-5).</td>
</tr>
</tbody>
</table>

*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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action/Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Select the Access Reports tab. The User Security Access report page is the default page displayed (see Figure 5-6).</td>
</tr>
<tr>
<td>2.</td>
<td>Locate the user in the Security List at the bottom of the page.</td>
</tr>
</tbody>
</table>
| 3.   | If necessary, narrow the list of users by following these steps:  
|      | a. 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,  
|      | b. Select a user ID status from the Select Status drop-down menu. Or,  
|      | c. Select an ID type from the Select ID Type drop-down menu.  
|      | d. 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.

Figure 5-7: Sample User Security Access report
<table>
<thead>
<tr>
<th>Table</th>
<th>Information Presented</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Identification</td>
<td>The User Identification table lists the following information:</td>
</tr>
<tr>
<td></td>
<td>• User ID</td>
</tr>
<tr>
<td></td>
<td>• Name</td>
</tr>
<tr>
<td></td>
<td>• Telephone number</td>
</tr>
<tr>
<td></td>
<td>• E-mail address</td>
</tr>
<tr>
<td></td>
<td>• User type</td>
</tr>
<tr>
<td></td>
<td>• User status</td>
</tr>
<tr>
<td></td>
<td>• Creation date (date on which the user’s account was created)</td>
</tr>
<tr>
<td></td>
<td>• Account end date (date on which the user’s account expires)</td>
</tr>
<tr>
<td>User Roles</td>
<td>The User Roles table lists the following information:</td>
</tr>
<tr>
<td></td>
<td>• Module</td>
</tr>
<tr>
<td></td>
<td>• Submodule</td>
</tr>
<tr>
<td></td>
<td>• Role</td>
</tr>
<tr>
<td></td>
<td>• Level</td>
</tr>
<tr>
<td></td>
<td>• Entity (typically, the HA to which the user belongs)</td>
</tr>
<tr>
<td>User Actions</td>
<td>The User Actions table lists the actions a user can take for each submodule.</td>
</tr>
<tr>
<td></td>
<td>Refer to appendix D for a complete list of access roles and their descriptions.</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action/Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Select the Access Reports tab. The User Security Access report page is the default page displayed.</td>
</tr>
<tr>
<td>2.</td>
<td>Select Privacy Act Access (see Figure 5-8). The Privacy Act Access report page appears (Figure 5-9).</td>
</tr>
</tbody>
</table>

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

**Figure 5-9: Privacy Act Access report page**
<table>
<thead>
<tr>
<th>Step</th>
<th>Action/Result</th>
</tr>
</thead>
</table>
| 3.   | Enter the report data filters:  
| a.   | Select a pre-defined report range from the **Report Period** drop-down menu; or, use the **Custom Dates** 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:  
| 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.

![Privacy Act Data Access Report](image)

| HQ Division  | Public and Indian Housing |
| HQ Office    | FO Field Operations       |
| Hub          | JPBT Baltimore Hub        |
| Field Office | JPBIH Baltimore Hub Office|
| Field Office HA | MDF01 ANNAFOLS HOUSING AUTHORITY |

Report generation Date: Wednesday, January 25, 2006 11:47:56 AM

![Figure 5-10: Sample Privacy Act Access report](image)

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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action/Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Select the Access Reports tab. The User Security Access report page is the default page displayed.</td>
</tr>
<tr>
<td>2.</td>
<td>Select <strong>Global User Search</strong> (circled in Figure 5-11). The Global User Search report page appears (see Figure 5-12).</td>
</tr>
</tbody>
</table>

![Figure 5-11: Accessing the Global User Search report page](image)

![Figure 5-12: Global User Search report page](image)
3. Determine if you want to search by user ID or by name.

- To search by user ID, type the user ID in the User-ID(s) field and select **Search Users** (see Figure 5-13).
  **Note:** You must separate multiple user IDs with commas.

- 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).
  **Note:** You must type at least the first three characters of the first name or last name.

**Tip:** When searching by name, clear the **Exact Match** check box to increase the number of search results.

![Figure 5-13: Searching for a user by user ID](image)
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.

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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action/Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Select the Access Reports tab.</td>
</tr>
<tr>
<td>2.</td>
<td>Select <strong>User Access by Submodule</strong> (circled in Figure 5-16).</td>
</tr>
</tbody>
</table>

---

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

---

**Figure 5-17: User Access by Submodule report page**
<table>
<thead>
<tr>
<th>Step</th>
<th>Action/Result</th>
</tr>
</thead>
</table>
| 3.   | Enter the report data filters:  
|      | 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:  
|      | 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 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](image)

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).

![Figure 6-2: Viewing an entire report on a single page](image)
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-logon 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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action/Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Log on to the PIC system.</td>
</tr>
<tr>
<td>2.</td>
<td>Move the cursor over the <strong>PIC Maintenance</strong> button.</td>
</tr>
<tr>
<td>3.</td>
<td>Select the <strong>Security Administration</strong> hyperlink.</td>
</tr>
<tr>
<td>4.</td>
<td>Select the Activity Reports tab (see Figure 6-5).</td>
</tr>
</tbody>
</table>

*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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action/Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Select the Activity Reports tab. The User Activity Query report page is the default page displayed (see Figure 6-6).</td>
</tr>
<tr>
<td>2.</td>
<td>Locate the user in the Security List at the bottom of the page.</td>
</tr>
<tr>
<td>3.</td>
<td>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.</td>
</tr>
<tr>
<td>4.</td>
<td>Select the User ID hyperlink to generate the report.</td>
</tr>
</tbody>
</table>

![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:** FO Field Operations
- **Hub:** SHCH Chicago Hub
- **Field Office:** NAF CHICAGO HUB OFFICE
- **Field Office HA:** E003 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 |
| Email Address | billuser@domain.gov |

**Activity Report**

<table>
<thead>
<tr>
<th>Summary Report</th>
<th>Total Connect Time</th>
<th>Total Number of Logins</th>
<th>Average Connect Time</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0.06s</td>
<td>3</td>
<td>0.02s</td>
</tr>
</tbody>
</table>

**Detailed Report**

<table>
<thead>
<tr>
<th>Sr No</th>
<th>Date</th>
<th>Operating System</th>
<th>Browser Name/Version</th>
<th>Client IP Address</th>
<th>Web Server Name</th>
<th>Activity Status</th>
<th>Login Begin</th>
<th>Login End</th>
<th>Total Time Logged On</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>02/16/2006 10:50:39</td>
<td>Windows NT</td>
<td>Microsoft Internet Explorer 6.0</td>
<td>90.200.30.99</td>
<td>HLANNW001</td>
<td>CRRNT</td>
<td>02/16/2006 10:50:39</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>2</td>
<td>02/16/2006 10:50:46</td>
<td>Windows NT</td>
<td>Microsoft Internet Explorer 6.0</td>
<td>90.200.30.100</td>
<td>HLANNW001</td>
<td>LOGOFF</td>
<td>02/16/2006 10:50:46</td>
<td>02/16/2006 10:58:16</td>
<td>0.02s</td>
</tr>
<tr>
<td>3</td>
<td>02/16/2006 10:54:53</td>
<td>Windows NT</td>
<td>Microsoft Internet Explorer 6.0</td>
<td>100.10.10.100</td>
<td>HLANNW003</td>
<td>ASINML</td>
<td>02/16/2006 10:54:53</td>
<td>02/16/2006 10:58:46</td>
<td>0.35s</td>
</tr>
</tbody>
</table>

* Insignificant Data.
** Session Timed out.

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>
<thead>
<tr>
<th>Table</th>
<th>Information Presented</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary Report</td>
<td>The Summary Report table lists the following information:</td>
</tr>
<tr>
<td></td>
<td>• Total time connected</td>
</tr>
<tr>
<td></td>
<td>• Total number of logins</td>
</tr>
<tr>
<td></td>
<td>• Average time connected</td>
</tr>
<tr>
<td>Detailed Report</td>
<td>The Detailed Report table lists the following information:</td>
</tr>
<tr>
<td></td>
<td>• Date</td>
</tr>
<tr>
<td></td>
<td>• Operating system</td>
</tr>
<tr>
<td></td>
<td>• Browser name and version</td>
</tr>
<tr>
<td></td>
<td>• Client IP address</td>
</tr>
<tr>
<td></td>
<td>• Web server name</td>
</tr>
<tr>
<td></td>
<td>• Activity status</td>
</tr>
<tr>
<td></td>
<td>• Login begin</td>
</tr>
<tr>
<td></td>
<td>• Login end</td>
</tr>
<tr>
<td></td>
<td>• Total time logged on</td>
</tr>
</tbody>
</table>
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:

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

![Figure 6-8: Accessing the New Users report page](image1)

![Figure 6-9: New Users report page](image2)
<table>
<thead>
<tr>
<th>Step</th>
<th>Action/Result</th>
</tr>
</thead>
</table>
| 3.   | Enter the report data filters:  
|      | a. Select a pre-defined report range from the **Report Period** drop-down menu; or, use the **Custom Dates** 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:  
|      | 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.

![Sample New Users report](image)

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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action/Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Select the Activity Reports tab.</td>
<td>The User Activity Query report page is the default page displayed.</td>
</tr>
<tr>
<td>2. Select <strong>Improper Logoff</strong> (circled in Figure 6-11).</td>
<td>The Improper Logoff report page appears (see Figure 6-12).</td>
</tr>
</tbody>
</table>

![Figure 6-11: Accessing the Improper Logoff report page](image1)

![Figure 6-12: Improper Logoff report page](image2)
3. Enter the report data filters:
   a. Select a pre-defined report range from the **Report Period** drop-down menu; or, use the **Custom Dates** 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:
   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.

![Improper Logoff Report](image)

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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action/Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Select the Activity Reports tab. The User Activity Query report page is the default page displayed.</td>
</tr>
<tr>
<td>2.</td>
<td>Select <strong>User Account Usage</strong> (circled in Figure 6-14). The User Account Usage report page appears (see Figure 6-15).</td>
</tr>
</tbody>
</table>

![Figure 6-14: Accessing the User Account Usage report page](image1)

![Figure 6-15: User Account Usage report page](image2)
<table>
<thead>
<tr>
<th>Step</th>
<th>Action/Result</th>
</tr>
</thead>
</table>
| 3.   | **Enter the report data filters:**  
|      | 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:**  
|      | 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 Account Usage Report](image)

**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
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.
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.
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](image)

---

**Privacy Act Statement and Compliance Notice**

**Welcome Brian Labarte!**

1/27/2006 10:59:44 AM

**IMPORTANT:** Please read the following carefully.

**Legal Warning**

Misuse of Federal information through the HUD Secure Connection website 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.

**Primary 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 PBH 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.

[Agree] [Decline]

**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.
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.

<table>
<thead>
<tr>
<th>Module</th>
<th>Submodule</th>
<th>Role Name</th>
<th>Role Description</th>
<th>Type of User</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIH Maintenance</td>
<td>User Profile</td>
<td>User Profile</td>
<td>Edit user information and change passwords.</td>
<td>All users</td>
</tr>
<tr>
<td>Security</td>
<td>Administration</td>
<td>Security Coordinator</td>
<td>Perform security administration tasks. Note: Role is currently under development.</td>
<td>HA User</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Recertify HA</td>
<td>Re-certify HA Security Admins and view reports.</td>
<td>HA User</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HA Certifier</td>
<td>Certify HA users on a quarterly basis.</td>
<td>HA User</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sec Coord</td>
<td>View, edit, and create users.</td>
<td>HUD User</td>
</tr>
<tr>
<td></td>
<td>Read Only</td>
<td>Read Only</td>
<td>View security reports and data.</td>
<td>HUD User</td>
</tr>
<tr>
<td></td>
<td>Read Only</td>
<td>Read Only</td>
<td>View security reports and data.</td>
<td>Guest</td>
</tr>
<tr>
<td>PIH Information</td>
<td>SEMAP</td>
<td>Read Only - SEMAP</td>
<td>View information in SEMAP.</td>
<td>HA User</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Edit SEMAP Role</td>
<td>View and edit information in SEMAP.</td>
<td>HA User</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Submit SEMAP Role</td>
<td>Create, view, edit, and submit information in SEMAP.</td>
<td>HA User</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Read only SEMAP</td>
<td>View information in SEMAP.</td>
<td>HUD User</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Edit SEMAP Role</td>
<td>View and edit information in SEMAP; view reports.</td>
<td>HUD User</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Approve SEMAP</td>
<td>View, edit, and approve SEMAP profiles and comments; view reports.</td>
<td>HUD User</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HQ SEMAP Appeal</td>
<td>Approve or reject HQ level appeals.</td>
<td>HUD User</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Read Only - Semap</td>
<td>View information in SEMAP.</td>
<td>Guest</td>
</tr>
<tr>
<td>Module</td>
<td>Submodule</td>
<td>Role Name</td>
<td>Role Description</td>
<td>Type of User</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------</td>
<td>------------------------</td>
<td>----------------------------------------------------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>PIH Information</td>
<td>Risk Assessment (HUD only)</td>
<td>Read Only Role</td>
<td>View Risk Assessment data, comments, and reports.</td>
<td>HUD User</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Edit Risk Assessment</td>
<td>View and edit Risk Assessment data and comments; view reports.</td>
<td>HUD User</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Approve R.A. Data</td>
<td>View, edit, and approve Risk Assessment data and comments; view reports.</td>
<td>HUD User</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Read Only Role</td>
<td>View Risk Assessment data.</td>
<td>Guest</td>
</tr>
<tr>
<td>Housing Inventory</td>
<td>Housing Authority</td>
<td>Read Only Role</td>
<td>View housing authority information, including Occupancy report.</td>
<td>HA User</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Edit HA Role</td>
<td>View and edit housing authority information, including Occupancy report.</td>
<td>HA User</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Submit HA Role</td>
<td>View, edit, and submit housing authority information, including Occupancy report.</td>
<td>HA User</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Read Only Role</td>
<td>View information in Housing Authority.</td>
<td>HUD User</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HA Exec Approve</td>
<td>View, edit, and approve information in Housing Authority.</td>
<td>HUD User</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Read Only Role</td>
<td>View Housing Authority information, including Occupancy report.</td>
<td>Guest</td>
</tr>
<tr>
<td>Development</td>
<td></td>
<td>Read Only - Privacy</td>
<td>View all building and unit data.</td>
<td>HA User</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Edit Development</td>
<td>View and edit all building, unit, and AMP data.</td>
<td>HA User</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Submit Development</td>
<td>View, edit, and submit all building, unit, and AMP data.</td>
<td>HA User</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Read Only - Privacy</td>
<td>View all building and unit data.</td>
<td>HUD User</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Edit Development</td>
<td>View and edit all building, unit, and AMP data.</td>
<td>HUD User</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HUD Approve</td>
<td>View, edit, submit, and approve all building, unit, and AMP data.</td>
<td>HUD User</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Read Only - Privacy</td>
<td>View all building, unit, and AMP data.</td>
<td>Guest</td>
</tr>
<tr>
<td>Module</td>
<td>Submodule</td>
<td>Role Name</td>
<td>Role Description</td>
<td>Type of User</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------------------</td>
<td>-----------------</td>
<td>-------------------------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Housing Inventory</td>
<td>Demolition &amp; Disposition</td>
<td>Read Only Role</td>
<td>View Demolition and Disposition data.</td>
<td>HA User</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Edit Demo Dispo</td>
<td>View and edit Demolition and Disposition applications.</td>
<td>HA User</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Submit Demo Dispo</td>
<td>View, edit, and submit Demolition and Disposition applications.</td>
<td>HA User</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Read Only Role</td>
<td>View Demolition and Disposition data.</td>
<td>HUD User</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Edit Demo Dispo</td>
<td>View and edit Demolition and Disposition applications.</td>
<td>HUD User</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Approve DD-FO</td>
<td>View Demolition and Disposition data; approve removal transactions.</td>
<td>HUD User</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SAC Staff</td>
<td>SAC staff members can create and view applications; add attachments or comments to applications.</td>
<td>HUD (SAC) User</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SAC Mgt</td>
<td>SAC Management (Director/Deputy Director) can approve and disapprove applications.</td>
<td>HUD (SAC) User</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Read Only Role</td>
<td>View Demolition and Disposition data.</td>
<td>Guest</td>
</tr>
<tr>
<td>Executive Summary</td>
<td>Executive Summary</td>
<td>Read Only Role</td>
<td>View housing authority summary information.</td>
<td>HA User</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Exec Read Only</td>
<td>View housing authority summary information.</td>
<td>HUD User</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Read Only Role</td>
<td>View housing authority summary information.</td>
<td>Guest</td>
</tr>
<tr>
<td>MTCS (Form-50058)</td>
<td>Submission</td>
<td>Read Only Role</td>
<td>View upload file error reports.</td>
<td>HA User</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Submit Form-50058</td>
<td>Submit files and view error reports.</td>
<td>HA User</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Read Only Role</td>
<td>View upload file error reports.</td>
<td>HUD User</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Submit Form-50058</td>
<td>Submit files with PHA permission and view error reports.</td>
<td>HUD User</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Read Only Role</td>
<td>View upload file error reports.</td>
<td>Guest</td>
</tr>
<tr>
<td>Module</td>
<td>Submodule</td>
<td>Role Name</td>
<td>Role Description</td>
<td>Type of User</td>
</tr>
<tr>
<td>-------</td>
<td>-----------</td>
<td>--------------</td>
<td>----------------------------------------------------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>MTCS (Form-50058)</td>
<td>Viewer</td>
<td>Read Only Role</td>
<td>View all sections of Form-50058 and reports, including privacy act data.</td>
<td>HA User</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Submit EOP Role</td>
<td>View all sections of Form-50058 and reports including privacy act data; submit online End of Participation (EOPs).</td>
<td>HA User</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Read Only Role</td>
<td>View all sections of Form-50058 and reports, including privacy act data.</td>
<td>HUD User</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Read Only Role</td>
<td>View all sections of Form-50058 and reports, including privacy act data.</td>
<td>Guest</td>
</tr>
<tr>
<td>Reports</td>
<td></td>
<td>Read Only Role</td>
<td>View Form-50058 Reports with privacy act data.</td>
<td>HA User</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Read Only Role</td>
<td>View Form-50058 Reports with privacy act data.</td>
<td>HUD User</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Read Only Role</td>
<td>View Form-50058 Reports with privacy act data.</td>
<td>Guest</td>
</tr>
<tr>
<td>Tenant ID Management</td>
<td></td>
<td>Read Only - Privacy</td>
<td>View Tenant ID Management reports.</td>
<td>HA User</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Submit Role</td>
<td>Generate and replace AID information; view Tenant ID Management reports.</td>
<td>HA User</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Validate SSN-AID</td>
<td>Generate and replace AID information; view Tenant ID Management reports.</td>
<td>HA User</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Read Only - Privacy</td>
<td>View Tenant ID Management reports.</td>
<td>HUD User</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Read Only - Privacy</td>
<td>View Tenant ID Management reports.</td>
<td>Guest</td>
</tr>
<tr>
<td>ADHOC</td>
<td>MTCS</td>
<td>Read Only Role</td>
<td>Generate and view an Ad Hoc Report containing Form-50058 data.</td>
<td>HA User</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Read Only Role</td>
<td>Generate and view an Ad Hoc Report containing Form-50058 data.</td>
<td>HUD User</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Read Only Role</td>
<td>Generate and view an Ad Hoc Report containing Form-50058 data.</td>
<td>Guest</td>
</tr>
<tr>
<td>Module</td>
<td>Submodule</td>
<td>Role Name, Submodule</td>
<td>Role Description</td>
<td>Type of User</td>
</tr>
<tr>
<td>------------------------</td>
<td>----------------------</td>
<td>----------------------</td>
<td>--------------------------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>PIC Downloads Building and Unit</td>
<td>Read Only Role</td>
<td>View ticket numbers and status for requested building or unit files.</td>
<td>HA User</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Submit Role</td>
<td>Request and download files containing building or unit data.</td>
<td>HA User</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Read Only Role</td>
<td>View ticket numbers and status for requested building or unit files.</td>
<td>HUD User</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Download B&amp;U Data</td>
<td>Request and download files containing building or unit data.</td>
<td>HUD User</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Read Only Role</td>
<td>View ticket numbers and status for requested building or unit files.</td>
<td>Guest</td>
<td></td>
</tr>
<tr>
<td>MTW (Moving To Work) Data Collection</td>
<td>Submit</td>
<td>Submit data files.</td>
<td>HA User</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Read Only</td>
<td>View ticket numbers and status for submitted files.</td>
<td>HUD User</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Viewer</td>
<td>Roles are currently under development.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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.

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

Go to [http://www.hud.gov/about/acronyms.cfm](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.

![Image of PIC Access Authorization Form for HA users](image_url)

Figure F-1: Sample PIC Access Authorization Form for HA users
Figure F-2: Sample PIC Access Authorization Form for HUD users