



# User Recertification Manual

*Public and Indian Housing (PIH)  
Real Estate Assessment Center (REAC)  
Inventory Management System (IMS)*

*U.S. Department of Housing and Urban Development*

**May 2011**

# Table of Contents

1.0 OVERVIEW .....	3
2.0 HIGH LEVEL WORK FLOW .....	3
3.0 PROCESS OVERVIEW .....	4
3.1 Recertification Process .....	4
3.2 Email Notifications .....	4
3.3 Certifying Users.....	5
APPENDIX A - INITIALIZATION STEPS (SUPER USERS ONLY) ...	11
<i>Initializing the Recertification Process</i> .....	11
<i>Initializing the Email Notification Process</i> .....	13
APPENDIX B - INITIALIZING THE SECURITY ROLES AND	
ASSIGNING ACTIONS .....	16
<i>Security Actions</i> .....	16
<i>Creating Security Roles and assign actions</i> .....	17



## 3.0 Process Overview

### 3.1 Recertification Process

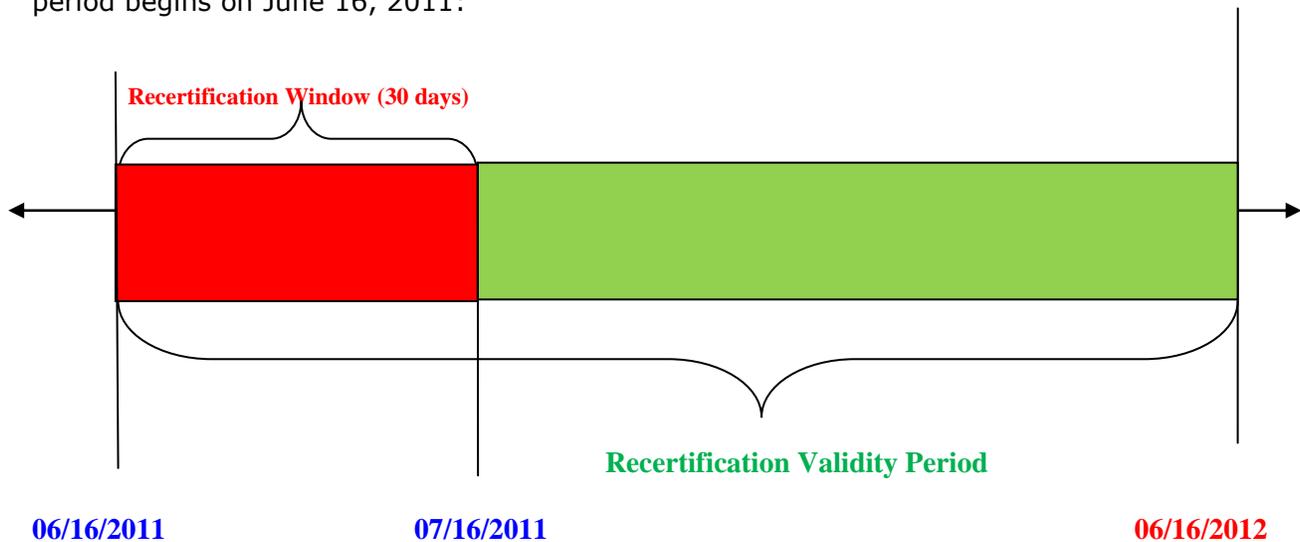
The recertification process allows security administrators to certify users in their respective organization within a specified timeframe known as Recertification Window. The recertification window begins on the Recertification start date. After the recertification window is over, all the uncertified users are inactivated the very next day.

For example, let us assume the following values for the process configuration parameters

Recertification Process Status	:	Active
Recertification Start Date	:	06/16/2011
Recertification Window	:	30 days.
Recertification Validity Period	:	365 days

In this example, the Recertification Process starts on 06/16/2011. The Security Coordinators will have 30 Calendar Days to recertify a user which means starting 06/16/2011, security coordinators can certify users until 07/16/2011.

Following diagram displays the certification process assuming that a new recertification period begins on June 16, 2011:

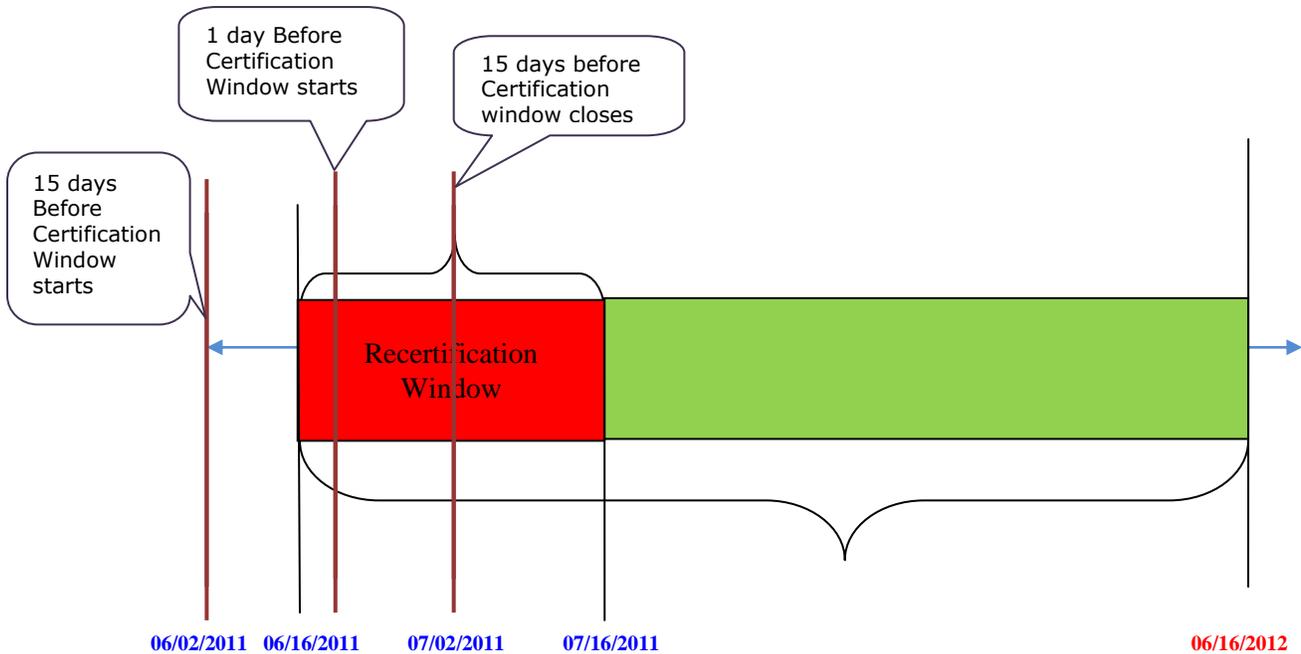


The system will send out notification emails to all the Security Coordinators through the built in email functionality in IMS. Details about this process is discussed in detail in the following section.

### 3.2 Email Notifications

When the Super User initializes the user recertification process as mentioned in the section "Initiating the Recertification Process" the email notification functionality will be scheduled internally to send emails to the "User Recertification - Security Administrators" group three times.

- The first email will be sent out 15 calendar days before the Recertification Window opens.
- The second will be sent out 1 calendar day before the Recertification Window opens.
- The third will be sent out 15 calendar days before the Recertification window closes.



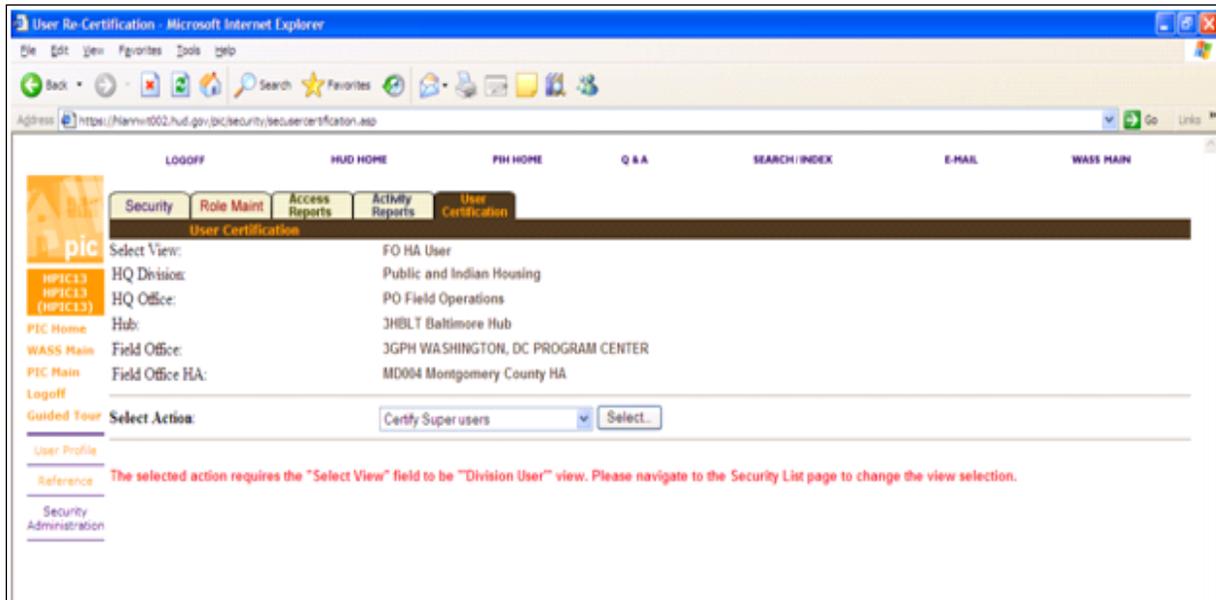
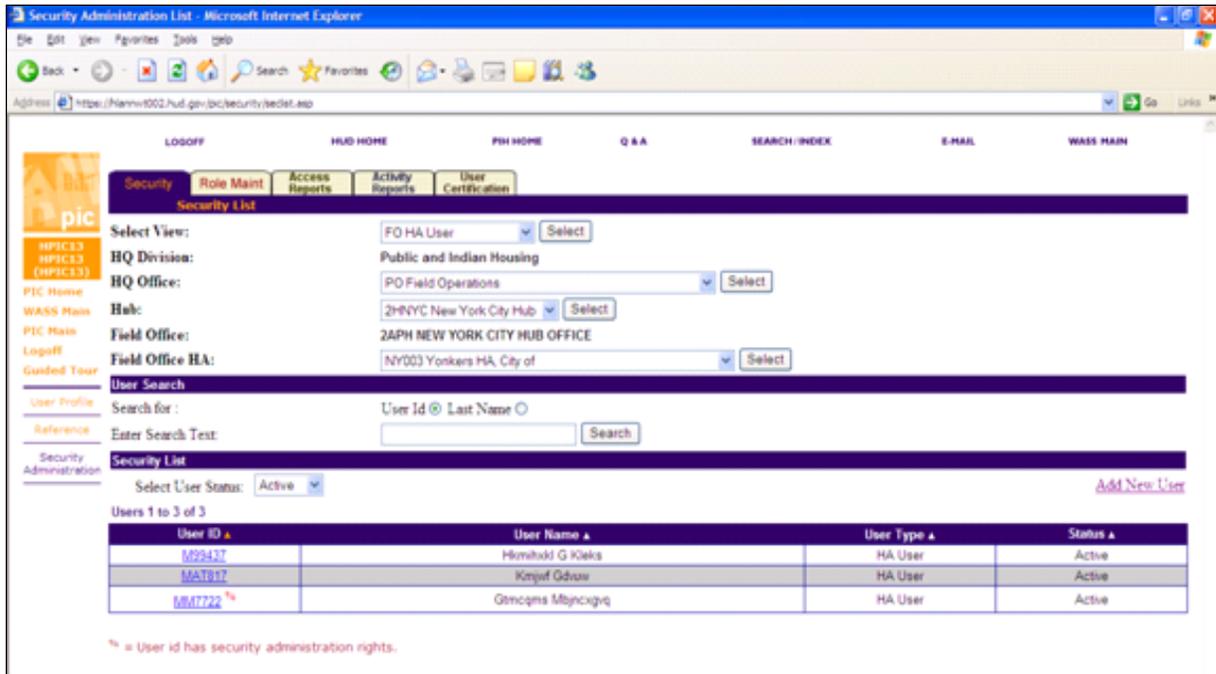
### 3.3 Certifying Users

To certify users the Security coordinators should go **System Administration** sub module under the PIC Maintenance Module. Navigate to **User certification** business function and the page is painted with the **User certification** tab.

#### 3.3.1 Certifying a HA User

By default the page is painted for the Division User view. To certify a HA user navigate to the **Security** tab and Select "**FO HA Users**" in the Select View option

Select the Hub and Field office of the HA user and then click on the **User Certification** tab.

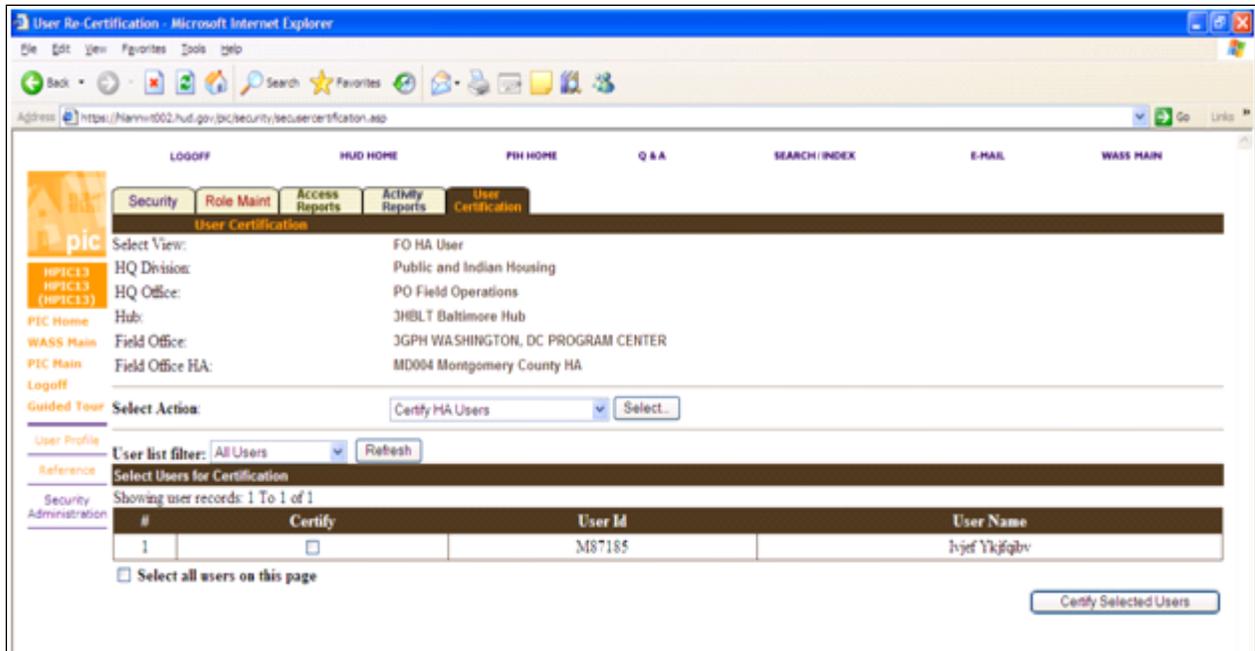


If any error message is displayed, please change the View in the Security tab.

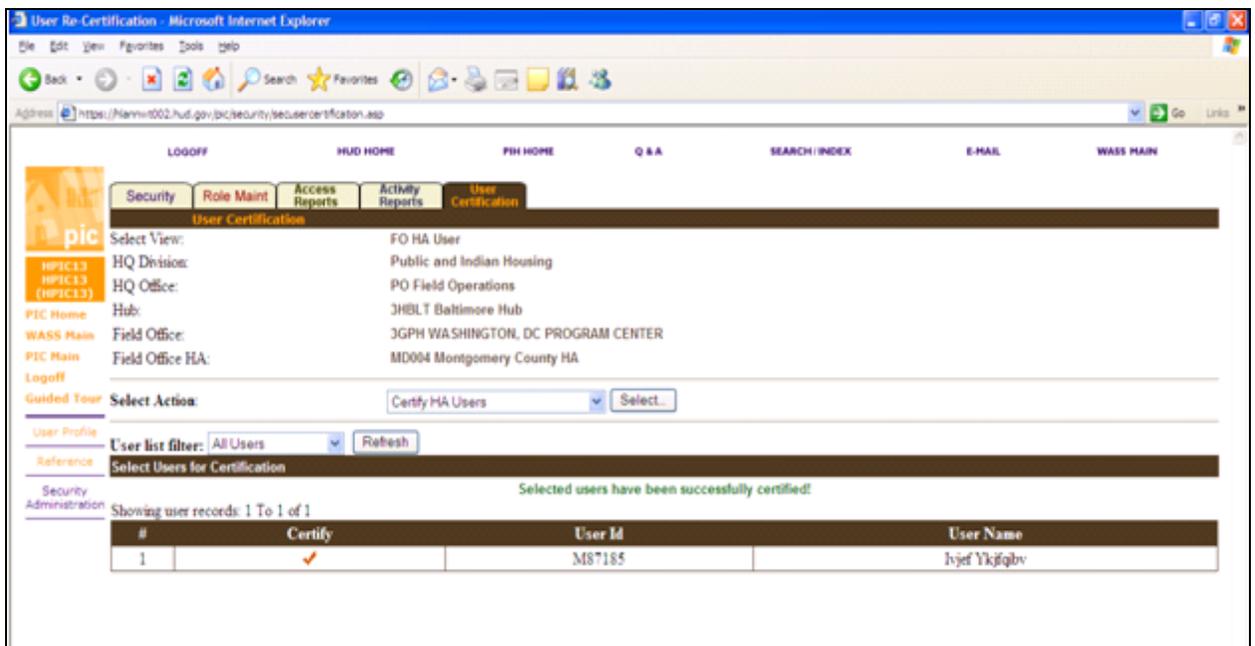
For example, in the screenshot above there is a error message

**"The selected action requires the "Select View" field to be "Division User" view. Please navigate to the Security List page to change the view selection."**

The reason for the above error message is that in the Select Action drop down it says "Certify Super Users" and an HA Security Coordinator cannot certify Super Users. The resolution is to select "Certify HA Users" to see the list of users that need to be certified under this HA.



Select the users that need to be certified by clicking on the Certify check box and click "Certify Selected Users" button. The selected users will have a checkmark under the "Certify" column as displayed below:

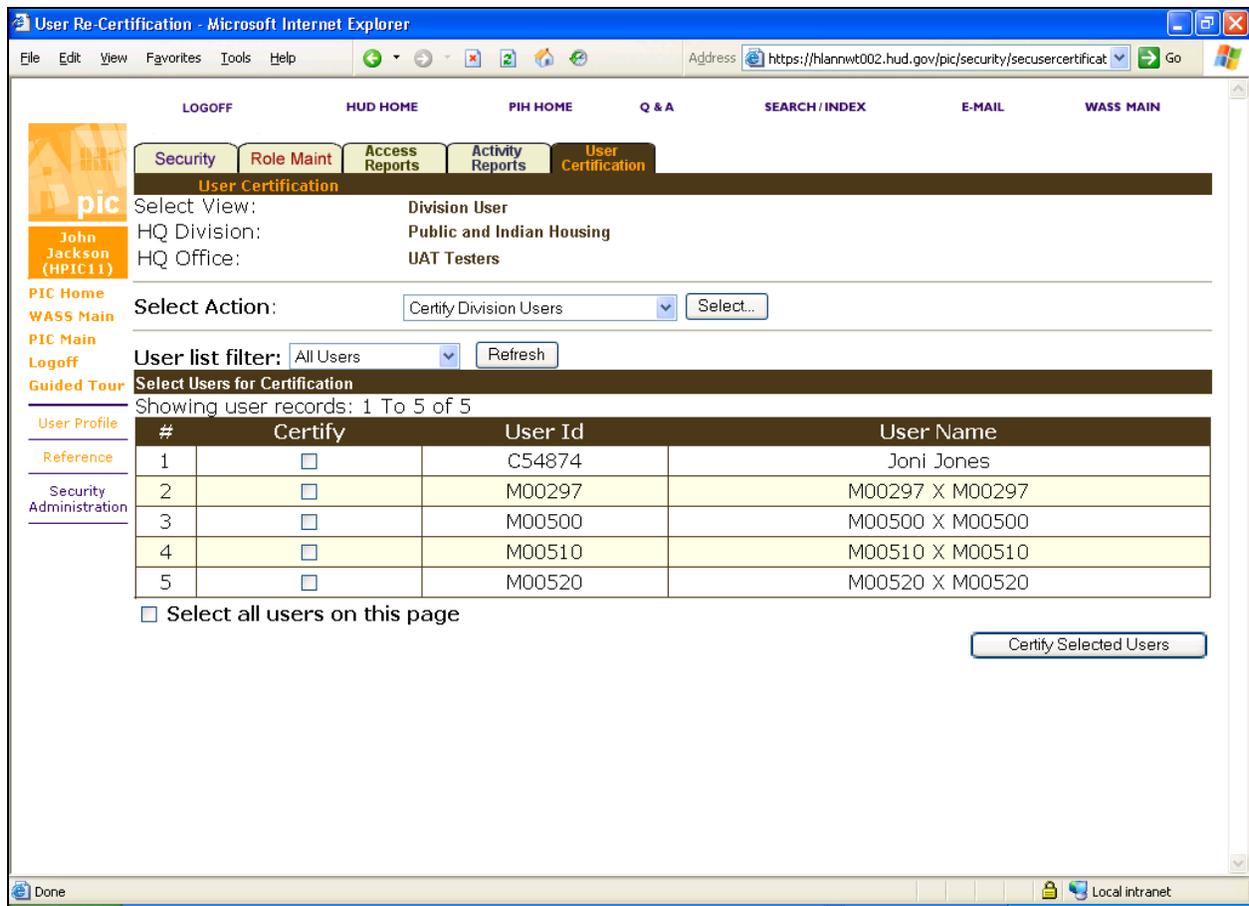


### 3.3.2 Certifying a Division User

Select Division User under the Security list page under Security tab and go to User Certification tab and select the Action "Certify Division Users"

The screenshot displays the 'Security Administration List' web application. The interface includes a top navigation bar with links like LOGOFF, HUD HOME, and SEARCH/INDEX. A secondary navigation bar contains tabs for Security, Role Maint, Access Reports, Activity Reports, and User Certification. The 'Security' tab is active, showing a 'Security List' section with search filters for Division User, HQ Division (Public and Indian Housing), and HQ Office (UAT Testers). A search bar is present with radio buttons for 'User Id' and 'Last Name'. Below the filters, a 'Select User Status' dropdown is set to 'Active'. A table lists users with columns for User ID, User Name, User Type, and Status. The table shows 10 users, including a Guest User and several Super Users.

User ID ▲	User Name ▲	User Type ▲	Status ▲
<a href="#">C54874</a>	Joni Jones	Guest User	Active
<a href="#">HHTC00</a> %	HHTC00 X HHTC00	Super User	Active
<a href="#">HHTC01</a> %	John X Doe	Super User	Active
<a href="#">HHTC02</a> %	HHTC02 X HHTC02	Super User	Active
<a href="#">HHTC03</a> %	HHTC03 X HHTC03	Super User	Active
<a href="#">HHTC04</a> %	HHTC04 X HHTC04	Super User	Active
<a href="#">HHTC05</a> %	HHTC05 X HHTC05	Super User	Active
<a href="#">HHTC06</a> %	HHTC06 X HHTC06	Super User	Active
<a href="#">HHTC07</a> %	HHTC07 X HHTC07	Super User	Active
<a href="#">HHTC08</a> %	HHTC08 X HHTC08	Super User	Active
<a href="#">HHTC09</a> %	HHTC09 X HHTC09	Super User	Active



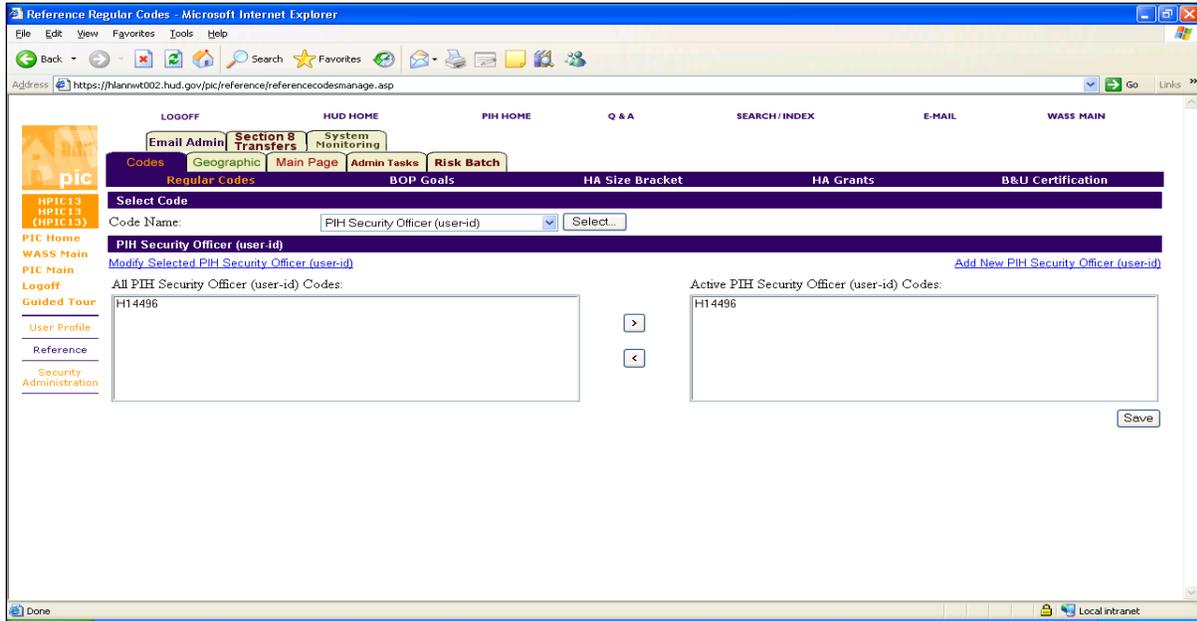
Select the users that need to be certified and click on **"Certify Selected Users"** button. The selected division users will get certified.

### **3.3.3 Certifying a Super User**

PIH-REAC Security coordinator can only certify the Super user and he/she should follow the same steps as described above to certify the Super Users.

### **3.3.4 Certifying PIH-REAC Security coordinator**

A back – end script will be submitted to certify PIH REAC Security Coordinator with the approval by CCB. The H-Id of PIH-REAC Security Coordinator is maintained in the Reference Module as **"PIH Security Office (user ID)"**. Currently this has been populated with the H-Id of **Gary Faeth**. This can also be changed in future by clicking the "Modify Selected PIH Security Officer (user ID)" link. Since this person is at level 1, he/she can certify all the users.



### **3.3.5 Non-Certified users**

All the users should be certified by the security coordinators within the Recertification Window period. The users not certified with in this period will become inactive. This is done internally in the system. These inactive users can be activated through the application. Upon activation, they will be automatically certified for that period.

# Appendix A - Initialization Steps (Super Users Only)

Following are the initialization steps that need to be performed by the Super Users to initialize the recertification, email notification processes and to set up the roles and actions for the users at different levels.

## Initializing the Recertification Process

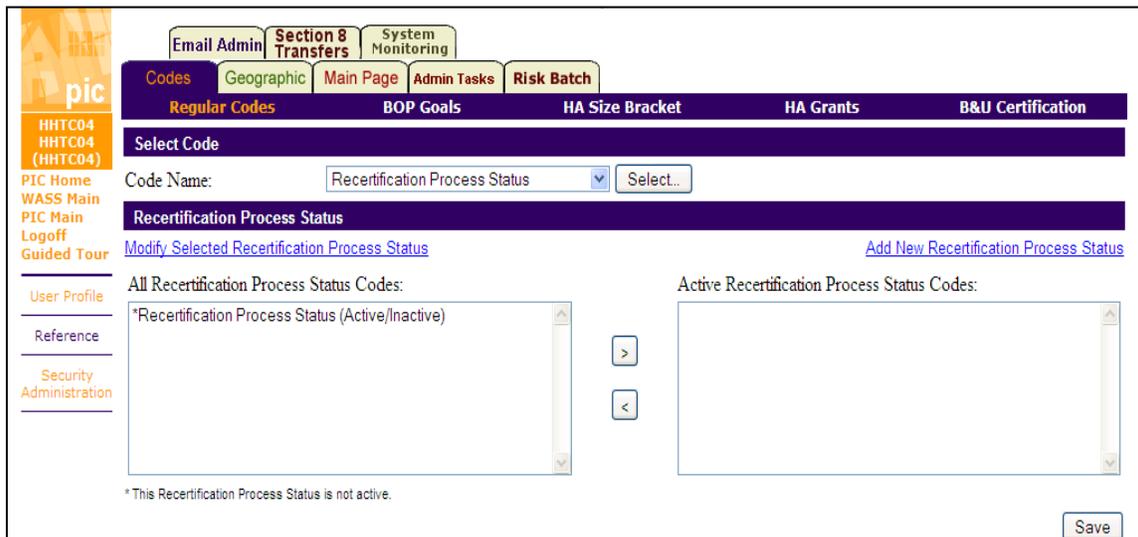
**The Recertification Process can be controlled within IMS through the Reference Sub-module. Typically the process initiation is one time task each year.**

**After initiation and subsequent successful run of the recertification process the configuration parameters need to be updated manually for the next cycle.**

**Super User** will have the ability to set the configuration parameters in order to initiate the User Recertification Process. This will be done by setting values for the following codes in the Reference Sub module.

- a. Recertification Process Status : The status of the process (Active/Inactive)
- b. Recertification Start Date : Beginning of a new user certification period.
- c. Recertification Window : Period for sec. coords. to certify users (days).
- d. Recertification Validity Period : Validity Period for the user certification (days).

**a) Recertification Process Status:** The *Recertification Process Status* indicates whether the process is currently active or inactive. The security coordinators can certify the users only when the process is active.



- b) Recertification Start Date:** This date value - stored in mm/dd/yyyy format - marks the beginning of a new user recertification period. Recommended value: 11/01/yyyy, where “yyyy” is the year of the certification.

The screenshot shows the PIC system interface for configuring Recertification Start Date. The top navigation bar includes links for LOGOFF, HUD HOME, PIH HOME, Q & A, SEARCH/INDEX, E-MAIL, and WASS MAIN. Below this is a secondary navigation bar with buttons for Email Admin, Section 8 Transfers, and System Monitoring. A main menu bar contains Codes, Geographic, Main Page, Admin Tasks, and Risk Batch. The primary menu below that lists Regular Codes, BOP Goals, HA Size Bracket, HA Grants, and B&U Certification. The left sidebar contains a vertical menu with links for PIC Home, WASS Main, PIC Main, Logoff, Guided Tour, User Profile, Reference, and Security Administration. The main content area features a 'Select Code' dropdown menu, a 'Code Name' field with a dropdown set to 'Recertification Start Date' and a 'Select...' button. Below this are two lists: 'All Recertification Start Date Codes' and 'Active Recertification Start Date Codes', both containing the value '11/01/2009'. Navigation arrows (> and <) are positioned between these lists. A 'Save' button is located at the bottom right of the main content area.

- c) Recertification Window:** This value signifies the number of days the security coordinators have to certify user. Recommended value: 30 days.

The screenshot shows the PIC system interface for configuring Recertification Window. The top navigation bar includes links for LOGOFF, HUD HOME, PIH HOME, Q & A, SEARCH/INDEX, E-MAIL, and WASS MAIN. Below this is a secondary navigation bar with buttons for Email Admin, Section 8 Transfers, and System Monitoring. A main menu bar contains Codes, Geographic, Main Page, Admin Tasks, and Risk Batch. The primary menu below that lists Regular Codes, BOP Goals, HA Size Bracket, HA Grants, and B&U Certification. The left sidebar contains a vertical menu with links for PIC Home, WASS Main, PIC Main, Logoff, Guided Tour, User Profile, Reference, and Security Administration. The main content area features a 'Select Code' dropdown menu, a 'Code Name' field with a dropdown set to 'Recertification Window (days)' and a 'Select...' button. Below this are two lists: 'All Recertification Window (days) Codes' and 'Active Recertification Window (days) Codes', both containing the value '30'. Navigation arrows (> and <) are positioned between these lists. A 'Save' button is located at the bottom right of the main content area.

d) **Recertification Validity Period:** This numeric value establishes the validity period for a user certification in number of calendar days. Recommended value: 365 days.

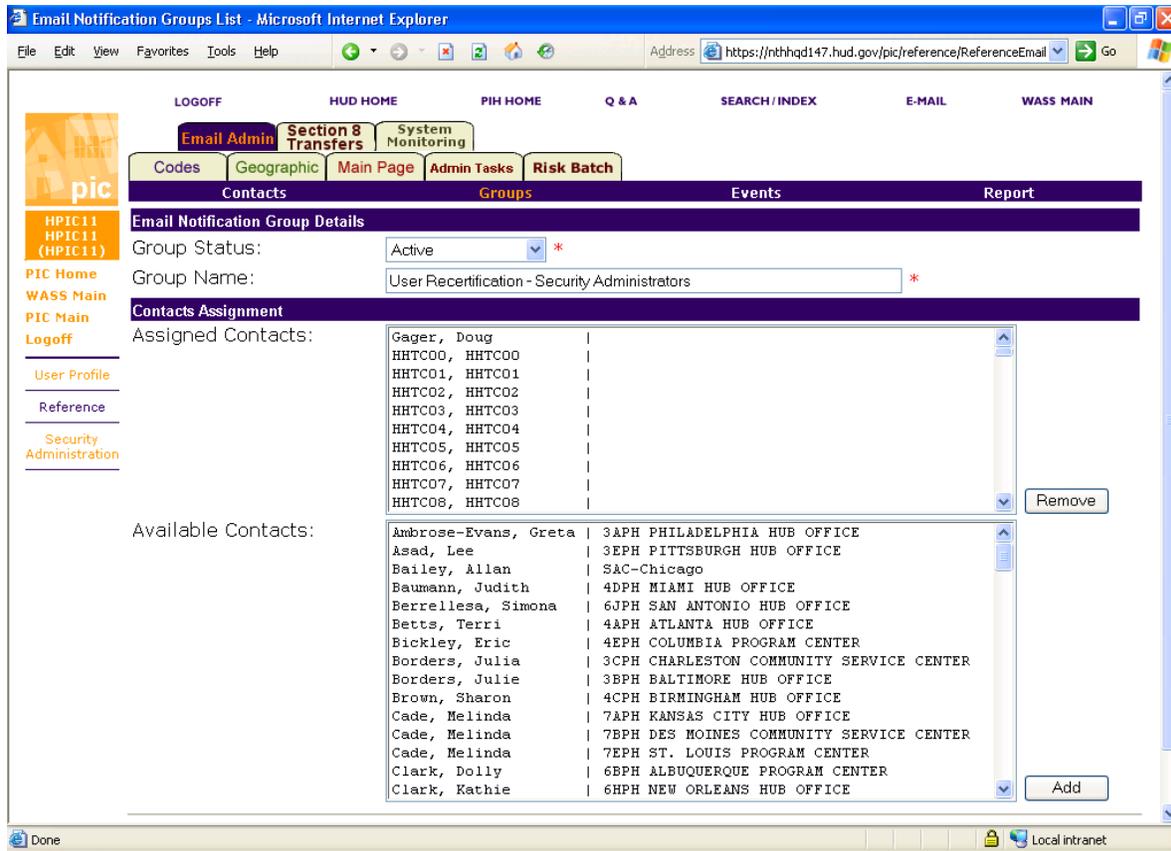
The screenshot displays the PIC system interface for configuring the Recertification Validity Period. The top navigation bar includes 'Email Admin', 'Section 8 Transfers', and 'System Monitoring'. Below this, a secondary bar contains 'Codes', 'Geographic', 'Main Page', 'Admin Tasks', and 'Risk Batch'. The main content area is titled 'Recertification Validity Period (days)'. It features a 'Code Name' dropdown menu set to 'Recertification Validity Period (days)' and a 'Select...' button. Below this, there are two lists: 'All Recertification Validity Period (days) Codes:' and 'Active Recertification Validity Period (days) Codes:'. Both lists currently contain the value '365'. Between the lists are '>' and '<' buttons for moving items. A 'Save' button is located at the bottom right. The left sidebar contains navigation links for 'User Profile', 'Reference', and 'Security Administration'.

### **Initializing the Email Notification Process**

The Email Notification process for User Recertification can be set up by the Super Users by utilizing the "Email Admin" business function under the "Reference" sub-module as mentioned below.

- **Setting the Recertification Group**

A new group called "User Recertification – Security Administrators" should be created under the page group "Groups" as shown below. This group will be automatically linked to the list of contacts. **Super Users need not assign any contacts to this group.**



- **Setting the Recertification Event List**

A new event called "User Recertification" should be added to the "Events" list with the following details to the **Default Message** section

Subject : IMS/PIC User Annual Recertification Reminder Notification  
 Header : Please Note,  
 Message Body: The User Recertification Process in IMS/PIC will take place between [recert\_start\_date] and [recert\_end\_date]. Any users not certified after the [recert\_end\_date] will be automatically inactivated.

Under the **Groups Assignment**, add the "User Recertification – Security Administrators" group. This will associate the "User Recertification – Security Administrators" group created above with this event.

Microsoft Internet Explorer window: Email Notification Events List - Microsoft Internet Explorer  
 Address: https://nthhq147.hud.gov/pic/reference/ReferenceEmail

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

Menu: Email Admin Section 8 Transfers System Monitoring

Sub-menu: Codes Geographic Main Page Admin Tasks Risk Batch

Navigation: Contacts Groups Events Report

**Email Notification Event Details**

Event Status: Active \*

Event Name: User Recertification \*

**Default Message**

Subject: IMS/PIC UAT User Annual Recertification Reminder Notificat \*

Header: Please Note,

Message Body: The User Recertification Process in IMS/PIC UAT will take place between [recert\_start\_date] and [recert\_end\_date]. Any users not certified after the [recert\_end\_date] will be automatically inactivated.

Footer: This is a internal message please do not respond to this emi

**Groups Assignment**

Assigned Groups: User Recertification - Security Administrato

Available Groups: B&U Approval, Demo-Dispo Actual Removal Group, Email Admin, SAC Group, SEMAP Annual Group

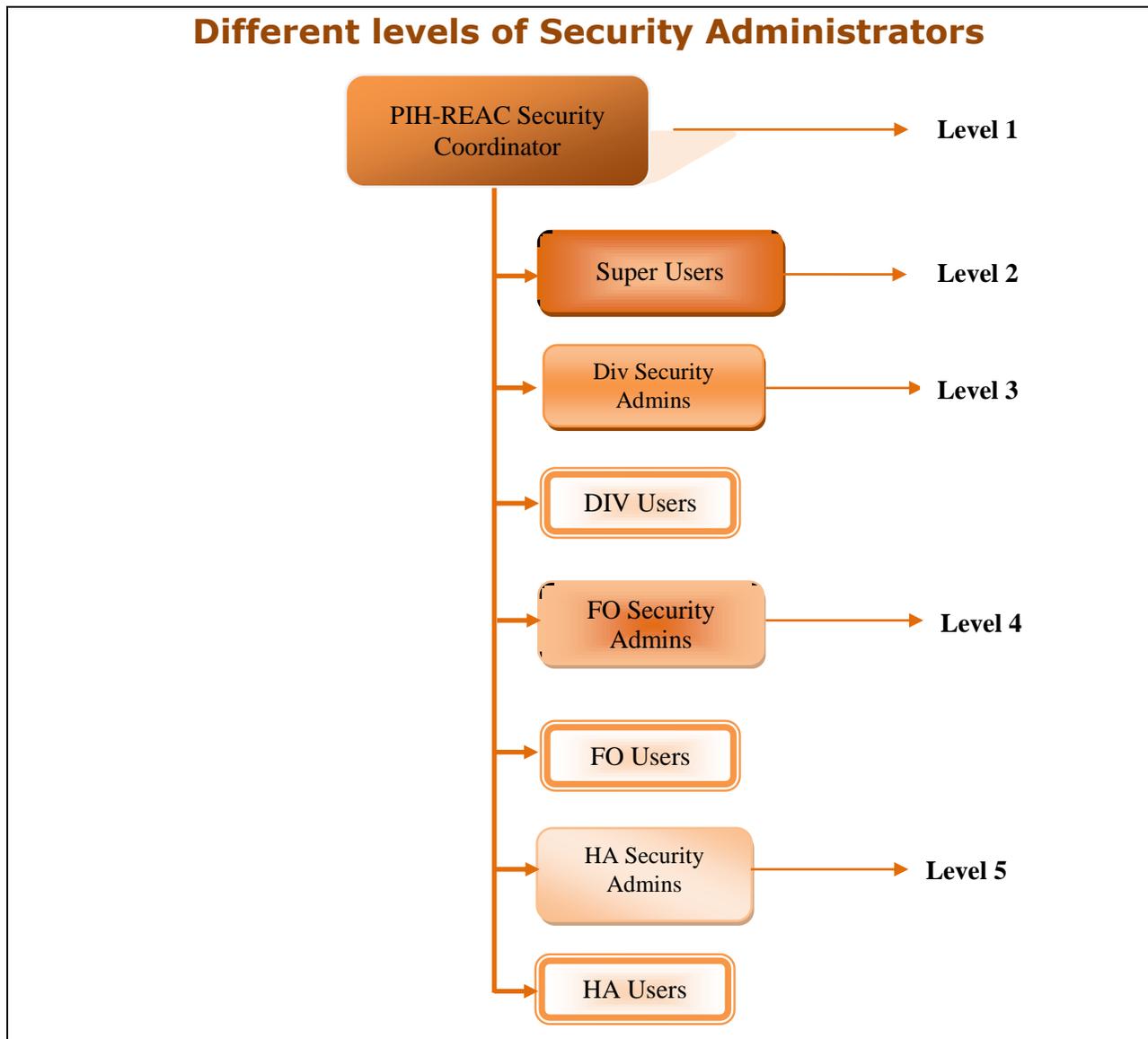
Buttons: Remove, Specify Group Data

Footer: Done Local intranet

# Appendix B - Initializing the Security Roles and Assigning Actions

## Security Actions

To certify a user, the Security Coordinator should have the appropriate security actions added to the existing roles or new roles based on the user types. The actions will be added to the appropriate Security Coordinator role such that the security coordinators at a particular level can certify ALL the Users below that level. The 5 levels are shown below.



The Security Coordinators at each level will be able to certify ALL users under their level. For Example, Division Security Coordinators can certify ALL the users below that level i.e. Division Users, FO Security Admins, FO Users, HA Security Admins, HA users.

**The security coordinators cannot certify themselves or any other security coordinators at their level.**

The following table lists the security coordinators at different level and the type of user they can certify.

User	Super Users	Div Security Coords.	Div Users	FO Security Coords	FO Users	HA Security Coords	HA Users
Sec. Coordinators PIH – REAC Security Coordinator	<input checked="" type="checkbox"/>						
Super Users		<input checked="" type="checkbox"/>					
Div Security Coords			<input checked="" type="checkbox"/>				
FO Security Coords					<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
HA Security Coords							<input checked="" type="checkbox"/>

### Creating Security Roles and assign actions

New Security Coordinator Roles are created for HUD and Super Users under the Security Administration Submodule with appropriate actions to certify other users. This will enable each Security Coordinator to certify the users under their level.

- For HA Users:**

An existing role “**HA Security coordinator**” role should be modified to add following created and appropriate actions:

- View User certification**
- Certify HA Users**

**User Certification**

- View User Certification
- Certify HA Users
- Certify HA Sec Admins

Actions should be added to this role under the User Certification sub module using **Role Maintenance**. This will enable all the HA users who are HA Security Coordinators to certify the HA Users.

- For HUD Users:**

The user type “HUD user” spans the Division as well as Field Office users therefore needs two additional roles in conjunction with the existing HUD security coordinator role.

**Sec Coord - W** - Two different roles will need to be created for different levels of HUD Users.

**i. Div Security Admins/ Coordinators(Level 3)**

User’s Manual - Recertification Process

**User Certification**

- View User Certification
- Certify HA Users
- Certify HA Sec Admins
- Certify FO Users
- Certify FO Sec Admins
- Certify Div Users
- Certify super users

This **existing** role should be modified to add following actions:

- View User certification
- Certify HA Users
- Certify HA Sec Admins
- Certify FO Users

**Div Recertification Admin** - This will be a new role and will have following actions:

- View User certification
- Certify HA Users
- Certify HA Sec Admins
- Certify FO Users
- Certify FO Sec Admins
- Certify Div Users

**User Certification**

- View User Certification
- Certify HA Users
- Certify HA Sec Admins
- Certify FO Users
- Certify FO Sec Admins
- Certify Div Users
- Certify super users

**REAC Security Admin** - This will be a new role created exclusively for REAC Security Coordinator (Gary Faeth) and it will have following actions:

- View User certification
- Certify HA Users
- Certify HA Sec Admins
- Certify FO Users
- Certify FO Sec Admins
- Certify Div Users
- Certify Super Users

**User Certification**

- **View User Certification**
- **Certify HA Users**
- **Certify HA Sec Admins**
- **Certify FO Users**
- **Certify FO Sec Admins**
- **Certify Div Users**
- **Certify Div Sec Admins**
- **Certify super users**

• **For Super Users:**

An existing role "Sec Coord - Super -W" for Super users will be modified to have following actions added to it:

- View User certification
- Certify HA Users
- Certify HA Sec Admins
- Certify FO Users
- Certify FO Sec Admins
- Certify Div Users
- Certify Div Sec Admins

**User Certification**

- View User Certification
- Certify HA Users
- Certify HA Sec Admins
- Certify FO Users
- Certify FO Sec Admins
- Certify Div Users
- Certify super users

**Super Users will be certified by the PIH – REAC Security Coordinator - Gary Faeth.**