

# ART ADMINISTRATION USER GUIDE



## FOR CHRA REGIONAL INFORMATION SERVICES DIVISIONS

Submitted By:  
Civilian Information Services Division (CISD)  
ATTN: DAPE-CPI  
Mail Stop #: 5595  
6010 6<sup>th</sup> Street, Building 1465  
Fort Belvoir, VA 22060-5595

June 2012  
Printed 7/5/2012 11:25 AM

Distribution authorized to Department of Defense (DoD) components and U.S. DoD specified contractors only, for administrative or operational use. Refer other requests for this document to the Office of the Assistant G-1 for CP ATTN: DAPE-CPI, 6010 6<sup>th</sup> Street, Bldg 1465, Fort Belvoir, VA 22060.

**FOR OFFICIAL USE ONLY**

**DOCUMENT HISTORY**

Date	Author	Description	Comment
12 June 2012	Robert E. Johnson	Initial Release	This guide provides instructions for maintaining Civilian Personnel Online (CPOL) account information and user account information for DCPDS.

**CONTENTS**

**1 INTRODUCTION ..... 1**

1.1 PURPOSE..... 1

1.2 ACCESS TO ART ADMINISTRATION ..... 1

**2 ART ADMINISTRATION TOOLS ..... 2**

2.1 GENERAL NAVIGATION TIPS ..... 2

2.2 HOW THE CPOL PORTAL USES THIS INFORMATION..... 2

2.3 MAINTAIN ACCOUNTS ..... 3

2.4 MAINTAIN GROUPS AND ASSIGNMENTS ..... 5

2.5 USER ACCESS AND SECURE VIEW UTILITIES ..... 9

## 1 INTRODUCTION

### 1.1 Purpose

The purpose of the Army Regional Tools (ART) Administration application is to maintain user and group permissions for ART and the Civilian Personnel Online (CPOL) Portal, and to maintain certain application properties.

- Use **Maintain Accounts** to perform the following activities:
  - Assign permissions directly to a user account\*
  - View and modify the contact information for a user account
  - Remove permissions to a user group\*
- Use **Maintain Groups and Assignments** to perform the following activities:
  - Define a new user group\*
  - View, Edit, and Delete an existing group\*
  - Assign or remove group assignments for one or multiple users
- Use **Create one or more ART components** to add a new menu option in the ART application\*
- Use **Edit one or more ART components** to view or modify the properties of a menu item in the ART application\*
- Use **User Access and Secure View Utilities** to perform the following activities:
  - View DCPDS user account permissions
  - Search for security profiles by name or org component(s)
  - Get an org component description
  - Generate a new secure view number

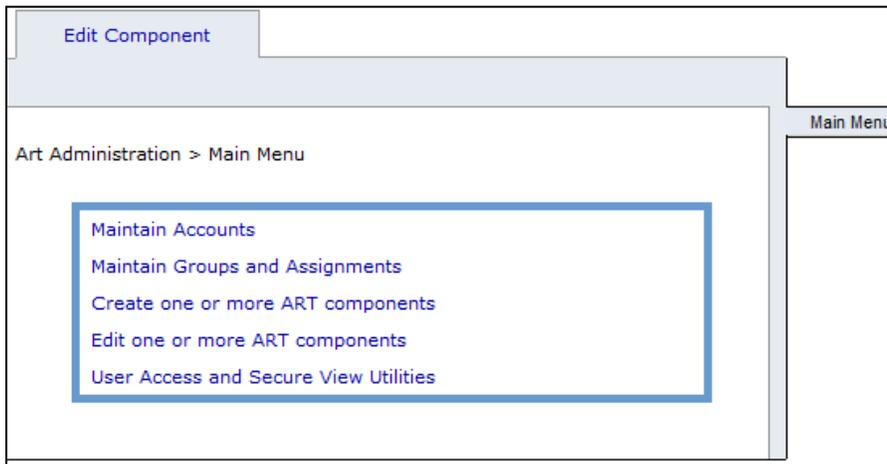
\* **Note:** *Although the section is available, it is intended for CISD use only.*

### 1.2 Access to ART Administration

In order to access the ART Administration application, users must have an HR Specialist tab for the CPOL Portal **and** must be assigned permission in the Access Control List (ACL) for the “Portal ART Administration” application’s “Portal ART Administration” role.

## 2 ART ADMINISTRATION TOOLS

The ART Administration menu is shown below.



There are 5 links available:

1. Maintain Accounts
2. Maintain Groups and Assignments
3. Create one or more ART components
4. Edit one or more ART components
5. User Access and Secure View Utilities

Each menu option is discussed in more detail in the following sections.

### 2.1 General Navigation Tips

Use the “Main Menu” link on the tab to the far right of the screen to return to the main menu from any screen.

**Note:** Any unsaved changes will be discarded if this link is used.

Some of the tools have sub-menus. Use the link on the tab at the top of the screen to return to the menu for that tool.

**Note:** Any unsaved changes will be discarded if this link is used.

### 2.2 How the CPOL Portal Uses This Information

The majority of the ART Administration functionality was designed to manage the specific menu options that should be presented to each user in the legacy ART application. However, the majority of this user access control is implemented by the tabs in the CPOL Portal, e.g. only HR Specialists get access to the Pay Data portlet, but Managers and HR Specialists can both access Org Structure.

The CPOL Portal only references the user's permissions and group assignments to perform the following functions:

- Determining which Helpdesk ticket types and ticket sub-types a user can create.
- Determining which Helpdesk "View Options" to present to the user, which sets the operations the user can perform, e.g. Ticket Report – Open, Ticket Report – Closed, Work Tickets, Work Tickets/Change Owner, etc.
- Determining which Citrix Links to display for each user.

## 2.3 Maintain Accounts

Use the Maintain Accounts option to perform the following activities:

- Assign permissions directly to a user account
- View and modify the contact information for a user account
- Remove a user's permissions to a user group

### 2.3.1 Searching for a User Account or User Group

1. After selecting "Maintain Accounts" from the main menu, the following screen will display.

Please enter the name or CSU userid of the account or group you wish to edit.

Name:

**The following user(s) were returned by the System.**

Test.02072, Atg (AKOTEST\_02072)  
 Test.02074, Atg (AKOTEST\_02074)  
 Test.02075, Atg (AKOTEST\_02075)  
 Test.02077, Atg (AKOTEST\_02077)  
 Test.02082, Atg (AKOTEST\_02082)  
 Test.02084, Atg (AKOTEST\_02084)  
 Test.02086, Atg (AKOTEST\_02086)

**The following group(s) were returned by the System.**

Testing Group (TEST001)

2. Search for a user or group. The search will automatically add wildcards to the beginning and end of the entered search criteria.
  - To maintain an individual user account, enter all or a portion of the user's CSU/ART username or the user's full name.
 

**Note:** Users who have not logged into the ART .asp application will not be retrieved by the search results. **Before the ART .asp application is decommissioned, the search will be changed to include all CSU users.**
  - To maintain a user group, enter all or a portion of the group code or name.
3. Matching users are listed first, followed by matching user groups. Select an account or group to edit.

### 2.3.2 Modifying User Account Properties

Account Properties will only populate for individual users not groups.

1. After selecting a user account, click on the “Account Properties” tab.

Please enter the name or CSU userid of the account or group you wish to edit.  
 Name:

**The following user(s) were returned by the System.**  
[Test.02072, Atg \(AKOTEST\\_02072\)](#)  
[Test.02074, Atg \(AKOTEST\\_02074\)](#)  
[Test.02075, Atg \(AKOTEST\\_02075\)](#)  
[Test.02077, Atg \(AKOTEST\\_02077\)](#)  
[Test.02082, Atg \(AKOTEST\\_02082\)](#)  
[Test.02084, Atg \(AKOTEST\\_02084\)](#)  
[Test.02086, Atg \(AKOTEST\\_02086\)](#)  
[Test.02088, Atg \(AKOTEST\\_02088\)](#)

**The following group(s) were returned by the System.**  
[Testing Only Group - DO NOT USE \(007007\)](#)  
[Testing Group \(TEST001\)](#)  
[Test Helpdesk Group \(TEST010\)](#)  
[Testing without DBA permissions \(TESTING 20110218\)](#)

Please Edit Account Information  
 User ID: AKOTEST\_02072  
 Name: Test.02072, Atg  
 DSN Phone Number:  -  -   
 Commercial Phone Number:  -  -   
 Email Address:   
 Logons Left until Account is Disabled:   
 Inactivate Account: Yes  No

[Manage User Settings for External Applications](#)

Click on the “Account Properties” tab

Click “Submit” to enter your changes

You can enter or modify the following information:

- DSN Phone Number
- Commercial Phone Number
- Email address
- You can specify a number of logons left before the account will be disabled
- You can inactivate an account

- Click on “Submit” once the changes have been made. Once the changes have updated, you will receive the following message:

**Note:** “Manage User Settings for External Applications” is no longer used via Art Administration. All external applications are controlled through ACL.

- Click on “Main Menu” to return to the ART Administration main menu.

## 2.4 Maintain Groups and Assignments

Use the Maintain Groups and Assignments option to perform the following activities:

- Define a new user group (CISD)
- View, Edit, and Delete an existing group (CISD)
- Assign or remove group assignments for one or multiple users.

### 2.4.1 Assigning or Removing Group Assignments

The Group Assignment tool performs:

- View User and Group Assignments
- Add single or multiple users to a single or multiple groups
- Remove single or multiple users to a single or multiple groups

- After selecting “Group Assignment”, a similar screen will display.

The Group Assignment screen has four selection boxes that will be used:

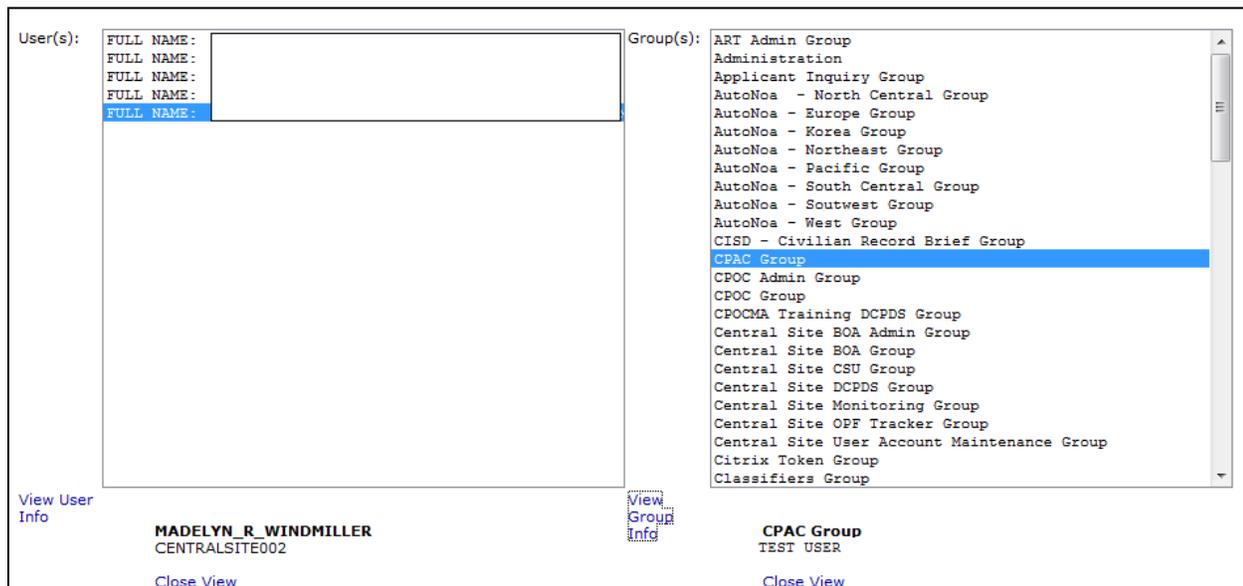
- Region
  - CPAC
  - User(s)
  - Group(s)
2. Select the servicing region of the user(s). A listing of CPACs will populate in the CPAC block.
  3. Select the CPAC that services the user(s) and click on “Submit”.
  4. A list of users whose organization information has been identified with the selected CPAC and Region will populate in the “User(s)” block.
  5. A listing of all groups will populate in the “Group(s)” block.

### 2.4.2 View User Info and View Group Info

Before you begin assigning or removing employees or groups, you should view the current assignments to verify if you need to proceed.

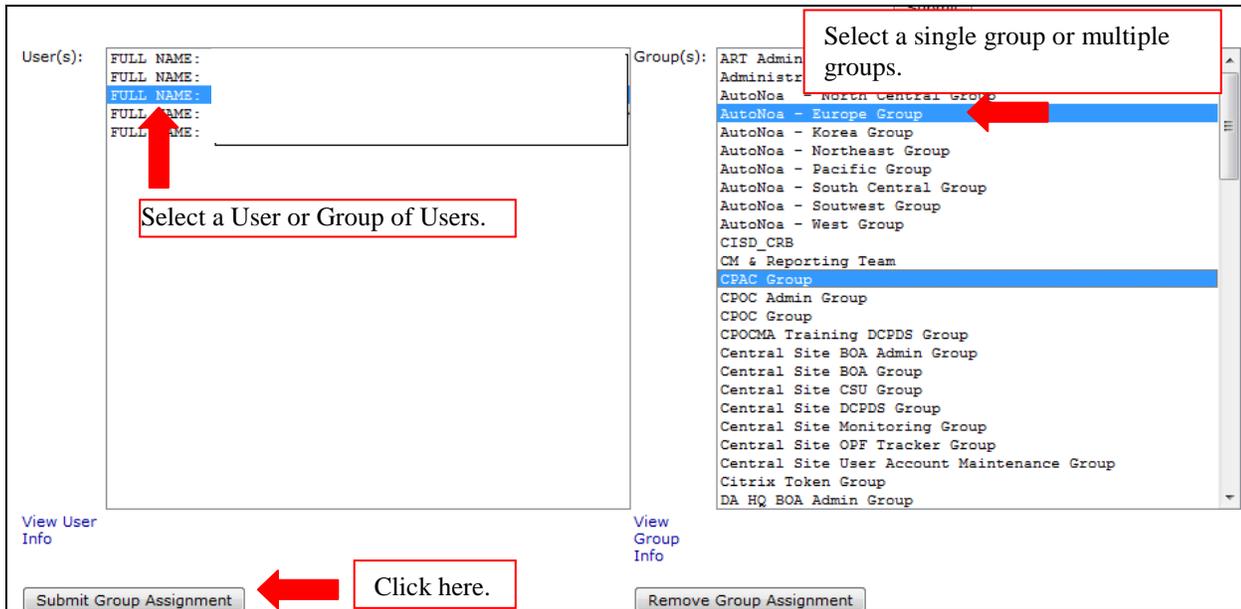
**Note:** You can use the Shift key to select a block of users/groups or you can use the Ctrl key to select multiple users/groups.

- View User Info will identify the assigned group(s) for the selected user(s). Select an employee or a group of employees and click on “View User Info”. To close the view screen, click on “Close View”.
1. View Group Info will identify the assigned employees for the selected group(s). Select a group or multiple groups and click on “View Group Info”. To close the view screen, click on “Close View”.

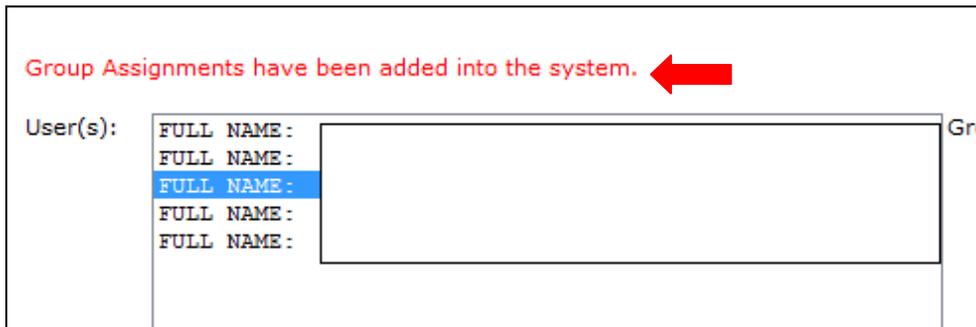


### 2.4.3 Add a User to a Group

1. From the “User(s)” block, select a user or a group of users.
2. From the “Group(s)” block, select a single group or multiple groups.
3. Click on “Submit Group Assignment”

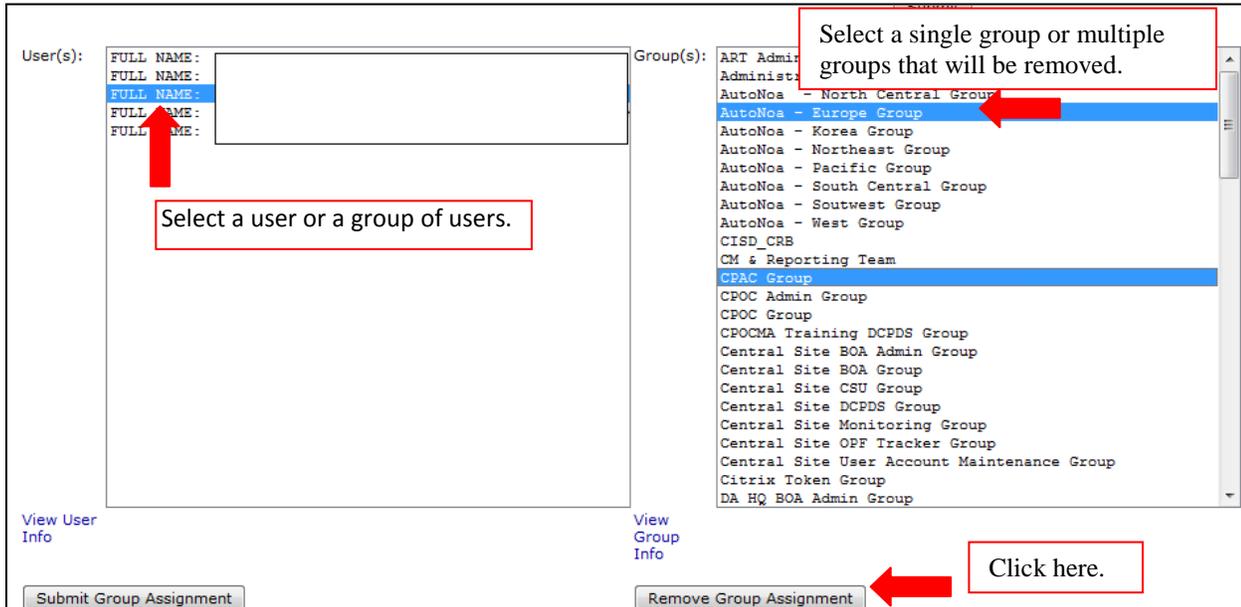


4. Once the groups have been assigned, you will receive the following notification at the top of the screen:



### 2.4.4 Remove a User from a Group

1. From the “User(s)” block, select a user or a group of users.
2. From the “Group(s)” block, select a single group or multiple groups.
3. Click on “Remove Group Assignment”



4. Once the groups have been removed, you will receive the following notification at the top of the screen:



## 2.5 User Access and Secure View Utilities

Use the User Access and Secure View Utilities option to perform the following activities:

- Check DCPDS user access
- Retrieve organization descriptions
- Generate the next Secure View number
- Retrieve an existing Secure View based on organizational input
- Retrieve an existing Secure View based on partial input

**Note:** The Utilities tab will always take you back to the main Utilities page.

### 2.5.1 Check User Access

Use Check User Access to view the following information on a user or multiple users:

- If an employee has a DCPDS User Account
- Date the account was built
- Date user last logged on
- Smart RPA number
- Routing Group Information
- Responsibility Access and the organizations associated with the responsibility
- Groupbox Information

The following search options are available when checking for user access. Unless otherwise noted, the search will automatically add a wildcard at the end of the search string. Wildcards can be added to the beginning or middle of the search string as needed.

Check User Access

By User ID
  By Name (last, first)
  By CCPO ID
  By UIC  
 By Org Component
  By Smart RPA
  By Groupbox Name

- **By User ID:** Allows the search for individual DCPDS user IDs.
- **By Name (last, first):** Allows you to search for individual employee names.
- **By CCPO ID:** Using the CCPO ID will pull all users for the CPAC. This is a helpful tool to find end-dated accounts that are still attached to active user records.
- **By UIC:** Using the Unit ID Code will pull all users for the UIC requested. You must enter the full UIC. No wildcards allowed.
- **By Org Component:** Allows you to search by organization string.
- **By Smart RPA:** This search will pull users with the given Smart RPA number assigned to their user accounts. It does not pull users who are assigned to responsibilities with the given Smart RPA number. You must enter the entire Smart RPA number. No wildcards allowed.
- **By Groupbox Name:** Retrieves a list of groupbox(es) that match the entered pattern. Select the groupbox to view the list of users who are attached to that groupbox.

The search results screen includes the following information:

- **End Date:** This will identify if you have any employees still attached to an end-dated user account.
- **Inbox Name:** Select the “Inbox Name” hyperlink to open the user’s account screen.
- **Full Name**
- **Org Component:** Select the “Org Component” hyperlink to isolate user accounts for a specific organization.
- **Last Logon Date:** Review the Last Logon Date to determine if a user with a DCPDS account has ever logged in or logged in recently. This information can be used to contact the organization and determine if the user is still at that organization.
- **Person Type:** This field identifies the type of user that has been built in DCPDS.

Once the Inbox Name has been selected, the following screen will appear:

Access for TEST.02084, AKO					
Person's Org Component:	<a href="#">AGSEW6D2AAACA</a>	Person Type:	Employee	Position Name:	EXTAG.EXTERNAL USER.2087767.ARSE.EXT
Working Title:		Email Address:	akotest.02084@us.army.mil	Last Logon Date:	
Password Date:		Creation Date:	28-APR-2011	End Date:	
RPA:		Description of RPA:		Default Printer:	
Routing Group Information					
Routing Group Name:	NE_REGION	Default Routing Group?			Y
Initiator:	Y	Requestor:	N	Authorizer:	N
Personnelist:	Y	Approver:	Y	Reviewer:	N
Access Information: AKOTEST.02084-COH					
Responsibility Name	Org Component	Responsibility Smart RPA			
CIVDOD PERSONNELIST					
My Workplace					
Groupbox Information					
User not attached to any groupboxes.					

There are four sections to the Access page.

- General person information contains information about the person who is associated with the user account. The person’s org component is a link to a list of other DCPDS users in that org component. Click on the link to generate the list.
- Routing Group Information contains information about the user’s assigned routing group and the actions available to the user (initiate, request, authorize, etc.).
- Access Information contains information about the user’s assigned responsibilities. The Org Component field is a link to the list of other DCPDS users who belong to org components that match that pattern. Click on the link to generate the list.
- Groupbox Information lists any groupboxes that the user can access. The Groupbox Name is a link to the other DCPDS users who have access to that groupbox. Click on the link to generate the list.

### 2.5.2 Retrieve Organization Descriptions

Retrieving the organization description provides the first two lines of the organization table build from DCPDS. This tool also allows the review of employees assigned to the organization information that has been selected and their type of access.

1. Enter a full or partial Org Component string and select “Get Org Component Description”.

Get an Org Component's Description  
 Enter a full or partial Org Component string and view descriptions:

2. Selecting the Org Component hyperlink will provide a listing of DCPDS users within that organization.

<b>Description of Org Component AGSEW6D2AAACA%</b>		
Org Component	Clear Text 2	Clear Text 3
<a href="#">AGSEW6D2AAACA</a>	CIVILIAN HUMAN RESOURCES AGENCY (CHRA)	NORTHEAST REGIONAL DIRECTOR'S OFFICE

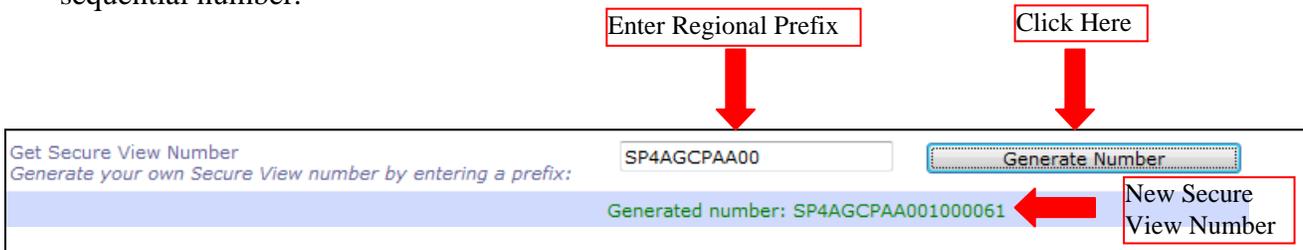
<b>Search for AGSEW6D2AAACA%</b>					
EndDate	Inbox Name	Full Name	Org Component	Last Logon Date	Person Type
			<a href="#">AGSEW6D2AAACA</a>	10-MAY-2011	Employee
			<a href="#">AGSEW6D2AAACA</a>	10-MAY-2011	Employee
			<a href="#">AGSEW6D2AAACA</a>	27-APR-2011	Employee
			<a href="#">AGSEW6D2AAACA</a>	06-MAY-2011	Employee
			<a href="#">AGSEW6D2AAACA</a>	13-MAY-2011	Employee
			<a href="#">AGSEW6D2AAACA</a>	12-MAY-2011	Employee
			<a href="#">AGSEW6D2AAACA</a>	13-APR-2010	Employee
			<a href="#">AGSEW6D2AAACA</a>	13-MAY-2011	Employee
			<a href="#">AGSEW6D2AAACA</a>	11-MAY-2011	Employee
			<a href="#">AGSEW6D2AAACA</a>	13-MAY-2011	Employee
			<a href="#">AGSEW6D2AAACA</a>	13-MAY-2011	Employee
			<a href="#">AGSEW6D2AAACA</a>		Employee
			<a href="#">AGSEW6D2AAACA</a>	01-JUL-2008	Employee
			<a href="#">AGSEW6D2AAACA</a>	18-APR-2011	Employee
			<a href="#">AGSEW6D2AAACA</a>	03-MAY-2011	Employee
			<a href="#">AGSEW6D2AAACA</a>	12-MAY-2011	Employee
			<a href="#">AGSEW6D2AAACA</a>		Employee
	<a href="#">822-41-2082</a>	TEST.02082, AKO	<a href="#">AGSEW6D2AAACA</a>		Employee
	<a href="#">AKOTEST.02084-COH</a>	TEST.02084, AKO	<a href="#">AGSEW6D2AAACA</a>		Employee
	<a href="#">822-41-2085</a>	TEST.02085, AKO	<a href="#">AGSEW6D2AAACA</a>		Employee
	<a href="#">822-41-2086</a>	TEST.02086, AKO	<a href="#">AGSEW6D2AAACA</a>		Employee
	<a href="#">822-41-2020</a>	TEST.TBD20, AKO	<a href="#">AGSEW6D2AAACA</a>		Employee
	<a href="#">822-41-2010</a>	TEST.TBD10, AKO	<a href="#">AGSEW6D2AAACA</a>		Employee
	<a href="#">822-41-2011</a>	TEST.TBD11, AKO	<a href="#">AGSEW6D2AAACA</a>		Employee
	<a href="#">822-41-2012</a>	TEST.TBD12, AKO	<a href="#">AGSEW6D2AAACA</a>		Employee
	<a href="#">822-41-2013</a>	TEST.TBD13, AKO	<a href="#">AGSEW6D2AAACA</a>		Employee
	<a href="#">822-41-2016</a>	TEST.TBD16, AKO	<a href="#">AGSEW6D2AAACA</a>		Employee

3. Selecting the Inbox Name hyperlink will provide the Access page for that user.

### 2.5.3 Generate Secure Views Numbers

Get Secure View Number allows you to generate a new Secure View number if you are building new user access for organization information that does not already exist in DCPDS. This tool is not used by all the regions; please follow your regional office guidance.

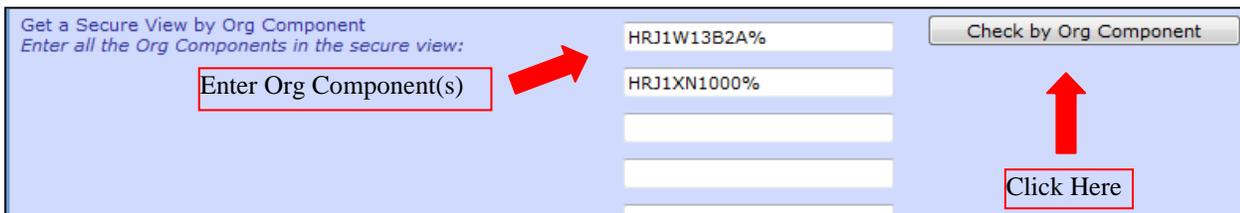
1. Enter your region’s prefix information and click on “Generate Number”. For example: SP4AGCPAA00. Once you click on “Generate Number”, the tool produces the next secure view sequential number.



### 2.5.4 Retrieve an Existing Secure View by Organization

This tool will search the existing Secure Views for one with matching org components.

1. Enter all of the org components being requested for access and click on “Check by Org Component”.



If a Secure View is currently built for the organizations that have been entered, the tool will identify the Secure View number, Responsibility Name(s) associated with that Secure View and which users are currently assigned to the Responsibilities identified.



- Secure View Matching Query Set: Lists other matching secure views that exist in DCPDS. Click the link to view the associated responsibilities and users.
- The lower portion of the screen lists responsibilities and users who are assigned to the first matching secure view.
- The User Name is a link to the details on the user’s account.

### 2.5.5 Retrieve an Existing Secure View by Partial ID

This tool will search the Secure View tables and identify if a secure view currently exists that matches the entered partial ID string.

1. Enter the partial ID string and click on “Check by String”.

Get a Secure View by Partial ID String <i>Enter what you know of the ID string:</i>	<input type="text" value="SP4AGCPAA00"/>	<input type="button" value="Check by String"/>
--	--	--

2. A listing of secure views will generate if the partial string is matched. Click on the individual secure view links to view the list of users assigned to that secure view.

<b>Secure Views like %SP4AGCPAA00%</b>	
	<a href="#">SP4AGCPAA000036155</a>
	<a href="#">SP4AGCPAA000041386</a>
	<a href="#">SP4AGCPAA000036255</a>
	<a href="#">SP4AGCPAA000039001</a>
	<a href="#">SP4AGCPAA000040817</a>