Direct Access User Roles and Functions

Overview

Introduction

This guide provides the procedures for requesting, recertifying, removing, and withdrawing User Roles and Functions in Direct Access (DA).

Please allow 24 hours after PPC approval to see the updated Roles in DA.

Direct Access Functional User Roles

DA Functional User Roles are position based. It is important to **review the requirements** of each User Role and Function to ensure all criteria is met, such as appropriate Approval Authority and/or a Designation Memo provided to PPC. For a list of DA Functional User Roles and the requirements associated with each role, refer to PPC's website at: https://www.dcms.uscg.mil/ppc/da/functionalroles/.

The below User Roles require a **Designation Memo** that must be submitted to PPC Customer Care prior to submitting a User Role request:

- CG Educational Services Officer
- CG Passport Acceptance Agent
- CG Training Officer
- CG Urinalysis Coordinator

Recruiter In Charge

For those requesting the **CG Recruiter In Charge** role and the member's position data in Direct Access does **NOT** indicate Recruiter In Charge, a Designation Memo is required and **MUST** be submitted to PPC Customer Care prior to submitting a User Roles request (see the Understanding Job Data user guide for reviewing a member's position data in DA).

Pending Requests

It is important that the member submitting the User Roles request **follow-up** with the Command Approver to ensure they are aware of the pending User Roles request that is awaiting command approval. If the User Roles request is **NOT** approved by the supervisor within 30 days of submission, the request will be considered invalid upon receipt at PPC and subsequently **DENIED**.

Termination of Roles

If a Command requires termination of User Roles prior to transfer or separation, notify PPC Customer Care. Include the member's Employee ID number and the User Role(s) and Function(s) to be revoked.

Contents

Topic	See Page
Requesting New User Roles	2
Recertifying User Roles	6
Removing User Roles	10
Withdrawing a User Roles Request	14

Requesting New User Roles

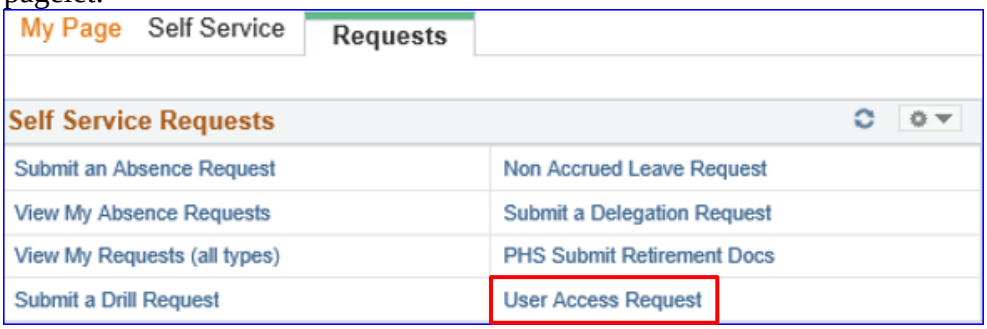
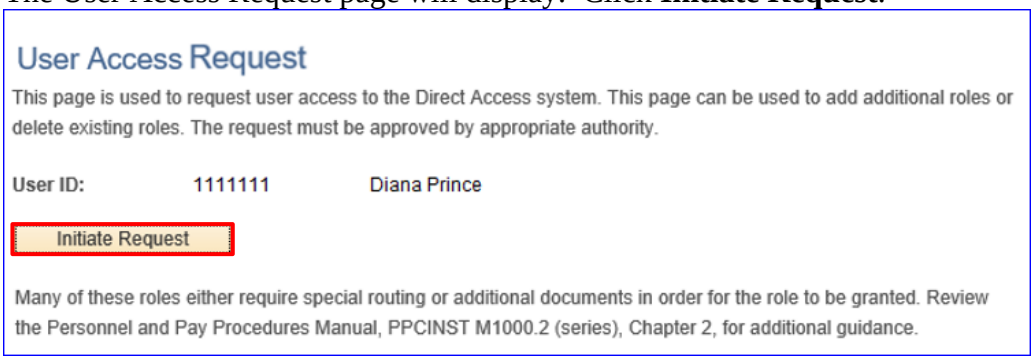
Introduction

This section provides the procedures for requesting new User Roles and Functions in Direct Access (DA).

Remember, please allow 24 hours after PPC approval to see the updated Roles in DA.

Procedures

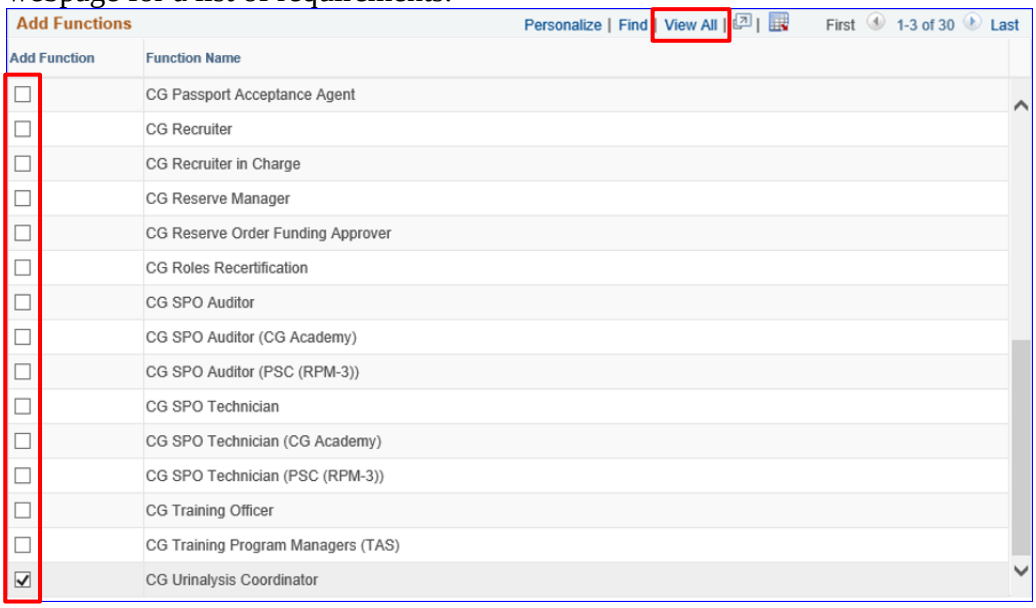
See below.

Step	Action
1	From the Requests tab, click **User Access Request** in the Self Service Requests pagelet. 
2	The User Access Request page will display. Click **Initiate Request**. 

Continued on next page

Requesting New User Roles, Continued

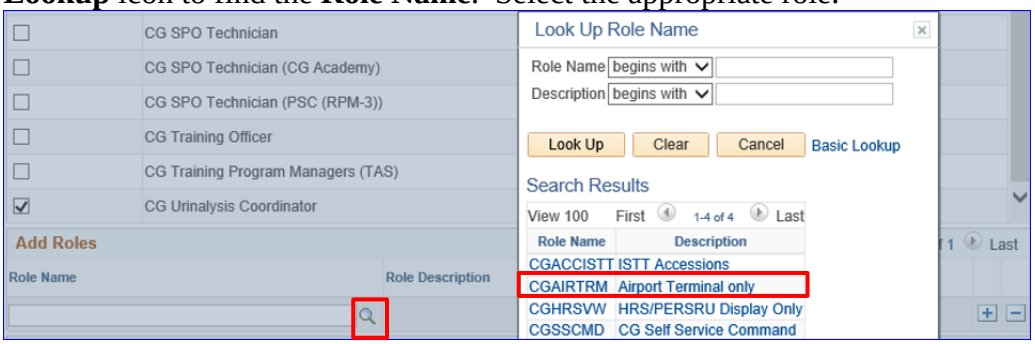
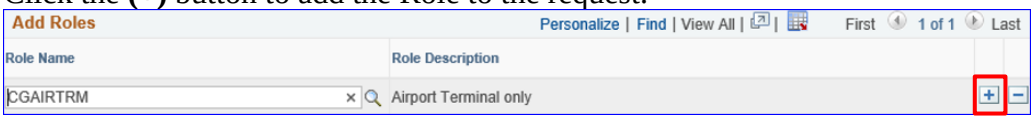
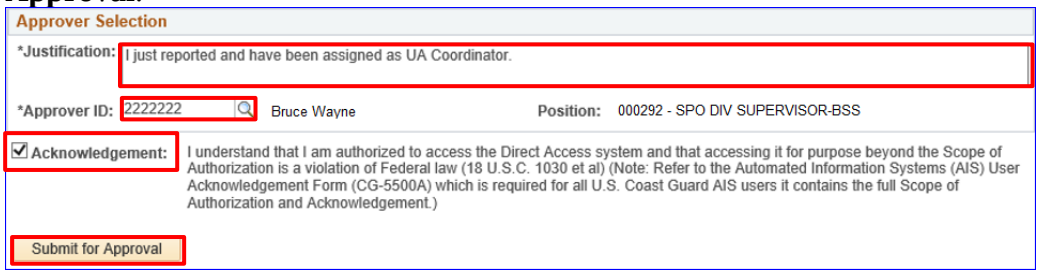
Procedures, continued

Step	Action
3	Any **Current Roles** and **Current Functions** for the member will display. Click **View All** (if necessary) to view the entire list of Current Roles and Current Functions. **NOTE:** When members PCS, their Roles are reset to Self Service only.
4	Under the **Add Functions** section, click **View All**. Scroll through and select the Functions the position requires. **NOTE:** It is important to **review the requirements** of each User Role and Function to ensure all criteria are met, such as appropriate Approval Authority and/or a Designation Memo provided to PPC. See the DA Functional Roles webpage for a list of requirements. 

Continued on next page

Requesting New User Roles, Continued

Procedures, continued

Step	Action
5	If a specific User Role or Function is not listed: under **Add Roles**, click the **Lookup** icon to find the **Role Name**. Select the appropriate role. 
6	Click the **(+)** button to add the Role to the request. 
7	Scroll to the bottom of the page and enter the **Justification** for requesting the User Role(s)/Function(s) (required). Enter the **Approver ID** (approver's Employee ID number) or use the lookup to locate the approver's Employee ID number. Review the statement and check the **Acknowledgement** box. Click **Submit for Approval**. 

Continued on next page

Requesting New User Roles, Continued

Procedures, continued

Step	Action
8	Once submitted, email notification will be sent to the Approver. It is important to follow up with the Approver. If the User Roles request is not approved within 30 days of submission, PPC will automatically **deny** the request. **NOTE:** Once the Approver approves the request, it will be sent to PPC for final approval. From: DoNotReply@direct-access.us Sent: Tuesday, June 05, 2018 12:48 PM To: Wayne, Bruce Subject: [Non-DoD Source] User Access Request – Waiting Approval User access request has been waiting for your approval. Requested For: Diana Prince Request ID: 0000032
9	Upon final approval, email notification will be sent to the requester: From: DoNotReply@direct-access.us Sent: Tuesday, June 05, 2018 14:59 PM To: Prince, Diana Subject: [Non-DoD Source] User Access Request – Approved Your user access request has been approved. Requested For: Diana Prince Request ID: 0000025
10	If the request is denied by either the first approver or PPC, this email notification will be sent to the requester: From: DoNotReply@direct-access.us Sent: Tuesday, June 05, 2018 14:59 PM To: Prince, Diana Subject: [Non-DoD Source] User Access Request – Denied Your user access request has been denied. Requested For: Diana Prince Request ID: 0000029

Recertifying User Roles

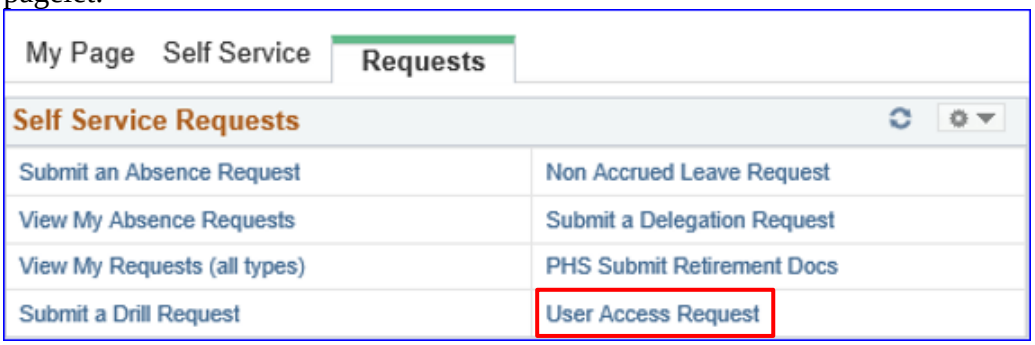
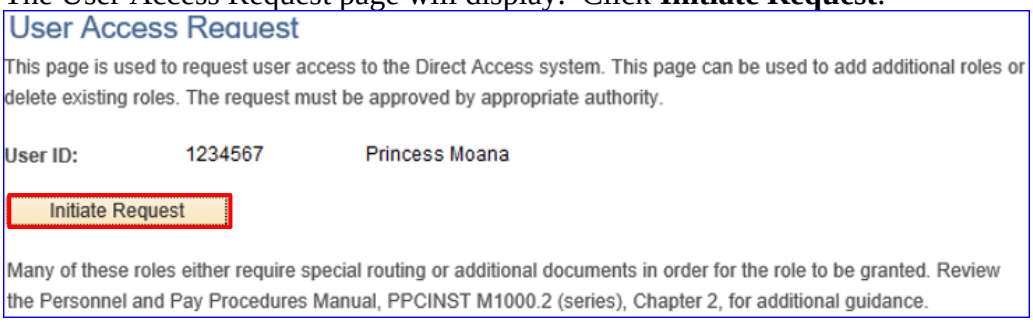
Introduction

This section provides the procedures for recertifying User Roles and Functions in Direct Access (DA).

Remember, please allow 24 hours after PPC approval to see the updated Roles in DA.

Procedures

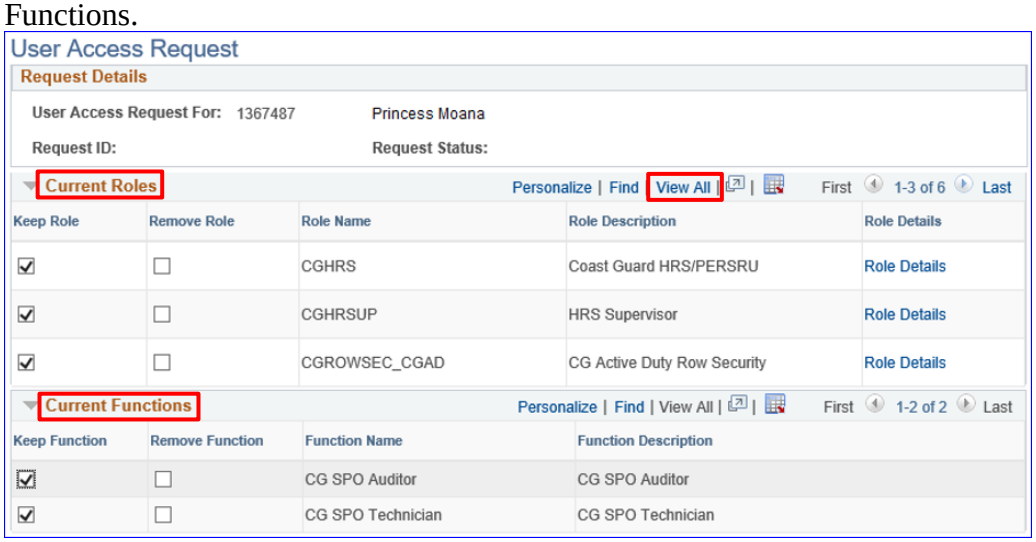
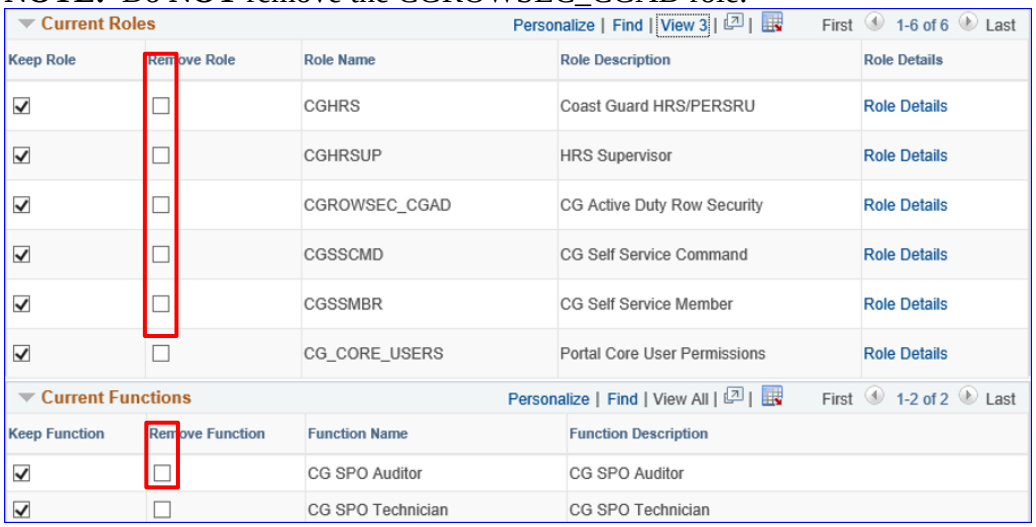
See below.

Step	Action
1	From the Requests tab, select **User Access Request** in the Self Service Requests pagelet. 
2	The User Access Request page will display. Click **Initiate Request**. 

Continued on next page

Recertifying User Roles, Continued

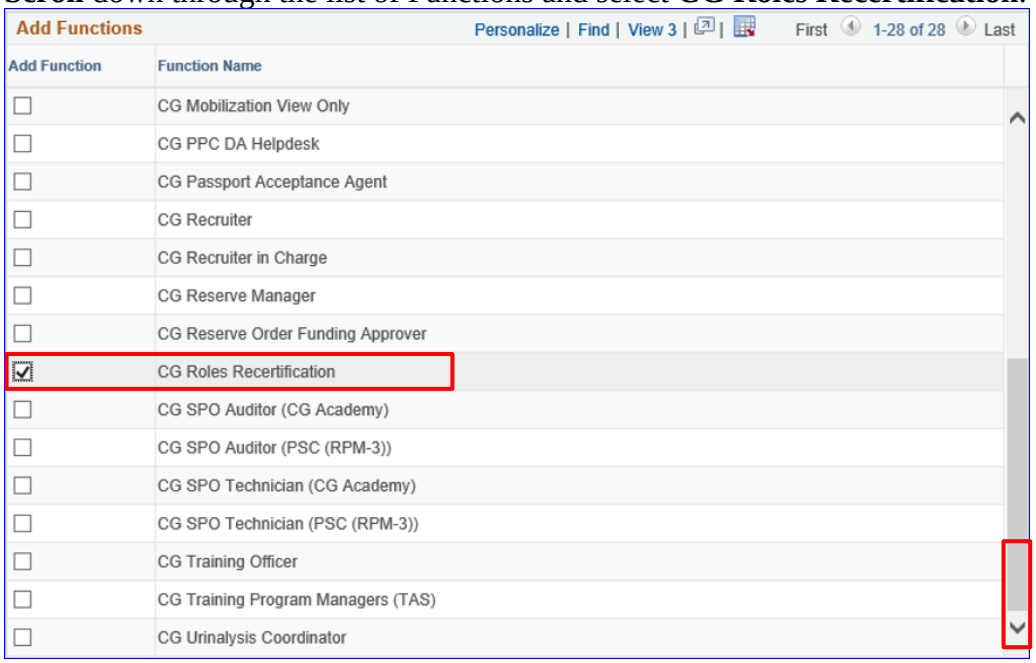
Procedures, continued

Step	Action
3	Any **Current Roles** and **Current Functions** for the member will display. Click **View All** (if necessary) to view the entire list of Current Roles and Current Functions. **NOTE:** When members PCS, their Roles are reset to Self-Service only. See the Requesting New User Roles section for information on how to add Roles and Functions. 
4	Review each Function and Role to ensure they are still valid. If the Function or Role is no longer required, select the appropriate **Remove Role** or **Remove Function** box (see the Removing User Roles section for more information). **NOTE:** Do **NOT** remove the CGROWSEC_CGAD role. 

Continued on next page

Recertifying User Roles, Continued

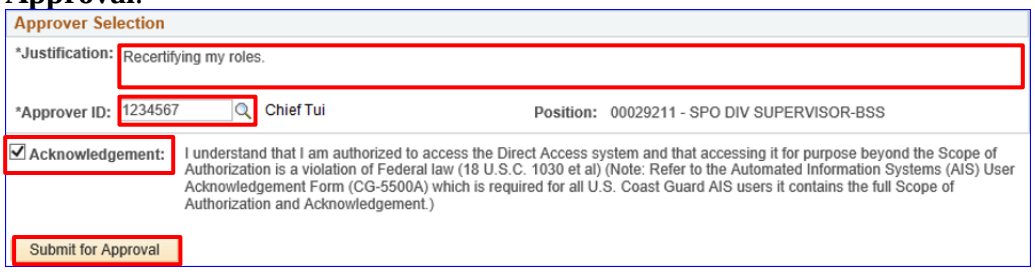
Procedures, continued

Step	Action
5	If everything is accurate, click **View All** in the **Add Functions** section.
6	**Scroll** down through the list of Functions and select **CG Roles Recertification**. 

Continued on next page

Recertifying User Roles, Continued

Procedures, continued

Step	Action
7	Scroll to the bottom of the page and enter the **Justification** for the User Access Request (required). Enter the **Approver ID** (approver's Employee ID number) or use the lookup to locate the approver's Employee ID number. Review the statement and check the **Acknowledgement** box. Click **Submit for Approval**. 
8	Once submitted, email notification will be sent to the Approver. It is important to follow up with the Approver. If the User Roles request is not approved within 30 days of submission, PPC will automatically **deny** the request. **NOTE:** Once the Approver approves the request, it will be sent to PPC for final approval.

Removing User Roles

Introduction

This section provides the procedures for removing User Roles and Functions in Direct Access (DA).

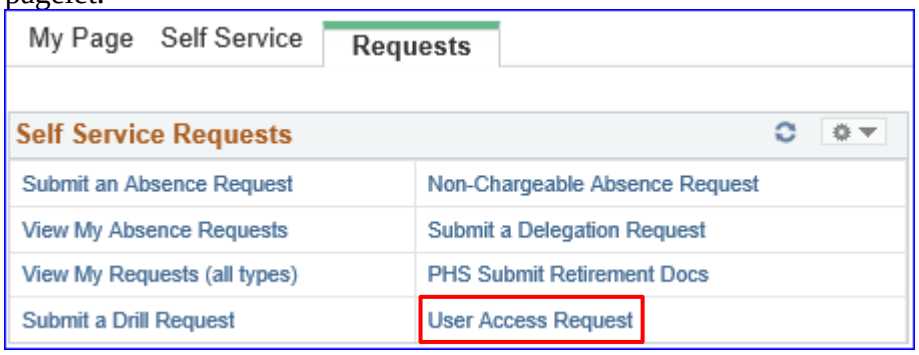
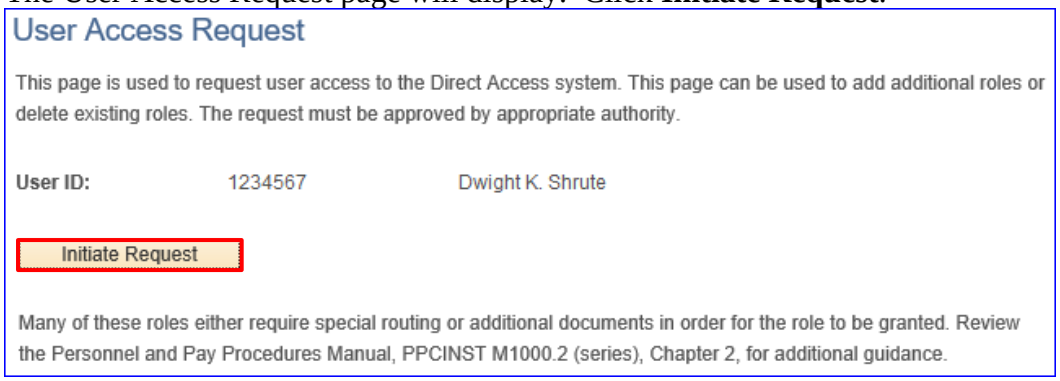
Please allow 24 hours after PPC approval to see the change in DA.

Termination of Roles

If a Command requires termination of User Roles prior to transfer or separation, notify PPC Customer Care. Include the member's Employee ID number and the User Role(s) and Function(s) to be revoked.

Procedures

See below.

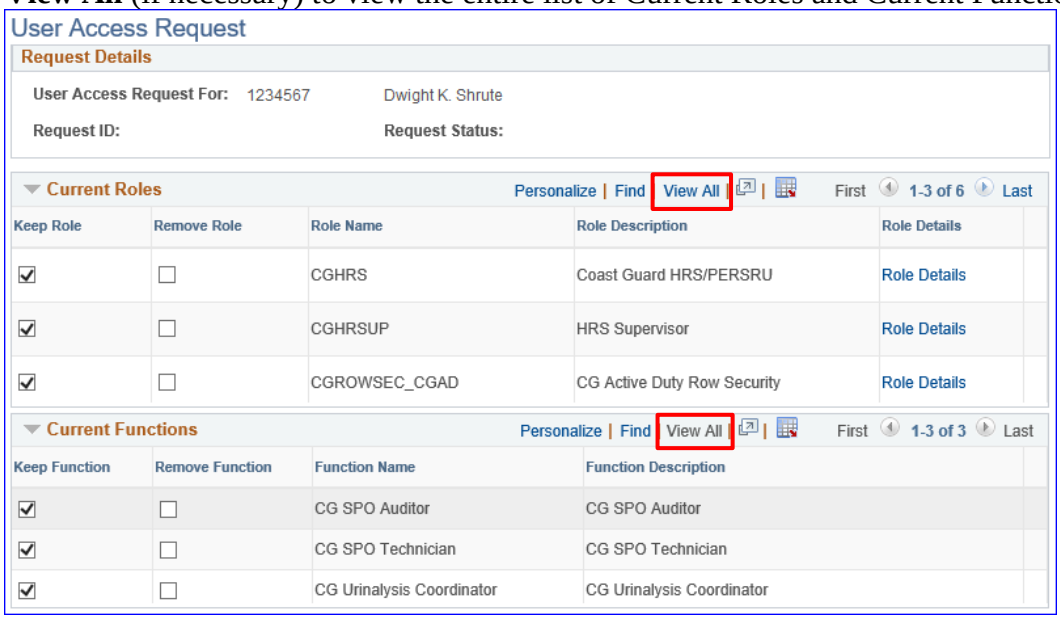
Step	Action
1	From the Requests tab, select **User Access Request** from the Self Service Requests pagelet. 
2	The User Access Request page will display. Click **Initiate Request**. 

Continued on next page

Removing User Roles, Continued

Procedures,
continued

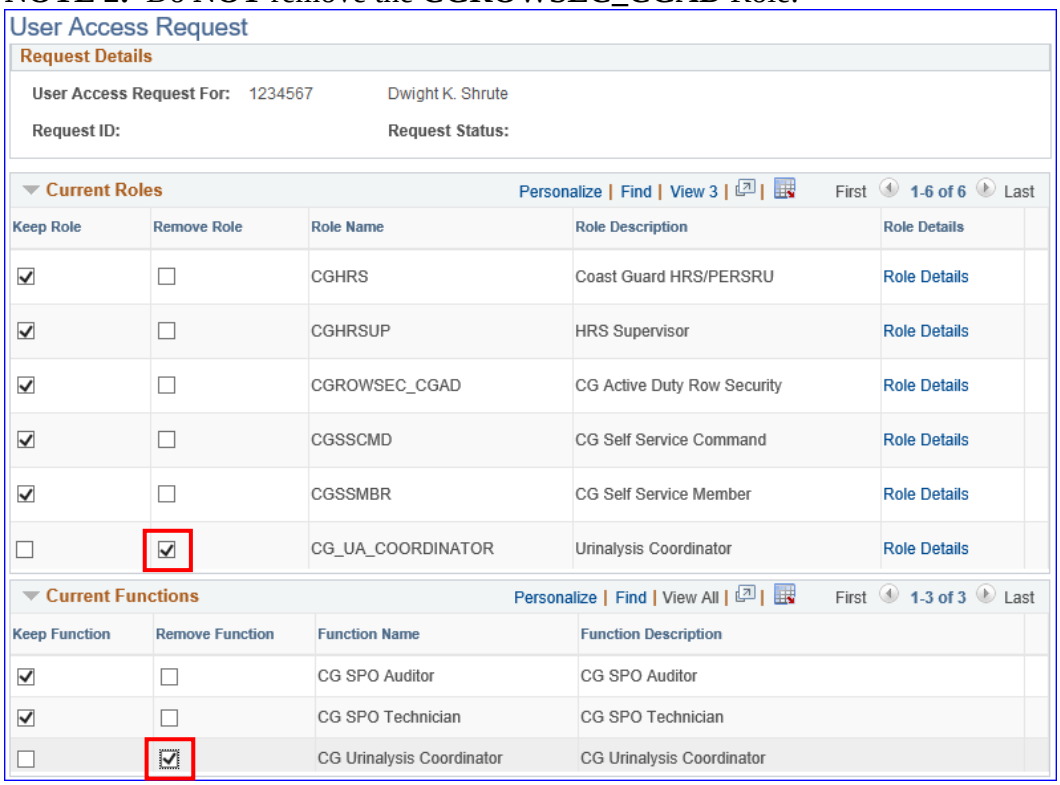
Step	Action
3	Any **Current Roles** and **Current Functions** for the member will display. Click **View All** (if necessary) to view the entire list of Current Roles and Current Functions.



Continued on next page

Removing User Roles, Continued

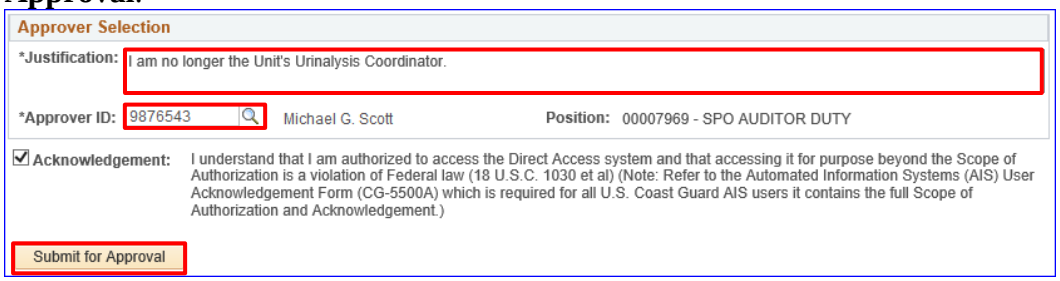
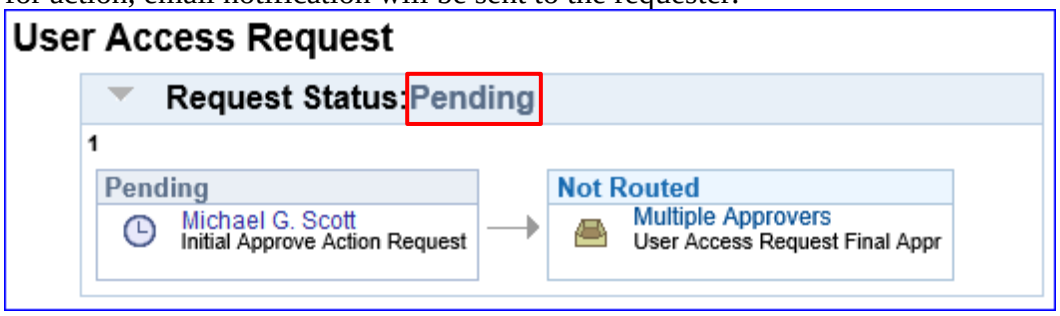
Procedures,
continued

Step	Action
4	Check the **Remove Role** box for each Role and/or Function to be removed. **NOTE 1:** For information on adding User Roles and Functions, see the Requesting New User Roles section. **NOTE 2:** Do **NOT** remove the **CGROWSEC_CGAD** Role.  User Access Request Request Details User Access Request For: 1234567 Dwight K. Shrute Request ID: Request Status: Current Roles — Personalize | Find | View 3 | First 1-6 of 6 Last Keep Role / Remove Role / Role Name / Role Description / Role Details ☑ ☐ CGHRS Coast Guard HRS/PERSRU Role Details ☑ ☐ CGHRSUP HRS Supervisor Role Details ☑ ☐ CGROWSEC_CGAD CG Active Duty Row Security Role Details ☑ ☐ CGSSCMD CG Self Service Command Role Details ☑ ☐ CGSSMBR CG Self Service Member Role Details ☐ ☑ CG_UA_COORDINATOR Urinalysis Coordinator Role Details Current Functions — Personalize | Find | View All | First 1-3 of 3 Last Keep Function / Remove Function / Function Name / Function Description ☑ ☐ CG SPO Auditor CG SPO Auditor ☑ ☐ CG SPO Technician CG SPO Technician ☐ ☑ CG Urinalysis Coordinator CG Urinalysis Coordinator

Continued on next page

Removing User Roles, Continued

Procedures,
continued

Step	Action
5	Scroll to the bottom of the page and enter the **Justification** for removing the User Role/Function (required). Enter the **Approver ID** (approver's Employee ID number) or use the lookup to locate the approver's Employee ID number. Review the statement and check the **Acknowledgement** box. Click **Submit for Approval**. 
6	The request is now in a **Pending** status and email notification has been sent to the Approver. Once the request is approved, it will forwarded to PPC for action. Once PPC takes for action, email notification will be sent to the requester. 

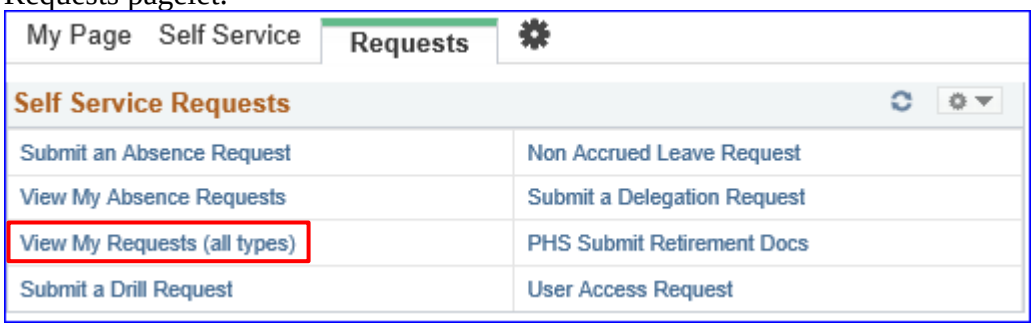
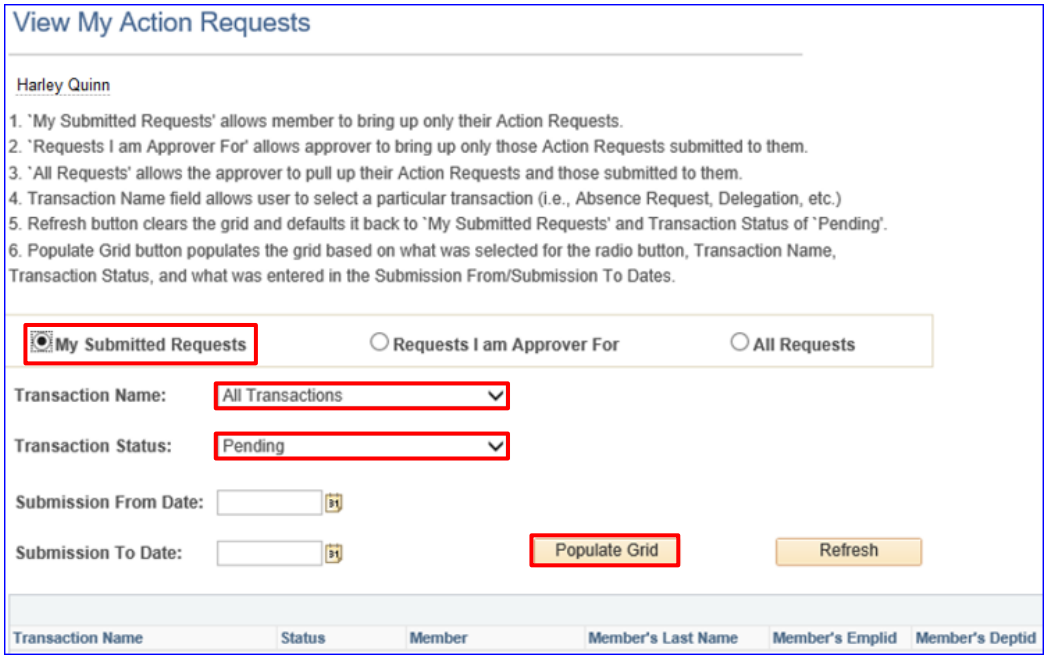
Withdrawing a User Roles Request

Introduction

This section provides the procedures for withdrawing a User Role request in Direct Access (DA) in the event the approver becomes unavailable (transferred, separated, TDY, etc.).

Procedures

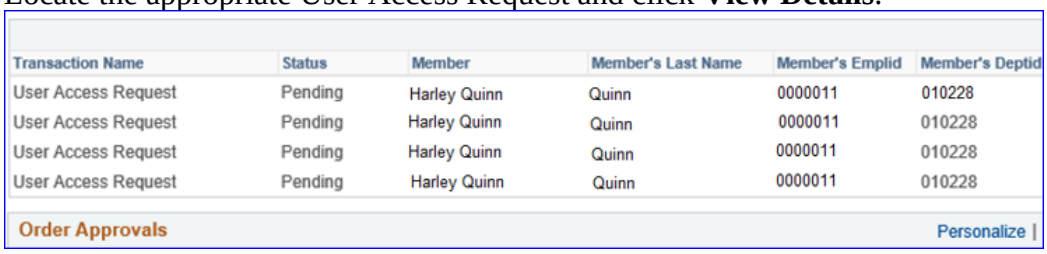
See below.

Step	Action
1	From the Requests tab, click **View My Requests (all types)** in the Self Service Requests pagelet. 
2	The View My Action Requests page will display. Ensure the **My Submitted Requests** button is selected. The **Transaction Name** will default to All Transactions and the **Transaction Status** will default to Pending. Click **Populate Grid**. 

Continued on next page

Withdrawing a User Roles Request, Continued

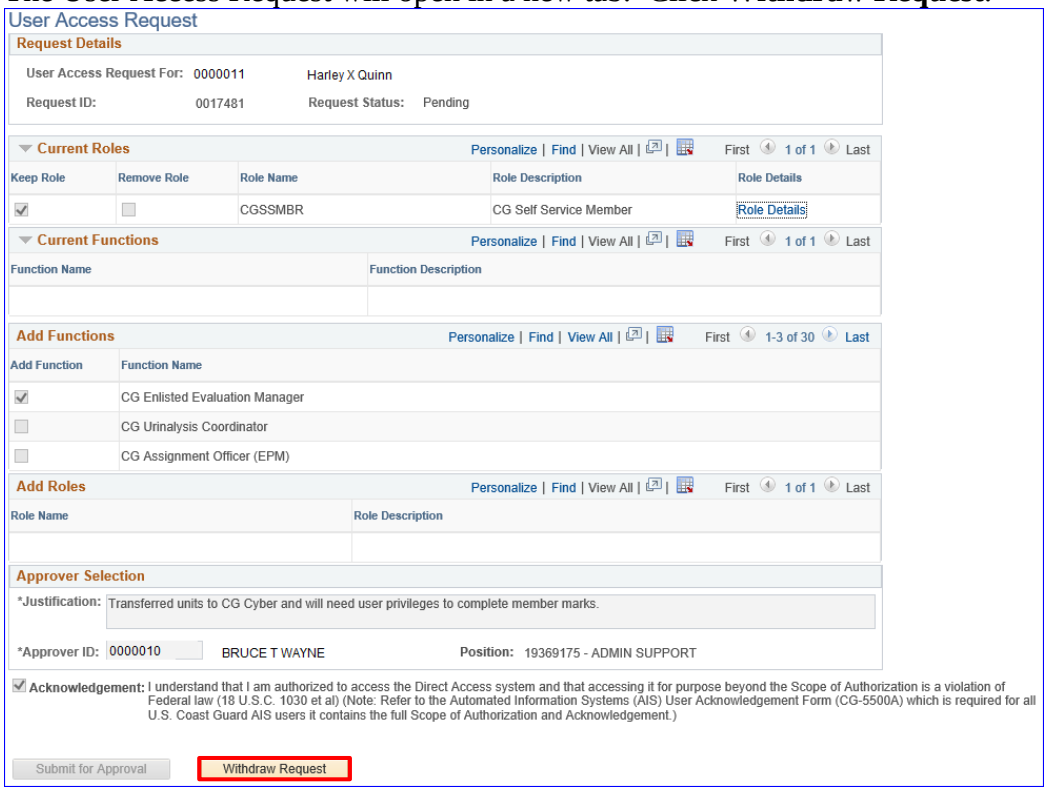
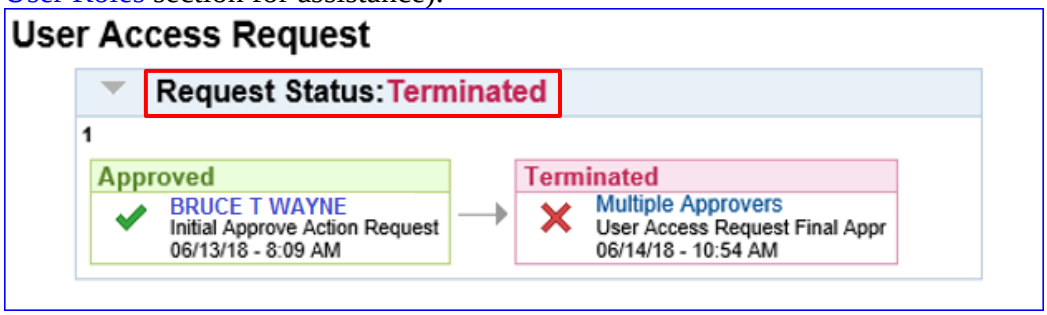
Procedures, continued

Step	Action
3	Any Pending User Access Requests will be listed. Scroll to the right and click **View All** to ensure all records are shown. Locate the appropriate User Access Request and click **View Details**. 

Continued on next page

Withdrawing a User Roles Request, Continued

Procedures,
continued

Step	Action
4	The User Access Request will open in a new tab. Click **Withdraw Request**. 
5	The **Request Status** will update from **Pending** to **Terminated**. ‘**X**’ out of the tab to return to View My Requests (all types). A new User Access Request will need to be submitted (see the Requesting New User Roles section for assistance).