Capacity Building Grant Program (Section 4 and RCB) DRGR Roll Out

DRGR Grantee User Account Roles and Setup

Overview

New for FY2015, HUD Community Planning Development (CPD) Capacity Building (CB) Grantees ("Grantees") will be using the Disaster Recovery Grants Reporting (DRGR) system to manage its grants. To utilize the system, Grantees must properly establish DRGR accounts for all applicable users and assign these users to roles that cover all applicable system functions. This guidance will provide an overview of the DRGR user account responsibilities and setup, and provide links to existing DRGR account training resources.

DRGR Grantee User Accounts and Roles

1. DRGR Grantee User Account

DRGR provides an interface for comprehensive grants management; therefore Grantees need multiple users in the system to handle all of the required user roles. Grantee users must have an active account to access the DRGR system and they must be associated with the capacity building grant award and certified by the Grantee Administrator user to access Grant files.

2. DRGR Grantee User Roles

When a new DRGR user account is setup by the Grantee Administrator, the Grantee Administrator has the ability to assign multiple roles to the Grantee user. The available roles include …

- View Only – Grantee user has access to the system to view grantee files, but has no authority to modify user accounts, edit files, or request/approve drawdowns;
- Grantee Admin - top level user responsible for requesting additional Grantee users and managing the user roles and grant access for existing Grantee users;
- Request Drawdown* – user has the ability to create drawdown vouchers in the DRGR Drawdown module;
- Approve Drawdown* – user has the ability to approve drawdown vouchers created by the Request Drawdown user(s);
- Submit Action Plan – user has the ability to not only make edits to the Action Plan, but also has the ability to submit the Action Plan to HUD; and
- Submit Performance Report - user has the ability to not only make edits to the performance report, but also has the ability to submit the performance report to HUD.

*** No single user may be given both drawdown roles. These roles have to be split between unique users.**

A single grantee user may have multiple roles. For example a Grantee Administrator can also have Approve Drawdown, Submit Action Plan, and Submit Performance report roles. In addition, the

Grantee Administrator has the ability to modify grantee user roles if the responsibilities of individuals change throughout the grant period. HUD strongly encourages the Grantee to have users in the system to backup each role to allow for continuity of roles in the case of a user's absence.

DRGR Grantee User Account Creation and Management

1. Grantee Administrator

As outlined in the roles section, the Grantee Administrator is the top level grantee user and is subsequently accountable for the following responsibilities:

- Requesting new grantee user accounts;
- Modifying grantee user accounts;
- Associating grantee users with grants in the system; and
- Certifying grantee users to access DRGR.

A Grantee's primary Grantee Administrator will be established in DRGR by the assigned HUD Representative. HUD will be in touch directly with the Grantee's authorized representative to collect the information needed to establish the initial Grantee Administrator account.

2. Grantee User Account Creation and Management

Grantee Administrators have the ability to request new grantee user accounts and modify existing grantee user accounts. However, the first grantee user setup in the system, the primary Grantee Administrator, must be established by HUD. HUD will provide Grantees with instruction on this process during the webinar training, if additional questions arise, please contact your HUD representative.

Grantee Administrators can request a new grantee user account and assign system roles using the "Request New User" link found on the left side of the Admin Module screen. Additionally, Grantee Administrators can edit existing grantee user accounts using the "Manage Existing Users" link on the left side of the Admin Module screen. All grantee user account requests and modifications are sent to HUD for approval prior to the new user accessing the system or the existing user accessing gaining/losing DRGR functions.

For specific instructions on these user account functions, please read this HUD DRGR Fact Sheet - New User Requests and Changes to Existing Users.

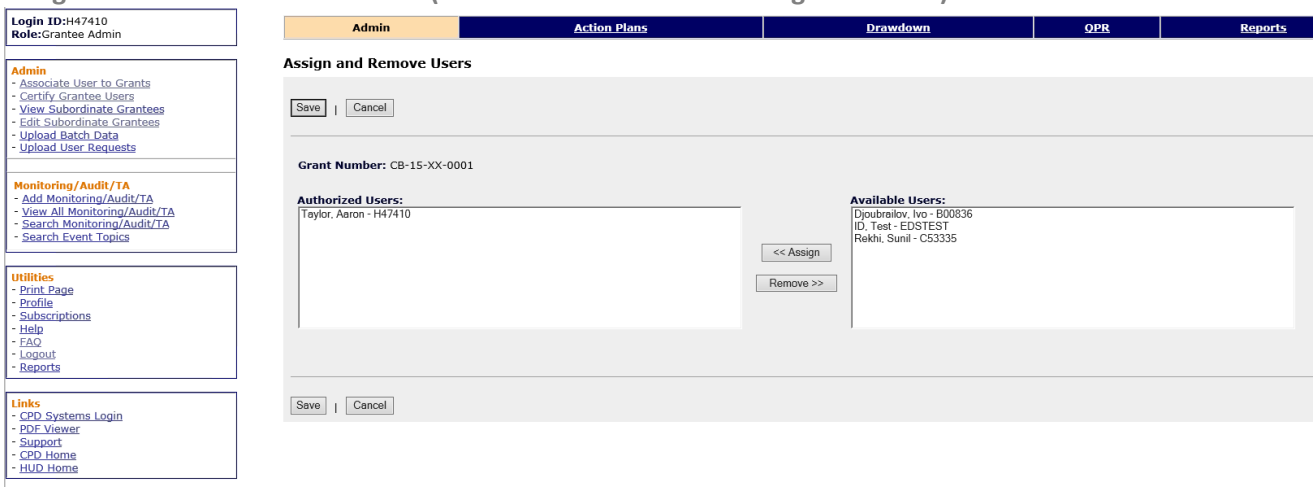
*** All new users are required to provide a five digit numerical security pin on the "Request New User" screen. This pin will be used to provide initial entry into the system and will be requested if the user calls the HUD national help desk for DRGR assistance or to unlock a DRGR account, please keep a record of the DRGR user security pins on file.**

3. Grantee User Account Association and Certification

In addition to managing accounts, Grantee Administrators must ensure that Grantee users maintain access to the system. When Grantee users are initially added to the system or existing system users are identified to work on a new grant, the users must be associated with the grant

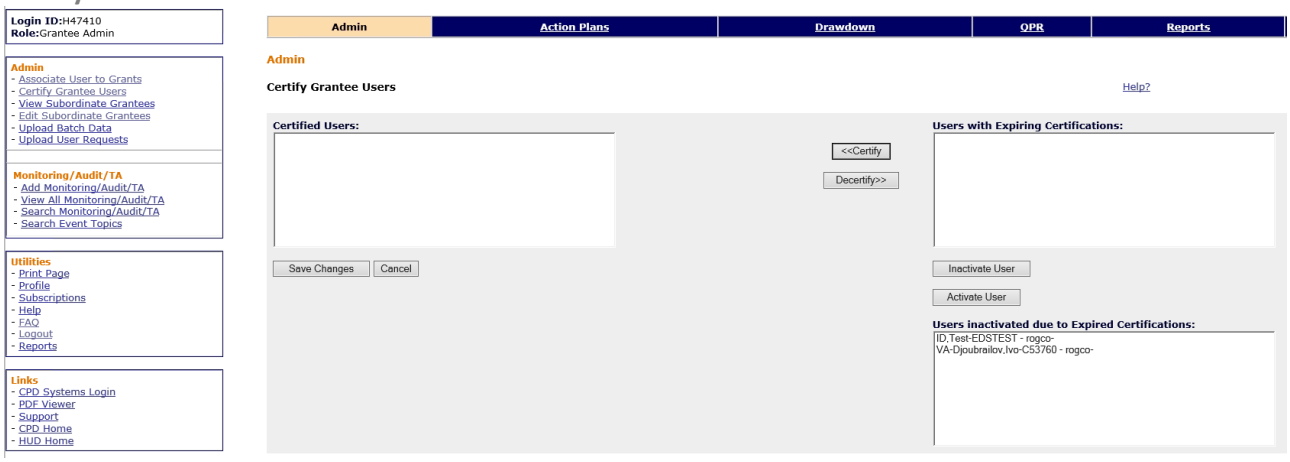
award. To complete this function, Grantee Administrators should click on the "Associate Users to Grant" link on the Admin Module screen and then select the specific grant award from the resulting list. The resulting webpage is called the "Assign and Remove Users" screen. On the screen, Grantee Administrators select specific users from the *Available Users* box and then click the "assign" button to move them to the *Authorized Users* box (see screen shot below). Once the user has been moved to the *Authorized Users* box click "save" and the Grantee user association will be complete.

Assign and Remove Users screen – (Associate Grantee users to a grant award)



Along with Grantee user account association, Grantee Administrators are also responsible for certifying Grantee users from its organization to access the DRGR system. All DRGR users must be certified/re-certified twice a year. The certification expirations dates are 6/30 and 12/31. If a Grantee user is not certified before the expiration date, then their account will lock and they will be unable to access the system until they are re-certified. To complete this function, Grantee Administrators should click on the "Certify Grantee Users" link on the Admin Module screen. The resulting webpage is called the "Certify Grantees Users" screen. On the screen, Grantee Administrators select specific users from the *Users with Expiring Certifications* box or *Users Inactivated* box and then use the directional buttons to the move the users into the *Certified Users* box (see screen shot below). Once the user has been moved to the *Certified Users* box click "save" and the Grantee user certification will be complete.

Certify Grantee Users screen



Grantees are encouraged to utilize the existing DRGR resources on the HUD Exchange if they have any issues or contact the assigned HUD representative for its grant award.