Page 3: Overview

Page 6
Roles & Authority
Foundational roles in JustGrants and details of the authority and abilities of each

Page 9
DIAMD
Step-by-step setup instructions for SMS, Voice, or Biometric secondary authentication that is necessary to access JustGrants

Page 30
User View
The navigation bar and various tabs that allow you to access the particulars of your award

Page 40
Role Reassignment
Step-by-step instructions for the Entity Administrator to reassign tasks based upon roles

Table of Contents
Overview

This guide will provide information to:

• Identify the six foundational external roles and their respective capabilities in JustGrants

• Navigate the JustGrants Entity Landing Page to view Entity-level information and act on assigned work

• Explain the use of the JustGrants navigational tab structure

As an introduction to the information in this guide, let’s first cover some of the new terms, processes, and features of JustGrants.

IMPORTANT

During the initial role-out of JustGrants, please be aware that:

• The system does not “auto save” your work.
• You will see a warning message after 10 minutes of inactivity (per security requirements).
• You will be automatically logged out if you are inactive for 15 minutes (per security requirements).
• Unsaved work will not be saved at logout.
JustGrants User: Basics

It’s here! With the new release of JustGrants, applicants and grantees have an entirely new system that provides increased access and transparency throughout the grant process. There are new terms and processes that align DOJ with the larger Federal Government to streamline the grants process for all users.

The first term of note is “Entity”, which is used in place of “Organization”. When you first open JustGrants, you will find the left navigation options are labeled “Entity Profile”, “Entity Users”, and “Entity Documents”.

Also, entity-level data now is managed in SAM.gov, which is considered the Federal Government’s “source of truth” or “authoritative source” of information regarding entities. Changes and updates to information are made in SAM.gov, then JustGrants pulls its entity information directly, ensuring data consistency and integrity.

JustGrants provides users with two notifications sections. One displays system-wide alerts across banners on the “Home” page, and the other provides “bell notifications” specific to the user.

The customized “Home” page is prepopulated with information relevant to the specific user. The “Home” page features “My Worklist”, which displays information based on all the user's designated roles, application assignments, and award assignments.

This update also features a brand-new, intuitive navigation system with a user-friendly visual design that clearly differentiates workspaces, distinguishes sections by font size, and improves data management using different colors to separate table sections.
JustGrants User: **Highlights**

---

**Key Takeaways**

- In addition to the introduction of **six foundational roles**, JustGrants introduces increased visibility among users within the entity – the Entity User and their Entity Profile – allowing for more efficient user management.

- **One Email Address = One User = One Entity.** Your login will be your email address. An external user cannot use the same email address to access different Entity pages.

- **One Email Address = One User = Multiple Roles = One User Experience.** All of the work and permissions associated with your login will be dynamically displayed on your home page.

- **Entity-level information (name, unique identifiers, etc.) is managed within SAM.gov**, eliminating the need for grant modifications to change this information.
Roles & Authority
There are six foundational roles created to ensure Entity Users have the authority and ability to carry out specific requirements and tasks.

**Entity Administrator**
Confirms information contained in the Entity Profile is current. Manages entity users, including user role assignments in DIAMD, and specific application and award-level assignments in JustGrants.

**Grant Award Administrator**
Submits programmatic-related award requirements, including Performance Reports, certain GAMs, and portions of the Closeout.

**Application Submitter**
Completes and submits applications on behalf of an entity, including Entity Assurances and Certifications.

**Alternate Grant Award Administrator**
Provides support to the Grant Award Administrator. Can initiate, but not submit, programmatic-related award requirements including GAMs.

**Authorized Representative**
Must possess legal authority within an entity to accept awards. This action binds the entity to the award terms and conditions.

**Financial Manager**
Certifies and submits financial information and all Federal Financial Reports on behalf of an entity.

Multiple roles can be assigned to a single user.
Entity Administrator

Key Takeaways

• The Entity Administrator (EA) is the key role within an entity.
• The EA bears responsibility for managing entity information in JustGrants.
• The EA is the gatekeeper and manages the entity users.
• The EA ensures the accuracy of the Entity Profile in JustGrants and makes changes, when necessary, in SAM.gov.
DIAMD

Digital Identity and Access Management Directory
DIAMD: Step 1

To access JustGrants, you must register in DIAMD.

After receipt of your JustGrants Welcome email, you will need to register your account in the system.

1) Select the “here” link in the email to begin the registration process.

**Note:** You will have a period from receipt to complete this process. After that, the Entity Administrator will need to restart the process with a re-invite.
Selecting the link from the email will open your web browser to DIAMD, where you will complete your login information details for the system.

2) Select a “forgot password question” from the dropdown menu.

3) Type your answer into the Answer box.
DIAMD: Steps 4 – 7

4) Optionally, create a question of your own.

5) If you choose your own question, type your question into the Custom question box.

6) Type your answer into the Answer box.

7) When done, select the Create My Account button.
8) Next, you will reset your password by following the directions for password security and creating your password in the Enter new password box.

9) Repeat the new password in the box below.

10) Select the Reset Password button.
Next, you will set up multifactor authentication for your account using either Secure Key or Biometrics, Google Authenticator, SMS (text), Voice Call, or Email Authentication. Here we will focus on SMS first, then Voice.

11) For SMS (text), select the Setup button under the SMS Authentication directions.

**Note:** Users with a biometric key are encouraged to use it for secondary authentication, as shown on page 23.
12) When you select SMS (text), a new selection box will open. Select your country from the dropdown menu.

13) Enter a phone number where you can receive an SMS (text) message in the Phone number box, then select the Send code button.
DIAMD: Steps 14 – 15

14) The system will send an SMS (text) message to the number you have entered. Once you receive it, enter the code in the Enter Code box.

15) Select the Verify button to submit the code for system second-level authentication.
16) The system will return to the multifactor authentication screen and acknowledge completion of **SMS Authentication** with a green check mark.

At this point, you can select the **Finish** button, or you can add an additional optional authentication factor.
17) For Voice Call Authentication, select the **Setup** button under the **Voice Call Authentication** directions.

*This process going forward mirrors the process for SMS (text) steps 12 and 16 and will conclude with an additional green check mark for Voice Call Authentication. Once completed, select the **Finish** button to complete multifactor authentication.*
18) After clicking the **Finish** button, you will arrive at the My Apps screen. Select the **JustGrants** tile to access the system.
DIAMD: Confirmation

Email Confirmation

After completing this process, you should receive an email confirming your enrollment.

The email confirms your enrollment details.
DIAMD

Biometric Security Key Access
DIAMD Biometric Key: Step 1

**Note:** Users with a biometric key are encouraged to use this method for secondary authentication. It is the DOJ preferred method.

You can also use a biometric security key as a secondary authentication method if phone or internet service are not available.

1) Select **Settings** to open the available choices.
2) Select **Setup** to begin the configuration of this method of multifactor authentication.
DIAMD Biometric Key: Step 3

3) Select **Enroll**.

**Enroll to set up your biometric key.**
You have two biometric choices.

4) Select the **USB security key** from the list.
5) Insert your security key and touch the biometric reader window on the key.
The system will pop up a window requesting permission.

6) Click **Allow** to grant your computer system permission to let DIAMD access the security key.
The system will log you out.

7) After you have been logged out, enter your login information again and click the Sign In button.
DIAMD Biometric Key: Step 8

A dialog box will open with a prompt.

8) Insert your security key and touch the biometric window to provide secondary authentication for the system.

You will see the progress of the authentication and then the system will open the DIAMD access page.
User View
When a user views the Landing Page, they will always see the top heading content and left navigation bar. The top heading contains the the logo, bell notifications, the Help icon, and User Logoff.

Currently the help icon is not connected but will continue to be displayed.
When a user views the Home Page, they will see tabs labeled Alerts, which displays system-wide notifications, and My Worklist, which displays the User's current assigned tasks. A “Load More” option may appear at the bottom of the alerts if more notifications exist than what are currently visible.

The alerts are color coded for Information (blue), Notifications (green), and Warnings (orange). The alert designations are managed internally by DOJ.

**NOTE:** User assigned work is found in My Worklist on the Home Page. All entity work will be found under the respective award and applications navigation tabs.
For entity profiles, entity-level information will be displayed on the Entity Profile; all entity users and DOJ users can see this information. SAM will populate Legal Name, Doing Business As Name (if applicable), DUNS, UEI, TIN, Business URL, Year Established, Fiscal Year (end), and SAM registration status (Expiration Date and Last Updated date). SAM data will populate the physical and mailing address, as appropriate. ROID is populated by DOJ once the entity has completed registration with ASAP.

Entity Administrators can change: Law Enforcement, Faith-Based Entity, and Designation of Entity’s Legal Address.

**NOTE:** If the SAM profile is marked as **Not Public**, only a mailing address will populate in the Entity Profile.
All entity users are displayed on this tab once 1) the Entity Administrator has added that user in DIAMD and 2) the user has successfully logged into JustGrants.

Entity users can select **View Details** to see information about each user, including their assigned roles. **Users can update their own User Profile information.**

Entity Administrators also will see the **Manage Users** button on their page.
Entity Administrators can upload documents to this location so that other entity users (and DOJ Users) can view and download those documents for use on specific application, award, and monitoring activities.

The forms located in this section are those that apply to the entity as a whole or relate to multiple applications and awards (e.g., indirect cost agreements, financial capability questionnaires).
Applications Tab

Users will be able to see what applications have been submitted by the entity and the status of each application. The list will consist of all DOJ applications, both active and closed.

All entity users will be able to view all of the entity’s applications; however, keep in mind that only users assigned to specific applications will be able to take actions within those applications.

**NOTE:** User assigned work is found in the Home screen under the Task List. All entity work is found under the Award and Applications navigation tabs.
The Awards tab includes a list of all DOJ awards, both active and closed – older Awards are being migrated into JustGrants. All entity users will be able to view all of the funded awards; however, keep in mind that only users assigned to specific awards will be able to take actions within those awards.

Also, Users assigned to an award can request a Grant Award Modification (GAM) by clicking on the Award Number; this takes the User to the “Funded Award Case”, where they can view all activities associated with a specific funded award.

**NOTE:** All entity work is found under the Award navigation tabs.
All DOJ entity monitoring activities are listed here, as well as the award status and contact information.
On the Federal Forms tab, you will find a list of forms generally used in the administration of federal funds.

**NOTE:** Federal Forms are created, edited, and deleted by DOJ personnel. Entity users can download and populate data in Federal Forms, but cannot add, edit, or delete.
Role
Reassignment
Role Reassignment

Individual user management.

Role assignment and management can be done by the Entity Administrator on an application-by-application and award-by-award basis, enabling Entities to more effectively manage users across an entity in one location.

1) Open the JustGrants Landing Page.
2) Select **Awards** from the navigation bar at the left. You may also select **Application** at this point to access roles. The page is slightly different but the process that follows is the same.
3) Select the checkboxes next to the awards you want to reassign.

4) Select the **Choose Role** dropdown menu to select the role you want to reassign. This filters the user view to show only those with that role available for assignment.

5) Select the **Assign to** dropdown menu to select the user you want to reassign.
Role Reassignment: Reassign

Users can only be assigned to roles assigned in DIAMD.

6) Select **Assign** to complete the action.