OJP User Account Activation

Job Aid Reference Guide

January 2023

Table of Contents

Overview

This guide will provide information to:

- Instruct a OJP user on what to do when receiving a system generated welcome email
- Instruct a OJP user on the steps required to successfully activate their account in order to access an OJP information system
- Navigate the My Apps page in order to authenticate and sign-on to an OJP information system

As an introduction to the information in this guide, some of the terms, processes, and features of DIAMD (Digital Identity and Access Management Directory) will be covered.

IMPORTANT

During the initial activation process, be aware that:

- Upon receipt of a welcome email, the user must activate their account within 3 days. Otherwise, the system will automatically expire the activation link in the welcome email after 3 days per OJP security controls and the user will have to call the Service Desk to get a new activation email sent.

Entity User: The *Basics*

The DIAMD (Digital Identity and Access Management Directory) system acts as the gatekeeper to Office of Justice Programs (OJP), U.S. Department of Justice (DOJ) information systems and provides secure user access and identity management functions.

This document provides instructions on the actions needed to be taken in DIAMD to register, activate, authenticate and access JustGrants, BVP, EEOP, and other OJP information systems integrated with DIAMD that utilize the concept of Entity Management.

Entity is the name used to describe a group or organization. Examples can be state, county, or local government, school district, corporation, or tribe, such as The County of Madison, Apache Tribe of Oklahoma, Pitney Bowes Inc, or Becky Lee Womens Support Fund.

Entity Administrator is the point of contact within an entity that manages member access. Entity administrators initiate invitation emails to members and assigns roles.

Entity Member is an end-user belonging to an entity.

User Roles are permissions granted to users to allow specific access to a system based on their role within an organization. Ex. AlternateGrantAwardSubmitter, FinancialManager, AuthorizedRepresentative.

Entity User: The *Basics*

Welcome Email is a DIAMD system generated email sent to an end user authorized to access an OJP information system. This email contains an activation link that the recipient must click on to begin the user account activation process.

User Account Registration is an end-user self-service online form to be completed by a new OJP user in order to create a new account for accessing an OJP information system. This process only applies to BVP and other OJP systems that do not utilize Entity Management and is not required for JustGrants or EEOP.

User Account Activation is an end-user self-service set of online steps required to activate a user's account created by an Entity Administrator before access to an OJP system can be granted. Used by JustGrants and EEOP users.

User Authentication is the process of identifying users that request access to a system. Access control often determines user identity according to credentials like username and password.

Forgot Password Question/Answer is a knowledge-based secret question and answer pair created during activation by a user that is used to securely change a forgotten password.

Password Reset is an end-user self service used to change a user's forgotten or expired password.

Multi-Factor Authentication is an authentication method that requires an end-user to provide two or more identity verification factors in order to gain access to OJP information systems.

JustGrants User: *Highlights*

Key Takeaways Specific to the JustGrants System

- **Entity Administrator** Creates user accounts, assigns roles and initiates invitation emails to members (end-users) of their organization. By default, the EA role is given access to JustGrants in addition to EEOP.
- **User Roles** Users can have multiple roles at a time in JustGrants Users are assigned roles by their Entity Administrator.
- **Email Address** A user's email address will serve as a unique identifier and be used as their login ID.
- **New Users.** New JustGrants users are invited to the system by their assigned Entity Administrator. For security purposes, new users will have to complete the account activation process.
- **JustGrants Accounts** are created upon authentication into JustGrants. No additional steps are required.
- **Welcome Email** Upon receipt of a welcome email, the user must activate their account within 3 days.
- **Service Desk** Contact JustGrants.Support@usdoj.gov or 833–872–5175, Monday through Friday from 5:00 a.m. to 9:00 p.m. ET; and Saturday, Sunday, and federal holidays from 9:00 a.m. to 5:00 p.m. ET

BVP User: *Highlights*

Key Takeaways Specific to the Bullet Proof Vest Program System

- **Default User Role.** Users can have only one role at a time in BVP. By default, all users are assigned the role name "Role-BVP-Applicant".
- **One Email Address = One User = One Role** A user's email address will serve as a unique identifier and be used as their login ID. Users will need a secondary email/account if they require an additional role in BVP.
- **Existing Users.** Existing BVP user accounts will automatically be registered in DIAMD and in the BVP system. However, for security purposes, existing users will have to complete the account activation process.
- **New Users.** New BVP users are required to self-register their account by clicking on "Register New Account" link on the BVP Login Page. DIAMD will auto provision the user account in the information system. For security purposes, new users will have to complete the account activation process.
- **Welcome Email** Upon receipt of a welcome email, the user must activate their account within 5 days.
- **Service Desk** For BVP support, call: 1-877-758-3787 or email: vests@usdoj.gov

EEOP User: *Highlights*

Key Takeaways Specific to the Equal Employment Opportunity Program

- **Entity Administrator** Assigns roles and initiates invitation email to their entity users. By default, the EA role is given access to EEOP.
- **User Role** Users can have only one role at a time in EEOP and is assigned by the Entity Administrator
- **One Email Address = One User = One Role .** A user's email address will serve as a unique identifier and be used as their login ID. Users will need a secondary email/account if they require an additional role.
- **Welcome Email** Upon receipt of a welcome email, the user must activate their account within 3 days.
- **Service Desk** For EEOP support, call: 202-307-0627 or email: EEOPITSupport@usdoj.gov

DIAMD

Digital Identity and Access Management Directory

User Account Activation Instructions

DIAMD: Step 1 (JustGrants Welcome Email Example)

To access an OJP information system, users must activate their account in DIAMD.

Upon receipt of a welcome email, a user must complete the account activation process.

1) Select the link labeled **"set your password"** in the email to begin the process.

Note: Users have 3 days to complete this process after receiving the invitation email. After the time has elapsed, the service desk to be contacted to restart the process. Your service desk contact information will be contained in the Welcome email (invitation).

User Account Activation

THE UNITED STATES DEPARTMENT of JUSTICE

Test User (diamd.testuser+008@gmail.com),

You are receiving this email because you were invited by Test Name944 to create a user profile in the corresponding Department of Justice (DOJ) System(s). Users must access Department of Justice (DOJ) system(s) through DOJ's secure user management system, the Digital Identity and Access Management Directory (DIAMD).

Take the following two steps within 72 hours of receipt of this email to set up and access your account:

1

1. Set your password
2. Log in to your dashboard

Once you have logged in, you will see your profile associated to the following entity:
Entity Name: Test Name944
Entity Administrator: Test User944 (diamd.testuser+944@gmail.com)

Your Entity Administrator (EA) is the only user role that can invite or re-invite anyone to work on your entity's behalf. Please contact your entity's EA if you need —

- to be re-invited due to a disabled account.
- different user roles.

JustGrants System Resources:

For more information about using JustGrants, visit the Training and Resources site.

If you need technical support with JustGrants:

- COPS Office and OJP applicants and award recipients should contact JustGrants.Support@usdoj.gov or 833–872–5175, Monday through Friday from 5:00 a.m. to 9:00 p.m. ET; and Saturday, Sunday, and federal holidays from 9:00 a.m. to 5:00 p.m. ET.
- OVW applicants and award recipients should contact OVWJustGrantsSupport@usdoj.gov or 866–655–4482.

This is an automatically generated email. Please do not reply to this email.

Department of Justice (DOJ)

If users have both JustGrants & EEOP roles, they'll see ystem resources for both in the welcome email

DIAMD: Step 1 (BVP Welcome Email Example)

To access an OJP information system, users must activate their account in DIAMD.

Upon receipt of an OJP welcome email, a user must complete the account activation process.

1) Select the link labeled **"here"** in the email to begin the process.

Note: Users have 5 days to complete this process after receiving the invitation email. After the time has elapsed, the service desk to be contacted to restart the process. The service desk contact information will be contained in the Welcome email (invitation).

User Account Activation

THE UNITED STATES DEPARTMENT of JUSTICE

Test User,

An account has been created for you to access the following Office of Justice Programs (OJP), U.S Department of Justice (DOJ) system(s):

- Patrick Leahy Bulletproof Vest Partnership (BVP)

1

To access your account please click here and set your password. The activation link will expire in 120 hour(s).

If you need assistance with Patrick Leahy Bulletproof Vest Partnership (BVP), please contact BVP Service Desk at vests@usdoj.gov or toll-free at 1-877-758-3787.

If you are unable to setup a Multi-Factor Authentication (MFA) method using a mobile device, please contact Service Desk using the contact information above.

This is an automatically generated email. Please do not reply to this email.

Department of Justice (DOJ)

BVP Service Desk
Phone: toll-free at 1-877-758-3787
Email: vests@usdoj.gov
Service Desk Hours:
Monday - Friday 8am-8pm EST

Select "here" to begin the user's registration.

DIAMD: Step 1 (EEOP Welcome Email Example)

To access an OJP information system, users must activate their account in DIAMD.

Upon receipt of an OJP welcome email, a user must complete the account activation process.

1) Click the link labeled **"Set your password"** in the email to begin the process.

Note: Users have 3 days to complete this process after receiving the invitation email. After the time has elapsed, the service desk to be contacted to restart the process. Your service desk contact information will be contained in the Welcome email (invitation)

User Account Activation

THE UNITED STATES DEPARTMENT of JUSTICE

Test User (diamd.testuser+928@gmail.com),

You are receiving this email because you were invited by Test Entity678 to create a user profile in the corresponding Department of Justice (DOJ) System(s). Users must access Department of Justice (DOJ) system(s) through DOJ's secure user management system, the Digital Identity and Access Management Directory (DIAMD).

Take the following two steps within 72 hours of receipt of this email to set up and access your account:

1. Set your password
2. Log in to your dashboard

Once you have logged in, you will see your profile associated to the following entity:
Entity Name: Test Entity678
Entity Administrator: Test User678 (diamd.testuser+678@gmail.com)

Your Entity Administrator (EA) is the only user role that can invite or re-invite anyone to work on your entity's behalf. Please contact your entity's EA if you need —

- to be re-invited due to a disabled account.
- different user roles.

Equal Employment Opportunity Program (EEOP) System Resources:

If you need assistance with Equal Employment Opportunity Program (EEOP), please contact EEOP Support at EEOPITSupport@usdoj.gov or 202–307–0627.

This is an automatically generated email. Please do not reply to this email.

Department of Justice (DOJ)

Select "Set your password" to begin the user's registration.

DIAMD: Steps 2 – 4

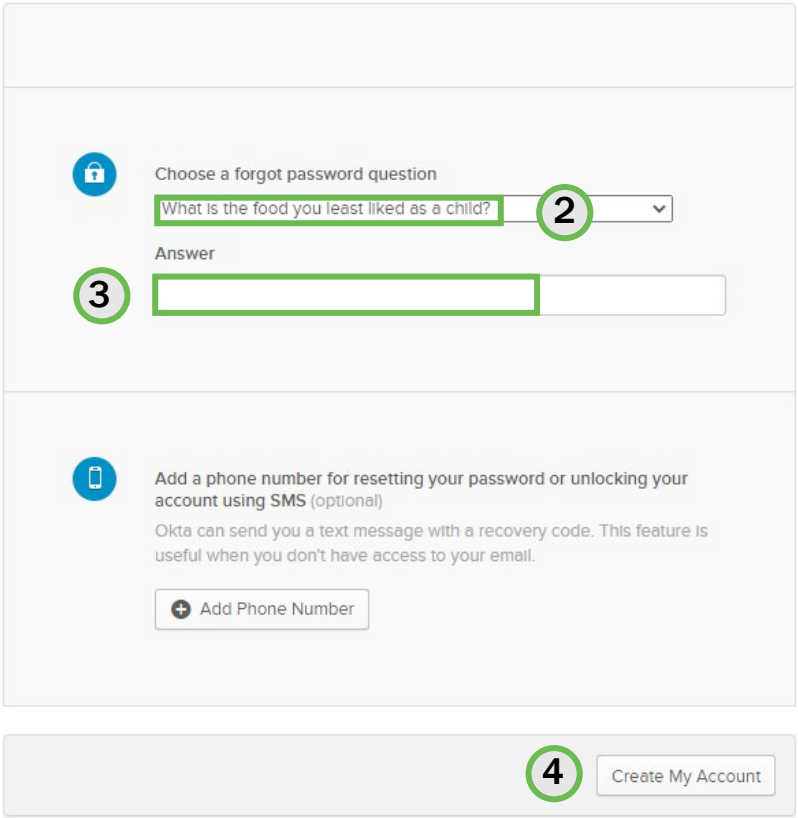
Forgot Password Question

Selecting the link from the email will open the web browser to DIAMD, where the user will provide login information details for the system.

2) Select a "**forgot password question**" from the dropdown menu.

3) Type the answer into the **Answer** box.

4) Click **Create My Account**



Select a question that only the user can answer

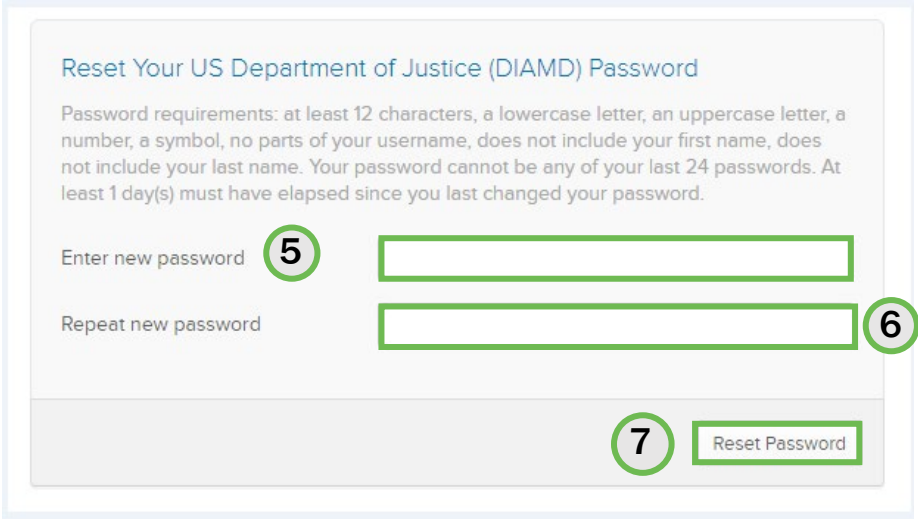
DIAMD: Steps 5 – 7

5) To reset a password, follow the directions for password security and create a password in the **Enter new password** box.

6) Enter the new password again in the **Repeat new password** box below.

7) Select the **Reset Password** button.

Password Reset



The six previously used passwords cannot be reused..

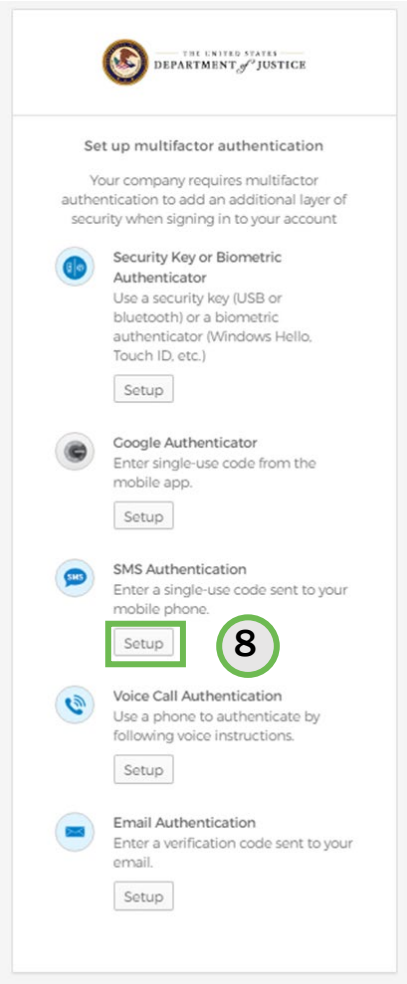
DIAMD: Step 8

Although not required, it is highly recommended that users setup a more secure multifactor authentication method using either Secure Key, Biometrics, or Google Authenticator instead of SMS. However, SMS (text), Voice Call, or Email Authentication are also supported.

8) For SMS (text), select the **Setup** button in the **SMS Authentication** directions.

Note: Although optional, users are encouraged to also setup the Voice Call Authenticator in the event a mobile device is lost or not working.

Multifactor Authentication



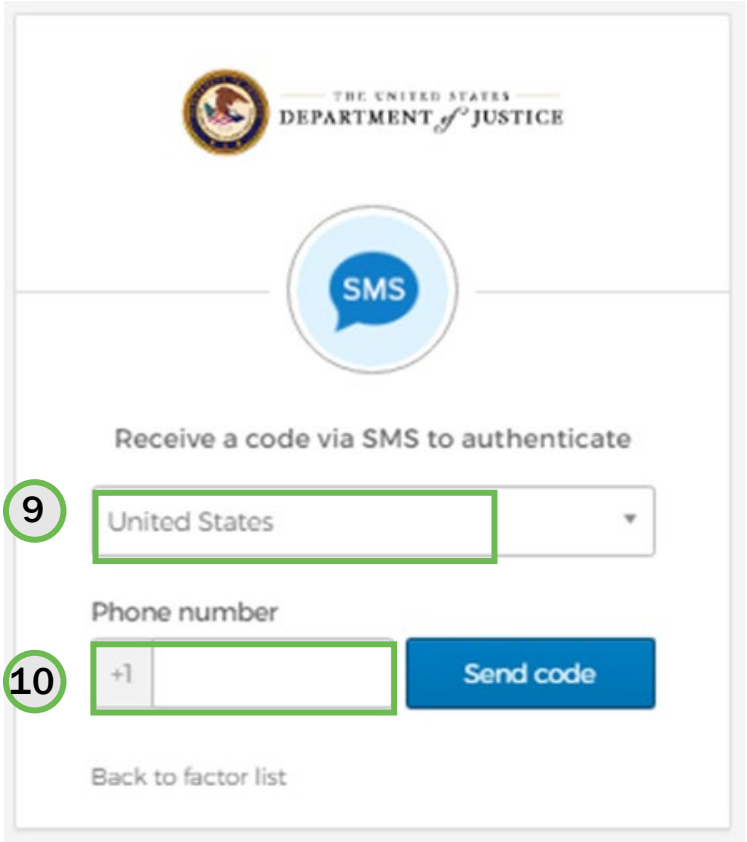
Use either SMS or a standard voice call for authentication.

DIAMD: Steps 9 – 10

SMS (text) Authentication

9) When selecting SMS (text), a new selection box opens. Select the appropriate country from the dropdown menu.

10) Enter the user's mobile phone number in the **Phone number** box, then select the **Send code** button to receive an SMS (text) message.



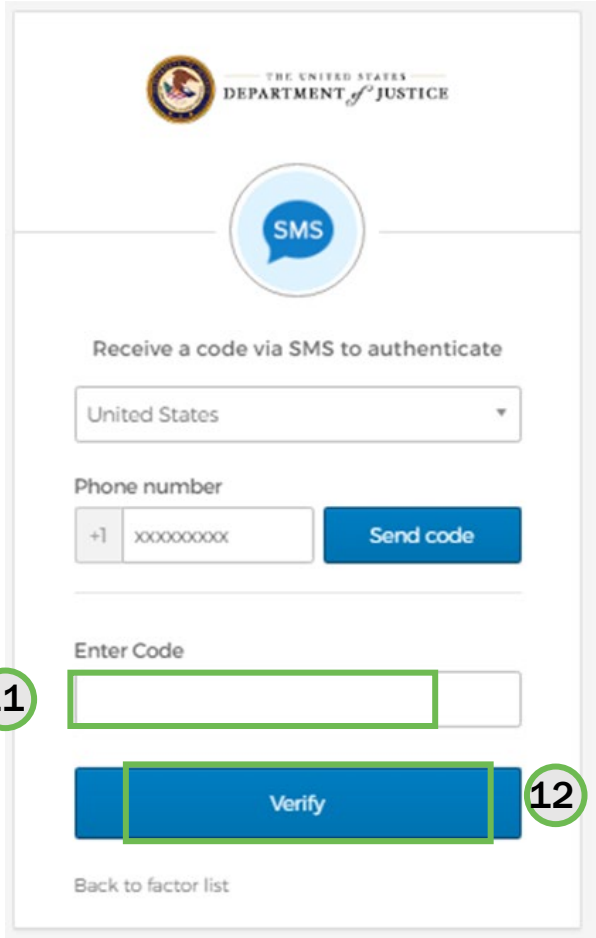
*"**Send code**" sends an SMS (text) with to the user's mobile device.*

DIAMD: Steps 11 – 12

11) The system will send an SMS (text) message to the phone number entered. Once received, enter the code in the **Enter Code** box.

12) Select the **Verify** button to submit the code for second-level authentication.

SMS (text) Verification



Enter the code sent via SMS (text) to the user's phone.

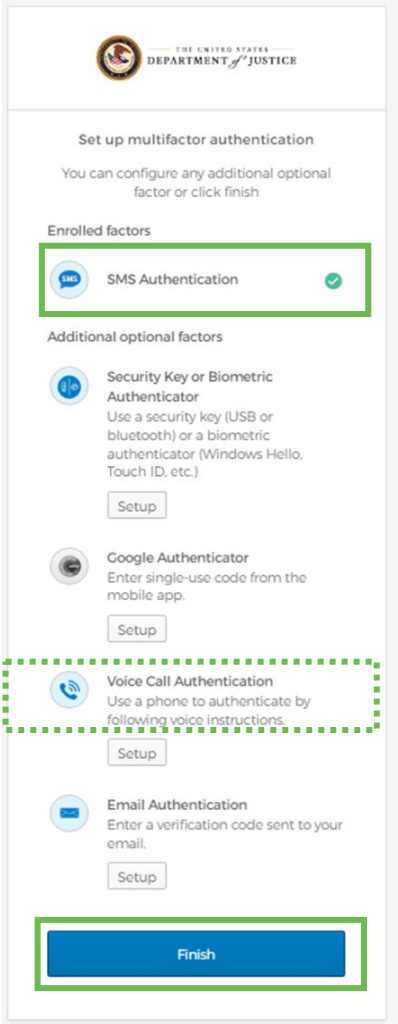
DIAMD: Step 13-14

13) The system will return to the multifactor authentication screen and note **SMS Authentication** completion with a green check mark.

14) Either select the **Finish** button to open the **My Apps** screen or add an additional authentication factor (optional).

Note: The user can setup multiple authentication methods and is not restricted to using only one. It is recommended to setup strong MFA using *Secure Key, Biometrics, or Google Authenticator.*

Additional Authentication



13

14

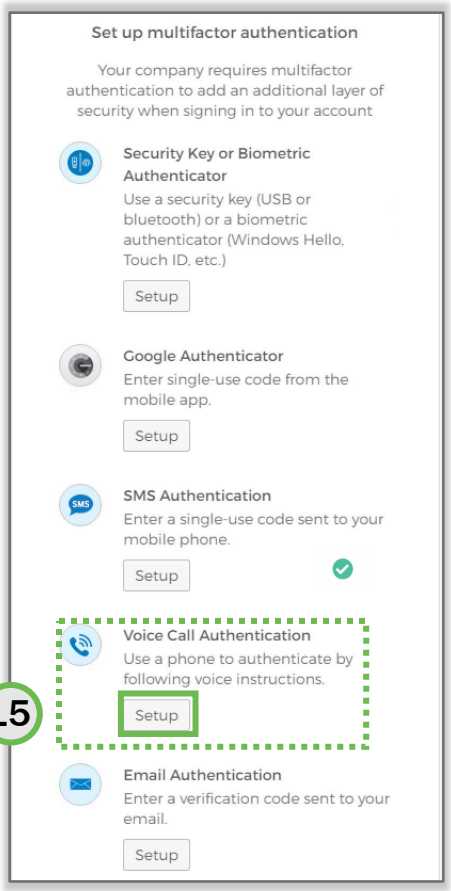
Add additional authentication, if desired. Voice Call is also recommended

DIAMD: Step 15

Voice Call Authentication

15. 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 9 and 10 and concludes with an additional green check mark for Voice Call Authentication. Once completed, select the **Finish** button to complete multifactor authentication.*



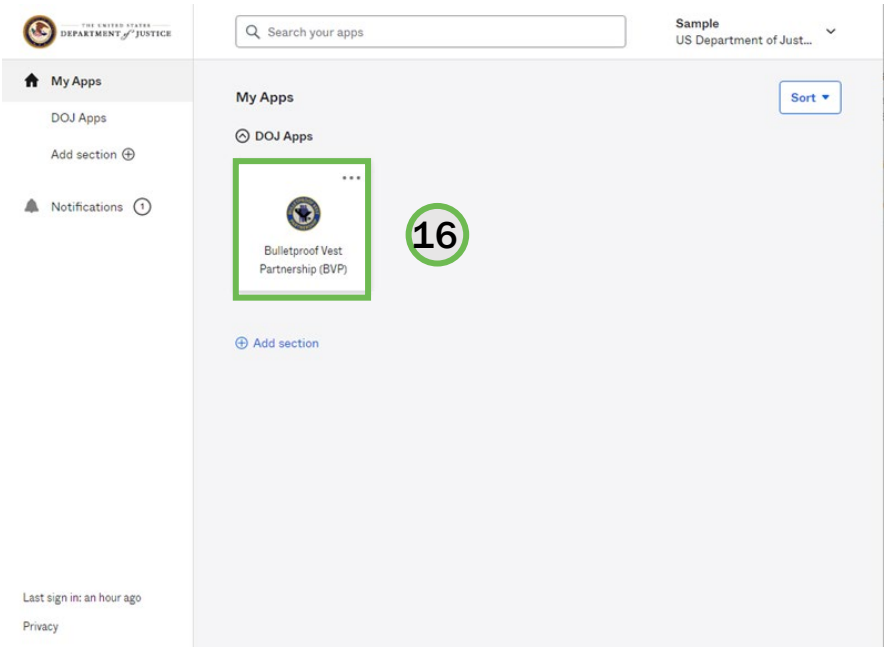
This is an optional process but is recommended.

DIAMD: Step 16

Note: After clicking the Finish button in Step 14, the user will be taken to the DIAMD My Apps page where "application tiles" for all applications the user has access to will be displayed.

16) In this example, the Bullet Proof Vest tile is shown. To access the system, simply click the tile.

My Apps Page



Select the tile corresponding to the OJP system you wish to access.