DISS JVS Creation of Physical Access Control Personnel User

For Determining Eligibility and Access

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

Version 1.1

June 23, 2021

REVISION HISTORY

DATE	VERSION	CHANGE DESCRIPTION	AUTHOR
5/11/2021	1.0	RELEASED ON DCSA TEMPLATE	DCSA
6/23/2021	1.1	MINOR EDITS/CORRECTIONS	DCSA

Creating a Physical Access Control Personnel (PACP) user

OVERVIEW

In the Defense Information System for Security (DISS) Joint Verification System (JVS), users with *Account Manager* and/or *Physical Access Control Personnel* roles can search for subjects to verify eligibility and access. This job aid will instruct Account Managers how to create a Physical Access Control Personnel user.

Creating a Physical Access Control Personnel (PACP) user

To create a user profile with the *Physical Access Control Personnel* role, the administrative user must possess the *Account Manager* role. Displayed in the figure below the administrative user is assigned the Account Manager role and the subject control panel options are customized according to the parameters of that role.

1. Begin by clicking the *Create Subject* link in the subject control panel. A new *Create Subject* tab will be created in the central viewing window for populating the subject's information.

2. All fields marked with an asterisk (*) must be completed to proceed. Click the green *Create Subject* button in the viewing window when done. This step will add a *User Detail* tab to the viewing window as shown on the next page.
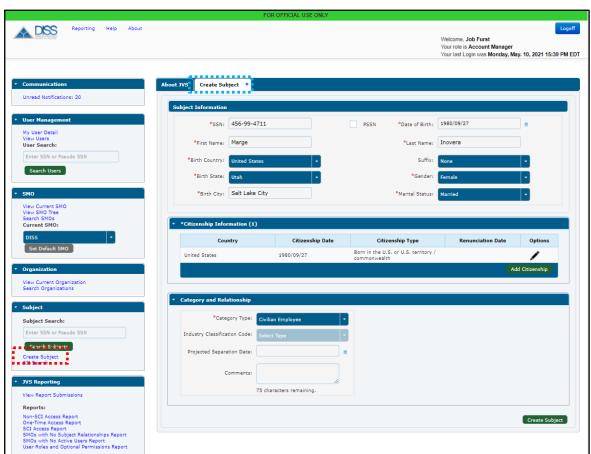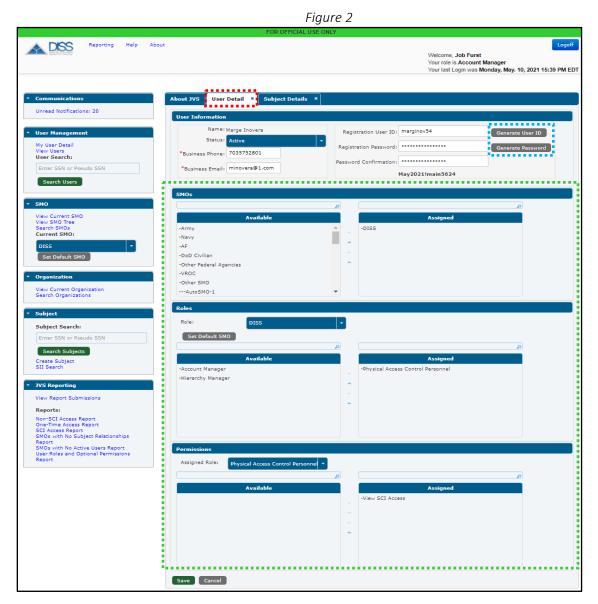
Figure 1

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

Creating a Physical Access Control Personnel (PACP) user (continued)

Continuing the process of creating the subject's profile, the *User Detail* tab is used to assign a Registration User ID and Registration Password, the user's SMO, Roles, and Permissions.

1. Use the *Generate User ID* and *Generate Password* buttons to autofill these fields. Note: the system generated password displays below the Password Confirmation field so it may be shared with the subject. It will be used to authenticate the user prior to PKI token association.

2. In the *SMO, Roles, and Permissions* fields below, select the desired item from the *Available* column and click the plus sign (+) in the middle to move the selection to the *Assigned* column. Double-clicking the selection will also move it to the opposite column.

3. When all selections are made click the green Save button at the bottom of the viewing window.

4. After saving, Account Manager must send the new user the link to the DISS website, the new username, and the system generated password. The Account Manager should advise the user to contact their local IT support if they have any issues (e.g. PKI certificate, SSL certificate) which prevents their connection to the DISS website.

Figure 2