

DISS JVS JOB AID

Joint Verification System (JVS) Tips And Tricks

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY



Agenda



- What is DISS?
- Account Access
- Program Security System Access Request (PSSAR)
- Joint Verification System (JVS) and Reporting User Manual
- User Roles
- Quick Tips
- Viewing Subject Details
- Validation of Records

DISS Components



System of Record for of all DoD employees, military personnel, civilians and DoD contractors in support of:

- Personnel Security
- Suitability
- Credential Management

Secure communications between Adjudicators, Security Officers, and Component Adjudicators.

There are three components of DISS

- Joint Verification System (JVS)
- Consolidated Adjudication Tracking System (CATS)
- Appeals System

Industry uses the Joint Versification System side of DISS



DMDC LINKS

DISS CATS LOGIN

DISS JVS LOGIN

DISS APPEALS LOGIN



<https://www.dcsa.mil/is/diss/>

Account Access



- Information on the account access process is posted in the DISS Account Management Policy and/or Account Request Procedure guides on the DCSA website.
- DISS will require new system access for each user.

<https://psa.dmdc.osd.mil/psawebdocs/docPage.jsp?p=DISS>

Users are required to have a Public Key Infrastructure (PKI) certificate smartcard/token in the form of a Common Access Card (CAC), Personal Identity Verification (PIV) card, or authorized External Certificate Authority (ECA) certificate.

Program Security System Access Request (PSSAR):



Note: Industry no longer required to submit LOA to receive a DISS account. KMP must sign the DISS PSSAR.

- When submitting the DISS PSSAR (account access request) make sure you are using the latest version of the DD FORM 2962 and it must be completed in its entirety. For guidance refer to the **PSSAR FAQs** found on the Personnel Security/Assurance DISS webpage <https://www.dcsa.mil/is/diss/dissresources/>.

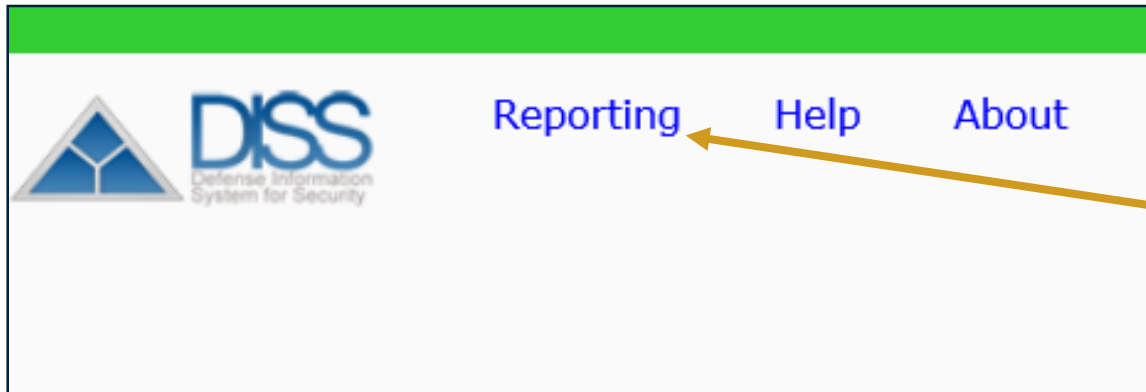
- **Common Rejections**

- PSSAR Part 2, Section 16b: Selecting everything in this section or alternatively selecting nothing at all.
- PSSAR Part 3, Sections 18 and 19: Certificates/training expired (more than one-year old) or dates on certificates do not match dates on PSSAR form.

User Manual



The User Manual for JVS and Reporting is designed for the users in the Security Management Office (SMO) who have access to view and edit personnel security information. The User Manual guides users through all of the functionalities of JVS and Reporting by following the control panels and menu options from the top of the webpage to the bottom.



DISS JVS User Manual is accessible inside DISS. To access the user manual click on Help link located at the top of the home page once you log into JVS.

Quick Tips - JVS

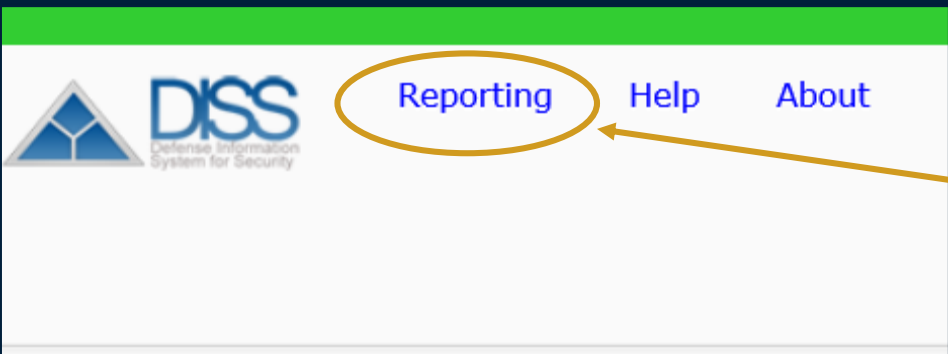


- **Tip 1:** When searching SMOs in DISS the asterisk (*) is not required for a “wild card” search.
- **Tip 2:** The IE browser “Back and Forward” icons do not work within DISS. It will cause an error and require you to log-in again. Use only the tabs and buttons within DISS to navigate.
- **Tip 3:** Inactivity in DISS for more than 10 minutes, DISS will log you out. You will get a warning at 8 minutes.

User Roles



Authorization in JVS is composed of a combination of: user's role(s); optional permissions granted to a user; the SMO the user is currently logged into; and the user's relationship type with the current SMO.

A screenshot of the DISS (Defense Information System for Security) Reporting App interface. The interface has a green header bar. Below it, on the left, is the DISS logo. To the right of the logo are three menu items: "Reporting", "Help", and "About". The "Reporting" item is circled in orange, and a yellow arrow points from the text box on the right to it.

You can run User Roles and Optional Permissions Report using the Reporting App. This report provides a list of the users belonging to the report user's SMO(s) and the roles and optional permissions that have been assigned to those users.

Ensure the correct user roles and permissions have been granted for each user to include, as applicable, your consultants, service providers, and/or subcontractors. As you read through the user manual it will tell you what roles and permission you need to complete those transactions.



Viewing a Subject Record

If the SMO “[details](#)” link is not showing in a Subject record - You will need to establish a category and relationship by clicking the “**Add Category**” radio button and “**Add Relationship**.”

▼ SMO Relationships

▼ Categories (2)

Category ▾	Effective Date ▾	Separation Date ▲	Expand
Industry	2020/09/09		▶
Industry	2020/09/09		▶

Add Category

▼ Relationships (1)

Category ▲	Relationship ▾	SMO ▾	Begin Date ▾	End Date ▾	Options	Expand
Select ▼	Select ▼					
Industry	Owning	DISS-DISS-12	2017/03/28			▶

Add Relationship

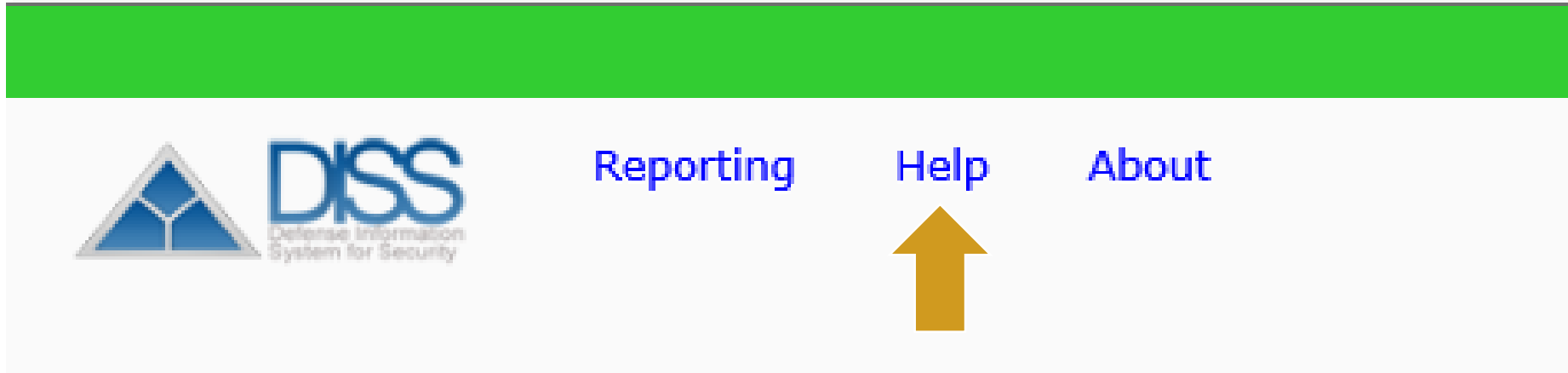
Once the category and relationship is established the Subject Details will appear. Subject Details will expand the record with other tabs relating to the subject.



It is important to validate the accuracy of all your records, particularly while you still have access to JPAS. The following are some of the discrepancies reported.

- Active employees (employees in JPAS PSMnet and Not in DISS)
- Current eligibility that is reflected
- Investigation not matching up to JPAS
- If placed in Continues Evaluation – date is not reflected
- Access (In access in JPAS not in DISS)

Questions



For more information about these DISS actions see the **Joint Verification System (JVS) and Reporting User Manual** which can be accessed in DISS in the upper left corner by clicking on Help or contact the **DISS Customer Call Center (CCC) at 1-800-467-5526**.

Note: If you encounter an issue with a specific record, be prepared to provide a screenshot via encrypted email.