Defense Information System for Security
Joint Verification System

JVS FOR AGENCY
• Brief DISS Overview
• Orientation to Higher Echelon Users Roles and Permissions
• Orientation to End-user functions
• Q&A
Learning Objectives

• Users will be able to describe the general framework of DISS
• Users will be able to identify and navigate the various functions of DISS JVS
• Users will be able to identify and explain the roles and responsibilities of higher level and end users
• Users will be able to define and compare various user relationships and functions within DISS JVS
System of Record for 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 Verification System side of DISS.
What is DISS

• A key component of the DoD’s strategy to modernize personnel vetting and improve mission readiness

• An enterprise-wide system that offers accelerated workflows, electronic adjudications, and secure document exchange

Key features
• Customer Service Requests (CSRs)
• Request for Action (RFA)
JVS Home Page Orientation

- **Communications**
  - Task Inbox
  - Unread Notifications: 12427

- **User Management**
  - My User Detail

- **SMO**
  - View Current SMO
  - View SMO Tree
  - Search SMOs
  - Create SMO Visit
  - View SMO Visits
  - Current SMO:
    - DISS
    - Set Default SMO

- **Organization**
  - View Current Organization
  - Search Organizations

- **Subject**
  - View Subjects
  - Mass Subject Transfer
  - Mass Indication
  - Mass Debrief
  - Create Subject
  - ST Search

---

**About JVS**

**ATTENTION DISS USERS!**

**CT Last Updated on:** May 4, 2021

Please review the DISS 13.4.3 Release Features and related operational notices.

**DISS 13.4.3 Enhancements**

- The following enhancements were included in this release:
  - Manage SMO Actions: Edit Affiliated Organization and Manage Clearance Level
  - Remove Suspend Access Labels from Incident Workflow in JVS

---

**Change Description**

<table>
<thead>
<tr>
<th>Change Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage SMO Actions: Edit Affiliated Organization and Manage Clearance Level</td>
</tr>
<tr>
<td>Remove Suspend Access Labels from Incident Workflow in JVS</td>
</tr>
</tbody>
</table>

**NOTICES**

- **ATTENTION:** Effective 15 MARCH 2021, DISS supports a Fed System of Record for all Eligibility, Access, and Visit data.
- **ATTENTION:** Effective 1 May 2021, DISS will be incorporated into the DISS System of Record. DISS will remove the SSO functionality.
- **ATTENTION:** Effective 1 May 2021, DISS will no longer display the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
- **ATTENTION:** Effective 1 May 2021, DISS will remove the user's information in the Account Manager.
HIGHER ECHELON USERS
Who We Are, What are Our Roles

Hierarchy Manager:
• Head of the Security Management Office (SMO)
• Create SMO Tree
• In addition to all privileges of an Account Manager

Account Manager:
• Manages user provisioning within organization
• Performs tasks such as creating and maintaining user profiles, roles, and permissions
• May work in subordinate “child” SMOs
View the SMO Tree

Too many children for SMO tree view. Use SMO search instead.

Note that if part of a very large tree, users will get a warning banner instead of a Tree Display.

Diagram showing parent-child relationship in the SMO Tree.
Create SMOs

The process model at the top of the page walks users through the process and indicates progress with the highlighted arrow.
Move SMOs (Hierarchy Change Request)

• If there are SMOs not within your hierarchy and you are not provisioned for the SMO, you will need to submit a Hierarchy Change Request (HCR).

• Send the HCR to dcsa.dcsa-northern.dcsa-dvd.mbx.diss-provisioning@mail.mil.
Create User—Program Security System Access Request (PSSAR)

- Use the DCSA DD FORM 2962 and complete in its entirety (not P&R form)
- Industry sends PSSAR to dcsa.dcsa-northern.dcsa-dvd.mbx.diss-provisioning@mail.mil

Note: PSSAR FAQs are at https://www.dcsa.mil/is/diss/dissresources/
Use the PSSAR information to set up the user’s SMO & roles note that optional roles are available.
USER FUNCTIONS
User Roles and Permissions

User Roles
- Security Managers
- Security Officers
- Security Officer Administrator
- Security Officer Visit Administrator

User Permissions
- Subject Management
- NDA Submission Process
- Access Management
- Visit Requests
SUBJECT MANAGEMENT
Search Subject

User enters either an SSN or PSSN in the search box and Clicks “Search Subjects”
Note: You can not view your own record. You will get an error message.
Subject Management actions will primarily be achieved working at the Tabs on the Subject Detail Screen.
Subject Details—Example SMO Relationships

If no SMO details...
Add a category...
And a relationship
NDA SUBMISSION PROCESS
Subject Details—Accesses > Add NDA

Select the green Add NDA/NDS link
Add NDA/NDS—Upload Document

Enter Date and Doc name

Select type from pulldown

Note: the “+Document” uploads the document to the queue, “Add Document” uploads that document to JVS.
### NDA/NDS History

#### Approved

<table>
<thead>
<tr>
<th>NDA/NDS</th>
<th>Signed Date</th>
<th>Effective Date</th>
<th>Show Document</th>
</tr>
</thead>
<tbody>
<tr>
<td>NDA</td>
<td>2021/05/24</td>
<td>2021/06/02</td>
<td>View Document</td>
</tr>
</tbody>
</table>

When submitted, JVS automatically sends an NDA/NDS Review task to CATS.

#### Pending

<table>
<thead>
<tr>
<th>NDA/NDS</th>
<th>Signed Date</th>
<th>Effective Date</th>
<th>Show Document</th>
</tr>
</thead>
<tbody>
<tr>
<td>NDA</td>
<td>2020/09/10</td>
<td>2020/09/11</td>
<td>Pending Approval from CATS</td>
</tr>
</tbody>
</table>

When submitted, JVS automatically sends an NDA/NDS Review task to CATS.
Rejected NDA

If rejected, a message will appear in the Task Inbox.

When rejected, the Security Officer has a task to revise the NDA before resubmitting.
ACCESS MANAGEMENT
Granting Access
When expanded the Associated Relationships show to include Type, SMO Name, Begin Date, Industry Classification Code (ICC), End Date and Termination Reason.
VISIT REQUESTS
Create SMO Visit

A New Visit Process model appears on the work bench.
Find & Select SMO

Enter data into one of the data fields, such as SMO Name.

Search based on the criteria entered.

If the search is too broad, it will generate an error banner.
Select SMO

Search results are listed at the bottom of the page.

Highlight the desired SMO and click next.
Visit Information

Fill in all pertinent information; at a minimum, all boxes with an *

Pull downs provide a menu for Reason and Access level
Visit Confirmation

Upon completion of the Visit information, a Confirmation page will appear: completing the process.
Clicking on a visit in the list will open visit details for that visit.
Visit Details allows users to manage the SMO visits via the Visit Actions pull down.

Users can edit, cancel, and change visit information here.
TAKE-AWAYS
Quick Tips

• When searching SMOs in DISS the asterisk (*) is not required for a “wild card” search

• DISS application works best with the following web browsers: Edge, Version 11 or above, Mozilla Firefox, or Chrome. Inactivity in DISS for more than 10 minutes will cause log out; a warning is posted at 8 minutes

• If you haven’t been provisioned for the right SMO(s), and cannot see your hierarchy, you’ll need to contact DCSA at dcsa.dcsa-northern.dcsa-dvd.mbx.diss-provisioning@mail.mil to request changes to your provisioned account

• If your hierarchy is inaccurate (missing SMOs, incorrect parent to child relationships, etc.) you will need to complete a Hierarchy Change Request (HCR) form

• Failure to login within 30 days will lock your account; 45 days the account will be deactivated
## Support Contacts

### Knowledge Center Inquiries

<table>
<thead>
<tr>
<th>Other DCSA Offices</th>
<th>DoD CAF Call Center</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DCSA Policy</strong></td>
<td><strong>Phone</strong> 301-833-3850* (SSOs and FSOs ONLY)</td>
</tr>
<tr>
<td></td>
<td><strong>Menu Options</strong> 5 -Industry</td>
</tr>
<tr>
<td><strong>DCSA Facebook</strong></td>
<td><strong>Email</strong> <a href="mailto:dcsa.meade.dcsa-dvd.mbx.dodcaf-callcenter@mail.mil">dcsa.meade.dcsa-dvd.mbx.dodcaf-callcenter@mail.mil</a></td>
</tr>
<tr>
<td></td>
<td>*Temporarily suspended due to COVID-19</td>
</tr>
<tr>
<td><strong>DCSA Twitter</strong></td>
<td><strong>DOHA</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Phone</strong> 866-231-3153</td>
</tr>
<tr>
<td><strong>DCSA’s System Liaison</strong></td>
<td><strong>Website</strong> <a href="mailto:dohastatus@ssdgc.osd.mil">dohastatus@ssdgc.osd.mil</a></td>
</tr>
<tr>
<td><strong>For Technical Issues with e-QIP</strong></td>
<td><strong>Updated as of January 2021</strong></td>
</tr>
<tr>
<td><strong>For Agent’s/ Investigator’s Identity or Status</strong></td>
<td></td>
</tr>
</tbody>
</table>