The Defense Information System for Security (DISS) Overview

NISPPAC DISS Working Group

Last Updated
07/19/2021

DISS

All slides are subject to change in a couple a weeks with system changes!

Next Release 13.4.5 projected for 27 July

DISS Roles/Permissions

JVS

Hierarchical Roles

Hierarchy Managers – Responsible for the SMO management throughout their Branch (creating child SMOs, editing and deactivating SOS) as well as Account Management to provision additional users.

Account Managers – Manages the users within their hierarchy by creating and maintaining user profiles, roles and permissions.

Security Managers – Functions as the manager for all subject actions within their Branch.

Non-Hierarchical Roles

Security Officer Standard – Responsible for the subject management of all personnel within their SMO. (2,4)

Security Officer Administrator – Less inherent privileges than the Security Officer Standard with most capabilities only through optional permissions. (3,5,6)

Component Adjudicator – Responsible for receiving the investigation for Suitability/HSPD-12 and making the determination if the DoD CAF is unable.

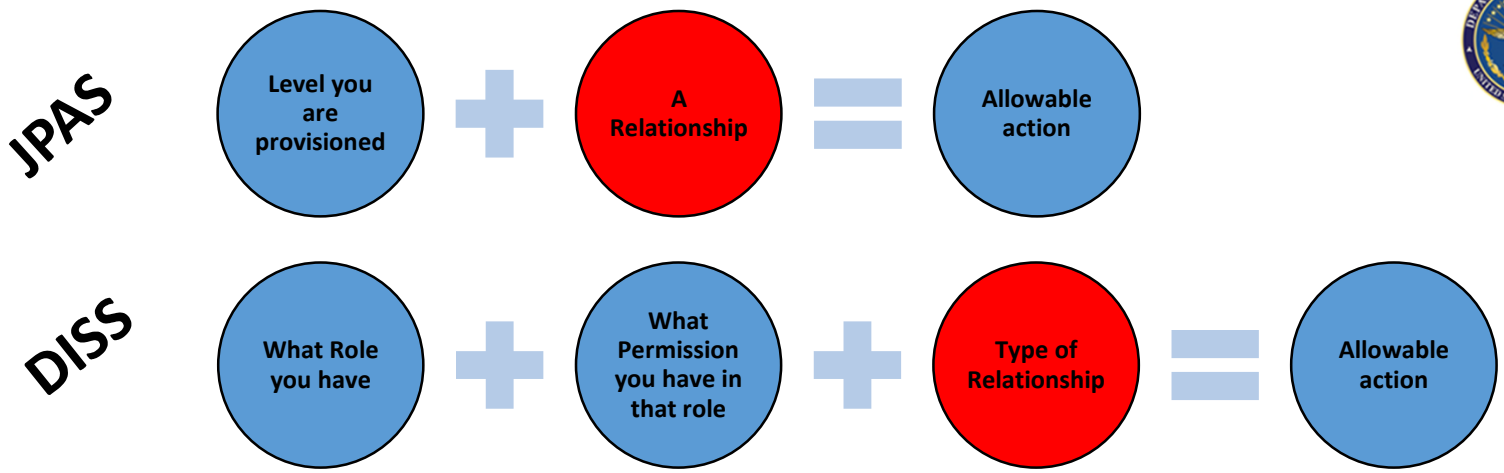
HR – Read only access to HSPD-12 and Suitability determinations. Can only receive communications from the DoD CAF.

Security Officer Visit Support – Inherent permissions relate to visit request functionality. Optional permissions can be granted to assist a Security Officer. (10)

Physical Access Control Personnel – Responsible for ensuring visitors have the proper access and need for entry. (7,8)

Note: There are some cases when you should not select "Deactivate" when removing User Accounts. If it is clicked and you hit save, then it will remove all accounts assigned to the User.

System Permissions



The key issue is around relationships:

- In JPAS, it didn't matter what type of relationship you had as long you had a relationship with the subject you needed to manage.
- In DISS, the type of relationship is one of the most important features of the system because it governs what your role can do to a record.

DISS User Matrix

- The user matrix allows you to see the Roles within DISS, along with the permissions for each role.
- The “Security Officer” role manages subjects associated with a SMO, in addition to corresponding with CATS and other SMOs on tasks. Users with this role can update subject information, create accesses, visits, and incidents, and establish and remove owning/servicing relationships with subjects.
- The “Security Manager” role provides the most functionality. Users with this role are most likely responsible for the subject management of all personnel within their SMO tree.
- *Note – “X” Mandatory Permission
  “O” Optional Permission

Permissions	Security Officer	Component Adjudicator	Human Resource Manager	Security Officer Admin	Security Manager	AccountManager	Hierarchy Manager
Access SMO Record	X	X	X	X	X	X	X
Add Adjudication History	O	O			O		
Add Investigation History	O	O			O		
Adjudicate Interim HSPD-12/Suitability		O					
Create Incidents	X			X	X		
Create SMO							X
Create Subject Information	X				X	X	X
Create User						X	X
Create Visit	X			O	X		
Deactivate SMO							X
Establish Subject Relationship	X	X		O	X		
Field Adjudication		X					
Grant Non-SCI Access	X			O	X		
Create CSR	X	X		X	X		
Initiate Investigation Request	X				X		
Maintain SMO						X	X
Manage DISS User						X	X
Manage Foreign Relationships	X			O	X		
Manage Foreign Travel	X			O	X		
Manage Organizations							X
Manage Periodic Reinvestigations	X	X		X	X		
Manage Polygraph	O			O	O		
Manage Reports						X	X
Manage SCI Access	O			O	O		
Manage SCI DISS User						O	O
Manage Tasks	X	X		O			
Modify Visit	X			O	X		
Remove Non-SCI Access	X			O	X		
Remove Subject Relationship	X	X		O	X		
Review Investigation Request	O	X			O		
Suspend Access	X			O	X		
Update Subject Information	X	X		O	X		
Update Subject PII							
View Non-SCI Access	X			X	X		
View SCI Access	O			O	O	O	O
View SMO Notifications	X	X	X	O	X	X	X
View Subject Information	X	X	X	X	X	X	X
View Subject List	X	X	X	X	X		
View User Notifications	X		X	X	X	X	X
View Visit	X			O	X		

Check out the Matrix here in the Account Management Policy

Hierarchy Management

Last Updated
07/19/2021

Hierarchy Management

- When data migration occurred, JPAS Levels were transferred to different SMOs in DISS. This means that if a user was provisioned for Levels 2, 4 and 5 for SMO 12AB3 in JPAS, there are now three SMOs in DISS, one for each level (12AB32, 12AB34 and 12AB35).

- In order to accurately assess the Hierarchy needs, users should understand the scope of their hierarchy by searching for all SMOs associated with their CAGE Code.

- All SMOs should be managed by the highest Parent with at least one Hierarchy Manager.

- It is important that all CAGE Codes within the hierarchy tree can be accessed and managed by a Security Manager/Officer. This can be done through provisioning for each SMO or by configuring the hierarchy to account for all SMOs, and provisioning for Security Manager at the highest Parent level.

Check your SMO's

- If you are responsible for more than one SMO, you will want to make sure they are all in your tree.

  https://classmgmt.com/nisppac/CheckYourSMOs.pdf

What do I do if:

- They are in the wrong order?
  - You can use the move SMO feature and adjust within your tree
- SMOs are missing?
  - If you have SMOs that are not yours, then you can use the "move SMO" to move it out and back to PSMO
  - If you are not able to remove the SMO due to not having a User account, you will need to submit a Hierarchy Change request

Hierarchy Change Request

Last Updated
07/19/2021

Hierarchy Change Request

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

- Send the HCR to dcsa.dcsa-northern.dcsa-dvd.mbx.diss-provisioning@mail.mil
  - All identified SMOs will be moved to the ONE Parent.
  - The Hierarchy Manager will be able to configure their Hierarchy under the identified Parent SMO.

When filling out the HCR, it's important to use the exact SMO Name as presented in DISS. This will assist DISS analysts with ensuring they have the proper information to complete the move.

How Communication Works In DISS

Last Updated
07/19/2021

How Communication Works In DISS

- You will receive notifications in DISS two ways:
  1. As a CSR
  2. Task Inbox

- CSR notifications will:
  - Display system-generated notifications about the user's subjects, such as the subjects' access status, relationship status, or the user's SMO, such as the creation, deactivation, or movement (when outside of the hierarchy) of a SMO.
- Task Inbox notifications will:
  - Display existing Customer Service Requests (CSR) and Requests for Action (RFA) for the user's current SMO. JVS users create CSRs to send to adjudicators in CATS, and they receive RFAs from adjudicators in CATS.

- *Note: You will not receive notifications about a Task sent to your Task Inbox. You should check these notifications periodically through the day.*

Editing a Subject Record

Last Updated
07/19/2021

Editing Subjects Record

- Under Subject Details, select the “Basic Info.” tab and scroll to the bottom of the page to find the Subject Personal Information
- Click on the green “Edit Subject Information” button
- Another window will open the “Update Subject” screen
- You will be able to add the middle name and other select information on subject
- If other information needs to be updated, such as citizenship or last name, a CSR should be submitted along with supporting documentation to facilitate the change
- Under Subject Details, select the “Contact Info” tab. Please add the email address for the subject. Going forward, on initial investigations, an email will be sent to the subject with the registration code. The DISS User/Initiator will also receive a notification with the registration code under “Unread Notifications.”

Creating Categories and Relationships

Last Updated
07/19/2021

Owning and Servicing

You really need to explore who is doing what actions in DISS, as roles only play one part. You will have to account for relationships too:

Owning

- Build the record
- Initiate Investigation
- View Investigation Detail
- Grant Access to include special categories
- Eligibility Notification
- Task inbox (CAF Messages)

Servicing

- **Service an existing access**
- Add FN Contact – with correct role
- Add FN Travel – with correct role
- View Subject details
- Visits request
- Adverse (Only submitting SMO can see)

The owner “owns” the person and the servicing SMO is only “servicing” the access owned by the owner

Creating Categories and Relationships

Things to know:

- In the current version of DISS, only one Industry category can be present in a subject record
- Category Organization information is not required in the current version of DISS
- When creating an owning relationship, access will need to be added separately
- When creating a servicing relationship, access should be added based on the owner's previously granted access
  - If the owning SMO has not granted access, you will not be able to complete the action to add a servicing relationship with existing access
- *When working with an IC agency who has an owning relationship with the industry subject, you may need to take a servicing relationship with the accesses granted by the agency*

Investigation Requests In DISS

Last Updated
07/19/2021

Investigation Requests In DISS

- You should receive one of these four notifications:
  1) Notification w/ instructions that include POB and Registration Code.
     - ✓ *Previously, the registration code was not being generated but this is now fixed.*
  2) Notification to use previous log-in information: *Investigation Request Initiated Successfully. Please request the subject to register into e-QIP with their prior established credentials.*
  3) AUB error – Failed to set AUB. Go back to the request and use the pencil button to find the error and update the request information.
  4) PII Mis-match
     - ➢ **You will need to call the DISS Applicant Knowledge Center 724-738-5090** for PII mis-match if no notification has been received in two business days.

Investigation Requests In DISS

- There have been a number of issues related to the information flow between DISS and eQIP.
- Make sure the email address is listed in the subject details under the Subject POC tab
- When an investigation has been successfully initiated, you will see a status of “Initiated” along with an eQIP ID # and a countdown clock – the countdown clock can be found by clicking the blue expand button.
- You will not be able to stop the investigation request until the subject returns it for review
  - The request will also expire after 30 days if the subject does not log in to eQIP
- Trusted workforce 2.0 initiative - If you have received a list or message (like thepne below) from VROC requesting a SF86, please work these records first before others in your subject listing.

Message:

The Jan 2021 Executive Correspondence (EC) was issued by the Security Executive Agent (ODNI) and the Suitability & Credentialing Executive Agent (OPM). The EC provides critical guidance to agencies on how to begin implementing mandatory personnel vetting reforms under the Trusted Workforce (TW) 2.0 initiative. Defense Information Security System (DISS) records indicated that the Subjects under your facility listed in the Excel spreadsheet attachment require a current eQIP to facilitate enrollment into Continuous Evaluation Vetting in compliance with TW 2.0.

If eligibility is still required please transmit an SF-86, electronic Questionnaire for Investigations Processing e-QIP, to the Defense Counterintelligence and Security Agency (DCSA) via DISS within 30 days.

If a periodic reinvestigation for a listed subject has been submitted in DISS, please disregard this message. If the subject has been recently enrolled in DoD CE; or has an open investigation, please disregard this message. If the subject no longer requires access to classified information, please update your SMO within DISS

Eligibility in DISS

Last Updated
07/19/2021

Eligibility in DISS

- List of Eligibilities that will show in DISS

DISS Eligibility	DISS Eligibility Determination	New Eligibility in DISS
None	None	None (Uncleared)
Confidential	Favorable	Confidential
Secret	Interim	Interim Secret
Secret	Favorable	Secret
Top Secret	Interim	Interim Top Secret
Top Secret	Favorable	Top Secret
SCI - ICD704	Favorable	TS/SCI
SCI - ICD704	Interim	Interim SCI
None	Administratively Withdrawn	Administratively Withdrawn
None	Denied	Denied
None	Loss Of Jurisdiction	Loss Of Jurisdiction
None	No Determination Made	No Determination Made
None	Revoked	Revoked

SCI In DISS

Last Updated
07/19/2021

SCI In DISS

- In order to grant Manage SCI Access or View SCI Access permissions, the Account Manager, Hierarchy Manager, must have the “Manage SCI DISS User permission”!!
- Must have Top Secret eligibility to have SCI Permissions
- Manage SCI allows a person to indoc to the SCI level ***(Verify with the customer that you have indoc authority.)***

Note – Verification should be in writing from the customer!!

- View SCI allows a person to see the SCI compartments
- When sending SCI visits, only one access can be added to the visit (additional SCI compartments can be added to the comments)
- Each IC customer will have different processes for adding SCI access in DISS (Contact your IC customer for additional guidance)

SCI In DISS cont.

- DISS does not have a drop-down menu for SCI accesses, and:
  - Each access must be added to the system as an individual relationship
  - *Example – If you have SI/TK the record will have an owning relationship for SI and an owning relationship TK*
- For this reason, it is possible that an IC agency will take an owning relationship with a subject to grant SCI accesses
  - The Industry owning SMO can take a servicing relationship with the accesses granted by the IC agency

Debriefing/Separating Access in DISS

Last Updated
07/19/2021

Debriefing Access in DISS

- There are two ways a subject can be debriefed:
  - Use the Access tab in the Subject Details to debrief the subject from access but leave the relationships intact
  - Separate the relationships, which will automatically debrief the subject
    - NOTE: This will also remove any servicing relationships and cancel any active visits for the subject under the separating SMO.

Submitting a Customer Service Request (CSR) in DISS

Last Updated
07/19/2021

Submitting a CSR in DISS

- Provide detailed information and supporting documentation
- Preconditions may exist
  - If a CSR option is not displayed, it means the CSR did not meet the preconditions and is not authorized for use on this record.
- Indoc assist CSRs – How does that work?
- https://classmgmt.com/nisppac/how_to_submit_a_CSR_in_DISS_v1.pdf

Types of CSRs available in DISS

- ✓ Provide Supplemental Information
- ✓ Request Reciprocity
- ✓ Request SCI Sponsorship
- ✓ Upgrade eligibility
- ✓ Interim Eligibility
- ✓ Interim SCI Eligibility
- ✓ Expedite Process Request
- ✓ Request Adjudication Reconsideration
- ✓ Recertify

Which CSR to Submit – and When

1 Submit a CSR in DISS

	Action to be taken
☐ Change in Marital Status/Cohabitation ("Scheduled" investigation only)	Submit CSR: Provide Supplemental Information
☐ Change in Marital Status/Cohabitation with Foreign National	Submit CSR: Provide Supplemental Information
☐ SSN Change	Submit CSR: Provide Supplemental Information
☐ Cancel "Scheduled" Investigation (Subject No Longer Requires Access)	Submit CSR: Provide Supplemental Information
☐ No Determination Made with Previous Valid Eligibility	Submit CSR: Recertify
☐ Reciprocity	Submit CSR: Request Reciprocity
☐ Request Adjudication on Closed Investigation (provided the closed investigation is over 30 days)	Submit CSR: Provide Supplemental Information (if DISS does not indicate Adjudication in progress)
☐ LOJ with Previous Valid Eligibility	Submit CSR: Recertify
☐ Request Adjudication on Closed Investigation (needs to move to a another DoD component for adj)	Submit CSR: Provide Supplemental Information
☐ Reopen "Discontinued" Investigation	Submit CSR: Provide Supplemental Information
☐ Upgrade/Downgrade Investigation	Submit CSR: Provide Supplemental Information
☐ DCSA requests a PR to be submitted but a PR is not required	Respond to RFA request from VROC

2 Contact the JPAS/DMDC Contact Center

	Action to be taken
☐ PII Change (No Longer has DOD/Military associations)	Follow JPAS Data Correction Checklist
☐ Change of Employment	Losing facility needs to separate in JPAS/DISS; gaining facility establishes relationship/indoctrinates in JPAS
☐ Cancel "Scheduled" Investigation (Employment Termination)	Losing facility needs to separate in JPAS/DISS
☐ Erroneous DOD/Military category	Follow JPAS Data Correction Checklist

3 Contact the Knowledge Center

	Action to be taken
☐ Status of investigation/adjudication (outside standard timeframes)	Contact VROC Knowledge Center at (888) 282-7682, Option #2 Email: dcsa.ncr.dcsa-dvd.mbx.askvroc@mail.mil

Visit Requests in DISS

Last Updated
07/19/2021

Visit Requests in DISS

- **Visits are still a work in progress**

- **On or near May 31, 2021, JPAS legacy visits were migrated into DISS**
  - JPAS legacy visits will be in created status only
  - This means that they cannot be archived without first making them active
  - If they are made active, the hosting SMO will receive the visit and all information associated with it. This could cause confusion if you have already duplicated visits in DISS.
- **It is important that the hosting SMO does not archive a visit before it has ended. Once archived, the visit becomes inactive and can no longer be edited by the creating SMO.**
  - Submit change request to help address the archive issues
  - Submit change request to help with all the notifications
  - Submit change request to help with sending SCI visit request

Foreign Travel and Foreign Contacts

Last Updated
07/19/2021

Foreign Travel and Foreign Contacts

- **On August 24, 2021 (6 months following the issuance of the 32 CFR part 117 "NISPOM Rule," Industry will be required to report foreign travel and foreign contacts for all cleared subjects**.
  - The draft ISL indicates that reporting will occur in DISS
- **An ISL will be released soon with the details of this requirement. SEAD 3 can be referenced for details prior to the release of the ISL.**

DISS Reports

Last Updated
07/19/2021

DISS Reports

- Many of the reports available in DISS have data or delay issues.
- The Periodic Reinvestigation report pulls information based on policy and not current DCSA specific timelines for when to submit a PR.
  - There may also be missing subjects due to current data discrepancies in the system.
- There is a known delay between the live information in DISS and what is contained on a report. The delay can be anywhere from 4-24 hours.

DISS Reports

- VROC reports provide oversight for industry users and minimize security vulnerabilities by ensuring all rules are followed.

***Note: VROC reports are accessible only to the following users:** VROC Security Managers, Application Admin, and Help Desk users. Each user views only the information for their part of the organizational hierarchy.*

- Types of VROC reports :
  - **Aging Interim:** The Aging Interim Report displays the industry subjects with interim eligibilities of Confidential, Secret, Top Secret, and SCI lasting nine months or longer.
  - **CSR:** The CSR Report displays all open CSRs submitted from industry SMOs, except the SCI Sponsorship CSR.
  - **Submitted Incident Report for Industry:** The Submitted Incident Report for Industry displays industry subjects with open incidents or incidents opened or closed within the last seven days.
  - **KMP:** The KMP Report displays all active industry KMPs. Industry KMPs are considered active if they have an Industry category not yet separated or do not have a Separation Date later than the date the report is generated.
  - **Overdue Periodic Reinvestigation:** The Overdue Periodic Reinvestigation Report displays industry subjects that are 90 days overdue for periodic review.

Who are “We”

- Aprille Abbott – NISPPAC Lead – (Mitre)
- Jeremy Wendell – Team Lead (Northrop Grumman)
- Rebecca Devore – (LMCO)
- Jane Dinkel – (LMCO)
- Tanya Elliott – (Analyst Warehouse)
- Sheila Garland – (Raytheon Technologies)
- Diane Griffin – (Security First & Associates)
- Daniel Grimes – (BAE Systems)
- Rene Haley – (Industrial Security Integrators)
- Brent Hall – (Boeing)
- Joe Jessop – (PSMNET)
- Jen Kirby – (Deloitte)
- SeKitha Nunn – (Raytheon Technologies)
- Rhonda Peyton – (Lovelace Biomedical)
- Quinton Wilkes – (L3Harris)
- Debbie Young - (GTRI)

Email the NISPPAC DISS working group your questions at NISPPACindustry@gmail.com

Help/Reference Links

- NISPPAC DISS working group DISS guides: https://classmgmt.com/nisppac.php - Resources Tab
- DISS Resource Page: https://www.dcsa.mil/is/diss/dissresources/
- For DISS Frequently Asked Questions (FAQs): https://www.dcsa.mil/is/diss/dissfaqs/
- For the most up to date provisioning instructions, and additional guidance/tips for when you log in, please visit the DCSA website at www.dcsa.mil


DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY


DEPARTMENT OF ENERGY
UNITED STATES OF AMERICA


ISOO
INFORMATION SECURITY
OVERSIGHT OFFICE


OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
UNITED STATES OF AMERICA

Questions?


DEPARTMENT OF DEFENSE
UNITED STATES OF AMERICA


U.S. DEPARTMENT OF
HOMELAND SECURITY