Defense Manpower Data Center

Personnel Security & Assurance

Defense Information System for Security (DISS) Frequently Asked Questions (FAQs)

Document Version 1.3
28 March 2017

Document History

Version	Date	Author	Comment / Change
1.1	11/21/2016	PMO	Initial Draft
1.2	12/01/2016	PMO	Updated FAQs Section 2: Application FAQs
1.3	03/28/2017	PMO	Updated FAQs Section 1: General Information

Table of Contents

Section 1: General Information

1. What is the Defense Information System for Security?

- DISS serves as the system of record for personnel security, suitability and credential management of all DOD employees, military personnel, civilians and DOD contractors. DISS also provides secure communications between Adjudicators, Security Officers and Component Adjudicators in support of eligibility and access management.

2. What are the Public Key Infrastructure (PKI) requirements for DISS?

- Each DISS user will be 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.

3. What are the web browser requirements for DISS?

- Each DISS user will be required to have a Web browser with Internet Explorer 10 or above, Firefox 11 or above. Each browser must maintain 128-bit security (SSL) encryption.

4. How do I get a DISS account?

- Detailed information on how to request a DISS account, including clearance requirements, PKI certificates, mandatory training, and Letter of Appointment (LOA) requirements, will be posted in the DISS Account Management Procedures on DMDC's DISS website.

5. Will the help desk number for DISS be the same as JPAS?

- Yes, the help desk number and support procedures are the same for DISS as they are today for JPAS and the Personnel Security Management Office for Industry (PSMO-i).
- Phone Number: 1(800) 467-5526. Customer Service Hours: 8:00 am – 8:00 pm ET, Monday – Friday (excluding Federal Holidays).

6. Will existing JPAS accounts work within DISS?

- No, DISS will require new system access for each Hierarchy Manager. The minimum requirements for system access are a completed Personnel Security System Access Request (PSSAR) form, Personal Identifying Information (PII) and cyber awareness training certificate. At this time, system training certificates are not required for system access. Once provisioned, the Account Manager can provision users within their Component/Agency/Company.

7. Will information be migrated into DISS from JPAS?

- Yes, all JPAS data will be migrated to DISS upon full deployment.

8. How will DMDC communicate upcoming deployments, modifications, and information regarding DISS?

- Users can find information on DISS by going to the DMDC DISS web page. Updates include: alerts, notices and release notes. User manuals will be provided within the landing page of the DISS application.

9. Who determines the access authorizations for DISS?

- A minimum of interim secret eligibility is required to access DISS. Account Managers within each Component/Agency/Company will determine the specific DISS customer user base and assign user roles based on Component/Agency/Company guidance and responsibilities.

10. Who designates Hierarchy Managers?

- Hierarchy Managers are designated by their Component/Agency/Company.

11. What is the DISS operational policy on printouts?

- Personnel are granted access to DISS for the specific purpose of verifying eligibility and determining access to classified information of their service members/employees and/or visitors. There is no authorized use of DISS printouts. Security Officers/Facility Security Officers should never print out any screen, screenshot, or provide DISS printouts to any agency or person.

12. Will I need to register my CAC or PIV?

- Yes, the registration process has to be completed every time you get a new or replacement CAC or PIV. The Hierarchy Manager will need to generate a new password. The pre-established registration user id and the newly generated password should be sent to the user. Thereafter, the user should re-register using the steps outlined below.
- Select their Email Certificate.
- Click on the login button and you will be redirected to the User Registration Page.
- Enter the pre-established user id and the newly generated password and click register.

Section 2: Application FAQs

13. Will a subject's record turn red in DISS with the submission of an Incident Report?

- No, files will not turn red in DISS. Only the submitting office can view incident, however, all offices can view whether or not an incident flag exists.

14. Will the back button and exit lock your account?

- No, the exit screen and back button will not lock your account. The user will have to login again upon exiting however.

15. How will Research, Recertify and Upgrade Requests (RRUs) be handled in DISS?

- RRUs will become customer service requests (CSRs) in DISS. Customer service requests allow specific workflows to be sent to the PSMO-I and DoD CAF for review and processing.

16. Is there an indication that a save took place after I click Save?

- Yes, there are indications throughout DISS when a save takes place.

17. How do I access e-QIP?

- http://www.opm.gov/e-qip
- The applicant's Security Officer must have first initiated the Investigation Request.

18. Can I view the applicant's personnel security questionnaire through DISS?

- Yes, the information can be viewed with either the Security Manager or Security Officer role.

Section 3: DISS Security Incidents and System Misuses

19. Can I logon to DISS using someone else's username/password or PKI certificate?

- It is against DoD policies to share username/password, any approved active Public Key Infrastructure (PKI) hardware, or allow an individual to access another person's DISS account or certificate in any manner or form. Only the authorized account and certificate holder is permitted to access/use his/her account. Examples of Approved

Active PKI hardware include Common Access Cards (CAC), Personal Identity Verification (PIV) cards, approved corporate badges, and External Certificate Authority (ECA) cards/tokens, among others.

20. What do I do if I witness a misuse of DISS?

- Please call the DMDC Contact Center 1(800-467-5526) to report any potential misuses of DISS you may have observed.

21. What happens in the event of an alleged DISS misuse?

- As the Cognizant Security Agent (CSA) for DISS, when DMDC is made aware of an alleged misuse of DISS, the system must be protected from loss of data confidentiality, integrity, and availability. As a result, the user(s) account(s) are administratively locked and placed in administrative review, preventing any access to DISS during the review. This practice limits risk to the system and its data. During an administrative review:
    - The alleged will receive an Incident Notification Letter and any DISS accounts connected to the incident are locked.
    - Once the relevant data surrounding the incident is gathered, the DISS Program Manager (along with government counsel when necessary) make a determination as to whether or not the incident occurred:
        i. If it is determined that the incident occurred, the user may have their account terminated and be permanently barred from receiving another DISS (or future replacement system) account. A misuse of technology security incident will also be placed on the user's DISS record for the DoD CAF to adjudicate.
        ii. If it is determined that the incident did not take place the user account may be unlocked.
    - When an administrative review is complete, the user will receive an Outcome Notification Letter, outlining the decision and any subsequent actions.

22. I have received a DISS incident notification letter, what should I do?

- Follow all instructions as outlined in the incident notification letter.
- If a user receives a DISS incident notification letter, they may choose to directly respond with a personal statement addressing the incident.
- Note that the user(s) account(s) under administrative review will not be accessible, so please make appropriate coordination with other FSOs/AFSOs/SOs in your organization regarding your DISS workload/tasks.
- All communication regarding a DISS incident and/or administrative review should be directed to the email address provided in the notification letter.

23. What happens to my account in the event of an administrative review?

- In order to protect the confidentiality, integrity, and availability of the data in DISS, the user's account will be locked and will not be accessible during the entire period of the administrative review.
    - In the rare circumstance where the integrity of an entire cleared organization/SMO is in question, all associated DISS user accounts may be locked.
    - Appropriate investigative agencies may also be informed (e.g. Defense Criminal Investigative Service (DCIS), DoD Inspector General (DoDIG), etc.) dependent on circumstances and severity of the alleged incident.
- DISS audit logs are reviewed by program leadership to determine exactly what actions were performed/taken by the subject inside of the system, to include every screen viewed and every action taken in DISS.
- Note that your account will not be deleted/removed *due to inactivity* during an administrative review.

24. How long do administrative reviews take to complete?

- Administrative reviews have no defined timeframe. Factors such as the severity of the misuse, the number of individuals involved, third party investigations/input, government counsel involvement, and size of audit files, among other factors can all vary from incident to incident.

25. What are consequences related to misuse of DISS, and is there an appeals process?

- If it is determined that a misuse has occurred the user is at risk of losing their DISS account as well as being barred from reapplying for a DISS account **PERMANENTLY.**
- A misuse of technology incident will be placed on the user's DISS record for eventual adjudication by the CAF.
- An appeals process does exist; however, **only new and relevant evidence** may be presented to be considered for an appeal.