DISS JVS Initial Login Job Aid For Associating Token on Initial Login

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY



Version 1.0

May 9, 2021



REVISION HISTORY

DATE	VERSION	CHANGE DESCRIPTION	AUTHOR
5/9/2021	1.0	RELEASED ON DCSA TEMPLATE	DCSA



Initial Login and Token Registration

Connection Issues

If users have issues connecting to DISS (e.g. PKI certificates, SSL certificates), they should contact their local IT support. The DISS provisioning team does not have the privileges necessary to help users resolve these types of local issues.

OVERVIEW

The link to access the Defense Information System for Security (DISS) Joint Verification System (JVS) can be found here: <u>https://www.dcsa.mil/is/diss/</u>. All users will need to register their token (e.g. CAC/PIV) upon first login to DISS. *This document is meant to serve as a guide to facilitate users' first login*.

Notice and Consent

- 1. Read the standard, mandatory DoD Notice and Consent
- 2. Click the "I Agree" button to continue

	And A Product And
	ormation and Technology for Better Decision Making
fense Information System for Secur	rity (DISS) Web Application
Standard Mandatory DoD Notice and Consent	
By clicking the "Lagers" consent box on this page, users are consenting to the terms of use of the Information hystem for Security framily of System (DISS F65) biolises to include the forferura of to constitute a misuse of DISS F05 that could result in termination of the DISS F05 account(s), docum future access to DISS F05 or future personnel security systems. Accounts remain locked for an inde As a reminder, it is a violation of DoD regulations to share authentication mechanisms including any authorated individuals, as a result, there is no such thing as a "company" or shared account. Only the Any authorated individuals have response to the stare authentication fuel hins of the Privacy of their DISS F05 and future personnel security systems' account(s), regardless of any access regu	application and agree to comply with the Privacy Act of 1574, applicable DoD regulations, other applicable laws, and Defense DISE folds access a forms of use are violated violation of these negations, issue, and/or the Account Management Policy can netration of the incident on the DISE FoS record, and may include disallowing the subject(s), organization, and/or company from eterminate length of time during administrative reviews preceding a final decision. Y username/baseword or any approved Public Key Infrastructure (PKI) certificate. DISE FoS accounts are only provisioned for the automated account holder is permitted to view/access/use the DISE FoS account via a subject(s) individually issued PKI credential. I Act of 1974, applicable DoD regulations, other applicable laws, and DISE FoS policies will risk immediate forfeiture and TERMINATION arements that may exist to support mission-critical and job-essential tasks.
You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-auth	horized use only.
By using this 15 (which includes any device attached to this 15), you consent to the following condit	dons:
 The USG routinely intercepts and monitors communications on this IS for purposes includin enforcement (LE), and counterintelligence (CI) investigations. 	sg, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law
 The USG routinely intercepts and monitors communications on this IS for purposes including enforcement (LE), and counterintelligence (CI) investigations. At any time, the USG may inspect and seize data stored on this IS. 	ig, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law
 The USG routinely intercepts and monitors communications on this IS for purposes including enforcement (LE), and counterintelligence (CI) investigations. At any time, the USG may inspect and seize data stored on this IS. Communications using, or data stored on, this IS are not private, are subject to routine mo 	ng, but not limited to, penetration teating, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law mitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.
 The USG routinely intercepts and monitors communications on this IS for purposes includin enforcement (LE), and counterintelligence (CI) investigations. At any time, the USG may inspect and seize data stored on this IS. Communications using, or data stored on, this IS are not private, are subject to routine mo This IS includes security measures (e.g., authentication and access controls) to protect USG 	ng, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law mitoring, interception, and search, and may be disclosed or used for any USG authorized purpose. 3 interests - not for your personal benefit or privacy.
 The USG routinely intercepts and monitors communications on this 15 for purposes includin enforcement (LE), and counterintelligence (CI) investigations. At any time, the USG may inspect and seize data stored on this 15. Communications using, or data stored on, this 15 are not private, are subject to routine mo This 15 includes security measures (e.g., authentication and access controls) to protect USG Notwithstanding the above, using this 15 does not constitute consent to PM, LE or CI investi services by attorners, psychotheraptics, or clergy, and their assistants. Stuch communication 	ng, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PH), law mitoring, interception, and search, and may be disclosed or used for any USG authorized purpose. 3 interests - not for your personal benefit or privacy. igative searching or monitoring of the content of privileged communications, or work product, related to personal representation or ms and work product are private and confributial. See User Agreement for details.

Figure 1



DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

Register your Token

- **1.** Insert your DoD approved PKI credential. The Identity Card Registration screen displays.
- **2.** Enter the User ID and Password given to you by the Account Manager (You are only required to enter this information for your first login, and when new DoD approved PKI credentials are received).
- 3. Click on the **Register** button. You are directed to the PII page as above.

	FOR OFFICIAL USE ONLY	
DISS Digital to Finally		
Identity Card Registration	Enter Registration Information	
You have been re-directed to this page because you have not registered your identity card with the DISS system. You must enter the user ID and password provided to you by the Help Desk and select Register to complete the process. After successfully registering you may use your card to log into the DISS system.	User ID: Password:	
ASSISTANCE For assistance or to report problems, please contact the Help Desk.	Register	
punterintelligence and Security Agency, 2020 All Rights Reserved.	FOR OFFICIAL USE ONLY	

Figure 2



Log in

1. After clicking 'Agree' on the notice and consent page, enter your DoD approved PKI credential before clicking on the Login button.

FOR OFFICIAL USE ONLY				
	Notice	Insert your DoD Approved PKI Credential and press the 'Login' button		
	AUTHORITY	to log on.		
	5 USC 301	Login		
	PURPOSE/ROUTINE USE			
	Information you provide is used to verify your identity and usage of this website.			
	DISCLOSURE			
	Voluntary. However, if you fail to provide the requested information, DCSA will not be able to verify your identity. If your identity is not verified, you will be unable to gain access to the website.			
	Prevent illegal access of Privacy Act data by closing your browser before leaving your computer.			
	ASSISTANCE			
	For assistance or to report problems, please contact the Help Desk.			
Defense Counterintelli	© Defense Counterintelligence and Security Agency, 2020 All Rights Reserved.			

Figure 3

2. A Personally Identifiable Information (PII) confirmation screen pops up. Read the statements on the screen, confirming you have completed PII training and comply with the requirements. Click "Yes, Continue" to proceed or click "No, Logoff" to logout of the application.

Confirmation
Personally Identifiable Information
DATA YOU ARE ABOUT TO ACCESS COULD POTENTIALLY BE PROTECTED BY THE PRIVACY ACT OF 1974. You must:
 Have completed the necessary training with regards to Security Awareness and safe-guarding Personally Identifiable Information. Ensure that data is not posted, stored or available in any way for uncontrolled access on any media. Ensure that data is protected at all times as required by the Privacy Act of 1974 (5 USC 552a(1)(3)) as amended and other applicable DoD regulatory and statutory authority; data will not be where dwith offshore contractors; data from the application, or any information derived from the application, shall not be published, disclosed, released, revealed, shown, sold, rented, leased or loaned to anyone outside of the performance of official duties without prior DCSA approval. Delete or destroy data from downloaded reports upon completion of the requirement for their use on individual projects. Ensure data will not be used for marketing purposes. Ensure distribution of data from a DCSA application is restricted to those with a need-to-know. In no case shall data be shared with persons or entities that do not provide documented proof of a need-to-know. Be aware that criminal penalties under section 1106(a) of the Social Security Act (42 USC 1306(a)), including possible imprisonment, may apply with respect to any disclosure of information in the application(s) that is inconsistent with the terms of application access. The user further acknowledges that criminal penalties under the Privacy Act (5 USC 552a(1)(3)) may apply if it is determined that the user has knowingly and willfully obtained access to the application(s) that is under slace prelenses.
ACCESSIBILITY/SECTION 508
The U.S. Department of Defense is committed to making its electronic and information technologies accessible to individuals with disabilities in accordance with Section 508 of the Rehabilitation Act (29 U.S.C. § 794d), as amended in 1998. For persons with disabilities experiencing difficulties accessing content on a particular website, please email the DoD Section 508 mailbox: DoDSection508@sod.mil. In your message, please indicate the nature of your accessibility problem, the website address of the requested content, and your contact information so we can address your issue. For more information about Section 508, please visit the DoD Section 508 website.
By clicking the "Yes, Continue" button below, users are consenting to the terms of use of the application and agree to comply with the Privacy Act of 1974; if you do not agree click the "No, Logoff" button.
Yes, Continue No, Logoff
Figure 4



Session Limits and Locked accounts

1. If you are logged into the JVS application and attempt to open an additional session in another browser window, you receive an error message.

FOR OFFICIAL USE ONLY		
	error has occurred: User is already logged into the application. Please try again.	
Notice	Insert your DoD Approved PKI Credential and press the `Login' button	
AUTHORITY	to log on.	
5 USC 301	Login	
PURPOSE/ROUTINE USE		_
Information you provide is used to verify your	r identity and usage of this website.	
DISCLOSURE		
Voluntary. However, if you fail to provide the r your identity. If your identity is not verified, yo	requested information, DCSA will not be able to verify ou will be unable to gain access to the website.	
Brovent illegal accors of Brivaev Act data by sk	lecina your browcor before leaving your computer	•

Figure 5

- **2.** The system automatically terminates the active session after a set amount of user inactivity. After which, the user is redirected to the Standard Mandatory DoD Notice and Consent page.
- **3.** If your user account has been locked, you receive an error message. Locked users should contact their Agency Account Manager.

FOR OFFICIAL USE ONLY		
The following error has occurred: E757 - User Locked Please co	ontact the Help Desk	
Notice	Insert your DoD Approved PKI	
AUTHORITY	button to log on.	
5 USC 301	Login	
PURPOSE/ROUTINE USE		
Information you provide is used to verify your identity and usage of this website.		
DISCLOSURE		
Voluntary. However, if you fail to provide the requested information, DMDC will not be a verify your identity. If your identity is not verified, you will be unable to gain access to t	able to	

Figure 6