



Defense Information System for Security (DISS) Web Application

Standard Mandatory DoD Notice and Consent

By clicking the "I agree" consent box on this page, users are consenting to the terms of use of the application and agree to comply with the Privacy Act of 1974, applicable DoD regulations, other applicable laws, and Defense Information System for Security Family of Systems (DISS FoS) policies to include the forfeiture of DISS FoS access if terms of use are violated. Violation of these regulations, laws, and/or the Account Management Policy can constitute a misuse of DISS FoS that could result in termination of the DISS FoS account(s), documentation of the incident on the DISS FoS record, and may include disallowing the subject(s), organization, and/or company from future access to DISS FoS or future personnel security systems. Accounts remain locked for an indeterminate length of time during administrative reviews preceding a final decision.

As a reminder, it is a violation of DoD regulations to share authentication mechanisms including any username/password or any approved Public Key Infrastructure (PKI) certificate. DISS FoS accounts are only provisioned for authorized individuals, as a result, there is no such thing as a "company" or shared account. Only the authorized account holder is permitted to view/access/use the DISS FoS account via a subject's individually issued PKI credential.

Any authorized/unauthorized user(s) and/or company/organization found in violation of the Privacy Act of 1974, applicable DoD regulations, other applicable laws, and DISS FoS policies will risk immediate forfeiture and TERMINATION of their DISS FoS and future personnel security systems' account(s), regardless of any access requirements 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-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law 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 monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect USG interests - not for your personal benefit or privacy.
- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

I Agree

DISS Login Screen

The screenshot shows the DISS login interface. At the top, there is a navigation bar with the DISS logo and a 'Help' link. On the right, a user is logged in as ERIC SMITH, with the role of Application Admin, and the last login time is Friday, Mar. 15, 2024 16:40 PM UTC. A 'Logout' button is visible next to the user information.

A 'Confirmation' dialog box is displayed in the center of the screen. The dialog box contains the following text:

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 shared with 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) under false pretenses.

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@osd.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, Logout" button.

At the bottom of the dialog box, there are two buttons: "Yes, Continue" and "No, Logout".

DISS PII Screen



Notice

AUTHORITY

5 USC 301

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.

Insert your DoD Approved PKI Credential and press the 'Login' button to log on.

Login

DISS Notice Screen

▼ **SMO Relationships (0)**

Category ▲ Select ▼	Relationship ▲ Select ▼	SMO ▲ <input type="text"/>	Begin Date ▲ <input type="text"/>	End Date ▲ <input type="text"/>	Expand
-------------------------------	-----------------------------------	--------------------------------------	---	---	---------------

No relationships found with that criteria.

Add Relationships
Remove Relationships

▼ **HSPD-12 and Suitability Determinations (2)**

Type	Determination	Determining CAF	Determining SMO Organization	Determination Date
IT 3	Favorable		94-AW IP-4	1997/11/06
Public Trust	Favorable		94-AW IP-4	1997/11/06

▼ **Polygraph (0)**

Type	Agency	Date Recorded
No records found.		

▼ **Foreign Contact(s) and Relative(s) (1)**

Type	First Name	Middle	Last Name	Citizenship	Begin Date	End Date
Brother	Test		Contact	Papua New Guinea	2022/08/01	

DISS SMO Relationships Screen

DISS_OPS DO_NOT_TOUCH TEST_SUBJECT [Subject Details](#)

SSN:	222-33-4444	DoD EDI PN:	1509814550
DOB:	1935/01/31	Eligibility Level:	None
Place Of Birth:	None, GA, United States	Eligibility Determination:	Administratively Withdrawn made on 2017-09-08 by Collab CAF
Exception Code:	None	Open Investigation:	No
Supporting Investigation:	SSBI	NDA Signed Date:	
Incident Report:		NDS Signed Date:	

[SII Search](#) [Report Incident](#)

▼ **Citizenship Information (1)**

Country	Citizenship Date	Citizenship Type	Renunciation Date
United States			

▼ **Accesses (0)**

Type	Status	Indoctrination Date	Granted By	Subject Category	Expand
No records found.					

▼ **Continuous Evaluation (0)**

Activity Description
No records found.

▼ **Adjudication History (6)**

DISS Subject Summary

Adjudication History (6)

Activity Description

Secret adjudication completed with a **determination of No Action by DoD CAF on 2018/02/27.**

Secret adjudication completed with a **determination of No Action by DoD CAF on 2019/01/08.**

Top Secret/SCI adjudication completed with a **determination of No Action by DoD CAF on 2019/07/30.**

1 2

Investigation History (2)

Activity Description

SSBI investigation 1234 has been **Completed** on 2019-07-29.

SSBI investigation has been **Completed** on 1997-10-24.

Investigation Requests (0)

Request Date	Status	Type	SMO	Agency	EQIP Id	Contract #	Options	Expand
No records found.								

Categories (1)

Category	Effective Date	Separation Date	Expand
Active Duty	2022/10/17		

[Add Category](#)

Category Organizations (0)

Organization Name	Category Name	Begin Date	End Date	Options
No subject organizations exist.				

SMO Relationships (0)

DISS Adjudication History Screen