DEFENSE INFORMATION SYSTEM FOR SECURITY (DISS)

ACCOUNT MANAGEMENT POLICY

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

Version 2.0

June 24, 2021

CONTENTS

REVISION HISTORY

DATE	VERSION	CHANGE DESCRIPTION	AUTHOR
2/12/2021	1.0	Released on DCSA template	DCSA
6/24/2021	2.0	Updated to include signature page	DCSA

NADAL.EMILIO.MALATE.1181005366

Digitally signed by NADAL.EMILIO.MALATE.1181005366
Date: 2021.06.24 15:36:04 -04'00'

DISS Product Owner
Information Systems Owner (ISO)

1. PURPOSE

This document outlines account management policy and guidance for the Defense Information System for Security (DISS). This policy is maintained by the Defense Counterintelligence and Security Agency (DCSA) National Background Investigation System (NBIS) Program Management Office (PMO) and shall be reviewed at least annually.

2. BACKGROUND

DISS is a Department of Defense (DoD) enterprise-wide information system (IS) for Personnel Security, Suitability, and Homeland Security Presidential Directive (HSPD-12) credentialing eligibility information. DISS is used to request, record, document, identify, and conduct personnel security actions within DoD and applicable federal shared service (FSS) agencies including management of security clearance eligibility and access to national security information, suitability and HSPD-12 determinations for personal identity verification (PIV) credentials, submitting adverse information, and verification of background investigations (BI), and/or adjudicative determinations, and/or status including enrollment in Continuous Evaluation (CE) program.

DISS consists of three sub-applications:

- Case Adjudication Tracking System (CATS): CATS is used by DoD and FSS adjudicative community for the purpose of performing security clearance, suitability, and HSPD-12 credentialing adjudications and recording eligibility determinations.
- Joint Verification System (JVS): JVS is primarily used by security officers (SO) and facility security officers (FSO), component adjudicators, and human resource managers to perform security and suitability management functions as well as recording access determinations, submitting incident reports, submitting visit requests, and communicating with the adjudicator.
- Appeals: Appeals are used by the Defense Office of Hearings and Appeals (DOHA) and DoD Personnel Security Appeals Board (PSAB) for the purpose of completing due-process for subjects appealing unfavorable adjudicative determinations.

DISS contains personally identifiable information (PII) as well as sensitive information on security clearance eligibility levels and the status of background investigations.

3. ORGANIZATION ROLES AND RESPONSIBILITIES

3.1 NATIONAL BACKGROUND INVESTIGATION SYSTEM (NBIS) PROGRAM MANAGEMENT OFFICE (PMO)

The NBIS PMO is responsible for the origination of the DISS Account Management Policy, the enforcement of that policy, and approving the account administration of the primary Hierarchy Manager for the military services, DoD agencies, DoD contractors, and FSS agencies. The military services, DoD agencies, DoD contractors, and FSS agencies are responsible for the overall administration and maintenance of DISS user accounts within their own hierarchy for security management office (SMO) and/or Consolidated Adjudication Facility (CAF).

3.2 DISS USER SUPPORT

The DCSA provides user support to all users but only provides account management support to the Hierarchy Manager and Account Manager. Issues or concerns that require attention should be submitted to DCSA NBIS PMO. DISS technical support is defined as customer support needed to resolve technical issues concerning user browser configuration, DISS accessibility via the internet, and DISS system malfunctions. Users may be required to contact their local area communications or network support for network or local access issue resolution. The DISS support contact information can be located on the DISS Resource page within the DCSA website.

3.3 DISS ACCOUNT MANAGER

There are two main roles within JVS that can create user accounts: The Hierarchy Manager and Account Manager. The primary function of the Hierarchy Manager is to serve as head of the SMO and manages the organizational structure of the SMO. A Hierarchy Manager inherits the role and permissions of the Account Manager. The primary function of the Account Manager is to oversee the creation, administration, and management of DISS user accounts within a SMO. The Hierarchy Managers and Account Managers are responsible for managing all DISS user accounts within their respective SMO and required to provide account management support for their users as set forth in this policy. This includes maintaining appropriate paperwork as set forth in this policy and guidance from the NBIS PMO (refer to section 4: Account Life-cycle below). Hierarchy Manager may establish additional/specific organizational policies to supplement this document; however, those policies may not conflict with or supersede this account management policy document or guidance from the NBIS PMO.

Security service providers' Account Managers shall follow any additional guidelines set by their organization for the management of another organization's account while adhering to any guidance provided by the NBIS PMO and/or DISS Account Management policy. A Hierarchy Manager and Account Manager are not authorized to manage his or her individual DISS account. Hierarchy Managers and Account Managers may only create user accounts for individuals within their own SMO hierarchy.

The Hierarchy Manager (if needed within organization) can provision subordinate Account Manager(s) who have the ability to manage additional users within their SMO/hierarchy by creating the appropriate user account and assigning the required roles and permissions. Additional JVS user accounts can be created by either the Hierarchy Manager or Account Manager. The primary Hierarchy Manager must be initially provisioned by DCSA for a SMO and must be a company employee (i.e., not a consultant, contractor, sub-contractor, or security service provider). Once a SMO has a primary Hierarchy Manager in place, the Hierarchy Manager can create and assign any additional Hierarchy Managers and/or Account Managers to the SMO. Hierarchy Managers may create subordinate SMOs and provide Account Management support for any SMO within their own organization, including Multiple Facility Organizations (MFO) or corporate family.

Please note, organization by company agreement, where similar to MFO - some smaller companies may elect to execute a written agreement with another company for continuity of operations as it pertains to DISS account management. This is acceptable, provided the effectiveness of this agreement is able to be validated and the contractor facility security officer (FSO) or designee maintains a DISS account in order to ensure timely receipt of DISS notifications.

The Hierarchy Manager and Account Manager must maintain a current record of every DISS account created for their SMO(s). Group/office accounts are not permitted. Each DISS account will correspond to only a single user who is responsible for all actions taken using that account.

CATS and/or Appeals user accounts can be created by contacting their respective CAF and/or Appeals Administrators. For a full list of user roles and permissions within the JVS, CATS, and appeals sub-systems, please refer to the respective system's user manual.

3.3.1 UNEXPECTED LOSS OF DISS ACCOUNT MANAGER

Account Managers may be unable to manage an account for a variety of reasons (e.g. job change, death, major illness, etc.). Therefore, each SMO is required to maintain at least a primary and secondary Hierarchy and/or Account Manager. Establishing contingency responses within the SMO, MFO or via company agreement pertaining to the loss of Account Manager(s) is the responsibility of each SMO Hierarchy and/or Account Manager.

4. ACCOUNT LIFECYCLE

4.1 DISS ACCOUNT REQUIREMENTS

Each individual accessing DISS must have a separate and unique account created by the individual's Account Manager. Each DISS account will correspond to a single user who is responsible for all actions taken using that account. The SMO Account Manager must maintain a current record and associated documentation of every DISS account established within their organization (PSSARS, personally identifiable information (PII) and cyber awareness training certificates). Access to the DISS application shall be granted to complete an individual's job duties. In order to receive a DISS account, a potential user must a U.S. Citizen and:

DoD and National Industrial Security Program (NISP) Users: Individual requesting access must have a completed Tier 3 or higher investigation with a favorable adjudication. JVS requires a minimum of Interim Tier 3 eligibility for JVS: CATS and/or Appeals requires a minimum of Interim Tier 5 eligibility.

Federal Shared Service Agencies: Individual requesting JVS access must have a completed Tier 2 or higher investigation with a favorable adjudication.

Access to DISS is authorized via means of government-furnished/approved or company-issued equipment with appropriate security controls in place. DISS users may not access their accounts from personal or home computers or over unsecured wireless networks. Sharing user names and passwords or PIV credentials is strictly prohibited and will result in termination of the offender's DISS account(s). Additionally, a misuse of technology incident will be recorded on the offender's DISS record. If you are part of a contract, your contracting office will be notified of the security incident.

4.1.1 PERSONNEL SECURITY SYSTEM ACCESS REQUEST FORM (DD FORM 2962) AND TRAINING

The DD2962, Personnel Security System Access Request (PSSAR) form, is used to collect information required to create an account in the DISS system, to formally document the account request, and to

provide accountability for the user account. PSSARs are also used to request account deactivations and to make changes to user roles and permissions. The PSSAR should indicate the name of the applicant and the specific job duties that require DISS access.

PSSARs shall be completed and filed for all users of the DISS system by the entity provisioning the user. PSSARs shall have the signature of the individual requesting an account, the signature of the nominating official, and signature of the validating official before account access is granted. The nominating official CANNOT be the same as the requestor.

PSSARs must remain on file by the Account Manager at the SMO, agency, service, or company until the account is deactivated. This includes the initial PSSAR activating an account and any subsequent PSSARs submitted (e.g. modification or deactivation requests). In circumstances where the account was created or modified by the DCSA CCC, the PSSAR must still be retained by the SMO.

PSSARs must be deleted/destroyed when no longer needed for administrative, legal, audit or other operational purposes (but not before the account termination) per OSD, Records & Information Management Program, File Number 1606-06.2 (GRS 24, Item 6b).

All new or modified account requests (to include account recreation after deactivation due to inactivity) will need to include proof of mandatory PII and Cyber Awareness training completion in addition to the PSSAR form (DD Form 2962). The DD Form 2962, PSSAR, Vol. 2, Jan. 2020 is located on the DISS Resource page within the DCSA website.

MANDATORY TRAINING COURSES REQUIRED FOR DISS ACCESS

The DISS disclosure agreement includes an acknowledgment that the user has "completed the necessary training with regards to Security Awareness and safe-guarding Personally Identifiable Information." This disclosure agreement specifically refers to the following courses required to receive a DISS user account, available at:

- Cyber Awareness Challenge/Information Assurance (IA) Security Training (two options available):
    - The DoD Cyber Exchange's Cyber Awareness Challenge
    - Service, company, or agency approved cyber awareness/IA security training course
- Personally Identifiable Information (PII) Training (three options available):
    - DoD Cyber Exchange's Identifying and Safeguarding Personally Identifiable Information (PII) Training
    - CDSE's Identifying and Safeguarding Personally Identifiable Information (PII) Course (requires a STEPP account)
    - Service, company, or agency approved PII training course

Note: Service, company, or agency approved cyber awareness, IA, and/or PII training course certificates may only be used and submitted to an already established SMO Hierarchy Manager or Account Manager for new user account provisioning. Appropriate training certificates shall be completed and filed with the SMO. Please note DCSA will not maintain these certificates of completion beyond the primary Hierarchy Manager account request creation; it is up to the SMO to maintain proof of training requirements as it will be requested in the event of a security incident and/or audit.

4.2 APPOINTMENT OF HIERARCHY MANAGERS

The primary DISS Hierarchy Manager must be a company employee. Subsequent Hierarchy Managers and Account Managers may be provided by security service providers (e.g., consultants, sub-contractors, etc.), however, the primary DISS Hierarchy Manager must be directly employed with the company or SMO.

DISS Hierarchy Managers and Account Managers shall establish and manage accounts for subordinate Hierarchy/Account Managers and maintain the accounts, PSSARs, and training certificates thereafter.

4.3 DISS ACCOUNT ACTIVATION AND TERMINATION

DISS Account Managers are responsible for following the proper procedures to request, create, modify, and deactivate user accounts. Please refer to the DISS Account Request Procedure guide located in the DISS Resource page for more information.

4.4 ACCOUNT TRANSFER BETWEEN ORGANIZATIONS OR COMPANIES

DISS accounts are prohibited from being transferred outside the SMO or organization of which it was created under (including MFO or corporate family). If a user leaves an organization, company, or the security service provider contract/agreement is terminated, the associated account in DISS must be deactivated by the owning or using SMO, organization, and/or company. If DISS access is required at a new SMO, organization, and/or company, a new DISS account shall be created by the gaining SMO, organization, and/or company.

4.5 DISS ACCOUNTS FOR CONTRACTORS WORKING AT GOVERNMENT AGENCIES

DISS accounts for contractors who perform personnel security management functions (such as information security program manager, special security officer, special security representative, etc.), on behalf of the military services, DoD agency, or FSS agency are the responsibility of the hiring Government Agency and must follow all policy and guidelines as set forth in this DISS Account Management policy and the NBIS PMO. This responsibility includes the immediate termination of an individual's DISS account in the event of an adverse personnel security action such as suspension, revocation, and/or denial of the eligibility or access.

If a punitive personnel action is reported in DISS and the user's account is not terminated, it could result in restrictions placed on the DISS use/permissions of the government agency responsible for the contractor account.

5. SECURITY

5.1 SYSTEM DATA

Contents of the DISS system are subject to the Privacy Act of 1974. Under the Privacy Act of 1974, personnel information retrieved through DISS must be safeguarded. Disclosure of information is in accordance with instructions as noted on the security banner associated with the DISS system.

The following policies place the impetus for maintaining the confidentiality, integrity, and availability for DISS.

- DoD Instruction 8500.01 Cybersecurity stipulates that all employees and contractors involved with the management, use or operation of DoD information systems must receive annual information assurance training and training on the use of personally identifiable information.
- DoD 5220.22-M annual refresher training is required to review security principles and responsibilities and to emphasize new security policies and practices developed from the preceding year.
- 32 CFR § 2004.20 National Industrial Security Program Executive Agent and Operating Manual mandates for the FSO, or those otherwise performing security duties, shall complete security training as specified in Chapter 3 and as deemed appropriate by the CSA.

5.2 PRIVACY ACT

DISS JVS is intended for use by SOs/FSOs to update other users with pertinent personnel security clearance access information in order to ensure the reciprocal acceptance of clearances throughout the DoD and federal community. DISS CATS is intended for use by adjudicators to support the process of rendering determinations of an applicant's eligibility for security clearance and provides a framework for assessing an applicant's trustworthiness and fitness. DISS Appeals is intended for use by users in the DOHA and DoD Personnel Security Appeals Board (PSAB) to complete adjudication for subjects who appeal the determination made on their case in CATS, or for subjects for whom a decision cannot be made in CATS.

DISS in its intended use, according to policy, does not include giving out the records to the subject of record for their personal use without a proper Privacy Act request or authorization from the record owner. Individuals seeking access to information about themselves contained in this system must send written signed inquiries to the Defense Counterintelligence and Security Agency, Office of FOIA and Privacy Act, 27130 Telegraph Road, Quantico, VA 22134-2253.

DISS contains not only clearance eligibility information, but investigation and adjudication information, as well as Incident Reports, some of which may have originated with a third-party agency requiring their review/comments before a disclosure is made. Therefore, DCSA does not authorize the direct disclosure of records by a security manager or FSO to the subject of record. Service schools requiring clearance verification can either request access themselves or have the user agency provide the subject's clearance verification.

5.3 SECURITY BANNER

ATTENTION ALL DISS USERS: Below is verbiage from the Standard Mandatory DoD Notice and Consent Banner:

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.*

Below is the DISS Privacy Act Security Banner verbiage:

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(I)(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(I)(3)) may apply if it is determined that the user has knowingly and willfully obtained access to the application(s) under false pretenses.*

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 1999. Send feedback or concerns related to the accessibility of this website to: DoDSection508@osd.mil. For more information about Section 508, please visit the DoD Section 508 website.

5.4 PASSWORD/PIN MANAGEMENT

A DISS password will be randomly generated by the system and provided to the Account Manager at the time an account is created or a password change is forced. The Account Manager shall relay, in person or via encrypted email, the randomly generated password to the user for a one-time self-registration of their CAC or PKI certificates.

This password will need to be used for a one-time self-registration of their CAC or PKI certificates to the user's DISS account. The user will have to use their username and password in order to self-register their CAC or PKI certificate to their user account. After registering the certificate, you will not be required to remember or change your password.

Note: you will need to register your certificate each time you get new CAC/PKI certificate, or when switching between different PKI certificates for the same user.

After registering your CAC/PKI certificate to your DISS user account, you will access DISS via PKI authentication *only*, using only your CAC, PIV, or External Certification Authority (ECA) credential.

The DISS system will lock a user ID after three consecutive failed attempts at the self-registration screen. DISS user accounts can be unlocked only by the associated DISS Hierarchy Manager and/or Account Manager.

The DCSA CCC can force password changes for Hierarchy Managers within DISS. Hierarchy Managers and Account Managers can force password changes within DISS for their own organization's users.

- PINs may be alpha numeric codes associated with your PKI credential and are managed differently depending on the specific type of credential used.
- For a DoD CAC, you have three attempts to enter a correct PIN. If you fail on the third attempt, your credential will be locked. In order to unlock your credentials, you will need to visit a DEERS/RAPIDS station to unlock your CAC before attempting to re-log into DISS.
- For a Federal PIV credential, contact the issuer of your PIV credential for reset policies.
- For External Certification Authority (ECA) and other DoD approved PKI credentials, this process can vary from issuer to issuer. *Note:* some issuers do not conduct a PIN/Password reset and will require the purchase of a separate credential. Please be forewarned and ask for the vendor's policy prior to purchase.

Never share DISS user names, passwords, PKI credentials, PINs, or other authentication information with any other individual, including anyone who is a designee or an alternate to the account holder. DISS does not have or allow company accounts. Sharing user names, passwords, or PIV/PKI credentials is strictly prohibited and will result in the termination of any associated or involved DISS accounts.

Violations of procedures will lead to the termination of the DISS account(s) or exclude culpable companies or persons from access to DISS for a specified or indefinite period of time. Information concerning violations of these procedures may also be referred to other federal agencies for consideration of administrative, civil, or criminal sanctions when circumstances warrant.

5.5 USER IDENTIFICATION (ID)

A DISS user ID is systematically generated at account creation and is unique to individuals. Group login accounts and the sharing of user IDs are strictly prohibited.

5.6 ACCOUNT ACTIVITY

An active DISS account is one that has been logged into within the past 30 days. An inactive DISS account is an account that has not been logged into in over 30 days. If a DISS account is inactive — i.e. not successfully accessed for more than 30 days, the DISS system shall automatically lock and suspend the account. The Hierarchy Manager or Account Manager will be able to reinstate access to the account, unless the account exceeds 45 days of inactivity. DISS accounts that have not been logged into for longer than 45 days are deactivated/removed per DoD Regulations (CYBERCOM TASKORD 13-0641). If an account is needed after 45+ days of inactivity, a new account will have to be created following the aforementioned guidelines.

5.7 ADMINISTRATIVELY LOCKED ACCOUNTS

DISS user accounts may be administratively locked due to suspected and/or confirmed policy violation(s) and/or misuse of DISS. Inquiries about locked accounts should be directed to the DCSA CCC. Accounts

remain locked for an indeterminate length of time during administrative review(s) preceding a final determination.

5.7.1 DEACTIVATED ACCOUNTS

Once an account has been deactivated (for any reason) a new user account will have to be established following the DISS Account Request Procedure guide. The primary and secondary account holders are responsible to maintain accounts and prevent them from being suspended or deactivated.

5.8 MISUSE OF DISS

By clicking the "I Agree" consent box on the DoD Security Banner page in the DISS application, 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 DISS policies to include the forfeiture of DISS access if terms of use are violated. Violation of these regulations and/or the DISS Account Management policy may lead DCSA to suspend or withdraw DISS access, permanently or temporarily terminate user(s) DISS account(s), document the incident on the DISS subject record of the violator(s), or may exclude culpable companies or persons from access to DISS and other personnel security systems, regardless of any access requirements that may exist to support mission-critical or job-essential tasks. Misuse of DISS may result in the account being administratively locked for a specified or indeterminate length of time during administrative reviews. The Defense Counterintelligence and Security Agency (DCSA) may also refer information concerning violations of these procedures to other Federal agencies for consideration of administrative, civil or criminal sanctions when circumstances warrant.

As a reminder, it is a violation of DoD regulations to share authentication mechanisms including any username/password or any approved PKI certificate. Sharing user names and passwords or PKI certificate is strictly prohibited and will result in immediate termination of the offender's DISS accounts (to include all persons who provided and received a shared PIV/PKI credential). Additionally, a misuse of technology incident will be recorded on the offender's DISS record. If you are part of a contract, your contracting office will be notified of the security incident.

DISS accounts are only provisioned for authorized individuals, as a result, there is no such thing as a "company, office, or shared account." Only the sole authorized account holder is permitted to view/access/use the DISS account via a subject's individually issued PKI certificate.

Misuses of DISS include, but are not limited to:

- Sharing username, password, CAC, or PIV/PKI certificate and/or associated PIN numbers
- Allowing non-cleared/unauthorized individuals to access the system
- Leaving the DISS application unsecure while logged in
- Allowing others to view data on the DISS screen that do not have the proper authorization
- Printing or taking screenshots of DISS data
- Querying the DISS application for "celebrity" records
- Entering test or "dummy" SSNs into DISS
- Knowingly entering false or inaccurate information into the DISS system

- Initiating investigations for subjects who you have no owning/servicing relationship with or are otherwise not appropriately sponsored for a security clearance
- Taking any action on your own record (e.g. submitting visit requests for yourself, attempting to indoctrinate yourself, establishing an owning/servicing relationship of yourself, etc.)
- Querying the DISS application for information you have no need to know and/or authority to view to conduct your official duties.
- Querying the DISS application for subject records or persons no longer affiliated with your SMO.
- Transferring or copying any DISS data to an outside system without prior written authorization.

DCSA as the System Manager (SM), Program Manager (PM), and Authorizing Official (AO), has the responsibility and ability to make determinations regarding system access, especially when a misuse of the system has occurred that may require an adjudicative determination. If a user has been previously locked out of any DoD personnel security system for misuse or violation of policy, they will not be granted a DISS account. This responsibility and authorization for DCSA to make risk-based authorization decisions is stated in the DoDI 8500.01 Enclosure 3: Procedures, Section 2: Risk Management, (3)(b).

> (b) Information protection requirements are satisfied by the selection and implementation of appropriate security controls in Reference (cj). Security controls are implemented at Tier 3 by common control providers, system managers (SMs), or PMs, and risk-based authorization decisions are granted by AOs.

Additionally, Enclosure 3: Procedures, Section 16: AO, (b):

> b. Render authorization decisions for DoD ISs and PIT systems under their purview in accordance with Reference (q).

If a DISS security violation has occurred and a legitimate requirement that DISS access is needed, DCSA may reinstate a DISS account to another individual associated with that company/agency, but not to the individual(s) who have violated this account management policy or DoD regulations. In order to reinstate or allow additional DISS user accounts, DCSA requires a written request from Agency/company's government Sponsor on their associated letterhead. The written request must include an acknowledgment that the government sponsor is aware of the DISS security violation and request DISS access to be granted to another individual in order to support mission-critical and job-essential tasks. Once DCSA has received all the requested information to satisfaction, DISS access may be granted.

ACRONYM LIST

Acronym	Definition
AM	Account Manager
AO	Authorizing Official
BI	Background Investigation
CAC	Common Access Card
CAF	Consolidated Adjudications Facility
CATS	Case Adjudication Tracking System
CCC	Customer Contact Center
CDSE	Center for Development of Security Excellence
CE	Continuous Evaluation
CI	Counterintelligence
COMSEC	Communications Security
CSA	Cognizant Security Agency
CSR	Customer Service Request
CYBERCOM	United States Cyber Command
DCSA	Defense Counterintelligence and Security Agency
DEERS	Defense Enrollment Eligibility Reporting System
DISA	Defense Information Systems Agency
DISS	Defense Information System for Security
DMDC	Defense Manpower Data Center
DoD	Department of Defense
DOHA	Defense Office of Hearings and Appeals
DSN	Defense Switched Network
ECA	External Certification Authority
FCL	Facility Clearance Level
FSO	Facility Security Officer
FSS	Federal Shared Service
HM	Hierarchy Manager
HSPD-12	Homeland Security Presidential Directive-12
IS	Information System
ISFD	Industrial Security Facilities Database
JVS	Joint Verification System
KMP	Key Management Personnel
LE	Law Enforcement

APPENDIX A: USER ROLES

JVS USER ROLES

- Security Officer: Security Officers manage subjects associated with a SMO, in addition to sending out and working on tasks from CATS and other SMOs. Users with this role can update subject information, create accesses, visits, and incidents, and establish and remove owning/servicing relationships with subjects.
- Security Officer Administrator (Security Officer Admin): A Security Officer Admin is subordinate to the Security Officer. The Security Officer Admin role has all the capabilities of the Security Officer with the exception of subject creation and tasks related to investigation requests.
- Security Officer Visit Administrator (Security Officer Visit Admin): A Security Officer Visit Admin is subordinate to the Security Officer Admin. The Security Officer Visit Admin role has all the capabilities of the Security Officer Admin with the exception of managing accesses and incidents, managing foreign travel and relationships, creating Customer Service Requests (CSR), managing polygraphs, managing periodic reinvestigations, and updating subject information.
- Account Manager: The Account Manager manages the Security Officers and the users within their Hierarchy. They perform tasks such as creating and maintaining user profiles, roles, and permissions. Account Managers can work in child SMOs of the SMO(s) they are provisioned in.
- Hierarchy Manager: The Hierarchy Manager is the head of the SMO. They have the same privileges as Account Managers but are also responsible for SMO management, including creating child SMOs and editing and deactivating SMOs.
- Security Manager: Security Managers have the general permissions of a Security Officer, such as creating and modifying visits, creating and managing subjects, and the ability to receive and send tasks. Security Managers can also work in child SMOs of the SMO(s) they are provisioned in.
- Human Resource Manager: The Human Resource Manager has read-only access to subject information. They are only able to receive communications from the DoD Consolidated Adjudications Facility (CAF).
- Component Adjudicator: The Component Adjudicator adjudicates HSPD-12 and Suitability cases sent for field determination from CATS.
- Physical Access Control Personnel: Physical Access Control Personnel can view subjects, SMOs, Organizations, and visit information to verify who should have physical access to a facility.
- Privacy Officer: The Privacy Officer has access to a subject's records and documents in a view-only capability.
- Help Desk: The Help Desk has permissions in the application to provide operational support to the JVS users.
- Application Administrator for DISS SMO only: The Application Admin has most of the permissions in the application to provide operational support to the JVS users. If the Help Desk is unable to

resolve the issue the JVS user is experiencing, they will escalate the issue to the Application Admin to assist with triaging the issue.

**These roles also have access to the Reporting application and can generate specific reports.*

NOTE: The create and edit functionalities for the accesses, visits, and incidents permissions displayed on the JVS Roles and Permission matrix are currently disabled and read-only in the user interface until a future release. All actions and determinations related to accesses, visits, and incidents need to be completed in the system of record, the Joint Personnel Adjudication System (JPAS).

JVS USER PERMISSIONS

The below table represents permissions for a given role. The "X" indicates a mandatory permission while "O" are optional.

Permissions	Security Officer	Component Adjudicator	HR Manager	Security Officer Admin	Security Manager	Account Manager	Hierarchy Manager
Access SMO Record	X	X	X	X	X	X	X
Add Adjudication History	O	O			O		
Add Investigation History	O	O			O		
Adjudicative 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		
Make 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				X		
Remove Subject Relationship	X				X		
Review Investigation Request	O				O		
Suspend Access	X				X		
Update Subject Information	X				X		
Updated Subject PII							
View Non-SCI Access	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		

Permissions*	Manage SCI Access	Modify Visit	Manage Periodic Investigations	Maintain SMO
Manage Tasks				
Tasks Supervisory Performances				
View SMO Subjects				
View Subject List				
Access SMO Record				X
Close Incident				
Conduct Verification				
Configure SMO Notification Settings				
Configure User Notification Settings				
Create Incidents				
Create SMO				X
Create Subject Information				
Create User				
Create Visit		X		
Deactivate SMO				X
Establish Subject Relationship				
Field Adjudication				
Grant Non-SCI Access	X			
Initiate Adjudication Request				
Initiate Investigation Request			X	
Lock SMO Notification Settings				
Maintain SMO				
Manage DISS User				
Manage Foreign Relationships				
Manage Foreign Travel				
Manage Organization				
Manage Periodic Investigations			X	
Manage Polygraph				
Manage Reports				

Manage SCI Access				
Manage SCI DISS User				
Modify Visit				
Overrise Investigation Request				
Remove Non-SCI Access	X			
Remove Subject Relationship				
Review Investigation Request			X	
Supervisor Capability				
Suspend Access	X			
Updated Subject PII				
Transfer Owning Relationship				
Updated Subject Information				
View Non-SCI Access	X			
View SCI Access	X			
View SMO Notification				
View Subject Information				
View User Notification				
View Visit		X		

**If a user has permissions in the first row, they will automatically inherit those permissions marked with an "X". For example, users with the "Access SMO Record" permission will automatically inherit the "Maintain SMO" permission.*

JVS ROLE COMBINATIONS

The below table represents possible role combinations. The "O" in the box indicates that the role combination is possible.

	Security Officer	Component Adjudicator	HR Manager	Security Officer Admin	Security Manager	Account Manager	Hierarchy Manager
Security Officer		O				O	O
Compound Adjudicator	O		O	O	O	O	O
HR Manager		O				O	O
Security Officer Admin		O				O	O
Security Manager		O				O	O
Account Manager	O	O	O	O	O		O
Hierarchy Manager	O	O	O	O	O	O	

APPENDIX B: PROCEDURES GOVERNING USE OF DISS

DoD, acting as a CSA, has designated the Information System, DISS, as the DoD system of record for security and suitability eligibility and access for DoD populations and Federal shared service Agencies.

DISS is a U.S. Government information system that contains official government records. The information in DISS must be protected from unauthorized disclosure and used only for authorized purposes. Contractors may only use their DISS accounts to manage the access records of their employees and consultants, and to verify the access levels and affiliations (e.g., employee of ABC Company) of incoming visitors who require access to classified information.

The following procedures are issued under the authority provided by laws, polices and regulations governing the use of government information systems. Agencies and Industry shall follow these procedures when using DISS and shall ensure that authorized users of DISS have been properly informed about these procedures and any other specific policies governing access to and use of DISS.

1. Agencies and Industry shall accurately maintain the DISS records pertaining to their employees and contractors, and consultants. DISS users must expeditiously update these records when changes occur (e.g., termination of employment).
2. Agencies and Industry are prohibited from placing false information in DISS, and DCSA will seek appropriate sanctions against users who knowingly place false information in DISS.
3. DoD issues DISS accounts exclusively for use by agencies and a specific contractor or corporate family of contractors. Persons given access to DISS as account holders may only use DISS on behalf of the agency, cleared contractor or corporate family of contractors through which the account was issued. For example, an employee of ABC Company holding a DISS account issued through ABC Company and who works at a government site is not authorized to use the contractor granted account in support of the government customer. If the government customer requires the contractor employee to review or update DISS records on behalf of the government customer, the government customer must provide a separate, newly created DISS account for the contractor employee to use — they may not share an existing user ID and password. DCSA account management can assist in this request.
4. The DISS primary Hierarchy Manager must be an agency/company employee. Subsequent Hierarchy Managers and Account Managers may be provided by security service providers (i.e., consultants and/or sub-contractors).
5. Industry may subcontract or obtain consultant support from security service providers for administering security services. The Industry company will provide a DISS account to the security service provider under the using Industry's security management office for the sole purpose of permitting the subcontractor or consultant to provide security services for the using company only. Subcontractors or consultants providing such security services must be under the direct supervision of the using contractor's FSO or FSO's designee.

6. Each individual accessing DISS must have a separate and unique account created by the individual's DISS Hierarchy Manager and Account Manager. The Hierarchy Manager and Account Manager must maintain a current record of every DISS account established as per *DISS Account Management Policy*, *Section 4.1.1, Personnel Security System Access Request Form (DD Form 2962) and Training*.
7. DISS users may never share their user IDs, passwords, PIV/PKI certificates, PINs, or other authentication information with any other individual, including anyone who is a designee or an alternate to the account holder.
8. Access to DISS is only authorized by means of company or government owned or approved equipment with appropriate security controls in place. DISS users may not access their accounts from personal or home computers or over unsecured wireless networks.
9. Industry companies are authorized to verify prospective employees' eligibility for access to classified information in DISS prior to an offer of employment being extended. However, they may not use DISS for recruiting purposes.
10. While access to DISS is only granted to Industry companies who have a legitimate need for such access in support of classified work being performed for the government, DISS is not a classified system. Defense Counterintelligence and Security Agency (DCSA) will not grant a facility security clearance (FCL) for the sole purpose of allowing a company or its employees to gain access to DISS.
11. Anyone that becomes aware of a DISS user violation of these procedures shall immediately report the nature of the violation, the names of the responsible parties, and a description of remedial action taken, to the servicing DCSA industrial security representative.

NOTE: *Violations of the procedures may lead DCSA to suspend or withdraw DISS access, terminate the DISS account, mark a technology incident on a violator's DISS record, or exclude culpable companies or persons from access to DISS and other personnel security systems for a specified or indefinite period. DCSA and/or DCSA may also refer information concerning violations of these procedures to other federal agencies for consideration of administrative, civil, or criminal sanctions when circumstances warrant.*