SYSTEM ACCESS REQUEST (SAR)

Enterprise Security System (ESS)
Phone: 888.282.7682

OMB No. Pending
OMB approval expires
XXXXXXXXXXXXXXX

PRIVACY ACT ADVISEMENT:

AUTHORITY: Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act.
PRINCIPAL PURPOSE: To record names, signatures, and Social Security Numbers for the purpose of validating the trustworthiness of individuals requesting access to Department of Defense (DoD) systems and information. NOTE: Records may be maintained in both electronic and/or paper form.
ROUTINE USES: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, these records or information contained therein may specifically be disclosed outside DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows: To a Federal, State, or local law enforcement agency when your agency becomes aware of a violation or possible violation of civil or criminal law; to the Department of Justice for the purposes of representing the DoD in pending or potential litigation to which the record is pertinent; to the Merit Systems Protection Board for the purpose of litigation or investigation of alleged or possible prohibited personnel practices; to a Federal agency when conducting an investigation or inquiry for security or audit reasons; or the General Services Administration in connection with its responsibilities for records management.
DISCLOSURE: Disclosure of this information (to include social security number) is voluntary; however, failure to provide the requested information will impede, delay or prevent further processing of this request.

1. TYPE OF USER

☐ **DoD** (Military or Civilian) ☐ **DoD Contractor** ☐ **Non-DoD NISP** ☐ **Non-DoD**

2. TYPE OF REQUEST:

☐ Create an Account ☐ Delete an Account ☐ Change User Level *(JPAS Only)*
☐ Name Change *(Last, First, Middle)*

From:	**To:**

3. USER INFORMATION (Must fill in completely; please type)

Last Name:	First Name:	Middle Name:
Social Security Number:	Date of Birth:	POB:
Job Title/Rank/Grade:		
Organization Name:	Office Symbol:	
CAGE Code *(NISP Contractor Only)*:		
Business/Duty Station Address *(street, city, state, zip code):*		
Telephone Number:	Fax Number:	
e-Mail Address:		

4. APPLICATIONS

Defense Central Index of Investigations (DCII) (Government Only)	**OTHER**
☐ Agency Site Administrator or Coordinator ☐ User : ☐ Query Agency Code_____ ☐ Add ☐ Delete ☐ Update ☐ File Demand *(Provide Accreditation Code):* _____ ☐ File Demand Print	☐ Industrial Security Facilities Database (ISFD) ☐ Secure Web Fingerprint Transmission (SWFT) ☐ Industry Site Administrator ☐ Industry User ☐ Other *(Please Specify)* _____ _____ _____

5. JCAVS

Type of Account Requested: ☐ Account Manager ☐ User

Permission Requested: ☐ Initiate PSI ☐ Review e-QIP ☐ Override PSI ☐ Approve e-QIP

Access Requested – Industry: (*Must submit signed Letter of Appointment*)		**Access Requested – Non-Industry:**	
☐ Level 2	Corporate Officer (SCI)	☐ Level 2	MACOM/Activity/HQ/Agency SSO
☐ Level 3	Company FSO Officer/Manager (SCI)	☐ Level 3	Base/Post/Ship/etc. SSO
☐ Level 4	Corporate Officers Manager	☐ Level 4	MACOM Non-SCI Security Manager
☐ Level 5	Company FSO Officers/Manager	☐ Level 5	Base/Post/Ship/Non-SCI Security Mgr
☐ Level 6	Unit Security Manager/Visitor Control	☐ Level 6	Unit Security Manager
☐ Level 7	Guard Entry Personnel	☐ Level 7	Collateral Entry Controller
☐ Level 8	Guard Entry Personnel (SCI)	☐ Level 8	SCIF Entry Controller
☐ Level 10	Visitor Management	☐ Level 10	Visitor Management

User's Last Name, First Initial: _____

6. JAMS USER ROLES (DoD/Non-Industry Only)

CAF: **CAF Team:** **Employee Code:**

☐ Account Manager	☐ Manager	☐ Computer Analyst	☐ Case Assignment Personnel
☐ Security Assistant	☐ Customer Support	☐ Adjudicator	☐ Management Support
☐ Pending User	☐ Supervisor	☐ Mailroom	

Special Case User Can Handle:

☐ CAF Employees ☐ Presidential Support ☐ GS-15/General Officer

Investigation Request Permissions:

☐ Review PSQ ☐ Approve e-QIP

User Permissions:

☐ SAP	☐ SCI	☐ TS	☐ Secret
☐ Reports	☐ JCAVS	☐ FOIA/PA	☐ LAA
☐ Case Management	☐ Update Case Component	☐ Assign CAF Cases	☐ Review Required
☐ Reassign to Other CAF	☐ Assign/Reassign Cases	☐ Reassign from Other Employee	

7. NOMINATING OFFICIAL'S CERTIFICATION (Note 1)

I certify that the above named individual meets the requirements for access and account management privileges. Furthermore, I certify that the named user requires account/access as indicated above in order to perform assigned duties.

Nominating Official's Printed Name	Nominating Official's Signature and Date
Nominating Official's Title	Nominating Official's Telephone Number

8. USER'S CERTIFICATION

I hereby certify that I understand that by signing this System Access Request, I am solely responsible for the use and protection of the user ID and password that I will be provided. I also understand that I am not authorized to share my user ID and password with any other individuals. I will utilize all tools and applications in accordance with the Account Management Policy and Security Policy, as well as all applicable U.S. laws and DoD regulations.

User's Printed Name	User's Signature and Date

9. VALIDATING OFFICIAL'S VERIFICATION (Note 2)

I have verified with the appropriate security official/manager that minimum investigative requirements for the above user have been met.

Clearance Level: _____ Type of Investigation: _____

Clearance Granted Date: _____ Date Investigation Completed: _____

Clearance Issued By: _____ Investigation Conducted By:_____

Printed Name of DoD Security Services Center Representative or Security Official	Signature of DoD Security Services Center Representative or Security Official, and Date

10. ADDITIONAL SAR DIRECTIVES

- The SAR must be signed by the Nominating Official and the User or it will not be processed.
- Refer to page 3 of this form and JPAS, ISFD, DCII and SWFT Frequently Asked Questions (FAQs) at https://www.dss.mil or https://www.dmdc.osd.mil/psawebdocs, for additional SAR submission procedures pertaining to the respective systems (for example, please be advised that the DSS DoD Security Services Center does not process JCAVS access requests for military personnel; these requests should be submitted to the appropriate military agency approving authority).
- SARs requiring DSS processing/approval should be submitted to the DoD Security Services Center via fax number 703.493.8965, e-mail address account.request@dsshelp.org, or mailing address DoD Security Services Center, 10430 Furnace Road, Suite 101, Lorton, VA, 22079. Please allow at least three (3) business days for the SAR to be processed by the DoD Security Services Center. Notification of access will be sent to the User's e-mail address. To ensure receipt of the access notification e-mail, add account.request@dsshelp.org to your e-mail contacts list.
- The completed SAR must be maintained by the account manager for a minimum of six (6) months after the account is deleted.

Notes:

1. Nominating Official may be the Facility Security Officer, KMP, Security Manager, Information Systems Security Officer, Agency Administrator, etc. In most cases, **the Nominating Official MUST be other than the User**.
2. Validating Official is either a representative of the DoD Security Services Center, or if the SAR is staying within the organization, the appropriate security official. For non-DoD government agency requests, non-DoD government agency security officials must complete this section.

SYSTEM ACCESS REQUEST (SAR) INSTRUCTIONS
Enterprise Security System (ESS)

SECTION	TITLE	INSTRUCTIONS
1	**TYPE OF USER**	Check the appropriate box for DoD (e.g., Military Branches, DoD Agencies), DoD Contractor Companies, Non-DoD NISP Partners and Non-DoD affiliated.
2	**TYPE OF REQUEST**	Check the appropriate box indicating purpose for the SAR.
3	**USER INFORMATION**	Must completely fill in. If no middle name, enter NMN. Ensure e-mail address is accurate; account access credentials are transmitted via e-mail.
4	**APPLICATIONS**	Check the application(s) and function(s) the user requires.
5	**JCAVS**	Check appropriate boxes. See definitions below. **NOTE:** The appointment letter must be drafted on company letterhead, must name the Primary Account Manager and must be signed by a corporate officer (KMP). The same KMP must sign both the SAR (nominating official) and the letter.
5	**ACCOUNT MANAGER**	Account Managers will provide account maintenance on all user accounts created within their company. Responsibilities include, but are not limited to, locking/unlocking accounts, resetting passwords, logging off users, deleting accounts when no longer needed and maintaining their Security Management Offices (SMO). Account managers will create any additional accounts that are required.
5	**USER**	Depending on the level of access, users may verify clearances, update accesses, process visit notifications, and handle all other functions within JCAVS.
5	**ACCESS REQUESTED – INDUSTRY**	Check appropriate block, using the following guidance: Level 2: SCI security personnel at Corporate level, with read and write access. Level 3: SCI security personnel at echelons subordinate to Level 2 at a particular geographic location, with read and write access. Level 4: Non-SCI security personnel at Corporate level, with read and write access. Level 5: Non-SCI security personnel immediately subordinate to Level 4, with read and write access. Level 6: Non-SCI security personnel immediately subordinate to Level 5, with read and write access. Level 7: Non-SCI security personnel who accomplish entry control (i.e., access to installations, buildings, etc.), with read-only access. Level 8: SCI security personnel who accomplish entry control, with read-only access. Level 10: Non-SCI security personnel who accomplish visitor management, with read-only access.
5	**ACCESS REQUESTED – DoD (NON-INDUSTRY)**	Self-explanatory; check appropriate block.
N/A	**TOP OF PAGE 2**	Ensure User's last name and first initial are entered at the top of the page in the space provided.
6	**JAMS USER ROLES**	Provide information and check appropriate boxes for user functions, access, and permissions. JAMS is only authorized for DoD CAFs.
7	**NOMINATING OFFICIAL'S CERTIFICATION**	The Nominating Official is the individual who is authorizing that the User should have the requested accesses. The Nominating Official may be a Corporate Officer (KMP), Facility Security Officer, Security Manager, Information Systems Security Officer, Agency Administrator, etc. **For JCAVS Industry Primary Account Managers, the SAR must be signed by the same KMP that signed the Appointment Letter. The Nominating Official CANNOT be the same as the User**. Exceptions include the company President, for JCAVS, and the FSO, for ISFD. *NOTE: SARs submitted without the Nominating Official's signature included will not be processed.*
8	**USER'S CERTIFICATION**	User must sign, acknowledging DoD/system policy.
9	**VALIDATING OFFICIAL'S VERIFICATION**	The DoD Security Services Center (for industry only) or the Security Manager must verify and indicate the following information on the following lines prior to signing: Clearance Level; Clearance Granted Date; Clearance Issued By; Type of Investigation; Date Investigation Completed; and Investigation Conducted By. For non-DoD government agency requests, the Chief of Security or designee must complete this section.
10	**ADDITIONAL SAR DIRECTIVES**	Provided to facilitate successful processing of the SAR.