NAME *(LAST NAME, FIRST NAME, MIDDLE INITIAL)* _____

PERSONNEL SECURITY SYSTEM ACCESS REQUEST (PSSAR)
DEFENSE MANPOWER DATA CENTER (DMDC) - Version 1

OMB No. 0704-0542
OMB approval expires 20211031

Return completed form to the appropriate Account Manager or DMDC Contact Center, as indicated in the instructions.

PRIVACY ACT STATEMENT

AUTHORITY: DoD 5200.2-R, Department of Defense Personnel Security Program Regulation; E.O. 12829, National Industrial Security Program; the JPAS Account Management Policy; and E.O. 9397, as amended.
PRINCIPAL PURPOSE(S): To request the establishment of user roles and access and validate the trustworthiness of individuals seeking access to DCII, SWFT, JCAVS, or JAMS.
ROUTINE USE(S): The blanket routine uses found at http://dpclo.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx may apply.
DISCLOSURE: Voluntary. However, failure to provide the requested information may impede, delay, or prevent further processing of your request. The Social Security Number is used to verify the trustworthiness status in JPAS.

TYPE OF REQUEST (REQUIRED) | **DATE** *(YYYYMMDD)*

☐ INITIAL ☐ MODIFICATION ☐ DEACTIVATE USER ID (EXISTING ACCOUNTS) _____

PART 1 - PERSONAL INFORMATION

1. **NAME** *(LAST, FIRST, MIDDLE INITIAL)*	2. **ORGANIZATION** Include Major Command	
3. **OFFICE SYMBOL/DEPARTMENT**	4. **TELEPHONE** *(DSN or COMMERCIAL)*	
5. **OFFICIAL E-MAIL ADDRESS**	6. **JOB TITLE AND GRADE/RANK**	
7. **OFFICIAL MAILING ADDRESS**	8. **CITIZENSHIP**	9. **DATE OF BIRTH** *(YYYYMMDD)*
10. **PLACE OF BIRTH** *(CITY & STATE/COUNTRY)*	11. **SOCIAL SECURITY NUMBER**	12. **CAGE CODE** *(CTR ONLY)*

13. **DESIGNATION OF APPLICANT** ☐ MILITARY ☐ DoD CIVILIAN ☐ INDUSTRY ☐ NON-DoD

PART 2 - APPLICATIONS

14. DEFENSE CENTRAL INDEX OF INVESTIGATIONS (DCII) (GOVERNMENT ONLY)

a. DCII AGENCY CODE _____ **OR DCII AGENCY ACRONYM** _____

b. USER PERMISSIONS

☐ QUERY (SEARCH) ☐ ADD ☐ UPDATE ☐ DELETE ☐ AGENCY ADMINISTRATOR ☐ EXECUTIVE ADMINISTRATOR
☐ FILE DEMAND *(PROVIDE ACCREDITATION CODE)*: _____ ☐ FILE DEMAND PRINT ☐ IA (ROOT ADMINISTRATOR)

15. SECURE WEB FINGERPRINT TRANSMISSION (SWFT) (GOVERNMENT/INDUSTRY)

a. PERMISSIONS - FINGERPRINT SUBMISSION

☑ USER ☐ MULTI-SITE UPLOADER ☐ SITE ADMINISTRATOR ☐ ORGANIZATION/COMPANY ADMINISTRATOR

b. PERMISSIONS - FINGERPRINT ENROLLMENT

☑ ENROLLER ☐ TRANSACTION VIEWER ☐ ENROLLER SITE ADMINISTRATOR ☐ ENROLLER GROUP ADMINISTRATOR

c. ADDITIONAL CAGE/ORGANIZATION CODE(S): _____ ☐ OTHER: _____

16. JOINT CLEARANCE ACCESS VERIFICATION SYSTEM (JCAVS) (GOVERNMENT/INDUSTRY)

a. TYPE OF ACCOUNT REQUESTED: ☐ ACCOUNT MANAGER

b. ACCESS REQUESTED - INDUSTRY:		**c. ACCESS REQUESTED - GOVERNMENT ONLY:**	
☐ 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 MGR/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

d. PERMISSION REQUESTED: ☐ INITIATE PSI ☐ REVIEW e-QIP ☐ OVERRIDE PSI ☐ APPROVE e-QIP

NAME *(LAST NAME, FIRST NAME, MIDDLE INITIAL)* _____

17. JOINT ADJUDICATION MANAGEMENT SYSTEM (JAMS) (CAF ONLY)

a. USER ROLES

CAF: _____ CAF TEAM: _____ EMPLOYEE CODE: _____

b. ACCESS REQUESTED:

- ☐ ACCOUNT MANAGER
- ☐ MANAGER
- ☐ COMPUTER ANALYST
- ☐ CASE ASSIGNMENT PERSONNEL
- ☐ SECURITY ASSISTANT
- ☐ CUSTOMER SUPPORT
- ☐ ADJUDICATOR
- ☐ MANAGEMENT SUPPORT
- ☐ PENDING USER
- ☐ SUPERVISOR
- ☐ MAILROOM

c. USER PERMISSIONS:

- ☐ SAP
- ☐ SCI
- ☐ TS
- ☐ SECRET
- ☐ REPORTS
- ☐ JCAVS
- ☐ LAA
- ☐ CASE MANAGEMENT
- ☐ UPDATE CASE COMPONENT
- ☐ ASSIGN CAF CASES
- ☐ REVIEW REQUIRED
- ☐ REASSIGN TO OTHER CAF
- ☐ ASSIGN/REASSIGN CASES
- ☐ REASSIGN FROM OTHER EMPLOYEE

d. SPECIAL CASE USER CAN HANDLE ☐ CAF EMPLOYEES ☐ PRESIDENTIAL SUPPORT ☐ GS-15/GENERAL OFFICER

e. INVESTIGATION REQUEST PERMISSIONS ☐ REVIEW PSQ ☐ APPROVE e-QIP

PART 3 - TRAINING

I HAVE COMPLETED AND ATTACHED TRAINING CERTIFICATES FOR:

18. ☑ **CYBER AWARENESS TRAINING** DATE *(YYYYMMDD)* _____

19. ☑ **PERSONALLY IDENTIFIABLE INFORMATION TRAINING** DATE *(YYYYMMDD)* _____

20. ☐ **JPAS TRAINING REQUIREMENTS** *(IF REQUESTING A JPAS ACCOUNT)* DATE *(YYYYMMDD)* _____

PART 4 - APPLICANT'S CERTIFICATION

I hereby certify that I understand that by signing this Personnel Security System Access Request, I am solely responsible for the use and protection of the account that I will be provided. I also understand that I am not authorized to share my account or logon credentials 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. I understand that if I violate any account management policy, security policy, U.S. laws or DoD regulations, my account will immediately be terminated, I will no longer be responsible for an account, and may be subject to criminal charges and penalties.

21. APPLICANT'S SIGNATURE	**22. DATE** *(YYYYMMDD)*

PART 5 - NOMINATING OFFICIAL'S CERTIFICATION

I certify that the above named individual meets the requirements for access, has the appropriate need-to-know, and if applicable, meets the requirements for account management privileges. I am also aware that I am responsible for ensuring this individual will follow all account policies, security policies, and all applicable DoD regulations and U.S. laws. Furthermore, I certify that the named Applicant requires account access as indicated above in order to perform assigned duties. **These duties include:**

Fingerprint enrollment and submission for Major Command: Location:
SON: SOI: IPAC:
Scanner Make: Model: S/N:

23. NOMINATING OFFICIAL'S PRINTED NAME *(LAST, FIRST, MIDDLE INITIAL)*	**24. NOMINATING OFFICIAL'S SIGNATURE AND DATE**
25. NOMINATING OFFICIAL'S TITLE	**26. NOMINATING OFFICIAL'S TELEPHONE NUMBER**

PART 6 - VALIDATING OFFICIAL'S VERIFICATION

I have verified that minimum investigative requirements for the above Applicant have been met and the Applicant has the necessary need-to-know to access the Personnel Security Systems requested.

27. ELIGIBILITY/ACCESS LEVEL:	**28. TYPE OF INVESTIGATION:**
29. ELIGIBILITY GRANTED DATE:	**30. DATE INVESTIGATION COMPLETED:**
31. ELIGIBILITY ISSUED BY:	**32. INVESTIGATION CONDUCTED BY:**
33. VALIDATING OFFICIAL'S PRINTED NAME *(LAST, FIRST, MIDDLE INITIAL)*	**34. VALIDATING OFFICIAL'S SIGNATURE AND DATE**

PERSONNEL SECURITY SYSTEM ACCESS REQUEST (PSSAR) INSTRUCTIONS

Please see the respective System Access Request Procedures available from the DMDC PSA website for supplemental guidance on completing and submitting this form.

Name. Last Name, First Name, Middle Initial of Applicant. If no middle initial, enter "NMN."

Type of Request. Select "initial" for a new account, "modification" for a change in privileges to an existing account, "deactivate" to remove all access and disable an existing account. Complete the User ID field if selecting "modification" or "deactivate."

Date. Date request is submitted.

Part 1 - Personal Information.

1. Name. Last Name, First Name, Middle Initial of Applicant. If no middle initial, enter "NMN."

2. Organization. Employing organization of Applicant.

3. Office Symbol/Department. Employing office symbol or department.

4. Telephone. Telephone number of Applicant. Enter DSN or Commercial as appropriate.

5. Official E-mail Address. Official e-mail address of Applicant to be used for account communication.

6. Job Title and Grade/Rank. Job title and pay grade or military rank of Applicant.

7. Official Mailing Address. Official mailing address of Applicant.

8. Citizenship. Country of citizenship. If dual, enter both countries.

9. Date of Birth. Applicant's date of birth.

10. Place of Birth. City and state, if born in the U.S. Otherwise, enter country and city.

11. Social Security Number. SSN of Applicant.

12. CAGE Code. Contractor only: CAGE code of Applicant.

13. Designation of Applicant. Mark (X) the appropriate box for DoD (e.g., military branches, DoD agencies, DoD contractor companies), non-DoD NISP partner or non-DoD affiliated.

Part 2 - Applications.

14. Defense Central Index of Investigations (DCII). Government applicants only.

14.a. DCII Agency Code/DCII Agency Acronym. Complete if requesting a DCII account. Provide the DCII Agency Code/DCII Agency Acronym if previously assigned by DCII Administrator and known. Otherwise, contact DMDC Contact Center for assistance

14.b. User Permissions. Requested user permissions are restricted to those granted to the Agency. Elevated permissions for the Agency must be requested from DCII Program Manager.

15. Secure Web Fingerprint Transmission (SWFT). For Government and Industry applicants.

15.a. Permissions - Fingerprint Submission. Applies to SWFT users. Indicate the requested user permission(s) by marking the appropriate checkbox, or list in item 15.c. on line "Other.

15.b. Permissions - Fingerprint Enrollment. Indicate the requested user permission(s) by marking the appropriate checkbox. Only complete this section if you possess or requested a SWFT account (Government only) and are cleared to use the web-based fingerprint enrollment system.

15.c. Additional CAGE Code(s). List only if different from item 12 of this form. Cannot add CAGE or Organization code(s) to account with Multi-Site Uploader permission. The Nominating Official must have the authority to permit the use of the CAGE Code(s) by Applicant.

16. Joint Clearance and Access Verification System (JCAVS). For Government and Industry applicants.

16.a. Type of Account Requested. Select "Account Manager" only if Applicant is to manage JCAVS accounts on behalf of the organization/ company/service.

16.b. Access Requested - Industry. Select appropriate permission(s).

16.c. Access Requested - Government Only. Select appropriate permission(s).

16.d. Permissions Requested. Select appropriate permission(s).

17. Joint Adjudication Management System (JAMS). CAF only.

17.a. JAMS User Roles. Provide information and select appropriate boxes for user functions, access and permissions. JAMS is only authorized for CAFs.

17.b. Access Requested. JAMS access requested.

17.c. User Permissions. JAMS user permission(s).

17.d. Special Case User Can Handle. Select high priority cases JAMS user can handle.

17.e. Investigation Request Permissions. Select Investigation Request permissions for JAMS user.

Part 3 - Training.

18. - 20. Training Requirements. Mark (X) the box to certify training was completed and enter the completion date for all new accounts. Training requirements are defined in the respective System Account Management Policies available from the DMDC PSA website. Certificates must be submitted with PSSAR.

Part 4 - Applicant's Certification.

21. Applicant's Signature. Signature of Applicant acknowledging DoD and system policies.

22. Date. Date application signed by Applicant.

Part 5 - Nominating Official's Certification.

23. Nominating Official's Name. Last Name, First Name, and Middle Initial. If no middle initial, enter "NMN."

24. Nominating Official's Signature and Date. The Nominating Official is the individual who is authorizing that the Applicant should have the access requested. For Industry, the Nominating Official must be listed in ISFD as a Key Management Personnel (KMP) in connection with the Facility Clearance, and if an Appointment Letter is needed, it must be signed by the same KMP. The Nominating Official CANNOT be the same as the Applicant unless it is a single person facility. For Government/Civilian, the Nominating Official must be the Security Officer/ Manager.

NOTE: PSSARs submitted without the Nominating Official's statement regarding *duties and signature* will not be processed.

25. Nominating Official's Title. Title of Nominating Official.

26. Nominating Official's Telephone Number. DSN or Commercial telephone number of Nominating Official.

Part 6 - Validating Official's Verification. Do not complete if self-nominating/validating.

27. Eligibility/Access Level. Eligibility/Access level of Applicant. See applicable System Account Management Policies/Access Request Procedures available from the respective DMDC PSA system website for minimum eligibility/ access requirements.

28. Type of Investigation. Type of investigation completed for Applicant.

29. Eligibility Granted Date. Date eligibility granted. If not final, state date of interim.

30. Date Investigation Completed. Date investigation completed.

31. Eligibility Issued By. Organization that issued eligibility.

32. Investigation Conducted By. Investigating agency.

33. Validating Official's Printed Name. Last Name, First Name, and Middle Initial. If no middle initial, enter "NMN."

34. Validating Official's Signature and Date. The Validating Official signature serves to affirm the information provided on the following lines (verify before signing): Eligibility/Access Level; Eligibility Granted Date; Eligibility 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.

Return completed forms to the appropriate Account Manager or the DMDC Contact Center as outlined in the respective System Access Request Procedures available from the DMDC PSA website.