NAME *(Last Name, First Name, Middle Initial)* _____

# PERSONNEL SECURITY SYSTEM ACCESS REQUEST (PSSAR)
## DEFENSE MANPOWER DATA CENTER (DMDC)

*OMB No. 0704-0496*
*OMB approval expires Mar 31, 2016*



**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/SORNs/blanket_routine_uses.html 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** — **DATE** *(YYYYMMDD)*

INITIAL ☐ MODIFICATION ☐ DEACTIVATE ☐ USER ID _____

### PART 1 *(To be completed by Applicant)* - PERSONAL INFORMATION

| | | |
|---|---|---|
| **1. NAME** *(Last, First, Middle Initial)* | **2. ORGANIZATION** | |
| **3. OFFICE SYMBOL/DEPARTMENT** | **4. PHONE** *(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** | **11. SOCIAL SECURITY NUMBER** | **12. CAGE CODE** *(NISP CTR ONLY)* |

**13. DESIGNATION OF PERSON**

☐ DoD MILITARY ☐ DoD CIVILIAN ☐ DoD CONTRACTOR ☐ NON-DoD NISP ☐ NON-DoD

### PART 2 *(To be completed by Applicant)* - TRAINING

**14.** ☐ **I have completed Annual Information Awareness Training.** DATE *(YYYYMMDD)*_____

**15.** ☐ **I have completed Personally Identifiable Information Training.** DATE *(YYYYMMDD)*_____

**16.** ☐ **I have completed JPAS Training Requirements** *(if requesting a JPAS account)*. DATE *(YYYYMMDD)*_____

### PART 3 *(To be completed by Applicant)* - APPLICATIONS

**17. DEFENSE CENTRAL INDEX OF INVESTIGATIONS (DCII)**

**AGENCY CODE**_____ **OR AGENCY ACRONYM** _____

**USER** *(Select Permissions Below)*

QUERY (SEARCH) ☐ DELETE ☐

ADD ☐ UPDATE ☐

**FILE DEMAND** *(Provide Accreditation Code)*: _____

FILE DEMAND PRINT ☐ EXECUTIVE ADMINISTRATOR ☐

AGENCY ADMINISTRATOR ☐ IA (ROOT) ADMINISTRATOR ☐

**18. SECURE WEB FINGERPRINT TRANSMISSION (SWFT)**

**CAGE CODE(S):** _____

☐ USER ☐ MULT. COMPANY UPLOADER ☐ ACCOUNT MANAGER ☐ EXECUTIVE ACCOUNT MANAGER ☐ SWFT ADMINISTRATOR

**19. JOINT CLEARANCE ACCESS VERIFICATION SYSTEM (JCAVS)**

**TYPE OF ACCOUNT REQUESTED:** ☐ ACCOUNT MANAGER ☐ USER

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

NAME *(Last Name, First Name, Middle Initial)* _____

| **20. ACCESS REQUESTED - INDUSTRY:** | | **21. 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 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 |

**22. JOINT ADJUDICATION MANAGEMENT SYSTEM (JAMS) USER ROLES (DoD/NON-INDUSTRY ONLY)**

CAF: CAF TEAM: EMPLOYEE CODE:

| **23. ACCESS REQUESTED:** | | **24. USER PERMISSIONS:** | |
|---|---|---|---|
| ☐ ACCOUNT MANAGER | ☐ CUSTOMER SUPPORT | ☐ SAP | ☐ CASE MANAGEMENT |
| ☐ MANAGER | ☐ ADJUDICATOR | ☐ SCI | ☐ UPDATE CASE COMPONENT |
| ☐ COMPUTER ANALYST | ☐ MANAGEMENT SUPPORT | ☐ TS | ☐ ASSIGN CAF CASES |
| ☐ CASE ASSIGNMENT PERSONNEL | ☐ PENDING USER | ☐ SECRET | ☐ REVIEW REQUIRED |
| | | ☐ REPORTS | ☐ REASSIGN TO OTHER CAF |
| ☐ SECURITY ASSISTANT | ☐ SUPERVISOR | ☐ JCAVS | ☐ ASSIGN/REASSIGN CASES |
| | ☐ MAILROOM | ☐ LAA | ☐ REASSIGN FROM OTHER EMPLOYEE |

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

**26. INVESTIGATION REQUEST PERMISSIONS:** ☐ REVIEW PSQ ☐ APPROVE e-QIP

**PART 4** *(To be completed by Applicant)* **- 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.

| **27. APPLICANT'S SIGNATURE** | **28. 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:

| **29. NOMINATING OFFICIAL'S PRINTED NAME** *(Last, First, Middle Initial)* | **30. NOMINATING OFFICIAL'S SIGNATURE AND DATE** |
|---|---|
| **31. NOMINATING OFFICIAL'S TITLE** | **32. 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.

| **33. CLEARANCE LEVEL:** | **34. TYPE OF INVESTIGATION:** |
|---|---|
| **35. CLEARANCE GRANTED DATE:** | **36. DATE INVESTIGATION COMPLETED:** |
| **37. CLEARANCE ISSUED BY:** | **38. INVESTIGATION CONDUCTED BY:** |
| **39. VALIDATING OFFICIAL'S PRINTED NAME** *(Last, First, Middle Initial)* | **40. VALIDATING OFFICIAL'S SIGNATURE AND DATE** |

## PERSONNEL SECURITY SYSTEM ACCESS REQUEST (PSSAR) INSTRUCTIONS

**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. Phone.** 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 U.S. citizen. Otherwise, enter country and city.

**11. Social Security Number.** SSN of Applicant.

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

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

### Part 2 - Training.

**14. - 16. 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.

### Part 3 - Applications.

**17. Agency Code/Agency Acronym.** Complete if requesting a DCII account.
**User:** Complete if requesting a DCII account.
**File Demand:** Complete if requesting a DCII account.

**18. CAGE Code(s).** CAGE code(s) of Applicant.

**19. Type of Account Requested.** Select "Account Manager" only if Applicant is to manage JCAVS accounts on behalf of the organization/ company service.
**Permissions Requested:** Select appropriate permission(s).

**20. Access Requested - Industry.** Select appropriate permission(s).

**21. Access Requested - Non-Industry.** Select appropriate permission(s).

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

**23. Access Requested.** JAMS access requested.

**24. User Permissions.** JAMS user permission(s).

**25. Special Case User Can Handle.** Select high priority cases JAMS user can handle.

**26. Investigation Request Permissions.** Select Investigation Request permissions for JAMS user.

### Part 4 - Applicant's Certification.

**27. Applicant's Signature.** Signature of Applicant acknowledging DoD and system policies.

**28. Date.** Date application signed by Applicant.

### Part 5 - Nominating Official's Certification.

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

**30. Nominating Official's Signature and Date.** The Nominating Official is the individual who is authorizing that the Applicant should have the access requested. The Nominating Official may be a Corporate Officer (KMP) listed in ISFD, Facility Security Officer, or Security Officer/Manager. For JCAVS Industry Account Managers, the PSSAR must be signed by the same KMP who signed the Appointment Letter. The Nominating Official CANNOT be the same as the Applicant unless it is a single person facility.
**NOTE:** PSSARs submitted without the Nominating Official's statement regarding duties and signature will not be processed.

**31. Nominating Official's Title.** Title of Nominating Official.

**32. Nominating Official's Phone Number.** DSN or Commercial telephone number of Nominating Official.

### Part 6 - Validating Official's Verification.

**33. Clearance Level.** Clearance level of individual. See applicable System Account Management Policies/Access Request Procedures available from the respective DMDC PSA system website for minimum clearance requirements.

**34. Type of Investigation.** Type of investigation completed for Applicant.

**35. Clearance Granted Date.** Date clearance granted. If not final, state date of interim.

**36. Date Investigation Completed.** Date investigation completed.

**37. Clearance Issued By.** Organization that issued clearance.

**38. Investigation Conducted By.** Investigating agency.

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

**40. Validating Official's Signature and Date.** The Validating Official signature serves to affirm the information provided on the following lines (verify before 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.

**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.**