Name *(Last, First, Middle Initial)*:

PERSONNEL SECURITY SYSTEM ACCESS REQUEST (PSSAR)
DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY (DCSA)

OMB No. 0704-0542
OMB approval expires XXXXXXXX

PRIVACY ACT STATEMENT

AUTHORITY: E.O. 12829, National Industrial Security Program; E.O. 10450, Security Requirements for Government Employment; E.O. 10865, Safeguarding Classified Information Within Industry; (DoDI) 1400.25, Volume 731, DoD Civilian Personnel Management System: Suitability and Fitness Adjudication for Civilian Employees; DoDM 5200.02, Procedures for the DoD Personnel Security Program; DoDI 5200.02, DoD Personnel Security Program (PSP); DoDD 5220.6, Defense Industrial Personnel Security Clearance Review Program; DoDI 5220.22, National Industrial Security Program (NISP); DoDI 5200.46, DoD Investigative and Adjudicative Guidance for Issuing the Common Access Card (CAC); Homeland Security Presidential Directive (HSPD) 12, Policy for Common Identification Standard for Federal Employees and Contractors; and E.O. 9397 (SSN), as amended.

PURPOSE(S): To request the establishment of user roles and access and validate the trustworthiness of individuals seeking access to Defense Central Index of Investigations (DCII), DoD Secure Web Fingerprint Transmission (SWFT), DoD Defense Information system for Security (DISS) or National Background Investigation Services (NBIS).

ROUTINE USE(S): Disclosure of records are generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended. See the appropriate System of Records Notice for the applicable routine uses: A complete list of the routine uses can be found in the system of records notice for the Department of Defense Personnel Vetting Records System, "DUSDI 02-DoD" at: https://www.federalregister.gov/documents/2018/10/17/2018-22508/privacy-act-of-1974-system-of-records; DUSDI 02-DoD, Personnel Vetting Records System at: http://dpcld.defense.gov/Privacy/SORNsIndex/DOD-Component-Notices/OSDJS-Article-List/

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.

PART 1 - 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 *(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)*

TYPE OF REQUEST

☐ **INITIAL** ☐ **MODIFICATION** ☐ **DEACTIVATE**

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)

TYPE OF REQUEST

☐ **INITIAL** ☐ **MODIFICATION** ☐ **DEACTIVATE**

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**

Name *(Last, First, Middle Initial)*:

16. DEFENSE INFORMATION SYSTEM FOR SECURITY - JOINT VERIFICATION SYSTEM (DISS-JVS)

TYPE OF REQUEST

☐ **INITIAL** ☐ **MODIFICATION** ☐ **DEACTIVATE**

a. SMO NAME: **ORGANIZATION/AGENCY CODE:**

b. ROLE REQUESTED AND OPTIONAL PERMISSIONS *(Mark All That Apply):*

☐ **SECURITY OFFICER**
- ☐ MANAGE POLYGRAPH
- ☐ VIEW SCI ACCESS
- ☐ MANAGE SCI ACCESS
- ☐ REVIEW INVESTIGATION REQUEST

☐ **COMPONENT ADJUDICATOR**

☐ **HUMAN RESOURCE MANAGER**

☐ **PHYSICAL ACCESS CONTROL**
- ☐ VIEW SCI ACCESS

☐ **PRIVACY OFFICER**

☐ **HELP DESK**

☐ **OTHER ROLES AND PERMISSIONS**

☐ **SECURITY OFFICER ADMIN**
- ☐ UPDATE SUBJECT INFORMATION
- ☐ GRANT NON-SCI ACCESS
- ☐ REMOVE NON-SCI ACCESS
- ☐ ESTABLISH SUBJECT RELATIONSHIP
- ☐ MANAGE FOREIGN RELATIONSHIPS
- ☐ REMOVE SUBJECT RELATIONSHIP
- ☐ CREATE VISIT
- ☐ VIEW VISIT
- ☐ SUSPEND ACCESS
- ☐ MANAGE TASKS
- ☐ MANAGE POLYGRAPH
- ☐ VIEW SCI ACCESS
- ☐ MANAGE SCI ACCESS
- ☐ VIEW SMO NOTIFICATIONS
- ☐ MANAGE FOREIGN TRAVEL
- ☐ MODIFY VISIT

☐ **SECURITY OFFICER VISIT ADMIN**
- ☐ VIEW SUBJECT LIST
- ☐ VIEW SCI ACCESS
- ☐ ESTABLISH SUBJECT RELATIONSHIP
- ☐ REMOVE SUBJECT RELATIONSHIP

☐ **SECURITY MANAGER**
- ☐ MANAGE POLYGRAPH
- ☐ VIEW SCI ACCESS
- ☐ MANAGE SCI ACCESS
- ☐ REVIEW INVESTIGATION REQUEST

☐ **HIERARCHY MANAGER**
- ☐ VIEW SCI ACCESS
- ☐ MANAGE SCI DISS USER

☐ **ACCOUNT MANAGER**
- ☐ VIEW SCI ACCESS
- ☐ MANAGE SCI DISS USER

☐ **APPLICATION ADMIN**

EXPLAIN OTHER

17. DEFENSE INFORMATION SYSTEM FOR SECURITY - CASE ADJUDICATION TRACKING SYSTEM (DISS - CATS)

TYPE OF REQUEST

☐ **INITIAL** ☐ **MODIFICATION** ☐ **DEACTIVATE**

a. APPLICATION LOCATION: ORGANIZATION DIVISION BRANCH TEAM

b. ROLE REQUESTED:

☐ EXECUTIVE CHIEF	☐ ADJUDICATOR	☐ PE SCREENER	☐ PROCESS TEAM
☐ DIVISION CHIEF	☐ TRAINEE	☐ GENERAL COUNSEL	☐ INDUSTRY PROCESS TEAM
☐ BRANCH CHIEF	☐ IT SCREENER 1	☐ OPM LIAISON	☐ QUALITY CONTROL
☐ TEAM CHIEF	☐ IT SCREENER 2	☐ METRICS	☐ PRIVACY OFFICER
☐ CV SCREENER	☐ IT SCREENER 3	☐ ADMINISTRATOR	

c. LIST ANY ELEVATED PERMISSIONS:

Name *(Last, First, Middle Initial)*:

18. DEFENSE INFORMATION SYSTEM FOR SECURITY - APPEALS

TYPE OF REQUEST

☐ **INITIAL** ☐ **MODIFICATION** ☐ **DEACTIVATE**

a. APPLICATION LOCATION: ORGANIZATION DIVISION BRANCH TEAM

b. ROLE REQUESTED AND OPTIONAL PERMISSIONS *(Mark All That Apply)*:

☐ **DOHA ADMIN** ☐ **PSAB ADMIN** ☐ **PSAB BOARD MEMBER** ☐ **PRIVACY OFFICER**

☐ MANAGE APPEALS USER ☐ MANAGE APPEALS USER ☐ **HELP DESK** ☐ **APPLICATION ADMIN**

19. NATIONAL BACKGROUND INVESTIGATION SERVICES (NBIS)

TYPE OF REQUEST

☐ **INITIAL** ☐ **MODIFICATION** ☐ **DEACTIVATE**

a. ROLE REQUESTED:

☐ SYSTEM MANAGER ☐ AUTHORIZER (GOVERNMENT ONLY) ☐ WORKFLOW MANAGER ☐ BUSINESS PROCESS MANAGER

☐ INTERNAL ORG MANAGER ☐ NBIS FINANCIAL MANAGER ☐ INITIATOR ☐ ORG MANAGER

☐ WORKLOAD MANAGER ☐ FINANCIAL MANAGER ☐ POINT OF CONTACT ☐ REVIEWER

☐ USER MANAGER ☐ INTERNAL USER MANAGER ☐ NOTIFICATION MANAGER ☐ ORDER FORM TEMPLATE MANAGER

☐ OTHER

b. LIST ANY ELEVATED PERMISSIONS:

PART 3 - TRAINING *(I have completed and attached training certificates for):*

20. ☐ CYBER AWARENESS TRAINING **DATE** (*YYYYMMDD)*

21. ☐ PERSONALLY IDENTIFIABLE INFORMATION TRAINING **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, and may be subject to criminal charges and penalties.

22. APPLICANT'S SIGNATURE	**23. DATE** *(YYYYMMDD)*

Name *(Last, First, Middle Initial)*:

PART 5 - NOMINATING OFFICIAL'S CERTIFICATION

24. 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.

25. NOMINATING OFFICIAL'S PRINTED NAME *(Last, First, Middle Initial)*	26. NOMINATING OFFICIAL'S TITLE

27. NOMINATING OFFICIAL'S TELEPHONE NUMBER	28. NOMINATING OFFICIAL'S SIGNATURE	29. NOMINATING OFFICIAL'S SIGNATURE DATE

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.

30. ELIGIBILITY/ACCESS LEVEL:	31. TYPE OF INVESTIGATION:
32. ELIGIBILITY GRANTED DATE:	33. DATE INVESTIGATION COMPLETED:
34. ELIGIBILITY ISSUED BY:	35. INVESTIGATION CONDUCTED BY:

36. VALIDATING OFFICIAL'S PRINTED NAME *(Last, First, Middle Initial):*

37. VALIDATING OFFICIAL'S SIGNATURE *(Last, First, Middle Initial):*	38. VALIDATING OFFICIAL'S SIGNATURE DATE

Name *(Last, First, Middle Initial)*:

PART 7 - PERSONNEL SECURITY SYSTEM ACCESS REQUEST (PSSAR) INSTRUCTIONS

Please see the respective Account Management Policy available from the DCSA website for supplemental guidance on completing and submitting this form.

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. Enter User ID if selecting "modification" or "deactivate."

Date. Date request is submitted by applicant.

Part 1 - Personal Information.

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

2. Organization. Employing organization or company name of applicant.

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

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 born in the U.S. Otherwise, enter city and country.

11. Social Security Number. Social Security Number (SSN) is required.

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

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

Part 2 - **Applications**.

14. DCII.

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.

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. SWFT.

a. Permissions - Fingerprint Submission. Applies to SWFT users. Indicate the requested user permission(s) by marking the appropriate box, or list in Item.

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

c. Additional CAGE Code(s). List only if different from box 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. DISS (JVS).

a. SMO Name or Organization/Agency Code. Security Management Office name or Organization/Agency code.

b. Role Requested and Optional Permissions. Indicate the requested user role(s) by marking the appropriate box, along with any optional permissions requested.

17. DISS (CATS).

a. **Application Location.** Organization Name, Division Name, Branch Name, Team Name.

b. **Role Requested**. Indicate the requested user role(s) by marking the appropriate box.

c. **List any Elevated Permission(s)**. This information is requested by the user.

18. **DISS - APPEALS**.

a. Application Location. Organization Name, Division Name, Branch Name, Team Name.

b. Role Requested. Indicate requested user role(s) by marking the appropriate box, along with any optional permission requested.

19. NBIS.

a.Role Requested. User Role being requested for system access.

b.Elevated Permissions. Optional permissions for requested roles.

Part 3 - Training.

20 - 21. Training Requirements. Mark in the box to certify training units completed and enter completion date for new accounts. Certificates must be submitted with PSSAR within one year of training completion date.

Part 4 - Applicant's Certification.

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

23. Date. Date application signed by Applicant.

Part 5 - Nominating Official's Certification.

24. Nominating Official's Certification Statement.

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

26. Nominating Official's Title. Title of Nominating Official.

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

28. Nominating Official's Signature. Nominating Official's Signature. The Nominating Official is the individual who is authorizing that the Applicant should have the access requested. The Nominating Official must be a Key Management Personnel (KMP) listed in NISS, Facility Security Officer, or Security Officer/Manager. The Nominating Official CANNOT be the same as the Applicant unless it is a single person facility.

29. Nominating Official's Signature Date.

Part 6 - Validating Official's Verification.

Do not complete if self-nominating/validating.

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

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

32. Eligibility Granted Date. Date clearance granted, indicating if interim. If not final, state date of interim.

33. Date Investigation Completed. Date investigation completed.

34. Eligibility Issued By. Organization that issued clearance.

35. Investigation Conducted By. Investigating agency.

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

37. Validating Official's Signature. The Validating Official signature serves to affirm the information provided on the following lines (verify before signing): Eligibility/Access Level; Eligibility Issued By; Type of Investigation and Investigation Conducted By. For non-DoD government agency requests, the Chief of Security or designee must complete this section.

38. Validating Official's Signature Date. Date Investigation Completed.