

Name (Last, First, Middle Initial):

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

 OMB No. 0705-0009
 OMB approval expires
 20250131

The public reporting burden for this collection of information, 0704-0542, is estimated to average 10 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding the burden estimate or burden reduction suggestions to the Department of Defense, Washington Headquarters Services, at whs.mc-alex.esd.mbx.dd-dod-information-collections@mail.mil. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS. Return completed form to the appropriate Account Manager or DCSA Contact Center, as indicated in the instructions.

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 (NIS); 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://dpclid.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 <input type="checkbox"/> MILITARY <input type="checkbox"/> DoD CIVILIAN <input type="checkbox"/> INDUSTRY <input type="checkbox"/> NON-DoD			

PART 2 - APPLICATIONS

14. DEFENSE CENTRAL INDEX OF INVESTIGATIONS (DCII) (GOVERNMENT ONLY)			
TYPE OF REQUEST			
<input type="checkbox"/> INITIAL <input type="checkbox"/> MODIFICATION <input type="checkbox"/> DEACTIVATE			
a. DCII AGENCY CODE		OR DCII AGENCY ACRONYM	
b. USER PERMISSIONS:			
<input type="checkbox"/> QUERY (Search) <input type="checkbox"/> ADD <input type="checkbox"/> UPDATE <input type="checkbox"/> DELETE <input type="checkbox"/> AGENCY ADMINISTRATOR <input type="checkbox"/> EXECUTIVE ADMINISTRATOR			
<input type="checkbox"/> FILE DEMAND (Provide Accreditation Code):		<input type="checkbox"/> FILE DEMAND PRINT <input type="checkbox"/> IA (ROOT ADMINISTRATOR)	
15. SECURE WEB FINGERPRINT TRANSMISSION (SWFT)			
TYPE OF REQUEST			
<input type="checkbox"/> INITIAL <input type="checkbox"/> MODIFICATION <input type="checkbox"/> DEACTIVATE			
a. PERMISSIONS - FINGERPRINT SUBMISSION:			
<input type="checkbox"/> USER <input type="checkbox"/> MULTI-SITE UPLOADER <input type="checkbox"/> SITE ADMINISTRATOR <input type="checkbox"/> ORGANIZATION/COMPANY ADMINISTRATOR			
b. PERMISSIONS - FINGERPRINT ENROLLMENT:			
<input type="checkbox"/> ENROLLER <input type="checkbox"/> TRANSACTION VIEWER <input type="checkbox"/> ENROLLER SITE ADMINISTRATOR <input type="checkbox"/> ENROLLER GROUP ADMINISTRATOR			
c. ADDITIONAL CAGE/ORGANIZATION CODE(S):			<input type="checkbox"/> 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):

- | | | |
|---|--|---|
| <input type="checkbox"/> SECURITY OFFICER | <input type="checkbox"/> SECURITY OFFICER ADMIN | <input type="checkbox"/> SECURITY MANAGER |
| <input type="checkbox"/> MANAGE POLYGRAPH | <input type="checkbox"/> UPDATE SUBJECT INFORMATION | <input type="checkbox"/> MANAGE POLYGRAPH |
| <input type="checkbox"/> VIEW SCI ACCESS | <input type="checkbox"/> GRANT NON-SCI ACCESS | <input type="checkbox"/> VIEW SCI ACCESS |
| <input type="checkbox"/> MANAGE SCI ACCESS | <input type="checkbox"/> REMOVE NON-SCI ACCESS | <input type="checkbox"/> MANAGE SCI ACCESS |
| <input type="checkbox"/> REVIEW INVESTIGATION REQUEST | <input type="checkbox"/> ESTABLISH SUBJECT RELATIONSHIP | <input type="checkbox"/> REVIEW INVESTIGATION REQUEST |
| <input type="checkbox"/> COMPONENT ADJUDICATOR | <input type="checkbox"/> MANAGE FOREIGN RELATIONSHIPS | <input type="checkbox"/> HIERARCHY MANAGER |
| <input type="checkbox"/> HUMAN RESOURCE MANAGER | <input type="checkbox"/> REMOVE SUBJECT RELATIONSHIP | <input type="checkbox"/> VIEW SCI ACCESS |
| <input type="checkbox"/> PHYSICAL ACCESS CONTROL | <input type="checkbox"/> CREATE VISIT | <input type="checkbox"/> MANAGE SCI DISS USER |
| <input type="checkbox"/> VIEW SCI ACCESS | <input type="checkbox"/> VIEW VISIT | <input type="checkbox"/> ACCOUNT MANAGER |
| <input type="checkbox"/> PRIVACY OFFICER | <input type="checkbox"/> SECURITY OFFICER VISIT ADMIN | <input type="checkbox"/> VIEW SCI ACCESS |
| <input type="checkbox"/> HELP DESK | <input type="checkbox"/> VIEW SUBJECT LIST | <input type="checkbox"/> MANAGE SCI DISS USER |
| <input type="checkbox"/> OTHER ROLES AND PERMISSIONS | <input type="checkbox"/> VIEW SCI ACCESS | <input type="checkbox"/> APPLICATION ADMIN |
| | <input type="checkbox"/> ESTABLISH SUBJECT RELATIONSHIP | |
| | <input type="checkbox"/> REMOVE SUBJECT RELATIONSHIP | |

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:

- | | | | |
|--|--|--|--|
| <input type="checkbox"/> EXECUTIVE CHIEF | <input type="checkbox"/> ADJUDICATOR | <input type="checkbox"/> PE SCREENER | <input type="checkbox"/> PROCESS TEAM |
| <input type="checkbox"/> DIVISION CHIEF | <input type="checkbox"/> TRAINEE | <input type="checkbox"/> GENERAL COUNSEL | <input type="checkbox"/> INDUSTRY PROCESS TEAM |
| <input type="checkbox"/> BRANCH CHIEF | <input type="checkbox"/> IT SCREENER 1 | <input type="checkbox"/> OPM LIAISON | <input type="checkbox"/> QUALITY CONTROL |
| <input type="checkbox"/> TEAM CHIEF | <input type="checkbox"/> IT SCREENER 2 | <input type="checkbox"/> METRICS | <input type="checkbox"/> PRIVACY OFFICER |
| <input type="checkbox"/> CV SCREENER | <input type="checkbox"/> IT SCREENER 3 | <input type="checkbox"/> ADMINISTRATOR | |

c. LIST ANY ELEVATED PERMISSIONS:

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.