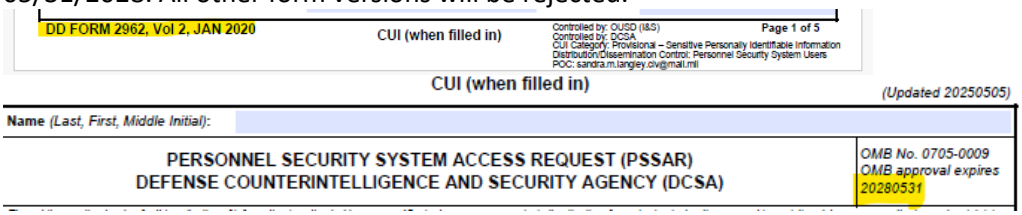
PSSAR Instructions for SWFT Org Admin Access

- Currently DCSA is only accepting the DD 2962 Vol 2, Jan 2020 form with the OMB expiration of 05/31/2028. All other form versions will be rejected.


DD FORM 2962, Vol 2, JAN 2020 CUI (when filled in) Controlled by: OUSD (I&S) Controlled by: DCSA CUI Category: Provisional – Sensitive Personally Identifiable Information Distribution/Dissemination Control: Personnel Security System Users POC: sandra.m.langley.civ@mail.mil Page 1 of 5

CUI (when filled in)

(Updated 20250505)

Name (Last, First, Middle Initial):

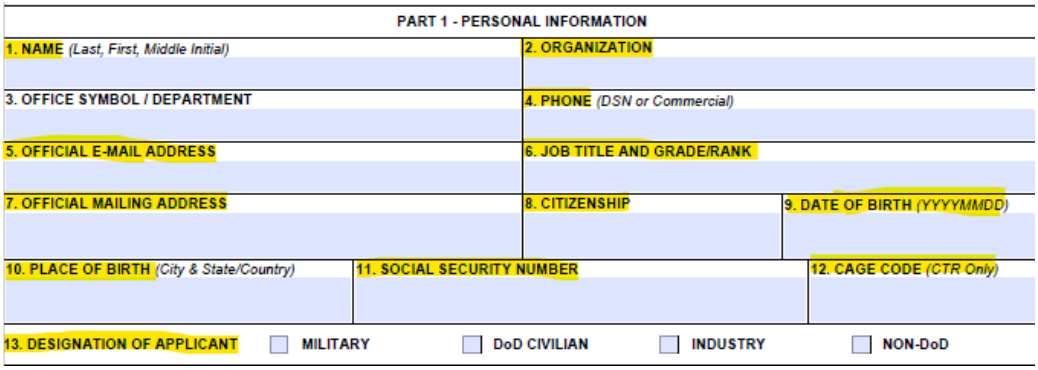
PERSONNEL SECURITY SYSTEM ACCESS REQUEST (PSSAR)
DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY (DCSA)

OMB No. 0705-0009
OMB approval expires 20280531

- Please enter your name at the top of each page


Name (Last, First, Middle Initial):

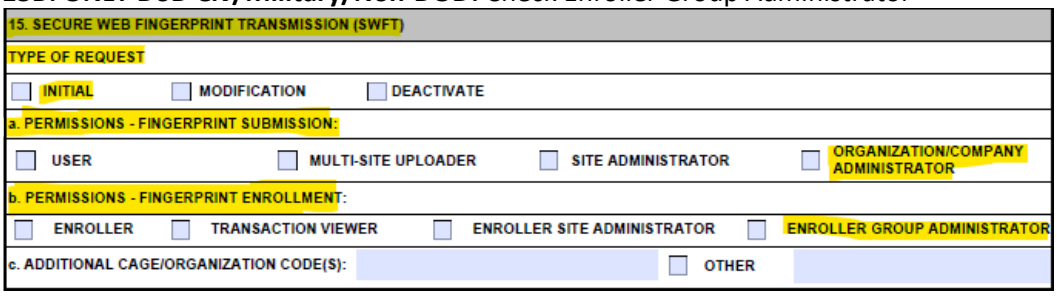
- Part 1: Fill out the highlighted sections
  - **Box 12:**
  - **Non-DOD/Military/DoD Civilian:** Leave this blank.
  - **Industry:** Please enter the cage code for your organization.


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**: Fill out the highlighted sections:
  - **15:** Type of Request; Check initial
  - **15A: ALL AGENCIES** Check Organization/Company Administrator
  - **15B: ONLY DoD Civ/Military/Non-DOD:** Check Enroller Group Administrator


15. SECURE WEB FINGERPRINT TRANSMISSION (SWFT)

TYPE OF REQUEST

☐ INITIAL ☐ MODIFICATION ☐ DEACTIVATE

a. PERMISSIONS - FINGERPRINT SUBMISSION:

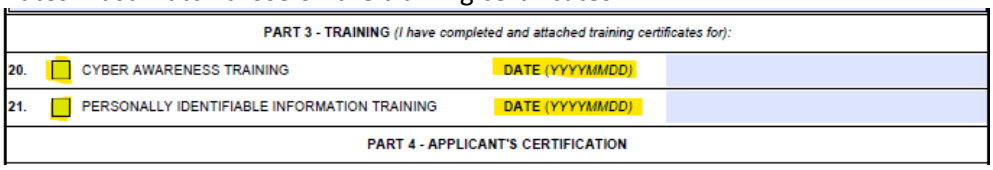
☐ USER ☐ MULTI-SITE UPLOADER ☐ SITE ADMINISTRATOR ☐ ORGANIZATION/COMPANY ADMINISTRATOR

b. PERMISSIONS - FINGERPRINT ENROLLMENT:

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

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

- **Part 3:** Please check the boxes for your completed training and include the dates
  - Dates must match those on the training certificates

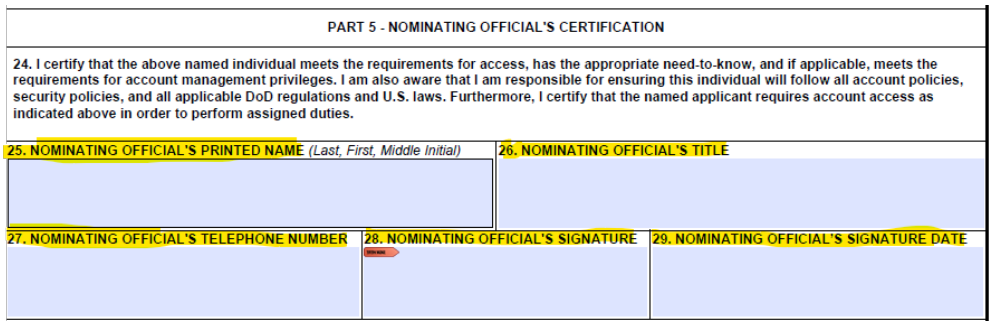


PART 3 - TRAINING *(I have completed and attached training certificates for):*		
20. ☐ CYBER AWARENESS TRAINING	DATE *(YYYYMMDD)*	
21. ☐ PERSONALLY IDENTIFIABLE INFORMATION TRAINING	DATE *(YYYYMMDD)*	
PART 4 - APPLICANT'S CERTIFICATION		

- **Part 4:** Please add your signature and date (This can be an electronic or ink signature)

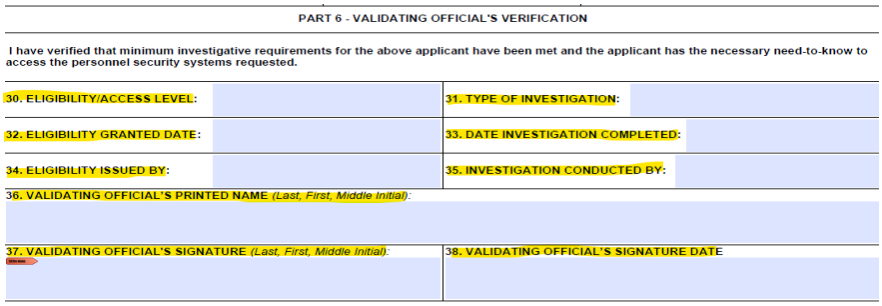
PART 4 - APPLICANT'S CERTIFICATION	
I hereby certify that I understand that by signing this Personnel Security System Access Request, I am solely responsible for the use and protection of the account that I will be provided. I also understand that I am not authorized to share my account or logon credentials 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)

- **Part 5:** Nominating Official:
  - **Industry**: The nominating official completing part 5 must be a KMP and be on the most recent Industry KMP list DCSA has for the organization.
  - **DoD Civ/Military/Non-DOD:** This needs to be someone within your organization that is nominating you for an account.



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: Someone who can verify your Public Trust/National Security investigation (This can also be the same person as your Nominating Official, if applicable.)
  - This **CANNOT** be filled out by the person requesting access.
  - **INDUSTRY ONLY:** If you are a single person facility, please specify this in your response and leave this section blank. A validating official will be found for you by DCSA.



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	

Training Requirements for SWFT Accounts

All SWFT PSSAR submissions must be accompanied by proof of completion of both of the following training courses. **The certificates must indicate that the course was completed within the past 12 months:**

1. Cyber Security Awareness/Information Assurance course (2 options):
   A. DISA training course: https://www.cyber.mil/cyber-awareness-challenge
   B. Training course provided by the cleared service/company/agency.

2. Personally Identifiable Information course (3 options):
   A. DISA training course: DoD Personally Identifiable Information https://www.cyber.mil/training
   B. DSS training course: https://www.cdse.edu/Training/eLearning/DS-IF101
   C. PII training course provided by the cleared company/agency (must be approved by the SWFT PM)

PSSAR Submission Process:
This box cannot receive encrypted emails. Please utilize one of the following options:

Add a password to Microsoft Word Doc
1. First, open the Office document you would like to protect.
2. Click the File menu
3. Select the Info tab
4. Select the Protect Document button
5. **Click Encrypt with Password**. Enter your password then click OK.

Add a password to Adobe Acrobat (pdf)
1. Open the PDF and choose Tools > Protect > Encrypt > Encrypt with Password.
2. If you receive a prompt, click **Yes** to change the security.
3. Select Require a Password to Open the Document, then type the password in the corresponding field

DOD SAFE Option:
1. **INDUSTRY/Non-DoD:** Please reach out to DCSAFTSTeam@mail.mil and request a DOD Safe drop
2. **DoD Civ/Military:** Go to safe.apps.mil and submit a DoD Safe request over to **DCSAFTSTeam@mail.mil**