DISS JVS PSSAR Job Aid for Agencies Needing SSN Look-up

For Establishing an Account Manager and Physical Access Control Users

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

Version 1.0

May 9, 2021

REVISION HISTORY

DATE	VERSION	CHANGE DESCRIPTION	AUTHOR
5/9/2021	1.0	RELEASED ON DCSA TEMPLATE	DCSA

FOR AGENCIES NEEDING *INITIAL* DISS JVS ACCESS FOR *SSN LOOK-UP ONLY*

OVERVIEW

Agencies can establish Defense Information System for Security (DISS) Joint Verification System (JVS) account access to allow Agency users to verify eligibility and access using Social Security Number (SSN) look-up. This job aid is meant to provide guidance to obtain an *initial* Account Manager accounts and Physical Access Control accounts. All users will need to submit the DCSA Personnel Security System Access Request (PSSAR) (DD Form 2962, Vol. 2., Jan. 2020) to be provisioned in DISS JVS. This document is meant to serve as a guide to facilitate making the PSSAR submission and JVS provisioning process as smooth as possible.

Prerequisites to filling out PSSAR

Before submitting a PSSAR, you must submit training certificates showing completion of both Cyber Security Awareness and Personally Identifiable Information(PII) training within the past year by submitting those training certificates with your PSSAR packet, to beprovisioned. The following information is provided for the mandatory training classes/certificates:

- Cyber Awareness Challenge/Information Assurance (IA) Security Training (two options available):
  - The DoD Cyber Exchange's Cyber Awareness Challenge
  - Service, company, or agency approved cyber awareness/IA security training course
- Personnally Identifiable Information (PII) Training (three options available):
  - DoD Cyber Exchange's Identifying and Safeguarding Personally Identifiable Information (PII) Training
  - CDSE's Identifying and Safeguarding Personally Identifiable Information (PII) Course (requires a STEPP account)
  - Service, company, or agency approved PII training course

Note: *Initial* Account Manager submissions to the DCSA DISS Industry Process Team requires the Defense Information Systems Agency (DISA)/DoD Cyber Exchange, or Center for Development of Security Excellence (CDSE) provided courses.

Service, company, or agency approved cyber awareness, IA, and/or PII training course certificates may be used and submitted for new user account provisioning.

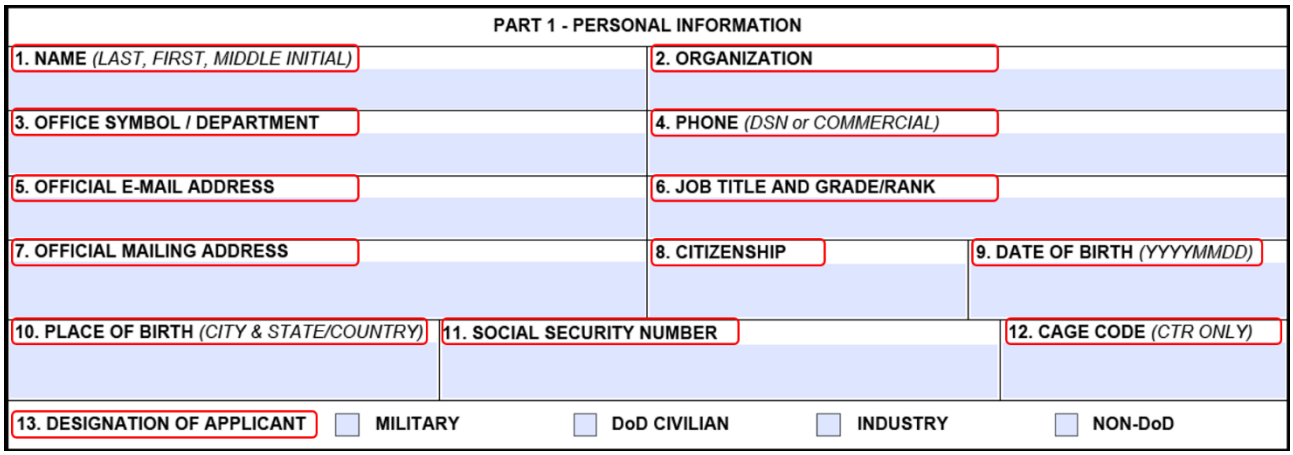
Download Correct PSSAR

The correct JVS account request form is the DD Form 2962, PSSAR, Vol. 2., Jan. 2020 and can be found in the "Access Request" section of the DISS Resources page. You can get to the DISS Home page by going to the following web address - at https://www.dcsa.mil/is/diss/dissresources/. Once there, click on the blue "PSSAR Form" hyperlink in the Access Request section. This is the only accepted PSSAR form for industry DISS JVS provisioning.

Filling out Part 1, Blocks 1-13

1) Fill out blocks 1-12 with the applicant's information. If you don't have an office symbol/department you can leave block 3 blank. Note: Cage Code (block 12) is for industry contractors only.

2) Complete Part 1 by filling out block 13



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	

Figure 1

Filling out Part 2, Blocks 14-15

For initial DISS JVS Account Requests, leave blank.

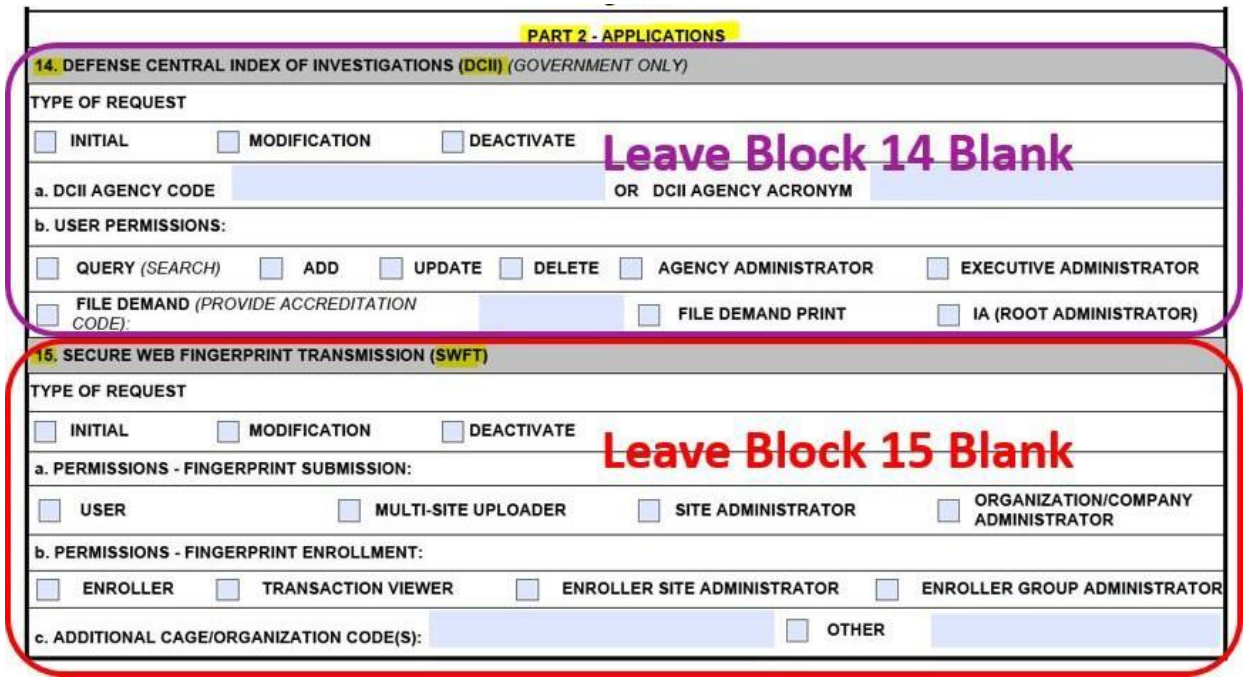


Figure 2

Filling out Part 2, Blocks 16

1. All new users select "Initial"

2. All new users put in their "Organizational/Agency Code" in Block 16.b.

3.a. Agency Hierarchy Managers select "Hierarchy Manager" and "View SCI Access" in Block 16.b.

3.b. Users that need read-only access to look up access and eligibility requirements by SSN select "Physical Access Control" and "View SCI Access" in Block 16.b.

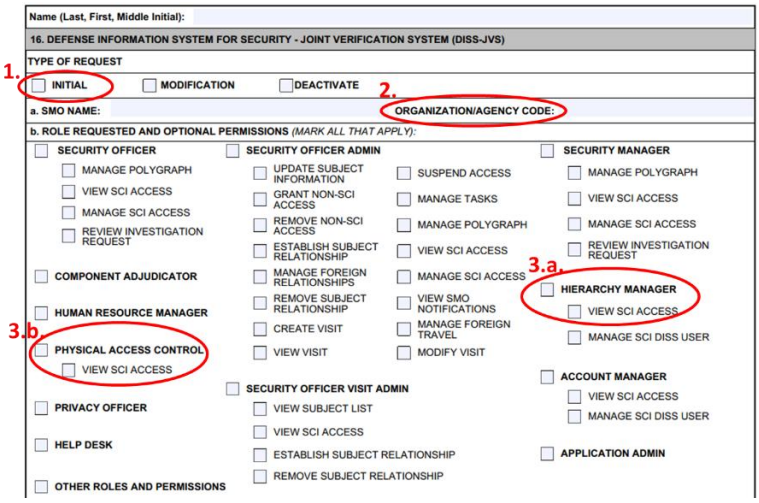


Figure 3

Filling out Part 2, Blocks 17-19

For initial DISS JVS Account Requests, leave blank.

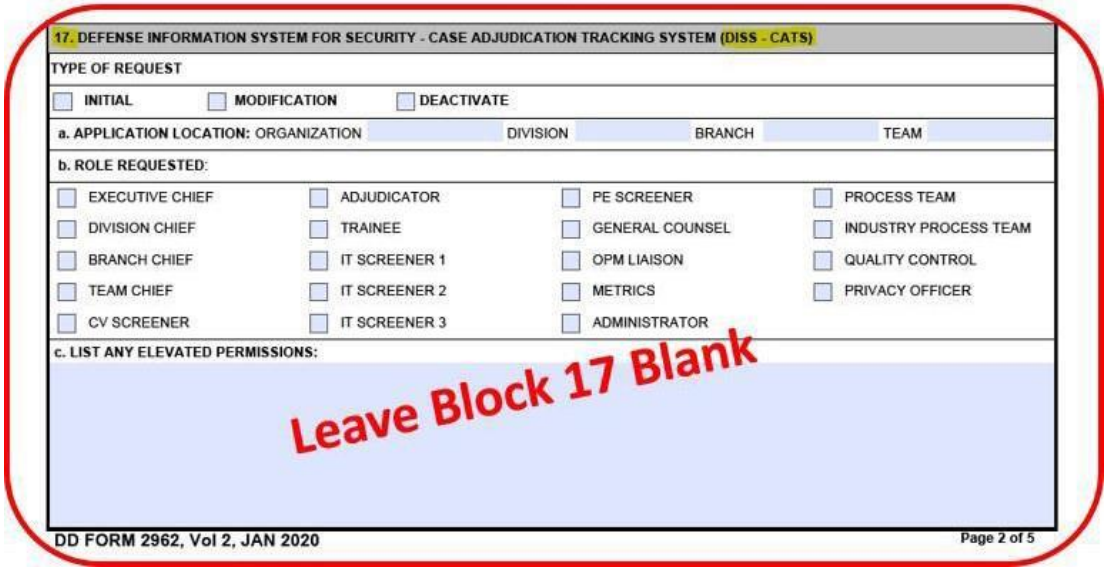


Figure 4

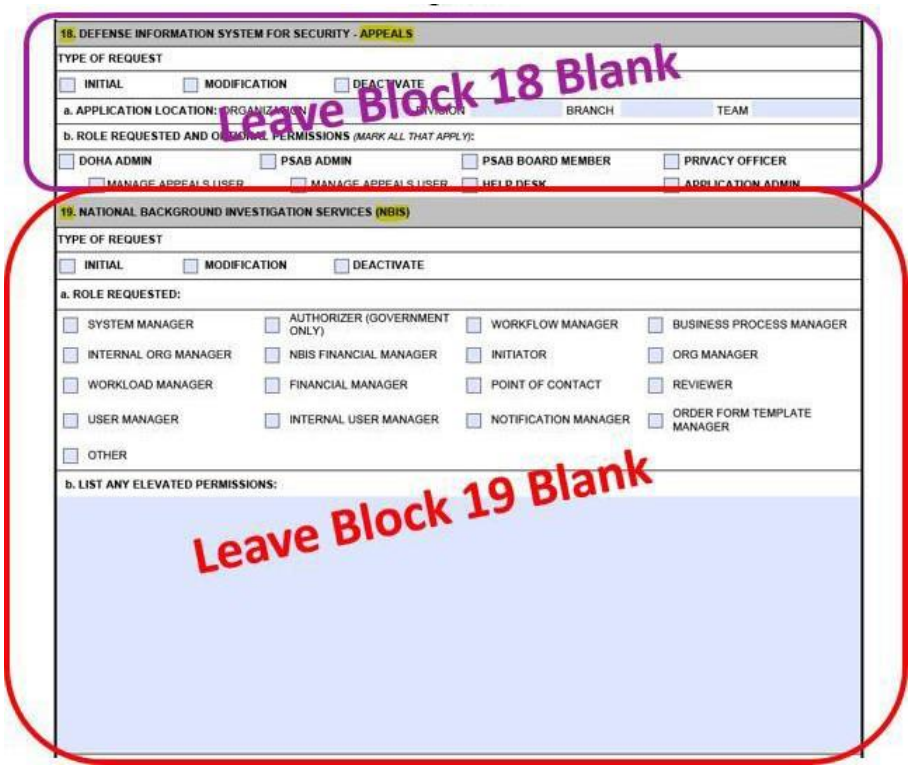


Figure 5

Filling out Part 3, Blocks 20-21

This part is the training verification portion. Remember that the applicant must have taken both the Cyber Awareness and PII Training classes within one (1) year of the date they are provisioned. That means that if either required training certificate is more than a year old at the moment DCSA begins to provision your account, it will trigger an automatic disapproval.

1. In block 20, check the Cyber Awareness Training block and then enter the date from the Cyber Awareness training certificate (date completed) in the date block on the right-hand side (circled below).
2. In block 21, check the PII Training block and then enter the date from the PII training certificate (date completed) in the date block on the right-hand side (circled below).

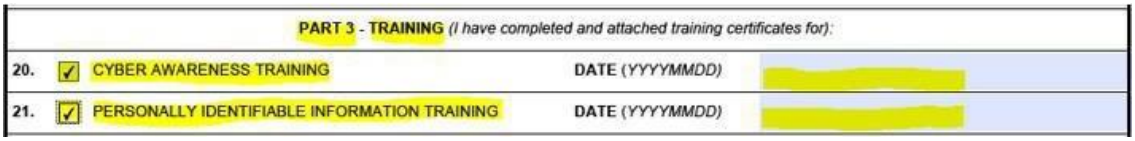


Figure 6

Part 4, Blocks 22-23

Blocks 22 and 23 is related to the applicant's certification. DCSA will accept either digital or wet (ink) signatures in block 22. However, wet (ink/type) date entry is mandatory in block 23.

1. Block 22 (circled below) requires the applicant's signature.
2. Block 23 (circled below) requires the date the applicant signed the PSSAR (required for wet signatures).

Figure 7

Part 5, Blocks 24-29

Part 5 (Blocks 24-29) relates to the nominating official's certification. Complete part 5, (Blocks 24-29) using the following information:

1. Block 24 (circled below), states that the nominating official certifies that the applicant meets the requirements for access, has the appropriate need-to-know,and meets all requirements for managerial DISS JVS system privileges. It also certifies that the nominating official is responsible to ensure the applicant will follow account policies, security policies, and all applicable DoD regulations and U.S. laws. Finally, the nominating official certifies that the named applicant requires account access as indicated to perform assigned duties (i.e. the roles of hierarchy manager and security officer).
2. Block 25 (circled below), requires the Nominating Official's complete printed name.
3. Block 26 (circled below), requires the Nominating Official's organizational title.
4. Block 27 (circled below), requires a good contact number to reach the Nominating Official (noswitchboards).
5. Block 28 (circled below), requires the Nominating Official's signature.
6. Block 29 (circled below), requires the date the Nominating Official signed the PSSAR (required for wet signatures).

Figure 8

Part 6, Blocks 30-38

Leave Part 6 blank.

Figure 10

Submitting PSSAR Packet

Send your signed DCSA PSSAR (DD Form 2962, Vol. 2, Jan.2020), both Cyber Awareness and PII Training certificates to DISS Provisioning at the following email address: dcsa.dcsa-northern.dcsa-dvd.mbx.diss-provisioning@mail.mil.

Note – Since the PSSAR packet contains PII, the document must be password protected prior to sending to DISS Provisioning. DO NOT send via encrypted email as the inbox does not accept encrypted email.

ADDITIONAL TIPS AND GUIDELINES:

1) Maintain an active DISS account by logging in at least every 30 days.

- An active DISS account is one that has been logged into within the past 30 days.
- An inactive DISS account is one that has not been logged into in over 30 days.
    - If a DISS account becomes inactive—i.e. not successfully accessed for more than 30 days, the DISS system shall automatically lock and suspend the account.
    - The user's agency Hierarchy Manager or Account Manager can unlock accounts without any assistance from DCSA until the account exceeds 45 days of inactivity.
- DISS accounts that have not been logged into for longer than 45 days are deactivated/removed per DoD regulations (CYBERCOM TASKORD 13-0641). If an account is needed after 45+ days of inactivity, a new account will have to be created.

2) Failure to follow provisioning instructions may result in the rejection of your provisioning package. Most common package rejection reasons:

- Selecting everything in PSSAR Part 2, Section 16b or alternatively selecting nothing at all.
- Certificates/training expired (more than one year old) or dates on certificates do not match dates on PSSAR form.
- Information missing (blank) or duties do not correspond to the roles requested in Part 2 Section 16b.
- KMP acting as the nominating official in the PSSAR is not cleared in connection with the facility clearance.