Frequently Asked Questions (FAQs)

DISS JVS Industry PSSARs

For Industry SMOs Needing a DISS JVS Hierarchy Manager

Version 2.4

Date Updated: 11/5/20

FAQs - DISS JVS Industry PSSARs –
For Industry SMOs Needing a DISS JVS Hierarchy Manager

Overview. **These FAQs and answers are meant to assist Industry FSOs/Security Managers in requesting a DISS JVS account for an Industry SMO(s) that do not have an existing hierarchy manager. Industry FSOs/Security Managers will need to utilize the DCSA 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 their PSSAR submission and JVS provisioning process as smooth as possible. ***Civil servant and military service component Security Officers and Security Managers should reach out to their security chain of command for their specific current guidance on DISS JVS provisioning.***

***Question 1 – Is there any information outlining the request procedures and requirements for requesting a DISS JVS account for an Industry SMO*?**

Answer – Yes. See the DISS Account Request Procedures found in the Access Request Section on the DISS Home page at https://www.dcsa.mil/is/diss/dissresources/ (refer to Figure #1 below).

Figure 1

FAQs - DISS JVS Industry PSSARs –
For Industry SMOs Needing a DISS JVS Hierarchy Manager

Question 2 – Are there any mandatory training requirements when requesting a DISS JVS account for an Industry SMO?

Answer – Yes. IAW the DISS Account Request Procedures, you must submit training certificates showing completion of both Cyber Security Awareness and PII training within the past year and submit those training certificates with your PSSAR packet in order to be provisioned. The following information is provided on the mandatory training classes/certificates:

There are two options for obtaining Cyber Security Awareness/Information Assurance completion certificates:

1. **Cyber Awareness Challenge - https://public.cyber.mil/training/cyber-awareness-challenge/ (After you get to the DISA website you may need to click on Training and then click on Cyber Awareness Challenge).**
2. **Annual security training provided by the cleared service/company/agency.**

There are two options for obtaining Personally Identifiable Information (PII) completion certificates:

1. **https://public.cyber.mil/training/identifying-and-safeguarding-personally-identifiable-information-pii/**
2. **http://www.cdse.edu/catalog/elearning/DS-IF101.html (you need a STEPP account)**

Question 3 – Where do I find the correct JVS account request form (DCSA PSSAR - DD FORM 2962, VOL 2, JAN 2020)?

Answer - The correct JVS account request form is the DCSA PSSAR (DD FORM 2962, VOL 2, JAN 2020) and it can be found in the DISS Resources section of the DCSA website. You can get to this section by going to the following web address - at https://www.dcsa.mil/is/diss/dissresources/. Once there, click on the Access Request section and then click on the "PSSAR Form" hyperlink. (See Figure #2). This is the only PSSAR form that will be accepted for industry DISS JVS provisioning.

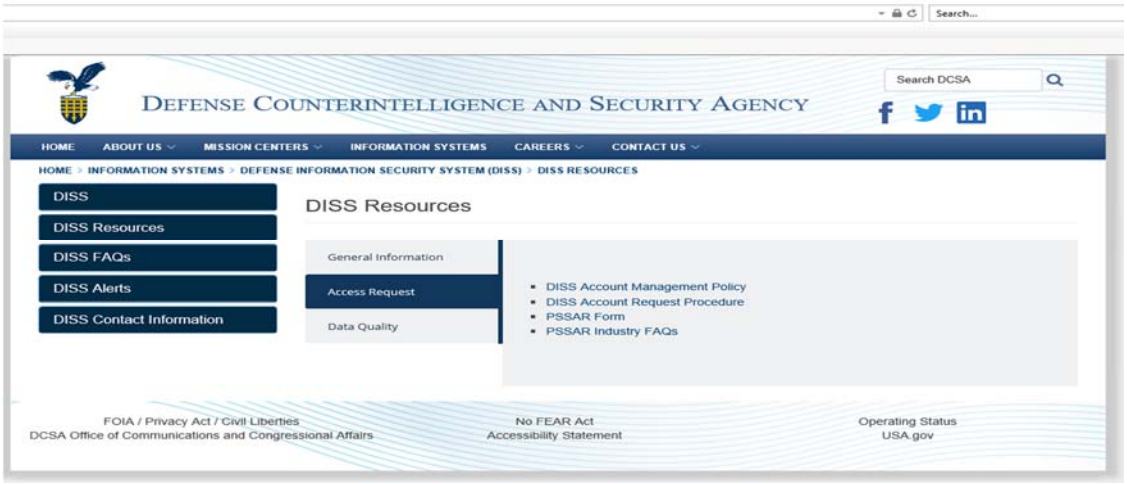


Figure 2

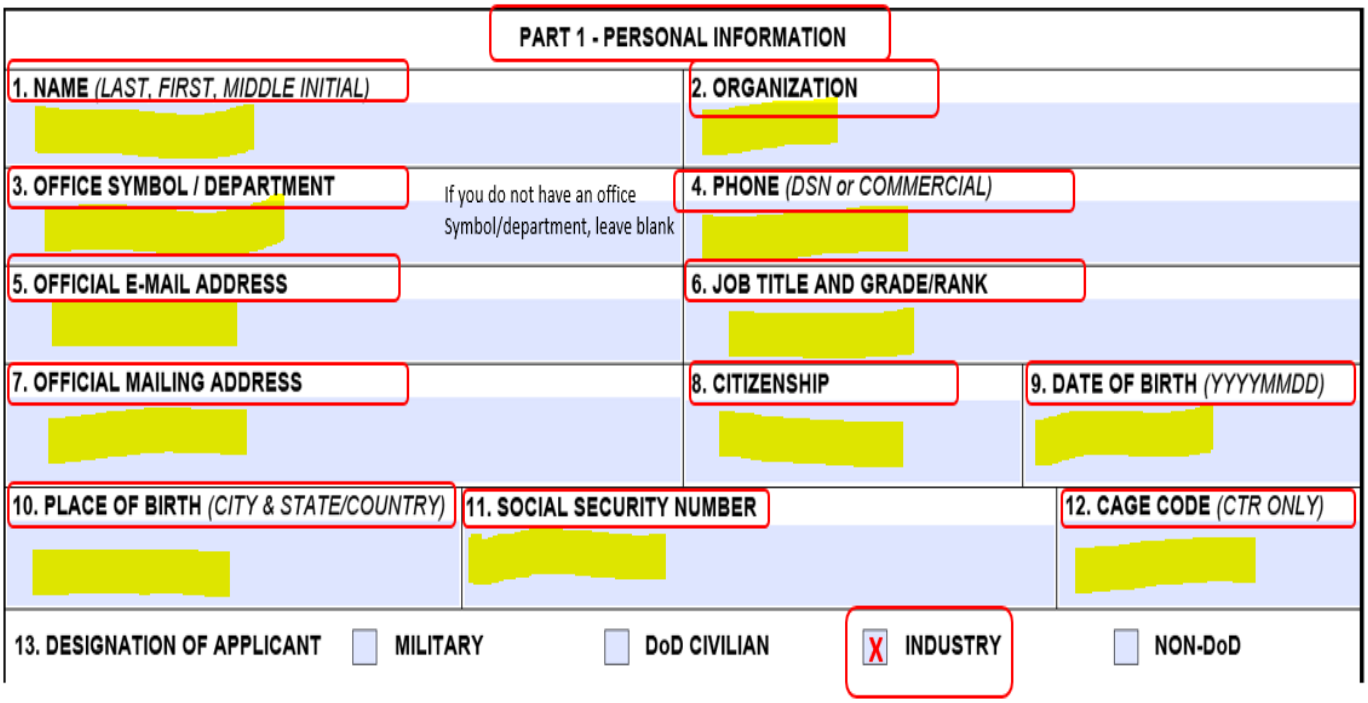
FAQs - DISS JVS Industry PSSARs –
For Industry SMOs Needing a DISS JVS Hierarchy Manager

Question 4 – What goes in Part 1 of the DCSA PSSAR (DD FORM 2962, VOL 2, JAN 2020)?

Answer - The personal information required in Part 1 of the *DCSA PSSAR (DD FORM 2962, VOL 2, JAN 2020)* pertains to the applicant (the FSO/Security Manager requiring the JVS account). Please refer to Figure #3 below.

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.**
2) **Complete Part 1 by filling out block 13 (circled in red below).**

Figure #3



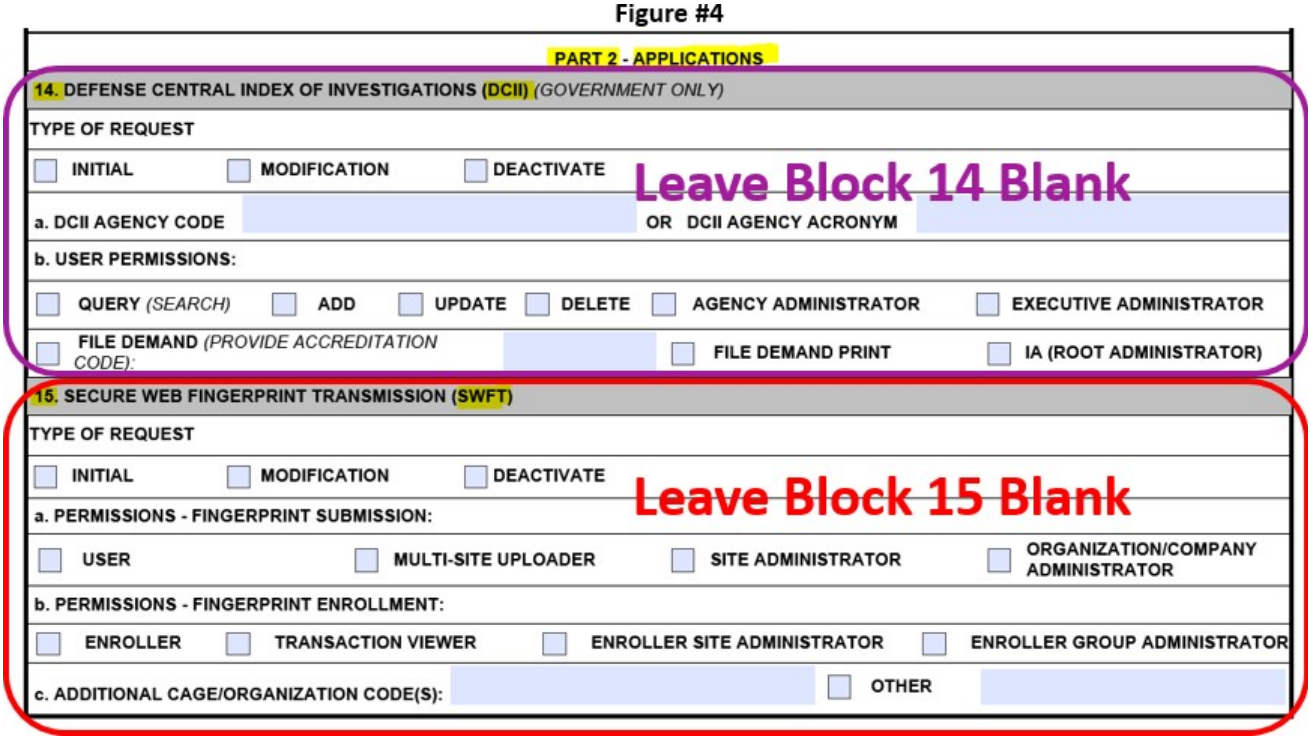
FAQs - DISS JVS Industry PSSARs –
For Industry SMOs Needing a DISS JVS Hierarchy Manager

Question 5 – What goes in Part 2 of DCSA PSSAR (DD FORM 2962, VOL 2, JAN 2020)?

Answer - The information required in Part 2 of the *DCSA PSSAR (DD FORM 2962, VOL 2, JAN 2020)* pertains to the systems (also known as applications) that the FSO/Security Manager is requesting an account(s) in. Please refer to Figure #4 below.

Answer (continued) - For initial DISS JVS Industry Account Requests leave Section 2, blocks 14 and 15 blank (only used for DCII and SWFT accounts).

Figure #4



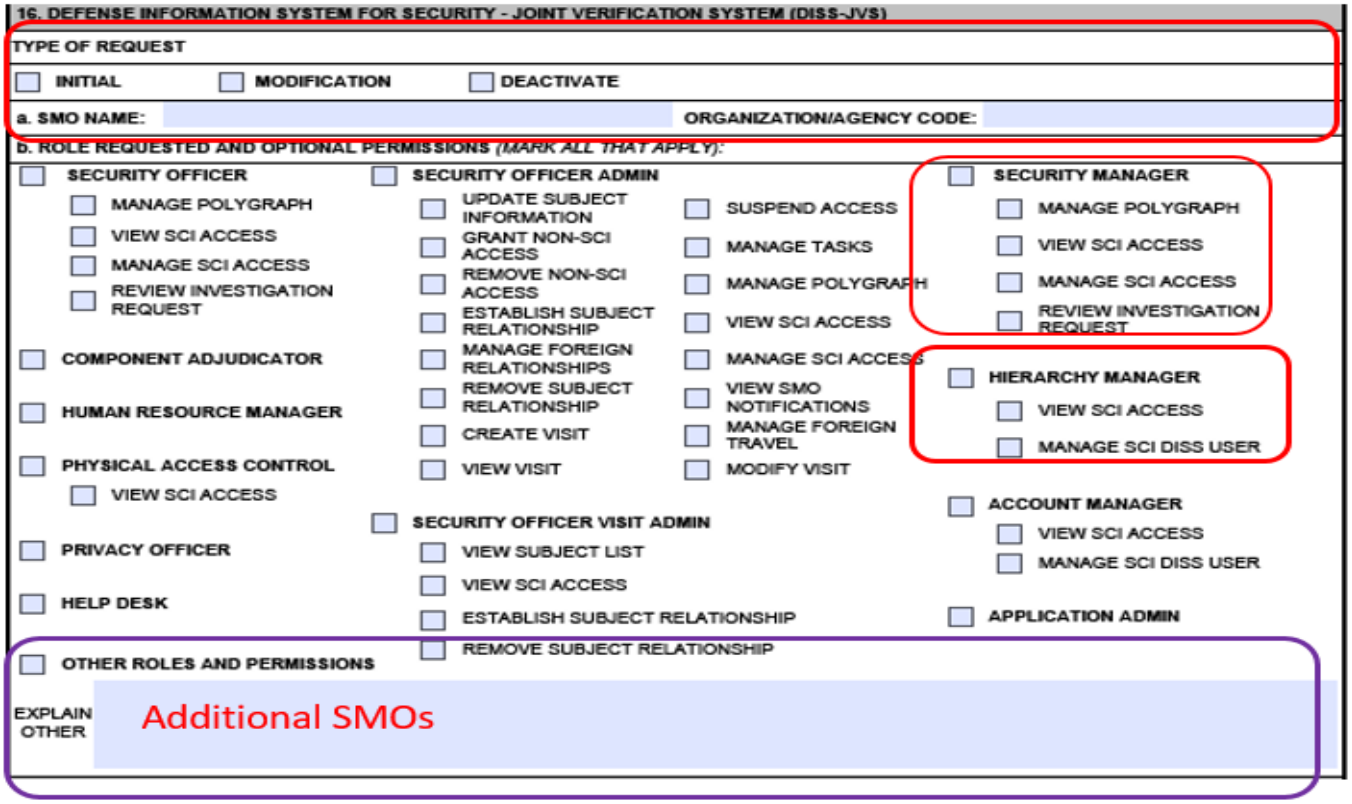
FAQs - DISS JVS Industry PSSARs –
For Industry SMOs Needing a DISS JVS Hierarchy Manager

- **Answer Part 2 (continued) – Refer to Figure #5 below. To obtain the ability to perform JVS account and user management functions as well as subject management functions equal to what JPAS account managers can currently do in JPAS, JVS applicants must complete the areas/blocks highlighted in red below and in Block 16.**

At a minimum each JVS applicant must:

1) **Enter their name in the name block at the top of the second page.**
2) **At the top of block 16 check the "Initial" block for the type of request.**
3) **In block 16 a. enter both the SMO Name and the organizations/agency Cage Code.**
4) **In block 16 b. check boxes for both the Security Manager and Hierarchy Manager roles.**
5) **Also in block 16 b. check the box for the Review Investigation Request permission.**
6) **Other Roles and Permissions section (circled below) can be used to list additional SMOs that the applicant needs provisioned in with the same roles and permissions listed if and only if those SMOs have the same KMP signing as nominating official. First check the "Other Roles and Permissions" option and then in the "Explain Other" section type "Additional SMOs" and then list those SMOs. If this block is not big enough to list all of those SMOs you can attach a list of the SMOs in your packet and simply put "See Attached List" in the "Explain Other" section.**

Figure #6

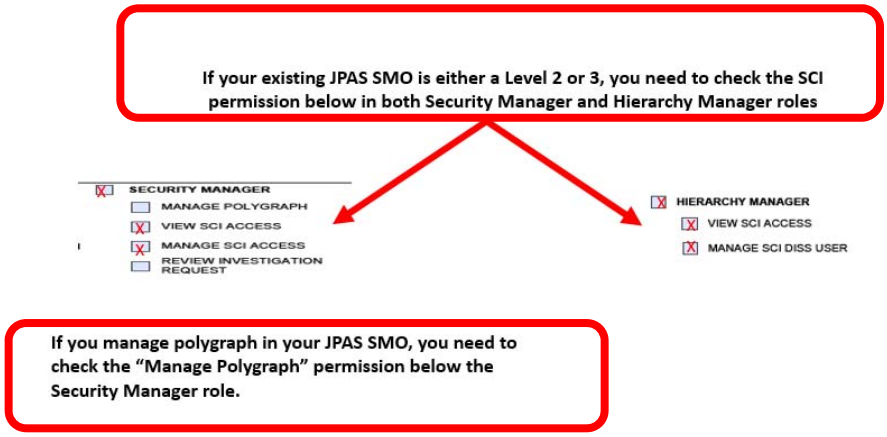


FAQs - DISS JVS Industry PSSARs –
For Industry SMOs Needing a DISS JVS Hierarchy Manager

Answer Optional Permissions – Not every applicant will need to check Optional permissions. If you don't handle polygraphs or SCI SMOs and SCI DISS Users, please disregard the remaining steps outlined in this optional permission section.

Answer Optional Permissions (continued) – Industry FSO/Security Manager applicants that currently manage polygraphs or manage SCI SMOs (level 2 or 3) and other SCI Users in their existing JPAS accounts will need to check those additional permissions under the Security Manager and Hierarchy Manager roles in block 16 b. Only those applicants need to refer to Figure #6 (below) to determine which of the highlighted optional permissions under the Security Manager and Hierarchy Manager roles they need to check to complete block 16 b.

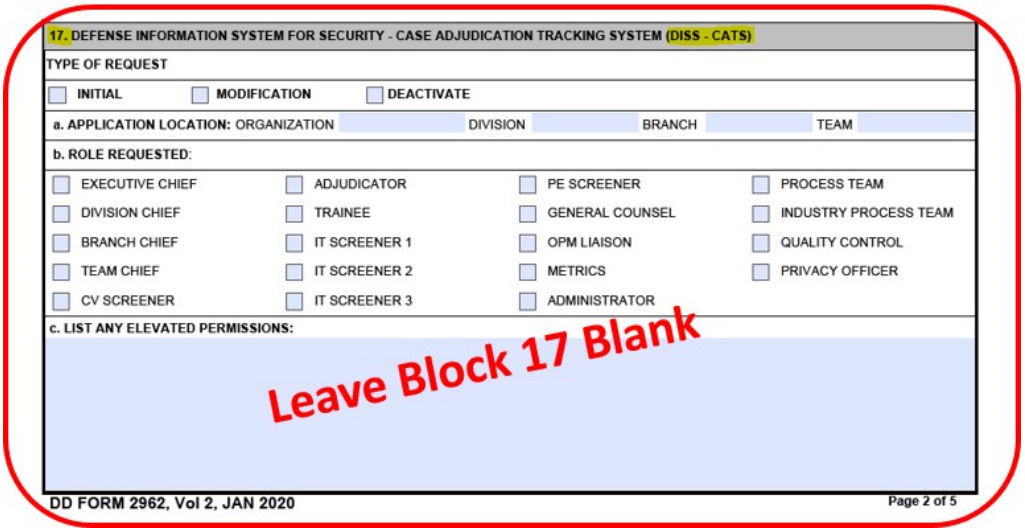
Figure #6



Answer Part 2 (continued) – Please refer to Figure #7 below. All JVS applicants should leave Section 2, block 17 blank (only used for DISS CATS accounts).

FAQs - DISS JVS Industry PSSARs –
For Industry SMOs Needing a DISS JVS Hierarchy Manager

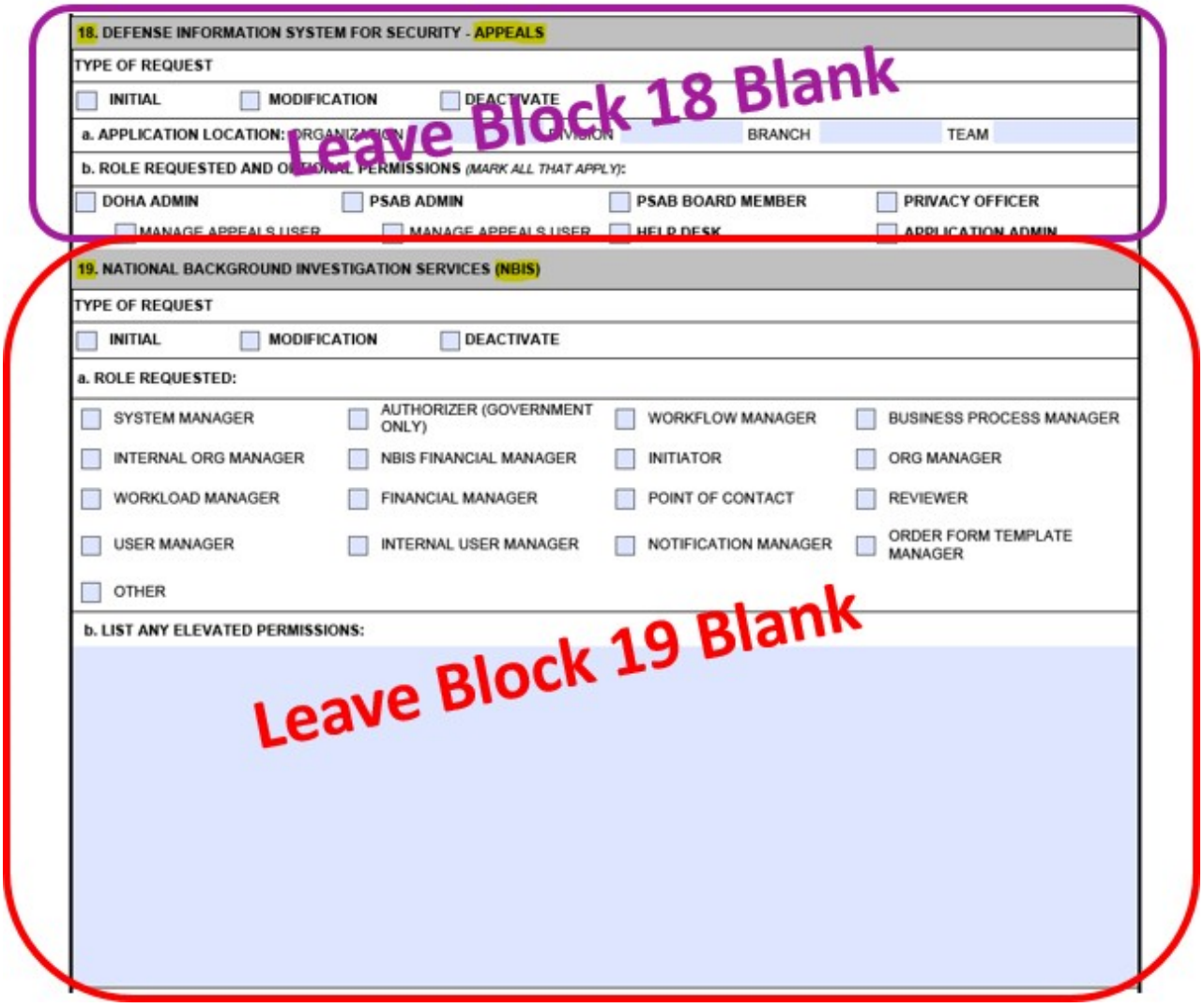
Figure #7



FAQs - DISS JVS Industry PSSARs –
For Industry SMOs Needing a DISS JVS Hierarchy Manager

Answer Part 2 (continued) – Please refer to Figure #8 below. All JVS applicants should leave Section 2, blocks 18 and 19 blank (only used for DISS Appeals and NBIS accounts).

Figure #8



FAQs - DISS JVS Industry PSSARs –
For Industry SMOs Needing a DISS JVS Hierarchy Manager

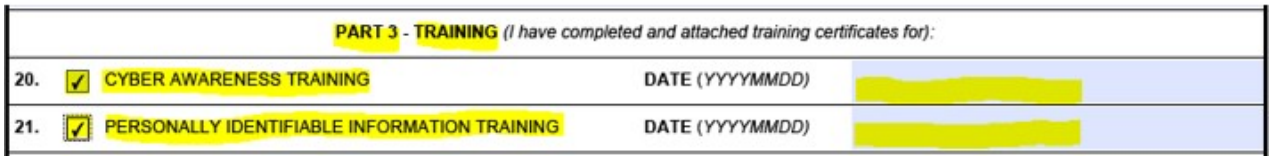
Question 6 – What goes in Part 3 of the DCSA PSSAR (DD FORM 2962, VOL 2, JAN 2020)?

Answer Part 3 – Training (Refer to figure #9 below). This part is the training verification portion. Remember that the applicant has to have taken both the Cyber Awareness and PII Training classes within one year of the date they are provisioned. That means that if either or both of these required training certificates are more than one year old at the moment DCSA begins to provision your account it will trigger an automatic disapproval.

Answer Part 3 (continued) - Refer to figure #9 below to complete Part 3 – Training:

1) **In block 20 check the Cyber Awareness Training block and then enter the date from the Cyber Awareness training certificate (the date it was 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 (the date it was completed) in the date block on the right hand side (circled below).**

Figure #9

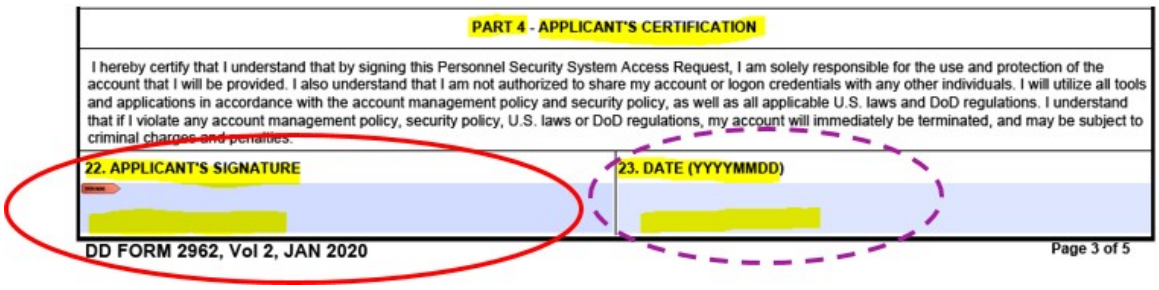


Question 7 – What goes in Part 4 of the DCSA PSSAR (DD FORM 2962, VOL 2, JAN 2020)?

Answer Part 4 – Refer to figure #10 below. This part is applicant's certification portion. DCSA will accept either digital or wet (ink) signatures, however, wet signatures require a mandatory date entry in block 23.

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

Figure #10



FAQs - DISS JVS Industry PSSARs –
For Industry SMOs Needing a DISS JVS Hierarchy Manager

Question 8 – What goes in Part 5 of the DCSA PSSAR (DD FORM 2962, VOL 2, JAN 2020)?

Answer Part 5 – Refer to figure #11 below. This part is the nominating official's certification portion. The nominating official completing part 5 must be an Industry KMP and be on the most recent industry KMP list DCSA has. Complete part 5 using the following information:

1) **Block 24 (circled below). There is nothing to fill out in this block. This block 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 in order 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 (no switchboards).**
5) **Block 28 (circled below) requires the Nominating Official's signature.**
6) **Block 29 (circled below) date the Nominating Official signed the PSSAR (required for wet signatures.)**

Figure #11

FAQs - DISS JVS Industry PSSARs –
For Industry SMOs Needing a DISS JVS Hierarchy Manager

Question 9 – What goes in Part 6 of the DCSA PSSAR (DD FORM 2962, VOL 2, JAN 2020)?

Answer Part 6 – Refer to figure #12 below. This part is the validating official's verification portion. Leave Part 6 blank. DCSA will perform the duties of validating official for every applicant will complete part 6.

Figure #12

Question 10 – What goes in my PSSAR packet?

Answer – Your PSSAR packet needs to include the completed *DCSA PSSAR (DD FORM 2962, VOL 2, JAN 2020)*, both Cyber Awareness and PII Training certificates.

Question 11 – How do I get my PSSAR packet to DCSA and are their special considerations since it contains PII?

Answer – Since the PSSAR packet contains PII it must be encrypted or sent via password protected document. You must send the entire PSSAR packet to DCSA utilizing the following email address: dcsa.dcsa-northern.dcsa-dvd.mbx.diss-provisioning@mail.mil.

Tips on how to password protect the document in Adobe Acrobat:

Please note: You can only create security envelopes in Acrobat Pro; not the Acrobat Reader. If you do not have access to Acrobat Pro, please contact the DISS provisioning team for alternate method.

1. Open Acrobat, click the **Tools Tab** and click "**Protect"**
2. Select the more options drop down and select "**Create Security Envelope"**

3. In the **"Create Security Envelope"** dialog box, click the "**Add File to Send"** button.
4. In the **Files to Enclose dialog box**, browse to select the file or files to add, highlight them and select "**Open"**. Note that you can add non-PDF files, and you can add more than one file. The **Currently Selected Files** window displays a list of the file(s) you have added. You can delete any file by selecting it and clicking Remove Selected Files.
5. Click **Next**.
6. In the Available Templates panel, select the template you want to use – "**eEnvelope with Signature"**, and then click **Next**.
7. Make sure "**Send the Envelope Later**" is selected and hit **Next**
8. In the Security Policy dialog box, first check the "**Show All Policies**" box. Select "**Encrypt with Password**". Click **Next**.
9. Complete the Identity panel if you haven't already established an identity and click **Next**
10. Click **Finish**. Now you'll choose your security settings.
11. In the **Password Security Settings** dialog box, set a password in the "**File Attachment Open Password**" field.
12. At the bottom choose "**Encrypt only file attachments**".
13. Click **OK**. Enter the password you entered in the previous step and hit **OK**. You can now save the file and send the envelope to the DISS provisioning team: dcsa.dcsa-northern.dcsa-dvd.mbx.diss-provisioning@mail.mil.
14. Send an **immediate follow-up email with the password** to open the envelope to the DISS provisioning team: **dcsa.dcsa-northern.dcsa-dvd.mbx.diss-provisioning@mail.mil.**

Additional Tips and Guidelines:

- **DISS account will expire if subject does not log into the account within 30 days.**
- **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**