DISS JVS Industry PSSAR Frequently Asked Questions (FAQ)

For Industry SMOs Needing a DISS JVS Hierarchy Manager

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

Version 1.0

February 12, 2021

REVISION HISTORY

DATE	VERSION	CHANGE DESCRIPTION	AUTHOR
2/12/2021	1.0	RELEASED ON DCSA TEMPLATE	DCSA

FOR INDUSTRY SECURITY MANAGEMENT OFFICES NEEDING AN *INITIAL* DISS JVS HIERARCHY MANAGER

OVERVIEW

These Frequently Asked Questions (FAQs) and answers are meant to assist Industry facility security officers (FSOs)/Security Managers and Key Management Personnel (KMP) in requesting a Defense Information System for Security (DISS) Joint Verification System (JVS) account for any Industry Security Management Office (SMO) that does not yet have an *existing* Hierarchy Manager. While this FAQ is meant to provide guidance to obtain an *initial* Hierarchy Manager account, guidance below may also be used for all other JVS user account requests. Industry facility security officers (FSOs)/Security Managers 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 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 and DISS Account Management Policy found in the Access Request Section on the DISS Resources page at https://www.dcsa.mil/is/diss/dissresources/.

QUESTION 2

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

Answer – Yes. In accordance with the DISS Account Request Procedures, you must submit training certificates showing completion of both Cyber Security Awareness and Personally Identifiable Information (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 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
- Personally 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: Service, company, or agency approved cyber awareness, IA, and/or PII training course certificates may only be used and submitted to an already established SMO Hierarchy Manager or Account Manager for new user account provisioning.

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

QUESTION 3

*Where do I find the correct JVS account request form (*DD Form 2962, PSSAR, Vol. 2, Jan. 2020*)?*

Answer - The correct JVS account request form is the DD Form 2962, PSSAR, Vol. 2, Jan. 2020 and it 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 PSSAR form that will be accepted for industry DISS JVS provisioning.

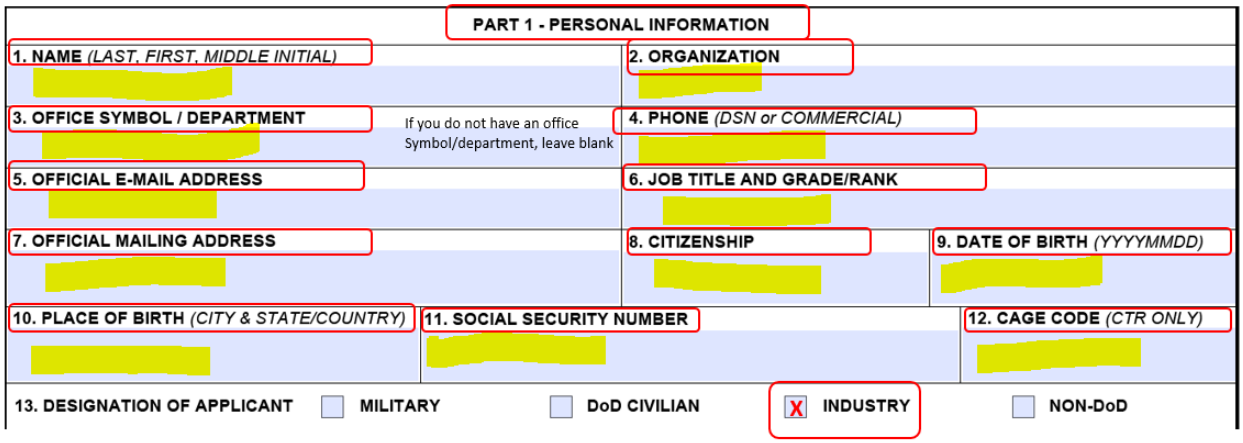
1) Fill out blocks 1-12 with the applicant's information. If you don't have an office symbol/department you can leave block 3 blank.

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

QUESTION 4

*What goes in Part 1 of the DCSA PSSAR (*DD Form 2962, PSSAR, Vol. 2, Jan. 2020*)?*

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



PART 1 - PERSONAL INFORMATION			
1. NAME *(LAST, FIRST, MIDDLE INITIAL)*		2. ORGANIZATION	
3. OFFICE SYMBOL / DEPARTMENT	If you do not have an office Symbol/department, leave blank	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

QUESTION 5

*What goes in Part 2 of DCSA PSSAR (*DD Form 2962, PSSAR, 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 #2** below. For initial DISS JVS Industry Account Requests leave Section 2, blocks 14 and 15 blank (only used for Defense Central Index of Investigations (DCII) and Secure Web Fingerprint Transmission (SWFT) accounts).

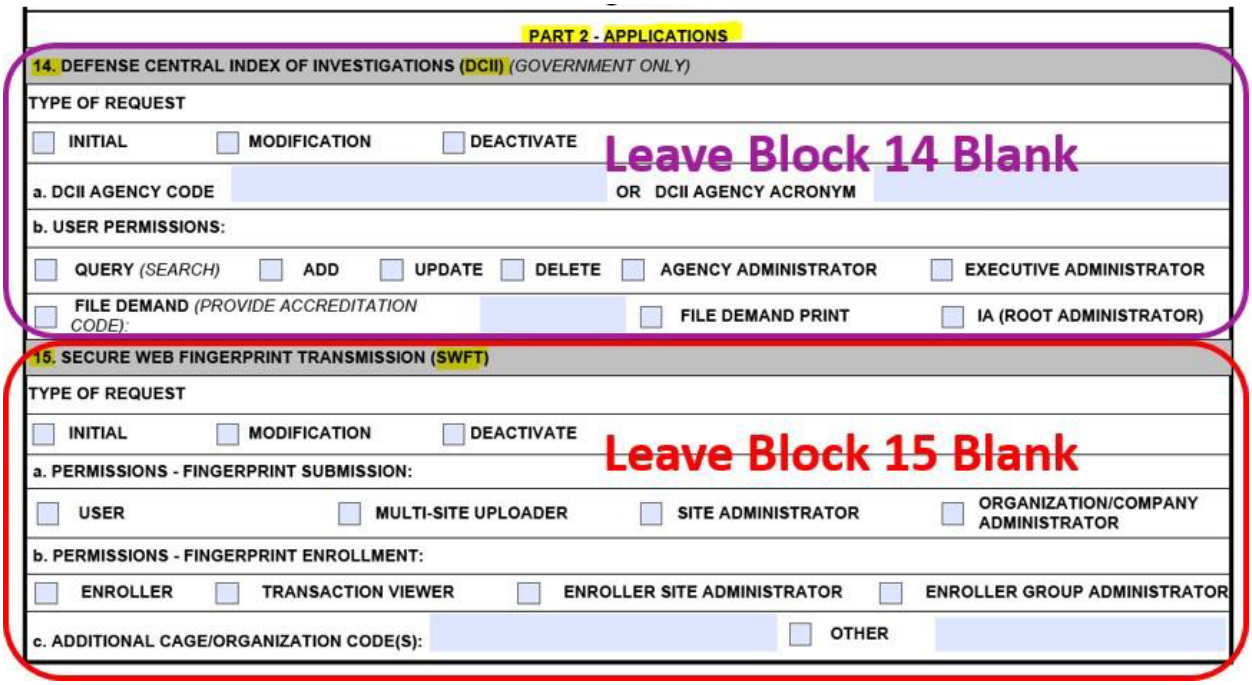


Figure 2

Answer Part 2 (continued) – Refer to **Figure #3** 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 16b. 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.

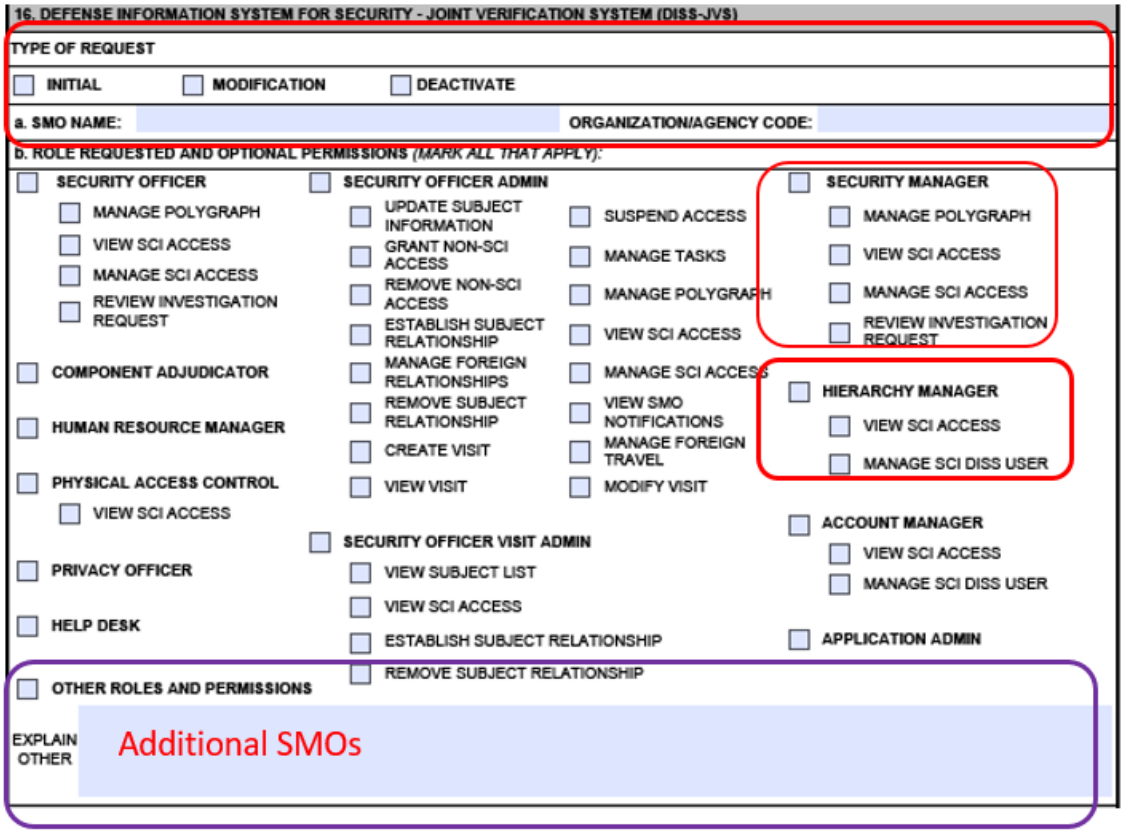


Figure 3

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

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 16b. Only those applicants need to refer to Figure #4 (below) to determine which of the highlighted optional permissions under the Security manager and hierarchy manager roles they need to check to complete block 16b.

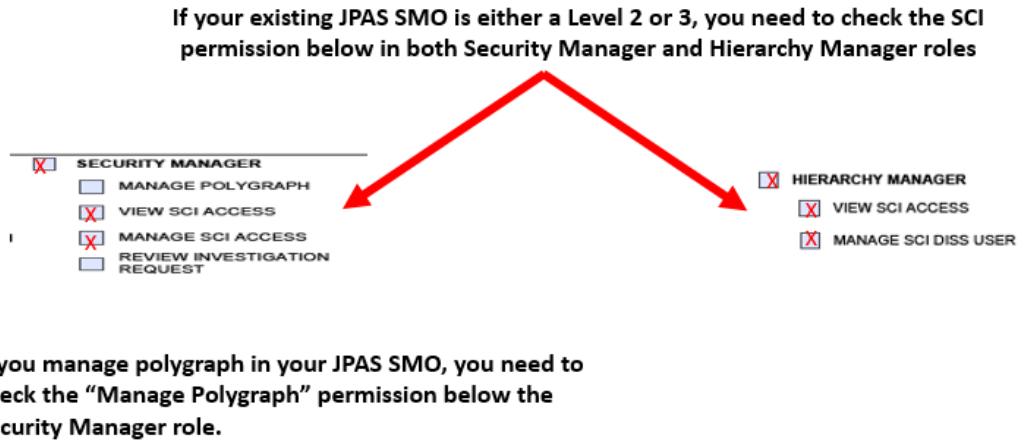


Figure 4

Answer Part 2 (continued) – Please refer to **Figure #5** below. All JVS applicants should leave Section 2, block 17 blank (only used for DISS CATS accounts).

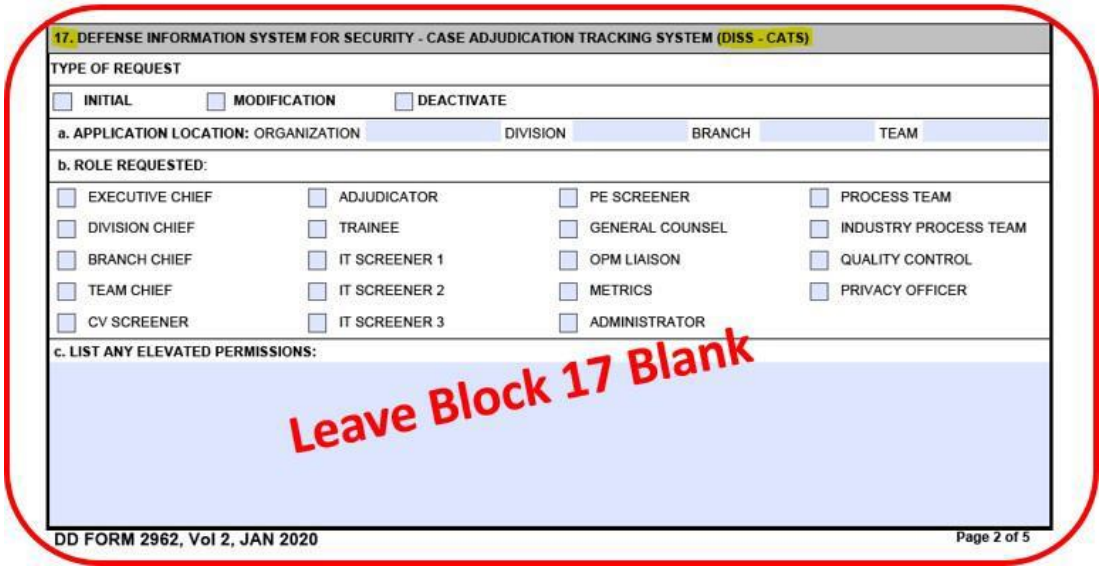


Figure 5

Answer Part 2 (continued) – Please refer to **Figure #6** below. All JVS applicants should leave Section 2, blocks 18 and 19 blank (only used for DISS Appeals and NBIS accounts).

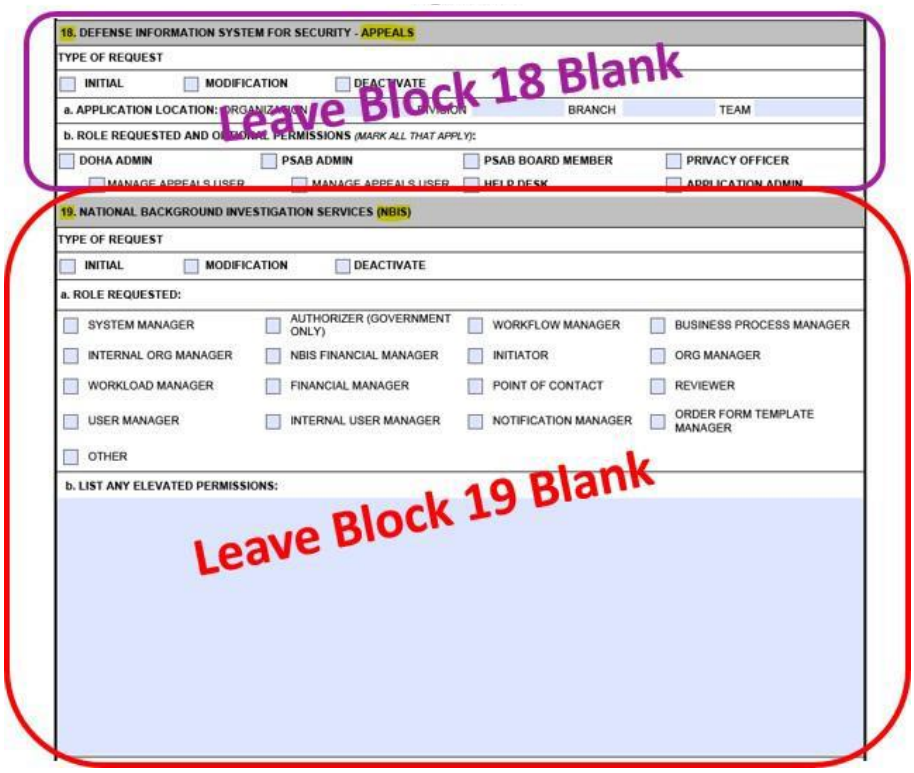


Figure 6

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 #7** 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 #7** 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).

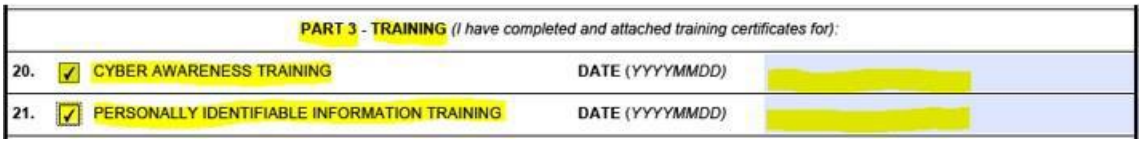


Figure 7

QUESTION 7

What goes in Part 4 of the DCSA PSSAR (Form 2962, Vol. 2, Jan. 2020)?

Answer Part 4 – Refer to **Figure #8** 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 8

QUESTION 8

What goes in Part 5 of the DCSA PSSAR (Form 2962, Vol. 2, Jan. 2020)?

Answer Part 5 – Refer to Figure #9 below. This part is the nominating official's certification portion. The nominating official completing part 5 must be an industry knowledge management professional (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 9

QUESTION 9

*What goes in Part 6 of the DCSA PSSAR (*DD Form 2962, PSSAR, Vol. 2, Jan. 2020*)?*

Answer Part 6 – Refer to **Figure #10** 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 10

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 the DCSA DISS Industry Provisioning Team utilizing the following email address: dcsa.dcsa-northern.dcsa-dvd.mbx.diss-provisioning@mail.mil.

ADDITIONAL TIPS AND GUIDELINES:

1) DISS account will expire if subject does not log into the account within 30 days.

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

3) 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