

*Defense Manpower Data Center*

---

Personnel Security & Assurance



**Joint Personnel Adjudication System (JPAS)  
Account Request Procedures**

**Document Version 5.0**

12/23/2016



## **Table of Contents**

1	New JPAS Account Checklist .....	3
2	How Do I Obtain a JPAS Account?.....	4
2.1	Military .....	4
2.2	DoD Agencies.....	4
2.3	Industry .....	5
2.3.1	Users: .....	5
2.3.2	Account Managers: .....	5
2.4	Non-DoD Government Agencies.....	6
3	How Do I Deactivate/Delete a JPAS Account? .....	6
4	JPAS Account Policies .....	7
4.1	Account Activity.....	7
4.2	Violations/Misuse of JPAS Accounts.....	7
5	Personnel Security System Access Request (PSSAR) Form .....	8
5.1	PSSAR Form Quick Tips for Industry Applicants .....	8
5.2	Most Common Reasons for PSSAR Rejection/Disapproval .....	10
6	Submitting the PSSAR Form, LOA, and Training Certificates.....	12
7	Blank PSSAR Form .....	12
8	Sample PSSAR Form.....	12



## 1 New JPAS Account Checklist

Following is a quick reference checklist to assist prospective JPAS users in completing the required steps for a JPAS account. All documentation is required regardless of whether you are requesting brand new account, or you are submitting for an account after having a previous account deleted due to inactivity.

*Note:* Direct link to the blank PSSAR is on pg. 12 of this document; however, please read the entire procedure to ensure all requirements are met before submitting your request.

- Meet clearance requirements:  
The minimum requirement for JPAS access is Interim Secret eligibility. JAMS access requires at minimum a favorably adjudicated SSBI with a Top Secret eligibility
- An Active owning and/or servicing Security Management Office (SMO), for Industry this means an active facility clearance (see section 2.3.2)
- Obtain an active PKI Certificate on a smartcard (CAC, PIV card, ECA PKI Certificate or other approved DoD PKI on a smartcard/token) prior to getting a JPAS account.<sup>1</sup>
- Take JPAS training<sup>2</sup> and include your course completion certificate of the appropriate access level you are requesting:
  - JCAVS User Level 7 & 8:** PS181.16  
<http://www.cdse.edu/catalog/elearning/PS181.html>
  - JCAVS User Level 10:** PS182.16  
<http://www.cdse.edu/catalog/elearning/PS182.html>
  - JCAVS User Levels 2 thru 6:** PS183.16  
<http://www.cdse.edu/catalog/elearning/PS183.html>
  - Or Personnel Security Management PS212.01  
<http://www.cdse.edu/catalog/classroom/PS212.html> (live classroom)
- Take Cyber Security Awareness/Information Assurance course (2 options).<sup>2</sup> and include your course completion certificate:
  1. <http://iatraining.disa.mil/eta/cyberchallenge/launchpage.htm>
  2. Annual security training provided by the cleared service/company/agency
- Take Personally Identifiable Information (PII) course (3 options).<sup>2</sup> and include your course completion certificate:
  1. <http://iatraining.disa.mil/eta/piiv2/launchPage.htm> or,
  2. <http://www.cdse.edu/catalog/elearning/DS-IF101.html> (need STEPP account)
  3. Approved existing corporate PII Training courses
- Complete Personnel Security System Access Request (PSSAR) Form
- Submit Letter of Appointment (LOA), if applicable. A LOA is required for ALL Account Managers

<sup>1</sup> Due to identity validation processes, PKI issuance can take some time. It is highly recommended to have your PKI hardware & certificates on hand before requesting an account as the account activity timer starts from when the account is created **not** from when the PKI is registered.

<sup>2</sup> See section 4.1.3 of our [Account Management Policy](#) for background and requirements for mandatory trainings. Please submit the actual course completion certificates - not memos, emails or automated logs.



**Once all elements in the list are completed**, please refer to the instructions below to submit your documentation to the appropriate JPAS Account Manager. **DO NOT** submit requests to the DMDC Contact Center unless you are requesting an Industry primary Account Manager account or a Non-DoD Government Agency account. DOD Agency and Military must go through the agency/services Account Manager. Account Managers are responsible for managing the accounts, keeping the PSSAR form, and training certificates. These items will be asked for during an audit or incident.

## 2 How Do I Obtain a JPAS Account?

### 2.1 Military

To obtain a new JPAS account required to perform your job duties on behalf of a military branch (applicants may be active duty military, civilians or contractors), contact an established JPAS Account Manager within your military branch. If you do not know whom to contact, please refer to the [JPAS POC Listing](#) on the DMDC JPAS User [web site](#) to locate a JPAS PMO for your military branch. To request an account, your JPAS Account Manager will need:

- A JPAS Personnel Security System Access Request (PSSAR) form must be completed, signed, and submitted. The signatures need to be your Commanding Officer, your Security Officer, and the applicant. To obtain a copy of the PSSAR form, navigate to the PSSAR Form section of this document
- A copy of your certificates of completion for both the CyberSecurity Awareness Challenge/Security training as well as one of the Personally Identifiable Information courses must be submitted with your PSSAR
- A copy of your certificate of completion for the JPAS training taken commensurate to the sub-system and level of access requested. Training must have been completed within the last year

*Note:* If a new Account Manager is required, also submit a LOA on your military branch's letterhead indicating who the account is for and the specific job duties that require JPAS access to your Account Manager. Your Branch Director or delegate must sign the letter. Delegates must be GS-14 grade (or military branch equivalent) or higher.

### 2.2 DoD Agencies

To obtain a new JPAS account required to perform your job duties on behalf of a DoD Agency (applicants may be active duty military, civilians or contractors), contact your agency's JPAS Account Manager and/or Facility Security Officer (FSO). To request an account, your JPAS Account Manager will need:

- A JPAS PSSAR form must be completed, signed, and submitted. The signatures need to be your Agency's Director or delegate, your Security Officer, and the applicant. To obtain a copy of the PSSAR form, navigate to the PSSAR Form section of this document



- A copy of your certificates of completion for both the CyberSecurity Awareness Challenge/Security training as well as one of the Personally Identifiable Information courses must be submitted with your PSSAR
- A copy of your certificate of completion for the JPAS training taken commensurate to the sub-system and level of access requested. Training must have been completed within the last year

*Note:* If a new Account Manager is required, also submit a LOA on your Agency's letterhead indicating who the account is for and the specific job duties that require JPAS access to your Account Manager. Your Agency Director or delegate must sign the letter. Delegates must be GS-14 grade (or Agency equivalent) or higher.

## 2.3 Industry

### 2.3.1 Users:

To obtain a new JPAS account required to perform your job duties on behalf of an Industry company, you will need to contact your company's JPAS Account Manager or FSO. Your JPAS Account Manager will process your request. To request an account, your JPAS Account Manager will need:

- A JPAS PSSAR form must be completed, signed, and submitted. The signatures need to be those of your Corporate Officer, your Security Officer, and the applicant. To obtain a copy of the PSSAR form, navigate to the PSSAR Form section of this document
- A copy of your certificates of completion for both the CyberSecurity Awareness Challenge/Security training as well as one of the Personally Identifiable Information courses must be submitted with your PSSAR
- A copy of your certificate of completion for the JPAS training taken commensurate to the sub-system and level of access requested. Training must have been completed within the last year

### 2.3.2 Account Managers:

If an Account Manager already exists at your company, submit all of the items in the Users section above, PLUS a LOA, to your existing Account Manager. Requests for additional Account Managers should **not** be submitted to the DMDC Contact Center. If there are **no** existing Account Managers or FSOs for your company, follow the process below and request to be the primary Account Manager for your company. The DMDC Contact Center will create your account. To request an account, you will need to submit the following items:

- A LOA on your company's letterhead naming the applicant as the company's primary JPAS Account Manager. A Corporate Officer or Key Management Personnel (KMP) listed in Industrial Security Facilities Database (ISFD) must sign the letter
- A JPAS PSSAR form must be completed, signed, and submitted. The signatures need to be those of your Corporate Officer, your Security Officer, and the



applicant. To obtain a copy of the PSSAR form, navigate to the PSSAR Form section of this document

- A copy of your certificates of completion for both the CyberSecurity Awareness Challenge/Security training as well as one of the Personally Identifiable Information courses must be submitted with your PSSAR
- A copy of your certificate of completion for the JPAS training taken commensurate to the sub-system and level of access requested. Training must have been completed within the last year
- If you are a brand new account manager or KMP at a cleared company, you will need to have both a facility clearance as well as a proper servicing relationship. For instructions on obtaining a facility clearance please see the [Checklist for a New Facility Clearance](#).

*Note:* A JPAS user can have multiple facilities under their JPAS account. However, a user can only request 1 facility per PSSAR, as the KMP of the facility needs to sign it. Typically the KMP is not the same for all the facilities.

After completing a PSSAR, certificates of training completion, and the LOA, please submit all to the DMDC Contact Center, as described in the Submitting the PSSAR Form section of this document. Once the account has been created, the DMDC Contact Center will contact you with your initial log-in credentials. Please review the Most Common Reasons for PSSAR Rejection/Disapproval section below prior to submitting your PSSAR, LOA and training certificates.

## 2.4 Non-DoD Government Agencies

Non-DoD/Other Federal Government agencies should utilize the Office of Personnel Management (OPM) Central Verification System (CVS) for personnel clearance eligibility verifications. OPM CVS contains information on background investigations, credentialing determinations, suitability determinations, and security clearances. OPM CVS contains a data bridge to JPAS for clearance reciprocity purposes.

## 3 How Do I Deactivate/Delete a JPAS Account?

JPAS accounts shall NOT be transferred between organizations/companies. If a user or Account Manager leaves an organization/company, the associated account in JPAS must be de-provisioned by the owning organization/company.

To deactivate a JPAS account, fill out a “deactivate” PSSAR to remove all access and disable an existing account. Complete the following fields of the PSSAR form:

- Type of Request (select “deactivate”)
- User ID Field, if known
- Date
- Box 1, Name of account holder



- Box 5, Official E-Mail Address (enter the email address of the Nominating Official so that DMDC Contact Center can communicate the completion of the request)
- Box 11, SSN of account holder
- Box 29, Nominating Official's Printed Name
- Box 30, Nominating Official's Signature
- Box 31, Nominating Official's Title
- Box 32, Nominating Official's Telephone Number

Account Managers should deactivate accounts of other Account Managers or users within their Security management Office, according to the provisions of the JPAS Account Management Policy. In the event when an organization or company does not have an Account Manager to perform the deactivation of accounts, please submit the deactivation request to the DMDC Contact Center by following the steps outlined in the section Submitting the PSSAR Form, LOA and Training Certificates of this document.

*Note:* LOA and Training Certificates are NOT required for deactivate account requests.

## 4 JPAS Account Policies

### 4.1 Account Activity

- **Active JPAS Account:**  
An active JPAS account is one that has been logged into in the past **30** days
- **Inactive JPAS Account:**  
An inactive JPAS account is an account that has not been logged into in the past **30** days. If a JPAS account is inactive for **31-44** days, the JPAS system will automatically lock the account. Only the company/agency Account Manager overseeing the user's account will be able to unlock the account
- **Deleting Inactive JPAS Accounts:**  
JPAS accounts that have not been logged into for longer than **45** days will be deleted per DoD Regulations (CYBERCOM TASKORD 13-0641). If a JPAS account is needed after it has been deleted de to inactivity, a new account will have to be established following the aforementioned request procedures to include all required documentation

### 4.2 Violations/Misuse of JPAS Accounts

By using the JPAS application, users are consenting to the terms of use of the application and are agreeing to maintain compliance with the Privacy Act of 1974 and all applicable JPAS rules and regulations, including the [JPAS Account Management Policy](#).



Misuse of JPAS will result in **termination** of the offender's JPAS account and exclude culpable companies or persons from future access to JPAS. Additionally, offenders will have a misuse of technology incident recorded on their JPAS record. Information concerning violations of JPAS policies and may be referred to other federal agencies for consideration of administrative, civil, or criminal sanctions when circumstances warrant.

Common misuses of JPAS include, but are not limited to:

- Sharing of username, password, CAC, or PIV cards and/or associated PIN numbers to access the system
- Allowing non-cleared individuals to access the system
- Leaving the JPAS application unsecure while logged in
- Allowing others to view data on the JPAS screen that do not have the proper authorization
- Printing or taking a screenshot of JPAS data
- Querying the JPAS application for 'celebrity' records
- Querying the JPAS application for your own record
- Entering test or "dummy" SSNs into JPAS
- Entering false or inaccurate information into the system
- Initiating investigations for subjects who you have no owning/servicing relationship
- Querying the JPAS application for information you have no need to know to conduct your official duties

## 5 Personnel Security System Access Request (PSSAR) Form

The PSSAR form must be completed for all new JPAS accounts, modifications to existing JPAS accounts, or deactivations of JPAS accounts.

### 5.1 PSSAR Form Quick Tips for Industry Applicants

These quick tips are targeted for Industry JPAS account applicants to assist in correctly completing the form and speed application processing.

#### Part 1

This section collects applicant's personal information. Complete boxes 1-13. Items to pay particular attention to are:

- Name (1) – This is the account user
- Organization (2) – The Company requesting access to JPAS. Applicant's employing organization
- Official e-mail address (7) – Use your official work address, do not enter personal email addresses. Google and Yahoo accounts are not appropriate for official business
- Social Security Number (11) - Required in order to locate the applicant in JPAS



- Designation of Person (13) – Do not select either DoD Military or DoD Civilian. If your Company is listed in the Industrial Security Facilities Database (ISFD) and your Nominating official is listed as KMP in the ISFD, select DoD Contractor. Otherwise, select another appropriate designation

#### Part 2

List date training was completed and provide certificates of completion to your Account Manager or the DMDC Contact Center, as appropriate.

#### Part 3

The PSSAR form is also used to request access to other PSA applications; DCII, SWFT, and JCAVS.

- DCII (17) – Not available to Industry Users
- SWFT (18): Provide your CAGE code and select desired role by clicking the appropriate box.
- JCAVS (19): Select the type of account requested section.
- JCAVS (20): In the box titled ‘Access Requested – Industry’, select the required access level.
- Skip boxes 21, 22, 23, 24, 25, and 26

#### Part 4 – Signature Required!

It is very important to take seriously the account policies, security policies and all applicable DoD regulations and U.S. Laws that you agree to comply with when you sign the form. Read this section carefully before signing.

- Applicant’s Signature (27) – Account Applicant must sign in this box

#### Part 5 – Signature Required!

This section should be completed by the Nominating Official. This individual is the person who authorizes your access to the application, and cannot be the same as the Applicant unless it is a single person facility. The before signing, the Nominating Official should carefully read the certification text. Signing indicates agreement with the statement.

- Statement of Duties: Duties which require access to application **MUST** be listed or PSSAR form will be rejected, this includes Account Manager duties
- Nominating Official’s Signature and Date (30) – The Nominating Official **must** be listed as KMP in the ISFD

#### Part 6 – Signature Required!

Part 6 provides confirmation that the user meets the security requirements for the application. The Validating Official provides the final signature for the form and must be provided by the requesting Company unless it is a single person facility, in which case the DMDC Contact Center will complete this part.



## 5.2 Most Common Reasons for PSSAR Rejection/Disapproval

The following outlines the most common reasons for DMDC Contact Center rejection/disapproval of the JPAS (JCAVS) PSSAR form. Avoiding these pitfalls will enhance the processing/approval timeline of your PSSAR submission, as long as account/access eligibility requirements are met.

### 1. No (or Incomplete) LOA Submitted with PSSAR (Industry primary Account Managers or Non-DoD Agency Account Managers) –

- a. Industry primary Account Managers: The LOA must be drafted on company letterhead, name the applicant as the company's primary Account Manager, and be signed by a KMP. The same KMP **must** sign both the PSSAR, as Nominating Official, and the LOA
- b. Non-DoD Agency Account Managers: The LOA must be drafted on your Agency's letterhead indicating who the account is for and the specific job duties that require JPAS access. Your Agency's Director or delegate **must** sign the letter. Delegates must be GS-14 grade (or agency equivalent) or higher

*Note:* LOAs are required for all types of Account Managers, but only those for Industry primary Account Managers or Non-DoD Agencies are to be sent to the DMDC Contact Center

### 2. Missing Training Certificates

Cyber Security Awareness/Information Assurance and Personally Identifiable Information (PII) courses are required annually. If you have not participated in the past year, you will need to update your training certification before submitting the form. JPAS training is required if you are applying for a JPAS account, and must have been completed within the past year, or applicant must provide proof of recent access to JPAS (example, access at a different DoD contracting company), and therefore have a thorough knowledge of the workings of the application. All certificates must accompany PSSAR form

### 3. Nominating Official is Not KMP in ISFD –

For Industry, the Nominating Official signature in the PSSAR must belong to a company KMP listed in the Industrial Security Facilities Database (ISFD)

### 4. No Statement of Duties in Nominating Official's Section

Duties which require access to application **MUST** be listed on PSSAR form will be rejected

### 5. Industry User or Additional Industry Account Manager, DoD Agency, or Military Request is submitted to the DMDC Contact Center –

These requests must be submitted within your military branch, company, or agency to the appropriate Account Manager with authority to create a JPAS



---

account. The DMDC Contact Center is not authorized to create these accounts in lieu of the responsible Account Manager

**6. Missing Signatures –**

All three signatures **must** be present on the PSSAR form. The three signatures boxes are: User Certification (the applicant), Nominating Official Certification (the KMP, Corporate Officer, or Agency Director), and the Validating Official's Verification (verifying your clearance information is accurate). The Validating Official's Verification may be left blank if it is a single person facility, in which case the DMDC Contact Center will complete this part. LOA must state it is a single person facility if the Validating Official's Verification box is blank

**7. Obsolete PSSAR Form Submitted –**

The current PSSAR is available in the Blank PSSAR Form section of this document. DSS Form 273, dated June 2011, will no longer be accepted or processed

**8. Applicant Already Possesses an Account –**

Prior to submitting a request for JPAS access, applicant should verify with their JPAS Account Manager to determine if an account already exists. If you do not have a JPAS Account Manager, then you may verify with the DMDC Contact Center

**9. Applicant Not Eligible Due to Lack of Security Clearance –**

At a minimum, an Interim Secret Clearance with an open investigation is required to possess a JPAS account. Applicant should not submit a PSSAR form until they have been granted at least an Interim Secret Clearance. JAMS access requires at minimum a favorably adjudicated SSBI with a Top Secret eligibility.

**10. Applicant Not Eligible For Requested Level –**

If Applicant has requested a Level 2, 3 or 8 account (which requires TS SCI) and has not been briefed in JPAS at a TS SCI level, the PSSAR will be rejected. Applicants should verify their clearance level prior to submitting the PSSAR

**11. CAGE Code Not Listed in ISFD –**

The CAGE code listed on the PSSAR could not be found in ISFD. The CAGE code must be listed in ISFD, because the facility must be cleared and the Nominating Official must be verifiable in ISFD as a KMP

**12. SSN Not Located in JPAS –**

The social security number (SSN) on the PSSAR was not located in JPAS. This would indicate either the SSN was entered incorrectly on the PSSAR or the applicant does not meet the minimum JPAS account eligibility/access requirements (does not have a record in JPAS)



---

## 6 Submitting the PSSAR Form, LOA, and Training Certificates

The LOA (if applicable), training certificates and completed PSSAR form (including all three signatures) should be submitted to your company/agency JPAS Account Manager IAW the policy outlined above. NOTE: LOA is required for Account Managers only.

Those applicants who meet the requirements to send to the DMDC Contact Center can submit the completed PSSAR, LOA (for Account Managers), training certificates, and proof of security clearance for non-DoD Government Agency applicants by email to:

[dmdc.contactcenter@mail.mil](mailto:dmdc.contactcenter@mail.mil)

Please annotate “PSSAR Request” on your email subject line to expedite processing.

**NOTE: If you are sending sensitive information via email:**

In order to protect Personal Identifiable Information (PII), please follow the instructions on the JPAS homepage to establish encryption capability with the DMDC Contact Center and ensure your privacy is maintained: [Contact Center Email Encryption](#).

## 7 Blank PSSAR Form

The blank PSSAR form is available at the following [link](#). Please fill out the appropriate information according to the instructions.

## 8 Sample PSSAR Form

Below is a sample PSSAR form for your reference. This is for informational purposes only; DO NOT submit the sample PSSAR form as it will be immediately rejected.



SAMPLE PSSAR - DO NOT SUBMIT

NAME (LAST NAME, FIRST NAME, MIDDLE INITIAL)

<b>PERSONNEL SECURITY SYSTEM ACCESS REQUEST (PSSAR) DEFENSE MANPOWER DATA CENTER (DMDC)</b>		OMB No. 0704-0406 OMB approval expires Mar 31, 2010
The public reporting burden for this collection of information 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 this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to the Department of Defense, Washington Headquarters Services, Executive Services Directorate, Directives Division, 4800 Mark Center Drive, Alexandria, VA 22350-3100 (0704-0496). 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 DMDC Contact Center, as indicated in the instructions.		
<b>PRIVACY ACT STATEMENT</b>		
AUTHORITY: DoD 5200.2-R, Department of Defense Personnel Security Program Regulation; E.O. 12829, National Industrial Security Program; the JPAS Account Management Policy; and E.O. 9397, as amended. PRINCIPAL PURPOSE(S): To request the establishment of user roles and access and validate the trustworthiness of Individuals seeking access to DCII, SWFT, JCAVS, or JAMS. ROUTINE USE(S): The blanket routine uses found at <a href="http://dpcio.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx">http://dpcio.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx</a> may apply. 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 in JPAS.		
TYPE OF REQUEST (REQUIRED) <input type="checkbox"/> INITIAL <input type="checkbox"/> MODIFICATION <input type="checkbox"/> DEACTIVATE USER ID (EXISTING ACCOUNTS)		DATE (YYYYMMDD) date form is submitted
<b>PART 1 - PERSONAL INFORMATION</b>		
1. NAME (LAST, FIRST, MIDDLE INITIAL) if no middle name, enter "NMN"	2. ORGANIZATION Applicant's place of business	
3. OFFICE SYMBOL/DEPARTMENT	4. TELEPHONE (DSN or COMMERCIAL) XXX-XXX-XXXX	
5. OFFICIAL E-MAIL ADDRESS no private addresses (Yahoo, Gmail, etc.)	6. JOB TITLE AND GRADE/RANK Applicant's title	
7. OFFICIAL MAILING ADDRESS place of business mailing address	8. CITIZENSHIP list all	9. DATE OF BIRTH (YYYYMMDD)
10. PLACE OF BIRTH (CITY & STATE/COUNTRY)	11. SOCIAL SECURITY NUMBER XXXXXXXXXX	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 If company /cage code is on KMP, select "Industry"		
<b>PART 2 - APPLICATIONS</b>		
14. DEFENSE CENTRAL INDEX OF INVESTIGATIONS (DCII) (GOVERNMENT ONLY) DCII permissions are established at the initial agency prior to submitting the PSSAR to the Contact Center		
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) (GOVERNMENT/INDUSTRY)		
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: _____		
16. JOINT CLEARANCE ACCESS VERIFICATION SYSTEM (JCAVS) (GOVERNMENT/INDUSTRY)		
a. TYPE OF ACCOUNT REQUESTED: <input type="checkbox"/> ACCOUNT MANAGER Account managers MUST be company employees		
b. ACCESS REQUESTED - INDUSTRY:		c. ACCESS REQUESTED - GOVERNMENT ONLY:
<input type="checkbox"/> LEVEL 2 CORPORATE OFFICER (SCI)		<input type="checkbox"/> LEVEL 2 MACOM/ACTIVITY/HQ/AGENCY SSO
<input type="checkbox"/> LEVEL 3 COMPANY FSO OFFICER/MANAGER (SCI)		<input type="checkbox"/> LEVEL 3 BASE/POST/SHIP/etc. SSO
<input type="checkbox"/> LEVEL 4 CORPORATE OFFICERS MANAGER		<input type="checkbox"/> LEVEL 4 MACOM NON-SCI SECURITY MANAGER
<input type="checkbox"/> LEVEL 5 COMPANY FSO OFFICERS/MANAGER		<input type="checkbox"/> LEVEL 5 BASE/POST/SHIP/NON-SCI SECURITY MGR.
<input type="checkbox"/> LEVEL 6 UNIT SECURITY MGR/VISITOR CONTROL		<input type="checkbox"/> LEVEL 6 UNIT SECURITY MANAGER
<input type="checkbox"/> LEVEL 7 GUARD ENTRY PERSONNEL		<input type="checkbox"/> LEVEL 7 COLLATERAL ENTRY CONTROLLER
<input type="checkbox"/> LEVEL 8 GUARD ENTRY PERSONNEL (SCI)		<input type="checkbox"/> LEVEL 8 SCIF ENTRY CONTROLLER
<input type="checkbox"/> LEVEL 10 VISITOR MANAGEMENT		<input type="checkbox"/> LEVEL 10 VISITOR MANAGEMENT
d. PERMISSION REQUESTED: <input type="checkbox"/> INITIATE PSI <input type="checkbox"/> REVIEW e-QIP <input type="checkbox"/> OVERRIDE PSI (GOV) <input checked="" type="checkbox"/> APPROVE e-QIP (GOV)		

DD FORM 2962, 20141203 DRAFT

PREVIOUS EDITION IS OBSOLETE.

Adobe Designer 9.0



SAMPLE PSSAR - DO NOT SUBMIT

NAME (LAST NAME, FIRST NAME, MIDDLE INITIAL) \_\_\_\_\_

**17. JOINT ADJUDICATION MANAGEMENT SYSTEM (JAMS) (CAF ONLY) FOR CAF ONLY; NOT FOR INDUSTRY CONTRACTORS**

**a. USER ROLES**  
CAF: \_\_\_\_\_ CAF TEAM: \_\_\_\_\_ EMPLOYEE CODE: \_\_\_\_\_

**b. ACCESS REQUESTED:**

<input type="checkbox"/> ACCOUNT MANAGER	<input type="checkbox"/> CUSTOMER SUPPORT
<input type="checkbox"/> MANAGER	<input type="checkbox"/> ADJUDICATOR
<input type="checkbox"/> COMPUTER ANALYST	<input type="checkbox"/> MANAGEMENT SUPPORT
<input type="checkbox"/> CASE ASSIGNMENT PERSONNEL	<input type="checkbox"/> PENDING USER
<input type="checkbox"/> SECURITY ASSISTANT	<input type="checkbox"/> SUPERVISOR
	<input type="checkbox"/> MAILROOM

**c. USER PERMISSIONS:**

<input type="checkbox"/> SAP	<input type="checkbox"/> CASE MANAGEMENT
<input type="checkbox"/> SCI	<input type="checkbox"/> UPDATE CASE COMPONENT
<input type="checkbox"/> TS	<input type="checkbox"/> ASSIGN CAF CASES
<input type="checkbox"/> SECRET	<input type="checkbox"/> REVIEW REQUIRED
<input type="checkbox"/> REPORTS	<input type="checkbox"/> REASSIGN TO OTHER CAF
<input type="checkbox"/> JCAVS	<input type="checkbox"/> ASSIGN/REASSIGN CASES
<input type="checkbox"/> LAA	<input type="checkbox"/> REASSIGN FROM OTHER EMPLOYEE

**d. SPECIAL CASE USER CAN HANDLE**  CAF EMPLOYEES  PRESIDENTIAL SUPPORT  GS-15/GENERAL OFFICER

**e. INVESTIGATION REQUEST PERMISSIONS**  REVIEW PSQ  APPROVE e-QIP

**PART 3 - TRAINING**

I HAVE COMPLETED AND ATTACHED TRAINING CERTIFICATES FOR:

18.  CYBER AWARENESS TRAINING DATE (YYYYMMDD) annual training required for all users

19.  PERSONALLY IDENTIFIABLE INFORMATION TRAINING DATE (YYYYMMDD) annual training required for all users

20.  JPAS TRAINING REQUIREMENTS (IF REQUESTING A JPAS ACCOUNT) DATE (YYYYMMDD) required for all requesting a JPAS account

**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, I will no longer be responsible for an account, and may be subject to criminal charges and penalties.

21. APPLICANT'S SIGNATURE \_\_\_\_\_  
*form will not be processed without signature acknowledging statement above*

22. DATE (YYYYMMDD) \_\_\_\_\_

**PART 5 - NOMINATING OFFICIAL'S CERTIFICATION**

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. These duties include:

*forms submitted without description of duties which require access will not be processed*

23. NOMINATING OFFICIAL'S PRINTED NAME (LAST, FIRST, MIDDLE INITIAL) *For Industry, must be on KMP list. Nominating official cannot be the same as Applicant unless it is a single person facility*

24. NOMINATING OFFICIAL'S SIGNATURE AND DATE  
*form cannot be processed without signature of nominating official*

25. NOMINATING OFFICIAL'S TITLE *single person facility*

26. NOMINATING OFFICIAL'S TELEPHONE NUMBER \_\_\_\_\_

**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.

27. ELIGIBILITY/ACCESS LEVEL: \_\_\_\_\_

28. TYPE OF INVESTIGATION: \_\_\_\_\_

29. ELIGIBILITY GRANTED DATE: \_\_\_\_\_

30. DATE INVESTIGATION COMPLETED: \_\_\_\_\_

31. ELIGIBILITY ISSUED BY: \_\_\_\_\_

32. INVESTIGATION CONDUCTED BY: \_\_\_\_\_

33. VALIDATING OFFICIAL'S PRINTED NAME (LAST, FIRST, MIDDLE INITIAL) *For industry, validation should be provided by the requesting Company unless it is a single person facility in which case the PSSAR team will do this. Specify it is a single person facility on the LOA or a memo attached to the PSSAR.*

34. VALIDATING OFFICIAL'S SIGNATURE AND DATE \_\_\_\_\_

DD FORM 2962 (BACK), 20141203 DRAFT



SAMPLE PSSAR - DO NOT SUBMIT

PERSONNEL SECURITY SYSTEM ACCESS REQUEST (PSSAR) INSTRUCTIONS	
Please see the respective System Access Request Procedures available from the DMDC PSA website for supplemental guidance on completing and submitting this form.	
<p><b>Name.</b> Last Name, First Name, Middle Initial of Applicant. If no middle initial, enter "NMN."</p> <p><b>Type of Request.</b> 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. Complete the User ID field if selecting "modification" or "deactivate."</p> <p><b>Date.</b> Date request is submitted.</p> <p><b>Part 1 - Personal Information.</b></p> <p>1. <b>Name.</b> Last Name, First Name, Middle Initial of Applicant. If no middle initial, enter "NMN."</p> <p>2. <b>Organization.</b> Employing organization of Applicant.</p> <p>3. <b>Office Symbol/Department.</b> Employing office symbol or department.</p> <p>4. <b>Telephone.</b> Telephone number of Applicant. Enter DSN or Commercial as appropriate.</p> <p>5. <b>Official E-mail Address.</b> Official e-mail address of Applicant to be used for account communication.</p> <p>6. <b>Job Title and Grade/Rank.</b> Job title and pay grade or military rank of Applicant.</p> <p>7. <b>Official Mailing Address.</b> Official mailing address of Applicant.</p> <p>8. <b>Citizenship.</b> Country of citizenship. If dual, enter both countries.</p> <p>9. <b>Date of Birth.</b> Applicant's date of birth.</p> <p>10. <b>Place of Birth.</b> City and state, if born in the U.S. Otherwise, enter country and city.</p> <p>11. <b>Social Security Number.</b> SSN of Applicant.</p> <p>12. <b>CAGE Code.</b> Contractor only: CAGE code of Applicant.</p> <p>13. <b>Designation of Applicant.</b> Mark (X) the appropriate box for DoD (e.g., military branches, DoD agencies, DoD contractor companies), non-DoD NISP partner or non-DoD affiliated.</p> <p><b>Part 2 - Applications.</b></p> <p>14. <b>Defense Central Index of Investigations (DCII).</b> Government applicants only.</p> <p>14.a. <b>DCII Agency Code/DCII Agency Acronym.</b> 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.</p> <p>14.b. <b>User Permissions.</b> Requested user permissions are restricted to those granted to the Agency. Elevated permissions for the Agency must be requested from DCII Program Manager.</p> <p>15. <b>Secure Web Fingerprint Transmission (SWFT).</b> For Government and Industry applicants.</p> <p>15.a. <b>Permissions - Fingerprint Submission.</b> Applies to SWFT users. Indicate the requested user permission(s) by marking the appropriate checkbox, or list in item 15.c. on line "Other."</p> <p>15.b. <b>Permissions - Fingerprint Enrollment.</b> Indicate the requested user permission(s) by marking the appropriate checkbox. Only complete this section if you possess or requested a SWFT account (Government only) and are cleared to use the web-based fingerprint enrollment system.</p> <p>15.c. <b>Additional CAGE Code(s).</b> List only if different from item 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.</p> <p>16. <b>Joint Clearance and Access Verification System (JCAVS).</b> For Government and Industry applicants.</p> <p>16.a. <b>Type of Account Requested.</b> Select "Account Manager" only if Applicant is to manage JCAVS accounts on behalf of the organization/company/service.</p> <p>16.b. <b>Access Requested - Industry.</b> Select appropriate permission(s).</p> <p>16.c. <b>Access Requested - Government Only.</b> Select appropriate permission(s).</p> <p>16.d. <b>Permissions Requested.</b> Select appropriate permission(s).</p>	<p>17. <b>Joint Adjudication Management System (JAMS).</b> CAF only.</p> <p>17.a. <b>JAMS User Roles.</b> Provide information and select appropriate boxes for user functions, access and permissions. JAMS is only authorized for CAFs.</p> <p>17.b. <b>Access Requested.</b> JAMS access requested.</p> <p>17.c. <b>User Permissions.</b> JAMS user permission(s).</p> <p>17.d. <b>Special Case User Can Handle.</b> Select high priority cases JAMS user can handle.</p> <p>17.e. <b>Investigation Request Permissions.</b> Select Investigation Request permissions for JAMS user.</p> <p><b>Part 3 - Training.</b></p> <p>18. - 20. <b>Training Requirements.</b> Mark (X) the box to certify training was completed and enter the completion date for all new accounts. Training requirements are defined in the respective System Account Management Policies available from the DMDC PSA website. Certificates must be submitted with PSSAR.</p> <p><b>Part 4 - Applicant's Certification.</b></p> <p>21. <b>Applicant's Signature.</b> Signature of Applicant acknowledging DoD and system policies.</p> <p>22. <b>Date.</b> Date application signed by Applicant.</p> <p><b>Part 5 - Nominating Official's Certification.</b></p> <p>23. <b>Nominating Official's Name.</b> Last Name, First Name, and Middle Initial. If no middle initial, enter "NMN."</p> <p>24. <b>Nominating Official's Signature and Date.</b> The Nominating Official is the individual who is authorizing that the Applicant should have the access requested. For Industry, the Nominating Official must be listed in ISFD as a Key Management Personnel (KMP) in connection with the Facility Clearance, and if an Appointment Letter is needed, it must be signed by the same KMP. The Nominating Official CANNOT be the same as the Applicant unless it is a single person facility. For Government/Civilian, the Nominating Official must be the Security Officer/Manager.</p> <p><b>NOTE:</b> PSSARs submitted without the Nominating Official's statement regarding duties and signature will not be processed.</p> <p>25. <b>Nominating Official's Title.</b> Title of Nominating Official.</p> <p>26. <b>Nominating Official's Telephone Number.</b> DSN or Commercial telephone number of Nominating Official.</p> <p><b>Part 6 - Validating Official's Verification.</b> Do not complete if self-nominating/validating.</p> <p>27. <b>Eligibility/Access Level.</b> Eligibility/Access level of Applicant. See applicable System Account Management Policies/Access Request Procedures available from the respective DMDC PSA system website for minimum eligibility/access requirements.</p> <p>28. <b>Type of Investigation.</b> Type of investigation completed for Applicant.</p> <p>29. <b>Eligibility Granted Date.</b> Date eligibility granted. If not final, state date of interim.</p> <p>30. <b>Date Investigation Completed.</b> Date investigation completed.</p> <p>31. <b>Eligibility Issued By.</b> Organization that issued eligibility.</p> <p>32. <b>Investigation Conducted By.</b> Investigating agency.</p> <p>33. <b>Validating Official's Printed Name.</b> Last Name, First Name, and Middle Initial. If no middle initial, enter "NMN."</p> <p>34. <b>Validating Official's Signature and Date.</b> The Validating Official signature serves to affirm the information provided on the following lines (verify before signing): Eligibility/Access Level; Eligibility Granted Date; Eligibility Issued By; Type of Investigation; Date Investigation Completed; and Investigation Conducted By. For non-DoD government agency requests, the Chief of Security or designee must complete this section.</p>
Return completed forms to the appropriate Account Manager or the DMDC Contact Center as outlined in the respective System Access Request Procedures available from the DMDC PSA website.	

DD FORM 2962 (INSTRUCTIONS), 20141203 DRAFT