



DEPARTMENT OF THE ARMY
OFFICE OF THE DEPUTY CHIEF OF STAFF, G-2
1000 ARMY PENTAGON
WASHINGTON, DC 20310-1000

15 May 2015

DAMI-CD

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Army Joint Personnel Adjudication System (JPAS) Management Guide

1. References:

a. Memorandum, HQDA, ODCS, G-2, 15 Jul 09, subject: Security Management Office (SMO) Contact Information in the Joint Personnel Adjudication System.

b. Memorandum, HQDA, ODCS, G-2, 17 Oct 05, subject: Joint Personnel Adjudication System (JPAS) Procedures Update.

2. The Department of Defense will transition from JPAS to the Joint Verification System (JVS) in FY 16. The JVS is an enterprise system that will enable the application of consistent standards and the reciprocal recognition of clearances throughout DoD. In preparation for migration to the JVS and in support of Continuous Evaluation incident reporting and Insider Threat mitigation, data housed in the JPAS must be accurate and consistently applied throughout the DoD and the Army.

3. This memorandum provides updated guidance on Army JPAS management and supersedes the above references. Effective immediately, each Army Command, Army Service Component Command, Direct Reporting Unit, and Army Agency Head will:

a. Ensure JPAS accounts and data entries are managed in accordance with the enclosed Department of the Army JPAS Management Guide.

b. Update the JPAS Security Management Office (SMO) contact information and validate JPAS accounts semi-annually (January and July).

c. Take the appropriate owning or servicing relationship in the JPAS for all personnel under their cognizance.

4. Security Managers are required to comply with the JPAS Management Guide. The JPAS procedures will be added to the Security Program Benchmarks for the HQDA, G-34 Army Protection Program Assessment.

DAMI-CD

SUBJECT: Army Joint Personnel Adjudication System (JPAS) Management Policy

5. The Office of the Deputy Chief of Staff, G-2 points of contact are Ms. Teane Smith, (703) 695-2629, teane.r.smith.civ@mail.mil and Mr. Sylvester Mitchell, (703) 695-2647, sylvester.mitchell1.civ@mail.mil.

Encl


GERRY B. TURNBOW
Director, Counterintelligence, Human
Intelligence, Disclosure & Security

DISTRIBUTION:

PRINCIPAL OFFICIALS OF HEADQUARTERS, DEPARTMENT OF THE ARMY
COMMANDER

U.S. ARMY FORCES COMMAND

U.S. ARMY TRAINING AND DOCTRINE COMMAND

U.S. ARMY MATERIEL COMMAND

U.S. ARMY PACIFIC

U.S. ARMY EUROPE

U.S. ARMY CENTRAL

U.S. ARMY NORTH

U.S. ARMY SOUTH

U.S. ARMY AFRICA/SOUTHERN EUROPEAN TASK FORCE

U.S. ARMY SPECIAL OPERATIONS COMMAND

MILITARY SURFACE DEPLOYMENT AND DISTRIBUTION COMMAND

U.S. ARMY SPACE AND MISSILE DEFENSE COMMAND/ARMY FORCES
STRATEGIC COMMAND

U.S. ARMY MEDICAL COMMAND

U.S. ARMY INTELLIGENCE AND SECURITY COMMAND

U.S. ARMY CRIMINAL INVESTIGATION COMMAND

U.S. ARMY CORPS OF ENGINEERS

U.S. ARMY MILITARY DISTRICT OF WASHINGTON

U.S. ARMY TEST AND EVALUATION COMMAND

U.S. ARMY INSTALLATION MANAGEMENT COMMAND

SUPERINTENDENT, UNITED STATES MILITARY ACADEMY

DIRECTOR, U.S. ARMY ACQUISITION SUPPORT CENTER

EXECUTIVE DIRECTOR, ARLINGTON NATIONAL CEMETERY

COMMANDER, U.S. ARMY ACCESSIONS SUPPORT BRIGADE

COMMANDER, U.S. ARMY WAR COLLEGE

COMMANDER, SECOND ARMY

CF:

DIRECTOR, ARMY NATIONAL GUARD

DIRECTOR OF BUSINESS TRANSFORMATION

COMMANDER, EIGHTH ARMY

COMMANDER, U.S. ARMY CYBER COMMAND

Department of the Army
Joint Personnel Adjudication
System (JPAS)
Management Guide

Table of Contents

- Part I- Overview3**
 - General.....3
 - Assistance with JPAS application.....3

- Part II- JPAS Account Management.....3**
 - DMDC JPAS Account Management Policy3
 - Establishing JPAS Accounts3
 - Account Managers Responsibilities3
 - Account Request Requirements4
 - Security Management Office (SMO) Management5
 - Account Activity5
 - Account Etiquette5
 - Misuse of JPAS Accounts.....6

- Part III- Personnel Security Actions in JPAS6**
 - Owning/Servicing Relationships6
 - Eligibility7
 - Indoctrinate/Access8
 - Downgrade/Removal of Access.....9
 - Debriefing9
 - Incident Reports9
 - Visit Request9
 - Foreign Travel10
 - Polygraphs.....10

Part I - Overview

1. **General.** The JPAS is the authorized Department of Defense (DoD) personnel security system of record. It is owned and operated by the Defense Manpower Data Center. Users should frequently visit the DMDC JPAS website for system updates and changes.
<https://www.dmdc.osd.mil/psawebdocs/docPage.jsp?p=JPAS>

2. Assistance with JPAS Application

a. Users must contact the Account Manager in their chain of command for account assistance and assistance with how to use the JPAS.

b. Users may contact the DMDC Customer Service for technical assistance with the JPAS:
<https://www.dmdc.osd.mil/psawebdocs/docPage.jsp?p=JPAS&fileNm=CustomerServiceContentInfo.htm>.

Part II - JPAS Account Management

1. **DMDC JPAS Account Management Policy.** JPAS accounts are created and managed in accordance with DMDC guidance. DMDC JPAS Account Management Policy may be viewed at
https://www.dmdc.osd.mil/psawebdocs/docRequest//filePathNm=PSA/appld=560/app_key_id=1559jsow24d/siteId=7/ediPnId=0/userId=public/fileNm=JPAS_Account_Management_Policy.pdf

2. **Establishing JPAS Accounts.** Each HQ Command appoints, in writing, a primary and alternate JPAS Account Manager. The Department of Defense Consolidated Adjudication Facility (DoD CAF) creates JPAS accounts for new Army Headquarter (HQ) Commands. HQ Command's JPAS Account Managers are responsible for creating subsequent accounts for Security Managers (SMs) and Special Security Offices (SSOs) within their subordinate commands.

3. Account Managers Responsibilities

- a. Create JPAS accounts for all subordinate commands.
- b. Issue additional account management policy/guidance for their Command/Organization.
- c. Maintain training certificates for all accounts created.
- d. Ensure the Letter of Appointment (LOA) is signed prior to creating each account.
- e. Maintain accountability for all accounts within their SMO.
- f. Ensure all SMs and SSOs have the appropriate level of access to JPAS.

g. Delete accounts when individuals depart the organization or no longer require JPAS access.

h. Unlock and logoff accounts for users within their command only.

i. Review and validate all accounts within the SMO every January and July.

4. **Account Request Requirements.** The following criteria must be met prior to the creation of a JPAS account:

a. **Investigation/Clearance Requirement.** Account Managers must have and maintain current Secret eligibility or an interim Secret granted by the DoD CAF based on a completed ANACI, NACLC, BI, SSBI or their respective Periodic Reinvestigations (PRs).

b. **Training.** Account Managers ensure all individuals with access to JPAS receive the appropriate instructor led or online training prior to granting system access. The below training and/or certificates are required for all JPAS account access:

(1) Cyber Security Awareness Training
<http://iase.disa.mil/eta/cyberchallenge/launchPage.htm> or Command specific annual security training.

(2) Personally Identifiable Information Training
<http://iase.disa.mil/eta/piiv2/disapii201/module.htm> or
<http://www.cdse.edu/catalog/elearning/DS-IF101.html>

(3) JPAS Training. Applicant must provide proof of recent access to JPAS or provide a certificate of training completed within the last year. The certificate of training must be commensurate to the JPAS sub-system and level of access requested.

i. JPAS/JCAVS Virtual Training for Security Professionals, STEPP course PS123.16 <http://www.cdse.edu/catalog/elearning/PS123.html>, or

ii. JCAVS Level 7 and 10 users may take Introduction to Personnel Security, STEPP course PS113.16 in lieu of the above JPAS training.
<http://www.cdse.edu/catalog/elearning/PS113.html> .

c. **Personnel Security System Access Request (PSSAR).** The PSSAR must be completed and signed by the Validating Official (Commander or Supervisor approving the account), Security Manager and applicant.
<http://www.dtic.mil/whs/directives/infomgt/forms/eforms/dd2962.pdf>.

d. **Letter of Appointment (LOA).** New accounts require a LOA on Command letterhead detailing the specific job duties that require JPAS access and individual (s) authorized a JPAS

account. DMDC requires a Commander or designee in the minimum grade of O-5/GG-14 equivalent to sign the LOA.

5. Security Management Office (SMO) Management

a. Account Managers creates Security Management Offices for the organization.

b. SMO information must be managed and updated when contact information changes (i.e., Primary and/or Alternate contact information changes) or at a minimum, semi-annually (January and July).

c. SMOs will be created using the following guidelines:

(1) SMO Code: Official organization's UIC followed by the JPAS account access level (i.e. A528FJ2 (SCI) or A528FJ4 (non-SCI)).

(2) SMO Name: Enter the Command name.

(3) SMO Location: Base or City, State (add country if OCONUS).

(4) E-mail: Enter the official government e-mail address of both the Primary and Alternate SM/SSO.

6. Account Activity

a. **Active JPAS Account.** An active JPAS account is one that has been logged into in the past 30 days.

b. **Inactive JPAS Account.** JPAS accounts are rendered inactive and locked by the system after 30 days of nonuse. Only an Account Manager in the User's chain of command can unlock the account.

c. **Deleting Inactive JPAS Accounts.** JPAS accounts are deleted by the system after 45 days of nonuse (on the 46th day). A new account must be established following the above account request procedures.

7. Account Etiquette

a. Users are prohibited from sharing their user name, password, or other authentication information with any other individual, including anyone who is a designee or an alternate to the account holder. Sharing of user names and passwords will result in account termination.

b. Prior to departure, users leaving their organization must notify their Account Manager to terminate their JPAS account.

c. Account Managers may only unlock accounts for individuals in their direct line of support.

d. Users may review JPAS records for official use only. Review of JPAS records for friends, colleagues or high profile cases is strictly prohibited unless it is for official business.

8. Misuse of JPAS Accounts

a. When signing into JPAS, Users consent to the terms of use for the system and agree to maintain compliance with the Privacy Act of 1974 and all applicable JPAS rules and regulations, to include the JPAS Account Management Policy.

b. Misuse of JPAS will result in termination of the JPAS account. Additionally, DMDC automatically submits a misuse of technology incident report in JPAS. At DMDC's discretion, information concerning violations of JPAS policy may be referred to other federal agencies for consideration of administrative, civil or criminal sanctions when circumstances warrant.

c. Reviewing a high profile individual's personnel security records without a justifiable need to know, querying your own record, or entering/viewing "dummy" social security numbers in JPAS is considered a misuse of JPAS and will result in account termination.

Part III- Personnel Security Actions in JPAS

1. **Owning/Service Relationship.** When in-processing personnel, SMs/SSOs will establish the appropriate owning or servicing relationship as described below. Organizations with unique requirements shall coordinate with other SMOs to determine the best owning and servicing relationship.

a. Security Managers.

(1) Security Managers takes an "owning" relationship (non-SCI SMO) for all personnel assigned to their command/unit.

(2) Security Managers takes a "servicing" relationship on all personnel they do not "own" but for whom they provide support services to (i.e. visitors, IMCOMs, contractors working onsite).

(3) SMs/SSOs may take a "servicing" relationship on incoming personnel that are still "owned" by the losing SMO. Once those individuals are out-processed from their previous organization, the gaining SM must change the relationship from "servicing" to "owning."

b. SSOs.

(1) SSOs will take an SCI owning relationship of all SCI indoctrinated personnel assigned to their organization.

(2) The owning SCI SMO may request an indoctrination assist from another organization. SSOs indoctrinating an individual into SCI access as a result of an indoctrination assist will take a “servicing” relationship.

c. Contract Support Element (CSE).

(1) CSE is the “owning” SCI SMO for all Army affiliated contractors requiring access to SCI.

(2) CSE is the “servicing” SCI SMO for Army affiliated contractors requiring access to SCI in situations where the “owning” SCI SMO is a non-Army element of DoD.

d. Industry.

(1) Contractor Facility Security Officers (FSOs) will “own” their personnel and create the appropriate category for the individual in JPAS (non-SCI SMO).

(2) CSE will own contractor personnel they indoctrinate into SCI access (SCI SMO only).

(3) Army Security Managers will establish servicing relationships with contractors working on a classified contract or an owning relationship for uncleared contractors that have a security action in progress.

e. U.S. Army Reserve Command (USARC).

(1) USARC will take an owning relationship on all Active Guard Reserve (AGR) and Troop Program Units (TPU).

(2) When an AGR/TPU Soldier is in mobilization, Contingency Operations Temporary Tour of Duty, active duty for special work, active duty for training or on annual training orders, Commands in which the Soldier is currently assigned will take a “servicing” relationship.

f. Human Resources Command (HRC).

(1) The Commander, HRC takes an owning relationship of all Individual Ready Reserves (IRR), Individual Mobilization Augmentees (IMA), and Retiree Recall personnel.

(2) When an IRR/IMA/Retiree Recall Soldier is in mobilization, Contingency Operations Temporary Tour of Duty, active duty for special work, active duty for training or annual training orders, Commands in which the Soldier is currently assigned takes a “servicing” relationship

2. Eligibility

- a. The most recent eligibility determination is reflected in the “Eligibility” field and takes precedence over earlier eligibility determinations.
- b. Adjudications are valid for all DoD personnel, regardless of which DoD agency made the adjudication.
- c. Scattered Castles is another valid means of verifying SCI eligibility in the event eligibility is not in the JPAS. The Scattered Castles eligibility may only be used to grant access to classified information if the eligibility was granted by a DoD agency. Submit a Request for Action (RFA) in the Case Adjudication Tracking System (CATS) portal requesting Scattered Castles eligibility be entered in the JPAS or recertified to the DoD.
- d. Contractors. The DoD CAF (Industry Division) enters the collateral adjudication determination; the DoD CAF (Army Division) enters the SCI adjudication determination.
- e. Interim Security Clearance Eligibility. Interim security clearance eligibility must be documented in JPAS before access is granted.

3. **Indoctrinate/Access.** Individuals may be granted access to classified information if they have the required eligibility in JPAS and have signed a Nondisclosure Agreement (NDA) in accordance with AR 380-5, Information Security Program.

- a. Prior to granting personnel access, SMs/SSOs will ensure the appropriate NDA date is recorded in the system.
- b. Once JPAS contains the appropriate NDA date, a new NDA will not be executed.
- c. When the original NDA date is not available for Military or Civilian personnel, it is acceptable to have the individual read and execute a new NDA for the purpose of recording the NDA date in JPAS.
- d. The newly signed Standard Form 312, Classified Information Nondisclosure Agreement, will be recorded in JPAS and the originals forwarded in accordance to AR 380-5 or subsequent G-1 guidance.
- e. The level of access will be entered into JPAS by SMs/SSOs using the Indoctrinate link. The Indoctrinate link will not appear if an individual’s investigation type does not meet the current investigation level.
- f. Personnel whose SCI eligibility/access information is not displayed in the JPAS may be granted SCI access provided there is current written verification of SCI eligibility on file and an RFA is submitted in the CATS portal, requesting the DoD CAF grant SCI eligibility in JPAS.

g. Internal access rosters for DoD personnel not derived from JPAS data are not authorized. Internal access rosters must be updated with new eligibility/access information when there is a change of eligibility/access in JPAS.

h. Contractor Access.

(1) The Facility Security Officer enters collateral access information for contractors.

(2) CSE may request administrative assistance (indoctrination assist) for SCI indoctrinations. A copy of the SCI indoctrination oaths and Non-Disclosure Statements (NDS) will be sent to CSE.

(3) The local SSO will enter SCI access as outlined in the indoctrinate assist. CSE may enter SCI access on behalf of the SSO.

4. **Downgrade/Removal of Access.** If an official duty position no longer requires access to the higher level of classified information, the individual's access will be downgraded to the proper level (i.e. An individual with TS eligibility/access is now in a position requiring Secret access. The access will be downgraded to Secret). If access is no longer required for a position, the individual shall be debriefed (AR 380-5) and access (es) removed from JPAS.

5. **Debriefing.** Individuals will be debriefed in accordance with AR 380-5 when departing/out-processing the organization of assignment. The SM/SSO documents debriefings and removes access in the JPAS. If the individual has been granted a transfer in status (collateral or SCI), remove the individual from the PSMNet but do not remove accesses from the JPAS.

6. **Incident Reports.**

a. SMs/SSOs will submit incident reports in JPAS only. Owning and servicing SMOs will coordinate prior to submission.

b. DA Form 5248-R, Report of Unfavorable Information for Security Determination, is completed and signed (in block 15) by the Commander to report adverse information.

c. Incident reports will contain the following information

(1) Basis of Report – offense/credible derogatory information

(2) Action taken

(3) Commanders recommendation

(4) Name, grade, title and contact telephone number of the submitting Security Manager. This information is mandatory and is annotated at the end of the incident report summary.

d. Incident reports are submitted via the JPAS incident report link.

e. The signed DA 5248-R for uncleared individuals or individuals with no JPAS records will be uploaded in the CATS portal using the Incident Report RFA.

f. Enclosures, such as supporting documentation, are uploaded via the Incident Report link in the CATS Portal.

7. **Visit Requests.**

a. In accordance with DMDC JPAS account management policy, it is prohibited to request a JPAS printout or send a JPAS printout to another organization that has JPAS and where the individual's record in JPAS has all of the required information.

b. Military, Civilians, and Contractors visiting Army activities are not required to submit visit authorization letters if their access level and SMO affiliation are accurate in the JPAS.

c. Visit requests submitted through JPAS will NOT be accepted if they do not reflect accurate eligibility, access, NDA Date, and appropriate SMO identification.

d. Visit requests will be cancelled when an individual out-processes or no longer has access to classified information.

8. **Foreign Travel.** Foreign travel will be entered in the CATS portal in accordance with memorandum, ODCS, G-2, 5 Dec 12, subject: Automated Foreign Contact and Foreign Travel Reporting.

9. **Polygraph.** Polygraph information may be entered into JPAS by any CAF or by a SMO that has been granted Polygraph privileges by an Account Manager.