OUTLINE SHEET 7.0

Joint Personnel Adjudication System (JPAS)

REFERENCE

SECNAV M-5510.30, Appendix E

OUTLINE

A. Joint Personnel Adjudication System (JPAS)(PSP, Appendix E)

1. Mandated personnel security system for all Department of Defense (DOD) personnel to include contractors and the Central Adjudication Facilities (CAFs)

2. Web based system accessed by going to www.dss.mil - Web page provides updated information on JPAS and access to JPAS login screen

3. JPAS is the overall system with two subsets:

   a. Joint Clearance and Access Verification System (JCAVS)

      - Used by authorized command security personnel
      - Functions as the master personnel security data base
      - Means by which commands can communicate with Department of the Navy Central Adjudication Facility (DON CAF)

   b. Joint Adjudication Management System (JAMS)

      - Used only by DON CAF and the other DOD CAFs
      - Serves as the permanent DOD personnel security investigation and clearance record
      - Means by which DON CAF can communicate with individual commands on personnel security actions

4. JCAVS Users

   a. Account Manager – Performs management functions in JCAVS (e.g., adding new users, unlocking users, etc.)- Recommend two Account Managers per command (e.g., Security Manager and Assistant)

NOTE: Anyone assigned as an Account Manager is also assigned as a User

b. User – Performs all the functions of the system, except for the read only and limited performance levels (see below)- Number of users and user levels determined by command

5. Non-SCI JCAVS User Levels

Level 4 - Security Managers and assistants at major commands (read and write access)

Level 5 – Security Managers and assistants at 3rd and 4th Echelon commands (read and write access)

Level 6 – Unit Security Managers and assistants (read and write access)

NOTE: A user at any one of the above levels performs the same functions in the system (e.g., a user at level 5 does not have more capabilities than one at level 6). The assignment of user level is tied to the level command is set up in JPAS under the Security Management Office Code. If a command is set up at level 5 in JCAVS then all read/write users at the command should be at that level.

Level 7 – Read only access (set up for access points where clearances and visit requests are checked)

Level 10 – Limited access – Only authorized to send and receive visit requests

6. SCI Levels

Level 2 – SSOs (SSO Navy Only) (read and write access)

Level 3 – Command SSOs and SSRs (read and write access)

Level 8 – SCI entry control personnel (read only access)

7. Investigative Requirements to be put on as a JCAVS User at a non-SCI Level (4, 5, 6, 7 or 8)

a. Final security clearance eligibility with a current NACLC, ANACI (civilians only), SSBI, SSBI-PR, or PPR (all these investigations will be covered in Lesson Topic 7.2, Personnel Security Investigations)

b. If prospective user does not have a current clearance eligibility based on one of the above, “interim access” to JCAVS can be granted if the individual has a Secret clearance eligibility based on an investigation completed before January 1999 and has submitted a NACLC which is documented in JCAVS as an open investigation

8. Investigative Requirements to be put on as a JCAVS User at a SCI Level (2, 3 or 8)

a. Final clearance with SCI access issued on a current SSBI or SSBI-PR (within 7 years) or have a clearance with a SSBI-PR submitted which is documented in JCAVS as an open investigation

b. In addition to meeting the above requirement must also be documented in JCAVS as having been granted SCI access

B. Guidelines on Using JCAVS (PSP Appendix E)

1. Adding new users and account managers on JCAVS

a. All personnel requesting JCAVS access must fill out a JCAVS System Access Request (SAR) Form, available from the JPAS web page *www.dss.mil*

(On “Office Symbol” line put Security Management Office code (explained below))

b. Submit to Account Manager at command or if none assigned to next senior in administrative chain of command

c. Account Manager who puts on user will maintain the JCAVS System Access Request (SAR)Form while user has JCAVS access and 1 year after being removed from the system (e.g., transfer from command)

d. When Account Manager performs function to add a user, JCAVS will generate a User ID and password. The User ID will stay the same, the password will have to be changed with first log in. Thereafter password must be changed every 90 days

NOTE: Sharing a User ID and password is prohibited. Commands can be denied access if account sharing is discovered.

2. Security Management Office (SMO) - How commands are established in JPAS is essential to the command operations of JCAVS

a. SMO screen can be viewed from both the User and Account Manager Menus but only an Account Manager can make changes to the SMO information

b. SMO screen should contain:

SMO Code: Command’s SMO Code should be command UIC or RUC and level (4, 5, or 6 non-SCI; 2 or 3 SCI). If command is assigned more than one UIC/RUC choose one as SMO code. (Do not have multiple SMO codes for one command – only exception would be if have a SCI SMO and a non-SCI SMO)

NOTE: Some Navy SMOs were set up with “N” in front up the UIC and some USMC with the MCC following the RUC

SMO Name: Use command’s plain language (message) address

SMO Location: Use command’s physical location (e.g., San Diego CA, Naples Italy)

Service Agency: Preset “N” for Navy or “M” for Marine Corps (Navy personnel cannot set up a Marine Corps account and vice versa)
Office Level: SMO level (Non-SCI 4, 5, or 6; SCI 2 or 3)

Active Date: When SMO was established in JPAS

Commercial Phone/Fax/DSN: Numbers for current command JCAVS POC (Person who DON CAF or other commands can contact)

Email: Command JCAVS POC’s email (two or three separate emails can be listed)

NRO/Service Secretary/OSD/ES Designations: N/A - Do not check boxes

Active Parent SMO(s): Usually immediate Senior in Chain of Command is listed as parent. All “Active Parent SMOs” must reflect Navy JCAVS Program Manager, level 4. Click “Add/Maintain Parent Relationships” button to add parent.

> NOTE: As a “parent” system allows monitoring of subordinate commands, i.e., functions as a management tool and as back-up to subordinate commands

Affiliated Users: Provides list of users assigned to SMO (Click “View” button)

3. “Owning” vs. “Servicing” Relationships - JCAVS is set up so a SMO can either “own” or “service” an individual.

    a. Normally individuals will be “owned” by their command SMO and can be owned by only one non-SCI SMO and one SCI SMO in a Person Category. **Commands must “out-process” individual upon transfer**

    b. “Servicing” normally occurs when individual is on a temporary basis outside owning command (SMO) (e.g., school assignment, TAD, servicing agreement). Individual can be serviced by multiple SMOs. (Owning” SMOs notified of actions taken by “servicing” SMO(s)

    c. Owning non-SCI and SCI SMOs will appear on individuals Person Summary (explained below)

4. Person Category or Categories in JCAVS

a. Individual’s status within DOD (e.g., active duty, reserve, civilian) - Data fed in by personnel databases (e.g., PID, DEERS, MCTFS, DCPDS)

b. If no person category exists then no personnel security actions can be documented in JCAVS on individual

c. Individuals can have more than one person category (e.g., individual is both a civilian employee and a reservist). When taking personnel security actions ensure correct person category is selected

5. Personnel Security Management (PSM) Net - Listing of all personnel SMO owns or services

a. Provides the following headings: SSN, Name, Person Category, Organization, Relationship, Change Button (can change relationship from owning to servicing or vice versa) and Remove Button (allows user to remove person from SMO)

b. Defaults to “sort by last name” but can sort by the other headings

NOTE: Must take action to own or service an individual before they appear in PSM Net

c. Associates commands with personnel for whom they have security responsibility - Based on security relationships with individual person categories rather than unit/organization

6. “Save” button - Hit only when sure this is what you want to save and hit only once. (Once the save button is hit the information is in the system tied to your user ID)

7. Person Summary Screen - Provides personnel security data on each individual in JPAS. (With a SSN user can view any person in JPAS)

a. Once an individual is owned/serviced links show up which allow SMO user to take and document security actions (these will be discussed in the personnel security lessons)

b. Information provided on Person Summary Screen

Top portion of screen

PID data: Name, SSN, Date of Birth, Place of Birth (may show N/A), Citizenship

Person Category/Categories: Status in JPAS, e.g., active duty, reserve

Date and type of PSI that is “pending” at OPM; (if applicable)

Date PSQ Sent (if applicable)

Other Information: Signature dates of Nondisclosure Agreement (NdA), Nondisclosure Statement (NdS) (SCI only), and Attestation. Polygraph information and Foreign Relation

Financial Consent and Disclosure: Appear but not yet populated

Middle portion of screen

Access blocks: (one block for each person category

Organization: Current organization

Organization Status: Contractor Facility Clearance

Occupation Code: Civilian – job series, USN enlisted – rating, USN officer – designator, USMC enlisted and officer – MOS

SCI SMO and non-SCI SMO: Owning SMO’s UIC/RUC, Organization name, SMO level and POC phone and email and “yes” or “no” indicated (as applicable) re Servicing SMO

Office Symbol:

Grade: Pay grade

Arrival date:

PS: Civilian position sensitivity

Office Phone Comm/DSN: SMO entry

Retire/Separation Date:

RNLTD: Projected arrival date

Proj UIC/RUC/PASCODE:

TADMSD: Service entry date

Interim: Interim clearance granted by command (if applicable)

Projected Departure date:

Bottom portion of screen

Investigation Summary: Current action on investigation

Adjudication Summary: Current DON CAF action (This is where current investigation completion date and DON CAF clearance adjudication will appear)

External Interfaces:

Perform SII Search: If investigation being done by Office of Personnel Management can get some information on investigation

DCII: Used by investigation/ adjudication personnel only