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

DAMI-CD (380-67) 17 Oct 05

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Joint Personnel Adjudication System (JPAS) Procedures Update

1. References:

a. Memorandum, HQDA G-2, DAMI-CD, 26 Jan 05, subject: Changes to Procedures re: Submission of Personnel Security Investigations (PSIs); and the Use of the Joint Personnel Adjudication System (JPAS).

b. Memorandum, HQDA G-2, DAMI-CD, 6 May 05, subject: Joint Personnel Adjudication System (JPAS) Implementation Extension.

2. Enclosure 1 supersedes references 1a and 1b. Enclosure 2 is a highlighted version of enclosure 1 and depicts recent changes and updated procedures to reference a.

3. We are not extending the deadline for the mandatory use of JPAS as the Army's personnel security system of record. Many Army organizations have moved swiftly to implement the use of JPAS and have made significant strides in creating their Security Management Offices, taking, owning, or servicing relationships; and entering their access/NDA information. We realize that there is still missing information within JPAS and that some personnel and/or units are still not listed in JPAS (and in some cases do not yet have JPAS access). This office will work with those organizations to assist in resolving any remaining issues. Unless the latter is the case, the procedures listed in enclosure 1 will be followed immediately.

4. Recent connectivity between JPAS and the Total Army Personnel (TAP) systems identified issues (e.g., incorrect person category, incorrect personnel identifying data, etc.,) that are being resolved with continued testing of the data. We recognize there are challenges and that it may still take several months to verify that the connectivity is complete and performing as desired.

DAMI-CD (380-67)
SUBJECT: Joint Personnel Adjudication System (JPAS) Procedures Update

5. Points of contact are Mrs. Julia Swan, (703)695-2629/DSN 225-2629, e-mail: Julia.swan@us.army.mil, or Ms. Teresa Nankivell, (703) 695-9605/DSN 225-9605, email: teresa.nankivell@us.army.mil. All inquiries should be addressed through your command channels.

2 Enclosures

THOMAS A. GANDY
Director, Counterintelligence, Human Intelligence, Disclosure and Security

DISTRIBUTION
Commander, Eighth Army, ATTN: EAGB/ACofS, G2
Commander, U.S. Army Europe and Seventh Army, ATTN: AEAGB-SAD-S
Commander, U.S. Army Forces Command, ATTN: AFIN-SD
Commander, U.S. Army Criminal Investigation Command, ATTN: CICG-SC
Commander, Chief, National Guard Bureau, ATTN: NGB-SDS (Ms. Gravely)
Commander, U.S. Army Corps of Engineers, Office of Security & Law Enforcement, ATTN: CECS-OI
Commander, U.S. Army Intelligence and Security Command, ATTN: IASE-IS
Commander, U.S. Army Medical Command, ATTN: MCOP-O-SI
Commander, U.S. Army Pacific Command, ATTN: APIN-SC (Mr. Quigley)
Commander, U.S. Army Training and Doctrine Command, ATTN: ATIN-SE
Commander, U.S. Army Materiel Command, ATTN: AMXMI-SCM
Commander, U.S. Army Test and Evaluation Command, ATTN: CSTE-OP-SSI
Commander, JFHQ-NCR/U.S. Army Military District of Washington (MDW) ATTN: J/G-3
Commander, U.S. Army South, ATTN: SOIN-SD
Commander, U.S. Army Special Operations Command, ATTN: ODCS, G-2
Director, Installation Management Agency, ATTN: SFIM-OP (Mr. Stout)
Deputy Commanding General, Military Surface Deployment and Distribution Command, ATTN: G2
U.S. Army Space and Missile Defense Command, ATTN: SMDC-IN-S
U.S. Army Records Management and Declassification Agency
US Army Network Enterprise Technology Command/9th Army Signal Command
DoD Homeland Security Office, ATTN: Security Manager
HQDA, Office of the Administrative Assistant to the Secretary of the Army, ATTN: Chief, Personnel & Physical Security Division
Army National Guard Readiness Center, ATTN: NGB-ARO-I
Program Executive Office – Simulations, Training, and Instrumentation (PEO-STRI), ATTN: SFAE-STRI-BOO (Security Office)
Commander, US Army Central Clearance Facility, ATTN: Ms. Chandler

JPAS System of Record Procedures

1. Effective 14 Feb 05, Commands with access to the Joint Personnel Adjudication System (JPAS) are to use the Joint Clearance and Access Verification System (JCAVS), a subsystem of JPAS, to perform the functions listed below. Commands/units that do not yet have JPAS access, will obtain that access and comply with the requirements listed below. (Please notify this office, through command channels, those organizations/activities that do not, but should have JPAS access).

a. Establish JPAS accounts: CCF will be the Army Account Manager for Army MACOMs, Reserve Command HQ, Reserve Support Commands, and the National Guard Bureau, to include the 50 State and US Territory National Guard HQ. Each MACOM will appoint an Account Manager. MACOM JPAS Account Managers will be given level 2 and/or level 4 accounts as appropriate. MACOM JPAS Account Managers will in turn create appropriate accounts for their subordinate units and subordinate Security Managers (SMs)/Special Security Offices (SSOs). Contract Support Element (CSE) INSCOM is the supporting SSO for Army-affiliated SCI Contractors. Account Managers will also ensure that all SMs/SSOs have the appropriate level of access based on their duties, training and scope of responsibility. When creating Security Management Offices (SMOs) within JPAS, ensure that the following information is filled in as described below on the Security Management Office Maintenance Screen. All fields with asterisks will also be filled in.

(1) SMO Name: Enter the Command Name and the physical location. For the location portion, use the same location construct as outlined in #2 below. (e.g. Army HQ, G-2, Washington, DC or Army Materiel Command, Fort Belvoir, VA)

(2) SMO Location: Option 1 - Base, State or Country; Option 2 - City, State or Country (e.g. Fort Polk, LA or Washington, DC or Stuttgart, Germany)

(3) e-mail: Primary SM/SSO POC Name, Phone, email; Alternate SM/SSO POC Name, Phone, email. (e.g. Joe Soldier, (123) 555-1234, joe.soldier@us.army.mil; Jane Civilian, (123) 555-4321, Jane.civilian@us.army.mil) Please ensure as a minimum, that each SMO have an alternate POC with their contact information listed, and that your SMO information contains all information as noted above.
This will cause the SMO fields on the Person Summary page to look like this:

Army HQ, G-2, Washington, DC, John Soldier, (123) 555-1234, joe.soldier@us.army.mil; Jane Civilian, (123) 555-4321, Jane.civilian@us.army.mil

This will make it easier for SMs/SSOs to track down and contact other security offices, especially when a member needs to be out-processed at their losing command prior to being in-processed at their new organization. An owning relationship can be established with only one SCI and one non-SCI SMO. This information can only be updated by an account manager and should be updated whenever critical information changes (i.e., Primary and or Alternate contact information). Please ensure this

information is kept current and that their JPAS accounts are deleted when no longer assigned as a Security Manager with your organization.

b. Training: Account Managers will ensure that all personnel with access to JPAS have received the appropriate live or online training prior to being granted system access. The JITA link is intermittently available; apparently it goes down on occasion. DSSA is currently working on updating the training module. It is expected that the new training link, JPAS Training System (JTS) will be available around the December timeframe and will be located on the JPAS website https://jpas.dsis.dod.osd.mil/. In the event that the JITA link is down, Account Managers should require all new users to read the JCAVS Desktop Resource (August 2004) and have it certified that the tutorial was read. Account Managers will be able to grant access to JPAS once a certified memorandum is completed. This resource will answer most frequently asked questions and will suffice as an interim measure to satisfy the training requirement.

c. Establish Owning/Servicing relationship/PSM Net: Every SM/SSO will create a relationship with each individual that they are responsible for. Every individual must be owned by a SMO in order for JPAS notifications (adjudications, suspensions, etc) to be transmitted to owning and servicing offices. To determine what type of relationship should exist, use the following guidelines.

(1) SSOs will take an "owning" relationship of all Sensitive Compartmented Information (SCI) cleared personnel that are in their SCI billets by becoming their SCI SMOs. CSE INSCOM will be the "owning" SCI SMO for all Army affiliated contractors requiring access to SCI.

(2) SSOs will take "servicing" relationship of all SCI personnel that they are providing support to when the individual's SCI billet is held by another command/organization. CSE INSCOM will be 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.

(3) Security Managers will take an "owning" relationship of all personnel within their command/unit by becoming their non-SCI SMOs. This will provide local Security Managers/Commands/Units with visibility of the status of all of their personnel. It will also cause initial questions regarding clearance issues to be directed to the local Security Manager.

(4) Security Managers will take a "servicing" relationship of all personnel that they do not "own" but for whom they provide supporting services to. (This may include consolidated security offices that provide final transmission of Personnel Security Investigation (PSI) forms and/or maintaining official security records) This will also ensure that servicing security offices can have oversight for all supported personnel and units. These consolidated security offices, in coordination with the owning office, will determine which personnel security functions will be performed by each office. Two important guiding principles should be adhered to. First, duplication of effort will be

avoided. Second, functions retained by an owning office should be based on that offices ability to effectively execute those functions. For example: Owning offices that service less than 25 personnel, should consider having most of their functions performed by the consolidated security office. Owning offices that do not have trained "0080-Security Specialists" to perform personnel security functions should also consider having their functions performed by their consolidated security office. Where none of the above conditions apply, it seems appropriate that consolidated security offices would provide support and assistance to the owning organizations.

(5) Contractor Security Officers have access to JPAS. They will "own" their personnel and enter the individual into JPAS. Defense Industrial Security Clearance Office (DISCO) will enter the collateral adjudication information. The Army Central Clearance Facility (CCF) will enter the SCI adjudication information. The FSO will enter the collateral access information. CSE will enter the SCI access information. Army SSOs and SMs will establish servicing relationships with their contractor personnel. CSE may request administrative assistance for SCI indoctrinations and may request that the local SSO enter the Indoctrination information into JPAS. A copy of the SCI Indoctrination oaths and Non-Disclosure Statements (NDS) will be sent back to CSE.

(6) Security Managers will not take an "owning" relationship in JPAS for Reserve soldiers who are currently on mobilization, COTTAD, ADSW, ADT, or AT orders. The United States Army Reserve Command (USARC) and the Army Human Resources Command - St. Louis will take the "owning" relationship. This pertains to the following categories of Reserve Soldiers: Individual Ready Reserves (IRR), Individual Mobilization Augmentees (IMA), Retirees, and Regional Readiness Reserve Commands (RRC) and Training Divisions (TD). Security Managers for these personnel should take a "servicing" relationship. An exception to the above will be Troop Program Units (TPU) that are managed offline. (Example Psychological Operations Group, Eighth Army, 7th ARCOM, etc.) In addition, if the Reserve Soldier has executed a SF312 and the information has been loaded into JPAS or needs to be loaded to JPAS, the original document should be sent to the following address: Commander, Human Resources Command, ATTN: AHRC-PLF (Security), 1 Reserve Way, St. Louis, MO 63132-5200 to be filed into the Soldier's electronic Official Military Personnel File (OMPF).

d. Use JPAS to Communicate with CCF: Communicating with CCF to request the following services will now be accomplished via the Request to Research, Recertify/Upgrade Eligibility (RRU) link on the Person Summary screen. All communications via JPAS to CCF will have in the Remarks Section POC information, e.g. name, grade, title, and contact telephone number of the submitting security manager. This information is mandatory.

(1) DA Form 5247: The Request to Research, Recertify/Upgrade Eligibilty (RRU) function in JPAS will replace the DA Form 5247. A statement of verification of citizenship, the document used for verification (when applicable), and dates of continuous federal service will continue to be provided with each RRU submission. CCF is working very diligently to eliminate the backlog of RRUs. What would help them

in this endeavor is for the field to discontinue (and must cease sending) the following types of RRUs:

:

a. Do not send duplicate RRUs by following up with a paper request (DA Fm 5247-R), trust that your RRU has been received in JCAVS. You should check the notification link in JPAS for verification that your RRU has been received.

b. Do not send requests for copies of DA Fm 873 (remember – JPAS is the system of record for verifying eligibility and accesses)., The only time CCF will electronically send a DA Fm 873, is when there is a "No Person Found" or "No Person Category Found" in JPAS.

c. Do not send requests for adjudication of completed investigations (CCF will adjudicate all investigations requiring eligibility) until they have been pending at CCF for 6 months.

d. Do not send RRUs requesting transfer of an Air Force eligibility and/or issuance of a DA Fm 873. (JPAS is DoD's system of record, no RRU is required). Once the appropriate Manpower Personnel System is uploaded into JPAS it will reflect the current service.

e. Do not send RRUs advising of name changes and requesting a new DA Fm 873. (Again, once the Personal Identification Data (PID) is uploaded into JPAS it should reflect current name – if not, then the individual concerned needs to go to their Personnel Officer and submit the necessary paperwork because the PID information is currently provided by the Defense Manpower Data Center (DMDC). Once the respective TAPs are connected to JPAS, JPAS will then be updated every two weeks (every other Thursday) beginning sometime between October and November 2005. You may also refer to the FAQs (question #16) located on JPAS's home page.

f. Do not send RRUs requesting Interim SCI eligibility. Utilize the Request Interim SCI link in JPAS for requests for Interim SCI eligibility. Email the required supporting documentation (SF 86 & compelling need) to: interimsci@CCF1.ftmeade.army.mil or by FAX (COMM): 301-677-2706, DSN: 622. NOTE: Must be a level 2 or 3 user to request Interim SCI eligibility.

g. Do not request downgrade of security eligibility, subject has a Top Secret Eligibility and only needs Secret access at his current unit – remember that administrative access downgrades are handled at the Unit level.

h. Do not request the status of an investigation. You can check on the status of an investigation by simply looking it up in JPAS to see if it is open, or by calling OPM at 724-794-5228. You must have a registered SOI and or SON. This may be accomplished by calling 724-794-5612 or forms to request an SOI and or SON can be found on the HQDA, G-2 website

http://www.dami.army.pentagon.army.mil/offices/dami-cd. PIPS Form 11 is used to establish an SOI. The PIPS Form 12 is used to establish a SON.

i. Do not send RRUs advising of a subject's retirement.

j. Do not send RRUs requesting reinstatement of a denied/revoked clearance without sending the required documentation. The required documentation is as noted in AR 380-67, 8-201.1 and will be faxed to CCF at 301-677-2706.

k. Do not send paper copy's of DA Fm 5247-R or DA Form 5248-R as RRUs receive priority over paper requests.

l. Do not send requests for adjudication of closed PSIs, including SBPRs (except when the PSI has been closed for more than 6 months);

(2) DA Form 5248-R: Unfavorable Information Reports.

a. The DA Form 5248-R (Report of Unfavorable Information for Security Determination) has been eliminated with one exception. When there is a "No Person Record" in JPAS, the unit will submit a hardcopy DA Fm 5248-R with documentation via mail or scanned and send an email to the address mentioned in paragraph (2) b. below. The unfavorable information reporting requirement will be accomplished via the JPAS Report Incident Link on the Person Summary Screen.

b. Enclosures or other supporting documentation previously submitted in conjunction with a 5248-R will be forwarded to CCF either by e-mail (INCIDENTREPORT@CCF1.ftmeade.army.mil) or when email is not available, by FAX (COMM: 301-677-2706, DSN: 622).

c. Security Managers and SSOs will be the only persons authorized to submit incident reports. Incident reports will be submitted by the SM who has knowledge of the unfavorable information. Owning and Servicing security offices will coordinate prior to submission.

d. Incident reports will contain the following information:

1. Basis of Report - offense/allegation;

2. Action Taken;

a. Commander's Recommendation (Ensure commander's recommendation is provided to CCF and is on file with the local security office);

b. Any supporting documentation being forwarded to CCF;

c. Name, grade, title and contact telephone number of the submitting security manager, annotated at the end of the summary. This information is mandatory.

(3) Requests for Interim SCI Eligibility: This function will now be accomplished via JPAS by clicking on the Interim SCI link found on the Person Summary Screen and providing the required information. (Do not forward or fax a paper copy of the JPAS Person Summary Screen). CCF acts upon all requests for Interim SCI Eligibility within 2 working days. Documentation supporting a request for interim SCI eligibility will be sent to CCF by e-mail INTERIMSCI@CCF1.ftmeade.army.mil or when email is not available, by FAX (COMM: 301-677-2706, DSN: 622. Remember, only SM/SSOs having either a 2 and 3 user level will have access to the Interim SCI link.

(4) Green Mailers: Effective with the implementation of JPAS, CCF green mailers will be eliminated. Information currently provided via green mailers that is not routinely reflected in JPAS will be disseminated in the "Notifications Link, Message to CAF". **REMINDER**: CCF will not be able to communicate with SMs/SSOs that do not have an owning or servicing relationship of the subject in question. CCF is only sending out green mailers when there isn't a SMO established who has an owning relationship with an individual. There must be an owning relationship before any servicing SMO can be notified.

(5) DA Form 873: With the implementation of JPAS, DA Form 873 has been eliminated. The only exception is when there is " No Person Record Found" or "No Person Category".

e. Verify current clearance level eligibility: Current eligibility for classified material access authorization will now be done by sighting the "eligibility" field on the Person Summary screen. Do not assume that the information on the Person Summary screen is all inclusive. Make it a practice to look at the Adjudicative Summary portion and the SII link for more current eligibility/investigation information. The latest eligibility determination takes precedence over earlier ones. Listed adjudications are valid for all DoD users, regardless of which agency made the adjudication (e.g. there is no need to request re-adjudication for an Army member solely because the listed adjudication was done by Navy). The information in this field only indicates the highest appropriate adjudication decision made. This field DOES NOT equate to the individuals current access level. The level of information that an individual currently has access to 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 revised investigative standards as outlined in HQDA Memorandum, 19 Feb 99, subject: Personnel Security. For those individuals requiring access up to Secret classified information and their current investigation type does not meet the revised standards, a NACLC (S-PR) will be submitted. Note - if the investigation type is an ENTNAC you will have to submit fingerprints cards as part of the investigation packet to OPM. In order to grant an individual access to classified information they must have: Current eligibility and a

signed a Non-Disclosure Agreement (NDA). These are the guidelines for granting/recording access based on JPAS information.

(1) SCI Access may be granted when the Person Summary Screen shows:

a. DCID 6/4 eligibility within the past 5 years; a SSBI within the past 5 years; and no break in service of more than 24 months; or

b. The Person Summary Screen shows DCID 6/4 eligibility, a completed SSBI beyond five years and a submitted SSBI-PR. SSOs must review the PSQ to ensure that no-significant derogatory information exists in order to indoctrinate without CCF review. There must also be no break in federal service (as defined in AR 380-67, 1-306.1) of more than 24 months.

c. You may grant SCI access when SCI eligibility information is missing in the JPAS Person Summary Screen provided you have written eligibility verification (that is current) on file, and an RRU has been submitted requesting SCI eligibility.

d. Scattered Castles is another valid means of verifying SCI accesses when a person is not found in JPAS.

e. Transfer in Status (TIS) is not currently an automated function available in JPAS. You may utilize the JPAS information (current accesses) provided you have taken an owning or servicing role of the individual. A paper request of a TIS is not required. (Army G2 will be asking for this functionality and would expect this change to take place sometime later this year or early next year.)

Note: The "Adjudication History" link will only appear after SCI SMOs in-process personnel into their PSM Net.

(2) Top Secret access may be granted when the Person Summary Screen shows Top Secret eligibility and the subject meets the same investigative/ derogatory/break in federal service requirements outlined in para 1.e(1)a or b above.

(3) Secret access may be granted when the Person Summary Screen shows:

a. Secret eligibility determination within the past 10 years; a PSI within the past 10 years; and no break in federal service of more than 24 months. If subject is a Federal Civilian employee in a Non-Critical/Sensitive position, ensure that the subject meets the requirements for Federal Civilian suitability as prescribed by AR 380-67, 3-202 and 3-401b(1)(b)1. This may require an ANACI. A current NACLC; submission of an ANACI, and criteria met as outlined in para 1.e(1)a or b above, meet eligibility requirements and no Interim clearance is required; or

b. Secret eligibility determination; an outdated PSI that met the scope of investigation for Secret eligibility at the time of the previous adjudication; no break in federal service of more than 24 months; and a newly submitted periodic reinvestigation. Again, the SM must review the PSI and local files to ensure that no-significant derogatory information exists in order to determine eligibility without CCF review. (Federal Civilian suitability determinations outlined in para a. above also apply.)

(4) In cases outlined above where the only issue is a break in federal service exceeding 24 months, submitting a new PSI will negate the disqualifying condition.

f. Verify current authorized access level: The access levels listed in JPAS under Non-SCI Access and SCI Access are entered by the subject's SMs and SSOs. This information will be used to grant access at both the individual's parent organization, as well as visited organizations within the DoD. Internal access rosters for DoD personnel that are not derived from JPAS are no longer authorized. The transmission of written "visit requests" is no longer required (IAW USD(I)'s policy memo dated 1 Apr 05 (memo found on https://daison-odcsint.us.army.mil), eliminated the requirement for VALS)and will only be used when required by a non-DoD organization or a DoD organization that does not have JPAS. It is critical that we adhere to this policy where possible. Information received by a valid VAL from a contractor will not be re-verified Army Command/Units with access to an individual's clearance/access information via JPAS will not require that clearance information be transmitted to them by any other means (e.g. faxed copy of the JPAS Person Summary Screen). In other words:

(1) Do not send or require to be sent (in any form, to include utilizing the JPAS Visit Certification function), a visit certification to another organization that has access to JPAS and where the subject is in JPAS with all the required information. For example, if you are going to visit some place that doesn't have access to your information via JPAS, then you'll need to do it hard copy. If someone is coming to visit your place and their information isn't in JPAS, or you don't yet have your JPAS set up, again you'll need to do it hard copy. I would expect that by now, most Army activities should have JPAS set up and running.

(2) Those personnel who are required to show proof of investigation and eligibility for attendance to schools may attach a copy of the JPAS Person Summary Screen to their school applications. This does not negate the Schools Security Managers of their responsibility to verify an individual's accesses in JPAS and if applicable, entering the appropriate access in JPAS.

(3) Personnel whose SCI eligibility information is missing in the JPAS Person Summary Screen will be granted SCI access provided there is current written verification of SCI eligibility on file and an RRU submitted for SCI eligibility. There are some cases where an individual has been indoctrinated and the information is not yet displayed in JPAS due to multiple

reasons (e.g., backlog, no person category, missing record, owner does not yet have JPAS etc.)

(4) Information needed to validate dates of visits and need-to-know is provided by the POC or sponsor. As to need-to-know, only the holder of the information can validate need-to-know. Remember, getting a clearance message /notification /email / fax/what ever, DOES NOT equate to "official command visitor" nor "need-to-know".

g. In-Processing: When in-processing personnel, SMs/SSOs will establish the appropriate relationship with their supported personnel as described in para 1.c. above. In addition, SMs/SSOs may take a servicing relationship of personnel that are inbound until they are released from their prior organization, at which time the relationship may be adjusted.

(1) Missing Information in JPAS: When a "No Record Found" and or "No Person Category" message comes up in JPAS, submit a Test Problem Report (TPR) for Data. The "Problem Block" in the TPR should read "Record Not Found or "No Person Category" (as applicable) in JPAS". Include the following information in the "Detailed Description Block": Subject's full name, SSN, DOB and affiliation (e.g., Active Army, Reserve, Civilian, etc. (Currently this action is taking up to two weeks or longer before results are seen in JPAS). The link to the TPR form can be found on JPAS's homepage. Note: When there are multiple names missing in JPAS, please send the information on an excel spreadsheet via email to BrannonD@ccf1.ftmeade.army.mil and cc to: Spurlock@ccf1.ftmeade.army.mil.

(2) When you see "No adjudication" in JPAS, submit an RRU as outlined in paragraph 1d.

h. Indoctrinate: When granting personnel access, SMs/SSOs will ensure that the appropriate NDA or NDS date is recorded in the system. Once the system contains the appropriate NDA and/or NDS date, a new NDA/NDS will not be executed. The access grant date will also be entered for each level of access granted (e.g. Secret, Top Secret, SI, TK, etc). When the original NDA date is not available on DA civilian/military personnel, it is acceptable to have the individual(s) read and execute a new NDA for the purpose of recording the NDA date in JPAS.

i. Interim Security Clearance Determinations: Currently, JPAS users may only input interim clearances/accesses if the subject meets criteria as outlined in AR 380-67. A modification has been added to JPAS allowing the Grant Interim link to display the "PSQ Sent" date has been entered by the SM vs. having to wait until the investigation actually shows as open. Interim access may be granted after following all of the current requirements as outlined in AR 380-67, to include submission of the PSI to Office of Personnel Management (OPM). Placing the PSI in the U.S. Mail or other courier service is sufficient to meet the requirement of "submitted". However, Security Managers **must remember to enter the clearance/access** information in JPAS after using the Grant Interim link.

j. Input Personnel Security Investigation Sent Date: For all personnel who have had PSIs submitted, but whose investigation is not yet completed, the PSQ date must be filled in. This is a required field. In turn this will allow you to not only issue interim clearances, but it will also allow Army to track the length of time it takes to open cases from the time of submission. It will also assist JPAS in notifying the submitter if a submitted case does not open after a certain amount of time (this notification will be available in JPAS at a later date).

k. Determine Status of Requested Personnel Security Investigations: Security Managers/SSO's will periodically check the "Person Summary" screen of JPAS to ensure that pending investigations have progressed appropriately (e.g. opened/scheduled, closed). This is especially critical within the first 30 days after submission of an investigation to ensure receipt and action by OPM. Issues related to the status of open or not yet opened investigations will be directed to OPM by calling OPM at 724-794-5228. Issues related to closed investigations pending adjudication, will be addressed to Army CCF using the RRU function, after an appropriate amount of time (currently 6 months) following case closure.

l. Unofficial Foreign Travel: JCAV Users with levels 2 and 3, having an owning or a servicing relationship with a person in the applicable person category must enter and update a person's unofficial foreign travel.

m. Suitability Determinations: SMs in levels 4 through 6 are responsible for recording suitability determinations (in JPAS) made by the DAA, COR, Child Care Coordinator and Civilian Personnel , etc., for Public Trust, IT or Child Care positions. Please refer to the JCAVS tutorial for "IT" for how-to guidance.

n. Polygraph: Polygraph information can be entered into JPAS by any CAF (through JAMS) or by a SMO that has been granted Polygraph privileges by a JCAVS Account Manager. Refer to the JCAVS Tutorial for additional guidance.

2. It is important to remember that OPM is the organization that conducts investigations for DOD. The Army CCF is the organization that reviews the completed investigations and makes adjudication determinations. Please direct your questions to the appropriate organizations after you check the status in JPAS. We now have an Army liaison at OPM effective September 05. This position is a work in progress subordinate to CCF. The Army Liaison will conduct open case reads, determine location of a subject of an investigation, coordinate re-opens, upscope and downscope cases as needed, make determination if additional leads are needed, and coordinate with OPM case analysts.In the future CCF may provide the MACOMs with the Army Liaision's contact information but not at this time again due to this being a developing position.

3. Please use your chain of command for JPAS related questions.