DEPARTMENT OF DEFENSE • DEFENSE SECURITY SERVICE, INDUSTRIAL SECURITY PROGRAM OFFICE

INDUSTRIAL SECURITY LETTER

Industrial Security letters will be issued periodically to inform Industry, User Agencies and DoD Activities of developments relating to industrial security. The contents of these letters are for information and clarification of existing policy and requirements. Local reproduction of these letters in their original form for the internal use of addressees is authorized. Suggestions and articles for inclusion in the Letter will be appreciated. Articles and ideas contributed will become the property of DSS. Contractor requests for copies of the Letter and inquiries concerning specific information should be addressed to their cognizant security office, for referral to the Industrial Security Program Office, Headquarters, DSS, as appropriate.

This Industrial Security Letter is devoted to issues involving personnel security clearances and the Joint Personnel Adjudication System (JPAS). Please read this entire ISL and if your facility does not already have an account on JPAS, please take immediate action to establish an account. As of October 1, 2004, JPAS will become the system of record for contractors under the security cognizance of this Department.

ISL 04L-2 **July 15, 2004**

Joint Personnel Adjudication System (JPAS)

Personnel Security Investigations Processing

Joint Personnel Adjudication System (JPAS)

JPAS is the official Department of Defense (DoD) automated system for personnel security clearance management. While JPAS has various applications for the Department of Defense, the application that contractors will use is the Joint Clearance and Access Verification System (JCAVS). Personnel security managers will use JCAVS to verify, annotate and/or update the level of access that has been granted to cleared personnel, as well as check on the status of investigations in process. It will also be used to record other security administration functions. Actions that can be taken by cleared facilities in JPAS/JCAVS include conversions, reinstatements, concurrent accesses, and terminations of personnel security clearances (PCLs), as well as other change notifications thereby eliminating the need to submit DISCO Forms 562.

1. How to Establish a JPAS Account

To obtain JPAS access, you should visit the JPAS website at https://jpas.osd.mil for account registration procedures. (Refer to ISL 04L-1 for additional guidance.) Your facility will need to designate an account manager as part of this process. The basic steps are as follows:

a. Submit the appropriate JPAS account registration forms to the JPAS Help Desk. The registration forms are available through the website at https://jpas.osd.mil/betaTestInfo/registrationForms.asp.

b. Provide the following data:

(1) Completed JPAS registration form for each company.

(2) Appointment letter designating a Primary Account Manager, along with a completed Access Request Form (ARF). The appointment letter must be on company letterhead and be signed by a corporate officer. The letter must include the account manager's full name, social security number, and contact information (i.e., telephone number, office address, and work email address). The letter must also include contact information for the corporate officer making the request. NOTE: An account manager may serve this role not only for all facilities within a multiple facility organization, but also for first and lower tier subsidiaries. The same corporate official must sign the appointment letter and the SAR. If the company designates an alternate account manager the same form/letter must be completed for that individual.

(3) If more than one cleared facility is going to be serviced by the same account, please provide a list denoting all company site locations/addresses for JPAS access that includes the static Internet Protocol (IP) address for each site.

c. Fax your registration forms to (202) 404-2930. On receipt of the registration forms, the JPAS Help Desk will verify the company's Facility Security Clearance (FCL). Once the FCL is verified, the site(s) will be added to the JPAS Access Control List.

d. The company will be notified via email that the JPAS account has been established. There will be two emails sent: one to identify the account password and one for the account user id.

2. JPAS Help Desk

The JPAS Help Desk hours are Monday through Friday, 0600–1800 EST. The telephone number is (202) 404-6692 or (202) 404-2923. Please review the information contained on the JPAS website, to include the training and the frequently asked questions before contacting the Help Desk.

3. JPAS Access and .edu Internet Addresses

Due to security concerns, cleared facilities with .edu Internet addresses cannot access JPAS. Organizations with .edu Internet addresses need to acquire a .com, .org, or .net account to gain access to JPAS.

4. Type of Investigation Required for Access to JPAS

Persons who access JPAS in read only or read and write capacity must have either a Secret clearance or an “eligibility” determination based on a favorably adjudicated NACLC. Secret clearances issued prior to January 1999 do not have a NACLC as their investigative basis. Those individuals will be granted access to JPAS if a NACLC is in process. When requesting a NACLC for these situations, Item 6, "Reason for Request" in the "National Agency Check Security Information" section of EPSQ 2.2, should be annotated with the following statement: "NACLC required for JPAS access."

Persons who will be entering information into JPAS concerning SCI briefings/debriefings must have eligibility for access based on a single-scope background investigation (SSBI). SCI eligibility and indoctrination must also be indicated.

5. JPAS User Levels

There are various user levels for JPAS access. User levels relate to specific roles, responsibilities and type of background investigation of the user, and each carries certain privileges (such as read, write, edit, etc.) Facility Security Officers with non-SCI access are normally at Level 5 with appropriate privileges to update records. Level 7 would involve read only access and would be appropriate for persons with visitor control responsibilities. The JPAS Help Desk will provide assistance regarding specific levels based on the user role and responsibilities.

6. JPAS Training

The JPAS Program Office and a representative of our Industry JPAS Advisory Group provide on-site courses introducing the DoD community to JPAS. Those sessions will continue and a schedule for those classes and information on enrollment are available on the DSS Academy (DSSA) section of the DSS website at https://www.dss.mil. The National Classification Management Society (NCMS) is developing training through their individual chapters. DSSA is integrating use of JPAS in all courses that they provide as appropriate. As your facility will now be responsible for maintaining your employees’ records in JPAS, it is critical that the employee designated as your account manager receives appropriate training and understands the importance of updating records as expeditiously as possible. Other contractor or government activities will grant access to classified information to your employees based on their access record within JPAS, so it is critical these records be properly maintained.

Training for JPAS uses the "Train the Trainer" concept. Companies are responsible for establishing centralized account management procedures and ensuring that personnel within their corporate family are trained prior to granting them access to the system. The Industry JPAS Advisory Group has also developed training materials and job aids that can be found on the JPAS website.

Those materials include:

a. Checklist for Industry Implementation of JPAS – This is a 2-page checklist that leads you through the steps to successfully implement and utilize JPAS within your facility.

b. The How To Book for JPAS – This is a basic tutorial that starts with how you login to the system (once you have obtained an account) and covers all of the functions of JPAS.

c. JPAS Account Manager Introduction – Another basic tutorial on how to manage your JPAS account.

d. JPAS User (Security Management) Introduction – Additional information on the various functions of JPAS

e. JPAS Proposed Implementation Guide – A guide that you can adapt for your company's internal JPAS implementation

f. JCAVs User Training and Certification Program –This document is an adaptable guide for use in certifying your personnel for access to JPAS. (Please note that certification is not required at this time.)

7. Personnel Security Management Network (PSM-Net)

JPAS allows for centralization of clearance management within a corporate family. Your PSM-Net consists of a security management office (SMO), or an association of security management offices under a hierarchical organizational structure and the personnel for whom they have security responsibility. If your facility is part of a multiple facility organization (MFO), your PSM-Net could consist of all of the facilities within that MFO. It could also include subsidiaries if personnel security actions for employees of those subsidiaries are going to be processed through the MFO.

Once your facility has obtained an account in JPAS, you will need to initially set up and take ownership of your PSM-Net. This allows you to take personnel security actions for those individuals as well as receive notifications of personnel actions. Please note that some of your personnel may have records reflecting personnel security eligibility with other contractors, government agencies or the military. Those affiliations may continue to exist if your employee is a reservist or a consultant to another contractor or government agency, and it will that entity's responsibility to update the employee's records within their area of responsibility. Before you conduct any transaction regarding these persons, it is critical that you have established ownership for these persons with an "Industry Tab" and your CAGE Code. An employee should only have one active Industry Tab within any corporate family. You are the "owner" of your employee's JPAS records. There are other entities that may "service" your personnel, such as DISCO or the entity that grants SCI eligibility – but those entities do not own your employee.

8. Contractor Responsibility for Reconciliation of Personnel Clearance Records in JPAS

After your JPAS account is established, your first responsibility is a 100 percent validation of clearance records in your PSM-net. Information in JPAS was compiled from various government databases and, as such, may contain discrepancies. Since you are responsible for your company's information in JPAS, it is imperative that you initiate corrective action within the system if you find information in your records that is incorrect. The following JPAS Data Validation Checklist is a guide that you can follow for checking your records.

a. Identifying Data: The JPAS screens contain basic identifying data - name, date and place of birth, social security number. If any of this information is incorrect please update the screen. You do not need to notify DISCO of changes that you make to these records. Use the Request Research/Recertify/Upgrade Eligibility (RRU) function to notify DISCO of changes that JPAS will not permit you to make, but are required to appropriately update the record

b. Eligibility: You will note eligibility information that includes the level of eligibility adjudicated by the government central adjudication facility (CAF). You cannot change this information but if you believe it is incorrect, please notify DISCO via the RRU function. Remember that your employee may have eligibility at a higher level than that on record at your facility due to previous employment or military service, but **they may not be granted access to classified information at a higher level than your facility security clearance.**

c. Non-Disclosure Agreement (NdA) signed: If this field is blank, enter the date the employee signed an SF 312. If this field is completed, the employee has signed an SF 312 at some previous time and it is not necessary for the employee to execute another SF 312 at your facility.

d. Attestation date: If your employee is contractually required to orally attest to his/her security responsibilities, enter the date it was performed here.

e. Industry (Contractor) Code: As stated above, make sure the record you are reviewing is for your CAGE code. You will note that industry CAGE codes appear in JPAS followed by an "-I". This was established to provide a distinction between CAGE codes and military unit codes within the system.

f. Non-SCI Access: Complete the access fields as appropriate. In most case you will enter Secret or Top Secret after "US"

9. Interim Eligibility Determinations

If an Interim clearance is denied, DISCO cannot post that information in JPAS. In this circumstance, the individual's eligibility will not be updated and contractors will no longer receive notification that an Interim has been denied. You will be able to tell the interim has been denied if a review of the employee's JPAS record shows an open investigation but no interim eligibility.

10. Security "Lock-out" from JPAS

JPAS users are "logged-out" of JPAS after 15 minutes of non-activity. To re-access JPAS, the user must enter their password and user ID. If a user exits JPAS without logging-out, the user will be "locked-out" of JPAS and action by the account manager or JPAS Help Desk must be taken for the user to re-access the system. Users are also locked out of JPAS if they do not access the system within a 60-day period.

11. Authorized Use of JPAS

JPAS contains official government records and privacy information regarding both government and industry employees. This information must be used only for official purposes, and must be protected from unauthorized disclosure. Querying JPAS for purposes outside of an official government security context is not authorized. However, verification of prospective employees' eligibility information is permitted prior to an offer of employment being extended. Cleared contractor organizations must ensure that authorized users have been properly trained. Although cleared contractors cannot grant access in JPAS to an employee unless the investigative basis is there, it is the contractor's responsibility to ensure JPAS records are accurately and expeditiously maintained. It is imperative that termination actions be taken promptly as other DoD users will be granting access to contractor employees based on this data.

12. Use of JPAS by Industrial Security Representatives (IS Reps)

DSS IS Reps will utilize JPAS during recurring Security Reviews. IS Reps will no longer review paper records during Security Reviews for electronic information available in JPAS (e.g., Letters of Consent, Visit Letters, employee terminations, etc.). DISCO will no longer issue Letters of Consent nor will contractors use the DISCO Form 562 to advise DISCO of any actions that can be performed in JPAS. Instead, they will use JPAS to review contractor account administration procedures as well as to verify clearance eligibility determinations, appropriate access levels, briefings, and terminations. Personnel clearance status change notifications (formerly accomplished through use of the DISCO Form 562) for contractor employees are now processed electronically by the contractor directly or through the "Request to Research/Upgrade Eligibility" (RRU) function. While cleared facilities are expected to implement NISPOM requirements, contractors should not duplicate, create or retain paper records for electronic information available in JPAS, but should make the information in JPAS available to their IS Rep during Security Reviews.

Personnel Security Investigations Processing

We regret that the transition to processing all personnel security investigations (PSIs) through the Office of Personnel Management (OPM) has not gone as smoothly as hoped. OPM does not exercise the flexibility that DSS may have employed regarding the extent of information provided by the applicant and the receipt of all documentation. In addition, in order to prepare investigative requests for transmission to OPM, which currently processes cases in paper, DSS now handles large volumes of paper, which has required the adoption of new processes and changes to existing processes.

To facilitate processing of investigative requests, contractors must ensure that all personnel security clearance requests contain all required documentation, to include the fingerprint card and release form. **Effective August 15, 2004, if all documentation is not received within 30 days of submission of the request for investigation, the investigation will be discontinued and any interim personnel security clearance will be administratively withdrawn.** To assist you in determining whether all required documentation for investigative requests have been properly received by DSS, contractors are encouraged to check the EPSQ receipts website (https://sclient.dss.mil/epsq/epsq.html) at least weekly. This website lists all investigative requests received from your facility, and identifies any documentation (e.g., fingerprint cards or releases) not yet received.

13. Incomplete Personnel Security Investigative Submissions Received Before April 23, 2004

Recently, many contractors received a letter from DSS requesting fingerprint cards and/or general release forms, as well as updated employee certifications and/or additional years of coverage for residence and employment for investigative requests received before April 23, 2004. Some of this documentation has not yet been received, and while we regret the inconvenience caused by this request, this documentation is needed or OPM will not accept the cases for processing. Contractors were instructed in the letter to send the complete investigation request package (e.g., Updated/Recertified "hard copy" of EPSQ, Release and Fingerprint Card) to the following address: **(Please note that this mailing address was established for the cases identified in the letter only. Do not send any other correspondence to this address or include anything else in the envelopes.)**

EPSQ Team
Defense Security Service
601 10th Street, **Suite 300**
Ft. Meade, MD 20755-5134

As a reminder, if the required documentation is not received by August 15, 2004, the investigative request will be discontinued since it cannot be processed by OPM and any industrial interim clearance issued will be withdrawn.

14. Most Common Reasons for Investigative Request Rejection

Clearance applications other than those noted above that need correction before the investigation is opened will be returned to contractors by DISCO. DISCO will include a cover sheet or letter that itemizes the specific items that need to be addressed.

The following items have been identified by DISCO as those that most often require corrective action:

a. Submitting only the signed and dated certification page or portions of the updated EPSQ when instructions called for submission of the complete package.

b. EPSQ reflects a change (such as a new residence) but does not reflect an effective date for the change.

c. EPSQs and fingerprint cards are received, but packages are missing general releases.

d. Releases are received without an EPSQ.

e. Fingerprint cards are received but no EPSQ has been submitted.

f. Releases are received with notes from the FSO indicating that the EPSQ was re-transmitted when instruction specifically directed hard copy re-submission.

g. Release forms are not dated, are missing the SSN, are illegible or appear to have been modified without the modifications being initialed by the subject.

h. Date of Birth (DOB) or Place of Birth (POB) discrepancies exist between the Fingerprint card and the SF86/EPSQ. They must match exactly.

i. Full middle name is not included on the Fingerprint card. The Fingerprint card must exactly match the SF86/EPSQ. If no middle name, indicate "NMN." If initial only, indicate "IO"

j. City, State, and Zip are not included for all residence and employment addresses

k. The Social Security Number and POB are not provided for cohabitants on SSBI requests

l. Employment and Residence gaps exist.

-Seven Years of Coverage is required for residence, employment for Confidential and Secret requests, for both initial clearances and periodic reinvestigations
-Ten Years of Coverage is required on all requests for initial Top Secret clearance.
-For Top Secret periodic reinvestigations, the requirement is five years of coverage or back to the date of the previous investigation, whichever is longer (but no more than 10 years, if the last investigation is older than 10 years).

m. Separation date and address of spouse are not provided for legal separations.

n. Marital status of previous spouses is not provided. If unknown, so indicate.

o. Debt information is not clarified. Indicate if debts are still outstanding. Add comments in the remarks section if needed.

p. The subject's certification of the accuracy of the EPSQ data is more than 180 days old. Depending on the date the applicant certified the content of the EPSQ, it may be necessary to have the applicant re-date the certification and initial the change on the form. OPM will not accept requests for investigation if the date of the applicant's certification is more than 180 days old.

q. Incorrectly requesting an Industrial NAC when a NACLC is required. An Industrial NAC is only used for trustworthiness determinations.

15. DSS Web Address for Current Information/Updates in Clearance Processing Procedures

DSS has established a specific web site for updates and alerts regarding personnel security processing procedures. Contractors should review this site at least weekly to ensure they are aware of the most recent procedures for submitting personnel clearance investigative requests. This guidance may be reviewed at http://www.dss.mil/whatsnew/opmrejects0528041.htm .

16. Checking Status of Investigations

You can use JPAS to check on the status of a pending investigation. If you do not yet have access to JPAS, you can check on the status of an employee’s investigation by calling the DoD Security Services

Center at 888-282-7682. (This center covers what was previously the DISCO Help Desk.) **Do not call OPM for status checks.**

17. Personnel Clearance Investigations and Employees Stationed Overseas

If you have employees in process for an investigation who are located outside the United States and you anticipate the employee returning to the United States in the near future, please contact DISCO Customer Service at 1-888-282-7682. This will ensure that we do not terminate the investigation or withdraw an interim clearance for those employees while we attempt to conduct the overseas leads necessary to complete the investigation.

18. Submission of Periodic Reinvestigations

As you are reviewing your employees' records in JPAS, please determine whether they require a Periodic Reinvestigation (PR), and submit necessary PR requests as soon as possible. A review of records in the JPAS indicates there are a significant number of cleared industry personnel who are overdue for their PR. PRs are required every five years for individuals cleared at the TOP SECRET level, every 10 years for those cleared SECRET and 15 years for CONFIDENTIAL clearances.

Prior to submitting an individual for a PR, please ensure that the individual still requires a security clearance and at the same level. If you determine that an individual currently requires access only at a lower level of classification or no longer requires a clearance, please terminate their access or downgrade it as necessary in JPAS.

If the employee is in process for a PR through another government agency please advise DISCO via the RRU function that a PR is in process and identify the processing agency if you can provide that information.