JPAS Updates

NCMS PACIFIC NW CHAPTER
28 MARCH 2013

TONI MACDONALD
THE BOEING COMPANY
Agenda

• Industry Team

• JPAS Rules/Procedures

• New Account Checklist

• JPAS Documentation

• JPAS Login Page

• DEERS Update

• DQI

• PRs

• Reports

• Help Desks

• eQIP by Design

• JVS

• Webinars
The JPAS Industry Team (est. 2004)

- Toni MacDonald (Boeing)
- Tanya Elliott (CACI)
- Quinton Wilkes (L-3 Communications)
- Steven Burke (Lockheed Martin)
- Rene Haley (Northrop Grumman)
- Susie Bryant (Raytheon)
- Carla Peters-Carr
- Shala Romandelvalle (BAE Systems)
- Sheila Garland (Ball Corporation)
Procedures Governing Use of JPAS by Cleared Contractors Defense Security Service

• National Industrial Security Program Operating Manual (NISPOM) paragraph 2-200b states that “When the CSA [Cognizant Security Agency] has designated a database as the system of record for contractor eligibility and access, the contractor shall be responsible for annotating and maintaining the accuracy of their employees’ access records. Specific procedures will be provided by the CSA.” The Department of Defense, acting as a CSA, has designated the Joint Personnel Adjudication System (JPAS) as the DoD system of record for contractor eligibility and access.

• JPAS is a U.S. Government information system that contains official government records. The information in JPAS must be protected from unauthorized disclosure and used only for authorized purposes. Contractors may only use their JPAS accounts to manage the access records of their employees and consultants, and to verify the access levels and affiliations (e.g., employee of ABC Company) of incoming visitors who require access to classified information.

• The following procedures are issued under the authority provided by NISPOM paragraph 2-200b. Contractors shall follow these procedures when using JPAS and shall ensure that authorized users of JPAS have been properly informed about these procedures and any other specific policies governing access to and use of JPAS.

1. Contractors shall accurately maintain the JPAS records pertaining to their employees and consultants. Contractors must expeditiously update these records when changes occur (e.g., termination of employment).

2. Contractors are prohibited from placing false information in JPAS, and DMDC will seek appropriate sanctions against contractors and contractor employees who knowingly place false information in JPAS.
3. DoD issues JPAS accounts exclusively for use by a specific contractor or corporate family of contractors. Persons given access to JPAS as account holders may only use JPAS on behalf of the cleared contractor or corporate family of contractors through which the account was issued. For example, an employee of ABC Company holding a JPAS account issued through ABC Company and who works at a government site is not authorized to use the contractor-granted account in support of the government customer. If the government customer requires the contractor employee to review or update JPAS records on behalf of the government customer, the government customer must provide a separate, newly created JPAS account for the contractor employee to use – they may not share an existing user ID and password.

4. The JPAS account manager must be a company employee. The JPAS account manager cannot be a subcontractor or consultant.

5. Contractors may subcontract or obtain consultant support for administering security services, not account management as stipulated in #4 above. The using contractor will provide a JPAS account to the subcontractor or consultant under the using contractor’s Security Management Office (SMO) for the sole purpose of permitting the subcontractor or consultant to provide security services for the using company. Subcontractors or consultants providing such security services must be under the direct supervision of the using contractor’s FSO or FSO’s designee.

6. Each individual accessing JPAS must have a separate and unique account created by the individual’s JPAS account manager. The account manager must maintain a current record of every JPAS account established as per JPAS Account Management Policy, Section 4.2: System Access Request Form.

7. JPAS users may never share their user IDs, passwords, PK certificates, PINs, or other authentication information with any other individual, including anyone who is a designee or an alternate to the account holder.
8. Access to JPAS is only authorized by means of company or government-owned equipment with appropriate security controls in place. JPAS users may not access their accounts from personal or home computers or over unsecured wireless networks.

9. Contractors are not permitted to change an existing date notation in JPAS for the Classified Information Nondisclosure Agreement (SF 312). Contractors must, however, input the date that the SF 312 was signed when JPAS does not reflect a date.

10. Contractors are authorized to verify prospective employees’ eligibility for access to classified information in JPAS prior to an offer of employment being extended. However, contractors may not use JPAS for recruiting purposes.

11. While access to JPAS is only granted to contractors who have a legitimate need for such access in support of classified work being performed for the Government, JPAS is not a classified system. DSS will not grant a facility security clearance (FCL) for the sole purpose of allowing a company or its employees to gain access to JPAS.

12. Any contractor with JPAS access that becomes aware of a violation of these procedures shall immediately report the nature of the violation, the names of the responsible parties, and a description of remedial action taken, to the servicing DSS Industrial Security Representative.

NOTE: Violations of the procedures may lead DMDC to suspend or withdraw JPAS access, terminate the JPAS account, mark a technology incident on a user’s JPAS record, or exclude culpable companies or persons from access to JPAS for a specified or indefinite period. DSS will also refer information concerning violations of these procedures to other federal agencies for consideration of administrative, civil or criminal sanctions when circumstances warrant.
JPAS New Account Checklist

• Clearance Requirements
  – The minimum requirement for JPAS access is Secret eligibility. Levels 2, 3 and 8 require an SSBI at minimum.

• Training Requirements
  – JPAS/JCAVS Virtual Training for Security Professionals
    • http://www.dss.mil/cdse/catalog/elearning/PS123.html
  – Personally Identifiable Information
  – Cyber Awareness Challenge/Security Training
    • http://iase.disa.mil/eta/cyberchallenge/launchPage.htm

• System Access Request (SAR) Form
  – Initial accounts for Primary Account Managers - send to the DoD Security Services Center
  – Subsequent accounts - send to appropriate JPAS Account Manager

• Letter Of Appointment (LOA)
  – Personnel Security System Access Request (PSSAR)

• Personnel Security System Access Request (PSSAR)
Letter of Appointment (LOA) – Samples

Example 1:

Date:

Subject: Letter of Appointment for JPASS Account Request

Requester:

- Requester’s full name:
- Office Address:
- Office Phone:
- Email:

Who the Account is for:

- Applicant’s full name:
- SSN or DODSS:
- Office Address:
- Office Phone:
- Email:

List specific job duties that require JPASS access:

Authorized by:

Title:

Org:

Signature:

Example 2:

Raytheon

2010 E. El Segundo Blvd.
El Segundo, CA 90245

DoD Security Services Center
3450 Fornoise Rd., Suite 101
Lorton, VA 22079

Subject: Letter of Appointment for JPASS User Account

Please process JPASS User Account for the following Raytheon Security Professional requiring access to JPASS.

Name:

Employee ID:

Job title:

Job duties that would necessitate access to JPASS:

Attached is the corresponding DSS Form 273 (System Access Request).

Regards,

Signature

Name of Nominating Official:
Title (RMP or PSQ):
Organization/BU:

By:
JPAS Documentation

- JPAS Account Management Policy *(1/30/13)*
  - Procedures Governing Use of JPAS by cleared Contractors
    - Appendix A: of JPAS Account Management Policy
- JPAS Account Request Procedures *(3/20/13)*
- JVS Modifications
- JPAS Points of Contact
- JPAS Policy Guidance *(2/12/13)*

- All documentation can be found on DMDC/JPAS Login screen
• Access Request Info
• Data Quality
• FAQs
• Alerts/Notices
• General Information
• Points of Contact
• Updates/Archives
• JVS Modifications
• Policy Updates
Industry Team

Defense Enrollment Eligibility Reporting System (DEERS)

- Last Name or Date of Birth (DOB) Issues for Industry
- Input the SSN and only the information that needs to be updated
- Spreadsheet is posted to: www.dss.mil
- Send this information to DISCO at DISCO.PMO@dss.mil. DISCO will in-turn transmit the information to DMDC which will work directly with DEERS to correct the information.

No More Spreadsheets, New Procedure in Place
New Procedure: PII Issues for Industry: (AKA DEERS Issue)

Industry FSOs need to monitor their employees’ records to ensure that names and/or DOBs are not updated with outdated information from the PDR. The following provides guidance if a name and/or DOB updates with incorrect information.

1. If the subject’s Personal Identifying Information (PII) is incorrect, check to see if the record contains a DoD Electronic Data Interchange Person Number (EDIPN). If not, then FSOs can update the record in JPAS.

2. If the record DOES contain an EDIPN and the Person Category is not Civilian or Military, the FSO or the subject will need to submit official documentation (e.g., passport, birth certificate, SSN card, or marriage certificate) to DMDC to support the change. Call the DEERS Support Office (DSO) at 1-800-538-9552 and tell them you need to correct the record for JPAS. DSO will ask you to fax the documentation to 1-831-655-8317. In the majority of cases, the Customer Service Representative (CSR) will be able to update the record immediately. It is important to tell DSO the correction is for JPAS and to make sure you fax the required document(s).

3. The PDR update occurs monthly on the day of the employee’s birth (e.g., if their birth date is 4/20, the record is updated on the 20th of every month). However, if the subject has an immediate need, the FSO can update the record in JPAS.

4. If the subject’s Person Category is Military, Civilian or Retiree, they will need to personally contact their Personnel Center, milConnect and/or DFAS to update the record.
Archived Records

- Reactivation requests can be auto approved if the following PII criterion matches the person’s JPAS database record:
  - Social Security Number (SSN)
  - Last Name (LN)
  - First Name (FN)
  - Date of Birth (DOB)

- If all PII criterion does not match, the request will go through the pre-existing manual approval process.

- If auto-activated, you will receive message indicating subject has been reactivated, otherwise you will receive message indicating “Request has been sent to Helpdesk”
Data Quality Initiative (DQI) 597 — Unsupported Access Debriefing

• DQI is a data clean up effort to improve overall quality of JPAS database
• DQI will effect records that have an active Access that is not supported by current eligibility
• Debriefing will occur if the Access listed on a record has:
  • a separation date
  • a separation status code
  • death date
  • no owning or servicing SMO
• Record will be assigned a current debrief date and will show ‘Admin Debriefed’ by the ‘JPAS Support Office’
Periodic Reinvestigations (3/15/13)

- **Guidance on submitting periodic reinvestigation**
  Effective April 1, 2013, the Defense Security Service (DSS), Personnel Security Management Office for Industry (PSMO-I) will only accept requests for Periodic Reinvestigations (PR) that are within 30 days of the investigation anniversary date. This is a change from the previous three-month (90 day) timeframe, and is consistent with changes in the DoD budget. Based on FY13 Personnel Security Investigation-Industry (PSI-I) requirement projections, sequestration is expected to pose a significant challenge to PSI funding. Moreover, under current policy governing funding for personnel clearances, DSS may be required to stop processing Top Secret Periodic Reinvestigations. If and when the decision is made, DSS will inform the community. Periodic Reinvestigation requests already initiated prior to April 1 will continue to be processed as appropriate.

Reports – Personally Identifiable Information (PII)

- All reports downloaded from JPAS contain PII
- It is our responsibility to protect all PII that is available in JPAS
- Don’t forget to pick up PII data from printers and/or fax machines
- Remember to encrypt e-mail messages containing PII
- Misuse of any JPAS PII can result in disciplinary action
Report Types

- **Act PC-Access/No PSM Net** - Lists organizations that have a Person Category for a subject without a PSM Net relationship owned or serviced.
- **Inv Rqst by Duty Pos** - This report indicates all Investigation Requests currently in your PSM Net by Duty Position.
- **Non-SCI Totals** - List of all Non-SCI Access’s, for owned and or serviced Person Categories in your PSM Net or subordinate organization.
- **Periodic Reinvest** - List of Personnel within your PSM Net or subordinate organization whose investigation may be out-of-scope and may require a Periodic Reinvestigation.
- **Personnel** - Detailed list of Personnel in your PSM Net and or subordinate organization, including access, eligibility and investigation information.
- **PSM Net Personnel** - Abbreviated list of all personnel in your PSM Net or subordinate organization.
- **SMO-No PSM Net** - Retrieve information regarding SMOs in your hierarchy that have not established a PSM Net.
- **SMO-No Users** - Retrieve information regarding SMOs in your hierarchy that have established their SMO but have no Personnel with an Owning or Servicing relationship in their PSM Net.
- **SMO-PC-No Access** - Retrieve information regarding SMOs in your hierarchy that have established their PSM Net but don’t have an access indoctrinated for a Person Category.
- **Suspense** - Retrieves information regarding Suspense information the JCAVS user created from a subject’s Person Summery screen / Suspense Data link.
- **Suspensions** - Information regarding Suspensions (eligibility and/or Access) for personnel in your PSM Net and or subordinate organization.
New DMDC Contact Center – 1 June 2013

• **JPAS, SWFT, e-QIP and DCII Users** should refer to the DMDC web pages at [https://www.dmdc.osd.mil/psawebdocs](https://www.dmdc.osd.mil/psawebdocs) for alerts, notices, user guide resources, etc., pertaining to these systems/applications. Users should bookmark the above-referenced DMDC web site URL to ensure continued receipt of the latest information concerning these systems/applications.

• **New DMDC Contact Information**
  - Phone number: 1-800-467-5526,
  - E-mail address: dmdc.contactcenter@mail.mil
  - Fax: 1-502-613-1096
Personnel Security Management Oversight Office (PSMO) Portal

- **DSS working with Industry to stand up a new Personnel Security Office**
- **Portal will be Industry specific – focus on process requests**
  - KMPs
  - PR Oversight
  - Aging Interims
  - Security Clearance Personnel Process
  - RRU
- **Looking to stand up NLT Oct 2013**
- **Will be located in Ft. Meade, exact location TBD**
**CATS Portal**

- **Case Adjudication Tracking System CATS**
  - Faster and easier communication between Security Managers, FSOs and DSS/CATS
  - Will be able to scan, upload and forward documents to the new DSS PSMO
    - SF 312’s
    - Incident Reports
  - Testing was to begin in January; deployment scheduled for September 2013
  - Training and rollout to be completed NLT 2nd QTR FY14
eQIP by Design

- Most of the Service Agencies have transitioned to eQIP by Design and have provided industry companies direct access to submit the SF 85s on their behalf.
- Industry currently initiates and submits to DISCO via JPAS
- DSS Planning Office is currently working with contractors on of e-QIP by Design Pilot Program to test the function through the OPM portal.
  - Better support and more efficient process
  - Quick response on current status
  - eQIP process will be eliminated from JPAS
JVS System Modifications

- DMDC has created a JPAS Users’ Checklist for upcoming changes to JVS.
  - In order for the person records to be properly migrated over to JVS, the JPAS team is asking that you review the company/service persons’ names and update the records.
  - The easiest way to find out if the Name (Last, First, Middle) does not meet the standards is to pull a JPAS report, import the data into Excel, and then perform a search on the Name fields for the invalid characters.
Name Corrections

The following characters are NOT allowed for last names:

1. [blank]
2. (NLN)
3. +
4. ....................................................
5. any number 0-9
6. last names with O like Oscar please ensure it's a O not a 0 (zero)
7. SSNs are not considered last names
8. periods should not be in the last name (SMITH JR. or ST. GEORGE). Last name should be SMITH, suffix should appear as JR (without period) or last name ST GEORGE
9. suffix should be in the suffix field and not the last name field (SMITH (JR.). Last name should be SMITH, Suffix should be JR
10. () (parenthesis)
11. _ (underscore)
12. " " (double quotes)
13. ** (asterisks)
14. ' (single quote/apostrophe) Note: Current policy does not allow apostrophes in JPAS. This guidance may change in the future to facilitate the transition to JVS

Characters that are allowed:

1. Alpha characters – A – Z, a – z
2. Hyphens are allowed
Phone Numbers

Ensure SMO Phone and Fax Numbers are accurate

[1] Area code surrounded by ( )
[2] Followed by a dash
[3] First 3 numbers
[4] Followed by a dash
[5] Last 4 numbers

Examples are: (123) – 456 – 1234
SMO Information

SMO Email Address

- All email addresses in the SMO Email Address Field need to be updated without name, phone, rank, title, or extra wording. The preference is
  - name@company.com
  - name@service.mil separated by semicolons (;) and no other wording

This will help expedite the data migration from JPAS to JVS
**DISCO Webinars:** [https://connect.dco.dod.mil/askdisco](https://connect.dco.dod.mil/askdisco)

- A series of live web events to address topics related to personnel security clearances for Industry.
- Intended for use by security specialists within the National Industrial Security Program.
- Hosted on the Defense Connect Online (DCO) and can be accessed from any computer with an Internet connection and Adobe's Flash Player.
- You do not need to register for a DCO account to attend a CDSE webinar. You may login as "Guest".
- Prior to the webinar, ensure your computer/ network connections are properly configured by going to: [https://connect.dco.dod.mil/common/help/en/support/meeting_test.htm](https://connect.dco.dod.mil/common/help/en/support/meeting_test.htm)

**Talk with the JPAS Team**

- Check the DMDC JPAS Homepage for the next scheduled opportunity to talk with the JPAS Team. All meetings will be held via Defense Connect Online (DCO) at the following link: [https://connect.dco.dod.mil/jpastalk](https://connect.dco.dod.mil/jpastalk)
Useful Websites

DMDC:  https://www.dmdc.osd.mil/psawebdocs/


DSS website:  http://www.dss.mil/

DEERS website:  http://tricare.mil/mybenefit/home/overview/Eligibility/DEERS/Updating


ISFD:  http://www.dss.mil/diss/isfd.html


NCMS:  https://www.classmgmt.com/Home/
## JPAS Industry Team Contact Information

### Industry Team PMOs
- Quinton Wilkes – Team Lead
  quinton.wilkes@L-3com.com
- Tanya Elliott
telliott@cai.com

### Industry Sub Team
- Toni MacDonald
  renita.macdonald@boeing.com
- Susie Bryant
  smbryant@raytheon.com
- Rene Haley
  rene.haley@ngc.com
- Steven Burke
  Steven.d.burke@lmco.com
- Carla Peters-Carr
carla.s.peters-carr@saic.com

### SWFT Industry Sub Team
- Sheila Garland
  sgarland@ball.com
- Shala Roman
  shala.romandelvalle@baesystems.com

---

**Customer Call Center**
888 282-7682
Questions?