Presented to: NCMS Central Virginia Chapter

March 24, 2011

Tanya Elliott, CACI
Transition from DSS to DMDC

- DMDC serves under the Office of the Secretary of Defense to collate personnel, manpower, training, financial, and other data for the Department of Defense.

- IT Systems transferred to DMDC: JPAS, DCII, SWFT, IRR

- New URL for JPAS: https://jpasapp.dmdc.osd.mil/JPAS/JPASDisclosure

- As of January 2011, JPAS allows the following log-in options:
  - Military/Civilian: User ID/Password or CAC Card
  - Industry: User ID/Password or CAC Card
    - Industry must have appropriate software for CAC

- DMDC is currently working with the Industry companies that have existing internal PKI or CAC requirements.
  - Internal companies with PKI or CAC must meet the DOD requirements
TPR Process

- The JPAS Test Problem Report (TPR) process will be modified due to JPAS’ transition from Defense Security Services (DSS) to the Defense Manpower Data Center (DMDC).
  - The TPR form on DSS web site will not be available in the future (project February 2011).
  - Faxing of TPRs will no longer be accepted.
  - All Personally Identifiable Information (PII)-related TPRs will need to be directed to the Personnel Centers (if military or civilian) or to the company's Security Officers (if industry).
    - DEERS is not a personnel center and cannot make PII-related JPAS modifications.
    - Industry-related PII issues should be directed to the DOD Call Center (888-282-7682).
  - All Technical-related TPRs will need to be directed to the JPAS Program Management Office (PMOs).
JPAS Acceptance Screen

- JPAS Updates will be posted to the JPAS Disclosure Screen, so be sure to bookmark this screen and NOT the Log In screen. Please note the DMDC URL to JPAS: https://jpasapp.dmdc.osd.mil/JPAS/jsp/JPASDisclosure.jsp
JPAS Log in Screen

- JPAS does not have “COMPANY ACCOUNTS”
  - It is against DOD Regulations to share username and passwords
    - Industry is the biggest offenders
    - DMDC will forfeit JPAS accounts regardless of mission critical requirements
- At a future date (slated to occur late CY 2011), JPAS will no longer accept usernames/passwords for access. JPAS users will be able to access the system with either a CAC or other DoD approved Public Key Infrastructure (PKI) certificates.
- Continue to use your username/password for the immediate future.
- The CAC Login is working for Industry as well as the government. If you have a CAC and have your government certificates loaded on the CAC it will work from your company computer if you have appropriate software and CAC reader.
The CAC Login is working for Industry as well as the government. If you have a CAC and have your government certificates loaded on the CAC it will work from your company computer if you have appropriate software and CAC reader.

The current time-out value for a JCVAS user is 45 minutes
- JCVAS user timeout setting will be changing in February 2011
- Current DOD regulations requires timeout after 15 minutes of inactivity and JPAS will be brought into compliance with policy
  - User must reauthenticate (i.e., re-enter CAC login or JPAS password) to re-enter JPAS
- DMDC will purge/delete accounts for users that have not log into JPAS in excess of 1 year. Projected January 2011.
DMDC will communicate upcoming deployments, modifications, and information regarding JPAS on the JPAS Welcome screen.

JPAS Updates will no longer be posted to DSS website.
JPAS Announcements

- JPAS User Support Documentation and Alerts are moving off of the DSS web site.
- Documentation will be in either JPAS or an upcoming DMDC User Support page.
  - DMDC will provide a new URL for the JPAS User Support page in upcoming weeks
- Currently alerts are on the Welcome screen once you log into JPAS
  - User must log into JPAS daily
- Additional information can be found on DMDC home page @ www.dmdc.osd.mil
Update to Release Investigation Request (new)

Release Investigation Request
Signature Forms, Attachments, and Release for Processing

NOT COMPLETING THESE TASKS WILL DELAY PROCESSING OF YOUR INVESTIGATION REQUEST

• Carefully follow the instructions provided below in the order displayed.
• If you are unable to complete these steps at this time (e.g., if you do not have access to a printer at your computer), you MUST return to e-QIP at a later time to complete the remaining steps.
• Contact your agency if you need assistance with printing these documents.

After you certified the completeness and accuracy of the information in your Investigation Request, e-QIP generated a printable archival copy of the information you provided. You are strongly advised to print a copy for your records. Properly dispose of any working copies that you may have printed while editing and reviewing your information, as those are not considered official. You will need Adobe Acrobat Reader or Adobe Acrobat to view the archival copy. Click the "Help" link for more information.

Step One
Click this link to display the archival copy, then print a copy to retain for your records.
Display the Archival Copy of this Investigation Request for Printing

Next you must provide the required signature form(s). The requesting agency must receive the signed form(s) to begin processing your Investigation Request. Print, sign, and submit the form(s) according to the instructions you have been provided. Print to only one side of each sheet of paper. Ensure that the text on the printed copy is legible and that all pages print. The printed text may not contain gaps, extraneous lines, or other errors caused by printer problems. Click the "Help" link for more information.

Step Two
Click the appropriate link to display or download the signature form(s), then sign and attach to your request, or submit the forms to the office requesting your investigation. If you are using assistive technology, select the "Signature Forms" link.

Signature Forms for Printing: Signature Forms

Use the following methods for attachments for your investigation request:

• Regular Fax, Mail, or Other - indicate how you plan to send each attachment

Step Three
Regular Fax, Mail, or Other

NOTE: Write your social security number and the Request ID number (7946623) on the margin of each attachment you submit.

Name/Description
Number of Pages
Method of Transmission

Faxed - Attachment will be faxed.
Add Expected Attachment

Expected Attachments

<table>
<thead>
<tr>
<th>#</th>
<th>Name/Description</th>
<th>Pages</th>
<th>Method</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>No records were found to display.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

IMPORTANT: YOUR BACKGROUND INVESTIGATION CANNOT START UNTIL YOUR AGENCY RECEIVES ALL REQUIRED SIGNED SIGNATURE FORMS.

When you have completed the steps listed above, you may release your Investigation Request for processing. Performing this step will electronically transmit your Investigation Request to the agency requesting your investigation, and you will no longer have online access to it for printing, review, or directly adding attachments.

Step Four
After you complete the previous step, click this button to release and transmit your Investigation Request to the requesting agency.

Release Request/Transmit to Agency
Training

- **JPAS Training for Security Professionals** – Course No. PS123.16 (8 hr web-based)
- **DSS Personally Identifiable Information (PII)** – Course No. DS-IF101.06 (45 min web-based)
- **eQIP** – Multiple courses to include: Initiating, Managing, Reviewing, and Solutions to Common Issues
- **Industrial Security Facility Database (ISFD)** – Course No. IS111.06 (5 hr web-based)

**Link to ENROL:** The following link will take you to the Defense Security Service (DSS) ENROL system: [https://enrol.dss.mil/enrol/lang-default/SYS_login.asp](https://enrol.dss.mil/enrol/lang-default/SYS_login.asp). where you can register for the course or create a new account.

For additional information regarding an ENROL account, contact the DoD Security Service Center, 1-888-282-7682, occ.cust.serv@dss.mil; for information about the course content contact IA/CND at DSSIACND@dss.mil
PRs for Cleared NISP Contractors (eftv 6/9/10)

- DISCO will identify and notify NISP cleared contractor facilities of cleared personnel who are eligible or overdue for a periodic reinvestigation (PR).

- Eligibility for a PR is contingent upon the access level and the closed date of the investigation.

- Once a cleared contractor facility is notified a PR is due, the contractor facility will have 60 days to submit the SF-86 to DISCO via JPAS.

- If the information is not received in 60 days, DISCO will assume the clearance is no longer required, remove the clearance eligibility and send notification to the FSO that the eligibility was withdrawn due to failure to submit the requested forms.

- If the cleared contractor facility identifies that the individual still requires a clearance after the eligibility has been withdrawn, the clearance eligibility will be reinstated upon submission of the required information. Access to classified information is not valid during the period that the eligibility is withdrawn until DISCO reinstates the clearance eligibility.
Loss of Jurisdiction

- When a subject has an eligibility of Loss of Jurisdiction, there is no clearance eligibility, i.e. the subject should be debriefed and no access provided until an eligibility that supports access is entered by a CAF. Loss of Jurisdiction is usually used in one of three instances:
  - An interim eligibility had been issued and then it is withdrawn until the final determination may be rendered.
  - Subject had a final eligibility. An incident report was submitted and there is no longer an active DoD association where subject requires clearance eligibility. The incident report will not be adjudicated until there is an active DoD association.
  - A CAF, other than DOHA, determines that a subject no longer requires access to SCI. If the subject still requires access to Top Secret the FSO should notify DISCO via R/R/U. In this instance, the FSO should debrief and remove the individual from SCI access. The collateral access should remain in JPAS to ensure that the collateral clearance need is identified. Failure to leave the collateral access in JPAS, may result in discontinuance of processing.
Foreign Passport Disposition

- DISCO will not grant or continue a personnel clearance if the individual possesses a current foreign passport.

- If the FSO accepts a surrendered passport and returns it while it is still current, you must submit an incident report with details concerning the return of the passport.

- Reasons for the return of the passport should be provided in the incident report.

- An incident report must be submitted if the passport is returned at the time of the individual's employment termination.

See DSS News dated: 11/20/09 “Foreign Passport Disposition Influences Personnel Clearance Eligibility” or click the following link: [http://www.dss.mil/diss/jpas/jpas.html](http://www.dss.mil/diss/jpas/jpas.html)
JPAS Today

JAMS + JCAVS = JPAS

Defense Manpower Data Center (DMDC)

**Joint Adjudication Management System**
- Used exclusively by CAFs for tracking adjudication actions and clearance results

**Joint Clearance Access Verification System**
- Used by security to indoctrinate eligibility information

**Joint Personnel Adjudication System**
- Provides “real-time” information regarding eligibility access and investigation status
JPAS Future

CATS + JVS = DISS

**Case Adjudication Tracking System**
- Used exclusively by CAFs for tracking adjudication actions and clearance results

**Joint Verification System**
- Used by security to indoctrinate eligibility information

**Defense Information Systems Security**
- Provides “real-time” information regarding eligibility access and investigation status
Case Adjudication Tracking System (CATS)

- CATS will replace JAMS

- CATS is the case management system that allows electronic transmission of investigative reports from the Office of Personnel Management to DISCO

- DISCO uses CATS to adjudicate electronic investigations, and CATS will update JPAS
  - CATS has been deployed to Army, DISCO, Navy
  - CATS is in process of deploying to WHS and AF
Joint Verification System (JVS)

- JVS will replace JCAVS

- JVS will provide the following benefits:
  - Continuous Evaluation/Incident Event Trigger Report working with ACES
  - Will provide SMOs a more robust work management tool
  - Will be able to leverage capabilities of other DISS systems to create a specialty management tool combining, tracking, and evaluating the information provided by CATS and ACES
  - Enterprise Services will be deployed with JVS
    - Portal
    - Workflow
    - Document Management
Defense Information System for Security (DISS)

- DISS will replace JPAS and incorporate Enterprise Services

- DISS will be used to implement Joint Reform Team (JRT) principles within DoD
  - Validate Need for hiring and clearance requests
  - Automated Records Check
  - Enhanced Subject Interview
  - Continuous Evaluation (annually for TS/SCI, every 5 years for S)

- DISS will be a single point of entry for the DoD security process
Transition Status

- **JAMS Migration to CATS:**
  - Phase 1: Requirement Gathering: Q3 – Q4 2009
  - Phase 2: Design and Development: Q3 2010 – Q4 2011

- Working with DMDC to decommission JPAS by April 2012
JVS Capabilities

- Working group sessions held with BTA and JPAS Industry Team Leads to review and define system requirements
- JVS will provide current JCAVS functionality
- Additional requirements identified:
  - Mass personnel updates
  - Electronic document transmission
  - Notifications, messaging, and correspondence
  - Robust reporting and business intelligence
  - Federated search
  - Clearance tracker
  - Digital signature
  - Excel based queries
Future Changes That Will Affect Industry

- New SF86 projected early 2011
  - Additional drop downs for yes/no questions (can yield up to 447 questions)
  - DISCO will not grant Interims until the NAC portion of FPC has been conducted – projected date – unknown
- Projected to Transition to e-QIP Direct in the future and at that time e-QIP investigation requests will no longer be initiated via JPAS
  - Account Management functions will be limited, permissions need to be defined/established (currently being worked)
  - DISCO will approve e-QIP for Industry and forward to OPM (projected)
  - e-QIP actions will be time stamped and can be seen from start to finish
- Everyone within federal government will have to transfer to e-QIP Direct, not just DoD
- Everyone with CAC card will be required to use it; must have CAC reader
- DMDC will require everyone to have some type of secure communication: Personal Identity Verification (PIV), Public Key Infrastructure (PKI) encryption or authentication
- URL for ISFD - https://isfd.dss.mil/ISFDweb
PSM Net Validation

- From the Main Menu select “PSM Net”
  - Will take you to JCAVS Maintain PSM Net Screen
- Select “Person Categories by Organization”
  - Click “Add” - Will take you to PSM Net Add Organization Category
- Hit “Select Organization” - Will take you to organization search
- Select DoD Contractor Companies
  - Enter your cage code (plus *) in last box
  - Click “Search” – selected cage will show up
  - Click blue link indicating cage code; company name will move to top line
  - Click “OK” – Will take you back to “PSM Net Add Org…”
  - Click “Search”
  - Search result will indicate all persons associated with your cage that are not in your PSM Net
- Determine if each person listed should be in your PSM Net
  - If Yes – In-process and indoctrinate
  - If No – In-process and out-process using the same date; then go to Maintain Person screen and enter separation date and separation code. At midnight the person will drop out of your PSM Net and will no longer be associated with your Cage
JPAS Industry Team
Quinton Wilkes, Lead

Industry PMO
Quinton Wilkes
quinton.wilkes@L-3com.com

Tanya Elliott
telliott@cai.com

Education & Training Sub Team
Toni MacDonald – Team Lead
renita.macdonald@boeing.com

Clyde Sayler
clyde.j.sayler@L-3com.com

Rhonda Peyton
rpeyton@schaferalb.com

Carla Peters-Carr
CARLA.S.PETERS-CARR@saic.com

JPAS Industry Sub Team
Tanya Elliott – Team Lead
telliott@cai.com

Susie Bryant
smbryant@raytheon.com

Rene Haley
Rene.haley@ngc.com

Wanda Walls
wanda.walls@lmco.com

3/21/11 - Page 24
Additional Contact Information

DOD Call Center

888-282-7682
occ.cust.serv@dss.mil

Air Force Account Managers

Mr. Charles Clemmer
charles.clemmer@pentagon.af.mil
202-767-0484
DSN: 297-0484

Army Account Managers

Denise Brannon Deborah.Brannon@us.army.mil
301.677.6374
DSN: 622.6374

Susan M Rogers
Susan.M.Rogers@us.army.mil
301.677.7035
DSN: 622.7035

Navy/Marine Corps Account Managers

Roxanne Chrisman
roxanne.chrisman@navy.mil
202-433-8869
DSN: 288-8869

Jill Kirk
Jill.kirk@usmc.mil
703.692.0157
DSN: 222-0157
Questions