

**Posted 20 March 2015**

**Attention! Do NOT Look Up or View Your Own Record in JPAS**

As part of the JPAS User Monthly Audit, JPAS systematically audits the database for various misuses to include users who query and/or look up their own records by viewing their Person Summary screen in JCAVS or selected themselves in JAMS. The DMDC JPAS Account Management Policy states that all users consent to the terms of use of the DoD System of Records and agree to comply with the Privacy Act of 1974, applicable DoD regulations, other applicable laws, and JPAS policies. The Account Management policy prohibits users from querying and/or looking up their own record in the Department of Defense (DoD) personnel security system of records; this a DoD Privacy violation and constitutes a misuse of JPAS. Notifications will be emailed to users who have violated JPAS policy by querying and/or looking up their own record within the last 30 days as a warning to the user.

**Posted 18 March 2015**

**NEW! JPAS Industry Persons to be added to the DoD Person Data Repository (PDR)**

JPAS will soon be providing identity information on cleared industry persons with no other DoD affiliation to the PDR in order to facilitate SIPRnet token issuance as well as JVS data migration. One of the requirements for SIPRnet tokens is for an individual to have an Electronic Data Interface Person Identifier (EDIPI) and providing personnel information in JPAS to the PDR will facilitate that identifier generation. As a result the JPAS records that had no EDIPI associated with it will now have one, and Industry FSOs will not be able to manually update data for those subjects directly in JPAS. Person data from the PDR will overwrite whatever is changed in the JPAS database once per month on the day of the subject's birth. As a result FSOs will now need to follow PDR data update instructions included in the [Data Correction Checklist](#). This data migration will occur over the next 60-90 days in small batches and is dependent on PDR's schedule.

**NEW! JPAS 1<sup>st</sup> Quarter 2015 Newsletter Published**

**Posted 9 March 2015**

**NEW! JPAS REPORTS:**

The JPAS report authentication errors are caused by a proxy server setting, when the end user refreshes their browser, or by a specific Internet Explorer download setting. These errors are outside of JPAS and located on the user's side. The workarounds are listed below.

Proxy Server: This type of error can occur when a duplicate report request is sent to JPAS due to the report runs longer than 2-5 minutes dependent on the user's proxy server settings. The user may receive this error when requesting reports in Immediate mode. The solution is to request the report in Background mode.

Browser Refresh: This type of error can occur when the user refreshes their browser while the report is being created. The solution is for users to not refresh their browser when a report is being generated or a report is being picked up.

Internet Explorer Security Setting: The third cause of this error is due to a security setting in Internet Explorer web browser that specifies whether or not the web browser will allow files to be downloaded from Internet websites.

IE 8 and 9: These browsers have a default setting for file download as Disabled. If the web browser asks the user if they want to allow the file to download and the setting is set at disabled, an authentication error will occur. The solution is for the users to change the security settings to Enable to allow for file download.

IE10 and higher: These browsers have a default setting for file download as Enabled. This is the value that JPAS Reports needs and may be set accurately for all end users, but some local user security configurations might have set this value to Disabled. The solution is for the users to verify the correct setting by going to Tools > Internet Options > Security Tab > Zone > Custom Level > File Download > Switch the toggle from disable to enable.

Pop-Up Windows: If users do not allow pop-up windows for the [jpaspi.dmdc.osd.mil](http://jpaspi.dmdc.osd.mil) website then they will also have issues with running JPAS reports. The JPAS Application website will pop-up in a new window to access the report application. If the pop-up messages are Disabled, the user will never be able to run or pickup any type of report. The solution is for users to Enable pop-up messages.

### **NEW!!! No Test or Fake SSNs in JPAS**

An email went out to users who have inserted, used, selected, or tested with a fake SSN in JPAS notifying them that test or fake SSNs are not allowed in JPAS. The email stated the Department of Defense Regulations and Defense Manpower Data Center (DMDC) Joint Personnel Adjudication System (JPAS) Account Management policies that prohibits users from entering or using false or inaccurate information including, entering test or "dummy" personal information into the Department of Defense (DoD) personnel security system of records. The current DoD Privacy Program, DOD 5200.11-R (May 4, 2007), regulation at C1.2 through C1.2.2 (Standard of Accuracy) explains that all personal information from a DoD system of records that is used or may be disclosed is accurate, relevant, timely, and complete for the purpose for which it is being maintained. The DoD regulation also requires users of the DoD system of records to make a reasonable effort to ensure that the information about an individual is accurate, relevant, timely, and complete prior to dissemination. The DMDC JPAS Account Management Policy states that all users consent to the terms of use of the DoD System of Records and agree to comply with the Privacy Act of 1974, applicable DoD regulations, other applicable laws, and JPAS policies.

JPAS is a fully audited database that reflects anytime a user selects, adds, modifies, or deletes anything in JPAS. Although users may question the validity of the email, the audit logs show that the user who received this email has inserted, used, selected, modified, and/or taught other users with these SSNs. An example of "test" or "fake" SSNs are SSNs with all 1's, 2's, 3's, 4's, 5's, 6's, 7's, 8's, or 9's. Another example is 123-45-6789.

After sending the email out, DMDC became aware of JPAS refresher training courses that were given using test SSNs for authorized users to select.

**Posted 3 March 2015**

### **Some Users Experiencing Authentication Error While Running Reports: Fix**

If the JPAS user receives an Authentication error while running a report in Immediate mode, re-run the report in background mode using the Submit & Pickup option after the initial report finishes. The Authentication error can be caused by refreshing the browser or by a proxy server configuration.

Additionally, if you have requested a report for immediate delivery, **DO NOT** refresh the browser window, this creates a duplicate report request and can also cause an authentication error.

Finally, some browser settings can also result in an authentication error. Older versions of Internet Explorer are defaulted to not automatically download files that are passed from the JPAS reports server to the user, to change this setting and prevent an authentication error, go to Tools → Internet Options → Security Tab → Zone → Select the Custom Level, then users will need to find the “File Download” option in the window and ensure the toggle is set to “Enable” for file download.

**Posted 20 February 2015**

**NEW VERSION of PSSAR Form Required to Request JPAS Access:**

Effective March 1st, all requests for JPAS account activations, modifications, or deletions **MUST** be submitted on the new PSSAR form. The new form is available on the left-hand navigation on this page under the header "[Access Request](#)." After March 1st, requests submitted on old versions of the form will be denied. Please note, DMDC is in the process of updating the version of the form on the DTIC website.

**Posted 5 February 2015**

**ACTION REQUIRED! Security Management Office (SMO) Contact information Update:**

SMO Points of Contacts need to ensure that their SMO Contact Information is current and in the correct format. Only the correct format will be accepted. Those with information in an incorrect format will not receive pertinent information such as messages concerning the JCAVS to JVS migration, Continuous Evaluation updates, etc. The following Email Address and Phone Number format are REQUIRED:

- Email Address field should **ONLY** contain an email address with NO additional wording before or after the email address.  
*Correct Format:* [jane.doe@email.com](mailto:jane.doe@email.com)  
*Incorrect Format:* For visit requests, email [jane.doe@email.com](mailto:jane.doe@email.com)
- Additional email addresses should be separated only by a semi-colon (;).  
*Example:* [jane.doe.civ@mail.com](mailto:jane.doe.civ@mail.com); [jane.doe.ctr@mail.mil](mailto:jane.doe.ctr@mail.mil)
- Phone Number format: Country Code + Area Code + Phone Number.
- Please see the [JVS Updates Document](#) for examples

**Please Make Any Necessary Email and Phone Number Corrections IMMEDIATELY**

**NEW! Federal Bureau of Investigations (FBI) SMO REMOVED:**

The FBI SMO has been removed. For visit requests, please contact your FBI Security Officer (SO) directly to process visit requests.

**NEW! JPAS Release 5.4.3.0 Coming Soon!:**

New JPAS release version 5.4.3.0 coming soon. Join us for a “Talk with the JPAS Team” DCO session on Thursday, 26 February 2015 at 1 PM ET to learn more. A follow up session will be held Tuesday, 3 March 2015 at 1 PM ET. Space and bandwidth may be limited so please join the DCO session early at the following link:

<https://connectcol.dco.dod.mil/jpastalk/>

Additional information on how to access our DCO meetings can be found [here](#). Check back regularly for updates as we near the meeting date.

### **JPAS Users with Nicknames in JPAS:**

DMDC has concluded the audit on all JPAS users regarding use of nicknames in JPAS. Please review all of your JPAS account holder's names in JPAS and ensure the user's name is their LEGAL NAME (on SSN, passport, etc.) and not their nickname. Notifications will be emailed to users and users have until 1 March 2015 to correct the JPAS record to be the LEGAL name. The email addresses that will be used are those in the JPAS User Profile.

**Posted 21 January 2015**

### **NEW! DQI-830 JPAS Subjects with N/A, Non-US Citizen or Blank**

DMDC has run the Non-US Citizenship DQI on 16 January 2015. This was 30 days after the final approval from USD (I) regarding the remaining JPAS subjects who do not have a U.S. Citizen indicator, the personnel center feeds, and the 15 December 2014 deadline.

**Do not call DSS, DEERS, or DOD CAF as they cannot assist.**

If a subject has fallen into the Administrative Withdrawal status due to a Non-Citizenship value, please follow the steps listed below:

1. Call the DMDC Contact Center at 1-800-467-5526
2. Have the Customer Service Representative (CSR) submit for a DRS ticket and get the call ticket number
3. Send an encrypted email with the SSN, Citizenship Paperwork along with the ticket number to the DMDC Contact Center to [dmdc.contactcenter@mail.mil](mailto:dmdc.contactcenter@mail.mil). You will need to exchange certs with the Contact Center to send an encrypted email and do NOT mark the message as 'Private' as the Contact Center will not be able to see it.
4. The Contact Center will ONLY submit a DRS ticket once the paperwork has been

### **Report Updates:**

20 January: During the testing, an issue was discovered thus causing a delay in the deployment of JPAS reports. The issue has been resolved and testing has been resumed. The JPAS reports testing is currently in User Acceptance Testing.

**Posted 19 December 2014**

### **DQI-830 JPAS Subjects with N/A, Non-US Citizen or Blank – 15 December Deadline**

DMDC has received the final approval from USD(I) concerning the remaining JPAS subjects who do not have a U.S. Citizen indicator, they will have their eligibility changed to "Eligibility Administratively Withdrawn." DMDC will process all of the service files from the 15th. Please ensure affected subjects submit all necessary paperwork to their personnel centers to ensure no one is negatively impacted. You can utilize the [JPAS Data Correction Checklist](#) as a tool to assist SO/FSO in identifying where to update the Citizenship information.

### **Subjects Requiring Periodic Reinvestigations (PR) – Debrief, Downgrade, or Lose**

In order to complete the requirements identified in the DNI memo "Strategy to Reduce the Periodic Reinvestigation Backlog Using a Risk-Based Approach," DMDC is working with the Military Services, DoD Agencies, and DSS (for Industry) to ensure that all JPAS subjects who do not have supporting, in-scope investigations no longer have access. As a result SOs/FSOs might be contacted in order to initiate re-investigations on subjects with out-of-scope investigations. If re-investigations are not opened on these subjects, the subjects may be administratively debriefed from access (DQI 597), lose their favorable eligibility and/or be downgraded to a lower eligibility. This may impact those military and civilian populations in regards to position sensitivity. Data has been provided to identified service and agency POCs.

Attention Industry: In working with DSS and USD(I), DQI 838 will be ran at the beginning of January to downgrade INDUSTRY ONLY subjects with an overdue PR. In order to maintain in-scope eligibilities for subjects with Industry categories in JPAS, a PR must be submitted. For instance if a subject were to have a Top Secret eligibility and an investigation older than 5 years, but younger than 10 with no open/ongoing investigation on record, the eligibility will be dropped to Secret. Subsequently when the investigation reaches 10 years and no open investigations are initiated, that eligibility will be downgraded to Confidential, if no action is taken beyond 15 years, the eligibility will be downgraded to a generic "Favorable." Corresponding accesses will also be removed during these downgrades (DQI 597), and record archive rules will still be in effect. Please note if the higher eligibility is required, the previous eligibility may be reinstated upon submission of an e-QIP for periodic review. If you believe there was an error made, you may submit an RRU to DOD CAF Industry for possible correction.

**Posted 3 December 2014**

### **PSSAR Retention Policy Guidance**

The current Personnel Security System Access Request (PSSAR) is being revised to incorporate clearer instructions and new SWFT roles and will be published soon. As part of the DMDC Contact Center JPAS account creation and the PSSAR publishing process, DMDC went to OSD, Records & Information Management Program for additional guidance on the requirement to store PSSARs. OSD, Records and Information Management Program recited File Number 1606-06.2 (GRS 24, Item 6b) which states files/records relating to the creation, use, and maintenance of computer systems, applications, or electronic records can be deleted/destroyed when no longer needed for administrative, legal, audit or other operational purposes (but not before the account termination). This has been a change in the previous information DMDC was given. The new requirement has been updated in the JPAS Account Management Policy.

**Posted 13 November 2014**

### **NEW!!! Director of National Intelligence Guidance**

On October 25, 2014, Director of National Intelligence (DNI), as the Security Executive Agent, issued ES 2014-00674 to all Federal Departments regarding the Adherence to Federal Laws Prohibiting Marijuana Use. The memo reminds agency heads that changes to state and District of Columbia laws pertaining to marijuana use **DO NOT** alter the federal laws prohibiting the use, sale, or manufacture of marijuana. An individual's disregard of federal law remains relevant in making determinations under the National Security Adjudicative Guidelines.

**Posted 17 October 2014**

### **NEW!!! Incorrect Air Force Separation Dates**

On 15 October, DMDC and the Air Force identified an issue where incorrect separation dates were provided to JPAS on Air Force categories. Root cause has been identified and DMDC and AF are working to ensure the affected records are restored and the issue does not occur again.

**Posted 10 October 2014**

### **NEW!!! Subjects Requiring Periodic Reinvestigations (PR)**

In order to complete the requirements identified in the DNI memo "Strategy to Reduce the Periodic Reinvestigation Backlog Using a Risk-Based Approach," DMDC is working with the Military Services, DoD Agencies, and DSS (for Industry) to ensure that all JPAS subjects who do not have supporting, in-scope investigations no longer have access. As a result SOs/FSOs might be contacted in order to initiate re-investigations on subjects with out-of-scope investigations. If re-investigations are not opened on these subjects, the subjects may be administratively debriefed from access and lose their favorable eligibility. Data will be provided to identified service and agency POCs.

### **NEW!!! JAMS User Accounts**

The JPAS team will be conducting an audit of JAMS accounts in order to remove access for accounts that do not meet account requirements. Any open cases associated with those accounts will be migrated to valid users at the DoD CAF.

### **DQI 690 - Military Subjects in the Individual Ready Reserve (IRR) or the Standby Reserve**

Service members that have been identified as being in the IRR or Standby Reserve who have Favorable eligibilities of Confidential, Secret, Top Secret, or SCI changed to a more generic "Favorable" eligibility if the IRR or Standby reservist does not have any other person categories at the time of the DQI, and have no activity for the past 24 months. The separation date from the active duty military category will be used to populate the favorable eligibility effective date. When the record is not serviced or updated for 24 months, the eligibility will be changed to "Eligibility Administratively Withdrawn." Former eligibilities will be restored if the subject is activated. It is important to note that the eligibility change to "Favorable" and/or "Eligibility Administratively Withdrawn" does not reflect adverse information placed on the subject and/or record.

### **DQI 691 - JPAS Records with No Activity or Ownership in the Past 24 Months**

Some JPAS records have not been properly archived due to lack of a separation date or having an open security incident. As a result, it has been determined that eligibilities of Confidential, Secret, Top Secret, or SCI are no longer needed. These records will now have the eligibility field changed to "Eligibility Administratively Withdrawn," if they meet the criteria of having no other person category, no activity on the person category and no owning or servicing SMO in the past 24 months. This initiative will affect all subject person categories in JPAS. It is important to note that the eligibility change to "Eligibility Administratively Withdrawn" does not reflect adverse information placed on the subject and/or record.

### **Report Updates:**

22 July: During our research to correct the issues, we found that IE automatically has a 60-minute timeout even though the report may still be running on the JPAS servers. Workarounds is to use Firefox and/or Chrome as those browsers do not have the 60-minute timeout function.

7 August: The JPAS team has improved the time of several long running reports. The CSV

formatting has been completed for all reports and is currently undergoing extensive testing. The JPAS team is also modifying the JPAS reports interface to resolve the memory issue. Once the interface modification, an additional round of testing with both the long running reports and the new interface modification will occur. After successful testing, the JPAS team will roll out the reports update.

18 September: The JPAS team is still continuing to test and make modifications to the reports to ensure the formatting and performance issues are fully addressed. After successful testing, the JPAS team will announce the deployment date of the new reports.

2 October: On the CSV report files, the DoD document protective marking, "For Official Use Only" (FOUO) will be placed on the header of the file verses the footer.

NEW Update: 10 October: If a report times out, please wait at least 2 hours before kicking off another large report; the report is still running in the background and can negatively impact the report server. The report remains in cache and will return relatively shortly after you kick off another report at the 2 hour mark. Also, once the new reports release is deployed, JPAS will be removing the capability for users to initiate more than 1 report in order to ensure load on the server is properly managed. Please see previous posted guidance in the JPAS General FAQ, question #40.

### **Posted 6 October 2014**

DMDC, OMB, ODNI, and USD(I) have been working together on several Data Quality Initiatives (DQI's) that will potentially affect cleared populations. These DQI's will begin running the week of September 22<sup>nd</sup> and end September 27<sup>th</sup>.

**Please Note Regarding DQI's 690 and 691:** *As a reminder, it is important to note that the eligibility change to "Eligibility Administratively Withdrawn" and/or "Favorable" **does not reflect adverse information** placed on the subject and/or record.*

### **DQI 689: Separation of Cleared Military and Civilian Categories**

Data Quality Initiative (DQI) 689 was successfully executed on the 22<sup>nd</sup> and 29<sup>th</sup> of September. The eligibility was modified to "Eligibility Administratively Withdrawn" for all Active Civilian and Military Person Categories with no other open person category activity AND did not have an owning and/or servicing Security Management Office (SMO) for their military/civilian person category for the past 2 years. DMDC has identified a discrepancy where if an Industry subject had recently separated, their eligibility was also modified. The JPAS team is currently working to restore these eligibilities.

### **DQI 690: Military Subjects who are Individual Ready Reserve or Standby Reserve**

USD(I) and Reserve Affairs are analyzing the effects of the DQI 690 and coordinating the best way to fulfill the requirement of handling Individual Ready Reservists (IRR) or Standby Reservists (SR) who do not have any other person categories. As a result, these IRRs/SRs do not have any valid need-to-know for access. Their eligibility will be changed to a generic "Favorable." This new eligibility will be backdated with the separation date populated on their last active military category. Please check back for an updated status.

### **DQI 691: Subjects that have had no Active Categories for the Past 2 Years**

DQI 691 will change the eligibility to “Eligibility Administratively Withdrawn” for those subjects whose record should have been archived, but were not due to either an open incident or case. DQI 691 is expected to run during October.

### **Security Management Office (SMO) Contact information Update**

SMOs Points of Contacts need to ensure that the SMO Contract information is current and in the right format. The following email address and phone number format are required:

- Email address field should ONLY have an email address with NO additional wording after the address. For example: [jane.doe@email.com](mailto:jane.doe@email.com) and NOT “For Visit Requests, email [jane.doe@email.com](mailto:jane.doe@email.com).”
- Additional email addresses should be separated by a semi-colon (;). Example: [jane.doe.civ@mail.com](mailto:jane.doe.civ@mail.com); [jane.doe.ctr@mail.mil](mailto:jane.doe.ctr@mail.mil)
- Phone number format: country code + area code + phone number. Example: 1+000+000+0000
- US Country code is 1
- Please see the [JVS Updates Document](#) for examples

### **Posted 18 September 2014**

DMDC, OMB, ODNI, and USD(I) have been working together on a Data Quality Initiative (DQI) that will potentially affect cleared populations. These DQI’s will begin running the week of September 22<sup>nd</sup> and end September 27<sup>th</sup>.

### **DQI 689: Separation of Cleared Military and Civilian Categories**

DQI 689 will separate all Active Civilian and Military Person Categories with no person category activity **AND** no owning and/or servicing Security Management Office (SMO) for the past 2 years.

### **DQI 690: Military Subjects who are Individual Ready Reserve or Standby Reserve**

DQI 690 is still in coordination with Reserve Affairs and USD(I). DQI 690 is looking at Individual Ready Reservist or Standby Reservist who do not have any other person categories and as a result do not have any valid need-to-know for access. Their eligibility will be changed to a generic “Favorable.” This new eligibility will be backdated with the separation date populated on their last active military category.

### **DQI 691: Affects Subjects that have had no Active Categories for the Past 2 Years**

DQI 691 will change the eligibility to “Eligibility Administratively Withdrawn.” of those subjects whose record should have been archived, but were not either due to an open incident or investigation.

### **JPAS Users with Nicknames in JPAS**

DMDC is currently conducting an audit on all JPAS users ensuring the **LEGAL** name is in the first, middle, and last name fields in JPAS. For example, if your identity credential states William Smith but your JPAS record has Bill Smith, your account will be flagged. If your identity credential states Elizabeth Smith but your JPAS record reflects Lizzie Smith or Elizabeth (Lizzie) Smith, your account will be flagged. This will be rolled out in phases giving users enough time to make the modification prior to their accounts being locked out. Please review all of your JPAS account holder’s names in JPAS and ensure the user’s name is their legal name (on SSN, passport, etc) and not their nickname.

**Posted 2 September 2014**

**DQI 689: Separation of Cleared Military and Civilian Categories**

DMDC, OMB, and USD(I) have been working together on a Data Quality Initiative (DQI) that will potentially affect cleared military and civilian populations.

DQI 689 will separate all Active Civilian and Military Person Categories with no owning and/or servicing Security Management Office (SMO) **AND** no JPAS activity or SMO relationship on the record for the past 2 years.

DMDC is unable to notify the Security Officers at the SMOs due to these JPAS subjects having no owning or servicing relationships. However, DMDC is trying to determine and notify the Services and DoD Agencies that may have been associated with the subjects prior to running DQI 689. Please review all civilian and military personnel to ensure subjects are appropriately owned and/or serviced so military and civilian subjects are not negatively impacted.

**Posted 9 August 2014**

**NEW UPDATE!!! JPAS Subjects with N/A, Non-US Citizen or Blank**  
**Please do not directly contact the DoD CAF or DEERS teams on citizenship issues**

**8 August 2014:**

DMDC has been working closely with the military and civilian personnel centers to get the U.S. Citizenship field updated across all databases (e.g., personnel center, PDR, JPAS) for JPAS subjects who are verified U.S. Citizens.

A request for an extension until 31 August 2014 was granted by USD(I).

Please note that DMDC will be pulling all JPAS subjects with a non-U.S. Citizenship, N/A, or blank value and providing these numbers to USD(I) on August 25, 2014. USD(I) will make a final outcome determination at that time. We ask that you continue to get this information updated as fast as possible so no JPAS subject is negatively impacted.

Please utilize the [JPAS Data Correction Checklist](#) as a tool to assist SO/FSO where to update the Citizenship information. Please see the prior 9 July 2014 update for additional information.

**9 July 2014:**

DMDC and USD(I) have been working together on ensuring that JPAS has accurate information. DMDC is currently working on a Data Quality Initiative (DQI) that will ensure individuals having access to classified information have JPAS records that are updated, accurate and complete. Security Officers (SO) or Industry Facility Security Officers (FSO) will be receiving notifications within the JPAS application regarding subjects who have a DoD eligibilities but their Citizenship field in JPAS has not been updated to be a U.S. Citizen as required by DoD Regulations. SO and FSO are required to ensure this field is in JPAS within 30 days of notification. If this data field is not updated, subjects may lose their eligibility and be debriefed from access.

Industry FSOs can manually update citizenship for subjects after verification of citizenship occurs. Industry FSOs may need to update DEERS if the subject has a prior DoD affiliation. This can be determined if an EDIPI is on the JPAS record.

SOs for DoD civilians or military services need to ensure the information is updated in their personnel centers (e.g. Army Human Resources Command who administer the Total Army Personnel Database (TAPDB), Navy Personnel Command, or the Human Resources specialist who has access to DCPDS, etc.) as these systems feed information into JPAS. Subjects with multiple person categories may need to update all relevant databases; for example, if a subject is a Reservist and a DoD Civilian both the military and civilian personnel center needs to be updated as both personnel centers feed into JPAS. Note that neither the DoD CAF, nor PDR (aka DEERS) are the source of military or civilian citizenship data nor they cannot assist in a data update request.

You can utilize the [JPAS Data Correction Checklist](#) as a tool to assist SO/FSO where to update the Citizenship information.

### **Posted 5 August 2014**

#### **JPAS Data Correction Checklist:**

Ever get frustrated trying to figure out what to do when a subject's PII keeps being overwritten or how to update a subject's PII? The JPAS team created a Step by Step document that will give you instructions on how to update a subject's PII in JPAS or keep it from being overwritten. See the new [JPAS Data Correction Checklist](#).

### **Posted 29 July 2014**

#### **Report Updates:**

Do not close blank screens as the reports are still running.

Update 17 June: The current formatting issue when exporting reports to Comma Separated Value (CSV) format will be corrected in a deployment to be released on 19 July, and users will then be able to generate CSV reports that adhere to the previous format.

Update 23 June: Some users are reporting error screens when cancelling reports, the JPAS team has confirmed that this is not a critical error, and that users can either click the "Log out" button at the top right of the screen and then close the window, or they can just close the error screen with no ill effect.

NEW! Update 22 July: On 2 July, the CSV reports were supposed to be corrected to be the old format. Unfortunately, one of the reports formats used created a memory issue. We are working to resolve the memory issue in addition to the other issues.

Possible workarounds:

NEW! IE 60 minute timeout: Not only is there some capability issues but the JPAS team just learned that the IE browser will automatically time out the session between the application and the browser after 60 mins. In the application, the query is still running but it will not be able to deliver to the browser due to the browser setting. Possible workaround is to use Firefox and Chrome.

### **Posted 11 July 2014**

## **Industry Overdue Periodic Reinvestigations**

On 7/10/2014, a JPAS message was sent to Facility Security Officers regarding a possibly overdue Periodic Reinvestigation being required for the subject. If this message concerned a subject's access at the NATO Secret level, please disregard the message if the NACLIC is within the 10 year scope.

If you received this message and you do not currently have access set for the subject, there is no need for a periodic reinvestigation and you may disregard the message.

If you think the message was received in error, please submit an RRU indicating such and the Personnel Security Management Office for Industry will research and respond.

For further information regarding overdue Periodic Reinvestigations, please visit the website at [http://www.dss.mil/psmo-i/indus\\_psmo-i\\_updates.html](http://www.dss.mil/psmo-i/indus_psmo-i_updates.html)

## **JPAS Subjects with N/A, Non-US Citizen or Blank**

DMDC and USD(I) have been working together on ensuring that JPAS has accurate information. DMDC is currently working on a Data Quality Initiative (DQI) that will ensure individuals having access to classified information have JPAS records that are updated, accurate and complete. Security Officers (SO) or Industry Facility Security Officers (FSO) will be receiving notifications within the JPAS application regarding subjects who have a DoD eligibilities but their Citizenship field in JPAS has not been updated to be a U.S. Citizen as required by DoD Regulations. SO and FSO are required to ensure this field is in JPAS within 30 days of notification. If this data field is not updated, subjects may lose their eligibility and be debriefed from access.

Industry FSOs can manually update citizenship for subjects after verification of citizenship occurs. Industry FSOs may need to update DEERS if the subject has a prior DoD affiliation. This can be determined if an EDIPI is on the JPAS record.

SOs for DoD civilians or military services need to ensure the information is updated in their personnel centers (e.g. Army Human Resources Command who administer the Total Army Personnel Database (TAPDB), Navy Personnel Command, or the Human Resources specialist who has access to DCPDS, etc.) as the these systems feed information into JPAS. Subjects with multiple person categories may need to update all relevant databases; for example, if a subject is a Reservist and a DoD Civilian both the military and civilian personnel center needs to be updated as both personnel centers feed into JPAS. Note that neither the DoD CAF, nor PDR (aka DEERS) are the source of military or civilian citizenship data nor they cannot assist in a data update request.

You can utilize the [JPAS Data Correction Checklist](#) as a tool to assist SO/FSO where to update the Citizenship information.

## **Attention Raytheon PKI Users:**

On 22 July JPAS will no longer accept your historical certificates for authentication according to your recent corporate PKI re-keying effort. Please work with your IT resources to update the certificates on your PKI devices to facilitate continued access. You will have to re-register your new certificates to access your account, so please work with your JPAS Account Managers to assist with temporary password generation as needed.

**Posted 10 June 2014**

**Last Name and DOB Values Now Required When Searching by DOD EDI PN**

The DoD Privacy Office requested DMDC to remove the EDI Search function as it was a violation of subjects PII. As a result, DMDC worked with all Services for over 8 months to keep the EDI Search function in JPAS as the functionality was still needed. The compromise was to allow SOs/FSOs to continue using EDI Search but now require Last Name and DOB values, much like the SII Search. The requirement to use Last Name and DOB values for EDI Search also eliminates possible JPAS misuse.

**Posted 2 June 2014**

**ATTENTION REPORT USERS: Do Not Close Blank Report Screen**

Following the migration to a new reports server, users will now see a pop up box stating that the requested report is loading and a blank screen will appear. **DO NOT CLOSE THE BLANK SCREEN;** your report is being processed. Wait for the loading icon to appear, which may take between 30 seconds and one minute, depending on the report and parameters selected. \*Regarding the Personnel Report only: the window pop up window stating that the report is being processed will remain open even after processing is complete. Once you have opened the report, you may close the pop up window.

**JPAS Reports Server Migration Completed**

DMDC migrated JPAS reports servers from one software package to another during the last outage period. As a result, the server might require fine tuning or additional configuration changes that might impact the availability of JPAS reports. During this time we appreciate your patience as updates are being made to our infrastructure.

Testing with the new reports server software has revealed some compatibility issues with Internet Explorer 9 and 10 users. These users might find that reports might not be rendered on screen as expected and they might have a consistent message that states “Please wait – Loading...” The JPAS team has identified a work around to assist users in turning off Compatibility View in IE9 and 10 so that reports can be properly generated, please see the following steps if you are affected:

- Select “Tools” from the IE menu bar.
- Select “Compatibility View Settings” option.
- Uncheck “Display all websites in Compatibility View”.
- Uncheck “Display all intranet sites in Compatibility View”.
- Click the Close button.
- Exit and re-open IE 9/10

**Posted 29 May 2014**

**Attention Civilian JPAS Subjects**

***Update 27 May:*** DCPDS has provided the corrected data and JPAS Civilian person records should now reflect the proper data.

Due to separation date data received on 25 APRIL 2014 from Civilian agencies, some Civilian JPAS subjects had their person categories erroneously separated, access removed, and the person category archived. The JPAS team is aware of the issue and is actively researching a solution with the Civilian Personnel Center to correct person records. Security Officers may want to verify your Civilian subjects and identify potential discrepant data. If discrepancy is identified, please contact the DMDC Contact Center.

**Posted 13 May 2014**

**Talk with the JPAS Team**

In support of the JPAS 5.4.0.0/5.4.1.0 release changes the JPAS team will be hosting a virtual meeting for all JPAS users on Thursday, 29 May starting at 1 PM ET at the following link:

<https://connectcol.dco.dod.mil/jpastalk>

**Posted 9 May 2014**

**Upcoming JPAS Reports Server Migration**

DMDC will be migrating JPAS reports servers from one software package to another during the next outage period. As a result, after 31 May, the server might require fine tuning or additional configuration changes that might impact the availability of JPAS reports. During this time we appreciate your patience as updates are being made to our infrastructure.

**Posted 2 May 2014**

**Clarification Regarding JCAVS' Person Summary Screen PRINTOUTS: [Policy No Longer in Effect: Printouts are no longer authorized]**

~~Military, DoD and non-DoD Civilian Users:~~ The printing out of the JCAVS Person Summary Screen can only be utilized when a Federal Government Agency requests the printout for reciprocity or compliance purposes **and** JPAS access is unavailable. JCAVS Person Summary Screen cannot be utilized for law enforcement or Privacy Act purposes. This printout screen can only be used to provide proof of investigation, eligibility, and access at that single point in time at the Federal Government Agency request.

~~Industry Users:~~ The guidance to military, DoD and non-DoD civilian JPAS users ~~does not~~ apply to National Industrial Security Program (NISP) JPAS industry users regarding JCAVS Person Summary Screen Printouts. Industry users should continue to follow current National Industrial Security Program Operating Manual (NISPOM) and Industrial Security Letters (ISL) guidance. Contact Defense Security Service with any questions. All ISLs are located at [http://www.dss.mil/isp/fac\\_clear/download\\_nispom.html](http://www.dss.mil/isp/fac_clear/download_nispom.html). The NISPOM is located at <http://www.dss.mil/documents/odaa/nispom2006-5220.pdf>.

~~ALL JCAVS PRINTOUTS must be protected from unauthorized disclosure. If a Federal Government Agency requests a printout for reciprocity or compliance purposes **and** JPAS access is unavailable at that agency, the record must be protected with a DD Form 2923 and according to the requirements for privacy/sensitive information and For Official Use Only (FOUO), Privacy Act of 1974, and DoD Privacy Program (DoD 5400.11-R).~~

~~All Privacy Act requests must be made according to the JPAS SoRN Record Access procedures. JPAS' SoRN is located at:~~

~~<http://dpclo.defense.gov/Privacy/SORNSIndex/DODwideSORNArticleView/tabid/6797/Article/6701/dm-dc-12-dod.aspx>. All law enforcement requests used for investigations must be forwarded to DMDC and printouts cannot be utilized.~~

**Attention Civilian JPAS Subjects**

Due to separation date data received on 25 APRIL 2014 from Civilian agencies, some Civilian JPAS subjects had their person categories erroneously separated, access removed, and the person category archived. The JPAS team is aware of the issue and is actively researching a solution with

the Civilian Personnel Center to correct person records. Security Officers may want to verify your Civilian subjects and identify potential discrepant data. If discrepancy is identified, please contact the DMDC Contact Center.

### **Posted 24 April 2014**

#### **JPAS Server Certificate Update**

The server certificate that helps to create a secure connection between users and the JPAS application is being replaced this week. There is a very low probability that users will be affected, but in the case that you might find yourself receiving a warning from your browser that the website is not trusted when you try to navigate to the sign on page, then you may not have DoD CA-27 installed in your local trust store.

There are two relatively simple solutions to rectify this issue:

1. Download and install the [InstallRoot v3.16](#) utility, and run the application to install all DoD certificates onto your machine (note Windows 8 users may have to use option 2)
2. Download the [DoD Root Certificate Package](#), open the resulting file and click through the folders on the right until you see a list of certificates, then double click "DoD CA-27" and choose the install option, and a wizard will guide you through the rest of the process

Once the certificate is installed, make sure that you close your browser and reopen before attempting to sign into JPAS again.

### **Posted 22 April 2014**

#### **Question of the Week:**

*Question:* What is a SAC? Do I know when OPM received my fingerprints?

*Answer:* Special Agreement Checks (SAC) are in addition to OPM's standard background investigations. OPM conducts SAC's for agencies that want to obtain single or multiple records checks for use in pre-screening, resolving individual security/suitability issues, or fulfilling other agency mission related objectives. A fingerprint check can be considered a SAC.

### **Posted 16 April 2014**

#### **Guidance to New Industry JPAS Account Holders**

The DMDC Contact Center is unable to process a PSSAR for applicants with no Owning or Servicing relationship in JPAS. When DMDC Contact Center receives a PSSAR for an applicant who is missing the required owning or servicing relationship in JPAS but has met all other requirements, the DMDC Contact Center will send the request to the Facility Clearance Branch (FCB) at the Defense Security Service (DSS), who will then establish a temporary 30-day servicing relationship for the applicant to facilitate creation of their JPAS account. FCB will notify the FSO of the action taken and the facility must establish a servicing or owning relationship with that subject under their own SMO within the 30-day timeframe or the account will be deleted.

For additional information on this topic please see the following [site](#)

### **Posted 14 April 2014**

#### **New Industry Guidance on Submitting Periodic Reinvestigations**

Effective April 10, 2014, the Defense Security Service (DSS), Personnel Security Management Office for Industry (PSMO-I) will accept requests for periodic reinvestigations that are within 90 days of the investigation anniversary date. This is a change from the current 30 day timeframe and reinstates the previous 90 day submission window.

Please see the following site for additional information:

[http://www.dss.mil/psmo-i/indus\\_psmo-i\\_updates.html](http://www.dss.mil/psmo-i/indus_psmo-i_updates.html)

### **Posted 11 April 2014**

#### **Attention NMCI JPAS Users!!!**

Starting on 11 April, some Navy Marine Corps Intranet (NMCI) users have been experiencing DMDC application connectivity issues, to include JPAS. Through feedback from some Navy user populations, it was determined that a recent group policy security update enabled all client machines on that network to support TLS 1.2 encryption protocols. JPAS servers are able to support these configuration changes, but only in certain, more recent browser versions with proper configurations in place. As a result, there have only been three work-arounds identified for NMCI users that have not been able to access JPAS, which include:

1. Disable the TLS 1.2 option under the advanced tab of the internet options dialogue
2. Disable the SSL 2.0 option
3. Upgrade your browser to IE 10 or later

Depending on local IT policy one or both of these options might not be available to the general user population and might require the assistance of an administrator. DMDC is continuing to coordinate with NMCI in order to ensure the impacts of these configurations as well as the solutions are understood.

### **Posted 24 March 2014**

#### **Indoctrination of Non-SCI Access**

With the release of JPAS 5.3.0.0 on 22 March 2014, an enhancement with regards to the minimum required investigations for non-SCI access was implemented. This list of investigations included a National Agency Check (NAC) as not meeting the requirements for access; however, this did not account for Interim Top Secret eligibilities that have a completed NAC and still have an open background investigation. As a result, Security Officers/Facility Security Officers may not be able to indoctrinate a subject into Interim Top Secret access even though a subject has the eligibility. A fix has been identified and will be put into the system on 19 April 2014. In the meantime, a work around has also been identified to ensure those individuals can be indoctrinated into Interim Top Secret. Please contact the DMDC Contact Center at 1-800-467-5526 if the indoctrination link is not appearing.

**Posted 19 March 2014**

**Missed the Talk with the JPAS Team DCO on Tuesday, March 18**

Talk with the JPAS Team DCO occurred on Tuesday, March 18 at 1 pm ET. If you missed the DCO, the PowerPoint presentation will not be distributed but majority of the information that was covered is available at the following locations.

- Information on the upcoming JPAS 5.3.0.0 deployment that will occur on the 22 March 2014 can be found on the [Latest Release Notes](#)
- [March 2014 JPAS Newsletter](#)
- The JPAS Welcome Screen inside the application for the instructions on Initiate an Investigation and How to Add a Person Category
- This page for the Top Reasons Why People Call the DMDC Contact Center and How to Encrypt PII to the DMDC Contact Center

Please continue to check this web page for upcoming Talk with the JPAS Team DCOs.

**March 2014 JPAS Newsletter** is now available [here](#).

**Top Reasons Why Users Call The DMDC Contact Center:**

DMDC has been analyzing the top call reasons JPAS users have been calling into the DMDC Contact Center requesting JPAS assistance on. The following are the top 4 items.

CALL: Can you unlock my account? I did not log off correctly.

ANSWER: The user can wait 15 minutes for the system to log you out automatically, contact your Account Manager or call the DMDC Contact Center.

CALL: What is the status of my PSSAR?

ANSWER: It takes 3-4 business days to process PSSARS on a first come, first serve basis. Please plan accordingly and use the PSSAR guide, Account Management Guide, and Request a JPAS Account checklist to ensure your PSSAR is processed the first time.

**“HOW-TO” TOP CALLS:**

How do I Initiate an Investigation on a Subject? And How do I Add a Person Category on a Subject?

ANSWER: The DMDC Contact Center Customer Service Representative (CSR) can walk a validated JPAS user through the steps. However, DMDC is adding these instructions INSIDE the JPAS application on the Welcome Screen for a limited time. Scroll down on the Welcome page for the instructions as they will be toward the bottom.

**Inactive Account Deletion Policy**

In order to comply with CYBERCOM [TASKORD 13-0641](#), JPAS/SWFT/DCII will be decreasing the inactive account deletion deadline from 90 days to 45. This change will not affect the current 30 day

account lock due to inactivity. Users should remember to login every 30 days to prevent any interruption in access. This enhancement is currently planned to be implemented on 9 March 2014.

The JPAS Account Manager Policy and Policy Updates are being updated to reflect this modification. Please note, only DoD Common Access Card holders will be able to access the original CYBERCOM task order.

### **SWFT and DCII Users**

SWFT and DCII are both enabling their systems for authentication for use with the same PKI credentials that JPAS accepts.

SWFT has already enabled logon and registration with DoD approved PKI certificates, and have removed the option for Username/Password logon as of 14 March 2014. Additional information on the SWFT PK Enablement effort can be found at the following site:

<https://www.dmdc.osd.mil/psawebdocs/docPage.jsp?p=SWFT>

DCII is currently planning to implement PKI for authentication by 31 May 2014 eliminating Username/Password. Additional information on the DCII PK Enablement effort can be found at the following site:

<https://www.dmdc.osd.mil/psawebdocs/docPage.jsp?p=DCII>

If you have additional questions, please contact the DMDC Contact Center.

### **Posted 17 March 2014**

#### **JPAS Data Correction Checklist:**

Ever get frustrated trying to figure out what to do when a subject's PII keeps being overwritten or how to update a subject's PII? The JPAS team created a Step by Step document that will give you instructions on how to update a subject's PII in JPAS or keep it from being overwritten. See the new [JPAS Data Correction Checklist](#).

#### **How to Encrypt PII to the DMDC Contact Center**

Please be aware that the [DMDC Contact Center](#) is able to receive encrypted email and attachments from users. This is useful for individuals attempting to transmit PSSAR requests via the DD Form 2962. Requestors can still submit their forms via secure email, using one of two options:

1. Standard S/MIME email encryption, for which you can find instructions [here](#)
2. Use the AES256 encryption option in WINZIP to password protect your attachments

Additional information on using WINZIP encryption can be found [here](#).

### **Posted 14 March 2014**

#### **DMDC Contact Center Fax Server is Unavailable**

Please be aware that the [DMDC Contact Center](#) is temporarily unable to receive FAX transmissions. This may affect individuals attempting to transmit PSSAR requests via the DD Form 2962. Requestors can still submit their forms via secure email, using one of two options:

3. Standard S/MIME email encryption, for which you can find instructions [here](#)
4. Use the AES256 encryption option in WINZIP to password protect your attachments

Additional information on using WINZIP encryption can be found [here](#).

### **Posted 10 March 2014**

#### **Upcoming JPAS Changes**

JPAS Release 5.3.0.0 will be deployed on 22 March 2014 and will incorporate several changes that will impact users. See the [Latest Release Notes](#) which outlines changes to the application and the associated impacts to users.

#### **Talk with the JPAS Team**

In support of the JPAS 5.3.0.0 release changes the JPAS team will be hosting a virtual meeting for all JPAS users on Tuesday, 18 March starting at 1 PM ET at the following link:

<https://connectcol.dco.dod.mil/jpastalk/>

### **Posted 10 February 2014**

#### **Inactive Account Deletion Policy**

In order to comply with CYBERCOM [TASKORD 13-0641](#), JPAS will be decreasing its inactive account deletion deadline from 90 days to 45. This change will not affect the current 30 day account lock due to inactivity. Users should remember to login every 30 days to prevent any interruption in JPAS access. This enhancement is currently planned to be implemented on 9 March 2014.

The JPAS [Account Manager Policy](#) and [Policy Updates](#) are being updated to reflect this modification. Please note, only DoD Common Access Card holders will be able to access the original CYBERCOM task order.

### **Posted 22 January 2014**

#### **State Laws and Impacts to Federal Security Clearances/Eligibility:**

There has been some inquiry as to recent changes to state laws and the potential effect on federal security clearances. Please note that regardless of state level decriminalization or legalization of schedule 1 narcotic possession or use, it is still a Federal level offense and subject to litigation under the Controlled Substances Act (USC Title 21). Beyond the legal issues, use of controlled substances may have a negative impact on the government's risk model for allowing access to classified materials. SOs/FSOs should report all substance abuse issues via the security incident process.

[Industrial Security Letter \(ISL\) 2006-02](#), also provides guidance on substance abuse reporting for industry.

For additional information on recent state legalization of marijuana and the lack of impact to Federal law, please see the following links:

<http://www.whitehouse.gov/ondcp/state-laws-related-to-marijuana>

<http://www.justice.gov/dea/druginfo/ds.shtml>

### **Posted 14 January 2014**

#### **Personnel Security System Access Request (PSSAR) Form Issues:**

Please note that the prior issues with the DD 2962 on the DTIC site have been resolved. Users should now be able to download and complete the form digitally for submission to the DMDC Contact Center.

### **Posted 6 January 2014**

#### **Personnel Security System Access Request (PSSAR) Form Issues:**

Potential users of JPAS, DCII and SWFT may have difficulty filling out the required DD Form 2962 (PSSAR) as the licenses required to allow the form to be edited in the free Reader version of Adobe Acrobat have temporarily expired. DMDC is currently working with other DoD organizations to restore the functionality to the site that houses the forms.

In the interim, there are two way to work around this issue:

1. Prospective users that have the Standard or Professional versions of Adobe Acrobat can save the file locally and edit it directly in their licensed software versions for normal digital submission to the DMDC Contact Center
2. The DMDC Contact Center is also accepting faxed or scanned copies of the required DD Form 2962, for those individuals that do not have access to Acrobat Standard or Professional. Please see the [Contact Customer Service](#) or [Account Request](#) pages for the required contact information.

Additional information on the DD Forms issue can be found on the [DoD Forms Management Program Site](#).

### **Posted 19 December 2013**

#### **DQI 68982 – Separation of Industry Categories with no Owning/Serviceing SMO:**

In January 2014 the JPAS team is planning to run a Data Quality Initiative (DQI) that will separate Industry person categories that are not Key Management Personnel (KMP). Upon separation, the majority of person records that meet the ownership criteria will be archived due to the fact that their existing separation date is greater then 2 years, a smaller portion will result in orphaned or ghost records due to lack of ownership. FSOs can take action to identify and correct these orphaned accounts in JPAS. Please see the [DQI 68982 presentation](#) under the Data Quality menu to the left of these announcements for further information.

### **Posted 4 December 2013**

#### **NEW! JPAS PSSAR CHECKLIST:**

- If the PSSAR form has any issues, the whole form will be denied even if it is requesting multiple accounts (e.g. JPAS, SWFT).
- All dates must be correct (e.g. cert dates match dates on PSSAR) and dates must be filled out (e.g. date at the top of the form, dates on the signature blocks).
- JAMS and DCII accounts cannot be created for Industry. Do not check any of these boxes as your PSSAR will be denied.
- Review the JPAS Account Management Policy to determine if the LOA and/or List of Duties in Part 5 have the necessary information and are filled out. If it does not, the PSSAR will be denied.
- All 3 certificates must be submitted with the PSSAR for all JPAS accounts.
- You can use the sample PSSAR as a guide but DO NOT SUBMIT the sample PSSAR. It will automatically be denied.
- Read the JPAS Account Management Policy and the Request JPAS Account PRIOR to submitting the PSSAR. As an applicant you must be aware of all the JPAS Account Management policies. The PSSAR can be found at the end of the Request JPAS Account.
- If you use the wrong PSSAR (DD645 DRAFT), it will automatically be denied.

**Posted 2 December 2013**

**Attention Industry Applicants: ISFD File Received.  
Resubmit PSSARS if Rejected Due to Inability to Verify in ISFD.**

DMDC was previously unable to process some of the new Industry JPAS or SWFT accounts due to DMDC not receiving the ISFD file or having the necessary access to ISFD. DMDC was unable to verify pertinent information (e.g. KMP, FSO, Primary, Secondary, Single Person Facility, Level of Facility) to grant a JPAS or SWFT accounts for Industry. DMDC has received the ISFD file from DSS on December 3, 2013. Industry applicants can now resubmit their previously rejected PSSARs, if the PSSAR was rejected for 'Unable to Verify in ISFD.' Please include your ticket number in the resubmission.

**Potential Upcoming JPAS Logon Issues**

At the end of this calendar year, the SHA1 Federal Root CA will be expiring and might be replaced along with the cross certificates that enable trust between the Federal Bridge the DoD Public Key Infrastructure (PKI) and External Certification Authority (ECA) providers. As a result, on 1 January 2014, when accessing the JPAS or other DoD websites, users might receive a warning that the sites they are visiting are "not trusted," this will be due to the fact that the clients are not able to validate the certification path of the DoD server certificates. In order to resolve this problem, please visit the following website and download and run the tool labeled "FBCA Cross Certificate Remover."

[http://iase.disa.mil/pki-pke/function\\_pages/tools.html](http://iase.disa.mil/pki-pke/function_pages/tools.html)

This reissuance may not affect the vast majority of current JPAS users as their local trust stores are more than likely already properly configured for access, but several other organizations, such as other Federal users and potentially some Industry users, might experience some of these connectivity issues. If you experience these issues and run the tool at the link above and still have issues please call the DMDC Contact Center as they can assist in troubleshooting.

**Posted 21 November 2013**

## **Removal of JPAS Accounts**

On 20 November a Data Quality Initiative (DQI) was run to remove JPAS accounts from users that have met the following criteria:

- Denied, revoked, suspended or otherwise unfavorable eligibility
- No owning and/or servicing SMO
- Have an account on a separated category
- An industry consultant category with account management role
- Inactivity (lack of logon) for 90 days

The vast majority of these removals were due to a separated category or lack of a owning or servicing SMO. If you happen to be one of the individuals affected by this initiative, and you still require access to JPAS, please work with your account manager to reinstate your access, ensuring you meet the requirements outlined in our "[Request a JPAS Account](#)" document. Please be aware that this DQI will be re-run on a monthly basis.

## **Upcoming JPAS Changes**

JPAS Release 5.2.0.0 will be deployed on 18 January 2014 and will incorporate several changes that will impact users, including:

- Removal of Collab CAF from JCAVS request screens
- Removal of the option to search records by EDIPI
- Display indoctrination date on SCI and non-SCI access history
- Users will be able to update their profiles at any time and add multiple SMO emails
- Current Eligibility will be included on person summary screens

In support of these changes the JPAS team will be hosting a virtual meeting for all JPAS users on Wednesday, 15 January starting at 2 PM ET at the following link:

<https://connectcol.dco.dod.mil/jpastalk/>

## **Posted 24 October 2013**

### **Resumption of PSI-I Processing**

As of 24OCT, Defense Security Services has resumed processing requests for Personnel Security Investigations for Industry (PSI-I) based upon the date of receipt. If you have submitted a request in the last 30 days and the subject no longer requires the investigation, please post a separation date so the request can be stopped. For additional information please see the [DSS website](#).

## **Posted 23 September 2013**

### **Personnel Security Special Access Request (PSSAR)**

As of 5 September 2013, the new Department of Defense Form (DD Form) 2962 is the official format for requesting a JPAS, DCII or SWFT account. The interim form (DD X645) will no longer be accepted for use on 1 October 2013. Please be sure to use the final approved form to which a link can be found in the "[Request a JPAS Account](#)" section on the JPAS homepage.

## **Posted 18 September 2013**

**DO NOT LOOK UP INDIVIDUAL JPAS RECORDS WITHOUT NEED TO KNOW!**

Looking up high profile individual's personnel security records without a justifiable need to know is considered a misuse of JPAS and will result in account termination. A full audit on users who accessed a high profile record will be conducted in order to determine any potential misuse. Justifications such as "I saw an incident on the news," "The subject may have visited my office," or "The individual might have previously been in my unit," are not considered need to know.

**Posted 12 September 2013**

**ATTENTION ALL JPAS USERS:**

**DO NOT SHARE JPAS ACCOUNTS!**

It is a violation of DoD Regulations to share username/password, any Approved Active Public Key Infrastructure (PKI) Certificate, or allow an individual to access another person's JPAS account in any manner or form. Only the authorized account holder is permitted to access/use his/her account.

Please read the **RED** text on the 'I Agree' page and note that it is wrongful to willingly use another individual's PKI certificate for authentication/logon as the certificate is the digital representation of another person's identity or to access another person's JPAS session. This is considered to be a misuse of technology and will result in a security incident and potentially, **permanent (there is no recourse)** debarment from having a JPAS account.

**Posted 3 September 2013**

**New!!! Resumption of TS PRs for Industry**

After carefully monitoring and managing industry submissions for initial clearance and reinvestigation requests, the Defense Security Service (DSS) has determined that sufficient funding is now available to resume processing deferred Top Secret PRs effective Aug. 28, 2013, for the remainder of the fiscal year. Additional information can be found [here](#).

**PSMNet Timeout Issue Resolution:**

PSMNet reports that took longer than 15 minutes to process were causing a timeout issue for users. As of July 25, a solution was implemented to display a portion of the records, allowing the report to continue processing in the background while the user is able to click through the results pages.

**Posted July 1, 2013**

**New!!! Use of PKI Certificates**

Please note that it is wrongful to willingly use another individual's PKI certificate for authentication/logon to JPAS as the certificate is the digital representation of another person's identity. This is considered to be a misuse of technology and will result in a security incident and potentially, permanent debarment from having a JPAS account.

**New!!! Suspension of TS PRs for Industry**

Defense Security Service (DSS) will suspend the submission of most Top Secret (TS) Periodic Reinvestigations (PR) for cleared industry personnel to the Office of Personnel Management (OPM) effective 14 June, 2013 through 30 September, 2013. Some exemptions apply:

- PRs for contractor personnel who are considered key management personnel
- PRs required for reciprocity or special/priority programs such as:
  - Special Access Programs
  - Personnel Reliability Programs
  - Presidential Support Programs
  - Access to certain SCI supporting the IC

This has no impact on initial submissions for Industry TS clearances. Additional information can be found [here](#).

### **REMINDER!! NO Test or “Dummy” SSNs in JPAS**

JPAS is a DoD System of Record, and therefore inputting test or “dummy” SSNs into the system is a violation of system policies and is STRICTLY prohibited. If you input test SSNs into JPAS, your account will be terminated and a misuse of technology incident will be recorded on your JPAS record.

### **NEW!!! HOT TOPIC: JPAS Printouts**

At “Talk with the JPAS Team” last week, there was a “hot” topic regarding JPAS Printouts. Current policy states that JPAS Printouts cannot be released to “any person or entity” which has been interpreted in various ways. The issue to be clarified is whether or not JPAS Printouts can be used for internal business (e.g. personnel/HR folders). DMDC has brought this issue to USDI and DSS Policy Offices for Industry clarification. Once DMDC has received clarification, we will post it. Until clarification has been received, please continue operating under your as-is internal business processes.

### **NEW! e-Fingerprint Countdown: 6 months left**

By December 31, 2013 all fingerprint images that are provided in support of background investigations must be captured and submitted electronically. Please visit the Secure Web Fingerprint Transmission (SWFT) web pages for more information on this USD(I) mandate at <https://www.dmdc.osd.mil/psawebdocs/docPage.jsp?p=SWFT>.

### **Reminders**

- Industry: FSOs might notice that their subject’s records might be reverting to old data (e.g. old names, incorrect dates of birth). This might be a result of incorrect data on file with the DoD. Please see our [Announcement Archive](#) for instructions for correction.
- JPAS Users are prohibited from looking up subjects of whom they have no need-to-know or authority.
- Industry: If you mistakenly enter an incorrect SSN while initiating an investigation, submit an RRU **before** any action is taken on the record.
- Please make sure your SMOs are set up properly by following the instructions in the [JVS Modifications](#) document in the left-hand navigation of this webpage. All information pertaining to JVS initiatives is located in the [JVS Modifications](#) document.
- JPAS Printouts and SWFT Account Requests – Please note that clearance verification for SWFT accounts is **NOT** a valid use for printing out JPAS person summaries. Do not include these printouts in your SWFT account request and please refer to our [Policy Updates](#) (specifically the 8/10/2012 posting) for more detailed guidance.

- **NEW!** Review JPAS Account Management Policy as DMDC is continuously auditing accounts. Any account user/certificate holder that is violating JPAS Account Policies will permanently lose their account.

**Posted May 10, 2013,**

### **SAR Procedure/Form Changes**

These changes will go into effect 1 June 2013

#### **SAR Procedure Changes:**

- The new System Access Request Form is now referred to as the Personnel Security Systems Access Request (PSSAR) form; tentatively DD Form 645. Please see the [Prospective SAR](#) form in our General Information section.
- DSS SAR 273 is obsolete for JPAS, DCII and SWFT accounts. DSS and DMDC will reject account requests submitted on the DSS SAR 273 after June 1. ISFD access applicants should continue to submit DSS Form 273 to the DoD Security Services Center (DSS).
- Part 2 Box 14, 15, and 16 – Training Required. Information Assurance (IA), Personally Identifiable Information (PII) and JPAS training courses are required for all NEW account JPAS applicants. See the Account Request Checklist for specific courses.
- If the PSSAR is submitted to the DMDC Contact Center for processing, proof of training must be submitted along with the PSSAR. If the PSSAR is submitted to the agency/service/company Account Manager for processing, no training certificates need to be submitted to DMDC; however, these certificates and/or attendee lists will be requested by DMDC in the event of a security incident or an audit.

#### **SAR Form Changes:**

- Part 2 Box 14, 15, and 16 – Training Required
- Part 3 Box 17 – DCII. DCII portion is just formatted differently
- Part 3 Box 18 – SWFT. Additional roles have been added
- Part 3 Box 19-26 – JPAS. JPAS portion is just formatted differently
- Part 4 Applicants Certification – Agreement wording has changed
- Part 5 Nominating Official's Certification – Agreement wording has changed
- Part 5 (right above Box 29 and 30) – User Assigned Duties – This field will replace the separate LOAs for regular user accounts. Account Managers will still need LOAs.
- Part 6 Validating Official's Certification – must be COMPLETED by the request agency. Exception to the change is that it is a single company entity or there is only one in the organization with a JPAS account.

**Posted April 14, 2013:**

### **JPAS Training Requirements**

In response to recent inquiries regarding implementation of new minimum training requirements for new JPAS user account provisioning, the following provides background and justification for these new standards, as well as annual re-certification requirements. These standards are defined in the [JPAS Account Management Policy](#) and new [Account Request Procedures](#).

The following policies place the impetus for maintaining confidentiality, integrity and availability for JPAS. The Designated Accrediting/Approving Authority (DAA) for JPAS is the DMDC Director.

- **DoD Directive 8500.1 Information Assurance and the Computer Security Act of 1987** stipulates that all employees and contractors involved with the management, use or operation of DoD information systems must receive annual information assurance training and training on the use of personally identifiable information.
  - DoD 5220.22-M, February 28, 2006 – Annual refresher training is required to review security principles and responsibilities and to emphasize new security policies and practices developed from the preceding year.
- **ISL 2012-03 May 14, 2012 FSO Training (NISPOM 3-102) NISPOM** paragraph 3-102 requires contractors to ensure facility security officers (FSOs) and other contractor personnel performing security duties complete security training considered appropriate by the Cognizant Security Agency (CSA).
- **NISPOM:**
  - 1-201. Facility Security Officer (FSO) – The FSO, or those otherwise performing security duties, shall complete security training as specified in Chapter 3 and as deemed appropriate by the CSA.
  - 8-101. Responsibilities – The CSA shall establish a line of authority for training, oversight, program review, certification, and accreditation of IS used by contractors for the processing of classified information.
  - 8-102. Designated Accrediting/Approving Authority – The CSA is the DAA responsible for accrediting information systems used to process classified information in industry.
  - 8-103.f.5.i – Ensures that personnel are trained on the Information System’s prescribed security restrictions and safeguards before they are initially allowed to access a system.

**Posted April 14, 2013 Procedures for PII Issues for Industry Subjects:**

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.

Note: Calling the DSO Helpdesk will not resolve any separation dates from previous military/civilian person categories. Individuals will need to contact their previous Personnel Centers, as PDR is a data repository and cannot separate personnel.

**Posted March 25, 2013:**

### **Countdown to electronic fingerprint capture and transmission**

By December 31, 2013 all fingerprint images that are provided in support of background investigations must be captured and submitted electronically.

Please visit <https://www.dmdc.osd.mil/psawebdocs/docPage.jsp?p=SWFT> for more information about this USD(I) mandate and to learn about the Secure Web Fingerprint Transmission (SWFT) system.

**Posted February 14, 2013:**

### **Data Quality Initiative (DQI) 597 - Administratively Debriefs Access**

JPAS has discovered data quality issues with records in JPAS where eligibility does not support the access level. An employee accessing classified information in error is of serious concern. Therefore, Security Officers (SO) and Facility Security Officers (FSO) should **proactively check** their records to ensure only those with proper eligibility have access in JPAS.

**DQI 597 will include DOD Civilians, Military, and Industry and will run 29 March 2013 starting at 4 pm PT / 7 pm ET.**

Following are the scenarios that will be addressed by DQI 597.

- Active access records related to separated/dead person categories with a separation/death date and/or separation/death status code
- Active access records where no owning or servicing SMO is associated with the person category
- Active Access records where Access is not supported by Eligibility
  - Incorporating scenario-based logic for Industry persons and begin removing all Access that isn't properly supported by a current Eligibility.
  - DOD Civilians and Military ran in July and August 2012 and will start running again in March.
  - **No SMO, No Access** – After all Services/Agencies have the ability to supply JPAS with SMO information, will expand DQI to debrief Access on all person categories where there is no SMO relationship

**Notification of Debrief:** JPAS will generate Notifications that will notify the Owning and Servicing SMOs when debriefing Access. It will read "Access has been administratively debriefed by the JPAS Support Office SMO."

### **Posted February 14, 2013: Mandatory Training for JPAS users**

JPAS was requested by our CIO to update our 'I Agree' Disclosure page as soon as possible. Due to the update, the change was not properly communicated to all parties. For this, we apologize for any inconvenience or confusion the update may have caused. As you are aware, DMDC tries to ensure all parties are notified of any modification or change prior to implementation; however, in this case, it did not occur as designed.

In order to assist with the questions being receiving, please see below for guidance:

[1] Cyber Security Awareness and Personally Identifiable Information (PII) training is required. If your agency/service/company is already performing this training internally, no additional training is needed.

[2] If your agency/service/company is not performing this training internally, outside training courses are available. Please see the [JPAS Account Request Document](#) and the [JPAS Account Management Policy](#) for reference.

[3] If you are Industry, the Cyber Security Awareness has two different types of training options - one is DOD and one is Non-DOD. DMDC's recommendation, if not done internally, is the DOD course.

[4] Certificates of completion do not need to be submitted to DMDC for verification. This should be tracked internally. However, starting in March 2013, Cyber Security (IA), PII, and JPAS training certificates will need to be included in all NEW JPAS account request submissions. A new System Access Request Form (SAR) with this requirement will be posted in March 2013.

[5] For more information regarding upcoming releases, please see JPAS Release Notes that get posted approx. 2 weeks prior to deployment.

**Posted: January 11, 2012:**

#### **Internal Audit of non-DoD federal JPAS user accounts**

Non-DoD federal level JPAS users, please be aware that JPAS is conducting an audit of your JPAS accounts. Accounts created under Non-DOD but belong to Industry and DoD will be deleted. A new account can be established under the appropriate person category. In support of this initiative, users of Non-DOD accounts have received an email message requesting two pieces of documentation.

DMDC has received documentation and is now in the process of updating records, accounts, and deleting those accounts that were established incorrectly as a Non-DOD or the requested documentation was not received.

**Posted: December 11, 2012:**

#### **JPAS Account Management Policy Updated for Non-DoD Government Agency Account Issuance**

The JPAS Account Management Policy has been updated with information regarding the issuance of non-DoD Government Agency JPAS accounts. Please refer to section 4.1 in the [JPAS Account Management Policy](#) or the [JPAS Policy Updates](#) documents available in the left-hand navigation bar.

**Posted: December 3, 2012:**

#### **Attention DoD Security Services (Call) Center Customers - Discontinuation of Written Personnel Clearance Eligibility Verifications**

As of 2 Jan 2013, the DoD Security Services (Call) Center no longer provides written personnel clearance eligibility verifications. Inquiries of this nature, which were typically received from a small

number of non-DoD federal government agencies, should be handled/resolved by authorized JPAS users within the requesting agency or use of OPM's Central Verification System (CVS), which contains a data bridge to JPAS for clearance reciprocity purposes.

### **Posted September 12,**

#### **2012: DOD CAF Consolidation:**

The latest release notes outlining specific user impacts are available [here](#).

The schedule for specific CAFs to be consolidated is to be conducted in 5 phases as outlined below in the corresponding JPAS releases. Each release will be accompanied by an application extended outage. All outages are advertised in the Outage Section at the bottom of this page. The following is the schedule for the non-Intel CAF transition to the DOD CAF.

- **23 SEPT, JPAS Release 4.7.0.0** – JS and WHS will transition (completed)
- **27 OCT, JPAS Release 4.7.1.0** – DISCO and DOHA will transition (completed)
- **18 NOV, JPAS Release 4.7.1.1** - Air Force CAF will transition.
- **16 DEC, JPAS Release 4.7.2.1** - Army CCF will transition.
- **27 JAN, JPAS Release 4.7.2.4** - Navy CAF will transition.

### **Posted August 3, 2012:**

#### **ASSISTANCE REQUIRED – Verify SMOs:**

Please make sure your SMOs are set up properly by following the instructions in the [JVS Modifications](#) document in the left-hand navigation of this webpage. If SMOs are not correctly set up with a valid UIC or Cage Code, they will **NOT** be migrated to JVS. All information pertaining to JVS initiatives is located in the [JVS Modifications](#) document.

### **Posted August 9, 2012:**

#### **Clarification Regarding JCAVS Person Summary Screen PRINTOUTS: [Policy No Longer in Effect: Printouts are not authorized]**

~~Military, DoD and non-DoD Civilian Users: JCAVS Person Summary Screen printouts can only be utilized when a Federal Government Agency requests the printout for reciprocity or compliance purposes, and JPAS access is unavailable at that agency. JCAVS Person Summary Screens cannot be utilized for law enforcement or Privacy Act purposes. This screen printout can only be used to provide proof of investigation, eligibility, and access at the single point in time of the request by the Federal Government Agency.~~

~~Industry Users: The guidance to military, DoD and non-DoD civilian JPAS users does not apply to National Industrial Security Program (NISP) JPAS industry users regarding JCAVS Person Summary Screen Printouts. Industry users should continue to follow current National Industrial Security Program Operating Manual (NISPOM) and Industrial Security Letters (ISL) guidance. Contact Defense Security Service with any questions. All ISLs are located here (<http://www.dss.mil/isp/industrial-security-letters.html>). The NISPOM is located here (<http://www.dss.mil/documents/odaa/nispom2006-5220.pdf>).~~

~~ALL JCAVS PRINTOUTS must be protected from unauthorized disclosure. If a Federal Government Agency requests a printout for reciprocity or compliance purposes and JPAS access is unavailable at that agency, the record must be protected with a DD Form 2923, Privacy Act Data Cover Sheet, according to the requirements for privacy/sensitive information and For Official Use Only (FOUO), Privacy Act of 1974, and DoD Privacy Program (DoD 5400.11-R).~~

~~All Privacy Act requests must be made according to the JPAS SoRN Record Access procedures. All law enforcement requests used for investigations must be forwarded to DMDC and printouts cannot be utilized. The JPAS SoRN is located at:  
<http://dpclo.defense.gov/privacy/SORNS/dod/DMDC12.html>.~~

### **Posted March 5, 2012:**

#### **Last Name or Date of Birth (DOB) Issues for Industry:**

Industry FSOs need to monitor their employees' records to ensure that names and/or DOBs are not updated with outdated information from PDR. 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). If a name and/or DOB updates with incorrect information, the person whose record is affected needs to officially, correct the name and/or DOB in PDR. The FSO will need to update the person's record in JPAS after the correction has been made in PDR. PDR requires official documentation (e.g. passport, birth certificate, SSN card, marriage certificate) to update a person's record.

\*Note\* Calling the DMDC Support Office Helpdesk will not resolve any separation dates from previous military/civilian person categories. Individuals will need to contact their previous Personnel Centers, as PDR is a data repository and cannot separate personnel.

If you have a DoD affiliation (Military, CAC holder, Retiree, Civilian, etc), there are many ways to update your record.

- Visit a local ID card office to add/remove family members. Call first to verify business hours or to set up an appointment.
- Sign in and update your addresses, e-mail address, and phone numbers online with milConnect.
- Call 1-800-538-9552 to update your information. (TTY/TDD: 1-866-363-2883)
- If you do not have any DoD affiliation, you may work through your FSO and DISCO to resolve the data issue. To efficiently track this information please find the Industry PII Spreadsheet located [here](#), and fax in the necessary information to (301) 833-3912 or email (DISCO.PMO@dss.mil) attention Planning Office.

#### **FOR OFFICIAL USE ONLY (FOUO)**

In accordance with DoD Regulations and the Privacy Act of 1974, you must safeguard personnel information retrieved through this system. DoD Regulations are: 5 USC 301 - Departmental Regulations, DoD 5200.1-R - The Information Security Program, Title 5, United States Code, Section 552a Public Law 93-579 (Privacy Act of 1974), DoD Directive 5400.07 - The Freedom of Information Act (FOIA) Program, DoDD 5400.11-R - DoD Privacy Program, and DTM-04-009 Security Classification Marking Instructions.