

# JPAS Policy Guidance

---

*Last updated 2/12/2013*

Please check this document frequently for new JPAS policies, guidance, and clarifications.

## 2/12/2013 Mandatory Training for JPAS users

As of January 19th 2013, the JPAS disclosure agreement has been modified to include an assertion that the user has “completed the necessary training with regards to Security Awareness and safe-guarding Personally Identifiable Information.” These training courses specifically refer to the following programs:

- CyberAwareness Challenge/Organizational security training (2 Options):
  1. <http://iase.disa.mil/eta/cyberchallenge/launchPage.htm>
  2. This includes any organization (service/company/agency) security training the subject may be required to take, such as annual NISP mandatory security training

**Note:** If you are an Industry user, 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. To access the Cyber Awareness Challenge, use this [DoD Cyber Awareness Challenge](#) link and select the training titled “Department of Defense Employees.”

- Personally Identifiable Information (2 options):
  1. [http://iase.disa.mil/eta/pii/pii\\_module/pii\\_module/index.html](http://iase.disa.mil/eta/pii/pii_module/pii_module/index.html) or,
  2. <http://www.dss.mil/cdse/catalog/elearning/DS-IF101.html> (Provided you have a STEPP account)

**Note:** To access the PII training, an industry user may select either one of these two links: [Defense Information Systems Agency \(DISA\) PII training](#) or, [Defense Security Service \(DSS\) PII training](#). If an industry user chooses to take the DSS PII training, a Security Training, Education and Professionalization Portal (STEPP) account is required. The “Sign up” link on the DSS PII training webpage provide instructions for current STEPP users and instructions for new users who will require a STEPP account to complete the DSS PII training.

**Note:** 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. If your agency/service/company is not performing this training internally, the training courses to complete this requirement are listed above. **Certificates of completion do not need to be submitted to DMDC for verification. This should be tracked internally.**

Starting in March 2013, once the new PSSAR form is implemented, new JPAS account requests will need to include proof of completion for these courses. For existing account holders, it is recommended that these certificates (or attendance lists) are maintained at an individual or service/company/agency level

on an annual basis. Please note DMDC will not maintain these certificates of completion beyond the new account request procedure; it is up to the individual/organization to maintain proof of their annual training requirement as it will be requested in the event of a security incident or an audit.

### **11/29/2012 Issuance of non-DoD Government Agency JPAS Accounts**

JPAS accounts for non-DoD government agencies are issued by exception. If a non-DoD government agency requests a JPAS account, the agency must have a National Industrial Security Program (NISP) agreement with the Department of Defense for industrial security services. In addition, the non-DoD government agency must formally explain why using the Office of Personnel Management's (OPM) Central Verification System (CVS) database to verify contract clearance information will not meet the needs of the agency, and explicitly state why a JPAS account is necessary. The agencies that have existing agreements with the DoD for industrial security services are listed in the National Industrial Security Program Operating Manual (NISPOM), paragraph 1-103b, and do not include sub-agencies. Lastly, the agencies must follow DMDC policy regarding the management of the account and adhere to the mandatory re-verification of individuals' eligibility requirements on an annual basis.

### **8/10/2012 JCAVS Person Summary Screen PRINTOUTS**

**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/fac\\_clear/download\\_nispom.html](http://www.dss.mil/isp/fac_clear/download_nispom.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>.

## **8/8/2012 Out of Scope Investigations and New JPAS Account Requests**

1. If a person's investigation is out of scope and they have no access, a request to create a new JPAS account will be denied.
2. If a person's investigation is ongoing and they have access, a request to create a new JPAS account will be approved

## **8/1/2012 Change to Industry Periodic Reviews (PR)s:**

The Defense Industrial Security Clearance Office (DISCO) will only accept requests for periodic reinvestigations that are within 90 days of the investigation anniversary date. This is a change from the previous six-month (180 Day) timeframe. The reduced time frame is consistent with improved Industry security clearance investigation/adjudication times. Periodic Reinvestigation requests already initiated at DISCO will continue to be processed as appropriate. JPAS will not change.

[http://www.dss.mil/disco/indus\\_disco\\_updates.html](http://www.dss.mil/disco/indus_disco_updates.html)

## **4/13/2012 Letter of Appointment (LOA) Required for All New JPAS Account Requests (with the exception of Military)**

LOA is required for all users (with exception of Military) to justify the account creation and keep awareness of who is accessing JPAS within each company or agency. Users whose accounts were created prior to this date are grandfathered-in under this policy.