

Defense Manpower Data Center

Personnel Security & Assurance



Joint Personnel Adjudication System (JPAS) Account Management Policy

Document Version 7.21

12/23/2016



Table of Contents

1 PURPOSE..... 3

2 BACKGROUND 3

3 ORGANIZATION ROLES AND RESPONSIBILITIES..... 3

 3.1 JPAS Account Manager 3

 3.2 DMDC Contact Center..... 3

 3.3 Distributed Account Management Process 3

 3.4 Technical Support and Training..... 4

 3.5 Account Management Support..... 4

4 ACCOUNT LIFECYCLE..... 4

 4.1 JPAS Account Requirements 4

 4.1.1 Personnel Security System Access Request Form..... 5

 4.1.2 Letter of Appointment..... 6

 4.1.3 Mandatory Training Courses 7

 4.2 Appointment of Top Hierarchical Account Managers 8

 4.3 JCAVS Account Activation and Termination..... 8

 4.4 JAMS Account Activation and Termination..... 9

 4.5 Account Transfer Between Organizations/Companies 9

 4.6 Unexpected Loss of an Account Manager 9

 4.7 JPAS Accounts for Contractors Working at Government Agencies..... 9

5 SECURITY 9

 5.1 System Data..... 9

 5.2 Privacy Act..... 9

 5.3 Security Banner 10

 5.4 Password/PIN Management 12

 5.5 User IDs..... 13

 5.6 Account Activity 13

 5.7 Locked Accounts..... 13

 5.8 Misuse of JPAS 13

ACRONYMS 14

APPENDIX A: PROCEDURES GOVERNING USE OF JPAS BY CLEARED CONTRACTORS 15



1 PURPOSE

This policy outlines account management guidance for the Department of Defense (DoD) Joint Personnel Adjudication System (JPAS). This policy is maintained by the JPAS Program Management Office (PMO) and shall be reviewed at least annually.

2 BACKGROUND

JPAS is the DoD System of Record for personnel security. JPAS is the master repository and centralized processing tool that provides the capability to perform comprehensive personnel security management of all DoD employees, military personnel, civilians and DoD contractors. JPAS contains personally identifiable information (PII) as well as sensitive information such as security clearance levels and the status of investigations.

JPAS consists of two sub-applications. The Joint Clearance Access and Verification System (JCAVS), and the Joint Adjudication Management System (JAMS) provide access to data contained in the JPAS database. JCAVS is designed to provide an interface for the security personnel community and JAMS is designed to provide an interface for DoD adjudicator personnel.

3 ORGANIZATION ROLES AND RESPONSIBILITIES

3.1 JPAS Program Manager

The JPAS Program Management Office (PMO) is responsible for the formulation of JPAS account management policy, the enforcement of that policy, and the account administration of the top hierarchical primary and alternate Account Managers (AM) for the Services, DoD Agencies, and DoD Contractors. The Services, DoD Agencies, and DoD Contractors are responsible for the administration and maintenance of JPAS accounts within their Security Management Office (SMO).

3.2 DMDC Contact Center

The DMDC Contact Center provides technical support to all users but only provides account management support to the primary AM for DoD Contractors. Issues or concerns that require the attention of the JPAS Program Manager should be submitted to the DMDC Contact Center.

3.3 Account Management

The function of Account Management is to extend the administration and management of JPAS user accounts across the Services, DoD Agencies, and DoD Contractors. AMs are authorized to manage all applicable JPAS user accounts within their respective SMO. This includes maintaining appropriate paperwork (see section 4.1 below) and providing account management support to their users as set forth in this policy and guidance from the JPAS PMO. Top hierarchical AMs may establish organizational policies to supplement this document; however, those policies may not conflict with this policy document or guidance from the JPAS PMO.

The AM shall be required to provide account management support to the tenant users as set forth in this policy. AMs shall follow any additional guidelines set by their organization for the courtesy management of another organization's account while adhering to any guidance provided by the JPAS PM – if the request is approved. An AM is not allowed to manage his or her individual JPAS account. Account managers shall not setup accounts or manage



accounts for any SMO outside their own or for organizations outside of the DoD. All AM must have an active person category for each SMO with which they are associated.

3.4 Technical Support and Training

JPAS Technical Support is defined as customer support needed to resolve issues concerning user browser configuration, JPAS accessibility via the Internet, and JPAS system malfunctions. Customer support for these Public Key Infrastructure technical issues shall be provided primarily via the [JPAS PKI Technical Troubleshooting Guide](#), available on the DMDC JPAS webpages. Users may be required to contact their local area communications or network support for issue resolution. All JPAS users are authorized to contact the DMDC Contact Center for further technical support requiring immediate resolution due to mission requirements for the aforementioned technical issues.

JPAS instructor led and computer based training is available through the Defense Security Service Center for Development of Security Excellence (CDSE) <http://www.dss.mil/seta/index.html> Specific Security Training, Education and Professionalization Portal (STEPP) courses are:

- **JCAVS User Level 7 & 8:** PS181.16
<http://www.cdse.edu/catalog/elearning/PS181.html>
- **JCAVS User Level 10:** PS182.16
<http://www.cdse.edu/catalog/elearning/PS182.html>
- **JCAVS User Levels 2 thru 6:** PS183.16
<http://www.cdse.edu/catalog/elearning/PS183.html>
- **Personnel Security Management**, STEPP course PS212.01:
<http://www.cdse.catalog/classroom/PS212.html> (live classroom)

3.5 Account Management Support

JPAS Account Management Support is defined as customer support needed to resolve issues concerning account maintenance, e.g., resetting passwords, locking or unlocking accounts, for the primary and alternate AMs within Unified Commands, DoD Agencies, Industry, and Other Organizations. Only authorized JPAS users may contact the DMDC Contact Center directly for account management support. Military Service, DoD Agency and DoD Contractors familiarize keep themselves updated with all documentation posted on the DMDC JPAS website in order to provide adequate support for their SMO.

4 ACCOUNT LIFECYCLE

4.1 JPAS Account Requirements

Each individual accessing JPAS must have a separate and unique account created by the individual's SMO AM. Account managers may only create user accounts for individuals within their own SMO/Organization. Each user must have an active person category for each SMO they're associated with. The account manager must maintain a current record of every JPAS account established. Office accounts are not permitted. Each JPAS account will correspond to a single user who is responsible for all actions taken using that account. Note that JCAVS and JAMS accounts cannot be simultaneously assigned to the same social security number.



Access to the JPAS application shall be granted only if necessary to complete an individual's job duties. In order to receive a JPAS account, a potential user must have a favorable security clearance eligibility determination. In JCAVS, Levels 4, 5, 6, and 7, require an Interim Secret eligibility. JCAVS levels, 2, 3 and 8 require a TS SCI. JAMS access requires at minimum a favorably adjudicated SSBI with a Top Secret eligibility. JPAS users who do not meet security clearance requirements cannot be assigned an account. Additionally, eligibility cannot be out of scope (i.e., must be current) unless potential users have submitted all required paperwork for a reinvestigation or their security manager confirms the out of scope status is due to deployment and authorizes the account. If a new JPAS account request is submitted for a person with an ongoing investigation and they already have access (to sensitive information), or have an interim clearance, their JPAS account request will be approved. Access to JPAS will be suspended for any of the following clearance eligibilities: "Pending Reply to Statement of Reasons," "Denied," "No Determination Made," "Revoked," "Loss of Jurisdiction," or "Action Pending."

Access to JPAS is authorized via means of contractor-issued (for contractors) or government-owned equipment (for government personnel and authorized contractors) with appropriate security controls in place. JPAS users may not access their accounts from personal or home computers or over unsecured wireless networks. Sharing user names and passwords or PK-logon credentials is prohibited and will result in termination of the offender's JPAS account. Additionally, a misuse of technology incident will be recorded on the offender's JPAS record. If you are part of a contract, your contracting office will be notified of the security incident.

Military Service, DoD Agency, and DoD Contractor AMs will create JCAVS accounts for their users and provide account management to those accounts. Accounts shall not be created for personnel outside your company. A description of JCAVS user levels and user security clearance requirements can be found in the [JPAS General FAQs](#) document, question 3, posted on the DMDC JPAS home page.

Non-DoD/Other Federal Government agencies should utilize the Office of Personnel Management (OPM) Central Verification System (CVS) for personnel clearance eligibility verifications. OPM CVS contains information on background investigations, credentialing determinations, suitability determinations, and security clearances. OPM CVS contains a data bridge to JPAS for clearance reciprocity purposes. Questions for access to OPM CVS should be directed to OPM.

4.1.1 Personnel Security System Access Request Form

The Personnel Security System Access Request (PSSAR) Form (link located inside the [JPAS Account Request Procedures](#) document on the JPAS homepage) is used to collect information required to grant an account in the JPAS system, to formally document the account request, and to provide accountability for the account. PSSARs are also used to request account deletions and to make changes to user levels, roles, and permissions.

PSSARs shall be completed and filed for all Military Service, DoD Agency, and DoD Contractors account managers and users of the JPAS system. PSSARs shall have the signature of the individual requesting an account, the signature of the nominating official,



and signature of the validating official before account access is granted. The nominating official CANNOT be the same as the requestor.

PSSARs must remain on file at the agency/military service/industry company until final disposition. This includes the initial PSSAR activating an account plus any subsequent PSSARs submitted to change user levels, roles, and permissions. In circumstances where the account was created or modified by the DMDC Contact Center, the PSSAR must still be retained by the industry company.

PSSARs must be deleted/destroyed when no longer needed for administrative, legal, audit or other operational purposes (but not before the account termination) per OSD, Records & Information Management Program, File Number 1606-06.2 (GRS 24, Item 6b).

Industry Users - Review ISL 04/02 for additional requirements to obtain JPAS Industry accounts and Appendix A: Procedures Governing Use of JPAS by Cleared Contractors for additional information related to contractors' use of JPAS.

4.1.2 Letter of Appointment

In addition to the PSSAR form, a Letter of Appointment (LOA) is required for all account managers (Industry, DoD Agency, Non-DoD Government Agency and Military). LOAs are not required for user accounts.

The LOA should be on your agency/company's letterhead and should indicate the name of the applicant and the specific job duties that require JPAS access. Simply stating "to do my job" is insufficient justification for a JPAS account. Letters will include applicant full names, social security numbers, and contact information (i.e., commercial and DSN work telephones, office addresses, and work email addresses).

Your Agency's Director (or delegate), Corporate Officer, or Key Management Personnel (KMP) listed in the Industrial Security Facilities Database (ISFD) must sign the letter. The authorization signature on the LOA shall be the same as the authorization signature on the PSSAR form. Agency delegates must be GS-14 grade (or agency equivalent) or higher. Include contact information for the Agency Director (or delegate), Corporate Officer, or KMP making the request (i.e., commercial and DSN work telephones, and office address).

LOAs must remain on file at the agency/military service/industry company until final disposition. This includes the initial LOA activating an account manager account, plus any subsequent LOAs submitted to change a normal user role up to an account manager role. A LOA is not required if adding standard user roles (for instance, a JCAVS user going from a level 10 to a level 6). In circumstances where the account was created or modified by the DMDC Contact Center, the LOA must still be retained by the industry company.

LOAs must be deleted/destroyed when no longer needed for administrative, legal, audit or other operational purposes (but not before the account termination) per OSD, Records & Information Management Program, File Number 1606-06.2 (GRS 24, Item 6b).



4.1.3 Mandatory Training Courses

As of January 19th 2013, the JPAS disclosure agreement has been modified to include an acknowledgement 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/Security Training (2 options):
 - <http://iatraining.disa.mil/eta/cyberchallenge/launchpage.htm>
 - Organization (service/company/agency) security training the subject may be required to take, such as annual NISP mandatory security training
- Personally Identifiable Information (PII) Training (3 options):
 - <http://iatraining.disa.mil/eta/piiv2/launchPage.htm>
 - <http://www.cdse.edu/catalog/elearning/DS-IF101.html>
 - Approved existing corporate PII training courses

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.

Note: Now that the Contact Center has transitioned to DMDC, all new or modified account requests (to include account recreation after deletion due to inactivity) will need to include proof of completion for these courses in addition to PSSAR and LOA requirements. For existing account holders, it is recommended that 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 annual training requirement as it will be requested in the event of a security incident or an audit. Additionally, for new accounts created by the DMDC Contact Center, the requestor must include certificates of completion for JPAS-specific courses offered by the STEPP program; this includes accounts for individuals who previously had accounts deleted due to inactivity. These are listed in our [Account Request Procedures](#) document, or refer to section 3.4 Technical Support and Training of this document. For new account requests, the JPAS training must have been completed within the last year. For existing users, provided the applicant has a current verifiable account and has taken an employment opportunity at another secure facility/company, JPAS training verification is not required for the modification of an account. There is no annual recertification requirement for JPAS training.

4.2 Appointment of Top Hierarchical Account Managers

Military Services, DoD Agencies, and DoD Contractors shall appoint their primary and alternate AMs and provide written verification of those appointments to the JPAS PMO. Documentation will include an Appointment Letter, on organizational letterhead, signed by the organization's Head, Commander, Director, or delegate or KMP, naming their top hierarchical primary and alternate AMs. The Appointment Letter may also be used to request removal/deletion of any current top hierarchical primary and alternate AMs the Military Services, DoD Agencies, and DoD Contractors wishes to remove from the position. Letters will include AM full names, social security numbers, and contact information (i.e., commercial and DSN work telephones, office addresses, and work email addresses). Letters will also include contact information for the organizational Head, Commander, Director, or designee or KMP making the request (i.e., commercial and DSN work telephones, and office address).

For primary and alternate AMs, an Appointment Letter shall be submitted with the applicable PSSAR requesting account activation, account deletion, or changes to user levels and permissions. The authorization signature on the PSSAR shall be the same as the authorization signature on the Appointment Letter. The JPAS AM shall establish and manage accounts for AMs and maintain the accounts, PSSARs, Appointment Letters and training certificates. Military Services, DoD Agencies, and DoD Contractors are responsible for sending the JPAS AM a PSSAR form requesting an account deletion when primary and alternate account managers no longer require access to JPAS.

4.3 JCAVS Account Activation and Termination

Top hierarchical AMs are authorized to establish and manage JCAVS user accounts only within their own respective SMO/Organization when there is an active person category associated with the SMO in JPAS. This includes maintaining appropriate paperwork and providing account management support to their JCAVS users as set forth in this policy. Top hierarchical AMs may establish organizational policies to supplement this document. A PSSAR and appropriate training certificates shall be completed and filed for each JCAVS system user. The PSSAR shall annotate the applicable account activation, deletion, or changes to user levels and permissions. Military Service, Unified Command, DoD Agency, Industry, and Other Organizational JCAVS users shall adhere to any additional account management policy requirements set forth by their organization.



4.4 JAMS Account Activation and Termination

PSSARs and training certificates for Central Adjudication Facility (CAF) adjudicators shall be submitted to their respective CAF AM who shall establish and manage their associated JAMS accounts and maintain these documents.

A PSSAR and training certificates shall be completed and filed for each JAMS system user. The PSSAR shall annotate the account activation, deletion, and any changes to user roles and permissions. JAMS users shall adhere to any additional account management policy requirements set forth by their CAF.

4.5 Account Transfer Between Organizations/Companies

JPAS accounts shall NOT be transferred between organizations/companies. If a user or AM leaves an organization/company, the associated account in JPAS must be deleted by the owning organization/company. If JPAS access is required at the new organization/company, a new JPAS account shall be created by the gaining organization/company.

4.6 Unexpected Loss of an Account Manager

Account managers may be unable to manage an account for a variety of reasons, e.g., job change, death, major illness, etc. Establishing contingency responses to the loss of AMs is the responsibility of each Military Services, DoD Agencies, and DoD Contractors. Each Military Services, DoD Agencies, and DoD Contractors must have a primary and alternate account manager.

4.7 JPAS Accounts for Contractors Working at Government Agencies

Accounts for contractors who perform personnel security management functions such as Information Security Program Manager, Special Security Officer, Special Security Representative, etc., on behalf of a Military Department (MILDEP) or DoD Agency are the responsibility of the hiring MILDEP or DoD Agency. This responsibility includes the immediate termination of an individual's JPAS account in the event of a personnel security action such as suspension, revocation, or denial of the access or clearance.

If a punitive personnel action is reported in JPAS and the user's account is not terminated, it could result in restrictions placed on the permissions of the MILDEP or DoD Agency responsible for the contractor account.

5 SECURITY

5.1 System Data

Contents of the JPAS system are subject to the Privacy Act of 1974. Under the Privacy Act of 1974, personnel information retrieved through JPAS must be safeguarded. Disclosure of information is in IAW instructions as noted on the security banner associated with the JPAS system.

5.2 Privacy Act

The Joint Clearance and Access Verification System (JCAVS) within JPAS is intended for use by security managers/security officers to update other JCAVS users with pertinent personnel security clearance access information in order to ensure the reciprocal acceptance of clearances throughout DoD.



Its intended use, according to policy, does not include giving out the JCAVS records to the subject of record for their personal use without a proper Privacy Act request or authorization from the record owner.

JCAVS contains not only clearance eligibility information but also Investigative Summary and Adjudication Summary information as well as Incident Reports, some of which may have originated with a third agency requiring their review/comments before a disclosure is made. Therefore, DMDC does not authorize the direct disclosure of JCAVS records by a security manager to the Subject of record. Service schools requiring clearance verification can either request JCAVS access themselves or have the user agency provide the subject's clearance verification.

5.3 Security Banner

ATTENTION ALL JPAS USERS

By clicking the "Agree" consent box on this page, users are consenting to the terms of use of the application and agree to comply with the Privacy Act of 1974, applicable DoD regulations, other applicable laws, and JPAS policies to include the forfeiture of JPAS access if terms of use are violated. Violation of these regulations, laws, and/or the Account Management Policy can constitute a misuse of JPAS that could result in termination of the JPAS account(s), documentation of the incident on the JPAS record, and may include disallowing the subject(s), organization, and/or company from future access to JPAS or future personnel security systems. Accounts remain locked for an indeterminate length of time during administrative reviews preceding a final decision.

As a reminder, it is a violation of DoD regulations to share authentication mechanisms including any username/password or any approved Public Key Infrastructure (PKI) certificate. JPAS accounts are only provisioned for authorized individuals, as a result, there is no such thing as a "company" or shared account. Only the authorized account holder is permitted to view/access/use the JPAS account via a subject's individually issued PKI credential.

Any authorized/unauthorized user(s) and/or company/organization found in violation of the Privacy Act of 1974, applicable DoD regulations, other applicable laws, and JPAS policies will risk immediate forfeiture and TERMINATION of their JPAS and future personnel security systems' account(s), regardless of any access requirements that may exist to support mission-critical and job-essential tasks.

DATA YOU ARE ABOUT TO ACCESS COULD POTENTIALLY BE PROTECTED BY THE PRIVACY ACT OF 1974. You must:

- Have completed the necessary training with regards to Security Awareness and safeguarding Personally Identifiable Information.
- Ensure that data is not posted, stored or available in any way for uncontrolled access on any media.
- Ensure that data is protected at all times as required by the Privacy Act of 1974 (5 USC 552a(I)(3)) as amended and other applicable DOD regulatory and statutory authority; data will not be shared with offshore contractors; data from the application, or any information derived from the application, shall not be published, disclosed, released,



revealed, shown, sold, rented, leased or loaned to anyone outside of the performance of official duties without prior DMDC approval.

- Delete or destroy data from downloaded reports upon completion of the requirement for their use on individual projects.
- Ensure data will not be used for marketing purposes.
- Ensure distribution of data from a DMDC application is restricted to those with a need-to-know. In no case shall data be shared with persons or entities that do not provide documented proof of a need-to-know.
- Be aware that criminal penalties under section 1106(a) of the Social Security Act (42 USC 1306(a)), including possible imprisonment, may apply with respect to any disclosure of information in the application(s) that is inconsistent with the terms of application access. The user further acknowledges that criminal penalties under the Privacy Act (5 USC 552a(I)(3)) may apply if it is determined that the user has knowingly and willfully obtained access to the application(s) under false pretenses.
- The U.S. Department of Defense is committed to making its electronic and information technologies accessible to individuals with disabilities in accordance with [Section 508 of the Rehabilitation Act \(29 U.S.C. § 794d\)](#), as amended in 1999. Send feedback or concerns related to the accessibility of this website to: DoDSection508@osd.mil. For more information about Section 508, please visit the [DoD Section 508 website](#).

UNDER THE PRIVACY ACT OF 1974, YOU MUST SAFEGUARD PERSONNEL INFORMATION RETRIEVED THROUGH THIS SYSTEM.

DOD NOTICE AND CONSENT BANNER

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.
- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.



5.4 Password/PIN Management

A JPAS password shall be randomly generated by the system and provided to the account manager at the time an account is created or a password change is forced. The account manager shall relay, via encrypted email, the randomly generated password to the user.

This password should be used to self-register non-CAC certificates to the user's JPAS account. The user will have to remember their username and password in order to self-register their non-CAC certificates. After registering certificates using your username and password, you will not be required to change your password. Note – you will need to register your certificates each time you get new certificates, or when switching between different certificates for the same user.

The JPAS system will lock a user ID after three consecutive failed attempts at the self-registration screen. JPAS user accounts can be unlocked only by the associated JPAS AMs.

The JPAS PM and DMDC Contact Center can force password changes for account managers within JPAS. JCAVS and JAMS AMs can force password changes within JPAS for their organization's users.

PINs are 6 digit numeric codes associated with your PK credentials and are managed differently depending on the specific type of credential used:

- For a DoD CAC, you have 3 attempts to enter a correct PIN. If you fail on the 3rd attempt, your credential will be locked. In order to unlock your credentials, you will need to visit a DEERS/RAPIDS station to unlock and subsequently use.
- For a Federal PIV, contact the issuer of the PIV for their reset policies.
- For ECA and other DoD approved PKI credentials, this process can vary from issuer to issuer. Note: some issuers do not conduct a PIN/Password reset and will require the purchase of a separate credential. Please be forewarned and ask the vendor's SOP prior to purchase.

Never share JPAS user names, passwords, PK certificates, PINs, or other authentication information with any other individual, including someone who is a designee or an alternate to the account holder. JPAS does not have “company accounts.” Sharing user names and passwords is prohibited and doing so will result in the termination of the account. In addition, a technology incident will be recorded on the offender's JPAS record.

Violations of procedures will lead to the termination of the JPAS account, or exclude culpable companies or persons from access to JPAS for a specified or indefinite period. Information concerning violations of these procedures may also be referred to other federal agencies for consideration of administrative, civil, or criminal sanctions when circumstances warrant.

If the company with the security violation has a requirement that JPAS access is needed, DMDC will reinstate a JPAS account to an individual associated with that company, but not to the individuals who have violated DoD Regulations. DMDC requires a written request from your company's Government Sponsor on their associated letterhead. The written request will include an acknowledgement that the Government Sponsor is aware a JPAS



security violation has occurred with this company and will request JPAS access to be given to another individual in order to support mission-critical and job-essential tasks. Once DMDC has received all the requested information, JPAS access can be granted.

5.5 User IDs

JPAS User IDs are systematically generated at account creation and are unique to individuals. Group login accounts and the sharing of User IDs are prohibited.

5.6 Account Activity

An active JPAS account is one that has been logged into within the past 30 days. An inactive JPAS account is an account that has not been logged into in over 30 days. If a JPAS account is inactive—i.e., not successfully accessed—for more than 30 days, the JPAS system shall automatically lock the account. The AM managing the account will be able to unlock the account, unless the account exceeds 45 days of inactivity. JPAS accounts that have not been logged into for longer than 45 days are deleted per DoD Regulations (CYBERCOM TASKORD 13-0641). If an account is needed, a new account will have to be established following the aforementioned guidelines.

5.7 Locked Accounts

Account managers may only unlock accounts for users within their SMO. Do not unlock accounts that have been locked by an Administrator unless you have permission from the locking Administrator.

Contacts

Name	Contact Information
DMDC Contact Center	1 (800) 467-5526 E-mail: dmdc.contactcenter@mail.mil

5.8 Misuse of JPAS

By clicking the “I Agree” consent box on the DoD Security Banner page in the JPAS application, users are consenting to the terms of use of the application and agree to comply with the Privacy Act of 1974, applicable DoD regulations, other applicable laws, and JPAS policies to include the forfeiture of JPAS access if terms of use are violated. Violation of these regulations, laws, and/or the Account Management Policy may constitute a misuse of JPAS that could result in termination of user(s) JPAS account(s), documentation of the incident on the JPAS record of the violator(s), and may include disallowing the subject(s), organization, and/or company from future access to JPAS or other personnel security systems, regardless of any access requirements that may exist to support mission-critical and job-essential tasks. Preceding a final outcome determination, JPAS accounts are locked for an indeterminate length of time during administrative reviews.

As a reminder, it is a violation of DoD regulations to share authentication mechanisms including any username/password or any approved Public Key Infrastructure (PKI) certificate. JPAS accounts are only provisioned for authorized individuals, as a result, there is no such thing as a "company" or shared account. Only the authorized account holder is permitted to view/access/use the JPAS account via a subject's individually issued PKI credential.



Misuses of JPAS include, but are not limited to:

- Sharing of username, password, CAC, or PIV cards and/or associated PIN numbers to access the system.
- Allowing non-cleared/unauthorized individuals to access the system.
- Leaving the JPAS application unsecure while logged in.
- Allowing others to view data on the JPAS screen that do not have the proper authorization.
- Printing or taking a screenshot of JPAS data.
- Querying the JPAS application for ‘celebrity’ records.
- Querying the JPAS application for your own record.
- Entering test or “dummy” SSNs into JPAS.
- Knowingly entering false or inaccurate information into the system.
- Initiating investigations for subjects who you have no owning/servicing relationship, or are otherwise not appropriately sponsored for a clearance.
- Taking any action on your own record (e.g., submitting visit requests, attempting to indoctrinate, establish an owning/servicing relationship of yourself, etc.)
- Querying the JPAS application for information or records you have no need to know and/or authority to view to conduct your official duties.
- Querying the JPAS application for records or persons no longer affiliated with your Security Management Office or the Department of Defense.

DMDC as the System Manager (SM), Program Manager (PM), and Authorizing Official (AO), has the responsibility and ability to make determinations regarding system access, especially when a misuse of the system has occurred that may require an adjudicative determination. This responsibility and authorization for DMDC to make risk-based authorization decisions is stated in the [DoDI 8500.01](#) Enclosure 3: Procedures, Section 2: Risk Management, (3)(b).

(b) Information protection requirements are satisfied by the selection and implementation of appropriate security controls in Reference (cj). Security controls are implemented at Tier 3 by common control providers, system managers (SMs), or PMs, and risk-based authorization decisions are granted by AOs

Additionally, Enclosure 3: Procedures, Section 16: AO, (a)(b):

b. Render authorization decisions for DoD ISs and PIT systems under their purview in accordance with Reference (q)

ACRONYMS

AM	Account Managers
CAF	Central Adjudication Facility
DoD	Department of Defense
JAMS	Joint Adjudication Management System
JCAVS	Joint Clearance Access and Verification System



LOA	Letter of Appointment
MILDEP	Military Department
JPAS	Joint Personnel Adjudication System
PM	Program Manager
PMO	Program Management Office
PSSAR	Personnel Security System Access Request
JUA	JPAS User Agency- if term is used

APPENDIX A: PROCEDURES GOVERNING USE OF JPAS BY CLEARED CONTRACTORS

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

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

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

1. Contractors shall accurately maintain the JPAS records pertaining to their employees and consultants. Contractors must expeditiously update these records when changes occur (e.g., termination of employment).
2. Contractors are prohibited from placing false information in JPAS, and DMDC will seek appropriate sanctions against contractors and contractor employees who knowingly place false information in JPAS.
3. DoD issues JPAS accounts exclusively for use by a specific contractor or corporate family of contractors. Persons given access to JPAS as account holders may only use JPAS on behalf of the cleared contractor or corporate family of contractors through which the account was issued. For example, an employee of ABC Company holding a JPAS account issued through ABC Company and who works at a government site is not authorized to use the contractor-granted account in support of the government customer. If the government customer requires the contractor employee to review or



- update JPAS records on behalf of the government customer, the government customer must provide a separate, newly created JPAS account for the contractor employee to use – they may not share an existing user ID and password.
4. The JPAS account manager must be a company employee. The JPAS account manager cannot be a subcontractor or consultant.
 5. Contractors may subcontract or obtain consultant support for administering security services, not account management as stipulated in #4 above. The using contractor will provide a JPAS account to the subcontractor or consultant under the using contractor's Security Management Office (SMO) for the sole purpose of permitting the subcontractor or consultant to provide security services for the using company. Subcontractors or consultants providing such security services must be under the direct supervision of the using contractor's FSO or FSO's designee.
 6. Each individual accessing JPAS must have a separate and unique account created by the individual's JPAS account manager. The account manager must maintain a current record of every JPAS account established as per JPAS Account Management Policy, Section 4.2: System Access Request Form.
 7. JPAS users may never share their user IDs, passwords, PK certificates, PINs, or other authentication information with any other individual, including anyone who is a designee or an alternate to the account holder.
 8. Access to JPAS is only authorized by means of company or government-owned equipment with appropriate security controls in place. JPAS users may not access their accounts from personal or home computers or over unsecured wireless networks.
 9. Contractors are not permitted to change an existing date notation in JPAS for the Classified Information Nondisclosure Agreement (SF 312). Contractors must, however, input the date that the SF 312 was signed when JPAS does not reflect a date.
 10. Contractors are authorized to verify prospective employees' eligibility for access to classified information in JPAS prior to an offer of employment being extended. However, contractors may not use JPAS for recruiting purposes.
 11. While access to JPAS is only granted to contractors who have a legitimate need for such access in support of classified work being performed for the Government, JPAS is not a classified system. DSS will not grant a facility security clearance (FCL) for the sole purpose of allowing a company or its employees to gain access to JPAS.
 12. Any contractor with JPAS access that becomes aware of a violation of these procedures shall immediately report the nature of the violation, the names of the responsible parties, and a description of remedial action taken, to the servicing DSS Industrial Security Representative.



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