DEFENSE SECURITY SERVICE

JOINT PERSONNEL ADJUDICATION SYSTEM (JPAS)
PRIVACY IMPACT ASSESSMENT

VERSION 1.0

CICN 0002-DOC-RPT-00413-00

20 NOVEMBER 2008

DSS PRIVACY IMPACT ASSESSMENT

Project Identifying Information

Name of Information Technology (IT) System:	Joint Personnel Adjudication System (JPAS)
OMB Unique Project Identifier (if applicable) and OMB Information Collection Requirement Number/Expiration Date (if applicable)	007-97-01-16-02-6321-00
Budget System Identification Number (SNAP-IT Initiative Number):	SNaP-IT Initiative #: 6321
System Identification Numbers(s) (IT Registry/Defense IT Portfolio Repository:	(DSS DITPR) 6696
Privacy Act System of Record Number (if applicable):	V5-05

Qualifying Questions

A Privacy Impact Assessment is required for all DSS projects with IT systems that maintain Personally Identifiable Information (PII) of at least ten individuals in the public, not counting members of the Armed Forces (to including Reserve and National Guard personnel) and DoD civilian employees (including non-appropriated fund employees).

(Please indicate whether your project meets the criteria requiring a PIA) Yes

If the answer is "yes", you are required to complete the Privacy Impact Assessment by completing the remaining questions on this form.

Privacy Impact Assessment Questions

1. Provide a brief summary or overview of the IT system (activity/purpose, present lifecycle phase, system owner, system boundaries and interconnections, location of system and components, and system backup).

   The following is a brief summary overview of the JPAS system:

   Activity/purpose: Joint Personnel Adjudication System (JPAS) is an N-Tier, Web-

based, Object Oriented application that provides the capability to perform comprehensive personnel security management of all DoD employees, military personnel, civilians, and DoD contractors. JPAS comprises a master repository and centralized processing through the following two application subsystems: The Joint Adjudication Managements System (JAMS) which supports the adjudication process and automates record keeping of the results; and The Joint Clearance and Access Verification System (JCAVS) which provides Security Managers current eligibility information and the ability to update a person's access and security history. Authorized JPAS users are allowed access to DoD eligibility and investigative information via the Web anywhere in the world, at any time of the day or night.

Present Lifecycle phase: Operations and Sustainment (O&S)

System Owner: Defense Security Service (DSS)

System Boundaries and interconnections: DSS server room located in Braddock Place in Alexandria, VA with a virtual Network (VPN) to the Production System. The VPN provides controlled access to applications; including a failover connection to Monterey, CA where the backup system is located.

Location of System and components: Braddock Place, Alexandria, VA

System backup: DMDC, Monterey, CA

2. Describe what information in identifiable form will be collected and the nature and source of the information (e.g. names, Social Security Numbers, gender, race, other component IT systems, IT systems from agencies outside DoD, etc.).

The following identifiable information is collected for JPAS:

Person identifying information on the person of the investigation includes: SSN, Name (all names used), Date of Birth, State of Birth, and Country of Birth.

The source of the information for the JPAS system is as follows:

The source of the information into JPAS is the eligibility and investigative data from the following interfacing systems:

Interface	Full Name
Accessions - Air Force	Accessions - Air Force

Accessions - Air Force Reserve	Accessions - Air Force Reserve
Accessions - Army	Accessions - Army
Accessions - Marines	Accessions - Marines
Accessions - Navy	Accessions - Navy
AF-FSD	Air Force - Full Service Directory
AFPC	Air Force Personnel Center
AFPC	Air Force Personnel Center
AMS	Acquisition Management System
Army NGB	Army National Guard Bureau
Army TAPDB	Total Army Personnel Database
DCPDS	Defense Civilian Personnel Data Systerm
DEERS-RBS	Defense Enrollment Eligibility Record System Real-time Broker Service
DIA/NGA	Defense Intelligence Agency
DISCO FCL	Defense Investigation Security Clearance Office - Facility Clearance Level
DoDIIS	Dept of Defense Intelligence Information System
eClearance/SII	eClearance/SII (access to PIPS system at OPM)
e-QIP	Electronic Questionnaire for Investigation Processing
Manpower (AF)	Manpower - Air Force
Navy	Navy

NSA	National Security Agency
OPM	Office of Personnel Management Open/Close Investigations
PSS	Person Search Service
Scattered Castles	Scattered Castles
USMC	United States Marine Corps

3. Describe how the information will be collected (e.g. via the Web, via paper-based collection, etc.).

The JPAS system collects information via the following methods:

1. Via batch files from DoD and the Office of Personnel Management (OPM) systems.
2. JPAS also provides a graphical user interface (GUI) that allows individual and selected users to enter and update Personnel Info Data (PID).

4. Describe the requirement and why the information in identifiable form is to be collected (e.g. to discharge a statutory mandate, to execute a Component program, etc.).

The personal identifiable information collected and stored in JPAS is necessary for the following reasons:

JPAS implements the provisions and requirements of DoD 5200.2.R "DoD Personnel Security Program". This enables DoD Security Managers to more efficiently and effectively review and individual's eligibility for access to classified and/or national security information prior to granting an access.

5. Describe how the information in identifiable form will be used (e.g. to verify existing data, etc.).

The information in JPAS is used by DoD Adjudicators and Security Managers to obtain accurate up-to-date eligibility and access information on all personnel (military, civilian, and contractor personnel). The DoD Adjudicators and Security Managers are also able to update eligibility and access levels of military, civilian, and contractor personnel nominated for access to sensitive DoD information.

6. Describe whether the system derives or creates new data about individuals through aggregation.

The JPAS system does not derive or create new data about individuals through aggregation.

7. Describe with whom the information in identifiable form will be shared, both internal to DSS and external to DSS (e.g. other DoD Components, Federal agencies, etc.).

The following describes with whom the identifiable form will be shared, both internally and externally to DSS:

Internal to DSS:

1. Defense Industrial Security Clearance Office (DISCO)
2. JPAS account holders in Industrial Security Program (ISP) and Personnel Security Clearance (PSC)

External to DSS:
A record from a system of records maintained by a DoD Component may be disclosed to a federal agency, in response to its request, in connection with the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the requesting agency's decision on the matter.

The information is shared outside of DSS with all JPAS registered users as follows.

JPAS Registered Users	
	Agency Names
Air Force (AFCAF)	Department of the Air Force Central Adjudication Facility
Army (ArmyCCF)	Department of the Army Central Clearance Facility
Collab CAF	Collab Central Adjudication Facility
DIA CAF	Defense Intelligence Agency Central Adjudication Facility
DISCO	Defense Industrial Security Clearance Office
DOHA	Defense Office of Hearing Appeals
Marine	United States Marine Corps
Navy (DoNCAF)	Department of the Navy Central Adjudication Facility
Joint Staff (JS CAF)	Joint Chiefs of Staff Central Adjudication Facility
NRO	National Reconnaissance Office
NSA	National Security Agency
WHS CAF	Washington Headquarters Services Central Adjudication Facility
OSD	Office of the Secretary of Defense

Industry	Industry

8. Describe any opportunities individuals will have to object to the collection of information in identifiable form about themselves or to consent to the specific uses of the information in identifiable form. Where consent is to be obtained, describe the process regarding how the individual is to grant consent.

Consent Question:

The individual cannot refuse to provide PII for the JPAS System.

9. Describe any information that is provided to an individual, and the format of such information (Privacy Act Statement, Privacy Advisory) as well as the means of delivery (e.g., written, electronic, etc.), regarding the determination to collect the information in identifiable form.

This is not applicable to the JPAS System.

10. Describe the administrative/business, physical, and technical processes and controls adopted to secure, protect, and preserve the confidentiality of the information in identifiable form.

The following is a general description of the privacy protections and controls in place to preserve the confidentiality of the information under control of the JPAS System:

Concise narrative answer:

Administrative: The user submits a System Access Request (SAR) to DSS. Upon DSS approving the SAR, the Help Desk creates the user account. Users must meet investigation and eligibility requirements for obtaining a JPAS Account.

Physical: Servers are in a room with access control at Braddock Place in Alexandria, VA.

Technical: To prevent unauthorized access to any resource within the JPAS System, application and system users are prompted to enter a valid user id and password prior to performing an action.

In order to control how application and system administrators access resources, the JPAS system utilizes a Role Based Access Control (RBAC) model. All user accounts within the JPAS system are assigned one or more

roles. When users attempt to access a resource, the appropriate system component will compare the user's roles against the security policy governing the requested resource.

The network infrastructure provides a secure, primary and secondary communication network made up of switches, routers, firewalls, and virtual local area networks (VLAN) to support data traffic for the servers. All communications to the user is accomplished through the Secure Socket Layer (SSL).

11. Identify whether the IT system or collection of information will require a System of Records notice as defined by the Privacy Act of 1974 and as implemented by DoD Directive 5400.11 "DoD Privacy Program," November 11, 2004. If so, and a System Notice has been published in the Federal Register, the Privacy Act System of Records Identifier must be listed.

System of Records Notice for JPAS has been published in the Federal Register and is located at http://www.defenselink.mil/privacy/notices/dss/V5-05.html.

12. Describe/evaluate any potential privacy risks regarding the collection, use, and sharing of the information in identifiable form. Describe/evaluate any privacy risk in providing individuals an opportunity to object/consent or in notifying individuals. Describe/evaluate further any risks posed by the adopted security measures.

-- The following is a description/evaluation of any potential privacy risks regarding the collection, use, and sharing of the information in identifiable form:

Collection of PII poses an amount of risk based purely on the single point of collection coupled with the aggregation of the information in electronic form. In JPAS the amount of PII and sensitive information retained and collected can encompass an individual's entire career as a potential holder/user of classified material. The information retained by JPAS is being stored in compliance with all applicable regulatory guidance and with the full and complete knowledge of the member. The privacy risks would include identification of persons who have been investigated and adjudicated for potential access to classified material. Further risks of reduced concern might be the potential focus of targeting by information collection, tracking, or most unlikely direct harm of the individual.

--The following is a description/evaluation of whether there is any privacy risk in providing individuals an opportunity to object/consent or in notifying individuals:

All personnel have the opportunity to request changes or removals through their Security Management Office. This notification or request would pose no risk to the individual.

-- The following is a description/evaluation of whether any further risks are posed by adopted security measures:

Current or future security measures will not pose any risk to individual privacy information unless a decision is made to remove or reduce the existing security measures.

13. State classification of information/system and whether the PIA should be published or not. If not, provide rationale. If a PIA is planned for publication, state whether it will be published in full or summary form.

Classification:

The JPAS System is an Unclassified System containing Controlled Unclassified Information.

Publication:

The JPAS PIA may be published in full form since it does not contain classified information.

14. Provide additional comments about the system should you feel it necessary.

JPAS Project Manager: Signed 20 Nov 2008
Title: DSS PM

Information Assurance Manager: Signed 20 Nov 2008
Title: DSS Information Assurance Manager

Chief of PLCM: Signed 20 Nov 2008
Title: Chief of Project Lifecycle Management

Senior Information Assurance Officer: Signed 20 Nov 2008
Title: DSS Senior Information Assurance Officer

DSS Privacy Officer: Signed 20 Nov 2008
Title: DSS Chief, FOIA/PA

REVIEWING OFFICIAL: Signed 20 Nov 2008
Title: DSS Chief Information Officer