SUPPORTING STATEMENT
for
OMB XXXX-XXXX, Personnel Security System Access Request (PSSAR) Form

A. JUSTIFICATION

1. Need for Information Collection

50 U.S.C. 401, Congressional declaration of purpose; 50 U.S.C. 435, Purposes; DoD 5200.2R, Department of Defense Personnel Security Program Regulation; DoD 5105.21-M-1, Sensitive Compartment Information Administrative Security Manual; E.O. 10450, Security Requirements for Government Employment; E.O. 10865, Safeguarding Classified Information Within Industry; E.O. 12333, United States Intelligence Activities; E.O. 12829, National Industrial Security Program; and E.O. 12968, Access to Classified Information.

JPAS requires personal data collection to facilitate the initiation, investigation and adjudication of information relevant to DoD security clearances and employment suitability determinations for active duty military, civilian employees and contractors seeking such credentials. As a Personnel Security System it is the authoritative source for clearance information resulting in accesses determinations to sensitive/classified information and facilities.

Specific uses include: facilitation for DoD Adjudicators and Security Managers to obtain accurate up-to-date eligibility and access information on all personnel (military, civilian and contractor personnel) adjudicated by the DoD. 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. **Security Managers working in private companies that contract with DoD and who need access to the JPAS system to update security-related information about their company's employees must complete DD Form 2962 to access the system.** Completion of the form assures JPAS users have the required need-to-know, security clearance, and requires applicants accept the responsibility to abide by relevant DoD regulations, laws and account management policies necessary to access the system.

2. Use of Information

The primary purpose of this information collection is: assuring JPAS users have the required need-to-know, security clearance and document the users' consent to abide by relevant DoD regulations, laws and account management policies governing JPAS account usage. JPAS facilitates DoD Adjudicators and Security Managers' access to accurate up-to-date eligibility and access information on all personnel (military, civilian, and contractor personnel) adjudicated by the DoD. 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.

JPAS limits the use of the information it contains to a specific population of authorized Security Managers, Adjudicators and Security Managers who are required to maintain a minimum clearance of DoD Secret in order to maintain access privileges. The primary means of

access is now via secured web portal located at the following link: https://jpasapp.dmdc.osd.mil/JPAS/JPASDisclosure.

3. Improved Information Technology

The Office of Personnel Management (OPM) has determined that the Standard Form (SF) 86 form may be *initiated* in JPAS by providing a minimal subject PII through the JPAS web application. From this point, the subject will fill out the OPM Standard Form (SF) 86 via the e-QIP web application.

4. Efforts to Identify Duplication

No similar information or verification procedure exists that can be used for this information collection. Data collected on DD form 2962 is not collected again unless a user is being modified or terminated from system access. Each time a user is created or modified the applicant must agree to abide by relevant DoD regulations, laws and account management policies, as the accesses and permissions are different for every user level. No culmination of data from other sources would provide the necessary information necessary for system access.

5. Methods Used to Minimize Burden on Small Entities

PII collection for all individuals is standardized for application access and small entities (companies of one individual) may have the DMDC Contact Center certify their clearance level on their behalf.

6. Consequences of Not Collecting the Information

If collection were stopped, ability to make suitability determinations for employment and access to classified information would be infeasible for active duty military, civilian employees and contractors.

7. Special Circumstances

This collection of information is not conducted under special circumstances; the respondent is asked to complete one form, one time. The information is used only for system access. No requirements are placed on the respondent after providing the information and the personal information collected is kept confidential to the qualification. This collection will be conducted in a manner consistent with guidelines contained in 5 CFR 1320.5 (d) (2).

8. Agency 60-Day Federal Register Notice and Consultations Outside the Agency

The 60-day Federal Register Notice announcing this information collection (as required by 5 CFR 1320.8(d)) was published in *Vol. 80, No. 64,Friday, April 3,2015 Federal Register, Number 64, page 18223*. No public comments were received.

9. Payments to Respondents

No payments, gifts, or guarantees are made to respondents who provide this information.

10. Assurance of Confidentiality

This information collection does not ask the respondents to submit proprietary, trade secret or confidential information to the Department.

11. Personal Identifying Information, Sensitive Questions and Protection of the Information

Personal Identifying Information (PII): Respondents are advised that their data is for OFFICIAL USE ONLY and will be maintained and used in strict confidence in accordance with Federal law and regulations and that those procedures are in place to protect the confidentiality of the information. The erroneous release of PII might cause legal action from individuals against DoD and/or the government.

Protection of the Information: All personal information provided by the subject and stored by JPAS falls under the Privacy Act of 1974.

In order to ensure confidentiality and integrity of data, both asymmetric Public Key Encryption and SSL/TLS encryption are both used for information exchange with JPAS.

Records are maintained in secure, limited access, or monitored areas. Physical entry by unauthorized persons is restricted through the use of locks, passwords, or other administrative procedures. Access to personal information is limited to those individuals who make account access determinations, update user records, verify access and eligibility information, and to perform their official assigned duties.

Social Security Number (SSN): Is requested to ensure accuracy of data involving the specified individual applicant. The SSN is obtained and stored in the initial record for proofing, vetting, and maintaining unambiguous identity for U.S. persons. With the SSN being used for personal identification in major DoD human resource systems (personnel, finance, and medical), it remains the only unique identifier that ensures the accuracy across all the systems for proper data retrieval. An applicant's SSN is used to keep all records together during the adjudication process.

Sensitive Questions (i.e. gender, race and ethnicity): The PSSAR Form does not directly collect information of this nature.

PIA: The Privacy Impact Assessments (PIA) for the Joint Personnel Adjudication Database is accessed at: https://www.dmdc.osd.mil/appj/dwp/rest/download?fileName=JPAS_PIA.pdf&groupName=websiteDocuments

SORNs: The following System of Records Notice (SORNs) oversees the collection of information in the Joint Personnel Adjudication Database: DMDC 12 DoD, Joint Personnel Adjudication System, October 14, 2010, 75 FR 63161.

http://dpclo.defense.gov/Privacy/SORNsIndex/DODwideSORNArticleView/tabid/6797/Article/6701/dmdc-12-dod.aspx

12. Estimates of Annual Response Burden and Labor Cost for Hour Burden to the Respondent for Collection of Information

a. Response Burden:

(1) Corresponds to OMB 83-I

Total annual respondents:	44,000
Frequency of response:	1
Total annual responses:	44,000
Burden per response:	10 minutes
Total burden hours:	7,333

b. Explanation of How Burden was Estimated –

Completion of the Personnel Security System Access Request (PSSAR) form for access to the JPAS application

- There is an average of 44,000 respondents each year which complete the PSSSAR form to become authorized users of the JPAS application in order to maintain/service JPAS records.
- Time to complete the form is 10 minutes.

PSSAR form Annual Respondents = 44,000 respondents

PSSAR form Annual Responses = 44,000 responses/year (complete form once)

PSSAR Form Burden Hours Calculation

Annual Hours To Complete PSSAR Form = (44,000 New Accounts Per Year X 10 minutes to complete form) / 60 minutes

7,333 PSSAR Form Burden Hours

c. Labor Cost to Respondents. There is a labor cost to the respondent.

Labor Cost Calculation:

7,333 annual hours were requested for the collection/maintenance of JPAS information. The average Security Manager salary per hour is $16.

Labor Cost = 7,333 annual hours X $16/hour = $117,328

Labor Cost (in thousands) = $117.3

*Hourly Rate information collected for Security Managers on Indeed.com and PayScale.com.

13. Estimates of Other Cost Burden for the Respondent for Collection of Information

a. Total Capital and Start-up Cost.

Total capital and start-up costs are approximately $100 per Industry user to obtain PKI credentials, if not approved for a Common Access Card (CAC) to access the JPAS system.

Total Capital/Startup Costs Calculation:

Total Capital/Startup Costs = $100/card X 44,000 Industry Users = $4,400,000

Total Capital/Startup Costs (in thousands) = $4,400

b. Operation and Maintenance Cost.

There are no operation or maintenance costs associated with completing the PSSAR form after initial completion of the form and acquisition of a PKI credential

Total Annual Cost (O&M) = $0 (in thousands)

14. Estimates of Cost to the Federal Government

a. Work load requirements and Estimated Costs

Total Annualized Cost to the Federal Government includes the $4,400 cost of procuring PKI credentials for Security Managers ineligible for a CAC card, and $0 O&M costs for Security Managers after initial completion of their form

Total Annualized Cost Requested Calculation:

Total Annualized Cost = $4,400 Startup + $0 O&M = $4,400

Total Annualized Cost Requested (in thousands) = $4,400

15. Changes in Burden

This is a collection in place operating without an OMB number.

Annual Hours Burden
The new total number of hours requested is: **7,333 hours**.
The current burden estimate is **0 hours**.
The change of burden hours is **increased by 7,333 hours**.

7,333 change in annual hours is the result of **program adjustment**, as DMDC is requesting revision to the PSSAR form for clarity to assist account applicants in its completion.

Annualized Cost Burden

The new annual cost burden is: **$4,400 (in thousands)**.
The current annual cost burden is **$0 (in thousands)**.
The change of annualized cost burden is an increase of $**4,400 (in thousands)**.

$4,400 change in annualized cost burden is the result of **program adjustment**, as DMDC is requesting approval of the PSSAR form for the purpose of facilitating access requests to JPAS.

16. Publication Plans/Time Schedule

Results of this information collection will not be published.

17. Approval Not to Display Expiration Date

Approval not to display the expiration data is not being sought.

18. Exceptions to the Certification Statement

No exceptions to the certification statement are being sought.

B. COLLECTION OF INFORMATION EMPLOYING STATISTICAL METHODS

Statistical methods are not employed for this collection of information.