

SUPPORTING STATEMENT

for

OMB 0704-TBD, Joint Personal Adjudication System (JPAS) – Defense Manpower Data Center

A. JUSTIFICATION

1. Need for Information Collection

50 U.S.C. 401, Congressional declaration of purpose (Attachment 1); 50 U.S.C. 435, Purposes (Attachment 2); DoD 5200.2R, Department of Defense Personnel Security Program Regulation (Attachment 3); DoD 5105.21-M-1, Sensitive Compartment Information Administrative Security Manual (Attachment 4); E.O. 10450, Security Requirements for Government Employment (Attachment 5); E.O. 10865, Safeguarding Classified Information Within Industry (Attachment 6); E.O. 12333, United States Intelligence Activities (Attachment 7); E.O. 12829, National Industrial Security Program (Attachment 8); and E.O. 12968, Access to Classified Information (Attachment 9).

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 access determinations to sensitive/classified information and facilities.

JPAS serves as the Department's primary mode of initiating OPM's Electronic Questionnaire for Investigation Processing (E-QIP) and also provides reciprocity for other Executive Branch partners via the Central Verification System (CVS).

2. Use of Information

The primary purpose of this information collection is: 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.

JPAS limits the use of the information it contains to a specific population of authorized Facility Security Officers (FSOs), 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 in JPAS is not collected again unless there is a gap in service large enough to facilitate a reinvestigation. No culmination of data from other sources would provide the necessary information 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.

Provided clearances are properly maintained / reinvestigated (10 years for Secret and 5 years for Top Secret) there would be no requirement to collect redundant information. If the aforementioned timelines are exceeded, the information required to initiate and complete a background investigation will need to be reproduced.

5. Methods Used to Minimize Burden on Small Entities

PII collection for all individuals is standardized for investigation initiation and adjudication and cannot be simplified.

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 enlistment purposes by the Department of Defense. No requirements are placed on the respondent after providing the information and the personal information collected is kept confidential to the qualification process and the individual's military records. 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. 77, No. 29, Monday, February 13, 2012, Federal Register, Number 29, page 7567* (Attachment 10). Public comments received in response to the notice requested a copy of the JPAS SORN. A copy was provided electronically to the inquiries.

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.

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

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 accordance with Federal law and regulations and that those procedures are in place to protect the information to the extent permitted by law. 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 adjudication determinations, update 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): JPAS does not directly collect information of this nature; however, it does store investigation results and corresponding adjudication information. Dependent upon type of background investigation being conducted, some or all of this sensitive information might be collected to verify that the individual in question is suitable to handle information related to national security.

PIA: The Privacy Impact Assessments (PIA) for the Joint Personnel Adjudication Database is accessed at (Attachment 11):

https://www.dmdc.osd.mil/appj/dwp/getfile.do?fileNm=JPAS_PIA.pdf&filePathNm=dataInq&appId=567&app_key_id=fh94ne8932er

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 (Attachment 12).
<http://dpclo.defense.gov/privacy/SORNS/dod/DMDC12.html>

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:	22,225
Frequency of response:	2
Total annual responses:	2,111,375
Burden per response:	20 minutes
Total burden hours:	703,792

b. Explanation of How Burden was Estimated.

There are 22,225 Respondents (Industry Users/Contractor Facility Security Officers (FSOs) authorized to respond/update records in JPAS). There are approximately 1,063,138 person records in JPAS with an Industry person category. Respondents (FSOs) typically update each person record they service in JPAS an average of 2 times per year, and each update takes about 20 minutes.

$(1,063,138 \text{ records} \times 2 \text{ updates per year}) / 22,225 \text{ respondents} = 95 \text{ responses per Respondent}$

Total Annual Responses Calculation:

Total Annual Responses = 22,225 Respondents x 95 responses each =

Total Annual Responses = 2,111,375

Total Burden Hours Calculation:

Total Annual Hours Requested = $(22,225 \text{ Respondents} \times 95 \text{ responses} \times 20 \text{ minutes per update}) / 60 \text{ minutes}$

Total Annual Hours Requested = 703,792

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

Labor Cost Calculation:

703,792 annual hours were requested for the collection/maintenance of JPAS information. The average Facility Security Officer salary per hour is \$16.

Labor Cost = 703,792 annual hours X \$16/hour = \$11,260,672

Labor Cost (in thousands) = \$11,260.7

*Hourly Rate information collected for FSOs 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 22,225 Industry Users = \$2,222,500

Total Capital/Startup Costs (in thousands) = \$2,222.5

b. Operation and Maintenance Cost.

703,792 annual hours were requested for the collection/maintenance of JPAS information. The average Facility Security Officer salary per hour is \$16 (average salary information collected for FSOs on Indeed.com and PayScale.com).

Total Annual Costs (O&M) Calculation:

Total Annual Costs (O&M) = 703,792 annual hours X \$16/hour = \$11,260,672

Total Annual Cost (O&M) = \$11,260.7 (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 \$2,222.5 cost of procuring PKI credentials for FSOs ineligible for a CAC card, and \$11,260.7 O&M costs for FSOs to maintain JPAS records as part of their main job responsibilities.

Total Annualized Cost Requested Calculation:

Total Annualized Cost = \$2,222.5 Startup + \$11,260.7 O&M = \$13,483,200

Total Annualized Cost Requested (in thousands) = \$13,483.2

15. Changes in Burden

This is an existing collection without an OMB number and therefore no current OMB inventory for hour burden exists.

An increase of **703,792 total annual hours** is the result of **program change**, as there was no existing OMB inventory for hour burden

This is an existing collection without an OMB number and therefore no current OMB inventory for annualized cost burden exists

An increase of **\$13,483.2 (in thousands)** is the result of **program change**, as there was no existing OMB inventory for annualized cost burden

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.