

SUPPORTING STATEMENT
for
OMB 0704-AAIZ, Defense Information System for Security

SUPPORTING STATEMENT – PART A

A. JUSTIFICATION

1. Need for the 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; DoD 5220.22-M; and E.O. 12968, Access to Classified Information.

The Defense Information System for Security (DISS) is a United States Department of Defense (DoD) automated system for personnel security, providing a common, comprehensive medium to record, document, and identify personal security actions within the Department including submitting adverse information, verification of security clearance status, requesting investigations, and supporting Continuous Evaluation activities. DISS 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.

DoD 5200.2R establishes regulations for personnel security that are mandatory for use by all DoD components. E.O. 12829, National Industrial Security Program (NISP) establishes the Department of Defense as the Executive Agent for NISP, and the Cognizant Security Agency (CSA) for DoD and non-CSA agencies, and lays out the responsibility for the CSA to maintain a system of eligibility and access determinations of contractor personnel. DoD 5220.22-M states that “When the CSA 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.” The aforementioned authorities and DoD regulations designate DISS as that system: a personnel security system serving as the authoritative source for clearance information resulting in access determinations to sensitive or classified information and facilities.

2. Use of the Information

The respondents for this information collection are 22,225 Facility Security Officers (FSOs) working in industry companies, who are responsible for the regular servicing and updating of the DISS records of individuals with an industry person category. The specific purpose of this information collection is for FSOs to update the DISS records of contractor personnel within their company and Security Management Office (SMO) to facilitate DoD Adjudicators and Security Managers obtaining accurate up-to-date eligibility and access information on contractor personnel.

This submission addresses the aforementioned public information collection, but does not cover the entirety of information contained in DISS, which is obtained from the following: individual persons; DoD personnel systems; Case Adjudication Tracking System (CATS); Continuous Evaluation Records; DoD and federal adjudicative facilities/organizations; DoD and Non-DoD agencies; and security managers, security officers, or other officials requesting and/or sponsoring the security eligibility or suitability determination or visitation of facility. Additional information may be obtained from other sources such as personnel security investigations, security representatives, subject’s personal financial records, military service records, medical

records, and unsolicited sources. Information collected from the individual, using Standard Form (SF) 85 is cleared under OMB Control Number 3206-0261. Information collected from the individual, using SF-86/85/85P is cleared under OMB Control Number 3206-0005.

DISS is the successor system to replace Joint Personnel Adjudication System (JPAS), previously approved OMB Control Number 0704-0496, which expired on 3/31/2016. Previous JPAS submissions covered the time burden on respondents of completing the DMDC system access request form, the DD Form 2962, which is, as of November 2015, covered under a separate OMB Control Number, 0704-0542, expiration 9/30/2018. The burden estimates associated with JPAS/DISS users completing and submitting the DD 2962 to request system access is no longer included.

DISS limits the use of the information it contains to a specific population of authorized FSOs, Adjudicators and Security Managers who are required to maintain a minimum clearance of DoD Secret in order to maintain access privileges. Privacy disclosures visible to DISS users are displayed in an accompanying screenshot to this submission. The means of access to DISS is via secure web portal (<https://dissportal.dmdc.mil/diss-jvs-ui/faces/consent.jsp>).

3. Use of Information Technology

100% of responses are collected electronically. The Office of Personnel Management (OPM) has determined that the Standard Form (SF) 86 may be initiated in DISS by providing a minimal amount of subject Personally Identifiable Information (PII) through the DISS web application. From this point, the subject will fill out the OPM SF-86/85/85P via the e-QIP web application. As referenced in Section 2, information collected from the individual using SF-86/85/85P is cleared under OMB Control Number 3206-0005.

4. Non-duplication

No similar information or verification procedure exists that can be used to collect this information. Data collected in DISS 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 contractors.

If clearances are properly maintained / reinvestigated (every 10 years for Secret and 5 years for Top Secret), then there is 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. As referenced in Section 2, information collected from the individual using SF-86/85/85P is cleared under OMB Control Number 3206-0005.

5. Burden on Small Business

There is no significant impact on small businesses.

6. Less Frequent Collection

If collection occurred less frequently, the ability to make suitability determinations for employment and access to classified information by contractors would be negatively impacted.

7. Paperwork Reduction Act Guidelines

This collection of information is not conducted under special circumstances. This collection will be

conducted in a manner consistent with guidelines contained in 5 CFR 1320.5 (d) (2).

8. Consultation and Public Comments

Part A: PUBLIC NOTICE.

The 60 Day Federal Register Notice for the collection was published on Thursday, March 22, 2018. The 60-Day FRN citation is 83 FRN 12571.

No relevant public comments were received.

A 30-Day Federal Register Notice for the collection published on Friday, June 1, 2018. The 30-Day FRN citation is 83 FRN 25445.

Part B: CONSULTATION

Defense Manpower Data Center (DMDC) regularly consults with important stakeholders on the topic of FSO usage of DISS, including the clarity and ease-of-use of the system, availability of system functionality and the continued importance of the DISS information collection mechanism to the Federal personnel security enterprise. These stakeholders include, but are not limited to, the Office of the Under Secretary of Defense for Intelligence (USD-I), Office of Personnel Management (OPM), National Background Investigation Bureau (NBIB), Accessions and Personnel centers of the Military Services, the Department of Defense Central Adjudicative Facility (CAF), and the DoD Defense Security Service (DSS).

9. Gifts or Payment

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

10. Confidentiality

DISS provides a Privacy Advisory advising users that they are accessing a system that contains Privacy Act information. Screenshots of the privacy advisory are provided with the OMB submission package for this collection. A Privacy Act Statement is provided on the SF-86/85/85P, cleared under OMB Control Number 3206-0005. Regarding Personally Identifiable Information (PII), respondents are advised that their data is for OFFICIAL USE ONLY and that PII will be maintained and used in strict confidence in accordance with Federal law. All personal information provided by the subject and stored by DISS 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 used for information exchange with DISS.

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. The Retention and Disposal Schedule for this collection, as listed on the SORN, is that "Records are destroyed no later than 16 continuous years after termination of affiliation with the DoD."

The Privacy Impact Assessment (PIA) for the Defense Information System for Security accompanies this submission in Tab D.

The System of Records Notice (SORN) oversees the collection of information in the Defense Information System for Security: DMDC 24 DoD, Defense Information System for Security, June 15, 2016, 81 FR 39032. (<http://dpcl.d.defense.gov/Privacy/SORNsIndex/DOD-wide-SORN-Article-View/Article/799795/dmdc-24-dod>)

11. Sensitive Questions

Sensitive Questions (i.e. gender, race and ethnicity): DISS 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.

Social Security Number (SSN) is requested to ensure accuracy of data involving the specified individual applicant or FSO. The SSN is obtained and stored in the initial record for proofing, vetting, and maintaining unambiguous identity for U.S. persons. As the primary method of personal identification in major DoD human resource systems (personnel, finance, and medical), the SSN remains the only unique identifier that ensures accuracy across all such systems for proper data retrieval. A copy of the SSN Justification Memorandum dated February 18, 2016, and Defense Privacy and Civil Liberties Division acceptance letter dated August 3, 2016, are included with the OMB submission package for this collection.

12. Respondent Burden, and its Labor Costs

a. Estimation of Respondent Burden

Estimation of Respondent Burden Hours					
	Number of Respondents	Number of Responses per Respondent	Number of Total Annual Responses	Response Time (Amount of time needed to complete the collection instrument)	Respondent Burden Hours (Total Annual Responses multiplied by Response Time) Please compute these into hours)
Collection Instrument #1: Servicing DISS records in the application by Facility Security Officers (FSOs)	22,225	45	1,000,125	20 minutes	333,375
Total	22,225	45	1,000,125	20 minutes	333,375

- There are 22,225 Facility Security Officers (FSOs) which are responsible for 22 to 23 DISS records with an Industry person category, and there are 500,000 such person records in DISS.
- FSOs typically update each person record they service in DISS an average of 2 times per year, taking about 20 minutes each time, resulting in approximately one million annual responses.
- The figure for “Number of Responses per Respondent” is drawn from the fact that each FSO works on between 22 and 23 DISS records annually (an average of 22.5), and each record is serviced twice annually on average (22.5 x 2 = 45 responses per respondent).

b. Labor Cost of Respondent Burden

Labor Cost of Respondent Burden					
	Number of Responses	Response Time per Response	Respondent Hourly Wage	Labor Burden per Response (Response Time multiplied by Respondent Hourly Wage)	Total Labor Burden (Number of Responses multiplied by Response Time multiplied by Respondent Hourly Wage)
Collection Instrument #1(DISS system – Servicing DISS records)	1,000,125	20 minutes	\$16*	\$5.33	\$5,334,000
Total	1,000,125	20 minutes	\$16*	\$5.33	\$5,334,000

Labor Cost Calculation:

333,375 annual hours were requested for the collection/maintenance of DISS information. The estimated Facility Security Officer salary per hour is \$16*.

Labor Cost = 333,375 annual hours X \$16/hour = \$5,334,000

Labor Cost (in thousands) = \$5,334.00

*Hourly Rate estimate for FSOs taken from United States Department of Labor, Bureau of Labor Statistics Occupational Employment Statistics page titled “33-9099 Protective Service Workers, All Other” Link: <http://www.bls.gov/oes/current/oes339099.htm>

13. Respondent Costs Other Than Burden Hour Costs

a. Total capital and start-up costs annualized over the expected useful life of the item(s):

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 DISS 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. Total operation and maintenance costs: **\$0 (in thousands)**

14. Cost to the Federal Government

a. Labor Cost to the Federal Government

Instrument #1: DISS

- a. Number of Total Annual Responses: 1,000,125
- b. Processing Time per Response: 0
- c. Hourly Wage of Worker(s) Processing Responses: \$0
- d. Cost to Process Each Response: \$0
- e. Total Cost to Process Responses: \$0

Overall Labor Burden to Federal Government

- a. Total Number of Annual Responses: 1,000,125
- b. Total Labor Burden: \$0

b. Operational and Maintenance Costs

- a. Equipment: \$0
- b. Printing: \$0
- c. Postage: \$0
- d. Software Purchases: \$0
- e. Licensing Costs: \$0
- f. Other: \$0
- g. Total (P: add A through F in this section): \$0

DISS is an enterprise-wide system for personnel security within the Department of Defense, and the processing of FSO responses is automated by the system, consuming miniscule amounts of system resources for operational and maintenance costs. Additionally, as the process of receiving FSO responses is automated, the labor cost to the Federal government is zero. Hence, the total cost to the Federal government of owning FSO responses as well as servicing and updating DISS records is zero.

15. Reasons for Change in Burden

This is a new collection being submitted for review, with a new associated burden.

16. Publication of Results

Results of this information collection are not published.

17. Non-Display of OMB Expiration Date

This submission does not seek approval to forego displaying the expiration date.

18. Exceptions to "Certification for Paperwork Reduction Submissions"

This submission does not seek an exception to the certification statement.