

SUPPORTING STATEMENT - PART A

Defense Information System for Security (DISS)

OMB Control Number 0705-0008

Summary of Changes from Previously Approved Collection

- There has been a burden increase in the following areas: number of DISS Records FSO Responsible, number of industry subject records, number of average subject updates/year, number of responses per respondent, total annual responses, respondent burden hours, total labor burden, and the annual cost burden. There's been a decrease in number of industry users, the total cost, and the annual hours burden.

1. Need for the Information Collection

These are the policies that govern the personal security mission.

- 50 U.S. Code (USC) § 3002 – Congressional declaration of purpose
- 50 USC § 3161 – Procedures
- DoD Instruction (DoDI) 5200.02 – DoD Personnel Security Program (PSP)
- DoD Manual (DoDM) 5200.02 – Procedures for the DoD Personnel Security Program (PSP)
- DoDM 5105.21 – Sensitive Compartmented Information (SCI) Administrative Security Manual
- Executive Order (EO) 10450 – Security Requirements for Government Employment
- EO 10865 – Safeguarding Classified Information Within Industry; EO 12333, United States Intelligence Activities
- EO 12829 – National Industrial Security Program
- DoDI 5220.31 – National Industrial Security Program
- EO 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.

DoDD 5143.01 establishes DoD policy and assigns responsibilities for administering the National Industrial Security Program (NISP), in accordance with Executive Orders 10865

and 12829, as amended, and in accordance with Title 32, Code of Federal Regulations (CFR) Part 117, "National Industrial Security Program Operating Manual,". CFR Part 117 states that "Contractors will annotate and maintain the accuracy of their employees' records in the system of record for contractor eligibility and access to classified information, when one has been designated by the CSA." 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 accesses determinations to sensitive or classified information and facilities.

2. Use of the Information

The respondents for this information collection are the 45,377 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 the Standard Form (SF) 85 is cleared under OMB Control Number 3206-0261, the SF85P is cleared under OMB Control Number 3206-0258, and the SF86 is cleared under OMB Control Number 3206-0005.

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 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.nbis.mil/diss-jvs-ui/faces/consent.jsp>).

3. Use of Information Technology

100% of responses are collected electronically. 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 SF-86/85/85P via the NBIS eAPP web application. As referenced in Section 2, information collected from the individual using the SF85 is cleared under OMB Control Number 3206-0261, the SF85P is cleared under OMB Control Number 3206-0258, and the SF86 is cleared under OMB Control Number 3206-0005.

4. Non-duplication

The information obtained through this collection is unique and is not already available for use or adaptation from another cleared source. 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.

5. Burden on Small Businesses

This information collection does not impose a significant economic impact on a substantial number of small businesses or entities.

6. Less Frequent Collection

Collected on an as needed basis for employment. 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 does not require collection to be conducted in a manner inconsistent with the guidelines delineated in 5 CFR 1320.5(d)(2).

8. Consultation and Public Comments

Part A: PUBLIC NOTICE

A 60-Day Federal Register Notice (FRN) for the collection published on Monday, May 20, 2024. The 60-Day FRN citation is 89 FR 43830.

No comments were received during the 60-Day Comment Period.

A 30-Day Federal Register Notice for the collection published on Monday, September 23, 2024. The 30-Day FRN citation is 89 FR 77493.

Part B: CONSULTATION

Defense Counterintelligence Security Agency (DCSA) 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 and Security (OUSD(I&S)), Office of Personnel Management (OPM), Accessions

and Personnel centers of the Military Services, and the Defense Office of Hearings and Appeals (DOHA).

9. Gifts or Payment

No payments or gifts are being offered to respondents as an incentive to participate in the collection.

10. Confidentiality

DISS provides a Privacy Act Statement 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. 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.

To ensure confidentiality and integrity of data, both asymmetric Public Key Encryption and Secure Socket Layer (SSL)/Transport Layer Security (TLS) encryption are used for information exchange with DISS.

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

The System of Records Notice (SORN) applicable to the collection of information in the Defense Information System for Security is the Personnel Vetting Records System, DUSDI 02-DoD (October 17, 2018; 83 FR 52420). It can be accessed here:

<https://www.federalregister.gov/documents/2018/10/17/2018-22508/privacy-act-of-1974-system-of-records>.

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 Records Retention and Disposal Schedules for DISS are DAA-0446-2021-0009 and DAA-0446-2019-0004; accompany this submission.

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. The original SSN Justification Memorandum has expired. An updated SSN Justification Memorandum has been routed to OATSD-PCLD for further processing. The updated SSN Justification Memorandum is included with the OMB submission package for this collection.

12. Respondent Burden, and its Labor Costs

Part A: ESTIMATION OF RESPONDENT BURDEN

1) Collection Instrument

DISS

- a) Number of Respondents: 20,994
- b) Number of Responses Per Respondent: 258
- c) Number of Total Annual Responses: 5,416,452
- d) Response Time: 20 minutes
- e) Respondent Burden Hours: 1,805,484 hours

2) Total Submission Burden

- a) Total Number of Respondents: 20,994
- b) Total Number of Annual Responses: 5,416,452
- c) Total Respondent Burden Hours: 1,805,484 hours

Part B: LABOR COST OF RESPONDENT BURDEN

1) Collection Instrument

DISS

- a) Number of Total Annual Responses: 5,416,452
- b) Response Time: 20 minutes
- c) Respondent Hourly Wage: \$18.93
- d) Labor Burden per Response: \$6.31
- e) Total Labor Burden: \$34,177,812

2) Overall Labor Burden

- a) Total Number of Annual Responses: 5,416,452
- b) Total Labor Burden: \$34,177,812

The hourly wage estimate for FSOs is based on from United States Department of Labor, Bureau of Labor Statistics Occupational Employment Statistics page titled "33-9099 Protective Service Workers, All Other" (<https://www.bls.gov/oes/current/oes339099.htm>).

13. Respondent Costs Other Than Burden Hour Costs

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 20,994 Industry Users = \$2,099,400

Total Capital/Startup Costs (in thousands) = \$2,099,400

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

14. Cost to the Federal Government

Part A: LABOR COST TO THE FEDERAL GOVERNMENT

1) Collection Instrument
DISS

- a) Number of Total Annual Responses: 5,416,452
- b) Processing Time per Response: 0
- c) Hourly Wage of Worker(s) Processing Responses: \$49.85
- d) Cost to Process Each Response: \$0
- e) Total Cost to Process Responses: \$0

2) Overall Labor Burden to Federal Government

- a) Total Number of Annual Responses: 5,416,452
- b) Total Labor Burden: \$0

Part B: OPERATIONAL AND MAINTENANCE COSTS

1) Cost Categories

- a) Equipment: \$0
- b) Printing: \$0
- c) Postage: \$0
- d) Software Purchases: \$0
- e) Licensing Costs: \$0
- f) Other: \$0

2) Total Operational and Maintenance Cost: \$0

Part C: TOTAL COST TO THE FEDERAL GOVERNMENT

1) Total Labor Cost to the Federal Government: \$0

2) Total Operational and Maintenance Costs: \$0

3) Total Cost to the Federal Government: \$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

The burden has increased since the previous approval date to 4,735,979 hours due to the fact that DISS is a new program that continues to onboard and grow, especially as DCSA expands its mission and requirements. The system now has the capability of pulling the response data precisely instead of relying on the analysts' best guess of response numbers.

Annual Hours Burden

The total number of hours requested is: 5,416,452 hours.

The current burden estimate is 680,655 hours.

The change of burden hours is an increase of 4,735,797 hours.

Annualized Cost Burden

The annual cost burden is: **\$34,177,812**

The current annual cost burden is **\$11,571,135**

The change of annualized cost burden is an increase of **\$22,606,677**

An increase of **4,735,797 hours** is the result of **Program Change** as DISS is a new program that continues to onboard and grow especially as DCSA expands its mission and requirements.

DISS is the replacement system to Joint Personnel Adjudication System (JPAS), previously approved OMB Control Number 0704-0496, which was officially discontinued on 3/20/2021. Previous JPAS submissions covered the time burden on respondents of completing the DCSA system access request form, the DD Form 2962, which is covered under a separate OMB Control Number, 0705-0009 (expires 1/31/2025). The burden estimates associated with JPAS/DISS users completing and submitting the DD 2962 to request system access is no longer included.

16. Publication of Results

The results of this information collection will not be published.

17. Non-Display of OMB Expiration Date

We are not seeking approval to omit the display of the expiration date of the OMB approval on the collection instrument.

18. Exceptions to “Certification for Paperwork Reduction Submissions”

We are not requesting any exemptions to the provisions stated in 5 CFR 1320.9.