PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

NBIS Defense Information System for Security (DISS) Version 2

2. DOD COMPONENT NAME:

Defense Counterintelligence and Security Agency

3. PIA APPROVAL DATE:

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: Federal contractors, military family members, and foreign nationals are included in general public.)*

- [ ] From members of the general public
- [ ] From Federal employees
- [x] from both members of the general public and Federal employees
- [ ] Not Collected *(if checked proceed to Section 4)*

b. The PII is in a: *(Check one.)*

- [x] New DoD Information System
- [ ] New Electronic Collection
- [ ] Existing DoD Information System
- [ ] Existing Electronic Collection
- [ ] Significantly Modified DoD Information System

c. Describe the purpose of this DoD information system or electronic collection and describe the types of personal information about individuals collected in the system.

DISS is a DoD enterprise information system for personnel security, providing a common, comprehensive medium to request, record, document, and identify personnel security actions within the Department including: determinations of eligibility and access to classified or national security information, suitability and/or fitness for employment, and HSPD-12 determination for Personal Identity Verification (PIV) to access government facilities and systems, submitting adverse information, verification of investigation and/or adjudicative status, support of continuous evaluation and insider threat detection, prevention, and mitigation activities.

The DISS family of systems is comprised of three components: the Case Adjudication Tracking System (CATS), the Joint Verification System (JVS) and Appeals. CATS is used by the DoD Adjudicative Community for the purpose of recording eligibility determinations. JVS is used by DoD Security Managers and Industry Facility Security Officers for the purpose of verifying eligibility, recording access determinations, submitting incidents for subsequent adjudication, and visit requests from the field (worldwide). Appeals is an Enterprise web application which enables users to complete adjudication for subjects who appeal the determination made on their case in CATS, or for subjects for whom a decision cannot be made in CATS.

These records may also be used as a management tool for statistical analyses, tracking, reporting, evaluating program effectiveness, and conducting research.

The types of personal information being collected includes: Name(s); Social Security Number; DoD ID Number; Personal Contact Information; Demographic information and information relating to security clearance eligibility.

d. Why is the PII collected and/or what is the intended use of the PII? *(e.g., verification, identification, authentication, data matching, mission-related use, administrative use)*

The intended use of the PII collected by DISS is for Security Clearance Investigation and Verification. Also data matching, as the SSN is the identifier that links all aspects of a security clearance investigation together; linked to other Federal agencies that continue to use the SSN as a primary identifier.

e. Do individuals have the opportunity to object to the collection of their PII? [x] Yes [ ] No

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object to the collection of PII.

The cleared individuals on whom the PII will be collected have given permission for information to be collected from them by voluntarily filling out the SF 85 and/or SF 86 Questionnaire for National Security Positions. Both the SF85 and SF86 state "The information you provide on this form, and information collected during an investigation, may be disclosed without your consent by an agency maintaining the

information in a system of records as permitted by the Privacy Act [5 U.S.C. 552a(b)], and by routine uses, a list of which are published by the agency in the Federal Register." Both the SF85 and SF86 list as a Routine Use, disclosure "to Executive Branch Agency insider threat, counterintelligence, and counterterrorism officials to fulfill their responsibilities under applicable Federal law and policy, including but not limited to E.O. 12333, 13587 and the National Insider Threat Policy and Minimum Standards given consent for data to be collected by voluntarily submitting the SF 85 or SF 86.

f. Do individuals have the opportunity to consent to the specific uses of their PII? [X] Yes [ ] No

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

DISS is not the initial point of PII collection. The individuals on whom the PII will be collected have given voluntary responses to information requested by official questionnaires (e.g., SF 85, SF 86). The Electronic Questionnaires for Investigation Processing (eQIP) is the initial point of PII collection; then PII is transmitted to DISS.

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. *(Check as appropriate and provide the actual wording.)*

[X] Privacy Act Statement [ ] Privacy Advisory [ ] Not Applicable

Privacy Act Statement is provided at initiation of investigation (SF 85, SF 85P and SF 86)

h. With whom will the PII be shared through data/system exchange, both within your DoD Component and outside your Component? *(Check all that apply)*

[X] Within the DoD Component	Specify.	Office of the Secretary of Defense (OSD); Under Secretary of Defense for Intelligence (USD(I)); Under Secretary of Defense for Acquisition, Technology and Logistics (AT&L); Washington Headquarters Services (WHS); Defense Security Services (DSS); Joint Chiefs of Staff (JCS)
[X] Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	U.S. Army; U.S. Air Force; U.S. Navy; U.S. Marine Corps; and Guard/Reserve Components
[X] Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	Specify.	U.S. Citizenship and Immigration Services; Office of Personnel Management; Federal Agencies that have employees, to include Contractors, eligible for security clearances and/or access to classified information.
[ ] State and Local Agencies	Specify.	
[X] Contractor *(Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)*	Specify.	Contractors with an active Facility Clearance and employees who are eligible to have a security clearance and/or access to classified national security information following National Industrial Security Program Operating Manual (NISPOM) regulations.
[ ] Other *(e.g., commercial providers, colleges).*	Specify.	

i. Source of the PII collected is: *(Check all that apply and list all information systems if applicable)*

[X] Individuals [X] Databases

[X] Existing DoD Information Systems [X] Commercial Systems

[X] Other Federal Information Systems

Information contained in this system is obtained from the individual (e.g. SF-85, Questionnaire for Non-Sensitive Positions, SF-85P, Questionnaire for Public Trust Positions, SF-86, Questionnaire for the National Security Positions, or self-reported information); DoD personnel systems (e.g. Defense Enrollment Eligibility Reporting System; Defense Civilian Personnel Data System; Electronic Military Personnel Record System, etc.); continuous evaluation records; DoD and federal adjudicative facilities/organizations; investigative agencies (e.g. Office of Personnel Management (OPM) Federal Investigative Services (FIS); 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, criminal or civil investigations, security representatives, subject's personal financial records, military service records, travel records, medical records, and unsolicited sources.

j. How will the information be collected? *(Check all that apply and list all Official Form Numbers if applicable)*

[X] E-mail [X] Official Form (*Enter Form Number(s) in the box below)*

[X] In-Person Contact [X] Paper

[X] Fax [X] Telephone Interview

[X] Information Sharing - System to System [X] Website/E-Form

[X] Other *(If Other, enter the information in the box below)*

SF 85; SF 86, and eQIP

k. Does this DoD Information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information must be consistent.

[X] Yes [ ] No

If "Yes," enter SORN System Identifier Personnel Vetting Records System, DUSD

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or http://dpcld.defense.gov/Privacy/SORNs/

or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

l. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority. DAA-0446-2021-0009

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

Records are destroyed no later than 16 years after termination of affiliation with the DoD. Investigative files and the computerized data bases which show the scheduling or completion of an investigation are retained for 16 years from the date of closing or the date of the most recent investigative activity, whichever is later, except for investigations involving potentially actionable issue(s) which will be maintained for 25 years from the date of closing or the date of the most recent investigative activity.

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statue or Executive Order.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
(2) If a SORN does not apply, cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply).

(a) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If direct statutory authority or an Executive Order does not exist, indirect statutory authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) If direct or indirect authority does not exist, DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component must be identified.

5 U.S.C. 9101, Access to Criminal History Records for National Security and Other Purposes; 10 U.S.C. 137, Under Secretary of Defense for Intelligence; E.O. 12968, Access to Classified Information; E.O. 12333 United States Intelligence Activities; E.O. 12829, National Industrial Security Program; E.O. 10450, Security Requirements for Government Employment; E.O. 10865, Safeguarding Classified Information Within Industry; E.O. 13467 Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees and Eligibility for Access to Classified National Security Information; E.O. 12968, as amended, Access to Classified Information; E.O. 13488, Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust; E.O. 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information; DoD Instruction (DoDI) 1400.25, Volume 731, DoD Civilian Personnel Management System: Suitability and Fitness Adjudication for Civilian Employees; DoD Directive (DoDD) 5205.16, DoD Insider Threat Program; DoDD 1145.02E, United States Military Entrance Processing Command (USMEPCOM); DoD 5200.2-R, DoD Personnel Security Program; DoD Manual 5105.21, Volume 1, Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Information and Information Systems Security; DoDI 1304.26, Qualification Standards for Enlistment, Appointment, and Induction; DoDI 5200.02, DoD

Personnel Security Program (PSP); DoDD 5220.6, Defense Industrial Personnel Security Clearance Review Program; DoDI 5220.22, National Industrial Security Program (NISP); DoDI 5200.46, DoD Investigative and Adjudicative Guidance for Issuing the Common Access Card (CAC); Homeland Security Presidential Directive (HSPD) 12, Policy for Common Identification Standard for Federal Employees and Contractors; and E.O. 9397 (SSN), as amended.

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (OMB) Control Number?

Contact the Component Information Management Control Officer or DoD Clearance Officer for this information. This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

[X] Yes [ ] No [ ] Pending

(1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
(2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, " DoD Information Collections Manual: Procedures for DoD Public Information Collections."
(3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

0704-0573 . OMB EXPIRATION DATE: 07/31/2021. The 60-Day Notice for 0704-0573, "Defense Information System for Security," published in the Federal Register on Monday, May 17. The Docket ID is DoD-2021-OS-0036.

SECTION 2: PII RISK REVIEW

a. What PII will be collected *(a data element alone or in combination that can uniquely identify an individual)***?** *(Check all that apply)*

[X] Biometrics	[X] Birth Date	[ ] Child Information
[X] Citizenship	[ ] Disability Information	[X] DoD ID Number
[ ] Driver's License	[ ] Education Information	[ ] Emergency Contact
[X] Employment Information	[ ] Financial Information	[X] Gender/Gender Identification
[X] Home/Cell Phone	[ ] Law Enforcement Information	[ ] Legal Status
[ ] Mailing/Home Address	[X] Marital Status	[ ] Medical Information
[ ] Military Records	[ ] Mother's Middle/Maiden Name	[X] Name(s)
[ ] Official Duty Address	[ ] Official Duty Telephone Phone	[ ] Other ID Number
[ ] Passport Information	[X] Personal E-mail Address	[ ] Photo
[X] Place of Birth	[ ] Position/Title	[ ] Protected Health Information (PHI)[1]
[ ] Race/Ethnicity	[ ] Rank/Grade	[ ] Religious Preference
[ ] Records	[X] Security Information	[X] Social Security Number (SSN) *(Full or in any form)*
[X] Work E-mail Address	[X] If Other, enter the information in the box below	

As well as information on SF 85, SF 85P and SF 86 and clearance/HSPD-12 eligibility information.

If the SSN is collected, complete the following questions.

(*DoD Instruction 1000.30 states that all DoD personnel shall reduce or eliminate the use of SSNs wherever possible. SSNs shall not be used in spreadsheets, hard copy lists, electronic reports, or collected in surveys unless they meet one or more of the acceptable use criteria.)*

(1) Is there a current DPCLTD approved SSN Justification on Memo in place?

[X] Yes [ ] No

If "Yes," provide the signatory and date approval. If "No," explain why there is no SSN Justification Memo.

The SSN Justification Memo signed April 26, 2018 by Michael V. Sorrento, DMDC Director, is currently pending revision and approval under DCSA. DCSA Privacy Office lead is Ms. Stephanie J. Courtney

(2) Describe the approved acceptable use in accordance with DoD Instruction 1000.30 "Reduction of Social Security Number (SSN) Use within DoD".

As required in DoDI 1000.30, the acceptable use for the Social Security Number (SSN) has been identified as 03, Security Clearance Investigation or Verification. The SSN is the single identifier that links all aspects of a security clearance investigation together. This use case is also linked to other Federal agencies that continue to use the SSN as a primary identifier.

(3) Describe the mitigation efforts to reduce the use including visibility and printing of SSN in accordance with DoD Instructoin 1000.30, "Reduction of Social Security Number (SSN) Use within DoD".

(4) Has a plan to eliminate the use of the SSN or mitigate its use and or visibility been identified in the approved SSN Justification request?

If "Yes," provide the unique identifier and when can it be eliminated?
If "No," explain.

[ ] Yes [X] No

Use of SSN is required for the case management function of DISS due to the background investigation requirements. Use of the SSN within DISS is for 'Security Clearance Investigation or Verification'. The SSN is the single identifier that links all aspects of a security clearance investigation together. This use case is also linked to other Federal agencies that continue to use the SSN as a primary identifier.

b. What is the PII confidentiality impact level[2]? [ ] Low [X] Moderate [ ] High

[1] The definition of PHI involves evaluating conditions listed in the HIPAA. Consult with General Counsel to make this determination.

[2] Guidance on determining the PII confidentiality impact level, see Section 2.5 "Categorization of PII Using NIST SP 800-122." Use the identified PII confidentiality impact level to apply the appropriate Privacy Overlay low, moderate, or high. This activity may be conducted as part of the categorization exercise that occurs under the Risk Management Framework (RMF). Note that categorization under the RMF is typically conducted using the information types described in NIST Special Publication (SP) 800-60, which are not as granular as the PII data elements listed in the PIA table. Determining the PII confidentiality impact level is

most effective when done in collaboration with the Information Owner, Information System Owner, Information System Security Manager, and representatives from the security and privacy organizations, such as the Information System Security Officer (ISSO) and Senior Component Official for Privacy (SCOP) or designees.

c. How will the PII be secured?

(1) Physical Controls. *(Check all that apply)*

- [x] Cipher Locks
- [x] Combination Locks
- [x] Key Cards
- [x] Security Guards
- [x] Closed Circuit TV (CCTV)
- [x] Identification Badges
- [x] Safes
- [x] If Other, enter the information in the box below

DCSA and other DoD component facilities housing these systems are protected by military or contract security personnel (guards). Physical entry to the facility is restricted by use of PIN accessible locks, video surveillance and the building is monitored 24 hours by guards. Physical accesses to rooms are controlled by combination lock, and by identification badges (swipe care systems, or similar security systems) which are issued only to authorized individuals.

Ensuring compliance with the Mission Assurance Category (MAC) II Sensitive Information Assurance (IA) security controls listed in Department of Defense Instruction (DoDI) 8500.2. If the DoDI has specific wording recommend placing here. In addition, the same for the NISPOM guidelines.

Each agency/company/Department is responsible for ensuring all physical controls are put in place regarding PII data. National Industrial Security Program Operating Manual (NISPOM) has guidelines that Industry follows.

(2) Administrative Controls. *(Check all that apply)*

- [x] Backups Secured Off-site
- [x] Encryption of Backups
- [x] Methods to Ensure Only Authorized Personnel Access to PII
- [x] Periodic Security Audits
- [x] Regular Monitoring of Users' Security Practices
- [ ] If Other, enter the information in the box below

(3) Technical Controls. *(Check all that apply)*

- [ ] Biometrics
- [x] Common Access Card (CAC)
- [x] DoD Public Key Infrastructure Certificates
- [x] Encryption of Data at Rest
- [x] Encryption of Data in Transit
- [x] External Certificate Authority Certificates
- [x] Firewall
- [x] Intrusion Detection System (IDS)
- [x] Least Privilege Access
- [x] Role-Based Access Controls
- [ ] Used Only for Privileged (Elevated Roles)
- [x] User Identification and Password
- [x] Virtual Private Network (VPN)
- [ ] If Other, enter the information in the box below

Records and case files are maintained on a DoD network accessible only to authorized personnel with proper SCI clearance. Access to records/case files are limited to only those person(s) responsible for reviewing/analyzing the record in the performance of their official duties and who are properly trained and certified in Privacy and Civil Liberty matters and have a need-to-know. Access to computerized data is restricted by passwords, which are changed periodically.

d. What additional measures/safeguards have been put in place to address privacy risks for this information system or electronic collection?

Access to personal information is restricted to those who require the records in the performance of their official duties, who are appropriately screened, investigated, and determined eligible for access. Access to personal information is further restricted by the use of Personal Identity Verification (PIV) cards for JVS and CATS. Access to self-report information by the subject is available by the use of a PIV. Physical entry is restricted by the use of locks, guards, and administrative procedures. All individuals granted access to this system of records are to have taken annual Information Assurance and Privacy Act training; and all have been through the information technology and/or security clearance eligibility process.