PRIVACY IMPACT ASSESSMENT (PIA)

For the

Defense Information System for Security (DISS)
Defense Manpower Data Center

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☐ (2) Yes, from Federal personnel* and/or Federal contractors.

☒ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

- ☐ **New DoD Information System**
- ☐ **New Electronic Collection**
- ☒ **Existing DoD Information System**
- ☐ **Existing Electronic Collection**
- ☐ **Significantly Modified DoD Information System**

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

- ☒ **Yes, DITPR** Enter DITPR System Identification Number: 1640
- ☐ **Yes, SIPRNET** Enter SIPRNET Identification Number:
- ☐ **No**

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

- ☒ **Yes**
- ☐ **No**

If "Yes," enter UPI 007-000000594

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. 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 should be consistent.

- ☒ **Yes**
- ☐ **No**

If "Yes," enter Privacy Act SORN Identifier DMDC 24 DoD

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date. 3/29/16

e. Does this DoD information system or electronic collection have an 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.

☒ **Yes**

Enter OMB Control Number	3206-0032
Enter Expiration Date	March 31, 2017

☐ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) 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) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect 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) 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 should 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.

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly 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.

DISS consists of two applications, the Case Adjudication Tracking system (CATS) and the Joint Verification System (JVS). 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).

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.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

Risks include unauthorized access to records or the improper handling, transmission or use of records by those authorized access to the records contained within DISS, which could result in personal or professional harm to an individual.

Access to personal information within DISS is restricted to those who have an established need-to-know in the performance of their official duties, who are appropriately screened, investigated and determined to be eligible for access. Access to personal information is further restricted by the use of Personal Identity Verification (PIV) cards for JVS and CATS. Physical entry is restricted by the use of locks, guards and administrative procedures.

All individuals granted access to these records have completed annual Privacy Act and Information Assurance training.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☒ **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)

☒ **Other DoD Components.**

Specify. U.S. Army; U.S. Air Force; U.S. Navy; U.S. Marine Corps; and Guard/Reserve Components

☒ **Other Federal Agencies.**

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.

☒ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

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. Do individuals have the opportunity to object to the collection of their PII?

☒ **Yes** ☐ **No**

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

Information provided by individuals for a security clearance is voluntary. However, the Department may not be able to complete an investigation, or complete it in a timely manner, if the individual does not provide the necessary information.

(2) If "No," state the reason why individuals cannot object.

j. Do individuals have the opportunity to consent to the specific uses of their PII?

☒ **Yes** ☐ **No**

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

By completing the SF 85, SF 85P and SF 86, individuals are consenting to the specific uses of their PII.

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

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒ **Privacy Act Statement** ☐ **Privacy Advisory**

☐ **Other** ☐ **None**

Describe each applicable format.

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

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.

SECTION 3: PIA QUESTIONNAIRE and RISK REVIEW

a. For the questions in subparagraphs 3.a.(1) through 3.a.(5), indicate what PII (a data element alone or in combination that can uniquely identify an individual) will be collected and describe the source, collection method, purpose, and intended use of the PII.

(1) What PII will be collected? Indicate all individual PII or PII groupings that apply below.

☒ Name	☒ Other Names Used	☒ Social Security Number (SSN)
☐ Truncated SSN	☐ Driver's License	☒ Other ID Number
☒ Citizenship	☐ Legal Status	☒ Gender
☐ Race/Ethnicity	☒ Birth Date	☒ Place of Birth
☒ Personal Cell Telephone Number	☒ Home Telephone Number	☒ Personal Email Address
☐ Mailing/Home Address	☐ Religious Preference	☒ Security Clearance
☐ Mother's Maiden Name	☐ Mother's Middle Name	☐ Spouse Information
☒ Marital Status	☒ Biometrics	☐ Child Information
☐ Financial Information	☐ Medical Information	☐ Disability Information
☐ Law Enforcement Information	☒ Employment Information	☐ Military Records
☐ Emergency Contact	☐ Education Information	☒ Other

If "Other," specify or explain any PII grouping selected.	As well as information on SF 85, SF 85P and SF 86 and clearance/HSPD-12 eligibility information.

(2) What is the source for the PII collected (e.g., individual, existing DoD information systems, other Federal information systems or databases, commercial 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.

(3) How will the information be collected? Indicate all that apply.

☐	**Paper Form**	☐	**Face-to-Face Contact**
☐	**Telephone Interview**	☐	**Fax**
☐	**Email**	☒	**Web Site**
☒	**Information Sharing - System to System**		
☐	**Other**		

If "Other," describe here.

(4) Why are you collecting the PII selected (e.g., verification, identification, authentication, data matching)?

DISS implements the provisions and requirements of DoD 5200.2-R “DoD Personnel Security Program.” This thereby enables DoD Security Managers to more efficiently and effectively review an individual’s eligibility for access to classified and/or national security information prior to granting access.

(5) What is the intended use of the PII collected (e.g., mission-related use, administrative use)?

Mission-related. Information within DISS is used by 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.

b. Does this DoD information system or electronic collection create or derive new PII about individuals through data aggregation? (See Appendix for data aggregation definition.)

☐ **Yes** ☒ **No**

If "Yes," explain what risks are introduced by this data aggregation and how this risk is mitigated.

c. Who has or will have access to PII in this DoD information system or electronic collection? Indicate all that apply.

☒ **Users** ☒ **Developers** ☒ **System Administrators** ☒ **Contractors**

☐ **Other**

All users, developers, system administrators and contractors must possesses the required security clearance, and be authorized and appropriately vetted by their organization before gaining access to the DISS system.

d. How will the PII be secured?

(1) Physical controls. Indicate all that apply.

☒	**Security Guards**	☒	**Cipher Locks**
☒	**Identification Badges**	☐	**Combination Locks**
☐	**Key Cards**	☐	**Closed Circuit TV (CCTV)**
☐	**Safes**	☐	**Other**

Ensuring compliance with the Mission Assurance Category (MAC) II Sensitive Information Assurance (IA) security controls listed in Department of Defense Instruction (DoDI) 8500.2.

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) Technical Controls. Indicate all that apply.

☒	**User Identification**	☐	**Biometrics**
☐	**Password**	☒	**Firewall**
☒	**Intrusion Detection System (IDS)**	☒	**Virtual Private Network (VPN)**
☒	**Encryption**	☒	**DoD Public Key Infrastructure Certificates**
☒	**External Certificate Authority (CA) Certificate**	☒	**Common Access Card (CAC)**
☐	**Other**		

(3) Administrative Controls. Indicate all that apply.

☒ **Periodic Security Audits**

☒ **Regular Monitoring of Users' Security Practices**

☒ **Methods to Ensure Only Authorized Personnel Access to PII**

☒ **Encryption of Backups Containing Sensitive Data**

☒ **Backups Secured Off-site**

☐ **Other**

e. Does this DoD information system require certification and accreditation under the DoD Information Assurance Certification and Accreditation Process (DIACAP)?

☒ **Yes. Indicate the certification and accreditation status:**

☒	**Authorization to Operate (ATO)**	**Date Granted:**	19 Aug 2015
☐	**Interim Authorization to Operate (IATO)**	**Date Granted:**	
☐	**Denial of Authorization to Operate (DATO)**	**Date Granted:**	
☐	**Interim Authorization to Test (IATT)**	**Date Granted:**	

☐ **No, this DoD information system does not require certification and accreditation.**

f. How do information handling practices at each stage of the "information life cycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individuals' privacy?

Collection:

Use: Use of information within the DISS family of applications requires need-to-know and CAC/PIV card to access information.

Retention/Destruction: DISS has a NARA approved record retention - 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

For OPM FIS investigative reports within CATS, those records will be maintained in accordance with General

Records Schedule 18 part 22 (a), and destroyed upon notice of death or not later than 5 years after the subject has separated/transferred.

Processing: DISS data can only be accessed by appropriately vetted employees.

Disclosure: Information is only disclosed to those external agencies listed in the Routine Use section and those within the DoD with an established need-to-know in the performance of their official duties.

g. For existing DoD information systems or electronic collections, what measures have been put in place to address identified privacy risks?

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.

h. For new DoD information systems or electronic collections, what measures are planned for implementation to address identified privacy risks?

N/A

SECTION 4: REVIEW AND APPROVAL SIGNATURES

Prior to the submission of the PIA for review and approval, the PIA must be coordinated by the Program Manager or designee through the Information Assurance Manager and Privacy Representative at the local level.

Program Manager or Designee Signature	LIU.JOHN.H.1260864382 Digitally signed by LIU.JOHN.H.1260864382 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=DODHRA, cn=LIU.JOHN.H.1260864382 Date: 2016.04.05 18:10:57 -07'00'
Name:	John H. Liu
Title:	Division Director, Personnel Security and Assurance Division
Organization:	Defense Manpower Data Center
Work Telephone Number:	831-583-2400
DSN:	
Email Address:	John.H.Liu.civ@mail.mil
Date of Review:	
Other Official Signature (to be used at Component discretion)	LANGLEY.SANDRA.M.1229729272 Digitally signed by LANGLEY.SANDRA.M.1229729272 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=DODHRA, cn=LANGLEY.SANDRA.M.1229729272 Date: 2016.04.05 18:35:59 -04'00'
Name:	Sandra M. Langley
Title:	Project Manager, DISS
Organization:	Defense Manpower Data Center
Work Telephone Number:	571-372-1079
DSN:	
Email Address:	Sandra.M.Langley.Civ@mail.mil
Date of Review:	04/05/2016

Other Official Signature (to be used at Component discretion)

PETERSON.SAMUEL.MARKEE.1288769903

Digitally signed by PETERSON.SAMUEL.MARKEE.1288769903
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=DODHRA, cn=PETERSON.SAMUEL.MARKEE.1288769903
Date: 2016.05.02 15:28:03 -07'00'

Name:	Samuel M. Peterson
Title:	Chief, Privacy and FOIA Branch
Organization:	Defense Manpower Data Center
Work Telephone Number:	831-583-2400
DSN:	
Email Address:	Samuel.M.Peterson2.civ@mail.mil
Date of Review:	

Component Senior Information Assurance Officer Signature or Designee

ONGARO.RICKY.LEE.1266916554

Digitally signed by ONGARO.RICKY.LEE.1266916554
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=DODHRA, cn=ONGARO.RICKY.LEE.1266916554
Date: 2016.05.02 15:39:51 -07'00'

Name:	Rick L. Ongaro
Title:	Director, Information and Assurance Division
Organization:	Defense Manpower Data Center
Work Telephone Number:	831-583-2400
DSN:	
Email Address:	Ricky.L.Ongaro.Civ@mail.mil
Date of Review:	

Component Privacy Officer Signature

HALABUK.VIKI.L.1263083470

Digitally signed by HALABUK.VIKI.L.1263083470
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=WHS, cn=HALABUK.VIKI.L.1263083470
Date: 2016.03.30 15:48:15 -04'00'

Name:	Viki L. Halabuk
Title:	Senior Privacy Analyst
Organization:	OSD/JS Privacy Office
Work Telephone Number:	571-372-0408
DSN:	
Email Address:	Viki.L.Halabuk.civ@mail.mil
Date of Review:	03/30/2016

Component CIO Signature (Reviewing Official)	HOFFMAN.KRIS.L.1230543697 Digitally signed by HOFFMAN.KRIS.L.1230543697 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=DODHRA, cn=HOFFMAN.KRIS.L.1230543697 Date: 2016.06.03 14:47:31 -07'00'
Name:	Kris L. Hoffman
Title:	Chief Information Officer
Organization:	Defense Manpower Data Center
Work Telephone Number:	831-583-2400
DSN:	
Email Address:	Kris.L.Hoffman.Civ@mail.mil
Date of Review:	3 June 2016

Publishing:

Only Sections 1 and 2 of this PIA will be published. Each DoD Component will maintain a central repository of PIAs on the Component's public Web site. DoD Components will submit an electronic copy of each approved PIA to the DoD CIO at: pia@osd.mil.

If the PIA document contains information that would reveal sensitive information or raise security concerns, the DoD Component may restrict the publication of the assessment to include Sections 1 and 2.

APPENDIX

Data Aggregation. Any process in which information is gathered and expressed in a summary form for purposes such as statistical analysis. A common aggregation purpose is to compile information about particular groups based on specific variables such as age, profession, or income.

DoD Information System. A set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes automated information system (AIS) applications, enclaves, outsourced information technology (IT)-based processes and platform IT interconnections.

Electronic Collection. Any collection of information enabled by IT.

Federal Personnel. Officers and employees of the Government of the United States, members of the uniformed services (including members of the Reserve Components), and individuals entitled to receive immediate or deferred retirement benefits under any retirement program of the United States (including survivor benefits). For the purposes of PIAs, DoD dependents are considered members of the general public.

Personally Identifiable Information (PII). Information about an individual that identifies, links, relates or is unique to, or describes him or her (e.g., a social security number; age; marital status; race; salary; home telephone number; other demographic, biometric, personnel, medical, and financial information). Also, information that can be used to distinguish or trace an individual's identity, such as his or her name; social security number; date and place of birth; mother's maiden name; and biometric records, including any other personal information that is linked or linkable to a specified individual.

Privacy Act Statements. When an individual is requested to furnish personal information about himself or herself for inclusion in a system of records, providing a Privacy Act statement is required to enable the individual to make an informed decision whether to provide the information requested.

Privacy Advisory. A notification informing an individual as to why information is being solicited and how such information will be used. If PII is solicited by a DoD Web site (e.g., collected as part of an email feedback/ comments feature on a Web site) and the information is not maintained in a Privacy Act system of records, the solicitation of such information triggers the requirement for a privacy advisory (PA).

System of Records Notice (SORN). Public notice of the existence and character of a group of records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. The Privacy Act of 1974 requires this notice to be published in the Federal Register upon establishment or substantive revision of the system, and establishes what information about the system must be included.