PRIVACY IMPACT ASSESSMENT (PIA)

For the

Secure Access (SA)
Defense Threat Reduction Agency

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	8646
☐	**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 007-97-05-08-02-0042-04

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 HDTRA 007

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. December 4, 2009

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

Enter Expiration Date

☒ **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.

42 U.S.C. 2165 The Atomic Energy Act of 1954
50 U.S.C. 797, The Internal Security Act of 1950
E.O. 10450, "Security Requirements for Government Employees," April 27, 1953, as amended
E.O. 12958 "Classified National Security Information," April 17, 1995, as amended
E.O. 9397, "Numbering System for Federal Accounts Relating to Individual Persons," November 22, 1943.

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.

For use by officials and employees of the Defense Threat Reduction Agency (DTRA) in the performance of their official duties related to determining the eligibility of individuals for access to classified information, access to buildings and facilities, or to conferences over which DTRA has security responsibility.

The system includes: Name; Social Security Number; date and place of birth; citizenship; grade/rank, service; organization, security clearance-related information; vehicle ID and decal number; picture identification; correspondence concerning adjudication/passing of clearances/accesses; identifies security managers and personnel authorized to request area access/badge/local area network.

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

Potential of mishandling privacy information is low. DTRA has a mandatory requirement tracked by the DTRA Learning Management System (LMS) for all individual's to complete Privacy Act Training. System access is monitored by system administrators and routinely checked for requirements of access. All users of the system are required to justify their access via their supervisor and digitally sign an acknowledge statement about the sensitivity of the data they will have access to.

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. Security and Counterintelligence Staff

☒ **Other DoD Components.**

Specify. Security and Counterintelligence Staff

☒ **Other Federal Agencies.**

Specify. Security and Counterintelligence Staff

☒ **State and Local Agencies.**

Specify. Law enforcement

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

Specify. Contractors have access to the information when required by contract performance requirements. When this is the case, applicable provisions as required by Federal Acquisition Regulations (FAR) 24.1, Protection of Individual Privacy, are included in the contract.

☐ **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.

Individuals can object to the collection of information in identifiable form about themselves before completing the appropriate DTRA forms. Information on individuals is obtained from various forms to include DTRA Form 10 (Request for Security Clearance/Access Verification); DTRA Form 3 (Request for Badge and Local Area Network); and the Request for Authorized Access (RFAA) sent by individual's owning organization; and from the DoD personnel security migration system, Joint Personnel Adjudication System (JPAS). Failure to provide the requested information may result in denial of the accesses requested.

(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.

DTRA Forms 3 and 10 have a Privacy Act statement detailing the authority, purpose, routine use, and the impact of an individual's voluntary disclosure of the personally identifiable information. These forms require the individual's signature, thereby granting consent. Failure to provide consent may result in denial of the accesses requested.

(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.	All forms (see answer to question j, Section 2 above) used to populate SA have a Privacy Act Statement and Advisory on them. Additionally, all reports printed from SA have a Privacy Act Statement and Advisory. Information given to an individual will be printouts of the appropriate screen displays. When the initial data collection occurred upon entry into the Federal civil service or one of the U.S. military services, or a request for a security clearance was submitted, there was a Privacy Act Statement on the forms(s) that listed the Authority, Principal Purpose for Soliciting the Information, Routine Uses, and Whether Disclosure is Voluntary or Mandatory.

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.