PRIVACY IMPACT ASSESSMENT (PIA)

For the

DTRA1
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	Hosted on 4301 (UNET)
☐	**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 Included in investment 007-000003828

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 013

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.

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.

5 U.S.C. 301, Departmental Regulations; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; and E.O. 9397 (SSN).

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.

DTRA1 uses Microsoft SharePoint technology to provide an internal Web site for worldwide use by DTRA employees on the DTRA unclassified network. DTRA1 offers technologies that provide users with tools and applications for organizing, storing, sharing, routing, and collaborating unclassified mission information. The primary capabilities are described below.

DTRA implemented the use of SharePoint My Profile to ensure accurate employee business data (name, office phone, cubicle, grade, photograph, etc.) are easily accessible from a central location for all employees to promote collaboration and enhance customer service.

Human Resources Directorate (HR) Military Awards, Civilian Awards, and Military Evaluations applications use DTRA1 to store, organize, collaborate, route, and track award/evaluation documents. The applications process and/or store the following fields: name, rank/grade, award amount, service, specialty, SSN, UIC-PASS Office, Location, Position, ETS, Arrival Date Departure Date.

The Enterprise Information System (EIS) is a Government off-the-shelf (SharePoint-based) application to improve the ability of DTRA to control unclassified assignments and correspondence, document actions taken, and locate records for reference purposes. The application is used to initiate, manage, and track assignments coming from outside DTRA as well as those generated within DTRA at the Director, Deputy Director, Executive Director, Chief of Staff, or Directorate-to-Directorate level. Current policy prohibits uploading PII-containing documents into EIS. However archived records may contain PII within correspondence or supporting documents.

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

Privacy risks to the individual associated with the collected PII are unauthorized access to the data or possible misuse of the data.

System Access Controls safeguard privacy. These access controls limit access to the application and/or specific functional areas of the application. These controls consist of privileges or permissions, general access, password control, and discretionary access control. Additionally, each user is associated with one or more permission roles. Each role provides specific privileges to a subset of the application contents. Users are granted only those privileges that are necessary for their job requirements. The same roles that protect the database tables also determine which features and menu items are enabled for the currently logged on user. All task and correspondence sites are created based on access level permissions set by the site creator to provide others the ability to view, add, change, or delete, as appropriate. Within these sites, the permissions can be set at the tasker, folder, or document level. The permission levels vary from Full control, Contribute, Modify Delete, and Read only.

Current policy prohibits users from uploading PII-containing documents into DTRA1. Further controls on the use of information collected by HR and EIS include the training of users on the assignment of permissions, authorized usage, and proper handling of PII data. Access to data is strictly limited to support personnel who are legally authorized to receive that information and have a need to see that information.

HR Application data is strictly limited to HR personnel who are legally authorized to receive/view the information and have a need to see the information. The following safeguards were implemented on the system housing the HR Application data:

1. Logical Separation of permissions
2. Logical Separation of Database
3. Transparent Database Encryption enabled for the individual databases that contain PII
4. The transport method of connection to the client must be https enabled using SSL3 or TLS1.X or greater

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. SharePoint My Profile sites can only be accessed by DTRA users. The HR Applications containing PII data are restricted to HR staff and limited to DTRA users with the need to know.

Tasks are created in EIS and assigned to a Directorate or Staff Office (D/SO). Once received by the D/SO, the task can be assigned further to action officers or another D/SO for a response.

☐ **Other DoD Components.**

Specify.

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

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

Specify.

☐ **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.

All personal data collected is voluntarily given by the individual. Forms that collect personal data maintained in this system contain a Privacy Act Statement, as required by 5 U.S.C. 552a(e)(3), allowing the individual to make an informed decision about providing the data. The statement advises the individual that the information provided is voluntary and provides the consequences of choosing not to participate with the information collection. Individuals may raise an objection with the DTRA Privacy Act Office during the data collection.

The individual initiates the collection and maintenance of his/her information for the purpose of travel, security, and personnel transactions. Release of this information is done with the individual's full cooperation and consent.

(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.

The individual grants consent by virtue of initiating the collection or maintenance of his/her information. The uses are normally for the purpose of travel, security, and personnel transactions. Withholding consent is accomplished by not initiating the collection of information. All personal data collected is voluntarily given by the individual. Forms that collect personal data for this electronic collection contain a Privacy Act Statement, as required by 5 U.S.C. 552a(e)(3), allowing the individual to make an informed decision about providing the data for the specific purpose of the collection.

(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.

Forms that collect personal data maintained in this system contain a Privacy Act Statement, as required by 5 U.S.C. 552a(e)(3), allowing the individual to make an informed decision about providing the data. The statement advises the individual that the information provided is voluntary and provides the consequences of choosing not to participate with the information collection.

Privacy Act Routine Uses are provided to individuals in writing for some of the DTRA forms they completed.

Individuals also sign an Authorization for Release of Information that details the purposes for which the data can be used. The Release remains valid for five years from the date of signature or until the individual has left DTRA.

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.