PRIVACY IMPACT ASSESSMENT (PIA)

For the

Cooperative Threat Reduction Reporting System (CTRRS) Network
Defense Threat Reduction Agency (DTRA)

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	9325
☐	**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 007-000001882

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

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. February 11, 2013

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.

1. Title 5 United States Code, Section 301 "Departmental Regulations"
2. 10 U.S.C. Chapter 157, Transportation
3. Department of Defense Joint Travel Regulations (Volume 2) and Joint Federal Travel Regulations (Volume 1)
4. 41 C.F.R Chapters 300-304, the Federal Travel Regulations
5. DoD Directive 4500.54E, "DoD Foreign Clearance Program (FCP)"

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.

The Cooperative Threat Reduction Reporting System (CTRRS) Network provides the backbone of information services needed to support information technology at the Cooperative Threat Reduction Support Center (CTRSC). These services include servers, storage, networking components, and software. CTRRS also hosts Web-based applications and tools. The applications and tools were created to support the DTRA Cooperative Threat Reduction (CTR) mission and facilitate collaboration and information sharing with CTR community and Federal contractors that support CTR. For example, CTRRS hosts a Web-based portal that supports CTR collaboration and knowledge sharing among DTRA, CTR partners, support contractors, and other entities. It will also host a database for processing mission trip information request(s). The database will help facilitate continental United States (CONUS) and outside the continental United States (OCONUS) travel documentation for personnel who support the CTR mission.

Data that may appear on the CTRRS network include information obtained during the conduct of official Government business, staged for administrative purposes, and incidental files containing PII that may be stored on the network. The PII is either associated with the individual who created the file (e.g., a request for some consideration) or files created by individuals in the course of routine administrative and mission support operations. This could include PII such as an individual's full name, organization, travel documentation, and contact information.

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

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

Technical safeguards including system access controls and network monitoring safeguard privacy. Access controls consist of role-based access controls that limit access to the CTRRS network and the hosted systems. Each role provides a combination of privileges to a subset of the network or system contents and functional areas. Users are granted only those privileges that are necessary to perform their job duties. Role-based access controls also determine which capabilities of an application are available to a user. CTRRS Network activity is monitored by the DTRA Network Operations Center for any suspicious activity on the network.

Before receiving access to the CTRRS network, users are required to go through a new account approval process. In addition, new users must take the DoD Information Assurance Awareness training course and the DoD Personally Identifiable Information training course. This training is required annually thereafter. Periodic briefings that address additional training are conducted during CTR all-hands meetings.

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. PII is shared during the conduct of official Government business with those with a need to know. It is shared within DTRA for reporting CTR mission-related activities and to ensure that trip information and documentation align with CONUS and OCONUS travel requirements per DoD and CTR policy and international agreements.

☒ **Other DoD Components.**

Specify. PII is shared during the conduct of official Government business with other

DoD components that have a need to know. Information will be shared via hard copy or manual data entry by an authorized CTR user into other DoD Component systems. It is shared for CTR mission-related activities with involved DoD components and offices including:

Deputy Assistant Secretary of Defense for Threat Reduction and Arms Control is provided with country clearance requests and travel letters to ensure alignment with existing agreements.

Office of the Secretary of Defense (OSD) is informed of country clearance requests and travel letters for compliance with OSD requirements.

Office of General Counsel is informed of country clearance requests and travel letters for legal requirements.

Aircraft and Personnel Automated Clearance System (APACS) is mandatory for all DoD travelers and DoD sponsored travel clearance requests. Trip fulfillment information (including PII) from the database hosted on the CTRRS network is manually entered into the APACS system.

☒ **Other Federal Agencies.**

Specify. PII is shared with the Department of State (DoS) during the conduct of official Government business for reporting purposes of CTR mission-related activities with which the DoS is involved. DoS is provided with country clearance requests and travel letters for review per DoS policies and guidance. Country clearance information may be entered into the DoS Electronic Country Clearance system, a DoS personnel travel request and approval system used by agencies whose in-country (foreign) approval is provided by a DoS Embassy.

☐ **State and Local Agencies.**

Specify.

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

Specify. PII is shared during the conduct of official Government business to CTR Advisory and Assistance Services (A&AS) contractors and Integrated contractors that have a contractual requirement and need to know. It is shared for reporting purposes of CTR mission-related activities with which CTR A&AS contractors and Integrated contractors are involved. In addition, CTR A&AS contractors enter country clearance requests into APACS. Integrated contractors that provide in-country (foreign) logistical support (e.g., hotel bookings, ground transportation, interpreters) receive trip itinerary information to ensure travelers have appropriate lodgings, transportation, etc.

Contractors must follow the applicable provisions as required by Federal Acquisition Regulations (FAR) 24.1, Protection of Individual Privacy.

☐ **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.

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

There are no automated means by which individuals can object to the collection of their PII. Completion of the requested information indicates consent. Individuals must object to the collection of PII about themselves verbally or informally via written means (i.e., an e-mail to their Program Manager), before engaging in the activity that requires PII collection.

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.

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

In some cases, a document may be compiled and saved on the CTRRS Network without the specific knowledge or consent of the affected individuals as part of ongoing Government and contractor operations that may involve the affected individuals; e.g., documented meeting minutes and after-action review documents that contain participant information. In these cases, individuals would not be given the opportunity to consent to the specific uses of their PII. An individual's use of the Automated Trip Request Information Process (ATRIP) database by entering their PII signifies consent to the specific uses of the PII.

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.	At present no PII is collected on the CTRRS network. Proper headers and footers, including a Privacy Act Statement, will be displayed in the future ATRIP database hosted on the CTRRS Network, and at the top of the page immediately under the title of any printed materials. The CTRRS Network may contain incidental PII as a general support system for CTR support contractors and Government personnel. If PII is derived from other official sources or records, a Privacy Act Statement or Privacy Advisory may have been provided to the individual. It is anticipated that the uses of the PII are covered by the original statements/advisories and are within the bounds of the purposes of the original sources. Other PII documented in the course of conducting official business are for administrative purposes and have no associated Privacy Act Statements or Privacy Advisories.

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.