PRIVACY IMPACT ASSESSMENT (PIA)

For the

Operations Center Emergency Notification and Recall System
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: 8447
- ☐ **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 007-000001892

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 HDTRA024

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, Department Regulations; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; Executive Order 9397, Numbering System for Federal Accounts Relating to Individual Persons [SSNs]; Executive Order 12656, Assignment of Emergency Preparedness Responsibilities; Presidential Decision Directive 67, Enduring Constitutional Government and Continuity of Government Operations; Federal Preparedness Circular 65, Federal Executive Branch Continuity of Operations; and DTRA/SCC-WMD Instruction 1424.1, Emergency Dismissal or Closure Procedures.

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 Operations Center Emergency Notification and Recall System resides on one of DTRA's unclassified local area network enclaves and allows direct support to the Operations Center (OC) for unclassified processing. These records support Agency requirements for personnel emergency notification, establishment of locator listings, and other official management functions where personnel and organizational point-of-contact information is required.

The type of personal information collected includes: individual's name, emergency contact information, organizational and home address, work and home telephone numbers, electronic mail, facsimile, cellular and pager numbers, and related information. Information is organized into emergency personnel rosters, contact listing files, organizational telephone directories, and listings of office personnel.

(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, general access, password control, Public Key Infrastructure (PKI), and discretionary access control. Additionally, each user is associated with one or more roles. Each role provides a combination of privileges to a subset of the database 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 buttons and menu items are enabled for the user currently logged on.

Further controls on using information within the OC include training users on the authorized use and proper handling of the PII data. Recall data access is strictly limited to DTRA OC personnel and system administrators who are legally authorized to receive that information and have a need to see that information.

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. Provided at DTRA Senior Leadership request to DTRA Senior Leadership by the Operations Center Watch Officer.

☐ **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.

Civilian employees who decline to provide contact information do so in writing in accordance with DTRA/ SCC-I Instruction 3020.1, Alert, Notification, and Recall Techniques, Policy, and Procedures.

(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.

Civilian employees who do not consent to DTRA using their contact information for recall and emergency purposes may opt out in writing in accordance with DTRA/SCC-I Instruction 3020.1, Alert, Notification, and Recall Techniques, Policy, and Procedures.

(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 and DTRA/SCC-I Instruction 3020.1, Alert, Notification, and Recall Techniques, Policy, and Procedures. Employee contact information will be only retained and used for recall and emergency notifications and maintained in an access-controlled system. This information is not for public release and is only for internal Agency use.

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.