



PRIVACY IMPACT ASSESSMENT (PIA)

For the

DTRA Unclassified Network (UNET)

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
- Existing DoD Information System
- Significantly Modified DoD Information System
- New Electronic Collection
- Existing Electronic Collection

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
- 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

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.

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.

This PIA does not cover a system that collects, uses, maintains, disseminates or processes PII. Systems connected to the UNET that are specifically structured to collect, use, maintain, disseminate or process PII are covered by separate PIA. This PIA covers incidental unstructured files containing PII that are stored on the unclassified network storage and used by individual employees and on-site contractors in the course of routine performance of their duties. The PII is either associated with the individual creating the file (e.g., a request for some consideration, leave requests, etc.) or working files created by individuals in the course of routine agency administrative and mission support operations.

The authorities for gathering the PII in any given file would be specific to that file, and are generally enumerated in the separate PIA's for the several information systems that gather and process that data.

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.

This PIA is to cover unstructured PII data that is found in working files created by government and support contractor personnel in the course of day-to-day business operations that is not associated with a specific database or information system. It covers incidental PII that may be included in individually prepared document files such as word processing documents, e-mails, and spreadsheets that are prepared by government and contractor personnel during the course of performing their routine duties. They are typically one-time documents or specialized personal lists or requests (e.g., contacts, rosters, e-mails, meeting attendance lists, leave requests, personnel-related matters, etc.) used by individuals or small work groups in the course of conducting internal government operations. The files may be placed in shared network directories to which personnel in addition to the creator of the file have access, or stored in the creators private storage space.

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

The primary risk is unauthorized access to or disclosure of the information to or by personnel who may have access to the shared storage directories who do not have a need to access the specific PII in the document. The primary control on the risk is the individuals who create the document, control distribution, and place it in the network storage. This risk is addressed through training of personnel in the handling of PII, and through providing technical means (encryption and access control) to control access to the documents.

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.

Government personnel who may have access to the network shared directory that contains the file containing the PII will have opportunity to see such PII and may be contained in the files in that directory.

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.

Contractor personnel who may have access to the network shared directory that contains the file containing the PII will have opportunity to see such PII and may be

contained in the files in that directory.

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.

If the document containing the PII was created in collaboration with the individual, the individual may have the opportunity to decline providing the PII.

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

In some cases the document may be compiled without the specific knowledge or consent of the effected individuals as part of on-going government operations that may involve the effected individuals; e.g., performance appraisal preparation.

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.

If the document containing the PII was created in collaboration with the individual, the individual has the opportunity to decline providing the PII.

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

In some cases the document may be compiled without the specific knowledge or consent of the effected individuals as part of on-going government operations that may involve the effected individuals; e.g., performance appraisal preparation.

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

- | | |
|--|---|
| <input checked="" type="checkbox"/> Privacy Act Statement | <input checked="" type="checkbox"/> Privacy Advisory |
| <input checked="" type="checkbox"/> Other | <input checked="" type="checkbox"/> None |

Describe each applicable format.

If the PII is derived from other official sources or records, a Privacy Act Statement or Privacy Advisory may have been provided to the individual. Since this is a general use system that may contain incidental PII, it is anticipated that the uses of the PII covered by this statement are within the bounds of the purposes of the original sources.

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.