



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Facility Access Control Network (FACNet)
--

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.

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," as amended
E.O. 12958 "Classified National Security Information," as amended
E.O. 9397, "Numbering System for Federal Accounts Relating to Individual Persons," (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.

This enclave includes a local area network and commercial-off-the-shelf (COTS) application software that supports multiple access readers, access cards/badges, video cameras, workstations, servers, and security alarms. It tracks and maintains a variety of personal and vehicle data that is collected and maintained so it can be used to determine and give an individual access into DTRA-managed facilities and spaces; to verify security clearance status of individuals requiring entry into restricted access areas; to account for building occupants and to effect efficient evacuation during simulated and actual threat conditions; to relay threat situations and conditions to DoD law enforcement officials for investigative or evaluative purposes; and to notify emergency points of contact of situations affecting a member of the workforce. The system contains documents relating to requests for and issuance of facility entry badges and passes and motor vehicle registration. The records contain the individual's name; Social Security Number (SSN); physical and electronic duty addresses; physical and electronic home addresses; duty and home telephone numbers; emergency-essential status; date and place of birth; citizenship; badge number, type of badge, badge issue and expiration dates; facility identification and user codes and dates and times of building entry; current photograph; physical descriptors such as height, hair and eye color; blood type; fingerprint data; handicap data; security clearance data; personal vehicle description to include year, make, model, and vehicle identification number; state tag data; operator's permit data; inspection and insurance data; vehicle decal number, parking lot assignment; parking infractions; the fact of participation in mass transit programs; and emergency contact data.

(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 disclosure. All personnel that have access to the PII data base receive annual training on the use, handling and safeguarding of PII.

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.

Officials and employees in the performance of their official duties related to the screening and selection of individuals for security clearances and/or special authorizations, access to facilities or attendance at conferences

Other DoD Components.

Specify.

Officials and employees of other DoD components in the performance of their official duties related to the screening and selection of individuals for security clearances and/or special authorizations, access to facilities or attendance at conferences,

Other Federal Agencies.

Specify. Officials and employees of other Government agencies in the performance of their official duties related to the screening and selection of individuals for security clearances and/or special authorizations, access to facilities or attendance at conferences

State and Local Agencies.

Specify.

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

Specify. Employees of Government contractors in the performance of their official duties related to the screening and selection of individuals for security clearances and/or special authorizations, access to facilities or attendance at conferences

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 accepting employment/assignment with the DTRA. Employment with the DTRA is contingent on the individual being able to obtain and maintain a valid security clearance. Failure to provide the information may preclude employment at DTRA.

(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.

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

This is a condition of employment at DTRA.

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 type="checkbox"/> Other | <input type="checkbox"/> None |

Describe each applicable format.

All forms and databases used to populate DTRA's FACNet have a Privacy Act Statement and Advisory on them. At initial sign on, a Privacy Act Statement appears on the FACNet screens. Additionally, all reports printed from DTRA's FACNet have a Privacy Act Statement and Advisory. Information given to an individual will be printouts of the appropriate screen displays. Information may be provided to a Preliminary Inquiry Officer or an Investigative Officer and will have the appropriate Privacy Act cover sheet.