



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Phantom Express Automated Access Control System

Army Installation Management Command, Fort Hood, Texas
--

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.

10 U.S.C. 3013, Secretary of the Army; Army Regulation 190-13, the Army Physical Security Program and E.O. 9397 (SSN) as amended.

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 Fort Hood Phantom Express system is an electronic entry control system that collects personal and vehicle information, which is employed to provide automated authentication and verification of personnel and vehicles entering the Fort Hood installation. The PE system will standardize and integrate identification, authorization, authentication, credentialing, and access into the Fort Hood installation.

The Phantom Express Automated Access Control System at Fort Hood, Texas provides enhanced installation force protection and security, it increases the safety for security forces and motorists, and it maintains traffic flow and gate capacity; all while reducing guard requirements and the costs associated with them.

The Phantom Express System has been developed to expedite, control, and manage entry into the Fort Hood installation through:

- Assuring positive personnel and vehicle identification.
- Granting or denying installation access to approved personnel and vehicles with a minimum of delay.
- Notification of unapproved access attempts.
- Enrollment of regular, full-time installation personnel and vehicles.
- Contractor, guest and visitor access enrollment.

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

The security requirements for the safe use, handling, storage and destruction of PII data is included in the training provided to PE operators, and is reinforced during routine checkups. The proper secure handling of reports is covered in PE standard operating procedures to prevent unintended exposure of data, and to preclude data loss. Reports printed out must be labeled "FOUO" when they contain Privacy Act data. PII awareness must be a sustained focus of the individual PE Site Managers and command sponsors; their daily management of the sites provides assurance against PII data compromise.

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 retained within the Phantom Express system on Fort Hood and is not exchanged with any other agency.

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.

The customer may object by declining to enroll in the Phantom Express System. The Army rules for accessing records, for contesting contents, and appealing initial agency determinations are contained in 32 CFR part 323, or may be obtained from the Fort Hood Police Administration Office, FOIA-PA Officer, Bldg 23020, Fort Hood, TX 76544, (254) 285-5060. Failure to provide the requested information will result in denial of an Access card or visitors pass and denial of entry to the Fort Hood installation and/or facilities.

(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 Army rules for accessing records, for contesting contents, and appealing initial agency determinations are contained in 32 CFR part 323, or may be obtained from the Fort Hood Police Administration Office, FOIA-PA Officer, Bldg 23020, Fort Hood, TX 76544, (254) 285-5060.

(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.

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

Describe each applicable format.

Privacy Act Statements, as required by 5 U.S.C 552a(e)(3), are provided at the collection point. The statement provides the following: collection purpose, authorities, external uses, the voluntary nature of the program, the fact that no consequences accrue for those who choose not to participate beyond denial of an Access card or visitors pass and denial of access to the installation and the name and number of the Privacy Act system notice governing the collection. The statement is included on paper and electronic collection forms. The Phantom Express Privacy Act Statement reads as follows:

AUTHORITY: Executive Order 9397; the Privacy Act of 1974, 5 U. S. C. 552a; DODD 8500.1

PRINCIPAL PURPOSE(S): To provide necessary information to the Fort Hood installation to determine if applicant meets access control requirements. Use of SSN is necessary to make positive identification of an applicant. Records in the Phantom Express system are maintained to support the Fort Hood physical security and information assurance programs and are used for identity verification purposes, to record personal property registered with the DoD, and for producing facility management reports. Used by security offices to monitor individuals accessing the Fort Hood installation and/or facilities. SSN, Drivers License Number, or other acceptable identification will be used to distinguish individuals who request entry to the Fort Hood installation and/or facilities.

ROUTINE USE(S): The "DoD Blanket Routine Uses" are set forth at the beginning of the DoD compilation of systems of records notices.

DISCLOSURE: Voluntary. However, failure to provide the requested information will result in denial of an Access card or visitors pass and denial of entry to the Fort Hood installation and/or facilities.

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.