



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Installation Access Control System - Drum

Department of the Army-Directorate of Emergency Services, Fort Drum, New York

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, as amended (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.

The Installation Access Control System - Drum (IACS) is a system developed by Defense ID and Fort Drum as a force protection program to manage personnel and installation access. It is a networked client/server database system designed to verify the access authorization of personnel entering the military installation by use of barcode technology. The Defense ID software application is used to enter personnel data into a database and retrieve that data for verification and validation at a later time. The program supports the adding, retrieving, updating, and displaying of information for individuals, who require access to Fort Drum. IACS enhances the military law enforcement mission by helping to provide a safe and secure community by allowing real time access to data. The program alerts installation gate guards to barred and suspended individuals and eliminates the need for cumbersome paper lists and manual checks which will allow for more timely processing while maintaining a safe and secure environment.

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

Risk: Userid/password used by someone other than who assigned.

Mitigation: Allocation of passwords is managed and password security policies enforced.

Risk: Mishandling of sensitive data, reports, or storage media.

Mitigation: Periodic assessments of access rights and privileges are performed.

Risk: Virus attacks and other malicious incidents.

Mitigation: System controls are predicated on preventing unauthorized users from accessing resources to minimize the risk presented by outside threats. The Installation Access Control System - Drum (IACS) will run on a closed network, and will not afford an outside threat the potential for system infiltration and compromise. Internal threat mitigation will occur through network and local server monitoring to detect, identify and prevent installation of malware, and by workstation audit and configuration validation/verification by the local site SSM. We will have training certification for operators and periodic audits of installed application and software/hardware components by SSM, which will minimize risk by assuring only authorized products are present, installed, and functioning in a manner consistent with DoD security policy.

Risk: PII data appears on certain reports.

Mitigation: The security requirements for the safe use, handling, storage and destruction of PII data is included in training. The proper secure handling of reports is covered in 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.

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.

Garrison Commander; Staff Judge Advocate; 902d Military Intelligence, Army Criminal Investigation Division, Army Inspector General

Other DoD Components.

Specify.

The "DoD Blanket Routine Uses" applies to IACS.

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.

Personnel can refuse to provide an approved identification at an access control point. Failure to provide an approved identification will result in the individual not being allowed entry onto Fort Drum.

(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.

Once the individual consented to the collection of PII they have given implicit consent to the specific uses of their PII by providing an approved identification at an access control point.

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 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 and the fact that no consequences accrue for those who chose not to participate beyond denial of access to the installation. The statement is included on paper and electronic collection forms. The Installation Access Control System Privacy Act Statement reads as follows:

AUTHORITY: 10 U.S.C. 3013, Secretary of the Army; Army Regulation 190-13, The Army Physical Security Program and Executive Order 9397, as amended (SSN).

PRINCIPAL PURPOSES(S): To provide necessary information to Fort Drum to determine if applicant meets access control requirements. Records in the Installation Access Control System are maintained to support Department of Defense physical security and are used for identity verification purposes, authentication of driving privileges, and for producing installation management reports. Used by security officers to monitor individuals accessing the installation. Name, SSN, date of birth, Drivers License Number, or other acceptable identification will be used to distinguish individuals who request entry to Fort Drum.

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 entry to Fort Drum.

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.

SECTION 3: PIA QUESTIONNAIRE and RISK REVIEW

a. For the questions in subparagraphs 3.a.(1) through 3.a.(5), indicate what PII (a data element alone or in combination that can uniquely identify an individual) will be collected and describe the source, collection method, purpose, and intended use of the PII.

(1) What PII will be collected? Indicate all individual PII or PII groupings that apply below.

- | | | |
|---|--|---|
| <input checked="" type="checkbox"/> Name | <input type="checkbox"/> Other Names Used | <input type="checkbox"/> Social Security Number (SSN) |
| <input checked="" type="checkbox"/> Truncated SSN | <input checked="" type="checkbox"/> Driver's License | <input checked="" type="checkbox"/> Other ID Number |
| <input type="checkbox"/> Citizenship | <input type="checkbox"/> Legal Status | <input type="checkbox"/> Gender |
| <input type="checkbox"/> Race/Ethnicity | <input checked="" type="checkbox"/> Birth Date | <input type="checkbox"/> Place of Birth |
| <input type="checkbox"/> Personal Cell Telephone Number | <input type="checkbox"/> Home Telephone Number | <input type="checkbox"/> Personal Email Address |
| <input type="checkbox"/> Mailing/Home Address | <input type="checkbox"/> Religious Preference | <input type="checkbox"/> Security Clearance |
| <input type="checkbox"/> Mother's Maiden Name | <input type="checkbox"/> Mother's Middle Name | <input type="checkbox"/> Spouse Information |
| <input type="checkbox"/> Marital Status | <input type="checkbox"/> Biometrics | <input type="checkbox"/> Child Information |
| <input type="checkbox"/> Financial Information | <input type="checkbox"/> Medical Information | <input type="checkbox"/> Disability Information |
| <input type="checkbox"/> Law Enforcement Information | <input type="checkbox"/> Employment Information | <input type="checkbox"/> Military Records |
| <input type="checkbox"/> Emergency Contact | <input type="checkbox"/> Education Information | <input checked="" type="checkbox"/> Other |

If "Other," specify or explain any PII grouping selected.

Hair color; eye color; Height; and Weight

(2) What is the source for the PII collected (e.g., individual, existing DoD information systems, other Federal information systems or databases, commercial systems)?

Data is collected from existing DoD databases, the Military Services, DoD Components, and from the individual.