



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Defense Manpower Data Center (DMDC) Defense Biometric Identification System (DBIDS) known in the EUCOM Area of Operations as the Installation Access Control System (IACS)

HQ U.S. Army Europe (HQ USAREUR)

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 3072 (DA08428)
- 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 007-97-01-15- 01-4035-00-403-254

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 DMDC 10 DoD

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. 113, Secretary of Defense; Directive-Type Memorandum (DTM) 09-012, Interim Policy Guidance for DoD Physical Access Control; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; DoD Directive 1000.25, DoD Personnel Identity Protection (PIP) Program; DoD Instruction 5200.08, Security of DoD Installations and Resources; DoD 5200.08-R, 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.

IACS electronically authenticates the identity of an authorized individual to verify their access authorization: FPCON, day, time of day, installation. IACS alerts registration personnel and installation gate guards to barred individuals, lost or stolen IDs, expired IDs, individuals wanted by law enforcement or individuals not authorized FPCON, day, time or installation.

Privately owned vehicle information includes name of vehicle manufacturer, model year, color and vehicle type, license plate number, and vehicle identification number (VIN).

The records support DoD physical security and information assurance programs, to issue individual facility/installation access credentials, and for identity verification purposes. The system also is used to record personal vehicles. Records are accessed by authorized personnel for law enforcement purposes.

IACS is a hardware/software-based personnel access verification system developed by the Defense Manpower Data Center (DMDC). IACS is a version of the Defense Biometric Identification System (DBIDS) that allows USAREUR to centrally manage installation access control. The system is networked USAREUR-wide and links all Installation Access Control Offices (IACO), MP Stations, and Access Control Points to a central database. With IACS, gate guards are able to scan all IACS-produced installation passes and DoD ID cards that are registered and verify access authorization from the central database. The system also enables the central restriction, amendment or cancellation of access privileges.

Personal information collected includes personal and employment.

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

IACS Registration/Gate Operations, computer monitors and paper forms placed and processed to prevent inadvertent viewing by unauthorized personnel.

Allocation of passwords is managed and password security policies enforced to minimize the possibility of loss of PII data on an individual basis by a compromise of userid and password. To initially access the IACS application, in addition to userid and password, a CAC/Teslin/Installation pass is scanned and a biometric fingerprint is used to authenticate an authorized users. When the screen save activates, a password is required to reenter the IACS application.

IACS runs on closed, encrypted NIPR network in the EUCOM AOR and prevents an outside threat or compromise (e.g. hacking/theft or virus attacks).

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.

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.

Voluntary. However, failure to provide the requested information will result in denial of an IACS installation pass, or short term visitors pass, or being allowed to be signed onto a U.S. military installation in the EUCOM AOR by an authorized individual.

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

N/A

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.

Voluntary. However, failure to provide the requested information will result in denial of an IACS installation pass. Host Nation citizens from Germany, for example sign a consent to collect personal information form called a "DATENSCHUTZERKLÄRUNG" prior to being issued an installation pass.

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

Describe each applicable format.

Host Nation citizens from Germany, for example sign a consent to collect personal information form (printed in German) called a "DATENSCHUTZERKLÄRUNG" prior to being issued an installation pass.

As required for U.S. Citizens, the Privacy Act Statement (below) is on IACS application forms Army in Europe (AE) Form 190-16a, APPLICATION FOR U.S. FORCES IN EUROPE INSTALLATION PASS and AE Form 190-16f, INSTALLATION ACCESS CONTROL SYSTEM (IACS) ACCESS-ROSTER REQUEST and also placed prominently at IACS registration offices and installation access control points (gates) where individuals are signed onto a military installation.

IACS PRIVACY ACT STATEMENT (For U.S. Citizens)
Authority: 5 USC 301 Departmental regulations; 10 USC 113, Secretary of Defense, Note at Pub. L. 106-65; 10 USC 136, Under Secretary of Defense for Personnel and Readiness; 18 USC 1029, Access Device Fraud; 18 USC. 1030, Computer Fraud; 40 USC Information Technology Management; 50 USC, Chapter 23, Internal Security; Pub. L. 103-398, Government Information Security Act; Pub. L. 100-235, Computer Security Act of 1987; Pub. L. 99-474, Computer Fraud and Abuse Act; EO 9397 (SSN).
Principal purpose(s): To identify personnel authorized routine or recurring access to installations under U.S. control.
Routine use(s): Those permitted under 5 USC 522a(b) of the Privacy Act and as specifically allowed outside the DOD pursuant to 5 USC 522a(b)(3) of the Privacy Act.
Disclosure: Voluntary; however, failure to provide any item of information will result in denial of entry onto U.S.-controlled installations.

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.