



PRIVACY IMPACT ASSESSMENT (PIA)

For the

FI U-ICAN - FORT IRWIN UNCLASSIFIED-INSTALLATION CAMPUS AREA
NETWORK

Fort Irwin Network Enterprise Center (NEC)

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.

DOD 8500.1, Cybersecurity, DODI 8510.01 Risk Management Framework for DoD Information Systems, AR 25-2 Information Assurance, Access Control Management Requirements collect Privacy Act information on system and to authorize access to information systems. Additionally AR 690-400 requires PII to be collected to support the civilian evaluation system requirements and AR 623-3 requires the collection of PII to support the Officer and NCOER evaluation system requirements.

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 IRWIN Unclassified/Classified Installation Campus Area Network (U-ICAN) provides unclassified and sensitive communications to the Fort IRWIN Garrison & Garrison tenant activities. The user workstations are primarily used to access email to include Army Knowledge On-Line (AKO), Department of Defense Information Network-Army (DoDIN-A), Enterprise Email, and other required unclassified websites. The FORT IRWIN U-ICAN environment covers the ICAN accreditation/authorization boundary. The U-ICAN is protected by physical security mechanisms, computer configurations (IAVA's, STIGS, AV, and HBSS), as well as environmental controls.

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

Minimal risk to personnel, DD Form 2875 contains minimum privacy information and completed forms are transmitted via secure network protocols, stored on encrypted drive segments and are only accessible to personnel with a need to know. Civilian Evaluations and OER/NCOER are processed on end user workstations with the capability to locally store and print copies of individual reports. Access restrictions are enforced by 2 factor authentication and the DoD PKI.

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.

With Security Managers and Cybersecurity personnel to approve and Systems Administrators to configure access to Information Systems, OERs and NCOERs are locally edited but centrally stored within the Army EES system. Civilian Evaluation report will be edited locally, transmitted and stored in the new DPMAP systems

Other DoD Components.

Specify.

With DISA when access to DISA system is required

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.

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

All DD Form 2875 entries are required before access to information systems can be authorized by DOD regulation, Active Duty and Civilian performance reports are mandatory for all civilians and active duty personnel.

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.

When Individuals sign the form requesting access they consent to the use as stated under the Privacy Act.

(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.

DD Form 2875 has Privacy Act Statement at the beginning of the first page. DPMAP and EES require the users to acknowledged the privacy act statement before accessing the systems.

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.