

PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

PIC U-ICAN - PICATINNY ARSENAL UNCLASSIFIED - INSTALLATION CAMPUS AREA NETWORK

2. DOD COMPONENT NAME:

United States Army

3. PIA APPROVAL DATE:

09/23/20

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: (Check one. Note: foreign nationals are included in general public.)

- From members of the general public From Federal employees and/or Federal contractors
- From both members of the general public and Federal employees and/or Federal contractors Not Collected (if checked proceed to Section 4)

b. The PII is in a: (Check one)

- New DoD Information System New Electronic Collection
- Existing DoD Information System Existing Electronic Collection
- Significantly Modified DoD Information System

c. Describe the purpose of this DoD information system or electronic collection and describe the types of personal information about individuals collected in the system.

The Picatinny Arsenal Unclassified ICAN (PIC U-ICAN) provides unclassified communications to the installation and tenant activities. User workstations are primarily used to access email to include Army Knowledge On-Line, Department of Defense Information Network-Army, Enterprise Email, and other websites. The PIC U-ICAN contains PII that is primarily collected to support user access requests. Other PII, such as personnel evaluations, personnel security clearances, and personnel resource management actions all utilize online databases and may be stored on individual user workstations and server shares on the ICAN.

d. Why is the PII collected and/or what is the intended use of the PII? (e.g., verification, identification, authentication, data matching, mission-related use, administrative use)

Verification & Authentication

e. Do individuals have the opportunity to object to the collection of their PII? Yes No

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object to the collection of PII.

All DD Form 2875 entries are required before access to information systems is authorized per DoD regulation.

f. 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.

When individuals sign the DD Form 2875 requesting access, they are consenting to the use as stated under the Privacy Act. When users login to personnel evaluation systems, DCPDS, or other DoD & Army websites to collect, use, or process PII, the user must acknowledge the Privacy Act Statement.

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. (Check as appropriate and provide the actual wording.)

- Privacy Act Statement Privacy Advisory Not Applicable

PRIVACY ACT STATEMENT

AUTHORITY: Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act.

PRINCIPAL PURPOSE: To record names, signatures, and other identifiers for the purpose of validating the trustworthiness of individuals requesting access to Department of Defense (DoD) systems and information. **NOTE:** Records may be maintained in both electronic and/or paper form.

ROUTINE USES: None.

DISCLOSURE: Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component? (Check all that apply)

Within the DoD Component

Specify.

Cybersecurity, SysAdmin, Personnel Security, Supervisors, and those with Resource Mgmt roles

Other DoD Components

Specify.

Other Federal Agencies

Specify.

State and Local Agencies

Specify.

Global Consulting International; In the DD254, it states "Ref 10j: For Official Use Only (FOUO) information or Personally Identifiable Information (PII) received or generated under this contract shall be controlled and protected, marked, and safeguarded, as specified in AR-25-55, DA Freedom of Information Act Program, AR 380-5 (Chapter 5), DA Information Security Program, and DoD 5200.01-M, Volume 4, DoD Information Security Program: Controlled Unclassified Information. This includes PII, as defined in Enclosure 2 of DoDD 5400.11 (DoD Privacy Program).

Contractor (Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)

Specify.

Other (e.g., commercial providers, colleges).

Specify.

i. Source of the PII collected is: (Check all that apply and list all information systems if applicable)

Individuals

Databases

Existing DoD Information Systems

Commercial Systems

Other Federal Information Systems

DD Form 2875 (System Authorization Access Request). Other PII for processing personnel evaluations, personnel security clearances, and personnel resource management actions may be downloaded from online databases to individual systems and server shares on the ICAN.

j. How will the information be collected? (Check all that apply and list all Official Form Numbers if applicable)

E-mail

Official Form (Enter Form Number(s) in the box below)

Face-to-Face Contact

Paper

Fax

Telephone Interview

Information Sharing - System to System

Website/E-Form

Other (If Other, enter the information in the box below)

DD Form 2875 (System Access Authorizations Request)

k. 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 must be consistent.

Yes No

If "Yes," enter SORN System Identifier

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or <http://dpcl.d.defense.gov/> Privacy/SORNs/
or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

A SORN is not required for this system.

I. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority.

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

NARA not required for this system.

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statute or Executive Order.

- (1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
- (2) If a SORN does not apply, 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) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.
 - (b) If direct statutory authority or an Executive Order does not exist, indirect statutory 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) If direct or indirect authority does not exist, 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 must be identified.

A SORN is not required for this system. DOD 8500.1, Cybersecurity, DODI 8510.01 Risk Management Framework for DoD Information Systems, AR 25-2 Information Assurance, and Access Control management requirements require collection of PII in order to authorize access to Information Systems.

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (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 No Pending

- (1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
- (2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, "DoD Information Collections Manual: Procedures for DoD Public Information Collections."
- (3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

An OMB Control Number is not required for this system.