



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Personnel Information Management System Korea (PIMSK)

U.S. Army, United States Forces Korea J1

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

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; Status of Forces Agreement, United States of America and the Republic of Korea; 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.

Personnel Information Management System Korea (PIMSK) is an enterprise information architecture; it is a secure e-Government portal designed to deliver tactical law enforcement information to the investigative arms of the United States Forces Korea (USFK) including the U.S. Customs Service. In addition, Personnel Information Management System Korea (PIMSK) assists USFK Commanders and USFK investigative agents in monitoring purchases of controlled items; producing ration control plates for authorized users; maintaining records of sales at duty-free retail facilities and suspected violators of the system; complying with Joint Service black-market monitoring control policy, and used for strength accounting, manpower management, and contingency planning and operations. The type of PII collected pertains to employment data, foreign national number, family information, and financial data.

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

Administrative: Access to the PIMSK will be controlled through a secure web login interface. Designated personnel will only have access to particular areas of PIMSK that have been deemed necessary for the individual to perform his or her duties. PIMSK users may request an account by submitting a System Authorization Access Request (SAAR) form with a supervisor's signature to the J1 Data Management office. PIMSK system administrators will review and approve/disapprove requests and users will be notified accordingly. PIMSK users will be restricted to managing and viewing records to their respective organizations. PIMSK administrators will have access to all PIMSK records.

Physical: All personnel entering the PIMSK computer room must have appropriate identification. Visitors to the room are always escorted. The PIMSK computer room is a restricted area and access is permitted to only authorized personnel. Physical entry is restricted by the use of locks and administrative procedures. Servers and workstations require CAC or other privileged authentication and access is limited to approved administrators.

Technical: PIMSK data is stored on a secure database server. An end user, using their web browser, will pass through the fire-wall to the web server. This connection between the end user and the web server is a secure encrypted SSL session. The web server provides the interface with the database server that processes the transaction and passes the data back to the end user's browser. Development and test web and database servers are also used. Access to PIMSK is controlled by a secure PIMSK login in the form of an authenticated CAC login. Any invalid attempts to access the application are recorded and user accounts are locked after 3 invalid attempts. Passwords (if stored) are encrypted in transmission, stored, and expire after 90 days.

Internal and external risks are associated with the protection of PII; however, risks are minimized to an acceptable level. Safeguards are employed to detect and minimize unauthorized disclosure, modification, and/or destruction of data; thus the U.S. Army, United States Forces Korea J1 has determined the risk to the individual's privacy to be minimal.

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.

Individuals may raise an objection with the USFK Privacy Act office during the public comment period of the Privacy Act system of records notice (if applicable) or during the data collection.

(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.

Individuals may raise an objection with the USFK Privacy Act Office during the comment period, during data collection, or at any time after the program is launched. If no objections are received, consent is presumed.

[Empty rectangular box]

(2) If "No," state the reason why individuals cannot give or withhold their consent.

[Empty rectangular box for providing reasons]

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.

PII data is automatically fed into the PIMSK system from other DOD Information Systems, therefore individuals in our system are not asked to provide PII data.

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.