



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Soldier Management System - Korea (SMS-K)

Eighth United States Army, G1, Camp Coiner, Korea

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 7980 (DA110998)
- 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 007-21-01-20-02-2307-00

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 A0600-8-23 AHRC

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; E.O. 9397 and 10450. Public Law 99-474 the Computer Fraud and Abuse act. Army Regulation 600-8-23, Standard Installation/Division Personnel System Database Management.

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 Eighth US Army G1 automated Human Resources web-based information system is known as the Soldier Management System – Korea (SMS-K). The business processes supported under this effort are Strength Management, Command Sponsorship, Joint Domicile, Foreign Service Tour Extensions (FSTE), Assignment Incentive Pay (AIP), Awards, Levy Briefs, Special Communities of Interest (COI), Postal Directory and Reporting.

SMS is the primary strength management tool to maintain theater personnel readiness in the forward-deployed Korean Theater of Operations. SMS gives local commanders, unit G1s/S1s, and theater strength managers a clear, accurate view of current and projected officer and enlisted strengths by MOS/AOC and skill level, by major subordinate command. It enables the allocation and assignment of Soldiers to meet unit readiness requirements.

The type of information collected is personal, employment and military.

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

Identity theft is a privacy risk if personal information is mishandled. This risk have been mitigated through administrative, technical, and physical safeguards.

Administrative, physical, and technical safeguards employed by the Eighth US Army G1 Office are commensurate with the sensitivity of personal data to ensure preservation of integrity and to preclude unauthorized use/disclosure. Access is limited to those individuals who require the records in performance of their official duties. Access is further restricted by the use of passwords which are changed periodically IAW AKO policy. Physical entry is restricted by the use of locks, guards, and administrative procedures.

Administrative: Access to the SMS-K website are controlled through a secure web login interface. Designated personnel will only have access to particular areas of SMS-K that have been deemed necessary for the individual to perform his or her duties. SMS-K users may request an account by submitting a System Authorization Access Request (SAAR) form DD2875 with a supervisor's signature to the G1 Data Management office. Eighth US Army G1 Manpower Division soldiers will review and approve/disapprove requests and users will be notified accordingly. SMS-K users will be restricted to managing and viewing records to their respective organizations. SMS-K administrators, programmers, and website developers will have access to all SMS-K records.

Physical: All personnel entering the SMS-K computer room, or work area, must have appropriate identification. Visitors to the room are always escorted and must sign a visitor access log. The SMS-K computer room is a restricted area and access is permitted to only authorized personnel only. 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: SMS-K data is stored on a secure database server. An end user, using their web browser, will pass through the firewall 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. Access to SMS-K is controlled by a secure SMS-K login in the form of an authenticated AKO ID and password login. Any invalid attempts to access the application are recorded and user accounts are locked after 3 invalid attempts. Passwords are not stored in the SMS-K database.

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.

On forms DD2875 System Authorization Access Request, and DA Form 4187 Personnel Action requests, individuals are given the opportunity to withhold their SSN; DD2875 and DA4187 describe the routine uses of the PII. If the person objects to providing SSN, the result will "impede, delay or prevent further processing of the request"

Otherwise, the majority of the Personally Identifiable Information used in our system is electronically sent, in an encrypted manner, from the Department of the Army Human Resources Command and cannot be altered by our system. Changes to records would need to be made in the DA HRC level.

(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.

On forms DD2875 System Authorization Access Request, and DA Form 4187 Personnel Action requests, individuals are given the opportunity to withhold their SSN. Forms DD2875 and DA4187 describe the routine uses of the PII. If the person objects to providing SSN, the result will "impede, delay or prevent further processing of the request"

Otherwise, the majority of the Personally Identifiable Information used in our system is electronically sent in an encrypted manner, from the Department of the Army Human Resources Command and cannot be altered by our system. Changes to records would need to be made in the DA HRC level.

(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.

Privacy Act Statement **Privacy Advisory**
 Other **None**

Describe each applicable format.

Form DA FORM 4187

AUTHORITY: - Title 5, Section 3012; Title 10, USC, E.O. 9397.
PRINCIPAL PURPOSE: Used by soldier in accordance with DA PAM 600-8-21 when requesting a personnel action on his/her own behalf (Section III)
ROUTINE USES: To initiate the processing of a personnel action being requested by the soldier.
DISCLOSURE: Voluntary. Failure to provide social security number may result in a delay or error in processing of the request for personnel action.
From DA FORM 4187

Form DD 2875

AUTHORITY: Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act.
PRINCIPAL PURPOSE: To record names, signatures, and Social Security Numbers 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.

Web site pages:

"UNCLASSIFIED, For Official Use Only (FOUO). PII may exist. Protect IAW DOD Regulation 5400.11 and Privacy Act of 1974"

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.