



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Accession Management Information System (AMIS)

U.S. Army, Deputy Chief of Staff for Personnel, G-1, U.S. Army Human Resources
Command (HRC), Alexandria

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.

5 U.S.C. 301, Departmental Regulations; 10 U.S.C. 3013, Secretary of the Army; as amended E.O. 9397 (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.

AMIS is an automated sub-system of the Total Officer Personnel Management Information System (TOPMIS) and is used to input officer accession records into the Total Army Personnel Data Base - Active Officer (TAPDB-AO) via DA form 160-R. Once DA form 160-R is collected from soldiers, an AMIS analyst manually enters the appropriate Soldier data into the system. Data entered may include: selected officer personnel data from the TAPDB-AO, the date of entry on active duty, selected information regarding current location/school for pre accessed officers, demographic data and assignment information on new officer accessions. It includes individual and mass record processing, erroneous record processing, report generation, Regular Army integration processing, AMIS active record data, Officer Record Brief (ORB) information and strength data. AMIS data will also assist in managing the Reserve Officer Training Corps (ROTC), U.S. Military Academy (USMA), Officer Candidate School (OCS), Judge Advocate General Corps (JAG) Recalls, Chaplains Corps, Warrant Officer and Surgeon General Reserve officer's accessions.

These records are maintained in a pre-accession status and are activated when the person becomes an active duty officer. After activation, the records are maintained the same as other officer data records within TOPMIS / TOPMIS II.

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

Due to the level of safeguarding, we believe the risk to individuals' privacy to be minimal. There are no risks in providing an individual the opportunity to object or consent, or in notifying individuals. Appropriate safeguards are in place for the collection, use and safeguarding of information.

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.

AMIS shares information directly with all Army components and major commands which includes Active, Reserve, and the National Guard, Army Staff Principals in the chain of command; Department of the Army Inspectors General, Army Audit Agency, Army Criminal Investigation Command, Army Intelligence and Security Command, Provost Marshal General; Assistant Secretary of the Army (Financial Management and Comptroller); the Army Reserve Command and to Commanders, Supervisors and their designated human resources and administrative personnel responsible for processing personnel actions.

Other DoD Components.

Specify. Office of the Secretary of Defense, Office of the DoD Inspector General, Defense Criminal Investigative Service; Defense Manpower Data Center.

Other Federal Agencies.

Specify. Office of Personnel Management; Department of Veterans Affairs; and the Social Security Administration

State and Local Agencies.

Specify. State unemployment compensation agencies

Contractor (Enter name and describe the language in the contract that safeguards PII.)

Specify. AMIS software is developed by Federal Government employees. Contractor support may be enlisted for other supporting functions, such as data base administration, etc. This exposure to PII warrants the additional safeguard. Science Applications International Corporation (SAIC) contractual language acknowledges the sensitivity of PII and describes the importance of protecting and maintaining the confidentiality and security of a Soldier's PII. The contractual language keys on training as a fundamental element in creating awareness and understanding of PII and why it is important to control and safeguard. The language also stresses securing PII material and equipment housing PII at the end of a work day. Contractual language directs and requires each SAIC employee in support of AMIS to have a National Agency Check prior to working on the program. The contract specifically states that contractor personnel will adhere to the Privacy Act, Title 5 of U.S. Code Section 522a, and all applicable agency rules and regulations.

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

Specify. Information will be available to authorized users with a need-to-know in order to perform official government duties

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.

Each individual has an opportunity to object by refusing to provide the requested PII based on the Privacy Act Statement presented at the time of entrance into military service and in each instance thereafter when PII is solicited by a Human Resource specialist/representative.

(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.

| |
|---|
| Each individual has an opportunity to object by refusing to provide the requested PII based on the Privacy Act Statement presented at the time of entrance into military service and in each instance thereafter when PII is solicited by a Human Resource specialist/representative. |
|---|

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

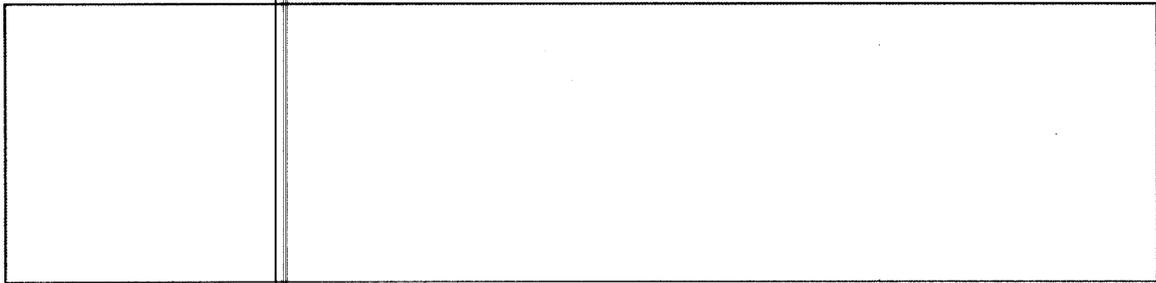
| |
|--|
| |
|--|

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.

| |
|---|
| AMIS receives existing PII data from other Army information systems. When data is collected directly from individual Soldiers, they are provided either a Privacy Act Statement or Privacy Advisory via DA form 160-R. DA from 160-R provides required language from the 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.