



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Army Lessons Learned Information System (ALLIS)

U.S. Army Training and Doctrine Command (TRADOC)

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.

10 U.S.C. 3013, Secretary of the Army and Army Regulation 350-1, Army Training and Leader Development

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.

Combination of hardware and software solutions with a user interface providing a repository of the organization's electronically stored data. The primary purpose of the ALLIS is to deliver lessons learned information to the Force. The system also provides an internal component consisting of document workflow and management features for personnel, training, and equipment. Personal information is collected for purposes of internal work management.

The type of PII includes personal, military, employment, educational information.

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

The information is stored on a server housed in a secure building at Fort Leavenworth KS. Fort Leavenworth provides physical security through the use of fences, gate guards and mobile security force. Additional physical security is provided through use of key card access to the building and monitored intrusion detection. The building has been approved for open storage of SECRET classified information. Electronic security is provided through use of CAC authentication to the web site, Active Directory authentication to network file system, and user ID/password authentication to the data store. All three are required to access the data store containing the PII. Additionally, access is limited to computers on the the network segment where the server resides and to only those personnel who need access to the specific piece of PII. Risks to individual privacy is minimal. Individuals have the option to exclude biographical information, but are required to submit information necessary for employment purposes; home address and phone number.

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. Army Staff Principals in the chain of command, Department of Army Inspector General, Army Audit Agency, U.S. Army Criminal Investigation Command, Intelligence and Security Command, Provost Marshall General, and Assistant Secretary of the Army (Financial Management and Comptroller).

Other DoD Components.

Specify. Internal DoD agencies that would obtain access to PII in this system, on request in support of an authorized investigation or audit, may include Department of Defense Inspector General and Defense Criminal Investigation Service.

Other Federal Agencies.

Specify. None

State and Local Agencies.

Specify. None

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

Specify.

None

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

Specify.

None

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.

Information is required for employment purposes to include telephonic notification of late work starts, contact for work related issues, and forwarding of correspondence after employment. Biographical entries are voluntary fields. Personnel are able to edit or remove their own information at any time. Information such as e-mail address must be accurate for work flows to work properly, but other information such as home address and phone number are not verified. Failure to provide accurate information to supervisors may create hardships for the employee.

(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.

PII is collected during in-processing. Personnel are informed how the PII will be used through appropriate Privacy Act Statements. Information is used strictly for employment related purposes. Personnel will be called at the provided phone number for work related issues. Employment related correspondence will be forwarded to the home address provided after the employment ends.

(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.

Upon arriving at the ALLIS Portal, users are advised that all information entered into this system may be monitored for authorized government purposes.

Individuals are provided a Privacy Act Statement during in-processing.

PURPOSE: Purpose of the ALLIS is to deliver lessons learned information to the Force. The system also provides an internal component consisting of document workflow and management features for personnel, training, and equipment.

SITE SECURITY: The information is stored on a server housed in a secure building at Fort Leavenworth, KS. Fort Leavenworth provides physical security through the use of fences, gate guards and mobile security force. Additional physical security is provided through use of key card access to the building and monitored intrusion detection. The building has been approved for open storage of SECRET classified information. Electronic security is provided through use of CAC authentication to the web site, Active Directory authentication to network file system, and user ID/ password authentication to the data store. All three are required to access the data store containing the PII. Additionally, access is limited to computers on the the network segment where the server resides and to only those personnel who need access to the specific piece of PII. Risks to individual privacy is minimal. Individuals have the option not to include biographical information, but are required to submit information necessary for employment purposes; home address and phone number.

ROUTINE USES: Provide document workflow and management features for personnel, training, and equipment for mission and administrative related purposes.

For military Personnel: Disclosure of personal information is voluntary. The Soldier is responsible to ensure the supervisor is able to contact him/her during non-duty hours in a manner acceptable to the supervisor. The standard is the Soldier's home phone or cellular phone. Failure to provide an acceptable contact method may subject the individual to disciplinary action. The Soldier's AKO email address is used for automatic work flow capability and is necessary for the individual to accomplish his/her work assignments. Additionally, the AKO email address is required before the Soldier can obtain network access. Failure to provide the AKO email address will make it impossible for the Soldier to accomplish assigned tasks and will subject the individual to disciplinary action.

For Department of the Army civilians: Disclosure of personal information is voluntary. The individual is responsible to ensure the supervisor is able to contact him/her during non-duty hours for work related notifications in a manner acceptable to the supervisor. The standard is the individual's home phone or cellular phone. Failure to provide an acceptable contact method can result in inconvenience for the individual who will not be notified of events such a post closures due to inclement weather. The individual's AKO email address is used for automatic work flow capability and is necessary for the individual to accomplish his/her work assignments. Additionally, the AKO email address is required before the individual can obtain network access. Failure to provide the AKO email address will make it impossible for the individual to accomplish assigned tasks and will subject the individual to adverse personnel action.

For Contractors: Contract requirements apply. Disclosure of personal information is voluntary. The individual's AKO email address is used for automatic work flow capability and is necessary for the individual to accomplish his/her work assignments. Additionally, the AKO email address is required before the individual can obtain network access. Failure to provide the AKO email address will make