



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Access Control Lists System (ACL)

Office of the Assistant G-1 for Civilian Personnel

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

This data collection instrument does not collect PII from the public

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; Army Regulation 690-200, General Personnel Provisions; and E.O. 9397 (SSN) as amended.

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 Access Control List (ACL) application provides an enterprise-wide authorization service for Army unique applications. The Access Control List application is an administrative tool designed to provide an efficient method of managing the access of subordinate users, the tools they use, and the roles they perform across the CISD enterprise. It will complement the System Access Nominations and Authorization Request (SANAR) form. Once a SANAR has been routed and approved, an administrator can use ACL to build an application authorization record for the user.

ACL uses PII (name, birth date, SSN, AKO ID, and work email address) for employment data and position information on civilian employees. This PII is used for identifying the appropriate users.

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

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 we believe 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. Army Staff Principals in the chain of command, Department of Army Inspector General, Army Audit Agency, US Army Criminal Investigative Command, US Army Intelligence and Security Command, Provost Marshal General and Assistant Secretary of the Army for Financial Management and Comptroller.

Other DoD Components.

Specify. Any internal DoD agencies, on request, in support of an authorized investigation or audit, may include Defense Manpower Data Center, Department of Defense Inspector General and Defense Criminal Investigative Service.

Other Federal Agencies.

Specify. In addition, Disclosure of records of the information contained therein may be specifically disclosed outside the Department of Defense (DOD) according to the Blanket Routine Uses set at the beginning of the compilation of systems of records, published annually in the Federal Register, and the disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act.

State and Local Agencies.

Specify.

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

Specify.

Within our current Performance Work Statement (PWS), Army Civilian Information Services (CIS) adheres to publications and documents applicable to the contract. The Contractor shall comply with all applicable privacy documents and publications and all changes to them that are in effect at contract start date. Local supplements to any of these publications are also applicable to this contract. The PWS may set a higher standard of performance than an applicable Army regulation. The PWS will have control over the regulations unless a particular PWS provision is in direct conflict with the applicable provision of the Army regulation. As outlined within AR 380-5, Department of the Army Information Security Program, the Computer Security Act of 1987 established requirements for protection of certain information in federal Government Automated Information Systems (AIS). This information is referred to as "sensitive" information, defined in the Act as: "Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, USC (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy."

- 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.

Entry of PII into ACL via the System Access Nomination and Authorization Request (SANAR) form is a necessary condition for receiving authorization to the internal networks. Although disclosure of the information is voluntary, failure to provide the information may impede or prevent the processing of the applicant's SANAR form.

(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.

Entry of PII into ACL via the System Access Nomination and Authorization Request form (SANAR or SAMR-CP-PS Form 1) is a necessary condition for receiving authorization to the internal networks. Although disclosure of the information is voluntary, failure to provide the information may impede or prevent the processing of the applicant's SANAR form.

(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.

Individuals submit their PII on a System Access Nominations and Authorization Request (SANAR) form which contains a Privacy Act Statement.

Privacy Act Statement

AUTHORITY: Public Law 99-474, the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, authorizes collection of this information.

PURPOSE AND USE: The information will be used to verify that you are an authorized user of a U.S. Department of the Army civilian personnel automated information system (AIS) and/or to verify completion of your government personnel security investigation. Although disclosure of the information is voluntary, failure to provide the information may impede or prevent the processing of your SANAR.

DISCLOSURE: Disclosure of records of the information contained therein may be specifically disclosed outside the Department of Defense (DOD) according to the Blanket Routine Uses set at the beginning of the compilation of systems of records, published annually in the Federal Register, and the disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act.