



PRIVACY IMPACT ASSESSMENT (PIA)

For the

ABERDEEN PROVING GROUND ELECTRONIC SECURITY SYSTEM (APG ESS)

AMC - CECOM - US ARMY COMMUNICATIONS-ELECTRONICS COMMAND

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

5 August 2013, Pending Approval

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; Army Regulation 190-13, the Army Physical Security Program, E.O. 9397 (SSN). Homeland Security Presidential Directive 12 (HSPD-12)

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.

To support Department of the Army physical security and access control programs; Information Assurance program; to record personal data registered with the Department of the Army; to provide a record of security/ access badges issued; to restrict entry to secure facilities and activities; The above initiatives will also support Homeland Security Presidential Directive 12 (HSPD-12), and is part of a broader effort to deny access to terrorists, criminals and other unauthorized persons.

Individuals name and photograph.

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

Personal data will include full name and photograph. Information will be stored on database within the Aberdeen Proving Ground Electronic Security System and will be verified during the electronic entry transaction process. Data will also be used to issue badges to designated employees who must access and work in restricted areas/facilities. Data will be stored on visitors to C4ISR facilities. Database will be accessible only to specific managers and security personnel through CAC, password and PIN authentication.

All users of the system are required digitally sign on to this security management system and acknowledge statement about the sensitivity of the data they will have access to.

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.

Special Security Officers and Managers employed within Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR)

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.

Yes, both employees and visitors may object in writing to the collection of their PII. Failure to provide PII may result in denial of access to C4ISR facilities.

(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.

Yes, both employees and visitors may object in writing to the collection of their PII. Failure to provide PII may result in denial of access to C4ISR facilities.

(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.

- | | |
|---|---|
| <input checked="" type="checkbox"/> Privacy Act Statement | <input type="checkbox"/> Privacy Advisory |
| <input type="checkbox"/> Other | <input type="checkbox"/> None |

Describe each applicable format.

A Privacy Act Statement is provided to individuals, either electronic or hard copy, when PII is being collected for this system. Electronically sent message will be provided to all Army Team C4ISR employees, notifying them of the requirement to store their PII. Privacy Act Statement will also be posted on organizational web site for review by employees.

Privacy Act Statement on the Aberdeen Proving Grounds Electronic Security System:

Privacy Act Statements, as required by 5 U.S.C. 552a(e)(3), are provided at the collection point. The statement provides the following: collection, purpose, authorities, external uses, the voluntary nature of the program and the fact that no consequences accrue for those who chose not to participate beyond denial of access to the Team C4ISR Campus. The statement is included on paper and electronic collection forms. The Aberdeen Proving Grounds Electronic Security System Privacy Act Statement reads as follows:

AUTHORITY: 10 U.S.C. 3013, Secretary of the Army, Army Regulation 190-13, The Army Physical Security Program and Executive Order 9397, as amended.

PRINCIPAL PURPOSE(S): To provide necessary information to Aberdeen Proving Grounds to determine if applicant meets access control requirements. Records in the Electronic Security System are maintained to support the Team C4ISR physical security and are used for identity verification purposes and used by security officers to monitor individuals accessing the Team C4ISR Campus. Personally Identifiable Information (PII) or other acceptable identification will be used to distinguish individuals who request entry to the Team C4ISR Campus.

ROUTINE USE(S): The "DoD Blanket Routine Use" are set forth at the beginning of the DoD compilation of systems of records notices.

DISCLOSURE: Voluntary. However, failure to provide the requested information will result in denial of entry to the Team C4ISR Campus.

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.