



PRIVACY IMPACT ASSESSMENT (PIA)

For the

ARMY INVESTIGATIVE ENTERPRISE SYSTEM(AIES)
--

INSCOM - CCF - Central Clearance Facility

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

OPM Equip 3206-0005 / DoD JPAS 0704-0496

Enter Expiration Date

OPM Equip: Pending / DoD JPAS: 31 Mar 2011

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; 50 U.S.C. 4039; and the National Security Act of 1947; E.O 10450 and 10865; 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 US Army Central Personnel Security Clearance Facility (USACCF) (UNCLASSIFIED) part of the MI Forest network resources are installed in Building 600 10th Street, Fort George G. Meade, MD 20755. These resources are operated and maintained by CCF ISA (Information Support Activity) government personnel. The CCF unclassified servers are located on the 1st Floor of Bldg 600 and are under the physical control of INSCOM (United States Army Intelligence and Security Command). The Army Investigative Enterprise System - UNCLASSIFIED (AIES) located in CCF at Fort George G. Meade defines three related systems: AFS (Army Fingerprint System), CATS (Central Adjudication Tracking System) and PSIP (Personnel Security Investigation Portal System). The function of AIES is ultimately to serve as the Army's enterprise solution for personnel security investigations (PSIs). Each sub-system is described below. First, AIES will serve as the PSI Portal (PSIP), through which security managers and civilian personnel advisory center (CPAC) staff initiate PSIs for current Army personnel and applicants. The primary inputs to the PSIP are requests for PSIs that are completed electronically by security managers or civilian personnel advisory center staff using this web-based application. In the future AIES will be linked to other systems of record such as Joint Personnel Adjudication System (JPAS) and Defense Integrated Military Human Resource System (DIMHRS); however, this capability is not yet established. The outputs are notification to CCF's Central Adjudication Tracking System (CATS) that a request for a PSI was submitted through e-QIP to the Office of Personnel Management (OPM). The function of the Army Fingerprint System (AFS) is to establish a single central store and forward server with connection to the Office of Personnel Management (OPM) for the secure submission of fingerprint data of Army personnel and applicants in conjunction with job-related personnel security investigations (PSIs). This not only ensures Army fingerprint data is transmitted appropriately, but minimizes the number of electronic connections with OPM, for each of which the Army is charged a fee. Once AFS is fully fielded, Army personnel worldwide will be able to use the electronic fingerprint machines, though the central store and forward server will remain under the control of Army CCF personnel. The Army intent is to work with other Service and DoD organizations to establish a DoD-wide network of electronic fingerprint machines, so as to minimize the number of fingerprint cards being mailed to OPM. The primary inputs to AFS are electronic fingerprints and associated identifying data. The output is an electronic file containing the same that is sent securely to OPM. The CCF Clearance Adjudication Tracking System (CATS) is an automated system used by the US Army CCF Adjudicators to provide an electronic case management system for security clearance determination. CATS receives personnel investigations from the Office of Personnel Management (OPM) in an electronic form directly into CATS. Currently CATS provides HRC an export of personnel security information (granted/denied/revoked). CATS also provides IRR (Investigative Records Repository) adjudication cases in electronic form. Future plans may include a direct interface to the Joint Personnel Adjudication System (JPAS) and Defense Central Index of Investigations (DCII).

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

Unauthorized release of PII, mitigated by compliancy IAW Information Assurance mandates and policies.

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.

Individuals are able to object by refusing to sign the Standard Form 86-1 and 86-2 Authorizations for Release of Information.

(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.

Individuals are able to object by refusing to sign the Standard Form 86-1 and 86-2 Authorizations for Release

of Information or consent by signing Standard Form 86-1 and 86-2 Authorizations for Release of Information.

(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 checked="" type="checkbox"/> Other | <input type="checkbox"/> None |

Describe each applicable format.

Disclosure of Information - The information you give us is for the purpose of investigating you for a national security position; we will protect it from unauthorized disclosure. The collection, maintenance and disclosure of background investigative information is governed by the Privacy Act.

Authorization for Release of Information - I Authorize any investigator, special agent, or other duly accredited representative of the authorized Federal agency conducting my background investigation, to obtain any information relating to my activities from individuals, schools, residential management agents, employers, criminal justice agencies, credit bureaus, consumer reporting agencies, collection agencies, retail business establishments, or other sources of information. This information may include, but is not limited to, my academic, residential, achievement, performance, attendance, disciplinary, employment history, criminal history record information, and financial and credit information. I authorize the Federal agency conducting my investigation to disclose the record of my background investigation to the requesting agency for the purpose of making a determination of suitability or eligibility for a national security position.