



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Civilian Application Tracking System (iCIMS® Talent Platform)

US Army Medical Command - Defense Health Program (DHP) Funded Application

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; Army Regulation 690-200, General Personnel Provisions; and 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.

The iCIMS® Talent Platform web-based application is used for recruiting and tracking applicants for civilian job positions. It is the industry's premier talent acquisition solution that enables HR professionals to manage their organization's entire talent lifecycle from sourcing to recruitment marketing to applicant tracking to onboarding all within a secure single web-based application. Providing innovative HR solutions, iCIMS gives recruiters the necessary tools to make the most informed hiring decisions, every time. The iCIMS Talent Platform is easy to use, scalable, and accessible from anywhere, anytime.

The records in the system are used in considering individuals who have applied for positions in the Federal service by making determinations of qualifications including medical qualifications, for positions applied for, and to rate and rank applicants applying for the same or similar positions. They are also used to refer candidates to Federal agencies for employment consideration, including appointment, transfer, reinstatement, reassignment, or promotion. Records derived from the office-developed or agency-developed assessment center exercises may be used to determine training needs of participants. These records may also be used to locate individuals for personnel research.

Records in this system contain identifying information to include name, date of birth, home address, education records, and employment records.

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

The privacy risks associated with the PII collected are unauthorized access, inaccurate information entered into the application, and unauthorized disclosure of PII. There are administrative, technical, and physical security safeguards in place to mitigate these risks. The specific security safeguards are addressed in Section 3 below.

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.

Contractor is iCIMS. iCIMS agrees that it will not at any time during the term of this Agreement or at any time thereafter, divulge any Proprietary or Confidential Information to any person or entity or use such information outside of ATS' standard service offering to Customer. iCIMS shall not use, modify, copy or reproduce such Proprietary or Confidential Information other than to fulfill its obligations under this Agreement. iCIMS will (a) avoid disclosure, loss or misuse of the Proprietary or Confidential Information in order to prevent it from falling into the public domain or the possession of any third party, which measures shall include the highest degree of care; (b) not provide disclose, permit to be disclosed, or otherwise make available such Proprietary or Confidential Information, directly or indirectly to any third party without the prior written approval of Customer or as permitted or required by law; (c) reasonably maintain Proprietary or Confidential Information in an appropriate and secure environment, both physically and electronically; and (d) notify Customer immediately in writing of any loss, misuse, or misappropriation of the Proprietary or Confidential information that may come to ATS' attention. Without the written consent of the Customer, iCIMS will not disclose Proprietary or Confidential Information or the terms of this Agreement to any third party other than iCIMS need-to-know agents and representatives whose duties justify their need to know such information, and then only such agents and representatives who have been advised of this Agreement and the obligations under this contract.

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.

The purpose for the collection of PII is described in the posted Privacy Act Statement. By completing the application process, job applicants are prompted to either grant or withhold their consent to the terms of the Privacy Act Statement. Any information provided as part of the application process is completely voluntary. However, failure to provide all the requested information could lead to rejection of the application due to inadequate data.

(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.

The specific uses of PII are described in the posted Privacy Act Statement. By completing the application process, job applicants are prompted to either grant or withhold their consent to the terms of the Privacy Act Statement. By submitting their application and resume, individuals are granting their consent to the specific uses of their PII. Individuals who object to the specific uses of their PII have the option of not submitting their application.

(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.

PRIVACY ACT STATEMENT

AUTHORITY:

The Civilian Corps web site is provided as a public service by the U.S. Army Medical Command under the Department of the Army. The collection of personally identifiable information through this web site is authorized by 10 U.S.C. Section 3013, Secretary of the Army; AR 600-20, Army Command Policy and E.O. 9397(SSN).

PRINCIPAL PURPOSE(S):

The principal purpose of this web site is to provide information about career opportunities for medical and dental professionals with the U.S. Army Medical Command, and to enable interested candidates to apply for open positions.

ROUTINE USE(S):

Information presented on the Civilian Corps web site is considered public information and may be distributed or copied. Use of appropriate byline/photo/image credits is requested. Personally identifiable information (PII) gathered through the Civilian Corps web site is utilized by the U.S. Army Medical Command (MEDCOM) solely for purposes associated with assessing your employment application. In keeping with this purpose, your PII may also be shared with other government agencies and organizations.

MANDATORY OR VOLUNTARY:

Any information you provide as part of the application process through the Civilian Corps web site is completely voluntary. However, failure to provide all the requested information could lead to rejection

of your application due to inadequate data.

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.