

## PRIVACY IMPACT ASSESSMENT (PIA)

**PRESCRIBING AUTHORITY:** DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

**1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:**

KEYSTONE-RETAIN-CS - KEYSTONE-Retention System - Client Server

**2. DOD COMPONENT NAME:**

United States Army

**3. PIA APPROVAL DATE:**

08/25/20

US Army Deputy Chief of Staff for Personnel / Human Resources Command (HRC)

### SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

**a. The PII is:** (Check one. Note: foreign nationals are included in general public.)

- |  |  |
|--|--|
| <input type="checkbox"/> From members of the general public  | <input type="checkbox"/> From Federal employees and/or Federal contractors |
| <input checked="" type="checkbox"/> From both members of the general public and Federal employees and/or Federal contractors | <input type="checkbox"/> Not Collected (if checked proceed to Section 4)   |

**b. The PII is in a:** (Check one)

- |  |   |
|--|---|
| <input type="checkbox"/> New DoD Information System                    | <input type="checkbox"/> New Electronic Collection      |
| <input checked="" type="checkbox"/> Existing DoD Information System    | <input type="checkbox"/> Existing Electronic Collection |
| <input type="checkbox"/> Significantly Modified DoD Information System |   |

**c. Describe the purpose of this DoD information system or electronic collection and describe the types of personal information about individuals collected in the system.**

KEYSTONE – Retention System Client Server (KEYSTONE-RETAIN-CS) supports US Army reenlistment, extension, reclassification, and Reserve Component transition requirements. It is a full-featured application for personnel recruiting and retention that enables better servicing of applicants through real-time visibility of opportunities, reduced processing time, and increased responsiveness to policy. It provides an integrated view of information and activities required to support recruiting and retention business processes, and presents applicants only with opportunities for which they are qualified.

PII collected includes identification data, military personnel data, dependent, financial, and education information.

**d. Why is the PII collected and/or what is the intended use of the PII?** (e.g., verification, identification, authentication, data matching, mission-related use, administrative use)

Identification and data matching: KEYSTONE-RETAIN-CS collects PII on individuals to identify and match applicants against Army position requirements, process individuals into jobs and Military Occupational Specialties, and assign training for Soldiers while they are in the Army.

Administrative use: PII serves as the primary way to determine the individual's eligibility for specific reenlistment options, training or incentives that may be available for individuals that meet specific reenlistment criteria.

**e. Do individuals have the opportunity to object to the collection of their PII?**  Yes  No

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object to the collection of PII.

Since data are not collected directly from individuals they are not provided a Privacy Act Statement or a Privacy Advisory from KEYSTONE-RETAIN-CS. However, individuals implicitly consent to capture and use of that information at the time of employment or enlistment in the Department of the Army, at which time they are provided a Privacy Advisory.

**f. 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.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

Since data are not collected directly from individuals they are not provided a Privacy Act Statement or a Privacy Advisory from KEYSTONE-RETAIN-CS. However, individuals implicitly consent to capture and use of that information at the time of employment or enlistment in the Department of the Army, at which time they are provided a Privacy Advisory.

**g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. (Check as appropriate and provide the actual wording.)**

- Privacy Act Statement     
  Privacy Advisory     
  Not Applicable

KEYSTONE-RETAIN-CS only extracts existing PII data from other Army information systems. Since data are not collected directly from individual they are not provided a Privacy Act Statement or Privacy Advisory. However, individuals implicitly consent to capture and use of that information at the time of employment or enlistment in the Department of the Army, at which time they are provided a Privacy Advisory.

**h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component? (Check all that apply)**

- Within the DoD Component

Specify.

Department of the Army Deputy Chief of Staff for Personnel, staff principals in the chain of command, Department of the Army Inspector General, Army Audit Agency, US Army Cadet Command, US Army Recruiting Command, US Army Criminal Investigation 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.

Defense Finance and Accounting Service (DFAS), Department of Defense Inspector General, Defense Manpower Data Center, National Guard Bureau (NGB), and Defense Criminal Investigative Service.

- Other Federal Agencies

Specify.

Office of Economic and Manpower Analysis.

- State and Local Agencies

Specify.

N/A.

- Contractor (Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)

Specify.

HRC contracts contain language addressing the applicable FAR privacy clauses, acknowledge the sensitivity of PII and describe the importance of protecting and maintaining the confidentiality and security of an individual's PII in the associated task orders. The contractual language keys on training as a fundamental element in creating awareness and understanding of PII and why it is important to control and safeguard. The language also stresses securing PII material and equipment housing PII at the end of a work day. Contractual language directs and requires each contract employee in support of this system to have a valid Secret clearance prior to working on the program. Contracts specifically state that contractor personnel shall adhere to the Privacy Act, Title 5 of the U.S. Code, Section 552A and applicable DOD, Army, and HRC rules and regulations.

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

Specify.

N/A.

**i. Source of the PII collected is: (Check all that apply and list all information systems if applicable)**

- Individuals       Databases  
 Existing DoD Information Systems       Commercial Systems  
 Other Federal Information Systems

PII is collected from the following DoD information systems: Army Training Requirements and Resources System of HQDA G1, Standard Installation/Division Personnel Reporting System - Army National Guard of NGB, Defense Joint Military Pay System - Active Component and - Reserve Component of DFAS, and Enlisted Distribution and Assignment System, KEYSTONE - Recruit Quota System - Client Server, Total Army Personnel Data Base - Active Enlisted and - Active Officer of HRC.

**j. How will the information be collected?** (Check all that apply and list all Official Form Numbers if applicable)

- |   |  |
|---|--|
| <input type="checkbox"/> E-mail   | <input type="checkbox"/> Official Form (Enter Form Number(s) in the box below) |
| <input type="checkbox"/> Face-to-Face Contact                                     | <input type="checkbox"/> Paper   |
| <input type="checkbox"/> Fax  | <input type="checkbox"/> Telephone Interview                                   |
| <input checked="" type="checkbox"/> Information Sharing - System to System        | <input type="checkbox"/> Website/E-Form  |
| <input type="checkbox"/> Other (If Other, enter the information in the box below) |  |

N/A.

**k. 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 must be consistent.

- Yes  No

If "Yes," enter SORN System Identifier

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or <http://dpcl.dod.mil> Privacy/SORNs/  
or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

N/A.

**l. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?**

(1) NARA Job Number or General Records Schedule Authority.

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

RN 601-280d. T10. Keep until no longer needed for conducting business, then retire to the AEA, the AEA will delete record when the record is 10 years old.

**m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statute or Executive Order.**

- (1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
- (2) If a SORN does not apply, 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) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.
  - (b) If direct statutory authority or an Executive Order does not exist, indirect statutory 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) If direct or indirect authority does not exist, 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 must be identified.

5 United States Code (USC) 552(a); 10 USC 505(d), 1176, 3258, 3259-3261, 7013 (Secretary of the Army), 3914, 3917, 12301(a), 12301(d), 12302, 12304, and 12305; 37 USC 308-309; Army Regulation 601-280, Army Retention Program; and Executive Order 9397 as amended (SSN).

**n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (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     No     Pending

- (1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
- (2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, " DoD Information Collections Manual: Procedures for DoD Public Information Collections."
- (3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

System does not collect PII from 10 or more members of the general public in a one-year period.