



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

DCM-HR-COE-FTK - Data Center Mainframe - Human Resources Center Of Excellence - FT Knox

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

### **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      13125 DA201187
- 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      A0600-8-104 AHRC

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 United States Code (USC) 301 and 552(a); 10 USC Sections 1142, 1143, 1176, 12301(a), 12301(d), 12302, 12304, 12305, 12731, 1413a, 1470-1480, 3013, 3258, 3259-3261 (repealed), 3914, 3917, 4302, 5013, 5043, 505(d), 8013, 10204, and Chapters 36 (Subtitles I-IV, Sections 616-646), 55, 58, 61, and Subtitles A (Part II), E (Parts I-IV); 37 USC 1006, 308, 309; 42 USC 10606; 44 USC 3101-3102, 3501; Title XII of Public Law 101-510; Public Laws (93-3097, 103-337 Div. A Title XVI Section 1662(b)(3), 107-314); Section 636, National Defense Authorization Act; Defense Acquisition Workforce Improvement Act; Department of Defense Directives 1030.1, 1200.7, 1235.10, 1300-15, 1300.22, 1310.1, 1332.18, 1332.35, 1352.1, 5000-58-R; Department of Defense Instructions 1300.18, 1300.19, 1300.20, 1304, 1320.4, 1320.12, 1320.14, 5000.2, 5000.58, 7730.54; USD Memo: General and Flag Officer Boards - Adverse Information of a Credible Nature, 19 July 2006; Army Regulations 25-1, 25-400-2, 40-3, 40-407, 135-133, 135-135, 140-1, 140-9, 140-10, 140-30, 140-50, 140-111, 140-145, 140-315, 380-381, 600-8-6, 600-8-19, 600-8-29, 600-8-104, 600-8-111, 600-18, 614-200, 621-5, 623-3, 635-40, 640-30, 690-200; DA Pamphlets 600-8-23, 600-81, 611-21; DA Memo 600-2, DA G1 Memo: Personnel Suitability Screening Policy (Enlisted and Officer), 9 March 2006; and Executive Order 9397 as amended (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 Data Center Mainframe - Human Resources Center of Excellence - Ft. Knox (DCM-HR-COE-FTK) provides a Mission Essential Hardware and Software Family of Systems Infrastructure to support the entire Human Resource Life Cycle of Active and Reserve Component Soldier Management. It is the parent system for the HRC mainframe, which includes three Total Army Personnel Data Bases and 22 mainframe systems and applications.

Types of PII collected are personal, contact, dependent, financial, medical, employment, education, and military information.

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

All systems and environments have threats that seek to exploit and cause harm to the information. Some threats are natural, some are inherent in the system design, some can be attributed to unauthorized personnel, and some to authorized personnel who make mistakes. Four general categories of threats exist: human-intentional, human-unintentional, structural, and natural. The system is maintained in a controlled facility. Appropriate technical, personnel, physical and operational safeguards are in place for the access, collection, use and protection of information. Due to the level of safeguarding, we believe the risk to individuals' 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.

Staff principals in the chain of command, Department of the Army Inspector General, Army Audit Agency, 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.

Department of Defense Inspector General and Defense Criminal Investigative Service.

**Other Federal Agencies.**

Specify.

N/A

**State and Local Agencies.**

Specify.

N/A

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

Specify.

Science Applications International Corporation contractual language acknowledges the sensitivity of PII and describes the importance of protecting and maintaining the

confidentiality and security of an individual's PII. 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 SAIC employee in support of TAPDB-R to have a valid Secret clearance prior to working on the program. The contract specifically states that contractor personnel will adhere to the Privacy Act, Title 5 of U. S. Code Section 552a, and all applicable agency rules and regulations.

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

Specify.

N/A

**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.

N/A

(2) If "No," state the reason why individuals cannot object.

Since data are not collected from individuals they are not provided a Privacy Act Statement or a Privacy Advisory from DCM-HR-COE-FTK. However, Soldiers 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.

**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.

N/A

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

Since data are not collected from individuals they are not provided a Privacy Act Statement or a Privacy Advisory from DCM-HR-COE-FTK. However, Soldiers 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.

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.

Since data are not collected from individuals they are not provided a Privacy Act Statement or Privacy Advisory by DCM-HR-COE-FTK. However, Soldiers 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.

**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.