



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

Personal Effects Tracking System (PETS)

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       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      10815 (APMS ID DA187387)
- 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 USC 301, Departmental Regulations; 10 USC 3013, Secretary of the Army; 10 USC 5013, Secretary of the Navy; 10 USC 5043 Commandant of the Marine Corps; 10 USC 5041(d), Marine Corps Function; 10 USC 8013, Secretary of the Air Force; Section 546 of Public Law 108-136, National Defense Authorization Act for Fiscal Year 2004; Section 562 of Public Law 109-163, National Defense Authorization Act for Fiscal Year 2006; DODD 1300.15, Military Funeral Support; DODD 1300.22, Mortuary Affairs Policy; DODI 1300.18, Personnel Casualty Matters, Policies, and Procedures; Office of the Assistant Secretary of Defense Memorandum: Defense Casualty Information Processing System, 22 October 1999; Joint Publication 4-06, Mortuary Affairs; Army Regulation 600-8-1, Army Casualty Program; Army Regulation 638-2, Deceased Personnel: Care and Disposition of Remains and Disposition of Personal Effects; Marine Corps Order 3040.4, Marine Corps Casualty Assistance Program (MARCORCASASTPRO); Bureau of Naval Personnel, Naval Military Personnel Manual (MILPERSMAN), Section 1770, Casualties and Survivors Benefits; NAVPERS 15555D, Bureau of Naval Personnel, Navy Military Funerals; U. S. Air Force Instruction 36-3002, Casualty Services; U. S. Air Force Instruction 34-242, Mortuary Affairs Program; U. S. Air Force Policy Directive 34-5, Mortuary Affairs; 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 Personal Effects Tracking System (PETS) provides tracking and accountability for personal effects (PE) received, processed and shipped at the US Army Human Resources Command Joint Personal Effects Depot (JPED) of deceased and wounded service members of the Armed Forces, contractors, and civilians. Each PE item is received at the JPED, and tracked via PETS to maintain accountability, chain-of-custody and to ensure that personal effects are delivered to the person authorized to receive the PE in accordance with applicable law and regulation. Authorized users use PETS to actively manage PE, run reports, and view photos of the PE.

PII collected includes personal, contact, dependent, emergency contact, and military record data.

(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; Army Inspector General; Army Audit Agency; US Army Criminal Investigation Command; US Army Intelligence and Security Command; Provost Marshall General; and Assistant Secretary of the Army for Financial Management and Comptroller.

**Other DoD Components.**

Specify.

Office of the Under Secretary of Defense for Personnel and Readiness, Personnel and Readiness Information Management; Defense Finance and Accounting Service; Defense Intelligence Agency; US Air Force; US Marine Corps; US Navy; Joint Services Records Research Center; DOD Inspector General; and Defense Criminal Investigative Service.

**Other Federal Agencies.**

Specify.

N/A

**State and Local Agencies.**

Specify.

State and Territory National Guard offices.

**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 a Soldier'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 ARTRAMS 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 522a, 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.

Individuals are not involved in the data collection process. Most cases involve deceased personnel. However, Service Members implicitly consent to capture and use of their information at the time of employment or enlistment in the Armed Services, 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.

Individuals are not involved in the data collection process. Most cases involve deceased personnel. However, Service Members implicitly consent to capture and use of their information at the time of employment or enlistment in the Armed Forces, 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.

Individuals are not involved in the data collection process, so neither a Privacy Act Statement nor a Privacy Advisory is provided. However, Service Members implicitly consent to capture and use of their information at the time of employment or enlistment in the Armed Forces, 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.