



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

Exceptional Family Member Program (EFMP)
--

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
- 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**

0704-0411

**Enter Expiration Date**

31 July 2017

**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.

Title 10 US Code Section 3013 (Secretary of the Army), and Chapter 55; Title 42 US Code Section 10606 (Victims' Rights, as implemented by DODD 1030.1, Victim and Witness Assistance Program); AR 40-407, Nursing Records and Reports; AR 608-18, The Family Advocacy Program; 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 Exceptional Family Member Program is a stand-alone application that is accessed through the Enlisted Distribution and Assignment System. It is a menu-driven application that allows users access to the Medical Update function, Education Update function, and the Reporting function. Both the Medical and Education Update Functions are online functions. The physical, mental and educational records of dependents are maintained through the online update functions. This information is taken into consideration before an assignment of an EFMP member is made. EFMP information is used to ensure the welfare of dependents is considered at assignment time. The Reporting function is both a batch and online system. The primary purpose is to provide hardcopy reports of EFMP records. Statistical reports are also generated.

Types of PII collected include personal, contact, and medical 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.

Headquarters, Department of the Army; all Army components and major commands (Army Audit Agency, US Army Cadet Command, Army Criminal Investigation Command, Army Deputy Chief of Staff G-1, Intelligence and Security Command, US Army Recruiting Command, Army Research Institute, US Army Reserve Command, Training and Doctrine Command; the Assistant Secretary of the Army (Financial Management & Comptroller); the DA Inspector General; the Provost Marshal General; Army staff principals in the chain of command; and supervisors and their designated HR and administrative personnel.

**Other DoD Components.**

Specify.

Defense Criminal Investigative Service, Defense Finance and Accounting Service, Defense Manpower Data Center, Defense Security Service, DoD Inspector General, National Guard Bureau, DoD Inspector General, Office of the Secretary of Defense (OSD), OSD (Personnel & Readiness), and the US Military Entrance Processing Command.

**Other Federal Agencies.**

Specify.

Office of Personnel Management, Department of Veterans Affairs, Department of Homeland Security, Citizenship and Immigration Services, Department of Justice, Department Health and Human Services, Federal Bureau of Investigation, Federal child protection services and family support agencies, Federal law enforcement and confinement/correctional agencies, Internal Revenue Service, Selective Service System, Social Security Administration and the National Academy of Sciences.

**State and Local Agencies.**

Specify.

State and local law enforcement agencies, motor vehicle departments, state & local confinement/correctional facilities, medical facilities, state and local child protection services and family support agencies. Information may also be disclosed to local and state Government agencies for compliance with their laws and regulations.

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

Specify.

N/A

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

Specify.

Hospitals and medical providers.

**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.

Information collection is voluntary for civilian employees and applicants for civilian employment, and they can object by refusing to provide the requested information; however, failure to respond will preclude successful processing of an application for family travel and/or command sponsorship. Collection of PII is mandatory for military personnel, and they do not have the opportunity to object to collection of PII, for refusal to provide required information would result in administrative sanctions or punishment under the Uniform Code of Military Justice.

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

N/A

**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.

Civilian employees and applicants for civilian employment consent to the use of their PII when they agree to provide the information. Military personnel are not afforded an opportunity to consent to use of their PII by EFMP, but implicitly consent to capture and use of their information at the time of employment or enlistment in the Department of the Army. Family members of military personnel and civilian employees provide their consent when they sign the required authorization for disclosure of medical information.

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

N/A

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 furnished a Privacy Advisory when PII is collected, and are advised of their rights under the Health Insurance Portability and Accountability Act (HIPPA) Act of 1996 as follows:

"Information will only be used by personnel of the Department of Defense and Military Departments to evaluate and document the medical needs of family members. This information will enable: (1) Military assignment personnel to match the needs of family members against the availability of medical services and to engage in case management after assessment is made; (2) Civilian personnel offices to determine the availability of medical services to meet the medical needs of family members of DoD and Military Department civilian employees; and (3) Managed care support contractor to support your application for further entitlement, i.e., the Extended Care Health Option (ECHO)."