PRIVACY IMPACT ASSESSMENT (PIA)

For the

US Army Family Advocacy System of Records (FASOR)
Department of the Army - US Army Medical Command

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 13777 (DA 201263)

☐ **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 A0608-18 DASG

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.

10 U.S.C. 3013, Secretary of the Army; 42 U.S.C. 10606 et seq., Victims' Rights, as implemented by Department of Defense Instruction 1030.2, Victim and Witness Assistance Program; Army Regulation 608-18, The Family Advocacy Program; 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 U.S. Army Family Advocacy System Of Records (Army FASOR) Web System was procured by the U.S. Army Medical Command to be used by the Army's Family Advocacy Program (FAP). The system stores data from the entries for statistical analysis required for program management and reporting to Department of Defense and Congress. The Army Family Advocacy System of Records (FASOR) statistical database and case management system tracks allegations of abuse for the Army Medical Command. The system also provides an administrative interface to facilitate Case Review Committee (CRC) meetings. The Army's Case Review Committee (CRC) reviews incidents of domestic abuse within the Army to ultimately decide whether the incident meet criteria for abuse and then discuss a treatment approach for the alleged offender and victim. The Decision Tree provides a series of automated decisions that allows the CRC members to vote on one factor at a time before determination occurs. The Decision Tree is also an automated way to capture the votes of the CRC Team members and to provide a final decision at the end of each incident review. System is web-based and is not a stand alone.

Information collected during interview include Unit and Commander Information, dates of abuse incidents, abuse incident numbers and locations, personal history information used to conduct assessments, make determinations of abuse, and devise treatment plans.

PII collected includes personal, financial, medical, employment, and educational.

(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 PII collected are unauthorized access, inaccurate information entered into the application, and unauthorized disclosure of PII. Security safeguards are in place to mitigate these risks.

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. US Army Medical Command, US Army Installation Management Command, Army Criminal Investigation Command, Army Deputy Chief of Staff for Personnel, Army G1, Army Intelligence and Security Command, Army Recruiting Command, Army Research Institute, Army Reserve Command and to Commanders, Army Reserves, Department of the Army Inspectors General, Provost Marshal General, Installation Management Command, Army Staff Principals in the chain of command, and Supervisors and their designated human resources and administrative personnel responsible for processing personnel actions.

☒ **Other DoD Components.**

Specify. Office of Secretary of Defense, DoD Family Advocacy Program, Defense Criminal Investigative Service; Department of Navy, US Marine Corps, US Air Force; Office of the DoD Inspector General and U.S. Military Entrance Processing Command.

☒ **Other Federal Agencies.**

Specify. Congress (Congressional inquiries); US Coast Guard; Federal child protection services and family support agencies, Federal law enforcement and confinement/correctional agencies.

☒ **State and Local Agencies.**

Specify. Law enforcement, child and protective service agencies, and courts of law for each state as ordered.

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

Specify. FAP employees contracted by the federal government use FASOR to conduct FAP duties and have access to this information based on privileging by the Army Central Registry System Administrators. There are provisions in the contract for requiring compliance with the Privacy Act and Health Insurance Portability and Accountability Act (HIPAA). The contractors receive training in these areas.

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

Specify. Civilian researchers - de-identified data.

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.

Individuals can object to the collection of PII during the intake process when they review and sign the Privacy Act Statement, Limits of Confidentiality Statement, and the Family Advocacy Program Information Paper. If the requested information is not furnished, comprehensive health care may not be possible, but CARE WILL NOT BE DENIED.

(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.

Individuals have an opportunity to consent to the specific uses of their PII during the intake process when they review and sign the Privacy Act Statement, Limits of Confidentiality Statement, and the Family Advocacy Program Information Paper. If the individual does not consent to to the specific uses of their PII, care will not be denied.

(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.

1. Privacy Act Statement - Health Care Records, DD Form 2005 is reviewed and signed by the client.

2. Limits of Confidentiality Statement is reviewed and signed for by the client. This statement describes of the limits of the confidentiality of the information which they are providing (for instance, if the client discloses child or intimate partner abuse, suicidality or homicidality, or criminal behavior during an interview, certain authorities must be notified).

3. Family Advocacy Program Information Paper is reviewed and signed for by the client. This Information Paper describes how the FAP works, the rights of the patient and how disclosure of certain information might affect the Service or Family member.

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.