

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:

Family Advocacy System Of Record (FASOR)

2. DOD COMPONENT NAME:

United States Army

3. PIA APPROVAL DATE:

Headquarters, US Army Medical Command

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 type="checkbox"/> Existing DoD Information System | <input checked="" 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.

The U.S. Army Medical Command (MEDCOM) has functional proponentcy for the treatment and case management of the Army Family Advocacy Program (FAP). The US Army Installation Management Command, Family Programs, has primary proponentcy over the Army FAP. To fulfill its responsibility as the functional proponent for the FAP, MEDCOM procured the Family Advocacy System Of Record (FASOR). FASOR is a web-based information system for use by the Army's FAP to collect and manage data regarding incidents of domestic violence and child abuse. This system stores FAP data for statistical analysis required for program management and reporting to Congress and the Department of Defense. It provides an electronic environment to facilitate incident management, including: (1) Case Review Committee meetings; (2) the decision process of domestic violence and child abuse incident determinations; (3) communications within the command; and (4) a treatment approach for the alleged offender and victim.

The FASOR has the following major components:

- Army Central Registry (ACR) Background Check to conduct checks for employment and maltreatment for FAP, Child Care, Human Resources and criminal / investigative purposes.
- FAP Client Intake allows the client to enter the data directly into FASOR using a temporary session key and the FASOR Administrator to manage the intake process.
- FAP Incident Data Entry (formerly DA 7517 section) allows entry of FAP data to manage incidents of abuse, conduct background checks, and provide data to meet high level requirements from Congress, DoD, Army, and other authorized agencies. Data may be auto-fed by the FAP Client Intake module and/or manually input.
- Case Review Committee (CRC), using an automated decision tree algorithm, allows entry of child and adult incidents for abuse determination by the installation's FAP committee.
- FAP Local Database allows generation of FAP local installation reports (e.g., incident, risk, abuse, abuse determination, military unit and FAP supervisory reports.)
- FAP Fatality Reports allows generation of FAP reports regarding local fatalities.

The categories of individuals with records in FASOR include DoD healthcare beneficiaries and members of the public. The DoD healthcare beneficiaries include military, military family members, and other individuals entitled to care in a military treatment facility. The members of the general public include intimate partners, former spouses and children of military members; individuals receiving or providing child care through a federally authorized program; and individuals referred by the FAP for problematic sexual behavior of a child. The types of PII collected include demographics as well as contact, financial, medical, employment and educational information.

This PIA updates the previous PIA approved on 20 September 2017.

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)

The PII is collected for identification purposes to match individuals with their respective records and reports. Additionally, information is collected to properly assess incidents of abuse and neglect and to ensure safety of victims through proper incident management. The PII collected is used for FAP mission-related and administrative purposes to include incident management, record keeping, conducting FAP registry checks, congressional inquiries and statistical analysis.

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.

Individuals have the opportunity to object to the collection of their PII during the FAP intake process. They receive and sign the Department of Defense (DD) Form 2005, Privacy Act Statement – Health Care Records which applies to all requests for personal information made by care treatment personnel for medical/dental treatment purposes and becomes a permanent part of the health care record. This Privacy Act Statement is provided in Section 1g below. If individuals object to the collection of their PII, comprehensive health care may not be possible, but care is not denied.

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.

Individuals have the opportunity to consent to the specific uses of their PII during the FAP intake process. They receive and sign DD Form 2005, Privacy Act Statement - Health Care Records, which outlines the specific uses of their PII and becomes a permanent part of health care record. This Privacy Act Statement is provided in Section 1g below. If the individuals object to the specific uses of their PII, comprehensive health care may not be possible, but care is not denied.

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

DD FORM 2005, June 2016, PRIVACY ACT STATEMENT - HEALTH CARE RECORDS

1. AUTHORITY FOR COLLECTION OF INFORMATION INCLUDING SOCIAL SECURITY NUMBER (SSN):

10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C. Chapter 55, Medical and Dental Care; 42 U.S.C. Chapter 32, Third Party Liability for Hospital and Medical Care; 32 CFR Part 199, Civilian Health and Medical Program of the Uniformed Services (CHAMPUS); DoDI 6055.05, Occupational and Environmental Health (OEH); and E.O. 9397 (SSN), as amended.

2. PRINCIPAL PURPOSES FOR WHICH INFORMATION IS INTENDED TO BE USED:

Information may be collected from you to provide and document your medical care; determine your eligibility for benefits and entitlements; adjudicate claims; determine whether a third party is responsible for the cost of Military Health System (MHS) provided healthcare and recover that cost; evaluate your fitness for duty and medical concerns which may have resulted from an occupational or environmental hazard; evaluate the MHS and its programs; and perform administrative tasks related to MHS operations and personnel readiness.

3. ROUTINE USES:

Information in your records may be disclosed to:

- Private physicians and Federal agencies, including the Department of Veterans Affairs, Health and Human Services, and Homeland Security (with regard to members of the Coast Guard), in connection with your medical care;
- Government agencies to determine your eligibility for benefits and entitlements;
- Government and nongovernment third parties to recover the cost of MHS provided care;
- Public health authorities to document and review occupational and environmental exposure data; and
- Government and nongovernment organizations to perform DoD-approved research.

Information in your records may be used for other lawful reasons which may include teaching, compiling statistical data, and evaluating the care rendered. Use and disclosure of your records outside of DoD may also occur in accordance with 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, which incorporates the DoD Blanket Routine Uses published at: <http://dpcl.dod.mil/privacy/SORNsIndex/BlanketRoutineUses.aspx>.

Any protected health information (PHI) in your records may be used and disclosed generally as permitted by the HIPAA Privacy Rule (45 CFR Parts 160 and 164), as implemented within DoD by DoD 6025.18-R. Permitted uses and disclosures of PHI include, but are not limited to, treatment, payment, and healthcare operations.

4. WHETHER DISCLOSURE IS MANDATORY OR VOLUNTARY AND EFFECT ON INDIVIDUAL OF NOT PROVIDING

INFORMATION:

Voluntary. If you choose not to provide the requested information, comprehensive health care services may not be possible, you may experience administrative delays, and you may be rejected for service or an assignment. However, care will not be denied.

This all inclusive Privacy Act Statement will apply to all requests for personal information made by MHS health care treatment personnel or for medical/dental treatment purposes and is intended to become a permanent part of your health care record.

Your signature merely acknowledges that you have been advised of the foregoing. If requested, a copy of this form will be furnished to you.

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

<input checked="" type="checkbox"/> Within the DoD Component	Specify.	US Army Public Health Center G-1, US Army Center for Substance Abuse Programs US Army Medical Command US Army Installation Management Command US Army Criminal Investigation Command US Army Deputy Chief of Staff for Personnel US Army Intelligence and Security Command US Army Recruiting Command Department of the Army Inspectors General Provost Marshal General US Army Human Resources Command
<input checked="" type="checkbox"/> Other DoD Components	Specify.	Defense Manpower Data Center
<input checked="" type="checkbox"/> Other Federal Agencies	Specify.	US Coast Guard Federal child protection services and family support agencies Federal law enforcement and confinement/correctional agencies
<input checked="" type="checkbox"/> State and Local Agencies	Specify.	Law enforcement, child and protective service agencies, and courts of law for each state as ordered.
<input checked="" type="checkbox"/> 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.	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 requiring compliance with the Privacy Act and Health Insurance Portability and Accountability Act (HIPAA). The contractors also receive training in these areas.
<input checked="" type="checkbox"/> Other (e.g., commercial providers, colleges).	Specify.	Researchers with an approved Institutional Review Board application and MEDCOM Data Sharing Agreement.

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

<input checked="" type="checkbox"/> Individuals	<input type="checkbox"/> Databases
<input checked="" type="checkbox"/> Existing DoD Information Systems	<input type="checkbox"/> Commercial Systems
<input type="checkbox"/> Other Federal Information Systems	

- Individuals: PII is collected from the FAP intake documents the individuals complete as well as from personnel who FAP personnel collaborate with to assess abuse and neglect incidents. These individuals include Child Protective Services and other investigative agency personnel; Military Unit Commanders; medical providers; witnesses; and family members.
- Existing DoD Information Systems: PII is collected from the electronic health records (EHR) to include Military Health System (MHS) GENESIS, Composite Health Care System (CHCS) and the Armed Forces Health Longitudinal Technology Application (AHLTA).

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

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

Official Forms:

- MEDCOM Form 811, Behavioral Health Intake-Psychosocial History and Assessment. Individuals receive and sign DD Form 2005, Privacy Act Statement - Health Care Records, before completing MEDCOM Form 811.

Other: A staff member manually enters the PII obtained from the EHR. The FASOR has no electronic interfaces with any external information systems.

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.d.defense.gov/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.

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.

KE5. Event is after the end of the calendar year in which the case is closed. Keep in CFA until event occurs then destroy 5 years after the event. Note: During the period of retention, if there is a new report on the same family within days or weeks, the record may be used to provide demographic and assessment information about the family so that the family need not be totally reassessed. Materials prepared using electronic media (e.g., word processing applications or e-mail) are to be printed and included in the official jackets. The electronic version is to be deleted when file copy is generated or when no longer needed for reference or updating.

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.

10 U.S.C. 7013, 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 (FAP); and E.O. 9397 (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.

The information collected in this system is for the diagnosis and treatment of medical disorders and is not considered a public information collection in accordance with DoDM 8910.01, V2, Encl 3, paragraph 8b(5).

SECTION 2: PII RISK REVIEW

a. What PII will be collected (a data element alone or in combination that can uniquely identify an individual)? (Check all that apply)

- | | | |
|--|--|--|
| <input type="checkbox"/> Biometrics | <input checked="" type="checkbox"/> Birth Date | <input checked="" type="checkbox"/> Child Information |
| <input type="checkbox"/> Citizenship | <input checked="" type="checkbox"/> Disability Information | <input checked="" type="checkbox"/> DoD ID Number |
| <input type="checkbox"/> Driver's License | <input checked="" type="checkbox"/> Education Information | <input checked="" type="checkbox"/> Emergency Contact |
| <input checked="" type="checkbox"/> Employment Information | <input checked="" type="checkbox"/> Financial Information | <input checked="" type="checkbox"/> Gender/Gender Identification |
| <input checked="" type="checkbox"/> Home/Cell Phone | <input checked="" type="checkbox"/> Law Enforcement Information | <input checked="" type="checkbox"/> Legal Status |
| <input checked="" type="checkbox"/> Mailing/Home Address | <input checked="" type="checkbox"/> Marital Status | <input checked="" type="checkbox"/> Medical Information |
| <input checked="" type="checkbox"/> Military Records | <input checked="" type="checkbox"/> Mother's Middle/Maiden Name | <input checked="" type="checkbox"/> Name(s) |
| <input checked="" type="checkbox"/> Official Duty Address | <input checked="" type="checkbox"/> Official Duty Telephone Phone | <input checked="" type="checkbox"/> Other ID Number |
| <input type="checkbox"/> Passport Information | <input checked="" type="checkbox"/> Personal E-mail Address | <input checked="" type="checkbox"/> Photo |
| <input checked="" type="checkbox"/> Place of Birth | <input checked="" type="checkbox"/> Position/Title | <input checked="" type="checkbox"/> Protected Health Information (PHI) ¹ |
| <input checked="" type="checkbox"/> Race/Ethnicity | <input checked="" type="checkbox"/> Rank/Grade | <input checked="" type="checkbox"/> Religious Preference |
| <input checked="" type="checkbox"/> Records | <input checked="" type="checkbox"/> Security Information | <input checked="" type="checkbox"/> Social Security Number (SSN) (Full or in any form) |
| <input checked="" type="checkbox"/> Work E-mail Address | <input checked="" type="checkbox"/> If Other, enter the information in the box below | |

Other: Spouse Information and photographs of injuries or other sequelae of abuse or neglect.

If the SSN is collected, complete the following questions.

(DoD Instruction 1000.30 states that all DoD personnel shall reduce or eliminate the use of SSNs wherever possible. SSNs shall not be used in spreadsheets, hard copy lists, electronic reports, or collected in surveys unless they meet one or more of the acceptable use criteria.)

(1) Is there a current (dated within two (2) years) DPCLTD approved SSN Justification on Memo in place?

Yes No

If "Yes," provide the signatory and date approval. If "No," explain why there is no SSN Justification Memo.

The approved SSN Justification Memo was signed by Ms. Cindy L. Allard, Chief, Defense Privacy, Civil Liberties and Transparency Division, on 6 December 2018.

(2) Describe the approved acceptable use in accordance with DoD Instruction 1000.30 "Reduction of Social Security Number (SSN) Use within DoD".

The Defense Privacy, Civil Liberties and Transparency Division (DPCLTD) accepted/approved the justification to use the SSN for the purposes of (2) Law Enforcement, National Security and Credentialing, since it receives information from federal, state and local law enforcement entities which may use the SSN as the primary identifier of sponsors, victims and alleged perpetrators of child and domestic violence. Additionally, this justification was approved for acceptable use (11) Legacy System Interface since FASOR is the Army's source of records for Departmental reporting under DoDM 6400.01, Volume 2.

(3) Describe the mitigation efforts to reduce the use including visibility and printing of SSN in accordance with DoD Instruction 1000.30, "Reduction of Social Security Number (SSN) Use within DoD".

To minimize the unauthorized disclosure of the SSN, the following business practices and security controls are in place:

- Administrative, technical, and physical security controls to prevent unauthorized access and unauthorized disclosure of SSN.
- Documents containing SSN have strict approval and release processes.
- Encryption is used to protect data in transit and data at rest.
- There is role-restricted access to the SSN data. Per approved procedures, only authorized personnel access the SSN data in the system.
- All personnel with access to the system database are required to sign non-disclosure agreements and are trained in the use and protection of personally identifiable information (PII).
- Data is never stored on mobile computing or removable electronic media.

(4) Has a plan to eliminate the use of the SSN or mitigate its use and or visibility been identified in the approved SSN Justification request?

If "Yes," provide the unique identifier and when can it be eliminated?

If "No," explain.

Yes No

Inclusion of the DoD ID number was a new requirement and planned for development and deployment across Army FAPs. In the interim, the SSN must be used to maintain the integrity and utility of FAP data in FASOR. The use of the DoD ID Number has been incorporated in the scheduled modernization of FASOR with an expected completion date of Fall 2024.

b. What is the PII confidentiality impact level²?

Low Moderate High

¹The definition of PHI involves evaluating conditions listed in the HIPAA. Consult with General Counsel to make this determination.

²Guidance on determining the PII confidentiality impact level, see Section 2.5 "Categorization of PII Using NIST SP 800-122." Use the identified PII confidentiality impact level to apply the appropriate Privacy Overlay low, moderate, or high. This activity may be conducted as part of the categorization exercise that occurs under the Risk Management Framework (RMF). Note that categorization under the RMF is typically conducted using the information types described in NIST Special Publication (SP) 800-60, which are not as granular as the PII data elements listed in the PIA table. Determining the PII confidentiality impact level is most effective when done in collaboration with the Information Owner, Information System Owner, Information System Security Manager, and representatives from the security and privacy organizations, such as the Information System Security Officer (ISSO) and Senior Component Official for Privacy (SCOP) or designees.

c. How will the PII be secured?

(1) Physical Controls. *(Check all that apply)*

- | | |
|---|--|
| <input type="checkbox"/> Cipher Locks | <input checked="" type="checkbox"/> Closed Circuit TV (CCTV) |
| <input type="checkbox"/> Combination Locks | <input checked="" type="checkbox"/> Identification Badges |
| <input checked="" type="checkbox"/> Key Cards | <input checked="" type="checkbox"/> Safes |
| <input checked="" type="checkbox"/> Security Guards | <input checked="" type="checkbox"/> If Other, enter the information in the box below |

Other: Paper-based records that are maintained behind double locked doors and in locked file cabinets.

(2) Administrative Controls. *(Check all that apply)*

- Backups Secured Off-site
- Encryption of Backups
- Methods to Ensure Only Authorized Personnel Access to PII
- Periodic Security Audits
- Regular Monitoring of Users' Security Practices
- If Other, enter the information in the box below

Other:

- System users receive Information Assurance, Privacy Act, and Health Insurance Portability and Accountability Act (HIPAA) training annually.
- System users are subjected to a FAP central registry check to confirm that they have no adverse information recorded in FASOR.

(3) Technical Controls. *(Check all that apply)*

- | | | |
|---|---|---|
| <input type="checkbox"/> Biometrics | <input checked="" type="checkbox"/> Common Access Card (CAC) | <input checked="" type="checkbox"/> DoD Public Key Infrastructure Certificates |
| <input checked="" type="checkbox"/> Encryption of Data at Rest | <input checked="" type="checkbox"/> Encryption of Data in Transit | <input checked="" type="checkbox"/> External Certificate Authority Certificates |
| <input checked="" type="checkbox"/> Firewall | <input checked="" type="checkbox"/> Intrusion Detection System (IDS) | <input type="checkbox"/> Least Privilege Access |
| <input type="checkbox"/> Role-Based Access Controls | <input type="checkbox"/> Used Only for Privileged (Elevated Roles) | <input checked="" type="checkbox"/> User Identification and Password |
| <input checked="" type="checkbox"/> Virtual Private Network (VPN) | <input type="checkbox"/> If Other, enter the information in the box below | |

d. What additional measures/safeguards have been put in place to address privacy risks for this information system or electronic collection?

All of the measures/safeguards to address privacy risks are identified in Section 2c above.

SECTION 3: RELATED COMPLIANCE INFORMATION

a. Is this DoD Information System registered in the DoD IT Portfolio Repository (DITPR) or the DoD Secret Internet Protocol Router Network (SIPRNET) Information Technology (IT) Registry or Risk Management Framework (RMF) tool³?

<input checked="" type="checkbox"/> Yes, DITPR	DITPR System Identification Number	13777 / APMS: DA201263
<input type="checkbox"/> Yes, SIPRNET	SIPRNET Identification Number	
<input checked="" type="checkbox"/> Yes, RMF tool	RMF tool Identification Number	793
<input type="checkbox"/> No		

If "No," explain.

b. DoD information systems require assessment and authorization under the DoD Instruction 8510.01, "Risk Management Framework for DoD Information Technology".

Indicate the assessment and authorization status:

<input type="checkbox"/> Authorization to Operate (ATO)	Date Granted:	
<input checked="" type="checkbox"/> ATO with Conditions	Date Granted:	9/1/2020
<input type="checkbox"/> Denial of Authorization to Operate (DATO)	Date Granted:	
<input type="checkbox"/> Interim Authorization to Test (IATT)	Date Granted:	

(1) If an assessment and authorization is pending, indicate the type and projected date of completion.

ATD - 9/1/2021

(2) If an assessment and authorization is not using RMF, indicate the projected transition date.

c. Does this DoD information system have an IT investment Unique Investment Identifier (UII), required by Office of Management and Budget (OMB) Circular A-11?

Yes No

If "Yes," Enter UII If unsure, consult the component IT Budget Point of Contact to obtain the UII

³Guidance on Risk Management Framework (RMF) tools (i.g., eMASS, Xacta, and RSA Archer) are found on the Knowledge Service (KS) at <https://rmfks.osd.mil>.

SECTION 4: REVIEW AND APPROVAL SIGNATURES

Completion of the PIA requires coordination by the program manager or designee through the information system security manager and privacy representative at the local level. Mandatory coordinators are: Component CIO, Senior Component Official for Privacy, Component Senior Information Security Officer, and Component Records Officer.

a. Program Manager or Designee Name	Pamela J. Porch	(1) Title	FASOR Program Manager	
	(2) Organization	Family Advocacy Program (FAP) Behavioral Health Service Line, HCD, G3/5/7 HQ, US Army Medical Command	(3) Work Telephone	210-295-7317
	(4) DSN	421-7317	(5) E-mail address	pamela.j.porch.civ@mail.mil
	(6) Date of Review		(7) Signature	
b. Other Official (to be used at Component discretion)	Mr. John P. Peterson	(1) Title	Chief, FOIA and Privacy Office	
	(2) Organization	Headquarters, US Army Medical Command	(3) Work Telephone	210-466-5933
	(4) DSN	460-5933	(5) E-mail address	
	(6) Date of Review		(7) Signature	
c. Other Official (to be used at Component discretion)	Mr. Alan W. Daugherty	(1) Title	Cyber Security Compliance Manager	
	(2) Organization	Headquarters, US Army Medical Command	(3) Work Telephone	210-221-7937
	(4) DSN	DSN 471-7937	(5) E-mail address	alan.w.daugherty.civ@mail.mil
	(6) Date of Review	07/22/20	(7) Signature	
d. Component Privacy Officer (CPO)	Myron F. Wong	(1) Title	Chief, Army Privacy and Civil Liberties	
	(2) Organization	RMDA/AHS/OAA	(3) Work Telephone	(571) 515-0243
	(4) DSN		(5) E-mail address	myron.f.wong.civ@mail.mil
	(6) Date of Review	01/28/21	(7) Signature	

e. Component Records Officer	Anthony D. Crawley-Gibson	(1) Title	United States Army Records Officer Chief, Army Records Management Division
	(2) Organization Records Management Declassification Agency (RMDA)	(3) Work Telephone	571-515-0218
	(4) DSN 94-312	(5) E-mail address	anthony.d.crawley-gibson.civ@mail.mil
	(6) Date of Review 01/22/21	(7) Signature	
f. Component Senior Information Security Officer or Designee Name	Cheryl L Hynes	(1) Title	Cybersecurity Division Chief
	(2) Organization Army CIO/G6	(3) Work Telephone	703-545-1549
	(4) DSN 865-1549	(5) E-mail address	cheryl.l.hynes.civ@mail.mil
	(6) Date of Review:	(7) Signature	
g. Senior Component Official for Privacy (SCOP) or Designee Name	Susan D. Tigner, SES	(1) Title	Executive Director, Army Headquarters Services (AHS), and Army SCOP
	(2) Organization AHS/OAA	(3) Work Telephone	(703) 545-4870
	(4) DSN	(5) E-mail address	susan.d.tigner.civ@mail.mil
	(6) Date of Review	(7) Signature	
h. Component CIO Reviewing Official Name	Nancy Kreidler	(1) Title	Director, Cybersecurity
	(2) Organization Army CIO/G6	(3) Work Telephone	703-545-1688
	(4) DSN 865-1688	(5) E-mail address	nancy.kreidler.civ@mail.mil
	(6) Date of Review	(7) Signature	

Publishing: Only Section 1 of this PIA will be published. Each DoD Component will maintain a central repository of PIAs on the Component's public Web site. DoD Components will submit an electronic copy of each approved PIA to the DoD CIO at: osd.mc-alex.dod-cio.mbx.pia@mail.mil.

If the PIA document contains information that would reveal sensitive information or raise security concerns, the DoD Component may restrict the publication of the assessment to include Section 1.