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:

Air Force Family Integrated Results & Statistical Tracking (AFFIRST) System

2. DOD COMPONENT NAME:

United States Air Force

3. PIA APPROVAL DATE:

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: foreign nationals are included in general public.)*

- [ ] From members of the general public
- [ ] From Federal employees and/or Federal contractors
- [x] From both members of the general public and Federal employees and/or Federal contractors
- [ ] Not Collected *(if checked proceed to Section 4)*

b. The PII is in a: *(Check one)*

- [ ] New DoD Information System
- [ ] New Electronic Collection
- [ ] Existing DoD Information System
- [x] Existing Electronic Collection
- [ ] 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.

To compile information on client's visits to enable the Center to refer clients to the appropriate support activity, i.e., Mental Health Clinic, Chaplain, Air Force Aid, etc. Information is compiled for statistical reporting to base, major commands, Headquarters United States Air Force, Department of Defense, Office of Secretary of Defense (OSD) and Congress. Reports and for program planning and evaluation. Personal demographic information (i.e., Name, DOD IN, Organization, Office Symbol, Marital status, etc.) and service delivery information is colletected.

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)*

Verification, identification and A&FRC mission-related use. The data elements being captured are important/necessary for obtaining an accurate picture/history of customer needs in order to help determine the best course of action(s) to meet all identified needs to ensure a high level of mission/family readiness and resiliency. In addition, data captured in, and reported from AFFIRST provides vital information concerning effectiveness of A&FRC services that is used by local A&FRCs and their MAJCOM, Operations/Airstaff Policy counterparts to help determine future direction and emphasis of services to obtain optimum mission/family readiness.

e. Do individuals have the opportunity to object to the collection of their PII? [x] 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.

A&FRC staff provide a Statement of Understanding (SOU) to advise customers that the information provided is voluntary and provides the consequences of choosing not to provide requested information. The Air Force rules for accessing records and for contesting contents and appealing initial agency determinations are published in Air Force Instruction 33-332, Air Force Privacy and Civil Liberties Program; 32 CFR part 806b; or may be obtained from the system manager.

f. Do individuals have the opportunity to consent to the specific uses of their PII? [x] 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.

The A&FRC staff provide a Statement of Understanding (SOU) to advise customers that the information provided is voluntary and provides the consequences of choosing not to provide requested information. Individuals seeking to determine whether this system of records contains information on themselves should address written inquiries to the system manager, or the installation Airman and Family Center. Official mailing addresses are published as an appendix to the Air Force's compilation of systems of records notices. Proof of identity such as an Armed Forces Identification Card/Common Access Card (CAC) will be required for personal visits.

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.)*

[X] Privacy Act Statement [ ] Privacy Advisory [ ] Not Applicable

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

10 U.S.C. 8013, Secretary of the Air Force; Air Force Instruction 36-3009, Airman and Family Readiness Centers; and E.O. 9397 (SSN), as amended.

PURPOSE(S):

To maintain a record of customer service data determining the effectiveness of Airman and Family Readiness Center activities and services and provide reports reflecting impact of services on mission and family readiness to leadership. Also used as a management tool for statistical analysis, tracking, reporting, evaluating program effectiveness, and conducting research.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, these records contained therein may be specifically disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

Congressional Inquiries Disclosure Routine Use: Disclosure from a system of records maintained by a DoD Component may be made to a congressional office from the record of an individual in response to an inquiry from the congressional office made at the request of that individual.

Data Breach Remediation Purposes Routine Use: A record from a system of records maintained by a Component may be disclosed to appropriate agencies, entities, and persons when (1) The Component suspects or has confirmed that the security or confidentiality of the information in the system of records has been compromised; (2) the Component has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Component or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Components efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

System of Records Notice: F036 AFPC Z, Air Force Family Integrated Results and Statistical Tracking (AFFIRST)

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

[ ] Within the DoD Component	Specify.	
[ ] Other DoD Components	Specify.	
[ ] Other Federal Agencies	Specify.	
[ ] State and Local Agencies	Specify.	
[ ] 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.	
[ ] Other *(e.g., commercial providers, colleges).*	Specify.	

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

[X] Individuals
[X] Existing DoD Information Systems
[ ] Other Federal Information Systems
[ ] Databases
[ ] Commercial Systems

Manual keying in of customer demographic and service delivery information. Additionally electronically via a Memorandum of Agreement (MOA) with the Defense Manpower Data Center (DMDC) for use of their Real-Time Broker (RTB) Web service that allows updating of AFFIRST customer record demographic data.

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

- [x] E-mail
- [ ] Official Form (*Enter Form Number(s) in the box below)*
- [x] Face-to-Face Contact
- [x] Paper
- [ ] Fax
- [x] Telephone Interview
- [x] Information Sharing - System to System
- [ ] Website/E-Form
- [ ] Other *(If Other, enter the information in the box below)*

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.

- [x] Yes
- [ ] No

If "Yes," enter SORN System Identifier: F036 AFPC Z

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or http://dpcld.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. T 36 - 07 R 02.00

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

Electronic Records are destroyed after one year or when no longer needed whichever is later. Electronic records are destroyed by erasing, deleting, or overwriting.

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 statue 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 United States Code (U.S.C.) 8013, Secretary of the Air Force: powers and duties; delegation by; as implemented by Air Force Instruction 36-3009, Airman and Family Readiness Centers; and Executive Order (E.O.) 9397 (Social Security Number - SSN), as amended.

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.

AFFIRST OMB Control Number: 0701-0070 Submitted renewal in Mar 2017. Awaiting approval of renewal.

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)*

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

One of the A&FRC core programs (per AFI 36-3009, Airman and Family Readiness Center) is Personal Financial Management. Financial service data is limited to information needed to complete a mutually agreeable spending/action plan to meet customer financial goals. All but last four of SSN is masked in the system.

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?

[x] Yes [ ] No

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

Signatory/Date Approved: Kimberly K. Toney, SES/USAF, AFPC Executive Director, 6 Apr 2017. According to HAF SAF/CIO A6 SSM memo submitted to DoD on 11 Aug 2017 for final processing/approval.

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

SSN uses for legacy system interfaces described in DODI 10003.30, Enclosure 2, Para 2.c.(11).

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

We are working towards transition to the DODID as the system primary record identifier vs. the SSN.

(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.

[x] Yes [ ] No

SSN. Can be eliminated in approximately 18 months.

b. What is the PII confidentiality impact level[2]? [ ] Low [x] Moderate [ ] High

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

[2] Guidance 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)*

- [x] Cipher Locks
- [x] Combination Locks
- [x] Key Cards
- [x] Security Guards
- [x] Closed Circuit TV (CCTV)
- [x] Identification Badges
- [x] Safes
- [ ] If Other, enter the information in the box below

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

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

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

- [ ] Biometrics
- [x] Encryption of Data at Rest
- [x] Firewall
- [x] Role-Based Access Controls
- [x] Virtual Private Network (VPN)
- [x] Command Access Card (CAC)
- [x] Encryption of Data in Transit
- [ ] Intrusion Detection System (IDS)
- [ ] Used Only for Privileged (Elevated Roles)
- [ ] If Other, enter the information in the box below
- [x] DoD Public Key Infrastructure Certificates
- [x] External Certificate Authority Certificates
- [x] Least Privilege Access
- [x] User Identification and Password

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

A&FRC staffs and MAJCOM/HQ Operations/Policy counterparts, System Administrators and Developer/Contractor (Developer/Contractor do not view records as a matter of course, but will perform proactive and reactive system maintenance of the records database (re-indexing, repairing corrupted records/files, etc.). Additionally, the aforementioned access is limited via user account (CAC Login required) permissions based on system role, security protocols and correlating interface limitations to visibility of only what is needed to perform assigned duties. Web access via secure SSL (HTTPS) connection and enforcement of need-to-know principle.

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) tool[3]?

[x] Yes, DITPR	DITPR System Identification Number	9051
[ ] Yes, SIPRNET	SIPRNET Identification Number	
[x] Yes, RMF tool	RMF tool Identification Number	1599
[ ] 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:

[x] Authorization to Operate (ATO)	Date Granted: 22 Dec 2016
[ ] ATO with Conditions	Date Granted:
[ ] Denial of Authorization to Operate (DATO)	Date Granted:
[ ] Interim Authorization to Test (IATT)	Date Granted:

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

(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?

[x] Yes [ ] No

If "Yes," Enter UII 007-000004814 If unsure, consult the component IT Budget Point of Contact to obtain the UII

[3]Guidance 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	Patrick I. Woodworth	(1) Title	Data & Resource Manager
(2) Organization	AFPC/DPFF	(3) Work Telephone	210-565-3280
(4) DSN	665-3280	(5) E-mail address	patrick.woodworth@us.af.mil
(6) Date of Review	01/26/18	(7) Signature	WOODWORTH.PATRICK.I.I.1171943546 Digitally signed by WOODWORTH.PATRICK.I.I.1171943546 Date: 2018.02.20 08:00:02 -06'00'
b. Other Official ***(to be used at Component discretion)***	David R. Belval	(1) Title	David R. Belval
(2) Organization	AFPC/DFCC	(3) Work Telephone	210-565-3203
(4) DSN	665-3203	(5) E-mail address	david.belval.2@us.af.mil
(6) Date of Review		(7) Signature	BELVAL.DAVID.ROBERT.1007397530 Digitally signed by BELVAL.DAVID.ROBERT.1007397530 Date: 2018.02.22 10:19:09 -06'00'
c. Other Official *(to be used at Component discretion)*	JUAN NIEVES	(1) Title	HQ AFPC FOIA/PA POLICY OFFICER
(2) Organization	HQ AFPC/DSME	(3) Work Telephone	210-565-3576
(4) DSN	665-3576	(5) E-mail address	juan.nieves.5@us.af.mil
(6) Date of Review		(7) Signature	NIEVES.JUAN.P C.1132704992 Digitally signed by NIEVES.JUAN.P C.1132704992 Date: 2018.02.23 11:01:29 -06'00'
d. Component Privacy Officer (CPO)		(1) Title	
(2) Organization		(3) Work Telephone	
(4) DSN		(5) E-mail address	
(6) Date of Review		(7) Signature	

e. Component Records Officer		(1) Title	
(2) Organization		(3) Work Telephone	
(4) DSN		(5) E-mail address	
(6) Date of Review		(7) Signature	
f. Component Senior Information Security Officer or Designee Name		(1) Title	
(2) Organization		(3) Work Telephone	
(4) DSN		(5) E-mail address	
(6) Date of Review:		(7) Signature	
g. Senior Component Official for Privacy (SCOP) or Designee Name		(1) Title	
(2) Organization		(3) Work Telephone	
(4) DSN		(5) E-mail address	
(6) Date of Review		(7) Signature	
h. Component CIO Reviewing Official Name		(1) Title	
(2) Organization		(3) Work Telephone	
(4) DSN		(5) E-mail address	
(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.mill.

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.