

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)

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.)

- | | |
|--|--|
| <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.

To compile information on client's visits to enable the Center to refer clients to the appropriate support/helping 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, DODID, Organization, Office Symbol, Marital status, etc.) and service delivery information is collected.

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 Airman & Family Readiness Center (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? 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? 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 A&FRC. 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.)

Privacy Act Statement Privacy Advisory Not Applicable

AUTHORITY:

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.

PRINCIPLE 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. iNF never disclosed to any entity outside of DoD official use.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, 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:

The DoD 'Blanket Routine Uses' published at the beginning of the Air Force compilation of systems of records notices apply to this system.

DISCLOSURE IS VOLUNTARY:

Voluntary

Site Restriction

This site is intended for the use of United States Government Agencies only. Do not reproduce or distribute the content of this site to a wider audience without coordination with the information owner and your unit public affairs office.

Monitoring Notice

This is a Department of Defense computer system. DoD computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Monitoring includes active attacks by authorized DoD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied, and used for authorized purposes. All information, including personal information, placed or sent over this system may be monitored. Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action. Use of this system constitutes consent to monitoring for these purposes.

External Links

None

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)

- | | | |
|---|----------|--|
| <input checked="" type="checkbox"/> Within the DoD Component | Specify. | United States Air Force |
| <input type="checkbox"/> Other DoD Components | Specify. | |
| <input type="checkbox"/> Other Federal Agencies | Specify. | |
| <input type="checkbox"/> State and Local Agencies | Specify. | |
| <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. | ThreeWire Systems, Inc, in performance of contract duties. Contract requires baseline IA controls be implemented to ensure PII is safeguarded. |
| <input type="checkbox"/> 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)

- | | |
|--|---|
| <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 | |

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)

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

- 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://dpclid.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.

Current SORN is in the process of being consolidated into F036 AF PC Q

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.

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 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 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, Air Force Family Integrated Results & Statistical Tracking (AFFIRST), Expiration Date: 30 Nov 2021

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 type="checkbox"/> Disability Information | <input checked="" type="checkbox"/> DoD ID Number |
| <input type="checkbox"/> Driver's License | <input type="checkbox"/> Education Information | <input type="checkbox"/> Emergency Contact |
| <input 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 type="checkbox"/> Law Enforcement Information | <input type="checkbox"/> Legal Status |
| <input checked="" type="checkbox"/> Mailing/Home Address | <input checked="" type="checkbox"/> Marital Status | <input type="checkbox"/> Medical Information |
| <input type="checkbox"/> Military Records | <input type="checkbox"/> Mother's Middle/Maiden Name | <input checked="" type="checkbox"/> Name(s) |
| <input type="checkbox"/> Official Duty Address | <input checked="" type="checkbox"/> Official Duty Telephone Phone | <input type="checkbox"/> Other ID Number |
| <input type="checkbox"/> Passport Information | <input checked="" type="checkbox"/> Personal E-mail Address | <input type="checkbox"/> Photo |
| <input type="checkbox"/> Place of Birth | <input type="checkbox"/> Position/Title | <input type="checkbox"/> Protected Health Information (PHI) ¹ |
| <input type="checkbox"/> Race/Ethnicity | <input checked="" type="checkbox"/> Rank/Grade | <input type="checkbox"/> Religious Preference |
| <input type="checkbox"/> Records | <input 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 | |

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?

- 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, 11 Mar 2021. Submitting to HAF SAF/CIO A6 with OMB number renewal package.

(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. 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.

- Yes No

SSN can be eliminated in approximately 18 months.

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

c. How will the PII be secured?

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

- | | |
|---|---|
| <input checked="" type="checkbox"/> Cipher Locks | <input checked="" type="checkbox"/> Closed Circuit TV (CCTV) |
| <input checked="" 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 type="checkbox"/> If Other, enter the information in the box below |

(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

(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 type="checkbox"/> Intrusion Detection System (IDS) | <input checked="" type="checkbox"/> Least Privilege Access |
| <input checked="" 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?

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.