PRIVACY IMPACT ASSESSMENT (PIA)

For the

Air Force Military Personnel System (AFMILPERS)
United States Air Force

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	10245
☐	**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 007-57-01-20-01-1237-00

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 F036 AF PC C, Military Personnel Records System

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.

Authority
10 United States Code (USC) 8013, Secretary of the Air Force: powers and duties; delegation by; as implemented by Air Force Instruction 40-501; and E.O. 9397 and 13478 (SSN)

Purpose
Military personnel records are used at all levels of Air Force personnel management within the agency for actions/processes related to procurement, education and training, classification, assignment, career development, evaluation, promotion, compensation, sustentation, separation and retirement.

Routine uses
In addition to those disclosures generally permitted under 5 U.S.C. 522a(b) of Privacy Act, these records or information contained therein may specifically be 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's compilation of systems of records notices apply to this system.

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.

AFMILPERS is an Air Force Personnel Center (AFPC)–developed web network, which allows users to access public and private pages in order to perform military personnel actions. There are numerous web applications that reside on the AFMILPERS, which share the same infrastructure. Some of these systems and applications include the Virtual Military Personnel Flight (vMPF), Assignment Management System (AMS), Reserve Management Vacancy System (RMVS), etc. These applications and others reside on the AF MILPERS infrastructure will inherit some of the network-related Information Assurance (IA) controls.

All of the names, Social Security Numbers, and other information are collected from the individual to ensure that the right person is logging in or submitting a request. The information that is pulled from the Military Personnel Data System (MilPDS) is used to execute component programs and to allow the Business Process Owner (BPO) to use this information to get the job done and help the customer in the field.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

Unless the system is hacked, vulnerability of privacy information is minimal. If the system is compromised, general customer demographic and a limited number of SSN accounts with associated date of birth information would be vulnerable. To limit this potential privacy risk, the applications within AFMILPERS only display full SSNs when absolutely needed.

Records are accessed by person(s) responsible for servicing the records system in performance of their official duties and by authorized personnel who are properly screened and cleared for need-to-know. Records are stored in locked room, cabinets, and in computer storage devices protected by computer system software.

Security perimeter protections (firewall, intrusion detection, router access control list, etc.) are also in place.

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. Air Education and Training Command (AETC), Air National Guard, and Air Force Reserve

☐ **Other DoD Components.**

Specify.

☒ **Other Federal Agencies.**

Specify. Dept of Veterans Affairs (VA) and Dept of Labor

☒ **State and Local Agencies.**

Specify. State VA Offices

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

Specify.

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

Specify.

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.

All personal data collected are voluntarily given by the subject individual. Forms that collect personal data to be maintained in this Information Technology (IT) investment contain a Privacy Act Statement, as required by 5 USC 552a(e), and in accordance with guidelines established in AFI 33-332, Privacy Act Program, Chapters 3, 7, and 12, allowing the individual to make an informed decision about providing the data. The statement of understanding advises the individual that the information provided is voluntary and provides the consequences of choosing not to participate with the information collection. Individuals may raise an objection with the Air Force Privacy Act office during the public comment period of the Privacy Act system of records notice (if applicable) or during the data collection.

(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.

Forms that collect personal data will contain a Privacy Act Statement, as required by 5 USC 552a(e)(3), and in accordance with guidelines established in AFI 33-332, Privacy Act Program, Chapters 3 and 7, and 12, allowing the individual to make an informed decision about providing the data or participating in the program. Individuals may raise an objection with the Air Force Privacy Act Office during the comment period (if applicable), during data collection, or at any time after the program is launched. If no objections are received, consent is presumed.

(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.	Forms that collect personal data will contain a Privacy Act Statement, as required by 5 USC 552a(e)(3), and in accordance with guidelines established in AFI 33-332, Privacy Act Program, Chapters 3 and 7, and 12, allowing the individual to make an informed decision about providing the data or participating in the program.

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.