PRIVACY IMPACT ASSESSMENT (PIA)

For the

Automated Records Management System (ARMS LC)
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	BI0006IV - 3194 - 1801
☐	**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 F036 AF PC C

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. 8013, Secretary of the Air Force; as implemented by Air Force Instruction 36-2608, and E.O. 9397 (SSN).

Air Force Instruction (AFI) 36-2608 Military Personnel Records

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.

Official Air Force repository for all Military Personnel Records. Manages the storage, retrieval and life-cycle of all Active Duty, Guard and Reserve personnel records.

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

Loss, theft, or misuse of personally identifiable information by unauthorized persons. Security perimeter protections (firewall, intrusion detection, router access control list, etc.) provided by the hosting enclave. Additionally, strict access control policies and procedures are implemented to ensure is restricted only to those individuals with a need-to-know through role based access schema. SSN is never displayed or exported to reports.

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 Force use

☒ **Other DoD Components.**

Specify. Army, Navy and Marines, All Staff Judge Advocates & Area Defense Counsels, Defense Finance and Accounting Service (DFAS)

☒ **Other Federal Agencies.**

Specify. Department of Veterans Affairs, Defense Investigative Services (DIS), Social Security Administration, U. S. Marshall Service, U. S. Postal Service, Federal Courts, Office of Personnel Management, National Personnel Records Center (NPRC) Prospective Employers, Federal Bureau of Investigation

☒ **State and Local Agencies.**

Specify. Local Law Enforcement Agencies,

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

Specify.

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

Specify. Surviving Family of Deceased Members, Colonel's Group, Funeral Homes, Employment Verification Companies, Public Universities Air Staff, Congressional Offices, Civilian Law Firms, Financial/Lending Institutions, Third Party Requesters (i.e. FOIAs), Immigration and Naturalization Service

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.

(2) If "No," state the reason why individuals cannot object.

Air Force Instruction (AFI) 36-2608 Military Personnel Records

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.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

Upon Air Force enlistment or appointment, member gives consent. If the member believes particular data is incorrect, they can file with the Air Force Board for Correction of Military Record to get the record corrected.

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.

Privacy Act Statement

Authority: 10 U.S.C. 8013, Secretary of the Air Force; as implemented by Air Force Instruction 36-2608, and E.O. 9397 (SSN) and DODI 3001.02

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 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, 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:

Records may be disclosed to the Department of Veterans Affairs for research, processing and adjudication of claims, and providing medical care.

To dependents and survivors for determination of eligibility for identification card privileges.

To the Civilian Health and Medical Program of the Uniformed Services (CHAMPUS) for determination of eligibility and benefits.

To local Immigration/Naturalization Office for accountability and audit purposes.

To State Unemployment Compensation offices for verification of military service related information for unemployment compensation claims; Respective local state government offices for verification of Vietnam 'State Bonus' eligibility.

To the Office of Personnel Management for verification of military service for benefits, leave, or Reduction in Force purposes, and to establish Civil Service employee tenure and leave accrual rate.

To the Social Security Administration to substantiate applicant's credit for social security compensation; Local state office for verification of military service relative to the Soldiers and Sailors Civil Relief Act. Information as to name, rank, Social Security Number, salary, present and past duty assignment, future assignments that have been finalized, and office phone number may be provided to military financial institutions who provide services to DOD personnel. For personnel separated, discharged or retired from the Air Force, information as to last known address may be provided to the military financial institutions upon certification by a financial institution officer that the facility has a dishonored check or defaulted loan.

To the Selective Service Agencies for computation of service obligation.

To the American National Red Cross for emergency assistance to military members, dependents, relatives or other persons if conditions are compelling.

To the Department of Labor for claims of civilian employees formerly in military service, verification of

service-related information for unemployment compensation claims, investigations of possible violations of labor laws and for pre-employment investigations.

To the Armed Forces Retirement Home to determine eligibility.

To Federal agencies, their contractors and grantees, and to private organizations, such as the National Academy of Sciences, for the purposes of conducting personnel and/or health-related research in the interest of the Federal government and the public. When not considered mandatory, the names and other identifying data will be eliminated from records used for such research studies.

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

Disclosure: Voluntary. Failure to provide the requested information may result in a delay or termination of your request.

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.

SECTION 3: PIA QUESTIONNAIRE and RISK REVIEW

a. For the questions in subparagraphs 3.a.(1) through 3.a.(5), indicate what PII (a data element alone or in combination that can uniquely identify an individual) will be collected and describe the source, collection method, purpose, and intended use of the PII.

(1) What PII will be collected? Indicate all individual PII or PII groupings that apply below.

☒ Name	☐ Other Names Used	☒ Social Security Number (SSN)
☐ Truncated SSN	☐ Driver's License	☐ Other ID Number
☐ Citizenship	☐ Legal Status	☒ Gender
☒ Race/Ethnicity	☐ Birth Date	☒ Place of Birth
☐ Personal Cell Telephone Number	☐ Home Telephone Number	☐ Personal Email Address
☒ Mailing/Home Address	☐ Religious Preference	☒ Security Clearance
☐ Mother's Maiden Name	☐ Mother's Middle Name	☒ Spouse Information
☒ Marital Status	☐ Biometrics	☒ Child Information
☐ Financial Information	☒ Medical Information	☒ Disability Information
☐ Law Enforcement Information	☐ Employment Information	☒ Military Records
☒ Emergency Contact	☐ Education Information	☒ Other

If "Other," specify or explain any PII grouping selected.	The ARMS LC database contains individual's SSN, subsystem code, reserve section id, member name, PAS code, grade, Office Phone Numbers, Inductions Information, Professional Certificates and state code along with other data elements that don't fall under the PIA. The actual Military Record may contain other PIA information on the physical document, but not in extractable "data" form.

(2) What is the source for the PII collected (e.g., individual, existing DoD information systems, other Federal information systems or databases, commercial systems)?

Military Personnel Data System (MILPDS)

(3) How will the information be collected? Indicate all that apply.

☒	**Paper Form**	☐	**Face-to-Face Contact**
☐	**Telephone Interview**	☐	**Fax**
☐	**Email**	☐	**Web Site**
☒	**Information Sharing - System to System**		
☐	**Other**		

If "Other," describe here.

(4) Why are you collecting the PII selected (e.g., verification, identification, authentication, data matching)?

During service (active, guard or reserve) these records are used by the Air Force to manage the member's assignment, training, advancement, and separation. After 62 years from separation, these records are transferred to the National Archives for storage under the authorization of 44 U.S.C 2107

(5) What is the intended use of the PII collected (e.g., mission-related use, administrative use)?

Official Air Force repository for all Military Personnel Records. Manages the storage, retrieval and life-cycle of all Active Duty, Guard and Reserve personnel records.

b. Does this DoD information system or electronic collection create or derive new PII about individuals through data aggregation? (See Appendix for data aggregation definition.)

☐ **Yes** ☒ **No**

If "Yes," explain what risks are introduced by this data aggregation and how this risk is mitigated.

c. Who has or will have access to PII in this DoD information system or electronic collection? Indicate all that apply.

☒ **Users** ☒ **Developers** ☒ **System Administrators** ☒ **Contractors**

☐ **Other**

If "Other," specify here.

d. How will the PII be secured?

(1) Physical controls. Indicate all that apply.

☒ **Security Guards**

☒ **Identification Badges**

☐ **Key Cards**

☐ **Safes**

☒ **Cipher Locks**

☐ **Combination Locks**

☐ **Closed Circuit TV (CCTV)**

☐ **Other**

If "Other," specify here.

(2) Technical Controls. Indicate all that apply.

☒ **User Identification**

☒ **Password**

☒ **Intrusion Detection System (IDS)**

☒ **Encryption**

☐ **External Certificate Authority (CA) Certificate**

☐ **Other**

☐ **Biometrics**

☒ **Firewall**

☐ **Virtual Private Network (VPN)**

☒ **DoD Public Key Infrastructure Certificates**

☒ **Common Access Card (CAC)**

If "Other," specify here.

(3) Administrative Controls. Indicate all that apply.

☒ **Periodic Security Audits**

☒ **Regular Monitoring of Users' Security Practices**

☒ **Methods to Ensure Only Authorized Personnel Access to PII**

☒ **Encryption of Backups Containing Sensitive Data**

☒ **Backups Secured Off-site**

☐ **Other**

If "Other," specify here.

e. Does this DoD information system require certification and accreditation under the DoD Information Assurance Certification and Accreditation Process (DIACAP)?

☒ **Yes. Indicate the certification and accreditation status:**

☒	**Authorization to Operate (ATO)**	**Date Granted:**	April 28 2008
☐	**Interim Authorization to Operate (IATO)**	**Date Granted:**	
☐	**Denial of Authorization to Operate (DATO)**	**Date Granted:**	
☐	**Interim Authorization to Test (IATT)**	**Date Granted:**	

☐ **No, this DoD information system does not require certification and accreditation.**

f. How do information handling practices at each stage of the "information life cycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individuals' privacy?

Paper based records are scanned into ARMS LC at the Air Force Personnel Center (AFPC) at Randolph Air Force Base, the Air Reserve Personnel Center (ARPC) in Denver Colorado, and the Business Technology Career Opportunities, Inc. (BTCO) contractor site in Wichita Kansas. Data based records flow electronically from ARPC and Electronic records flow from other internal systems at AFPC.

During service (active, guard or reserve) these records are used by the Air Force to manage the member's assignment, training, advancement, and separation. After 62 years from separation, these records are transferred to the National Archives for storage under the authorization of 44 U.S.C 2107

g. For existing DoD information systems or electronic collections, what measures have been put in place to address identified privacy risks?

Information is used for official use only. Role based access restricts use by unauthorized users of the system. Measures include CAC enabled, firewalls, SSL (https), intrusion detection, and port security.

h. For new DoD information systems or electronic collections, what measures are planned for implementation to address identified privacy risks?

Unless the system is hacked, vulnerability of privacy information is minimal. If the system is compromised the following could be at risk: General customer demographics; Social Security Numbers and any information in the Official Military Personnel File (OMPF). The risks of compromise to this information is minor since the records will the stored in a restricted area of AFPC and only administrators and individuals with need-to-know will have access.