



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Air Force Defense Integrated Military Human Resources System (AF DIMHRS)
--

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
- 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

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.

In accordance with Office of Management and Budget (OMB) Memorandum M-03-22, Defense Integrated Military Human Resources System (Personnel and Pay) (DIMHRS), as defined as a major information system merging a significant amount of data, is required to conduct a Privacy Impact Assessment (PIA) for electronic information systems and collections.

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.

AF DIMHRS will provide the Air Force with an integrated, multi-component personnel and pay system. The system will streamline Air Force Human Resources (HR), enhancing the efficiency and accuracy of personnel and pay procedures. AF DIMHRS will provide each service member with a single, comprehensive record of service that will feature a self-service capability that allows the service member to update selected personal information. HR Specialists, Commanders, and others will have access to Airmen personnel and pay information as required to support their decisions and responsibilities across the Air Force. The web-based HR tool will be available 24 hours/day.

The types of PII that will be collected are name, other names, Social Security Number, truncated SSN, driver's license, other ID number, citizenship, legal status, gender, race/ethnicity, birth date, place of birth, personal cell phone number, home telephone number, personal e-mail address, mailing/home address, religious preference, security clearance, mother's maiden name, mother's middle name, spouse's information, marital status, biometrics, child information, financial information, medical information, disability information, law enforcement action, employment information, military record, emergency contact, education information, person of interest type (supervisor, approving authority, performance evaluator, etc.) department (UIC they support), business unit (active, reserve, guard), geographic location, salary plan, grade, professional certificates, business e-mail address, office phone number(s), mailing/office address, induction information, vehicle identifiers and father's middle name.

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

The risk associated with DIMHRS in regards to PII collected is similar to that of any system in which a service member's information is stored and utilized to ascertain pay and benefits. Protection requirements that serve as the foundation for DIMHRS privacy practices are derived from DoDD 8500.2, IA Implementation, and are explicitly defined in the DIMHRS Security Requirements Traceability Matrix (S-RTM). These will be adapted to AF DIMHRS. Awareness and training for all developers and others affected by the privacy plan include local awareness and training, and user consent forms to acknowledge user responsibilities for protecting data. In order to monitor user compliance with these required rules of behavior, there are periodic audits of Developer IT assets. Once implemented, AF DIMHRS will also have an auditing process to track the actions of any user with access other than self-service. These controls will be incorporated into the AF DIMHRS Information Technology Security Certification and Accreditation Process (DITSCAP) framework with supporting processes to ensure compliance.

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.

HR Specialists, Major Commands, Recruiting Command, National Guard Bureau, U.S. Air Reserves, Department of the Air Force staff, and others will have access to Airman personnel and pay information as required to support their decisions and responsibilities across the Air Force.

Other DoD Components.

Specify.

Defense Manpower Data Center (DMDC), Defense Financial and Accounting Service (DFAS), United States Air Force.

Other Federal Agencies.

Specify.

Veterans Administration, Red Cross

State and Local Agencies.

Specify.

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

Specify.

Both Booz Allen Hamilton, Tecolote, Jacobs, and Mitre and developer and integration contractor will have access for the purpose of establishing a functional system. Contracts will specify the sensitive nature of the data and require a nondisclosure statement from each individual with access to the system and data.

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.

When individuals initially provide personal information needed to enlist in the Military to the United States Military Entrance Processing Command (USMEPCOM), personal data is voluntarily given by the applicant and collected via electronic or manual forms. Forms requesting privacy information contain an applicable privacy statement. This information is subsequently uploaded through system interface to DIMHRS.

(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.

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

When requested in writing, information is provided to individuals in accordance with guidance prescribed in Air Force Instruction 33-332 (The Air Force Privacy Act Program). DoD 5400.11-R May 2007 also establishes that Information or records about an individual shall only be maintained in a system of records that is relevant and necessary to accomplish a DoD Component purpose, in this case, DIMHRS, is required by a Federal statute or an Executive Order. Notices of all Air Force systems of records are required by the Privacy Act to be published in the "Federal Register," but as this information is being disclosed to officers and employees of the DoD who have a need for the record in the performance of their duties, disclosure may occur without explicit 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.

AUTHORITY: 10 U.S.C. 113 note, Secretary of Defense; 10 U.S.C. 3013, Secretary of the Army; 10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C. 8013, Secretary of the Air Force; 14 U.S.C. 5 and 92, Coast Guard; 37 U.S.C., Pay and Allowances of the Uniformed Services; and E.O. 9397 (SSN).

PRINCIPAL PURPOSE(s): The Department of the Air Force is proposing to establish a new system of records that will re-engineer and transform the way the Air Force conducts Human Resources Management by providing fully integrated military personnel and pay capabilities to all Components of the Air Force (Active Duty, Air National Guard, and Air Force Reserves). Producing a single logical record of service for each officer/enlisted, the Air Force-Integrated Personnel and Pay System (AF-IPPS) will provide Combatant Commanders real-time accurate force strength and readiness, better tracking of personnel into and out of theaters of operations, enhanced mission planning and support. This single, logical record of service will become the Air Force's authoritative source of data used to populate the Department of Defense's Enterprise Information Warehouse (EIW). When fully deployed AF-IPPS will allow A1 to be aligned with the Air Force's strategic vision and most importantly provide a robust solution with the adaptability to effectively manage Air Force personnel in the ever changing operational concepts of mobilization, activation, contingency operations, requirements, and assign actions.

ROUTINE USE(S): None. The "Blanket Routine Uses" set forth at the beginning of the Air Force's Compilation of Systems of Record Notices also applies to this system.

DISCLOSURE: Voluntary, When individuals initially provide personal information needed to enlist in the Military to the United States Military Entrance Processing Command (USMEPCOM), personal data is voluntarily given by the applicant and collected via electronic or manual forms. Forms requesting privacy information contain an applicable privacy statement. This information is subsequently uploaded through system interface to DIMHRS.

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.

