

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 Directory Services (AFDS) - NIPR

2. DOD COMPONENT NAME:

United States Air Force

3. PIA APPROVAL DATE:

06/19/20

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
 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 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.

Air Force Directory Services (AFDS) facilitates data transparency for Air Force and Department of Defense systems and applications by providing a single source from which to obtain identity data. AFDS receives information related to individuals from DoD and AF sources, consolidates the data into a standardized record and distributes records to AF customers for identity management and authentication. AFDS customers are system owners that use data to validate identity of users (i.e. CCE or Portal).

Type of personal information: Citizenship, Employment Information, Home/Cell Phone, Mailing/Home Address, Military Records, Official Duty Address, Work Email Address, Birth Date, Education Information, Official Duty Telephone number, Personal E-mail Address, Position/Title, Rank/Grade, DoD ID Number, Gender/Gender Identification, Name(s), Other ID Number, and Social Security Number. (ref. section 2a of this document)

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)

PII is provided by DoD and AF sources to AFDS; AFDS provides the AF customers the information to allow customers to confirm the identity of users for their respective system.

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.

AFDS receives PII from DoD and AF sources; those sources are required to notify individuals of the collection of respective PII. AFDS systems do not interface with individuals only DoD and AF approved authoritative sources.

AFDS falls under Exception 1 (DoD employees who have a need to know the information in the performance of their official duties) and Exemption 3 (The DoD 'Blanket Routine Uses' published at the beginning of the Air Force's compilation of System of Record Notices) apply to this system.

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.

AFDS receives PII from DoD and AF sources; those sources are required to provide the opportunity to consent to the specific uses of their

respective PII. AFDS systems do not interface with individuals only DoD and AF approved authoritative sources.

AFDS falls under Exception 1 (DoD employees who have a need to know the information in the performance of their official duties) and Exemption 3 (The DoD 'Blanket Routine Uses' published at the beginning of the Air Force's compilation of System of Record Notices) apply to this system.

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

Data is not collected directly from individuals. Systems from which data is collected are responsible for ensuring a Privacy Act Statement is provided upon collection.

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.

129 RQW Mission Readiness
2AF Technical Training Operations
690th Network Support Squadron
844 Communications Group
Advanced Distance Learning Service
AETC/A6 Student Network Account Management
AFSPC AF IT E-Learning
Air Education and Training Command A5T Service Management Tool
Air Expeditionary Force Combatant Commander's Toolkit
Air Force Civil Engineer Center
Air Force Fitness Management System II
Air Force Institute of Technology
Air Force Medical Information Systems Branch
Air Force Personnel Center (AFPC) Secure Web Applications (AFPOA)
Air Force Personnel Operations Agency (AFPOA) Air Force Business Objects (Civilian) Applications
Air Force Public Affairs Agency
Air Force Public Key Infrastructure
Air Mobility Command (AMC) Geo Integration
Air Mobility Command Aircrew Operations and Training Division
Automated Civil Engineer System
Consolidated Air Force Active Directory
Education & Training Management System
Enterprise Environmental Safety & Occupational Health Information Assurance Technology Assistance Center
Legacy Logistics Division Supply Systems Branch
Integrated Logistics System-Supply
Officer Professional Military Education
Operationalizing & Professionalizing the Network
Secretary Air Force/Acquisition (SAF/AQH) Acquisition Career Management System
Air Education and Training Command A5T Service Management Tool
Total Force Officer Training
Unit Identification Code
United States Air Force Academy
United States Air Force Central
United States Air Force NexGen IT
United States Air Force Surgeon General's Office
Enterprise IT Service Management
688 Cyber Wing
Air Force Personnel Operations Activity Cloud Management
Office A1 Virtual Data Center
Forms and Accounting Management Service
Resource Management Information System
Enterprise IT as a Service
Mission Planning Central

<input checked="" type="checkbox"/> Other DoD Components	Specify.	Defense Information System Agency (DISA Cross Domain Enterprise Solution) Defense Information Systems Agency (DISA) Enterprise User Defense Manpower Data Center United States Navy US Army Information Technology Agency Joint Strike Fighter
--	----------	---

<input type="checkbox"/> Other Federal Agencies	Specify.	<input type="text"/>
<input type="checkbox"/> State and Local Agencies	Specify.	<input type="text"/>

<input 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.	<input type="text"/>
--	----------	----------------------

<input type="checkbox"/> Other (e.g., commercial providers, colleges).	Specify.	<input type="text"/>
--	----------	----------------------

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

<input 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	

Military Personnel Execution System
 ADLS Advanced Distributed Learning Service
 DCPDS Defense Civilian Personnel Data System
 DISA IDMI Defense Information System Agency Identity Management Interface
 DMDC (DEERS) Defense Manpower Data Center (Defense Enrollment Eligibility Reporting System)
 GDS Global Directory Services
 MilPDS Military Personnel Data System
 MPES Manpower Programming and Execution System
 Air Force Public Key Infrastructure
 Global Combat Support System
 Unit Identification Code
 United States Navy

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

<input type="checkbox"/> E-mail	<input type="checkbox"/> Official Form (Enter Form Number(s) in the box below)
<input type="checkbox"/> Face-to-Face Contact	<input type="checkbox"/> Paper
<input type="checkbox"/> Fax	<input 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://dpcl.d.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

NOTE: Sections 1 above is 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 if they contain information that would reveal sensitive information or raise security concerns.