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 Identity - SIPR (AFID)

2. DOD COMPONENT NAME:

United States Air Force

3. PIA APPROVAL DATE:

12/12/23

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: Federal contractors, military family members, and foreign nationals are included in general public.)*

- ☐ From members of the general public
- ☒ From Federal employees
- ☐ from both members of the general public and Federal employees
- ☐ 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 Identity (AFID) facilitates data transparency for Air Force, Space Force and Department of Defense systems and applications by providing a single source from which to obtain identity data. AFID 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. AFID 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 AFID; AFID 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.

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

AFID 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.

AFID 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. AFID systems do not interface with individuals only DoD and AF approved authoritative sources.

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

h. With whom will the PII be shared through data/system exchange, both within your DoD Component and outside your Component? *(Check all that apply)*

☒ Within the DoD Component	Specify.	Defense Information Systems Agency (DISA) Enterprise User 152d Air Operations Group (152 AOG) 157th Air Operations Group (157 AOG) (157 AOC) 183d Air and Space Operations Center (183 AOC) 193d Air Operations Group (193 AOG) (112 AOC) 217th Air Operations Group (217 AOG) 321st Air Mobility Operations Squadron (321 AMOS) Air and Space Operations Center (AOC) (15 AMOS) 56 ACOMS/613 AOC - PACOM 601st Air Operations Center (601 AOC) 603 ACOMS (603 AOC) 612th Air Operations Center (612 AOC) 621st Air Mobility Operations Squadron (21 AMOS) 690th Network Support Squadron (USAFE SIPR Account Management) 691st Cyberspace Operations Squadron (691 COS)/83d Network Operations Squadron (83 NOS) (USAFE SIPR Account Management Provisioning) 700th Air Support Squadron (700 ASUS) 700th Air Support Squadron Air Operational Support Facility 701st Combat Operations Squadron (701 COS) 710th Combat Operations Squadron (710 COS) Air Force Special Operations Command Operations Center (AFSOC OC) Combined Air Operations Center-Experimental (CAOC-X) ADV Combined Air Operations Center-Experimental (CAOC-X) CORE Combined Air Operations Center-Experimental (CAOC-X) BSLN11 Secretary of the Air Force (SAF/AAH) United States Air Force Central (USAFCENT) NOSC Air Operations Center Weapon System Production Center Hybrid Suite Global Combat Support System Global Combat Support System White Pages Global Directory Service
☒ Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	Defense Information Systems Agency (DISA)
☐ Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	Specify.	
☐ State and Local Agencies	Specify.	
☐ 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.	
☐ 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)*

☐ Individuals
☒ Existing DoD Information Systems
☐ Other Federal Information Systems
☐ Databases
☐ Commercial Systems

DISA IDMI Defense Information System Agency Identity Management Interface
DMDC (DEERS) Defense Manpower Data Center (Defense Enrollment Eligibility Reporting System)
GDS Global Directory Services

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

☐ E-mail
☐ In-Person Contact
☐ Fax
☒ Information Sharing - System to System
☐ Other *(If Other, enter the information in the box below)*
☐ Official Form (*Enter Form Number(s) in the box below)*
☐ Paper
☐ Telephone Interview
☐ Website/E-Form

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://dpcld.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.

A SORN is not required because AFID is not the System of Record; the authoritative source providing data is the system of record and AFID is a re-distributor. AFID does not originate the record, AFID distributes to Air Force agencies for authentication of users.

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. DAA-GRS-2013-0006-0003

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

GRS 3.2 (Information Systems Security Records) Item 30 - System Access Records -- Destroy when business use ceases.

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 statue 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 9013 (USC 9013): Secretary of the Air Force
- Department of Defense Instruction 8330.01 (DoDI 8330.01)
- Executive Order 9397 (SSN), as amended
- Executive Order 13478
- Privacy Act of 1974 section 3(e)(3)
- Critical Infrastructure Assurance, Presidential Decision Directive 63 (PDD-63) "Critical Infrastructure Protection'" 22 May 1998
- Paperwork Reduction Act of 1995 (44 U.S.C. 3501-3520)
- Air Force Policy Directive Instruction 33-3, Information Management, 23 April 2010

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.

AFID systems do not interface with individuals only DoD and AF approved authoritative sources.

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.