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:

Department of the Air Force Identity Credential and Access Management (DAF ICAM)

2. DOD COMPONENT NAME:

United States Air Force

3. PIA APPROVAL DATE:

06/11/24

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.

Identity, Credential, and Access Management (ICAM) enhances the Department of the Air Force's (DAF) cybersecurity program and enables the right individual to access the right resource at the right time for the right reason. ICAM is technical pre-requisite for the implementation of the Zero Trust framework. ICAM is crucial for achieving DAF's goals such as secure information sharing, Multi-Domain Operations, cloud migration, and financial management audit findings remediation. Successful implementation will enforce visibility, compliance, and accountability within the Department of Defense Information Network (DoDIN).
AFLCMC/HNID will be managing daily operations and primary beneficiaries are all system owners that have an application or system platformed within the AFIN. End users, and security operators will also see benefits related to user experience and ability to monitor and secure.
ICAM is platformed in Air Force Cloud One and is dependent, in part, on the infrastructure provided by Cloud One.
DAF ICAM will receive the following attributes from authoritative sources: Citizenship, Employment Information, Military Records, Official Duty Address, Work E-mail Address, Education Information, Official Duty Telephone Phone, Position/Title, Rank/Grade, Security Information, DoD ID Number, Name(s), Training Data, Job Position, Job Specialty, Organization and MAJCOM Affiliation.

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)*

A confirmed identification and authentication of individuals is mandatory for secure access to DAF resources.

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.

PII is not collected from individuals but rather from authoritative sources. Those sources provide the option of objection.

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.

PII is not collected from individuals but rather from authoritative sources. Those sources provide the option of consent.

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

Users are not requested to provide PII data. The data is received from authoritative sources. The standard DoD consent to use IS banner is displayed when accessing the system:
-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details. "

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.	Air Force Identity A1 Digital Transformation Agency (A1 OKTA)
☐ Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	
☐ 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 ☐ Databases
☒ Existing DoD Information Systems ☐ Commercial Systems
☐ Other Federal Information Systems

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

☐ E-mail ☐ Official Form (*Enter Form Number(s) in the box below)*
☐ In-Person Contact ☐ Paper
☐ Fax ☐ Telephone Interview
☒ Information Sharing - System to System ☐ Website/E-Form
☐ 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 DoD-0015

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.

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.
T 33 - 25 R 08.00 - Audit Documents -- If the DoD information system contains sources and methods intelligence (SAMI), then audit records are retained for 5 years. Otherwise, audit records are retained for at least 1 year.

Note 1: Among the dispositions cited in this field, the one with the longest retention time will be used on the system's records data.
Note 2: If any disposition cited in this field has a pending or unscheduled disposition, treat records as permanent retention until an approved NARA disposition is published.
Note 3: If any disposition cited in this field have a permanent retention, retain the records, and prepare for transfer to NARA as scheduled.

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.

The Privacy Act of 1974 - Title 5, United States Code, Section 552a, section 3(e)(3)
Additionally, the "need to know" exception authorizes the intra-agency disclosure of a record for necessary, official purposes. See OMB 1975 Guidelines, 40 Fed. Reg. 28,948. 28,950-01, 28,954 (July 9, 1975). The Privacy Act's legislative history indicates an intent "to give the term 'agency' its broadest statutory meaning," and to permit "need to know" disclosures between components of large agencies. SailPoint has a need to know and access individual records to create an identity store where that user's information will be provided back to them.
DoD Directive 5400.11 - 8 May 2007, Incorporating Change 1, September 1, 2011
This directive aligns with the Privacy Act of 1974 and notes that the creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of personally identifiable information (PII) maintained in a system of records to that which is legally authorized, relevant, and reasonably deemed necessary to accomplish a DoD function. SailPoint IIQ is able to collect, use and maintain PII from a system of record to accomplish the DAF's IGA and ICAM functions.
DoD Regulation 5400.11-R - 14 May 2007
10 U.S.C. 2222, Defense Business Systems: Business Process Reengineering; Enterprise Architecture
DoD Instruction 8320.02, Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense
DoD Instruction 8320.07, Implementing the Sharing of Data, Information, and Information Technology (IT) Services in the Department of Defense
DoD Instruction 8520.03, Identity Authentication for Information Systems.

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.

This is a DAF system, in a DAF environment, utilized by authorized DAF entities... no public collection occurs.

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.