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:

Enterprise Information Technology as a Service (EITaaS) Wave 1

2. DOD COMPONENT NAME:

United States Air Force

3. PIA APPROVAL DATE:

11/02/23

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
- [x] 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
- [x] 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.

EITaaS Wave1 leverages the ServiceNow SaaS solution to provide an Enterprise IT Service Management capability(E-ITSM). Information technology service management (ITSM) is the activities that are performed by an organization to design, build, deliver, operate and control information technology (IT) services offered to customers. This system is located in an Azure IL5 cloud and is accessible through a DISA BCAP. Designed to be a highly flexible and easy-to-use development environment, the ServiceNow Platform enables nearly anyone – no-code to professional coders – to digitize and automate departmental and cross-enterprise workflows, create mobile-first applications, streamline work with AI-powered experiences, and measure and optimize business processes, while mitigating risk. Enterprise organizations of every size and industry use the ServiceNow Platform's wide variety of best in class out-of-the-box workflow applications for IT, security operations, customer service, and human resources.

Types of personal information that will be utilized is as follows: Names: Official Duty address; Work eMail Address; Official Duty Phone; Position Title; Rank Grade; DOD ID number; Assigned MAJCOM, assigned Unit, Assigned Unit Location, Assigned Unit Street, Assigned Unit Zip Code, Attached MAJCOM, attached Unit, Attached Unit Location, Attached Unit Name, building, Category, common name (cn), Distinguished Name (dn), Duty Phone Commercial, Enterprise User Name, Federated Assured Personal Identifier (fapi), mail, Mobile Phone, Parent Unit Name, Projected Unit, Projected Unit Date, rank, Room, Service, Last Name (sn), login name, work contact information, administrative organization, duty organization, department. The data will remain on Government Furnished Equipment (GFE) and will be encrypted if stored.

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)*

Verification and validation of user's identity against existing AF Directory, data matching, and mission-related use.

e. Do individuals have the opportunity to object to the collection of their PII? [ ] Yes [x] 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 data utilized is derived from an existing system and used to identify individuals requesting service support.

f. Do individuals have the opportunity to consent to the specific uses of their PII? [ ] Yes [x] 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 data utilized is derived from an existing system and used to identify individuals requesting service support.

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

PII is not collected from End Users. Its pulled from the AF Identity Management System.

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.	USAF
☐ 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

Existing DOD Information systems: Data will be derived from - Air Force Identity(AFID) Management; BMC Remedy.

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)*

System to System:
Data will be derived from - Air Force Identity(AFID) Management;

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 ICAM - 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-2013-0005-0004

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

(3) Retention Instructions.

GRS 3.1, Rule 20 - Information technology operations and maintenance records -- Destroy 3 years After agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated or superseded, but longer retention is authorized if required for business use.
Note 1: Among the disposition(s) cited in this field, the one with the longest retention time will be used on the system's records data.
Note 2: If one or more of the disposition(s) cited in this field have the disposition authority of "Unscheduled" and/or "Column D Disposition" with "Disposition pending", treat these records data as if they have a permanent retention and do not dispose them until the unscheduled status is updated by a National Archives and Records Administration (NARA-approved records disposition schedule, either pre-approved by a NARA General Records Schedule (GRS) or by a NARA-approved customized disposition schedule via the AF Form 525 process in AFI 33-322.
Note 3.: If one or more of the disposition(s) cited in this field have a permanent retention or "Column D Disposition" with "Retire as permanent", do *not* delete the records data, retain the data (it may be 25-30 years before the time of accessioning), and then before the time of accessioning, prepare the records

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.

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.

No information from the general public is collected.

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