

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:

CLOUD1-AF (C1) (formerly Air Force Common Computing Environment 2.0) - NIPR

2. DOD COMPONENT NAME:

United States Air Force

3. PIA APPROVAL DATE:

03/29/21

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.

Disclaimer: This PIA does not cover systems developed or added to Cloud One environment, those systems will require a separate PIA if they collect PII.

Description:

The Cloud One Air Force (AF) IaaS and PaaS Initiatives provides a consolidated cloud infrastructure environment for authorized users with CAC for the purpose of software lifecycle development and sustainment needs. The Cloud One Initiative is an infrastructure common service covered by the Cloud One (C1) ATO.

AFPEO C3I&N has established a Common Computing Environment - Air Force Cloud One in multiple cloud environments that will facilitate the implementation of the DoD and AF Cloud Strategy, operate and leverage several key capabilities to include; identity and access management (IdAM), auditing, automated provisioning of networks/infrastructure/platforms (to include STIG compliance), messaging and mediation, boundary protection, etc.

Categories of personal information collected in the Initiative include, however may not be limited to; last name, first name, middle initial, Cadency of name (e.g., Sr, Jr, III), Electronic Data Interchange Person Identifier (EDIPI), login name, persona username, rank, job title, primary and other work e-mail addresses, assigned unit name code and location, attached unit name code and location, major command, assigned major command, personnel category code, distinguished name, Country of Citizenship, Persona E-mail address, DoD component, Directory publishing restrictions, and Pay grade. (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)

Mission-related use and administrative use as determined by each Air Force entity collecting the data.

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.

The Cloud One environment is approved for the transfer and storage of UNCLASSIFIED files in any format to include FOUO, controlled unclassified information (CUI) which may contain PII that may have been collected via another method (i.e. another source). The AF entity collecting PII is responsible for ensuring owners of the PII have the opportunity to object to the collection of their PII and that all requirements regarding notification and consent have been complied with prior to the PII being introduced in to any Cloud One environment.

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.

The Cloud One environment is approved for the transfer and storage of UNCLASSIFIED files in any format to include FOUO, controlled unclassified information (CUI) which may contain PII that may have been collected via another method (i.e. another source). The AF entity collecting PII is responsible for ensuring owners of the PII have the opportunity to object to the collection of their PII and that all requirements regarding notification and consent have been complied with prior to the PII being introduced in to any Cloud One environment.

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

This is the responsibility of the collecting AF entity.

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.
- 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

This is the responsibility of the collecting AF entity.

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)

This is the responsibility of the collecting AF entity.

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://dpcltd.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.

This is the responsibility of the collecting AF entity. A SORN is not required because Cloud One is not the System of Record; the authoritative source providing data is the system of record and Cloud One is storage hosting environment. Cloud One does not originate the record, Cloud One distributes to DoD and Air Force agencies for authentication of users.

I. 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.

(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 -- 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 statute 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 33-3, Information Management, 21 Jun 2016

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.

Cloud One systems do not interface with individuals only DoD and AF approved authoritative sources

SECTION 2: PII RISK REVIEW

a. What PII will be collected (a data element alone or in combination that can uniquely identify an individual)? (Check all that apply)

- | | | |
|--|---|--|
| <input type="checkbox"/> Biometrics | <input checked="" type="checkbox"/> Birth Date | <input type="checkbox"/> Child Information |
| <input checked="" type="checkbox"/> Citizenship | <input type="checkbox"/> Disability Information | <input checked="" type="checkbox"/> DoD ID Number |
| <input type="checkbox"/> Driver's License | <input checked="" type="checkbox"/> Education Information | <input type="checkbox"/> Emergency Contact |
| <input checked="" type="checkbox"/> Employment Information | <input type="checkbox"/> Financial Information | <input checked="" type="checkbox"/> Gender/Gender Identification |
| <input checked="" type="checkbox"/> Home/Cell Phone | <input type="checkbox"/> Law Enforcement Information | <input type="checkbox"/> Legal Status |
| <input checked="" type="checkbox"/> Mailing/Home Address | <input type="checkbox"/> Marital Status | <input type="checkbox"/> Medical Information |
| <input checked="" type="checkbox"/> Military Records | <input type="checkbox"/> Mother's Middle/Maiden Name | <input checked="" type="checkbox"/> Name(s) |
| <input checked="" type="checkbox"/> Official Duty Address | <input checked="" type="checkbox"/> Official Duty Telephone Phone | <input checked="" type="checkbox"/> Other ID Number |
| <input type="checkbox"/> Passport Information | <input checked="" type="checkbox"/> Personal E-mail Address | <input type="checkbox"/> Photo |
| <input type="checkbox"/> Place of Birth | <input checked="" type="checkbox"/> Position/Title | <input type="checkbox"/> Protected Health Information (PHI) ¹ |
| <input type="checkbox"/> Race/Ethnicity | <input checked="" type="checkbox"/> Rank/Grade | <input type="checkbox"/> Religious Preference |
| <input type="checkbox"/> Records | <input type="checkbox"/> Security Information | <input checked="" type="checkbox"/> Social Security Number (SSN) (Full or in any form) |
| <input checked="" type="checkbox"/> Work E-mail Address | <input type="checkbox"/> If Other, enter the information in the box below | |

If the SSN is collected, complete the following questions.

(DoD Instruction 1000.30 states that all DoD personnel shall reduce or eliminate the use of SSNs wherever possible. SSNs shall not be used in spreadsheets, hard copy lists, electronic reports, or collected in surveys unless they meet one or more of the acceptable use criteria.)

(1) Is there a current DPCLTD approved SSN Justification on Memo in place?

- Yes No

If "Yes," provide the signatory and date approval. If "No," explain why there is no SSN Justification Memo.

Since PII collection is not under the control of the Cloud One Program Office, it is not possible to definitively identify what is collected. Note, SSNs are permitted as long as Cloud One is not the initial method of collection and the SOR where the SSN originated from must have a valid SSN justification memo. AF entity that utilize and store SSNs in Cloud One as a functional framework (IT investment) must comply with AFI 33-332 and DODI 1000.30.

(2) Describe the approved acceptable use in accordance with DoD Instruction 1000.30 "Reduction of Social Security Number (SSN) Use within DoD".

This is the responsibility of the collecting AF entity.

(3) Describe the mitigation efforts to reduce the use including visibility and printing of SSN in accordance with DoD Instruction 1000.30, "Reduction of Social Security Number (SSN) Use within DoD".

This is the responsibility of the collecting AF entity.

(4) Has a plan to eliminate the use of the SSN or mitigate its use and or visibility been identified in the approved SSN Justification request?

If "Yes," provide the unique identifier and when can it be eliminated?
If "No," explain.

- Yes No

This is the responsibility of the collecting AF entity.

b. What is the PII confidentiality impact level²?

- Low Moderate High

¹The definition of PHI involves evaluating conditions listed in the HIPAA. Consult with General Counsel to make this determination.

²Guidance on determining the PII confidentiality impact level, see Section 2.5 "Categorization of PII Using NIST SP 800-122." Use the identified PII confidentiality impact level to apply the appropriate Privacy Overlay low, moderate, or high. This activity may be conducted as part of the categorization exercise that occurs under the Risk Management Framework (RMF). Note that categorization under the RMF is typically conducted using the information types described in NIST Special Publication (SP) 800-60, which are not as granular as the PII data elements listed in the PIA table. Determining the PII confidentiality impact level is

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.