# 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:**

Cyberspace Infrastructure Planning System (CIPS)

**2. DOD COMPONENT NAME:**

United States Air Force

**3. PIA APPROVAL DATE:**

01/23/2026

## 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.**

The Cyberspace Infrastructure Planning System (CIPS) supports three of the four top resource priorities for DoD: 1) readiness and sustainability, 2) modernization, and 3) infrastructure for cyber operations systems. In so doing, this system is a key component of Cyber Warfare. It provides a capability that is critical to the success of network centric warfare, a component of Cyber Warfare. To that end, CIPS delivers a real time, enterprise capability necessary for deliberate cyberspace infrastructure planning and management across the DAF. At its heart, CIPS is an infrastructure lifecycle management database system. It is enterprise, web-based, cloud-based (both IL5/NIPRNET and IL6/SIPRNET), and used by over 8K users, at over 340 AF installations, to assess, plan, prioritize, install, document & maintain cyber infrastructure, managing over $4B in documented cyber requirements.
Information collected about individuals is a by-product of storing the DD2875 within CIPS such as: Name, official email, Phone #, grade/ rank, user ID #, organization, citizenship, designation of person, mailing address, supervisor name, email address and organization.

**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 - when calling the help desk.

**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.

Disclosure of System Authorization Access Request information is voluntary; however, failure to provide information will prevent further processing of the account request.

**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.

Individuals who need access to CIPS can either fill out the required fields on the website or stop and not get an account.

**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

Authority: Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act. Principal Purpose: To record name, signature, and other identifiers for the purpose of validating the trustworthiness of individuals requesting access to Department of Defense (DoD) systems and information. Note: Records may be maintained both electronic and/or paper form. Routine uses: None. Disclosure of this information is voluntary, however, failure to provide the requested information may impede, delay or prevent further processing of the request.

**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 CIPS PMO Team |
| ☐ | 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. | The contractor Inalab Consulting is responsible for safeguarding the PII. Contractor will comply with FAR 52.224-1, FAR Privacy Act Notification, 52.224-2 Privacy Act and FAR 39.105. |
| ☐ | 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 | | |

CIPS does not share any PII through data exchange

**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)* | | |

DD FORM 2875

**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. N1-AFU-88-19;N1-AFU-88-26; DAA-GRS-2013-0005-0004

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

(3) Retention Instructions.

T 17 - 03 R 11.00 - Project File Original (Master), Program Engineering Files--Destroy 2 years after program completion or cancellation
T 33 - 02 R 02.00 - C4I Capabilities Planning, C4I Plans, and Blueprints -- Destroy 1 year after superseded.
GRS 3.1 Item 20 – Information Technology Operations and Maintenance -- 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 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.

Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act.

**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.

CIPS does not collect from members of the public.