



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

Total Human Resource Managers Information System (THRMIS)
---

United States Air Force (USAF)
--------------------------------

### **SECTION 1: IS A PIA REQUIRED?**

**a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).**

- (1) Yes, from members of the general public.
- (2) Yes, from Federal personnel\* and/or Federal contractors.
- (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.
- (4) No

\* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

**b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.**

**c. If "Yes," then a PIA is required. Proceed to Section 2.**

**SECTION 2: PIA SUMMARY INFORMATION**

**a. Why is this PIA being created or updated? Choose one:**

- New DoD Information System
- Existing DoD Information System
- Significantly Modified DoD Information System
- New Electronic Collection
- Existing Electronic Collection

**b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?**

- Yes, DITPR**      Enter DITPR System Identification Number
- Yes, SIPRNET**      Enter SIPRNET Identification Number
- No**

**c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?**

- Yes**
- No**

If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

**d. 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 should be consistent.

- Yes**
- No**

If "Yes," enter Privacy Act SORN Identifier

DoD Component-assigned designator, not the Federal Register number.  
Consult the Component Privacy Office for additional information or  
access DoD Privacy Act SORNs at: <http://www.defenselink.mil/privacy/notices/>

or

**Date of submission for approval to Defense Privacy Office**

Consult the Component Privacy Office for this date.

**e. Does this DoD information system or electronic collection have an 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**

**Enter OMB Control Number**

**Enter Expiration Date**

**No**

**f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.**

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) 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) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect 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) 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 should be identified.

The authority to collect Privacy Act (PA) information is derived from 10 United States Code (U.S.C.) 8013, Secretary of the Air Force: powers and duties.

**g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.**

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

THRMIS is an Air Force web based Total Force reporting and analysis tool deployed for HQ USAF Career Field Managers (CFMs) and Action Officers (AOs) to help in assessing and analyzing the health and sustainability of career fields and supporting decision making. THRMIS integrates disparate data bases (active duty, Air Force reserve, Air National Guard, and civilian personnel and AF manpower) into a single data warehouse. Each month data extracts from the systems of record Military Personnel Data System (MilPDS), Defense Civilian Personnel Data System (DCPDS) and Manpower Programming and Execution System (MPES) are added to the data warehouse. THRMIS is not a transactional system. A business intelligence (BI) software application allows users to generate reports with functionality to perform data mining and drill down. THRMIS is in maintenance mode. Full Operational Capability (FOC) was achieved on 1 Oct 2002.

The Air Force Deputy Chief of Staff for Manpower and Personnel (AF/A1) is the system owner. Day-to-day operation, management, and oversight are conducted by the Headquarters Air Force Management Division, (HAF/A1PF). The HAF/A1PF point of contact is Mr. William A. Scott, 703-604-0843, william.scott@pentagon.af.mil. THRMIS resides on the Headquarters Air Force Network (HAFNET). Servers are located in 844 Communications Squadron (CS) facilities in the Pentagon. Personnel from the 844 CS provide the full range of systems administration, monitoring, and connectivity support to ensure THRMIS operates properly on the Non-classified Internet Protocol Router Network or NIPRNET. This includes saving a daily transactional log and performing a full-system backup once each week. The HAF Special Programs and Support Branch (HAF/A1PFS) provides application administration, user account management, systems analysis, and any required day-to-day maintenance.

Primary users of THRMIS are HQ USAF Career Field Managers (CFMs) and Air Staff Action Officers (AOs). Users must have a username and password to access the system. User accounts are created and managed within HAF/A1PFS. Users can execute pre-built reports that are shared by all users or create their own using the ad hoc functionality of the BI. Reports returned through the web are aggregate counts (summaries and statistics). An individual's name and/or Social Security Number (SSN) are not returned with any output of data. Special requests made for names require review and execution through THRMIS administrators. The use of SSNs by AF analysts when accessing the data warehouse is addressed in item 13.

The sources of information in identifiable form are data extracts from the MilPDS and DCPDS produced at the Air Force Personnel Center (AFPC). Personal data that is stored within THRMIS includes the following on Air Force military service members and civilians:

- Name
- SSN
- Gender
- Race
- Date of Birth

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

The potential privacy risks associated with downloading data including information in identifiable form from the systems of record and storing it in the THRMIS data warehouse are minimal because of access requirements and restrictions. Although identifiable information is in the data warehouse an individual's record cannot be retrieved using name or SSN via the web interface. Thus, a user cannot include this identifiable information (name and SSN) in a report output via the web.

**h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)?** Indicate all that apply.

**Within the DoD Component.**

Specify.

**Other DoD Components.**

Specify.

**Other Federal Agencies.**

Specify.

**State and Local Agencies.**

Specify.

**Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify.

**Other** (e.g., commercial providers, colleges).

Specify.

**i. Do individuals have the opportunity to object to the collection of their PII?**

**Yes**  **No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object.

Not applicable as THRMIS is not a system of record but relies on extracts from MilPDS and DCPDS. However, the Air Force rules for accessing records and for contesting and appealing initial agency determinations are published in Air Force Instruction (AFI) 33-332. As to SSN, the Air Force requests an individual's SSN upon entering the military service or becoming a civilian employee. All information required by law is provided at that time. The SSN is used to establish and access an individual's personnel record in MilPDS and DCPDS.

**j. 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.

Not applicable as THRMIS is not a system of record but relies on extracts from MilPDS and DCPDS. However, the Air Force rules for accessing records and for contesting and appealing initial agency determinations are published in Air Force Instruction (AFI) 33-332. As to SSN, the Air Force requests an individual's SSN upon entering the military service or becoming a civilian employee. All information required by law is provided at that time. The SSN is used to establish and access an individual's personnel record in MilPDS and DCPDS.

**k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.**

**Privacy Act Statement**                       **Privacy Advisory**  
 **Other**     **None**

Describe each applicable format.

Individuals are not asked to provide PII data for THRMIS. The sources of information in identifiable form are data extracts from the MilPDS and DCPDS produced at the Air Force Personnel Center (AFPC). However, Privacy Act Statements are provided to individuals when entering military service or the civilian workforce that any PII may be collected and maintained on them for agency use.

--

**NOTE:**

**Sections 1 and 2 above are 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 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.**



















