



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

COMMAND MAN-DAY ALLOCATION SYSTEM (CMAS)
--

Air Force
-----------

### **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.

Title 10 USC 12301 and National Defense Authorization Act (NDAA) 2005  
AUTHORITY: 10 USC 12301 (d) and 801344 USC 3101; and EO 9397.

**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.**

CMAS database contains contact and supplemental information about Mil-Pers Man-day information for maintaining, accounting, and reporting Air Force Military Personnel Appropriation (MPA) Man-day information to higher headquarters level. CMAS is a management tool and provides Major Air Commands the capability to process MPA Man-day authorizations to place Air National Guard (ANG) and Air Force Reserve (AFR) members on active duty in support of the Air Force mission. CMAS was developed under Computer Systems Requirement Document (CSRD) 93-7182, with HQ USAF/A1MP approval and applies to all AF Commands and Agencies. Our Mission Assurance Category is MACIII.

The CMAS database contains ANG and AFR member names, Social Security Numbers, and local supplemental information of CMAS users located at various Air Reserve Component (ARC) base-level wings; i.e., official office symbol, e-mail address. We provide a notice at the beginning (front page of CMAS) or when the input user opens CMAS to enter mission data. Individuals do not disclose privacy information directly to CMAS. Prior to the information being entered into any military computer system (CMAS notwithstanding) it is disclosed to wing-level personnel by the member who would be performing the tour at the time of enlistment or commissioning. This is a standard military requirement of all members, regardless of affiliation.

CMAS is "owned" by the Air Force Office of End Strength Accounting, AF/A1MP, Directorate of Manpower and Personnel, Pentagon, Washington D.C.; and are physically located and maintained at Scott AFB IL, under contract by Harris Technical Services Corporation, Alexandria VA.

CMAS is a stand-alone system and has no interfaces to other DoD or Non-DoD systems. CMAS is on the Internet under dot MIL.

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

Other than risks posed by adopted security measures for applications and individuals with CAC access, no other potential risks are anticipated from either intentional or unintentional human threat.

The CMAS Database can only be accessed by: (a) Base Level Military Personnel with approved access by MAJCOM MPA Man-Day manager to those functional manager accounts. System Access Applications developed by and managed with oversight of the AF CMAS Lead Agent and Team CMAS via application unique account and password procedures. CMAS is also preparing to go to Common Access Card (CAC) access for even tighter security control of the database under the MAJCOM administrators. Users will be required to use COMMON Access Card (CAC) when applying for permission to use the system.

Agents of TEAM CMAS act as administrators of the CMAS database after having completed annual Privacy Act training requirements and various legal protections such as non-disclosure statements.

The CMAS Database is additionally protected by a "security/entitlements" feature that controls software access to specific fields and records depending on the business application, user level, and role or privileges allowed. This security feature is documented in the design specification under configuration control. Again, the individual does not access the system. A privacy notice is available at the time a user logs onto the system.

**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.

Information in the CMAS database is used internally by applications and System users within the Component only. There is no access outside the Military.

**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.

The collection of identifiable information is essential to the processing of MPA man-day tour requests and the generation of formal orders for ARC members performing active duty augmentation.

If a member would object to his/her Name & SSAN being entered into CMAS, then the member would forfeit the opportunity to perform MPA active duty.

**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.

The collection of identifiable information is essential to the processing of MPA man-day tour requests and the generation of formal orders for ARC members performing active duty augmentation.

If a member would object to his/her Name & SSAN being entered into CMAS, then the member would forfeit the opportunity to perform MPA active duty.

**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.

**AUTHORITY:** 5 U.S.C. Section 301; 10 U.S.C. Sections 1074(c)(1) and 1095(k)(2); 10 U.S.C. Chapter 147; 50 U.S.C. Chapter 23; E.O. 10450, as amended

**PURPOSE:** To request Military Personnel Appropriation (MPA) authorization for temporary active duty to support active USAF contingent and operational missions requirement.

**ROUTINE USES:** To Federal and State agencies and private entities, as necessary, on matters relating to temporary active duty in support of USAF contingent.

**DISCLOSURE:** Voluntary; however, failure to provide information may result in denial of MPA man-day authorization.

--

**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.**

















