



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

AMC COOP Information Management System (ACIMS)  
[Registered Child Dependency of DA176310 DITPR 9865 REDSTONE-NIPR-ICAN  
- REDSTONE\_ARSENAL\_SBU\_IP\_DATA\_ICAN]

U.S. Army Aviation and Missile Life Cycle Management Command (AMCOM)

### 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.

10 U.S.C. 5013, Secretary of the Army; DoD Instruction 3001.02, Personnel Accountability in Conjunction With Natural or Man-made Disasters; Army Regulation 500-3, U.S. Army Continuity of Operations Program Policy and Planning

**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.

ACIMS provides a management tool to help ensure Continuity of Operations (COOP) requirements are readily available to respond, recover, and reconstitute mission critical tasks during a man-made or natural incident. ACIMS will process, store and supply data supporting resource requirements to implement work around solutions for portions of day to day operations which cannot be immediately restored, and ultimately, restoring processes to normal operational status. This product supports Life Cycle Management Command, and can be used by government and contractor employees. This product was internally developed, and provides real-time processing. This product resides within a web-application on an NT Platform. ACIMS does not interface with any other systems.

Types of personal information collected include name, home telephone number and an alternate "emergency" telephone number. The "emergency" contact number is an additional number at which the individual may be reached during a COOP emergency if he or she cannot be contacted using his/her work or home telephone numbers.

NOTE: This application does not require a separate DIACAP accreditation. This application inherits accreditation from the Redstone Arsenal ICAN registered in APMS as AITR #DA176310, "RED-NIPR-ICAN - REDSTONE ARSENAL DOIM NIPRNET ENCLAVE". This application is included in the AMCOM Enterprise Network (AEN) Tenant Security Plan (TSP) that is accepted by the Redstone NEC as an artifact to the ICAN DIACAP. This follows the NETCOM Best Business Practice (BBP) number 07-DC-M-0008. This is a Government Off-The-Shelf (GOTS) software application; it does not meet the definition of Information System in the DIACAP Guidance, AR 25-2. IAW AR 25-2 Chapter 5 only Information Systems require accreditation or Authority to Operate (ATO). This software application requires a Certificate of Networthiness (CON).

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

The risk associated with the PII being collected is that individuals who participate could have their phone numbers released. Our assessment determines that due to the nature of the PII collected there is a reduced risk of harm to individuals. This risk is further mitigated through the use of firewalls, antivirus software, CAC access, encryption and physical security measures in place related to the facility.

**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.

There is no electronic data exchange within or outside our DoD component. There is limited, role-restricted access for each AMC subordinate command's COOP management team. The role restrictions disallow any access to data outside the COOP management teams own command. The ACIMS system administrator role provides access for system management purposes only.

**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.

Individuals have the opportunity to object to the collection of PII by not utilizing the system. If the individual chooses not to voluntarily provide the information, it may prevent the individual from participating in the programs managed by the system. The individual consents to use by inputting the requested data. The posted Voluntary Information Disclosure Policy states the PII data collection is voluntary, why it is requested, how it will be used and to whom it may be released.

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

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 PII collected is used for only one purpose and participation is strictly voluntary. If the individual does not provide information then they do not consent to the using their PII. Since this system has only one specific purpose, the individual is not able to specify the use of their information other than not providing it and being a part of the system.

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.

When the individual is asked to provide PII data, they are presented with the Voluntary Information Disclosure Policy which states that PII data collection is voluntary, why the data is requested, how it will be used, and to whom it may be released.

A Security and Privacy Notice is also provided to the individual which states that no personal information about them will be collected when utilizing the product unless the individual chooses to provide that information.

-----  
Voluntary Information Disclosure Policy and Privacy and Security Notice:

Thank you for visiting our product and reviewing our privacy policy. Our privacy policy is clear: We will collect no personal information about you when you visit our product unless you choose to provide that information to us.

-----  
1. This product is provided with controlled access by the U.S. Army Aviation & Missile Command.

2. Information presented on this application / website is considered unclassified information and is accessed by authorized users unless otherwise specified. Use of appropriate byline / photo / image credits is requested.

3. For product management, information is collected for statistical purposes. This government computer system uses software programs to create summary statistics, which are used for such purposes as assessing what information is of most and least interest, determining technical design specifications, and identifying system performance or problem areas. No user-identifying information is collected for this analysis. The information collected includes the following types of data:

- a. Number of Hits for Home Page and Number of Successful Hits for Entire Product
- b. Number of User Sessions (from United States and International) and Most Active Countries
- c. Most and Least Requested Pages
- d. Top Entry and Exit Pages
- e. Single Access Pages and Number of Page Views
- f. Most Downloaded Files
- g. Most Submitted Forms and Scripts
- h. Most Active Organizations or Companies that Accessed Product

4. For product security purposes and to ensure that this service remains available to all users, this