



PRIVACY IMPACT ASSESSMENT (PIA)

For the

AIR RESERVE ORDER WRITING SYSTEM-RESERVES

United States 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

007-57-01-20-01-1800-00

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.

Authority for Maintenance of the System: 5 U.S.C. 301, Departmental Regulations; 10 U.S.C., Chapter 11; 37 U.S.C.; 10 U.S.C. 8013, Secretary of the Air Force; Department of Defense 5000.2-R, Mandatory Procedures for Major Defense Acquisition Programs (MDAPS) and Major Automated Information System (MAIS) Acquisition Programs; Air Force Policy Directive 65-6, Financial Management; Air Force Reserve Command Instruction 65-601, Budget Programming and Financial Management and E.O. 9397 (SSN).

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.

The AROWS-R is an order writing tool developed by US MARINE CORPS TECH SERVICES ORG, KANSAS CITY, Technology Services Organization, which will replace several of our legacy order writing and related systems. The AROWS-R is an Automated Information System (AIS) Application as defined by Department of Defense Instruction (DoDI) 8500.2, Information Assurance (IA) Implementation. The AROWS-R is a mission support information system that automates tasks and functions of order writing and processing through the Air Force Reserve Command. It is a web based, responsive and flexible information system in support of Air Force Reserve order writing. It will provide automated support for information management as it relates to order writing so that all levels of order writing have timely and accurate real time information for management decision support.

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

AROWS-R is a web based which creates the risk associated with accessing PII data over the internet. Safeguards to address these risks include: Records are stored in office buildings protected by guards, controlled screening, use of visitor registers, electronic access, and/or locks. Access to records is limited to individuals who are properly screened and cleared on a need-to-know basis in the performance of their official duties. Username/passwords are used to control access to the systems data, and procedures are in place to deter and detect browsing and unauthorized access. Physical and electronic access are limited to persons responsible for servicing and authorized to use the record system.

A determination was made for AROWS-R to use SSL 128 bit encryption for data transmission. In accordance with AFMAN 33-223, Methods of Identification and Authentication, 19 Jul 2004, users access the AROWS-R url and are prompted to enter their user name and password for authentication. This can be accessed from a .com or a .mil site. AROWS-R uses the approved Air Force PKI certificates to force all authorized users to connect via a secure web HTTPS connection SSL using port 443. Users are assigned roles by their functional manager which determines the level of data access they receive.

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.

US MARINE CORPS TECH SERVICES ORG, KANSAS CITY, Technology Services Organization S&K Aerospace Contractor personnel. The FM/S&K contract includes the following clauses regarding Privacy in the Clauses section of the contract: FAR 52.224-1 Privacy Act Notification-APR 1984; FAR 52.224-2 Privacy Act-APR 1984; FAR 52.239-1 Privacy or Security Safeguards Aug 1996

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.

Information is received from system interfaces. AROWS-R receives this information as a data feed from MILPDS.

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.

Information is received from system interfaces. AROWS-R receives this information as a data feed.

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.

Information is received from system interfaces. AROWS-R receives this information as a data feed.

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.

