PRIVACY IMPACT ASSESSMENT (PIA)

For the

Air National Guard Reserve Order Writing System (AROWS)
United States Air Force (USAF), Air National Guard (ANG)

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	☐	New Electronic Collection
☒	Existing DoD Information System	☐	Existing Electronic Collection
☐	Significantly Modified DoD Information System		

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	0879
☐	**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 007-57-01-20-01-2729-00

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 F033 AF D

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.

13 August 2009 (Date modification was submi

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.

Authority to collect information is inherited from the legal authority governing the Military Personnel Data System (MilPDS).

Additional legal authority to collect and maintain a system of records is contained in:
10 United States Code (USC) 8013, Secretary of the Air Force
Joint Federal Travel Regulation
Air Force Instruction 33-328, Administrative Orders
Air Force Instruction 33-332, Privacy Act Program
Air Force Instruction 65-103, Temporary Duty Orders
ANG Instruction 33-101, Air National Guard Special Orders
ANG Instruction 65-101, Air National Guard (ANG) Workday Accounting and Reporting Procedures
Executive Order (EO) 9397, (Social Security Number – 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.

AROWS is a web based (CAC enabled) information system designed to support the Air National Guard (ANG) order writing process, in direct support of the Air Force and the National Guard Bureau (NGB) missions. It provides the capability for Order Specialists to create all types of orders ranging from Annual Training to Mobilization orders, including Temporary Duty (TDY), Permanent and Temporary Change of Station (PCS/TCS) for technicians (civilians), and call to military duty and civilian travel, in an automated, fast and accurate manner. AROWS is required in order for the NGB to comply with the Chief Financial Officers (CFO) Act as it relates to the execution of over $3.0 billion of the ANG Military Personnel Appropriation.

AROWS collects and maintains several different types of personal information about the Guardsmen, this information includes, his/her full name; social security number; legal status; gender/sex; and date of birth. This information is provided by the Guardsmen to the Order Specialist via the Air National Guard Order Application Request (NGB 336) form.

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

Unless AROWS is hacked, vulnerability of privacy information is minimal. As a hosted system by the Space and Naval Warfare (SPAWAR) Systems Command (SSC) Information Technology Center (ITC) located at 2251 Lakeshore Drive, New Orleans, LA 70145, (SSC NOLA), AROWS relies on the protection mechanisms of the Core Services Architecture (CSA) environment, as managed by SSC NOLA to meet network, enclave, vulnerability management and anti-virus requirements. The CSA environment provides firewall, intrusion detection, boundary monitoring and secure remote access for AROWS.

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. AROWS shares information with several systems to ensure that Guardsmen in a military status are properly paid and travel authorization requests for dual-status military technicians (civilians) are properly processed. AROWS shares information with the following systems: General Accounting Finance System (GAFS); Military Personnel Data System (MilPDS); Integrated Military Pay System (IMPS); and Reserve Travel System (RTS).

Additionally, AROWS is schedule to share information with the Defense Enterprise Accounting and Management System (DEAMS) during the first quarter FY 2010.

☐ **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.

PII data from individuals are required to process any Orders request. If the individual has issue with the use of their privacy information to create their orders, they can address it to their Commanding Official; however, this may prevent them from being able to use official government travel.

(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.

Individuals consent to the collections of privacy information by completing the Air National Guard Order Application Request (NGB 336) form.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

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.

On the NGB IMT 336, a PRIVACY ACT STATEMENT is identified. The prescribing directive for the NGB IMT 336 is the ANG Instruction 33-101, Air National Guard Special Orders.

1. AUTHORITY: Title 5 USC Section 552a; and Executive Order 9397.
2. PURPOSE: Information provided will be entered into the Air National Guard Reserve Order Writing System (AROWS).
3. ROUTINE USES: None.
4. DISCLOSURE: Voluntary; however, if SSN is not provided, order application request will not be processed.

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.