PRIVACY IMPACT ASSESSMENT (PIA)

For the

AMARC Business System
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**
- ☐ **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: 219
- ☐ **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 007-57-01-03-01-8070-00-405-145

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.

5 U.S.C. 301, Departmental Regulations; 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.

Activity/Purpose:
The ABS supports production and financial business operations. Areas of operation include the reclamation of critical aircraft components, the maintenance, repair and overhaul of aircraft, the storage, re-preservation and disposal of aircraft, engines and equipment, financial planning, execution and reporting to meet internal and external requirements.

The ABS uses Commercial-Off-the-Shelf (COTS) products to provide 309 AMARG managers with the labor and financial information needed to meet mission requirements. Individual names, social security numbers and hourly wages are collected for use within the ABS.

Present Life-Cycle Phase:
Operations and Support

System Owner:
The ABS is maintained by 309 SPTS/MXDSA, 4860 S. Superior Ave., Davis-Monthan AFB, AZ., 85707-4305.
The POC is Mr. James M. Bohan, (e-mail, james.bohan@dm.af.mil), Comm (520) 228-8440.

System Boundaries and Interconnection:
All applications reside on servers within bldg. 7328, 309 AMARG, 4860 S. Superior Ave., Davis-Monthan AFB, AZ, 85707-4305. Users access the ABS through the DM network, the purpose of which is to provide a data communication link between clients and servers. There is no data flow between the 309 AMARG and the Davis-Monthan servers.

(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 collected involves names, social security number and salary sensitivity. Risks are addressed by limiting access to the ABS, to users with a completed background investigation and more specifically to PII data on a user-need-to-know basis.

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. Only specific individuals within the 309 AMARG financial community with a need-to-know have access to PII.

☐ **Other DoD Components.**

Specify. N/A

☐ **Other Federal Agencies.**

Specify. N/A

☐ **State and Local Agencies.**

Specify. N/A

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

Specify. N/A

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

Specify. N/A

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.

Individual consent is implied with employment. The PII comes to the ABS from the payroll system for government employees. Any objections are made before 309 AMARG receives the PII. For contractors, the PII comes from the contracting company. Any objections by the employee would be made to his company prior to the PII being passed to the ABS.

(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.

Individual consent is implied with employment. Applicants can decline employment.

(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.	This PII information is collected by OPM or for contractors, the contracting company when employment is accepted. Individuals are given a privacy act statement allowing them to make an informed decision on granting PII. A privacy advisory is given to the individual stating how the PII will be used.

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.