PRIVACY IMPACT ASSESSMENT (PIA)

For the

Job Order Cost Accounting System (JOCAS II)
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: H096 /3
- ☐ **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 007-57-01-01-01-1033-00-402-124

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 F065 HAF B

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.

U.S. GAO Policy and Procedures Manual, Title 2, Accounting (which includes documentation on Cost Accounting Standards (CAS))
DODI 3200.11, Major Range Test Facility Base (MRTFB)
DOD 7000.14, Financial Management Regulation, Volume 4, Accounting Policies and Procedures
Air Force Instruction 65-601, Vol. I, Budget Guidance and Procedures
AFR 170-29, Minimum Requirements of Cost Accounting System
AFR 177-13, Accounting for Research and Development
AFMCI 65-602, Uniform Reimbursement and Pricing Procedures
AFMCI 65-603, Appropriation Reimbursement Procedures
F065 HAF B, JOCAS II SORN

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 Job Order Cost Accounting System is a CFO-compliant, web-based cost accounting system designed to capture/report full project cost, and generate bills for reimbursable efforts. It also provides managers real-time cost data and transaction recording to facilitate informed management decisions. In addition to manual data entry, JOCAS II interacts with several other standard financial and human resource systems.

The flexibility of JOCAS II accommodates a wide variety of organizations (primarily the Major Range and Test Facility Bases (MRTFBS) and Research Labs) within Air Force Material Command, Air Force Space Command, and Air Combat Command. JOCAS II is currently being utilized by the following AF sites: Arnold, Brooks, Edwards, Eglin, Hanscom, Holloman, Hill, Kirtland, Nellis, Patrick, Rome, Tyndall, Vandenberg, and Wright Patterson.

SAF/FMP owns JOCAS II, which is currently in an Operations & Support phase (Steady State / Sustainment). The point of contact is Gregory Fecher (email: gregory.fecher@wpafb.af.mil, telephone: 937-257-0498). However, 554 ELSG/FN is responsible for program management of the system, Randy Campbell (email: rrandy.campbell@wpafb.af.mil, telephone: 937-257-9567) is the Program Manger for JOCAS II.

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

There is a low privacy risk that unauthorized users are granted access to personnel data because of the security processes and business rules enforced in the JOCAS II application as well as the manual process enforced at each JOCAS II production site. This risk exists because one approved JOCAS II official (official must have database / system administrative privileges) can provide another individual access to personnel records on the local database.

JOCAS II will create, maintain, and protect an audit trail of security-relevant events. Access to audit information will be limited to the ISSO, the system administrators, and those authorized by the DAA.

Identification and authentication (I&A) is tracked and retained for all users. Both successful and unsuccessful logons are audited. JOCAS II also tracks system restarts and unsuccessful access attempts to the audit or files. Other events and information are tracked in the audit log, as directed by the ISSO and system administrators.

Automated and manual auditing techniques are applied. Security-relevant events that meet audit requirements are collected, processed, and stored by automated means. Analysis of collected audit data is performed using a combination of automated and manual techniques. Audited information is not required for real-time analysis.

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. United States Air Force

☒ **Other DoD Components.**

Specify. Defense Civilian Pay Service (DCPS)

☐ **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.

To obtain a JOCAS II account, the Contractors must complete and sign a DD Form 2875, which requires a SSN. Signing the DD Form 2875 grants consent to use the information. If the individual objects to providing his/her SSN he/she will not be granted a JOCAS II account. A JOCAS II approved official can still create the individual's personnel record using a "dummy" SSN in order to capture labor cost information. However, Civil Service and Military personnel grant consent as an initial condition of their employment. Any objection to maintaining the SSN must be processed through the appropriate personnel offices.

(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.

To obtain a JOCAS II account, the Contractors must complete and sign a DD Form 2875, which requires a SSN. Signing the DD Form 2875 grants consent to use the information. If the individual objects to providing his/her SSN he/she will not be granted a JOCAS II account. A JOCAS II approved official can still create the individual's personnel record using a "dummy" SSN in order to capture labor cost information. However, Civil Service and Military personnel grant consent as an initial condition of their employment. Any objection to maintaining the SSN must be processed through the appropriate personnel offices.

(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.

The JOCAS II Personnel Master record contains an information message that users must comply with the Privacy Act of 1974. In addition, personnel are required to complete a DD Form 2875 to obtain a JOCAS II account. The DD Form 2875 contains the Privacy Act Statement below:

PRIVACY ACT STATEMENT

Authority: Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act.

Principal Purpose: To record names, signatures, and Social Security Numbers for the purpose of validating the trustworthiness of individuals requesting access to Department of Defense (DoD) systems and information. NOTE: Records may be maintained in both electronic and/or paper form.

Routine Uses: None.

Disclosure: Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.

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.