PRIVACY IMPACT ASSESSMENT (PIA)

Defense Enterprise Accounting and Management System (DEAMS)
Department of the 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 "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate personally identifiable information (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) 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: 465

☐ **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** **Enter UPI:** 007-57-01-01-01-0487-00

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

☐ **No**

d. Does the DoD information system or electronic collection have 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 Enter Privacy Act SORN Identifier**: F065 AFMC A

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.

☐ **No**

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 provision of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute and/or EO do 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; Department of Defense Financial Management Regulation (DoDFMR) 7000.14-R Vol. 4; 5 U.S.C. Sections 2105c, 5531, and 5533; and E.O. 9397 (SSN).

5 U.S.C. 552a (b) of the Privacy Act of 1974, these records contained therein may specifically be disclosed outside the Department of Defense as a routine use pursuant to 5 U.S.C. 552a (b)(3) as follows:

The DoD Blanket Routine Uses published at the beginning of the Air Force's compilation of systems of records notices apply to this system.

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.

DEAMS has established a system of records to replace financial accounting legacy systems with a new system, DEAMS now provides an integrated solution maintaining general ledger, accounts payable, accounts receivable, financial reporting, and billing information for the government.

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

DEAMS data has the potential to be compromised based on physical intrusion into the system and misuse of data outside the system via reporting. DEAMS data is maintained in a controlled facility. DEAMS consist of multiple environments, that include GCSS-AF Production & Pre-Production and the 643 ELSS Capabilities Integration environment (CIE). Physical entry is restricted by the use of locks, guards, and is accessible only to authorized personnel. Access to records is limited to person(s) responsible for servicing the record in performance of their official duties and who are properly screened and cleared for a need-to-know. Users access the DEAMS URL and are prompted to insert their Common Access Card (CAC) for authentication. Once their card is entered they must enter a valid CAC Pin. DEAMS production access is in accordance with AFSSI 8520 Identification and Authentication 18 Jun 09; users access the DEAMS URL and are prompted to insert their CAC for authentication. Once their card is entered they must enter a valid CAC Pin to enter DEAMS Portal site. The GCSS-AF Tivoli Access Manager (TAM) 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 Manager. The role or roles assigned to a user determine the level of data access that user will receive. Users input data into DEAMS which will allow access or query the database for reports and tables. DEAMS Pre-production and CIE access is controlled via DD FORM 2875. All PII is transmitted via HTTPS and the identification information is encrypted against possible interception of the data. All screens and reports that contain PII have been marked with the appropriate Privacy Act and FOUO statements.

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: Air Force, Air Reserve

☑ **Other DoD Components**.

Specify: Defence Finance and Accounting Service (DFAS), TRANSCOM

☐ **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 the method by which individuals can object to the collection of PII.

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

This is not applicable to the data within DEAMS. The PII is collected from the individuals by resources that are users of the Defense Civilian Personnel Data System and users of DODAAF. The PII is then interfaced directly from that system into DEAMS via secure transmission. This data is used to verify that the individual is valid for some type of disbursement from the DoD.

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.

This is not applicable to the data within DEAMS. The PII is collected from the individuals by resources that are users of the Defense Civilian Personnel Data System and users of DODAAF. The PII is then interfaced directly from that system into DEAMS via secure transmission. This data is used to verify that the individual is valid for some type of disbursement from the DoD."

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 is not applicable to the data within DEAMS. The PII is collected from the individuals by resources that are users of the Defense Civilian Personnel Data System and users of DODAAF. The PII is then interfaced directly from that system into DEAMS via secure transmission. This data is used to verify that the individual is valid for some type of disbursement from the DoD.

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 can restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.