

PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

Defense Enterprise Accounting and Management System (DEAMS)

2. DOD COMPONENT NAME:

United States Air Force

3. PIA APPROVAL DATE:

09/13/21

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: (Check one. Note: foreign nationals are included in general public.)

- From members of the general public From Federal employees and/or Federal contractors
 From both members of the general public and Federal employees and/or Federal contractors Not Collected (if checked proceed to Section 4)

b. The PII is in a: (Check one)

- New DoD Information System New Electronic Collection
 Existing DoD Information System Existing Electronic Collection
 Significantly Modified DoD Information System

c. Describe the purpose of this DoD information system or electronic collection and describe the types of personal information about individuals collected in the system.

DEAMS is the core accounting and finance system for the Air Force. The type of personal information obtained through data interface with other systems are SSN, name, financial information, birthdate, employee ID number, and employment information. Other information such as security clearance, citizenship, and name are provided when requesting access.

d. Why is the PII collected and/or what is the intended use of the PII? (e.g., verification, identification, authentication, data matching, mission-related use, administrative use)

1. Identification - DEAMS utilizes the employee's SSN to establish a personnel record to match with interface files.
2. Data matching - The SSN is utilized by DEAMS legacy system interfaces.

e. 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 to the collection of PII.

PII is interfaced directly from legacy systems via the GCSS-AF Enterprise Service Bus (ESB) to control any and all traffic going into and coming out of each DEAMS operational environment via secure transmission. This data is used for processing and recording payroll, travel payments, and miscellaneous payments.

f. 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.

PII is interfaced directly from legacy systems via the GCSS-AF Enterprise Service Bus (ESB) to control any and all traffic going into and coming out of each DEAMS operational environment via secure transmission from authorized sources and is recorded as a part of financial records.

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. (Check as appropriate and provide the actual wording.)

- Privacy Act Statement Privacy Advisory Not Applicable

AUTHORITY FOR THE MAINTENANCE OF THE SYSTEM:

5 U.S.C. 301, Departmental Regulations; Department of Defense Financial Management Regulation (DoDFMR) 7000.14-R Vol. 4 – Accounting Policy; 5 U.S.C. Sections 5335 (periodic step-increases), 5531 (Definitions), and 5533 (Dual pay for more than one position, limitations, exceptions); and E.O. 9397 (SSN) as Amended by Executive Order 13478 signed by President George W. Bush on November 18, 2008; 5 U.S.C. § 2105(a)(1)(C) – Employee; Department of Defense Directive 5118.05, Defense Finance and Accounting (DFAS); Air Force Policy Directive 65-1, Management of Financial Services

PURPOSE OF THE SYSTEM:

The Defense Enterprise Accounting and Management System (DEAMS) was established to transform the U.S. Air Force (USAF) and United States Transportation Command (USTRANSCOM) financial management processes and systems. The primary objective of DEAMS is to produce an auditable financial system by re-engineering and standardizing DoD accounting and financial business processes, using Joint Financial Management Improvement Program/Financial Systems Integration Office certified Commercial-Off-The-Shelf (COTS) software. DEAMS delivers the core accounting and financial reporting system to support all Air Force Commands and Unified Commands where the Air Force is the executive agent. DEAMS will improve timeliness by centralizing control and interfacing with more than 80 financial and financial impacting systems such as travel, payroll, disbursing, transportation, logistics, acquisition, operational, and USTRANSCOM non-core accounting support systems that generate financial events. The system utilizes employees' SSN internally to establish a personnel record to match with interface files, which are used by DEAMS legacy system interfaces, and to ensure duplicate user accounts are not created within the system.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

In addition to those disclosures generally permitted under 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:

- To the Office of Personnel Management (OPM) for the purpose of addressing civilian pay and leave, benefits, retirement deduction, and any other information necessary for the OPM to carry out its legally authorized government-wide personnel management functions and studies.
- To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the federal government when necessary to accomplish an agency function related to this system of records.
- To any component of the Department of Justice for the purpose of representing the DoD, or its components, officers, employees, or members in pending or potential litigation to which the record is pertinent.
- In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body or official, when the DoD or other Agency representing the DoD determines that the records are relevant and necessary to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.
- To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.
- To appropriate agencies, entities, and persons when (1) the DoD suspects or has confirmed that there has been a breach of the system of records; (2) the DoD has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the DoD (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the DoD's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.
- To another Federal agency or Federal entity, when the DoD determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

Disclosure: Mandatory - DEAMS is the Air Force's core accounting and finance system which contains employee data for active duty and government civilians. PII is interfaced directly from other DoD systems into DEAMS via secure transmission. Just like the systems it interfaces with, DEAMS utilizes the employee's SSN for recording payroll, travel payments, and miscellaneous payments. To process payroll DEAMS must establish an employee record. Employee records are utilized by user access processes and the payroll process. To prevent a duplicate employee record the user's access request must include SSN. Accordingly, DEAMS will collect the SSN with user access requests through the DEAMS Help Desk.

SORN: Defense Enterprise Accounting and Management System (DEAMS), F065 AFMC A

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component? (Check all that apply)

- | | | |
|--|----------|--|
| <input checked="" type="checkbox"/> Within the DoD Component | Specify. | <input type="text" value="Air Force"/> |
| <input checked="" type="checkbox"/> Other DoD Components | Specify. | <input type="text" value="DISA, DFAS, ANG, AFRC, GSA, DLA"/> |
| <input type="checkbox"/> Other Federal Agencies | Specify. | <input type="text"/> |

<input type="checkbox"/> State and Local Agencies	Specify.	<input type="text"/>
<input type="checkbox"/> Contractor (Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)	Specify.	<input type="text"/>
<input type="checkbox"/> Other (e.g., commercial providers, colleges).	Specify.	<input type="text"/>

i. Source of the PII collected is: (Check all that apply and list all information systems if applicable)

<input checked="" type="checkbox"/> Individuals	<input type="checkbox"/> Databases
<input checked="" type="checkbox"/> Existing DoD Information Systems	<input type="checkbox"/> Commercial Systems
<input type="checkbox"/> Other Federal Information Systems	

Individual will provide PII information when requesting access to the DEAMS system. DEAMS interfaces with the following legacy systems in either an inbound or outbound exchange flow: Air Reserve Order Writing System (AROWS), Reserve Travel System (RTS), Centralized Disbursing System (CDS), Commercial Operations Integrated System (COINS), Corporate Electronic Funds Transfer (CEFT), Defense Civilian Payroll System (DCPS), Defense Civilian Personnel Data System (DCPDS), Defense Travel System (DTS), Internal Review SeaSide (IRSS), Standard Procurement System (SPS), 1099 TRP interface with DFAS, Wide Area Workflow (WAWF), and MyInvoice (MYIN).

j. How will the information be collected? (Check all that apply and list all Official Form Numbers if applicable)

<input checked="" type="checkbox"/> E-mail	<input checked="" type="checkbox"/> Official Form (Enter Form Number(s) in the box below)
<input checked="" type="checkbox"/> Face-to-Face Contact	<input type="checkbox"/> Paper
<input type="checkbox"/> Fax	<input checked="" type="checkbox"/> Telephone Interview
<input checked="" type="checkbox"/> Information Sharing - System to System	<input type="checkbox"/> Website/E-Form
<input type="checkbox"/> Other (If Other, enter the information in the box below)	

System Authorization Access Request (SAAR) DD Form 2875 v 1.8.2 (all PII elements except for SSN)

k. 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 must be consistent.

Yes No

If "Yes," enter SORN System Identifier

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or <http://dpcl.d.defense.gov/Privacy/SORNs/>
or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

l. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority.

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

T 65-01 R 01 01.00 Financial Management Program Control--Destroy when superseded, obsolete or no longer needed.
All records and data in the system will be retained based on the schedules defined in Defense Finance and Accounting Service 5015.2-M, Records Disposition Schedule. Paper records and DVDs are shredded, electronic records are degaussed.

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statute or Executive Order.

- (1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
- (2) If a SORN does not apply, 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) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.
 - (b) If direct statutory authority or an Executive Order does not exist, indirect statutory 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) If direct or indirect authority does not exist, 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 must be identified.

5 U.S.C. 301, Departmental Regulations; Department of Defense Financial Management Regulation (DoDFMR) 7000.14-R Vol. 4 – Accounting Policy; 5 U.S.C. Sections 5335 (periodic step-increases), 5531 (Definitions), and 5533 (Dual pay for more than one position, limitations, exceptions); and E.O. 9397 (SSN) as Amended by Executive Order 13478 signed by President George W. Bush on November 18, 2008; 5 U.S.C. § 2105(a)(1)(C) – Employee;
10 U.S. Code § 8022 – Financial Management; Department of Defense Directive 5118.05, Defense Finance and Accounting (DFAS); Air Force Policy Directive 65-1, Management of Financial Services

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (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 No Pending

- (1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
- (2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, " DoD Information Collections Manual: Procedures for DoD Public Information Collections."
- (3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

Per DoD Manual 8910.01 Volume 2;
Enclosure 3 , Paragraph 7b (2) Federal employees are not considered members of the public when they respond to a collection of information within the scope of their employment
Enclosure 3, Paragraph 8b (1), (6), (11) describes various information collections that are not considered public information collections; of which para (6) states that "A request for facts or opinions addressed to a single person" and para (11) refers to this information being collected within the scope of their normal employment.
Per DoD 5400.11-R, C1.3.1.1;
"When a DoD Component contract requires the operation or maintenance of a system of records or a portion of a system of records or requires the performance of any activities associated with maintaining a system of records, including the collection, use, and dissemination of records, the record system or the portion of the record system affected are considered to be maintained by the DoD Component and are subject to this Regulation. The Component is responsible for applying the requirements of this Regulation to the contractor. The contractor and its employees are to be considered employees of the DoD Component for the purposes of the criminal provisions of Reference (b) during the performance of the contract."
Since the data being collected is within the scope of normal employment from Federal Employees, Contractors, and Foreign Nationals (who are employed by the U.S. Air Force as Federal Employees or Contractors), an OMB Control number would not be required.

NOTE: Sections 1 above is 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 if they contain information that would reveal sensitive information or raise security concerns.