PRIVACY IMPACT ASSESSMENT (PIA)

For the

Defense Agencies Initiative (DAI)
Business Transformation Agency (BTA)

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 7518

☐ 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 1686

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 SORNs DPR 34 (DCPDS) and T7335 (DCPS) encompass DAI.

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. DRP 34 (21 APR 06) - T7335 (12 DEC 08)

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.

The Business Transformation Agency (BTA), Defense Agencies Initiative, 10 U.S.C. Sec. 2222 et seq., authorized the system. DAI is an Enterprise Resource Planning (ERP) system to support Defense Agencies and Field Activities. DAI will provide for the time keeping and payment of civilian personnel; general ledger accounting; development of requirements; solicitation and award of purchase orders and contracts; receipt and acceptance of supplies and services; property management and payments to vendors.

DAI uses certain data from and sends data to Defense Civilian Personnel System (DCPS) and Defense Civilian Personnel Data System (DCPDS). Each system cited certain authorities as noted below. DAI uses only such data as are required for timekeeping; financial reporting; property management; procurement; receipt processing and acceptance; and payment.

DCPDS SORN T7335 authorities: 5 U.S.C. 301, Departmental Regulations, 5 U.S.C. Chapters 53, 55 and 81, and Executive Order 9397 (SSN) as amended in November 2008.

DCPS SORN DPR 34, authorities: 5 U.S.C. 301, Department Regulations; 5 U.S.C. Chapters 11, 13, 29, 31, 33, 41, 43, 51, 53, 55, 61, 63, 72, 75, 83, 99,; 5 U.S.C. 7201, Antidiscrimination Policy; 10 U.S.C. 136; Under Secretary of Defense for Personnel and Readiness; Executive Order 9830; Amending Civil Service Rules and Providing for Federal Personnel Administration, as amended; Executive Order 9397 (SSN) as amended in November 2008; and 29 CFR 1614.601, EEO Group Statistics.

In January 2007, the Defense Business Systems Management Council (DBSMC) also approved this initiative under BTA. DAI Records System is a Financial Management System that provides auditable accounting of Department of Defense (DoD) programs. Routine uses of this system of records will include "Time and Attendance" using the information from DCPS and DCPDS.

Another feature associated with pay, results from a Claim for Reimbursement.

- Claim for Reimbursement/Miscellaneous Pay: For Miscellaneous Pay action, the Government Employee in DAI will be established under a second record that will contain the SSN. This file will also contain certain information drawn from CEFT. The claim becomes a DAI purchase order. The authorities that cover this collection are drawn from:

i) the Standard Form (SF) 1164 itself where it states:

"In compliance with the Privacy Act of 1974, the following information is provided: Solicitation of the information on this form is authorized by 5 U.S.C. Chapter 57 as implemented by the Federal Travel Regulations (FPMR 101-7), E.O. 11609 of July 22 1971, E.O. 11012 of March 27, 1962, E.O. 9397 of November 22, 1943, and 26 U.S.C. 6011(b) and 6109. The primary purpose of the requested information is to determine payment or reimbursement to eligible individuals for allowable travel and/or other expenses incurred under appropriate administrative authorization and to record and maintain costs of such reimbursements to the Government. The information will be used by Federal agency officers and employees who have a need for the information in the performance of their official duties. The information may be disclosed to appropriate Federal, State, local, or foreign agencies, when relevant to civil, criminal, or regulatory investigations or prosecutions, or when pursuant to a requirement by this agency in connection with the hiring or firing of an employee, the issuance of a security clearance, or investigations of the performance of official duty while in Government service. Your Social Security Account Number (SSN) is solicited under the authority of the Internal Revenue Code (26 U.S.C. 6011(b) and 6109) and E.O. 9397 as amended in November 2008, for use as a taxpayer and/or employee identification number; disclosure is MANDATORY on vouchers claiming payment or reimbursement which is, or may be, taxable income. Disclosure of your SSN and other requested information is voluntary in all other instances; however, failure to provide the information (other than SSN) required to support the claim may result in delay or loss of reimbursement." and

DAI will serve as the official general ledger for participating agencies. "System to system" interfaces that exist include the following.

- Electronic Funds Transfer (EFT), SORN T7320, (October 15, 2004, 69 FR 61225) authorities: 5 U.S.C. 301, Departmental Regulations; Pub.L. 104-134, Debt Collection Improvement Act of 1996; DoD Financial Management Regulation 7000.14-R, Volumes 7B, 7C, 8, Military Pay Policy and Procedures - Retired Pay, Military Pay Policy and Procedures - Active Duty and Reserve Pay, Civilian Pay Policy and Procedures; and E. O. 9397 (SSN) as amended in November 2008.

- Purchase Card SORN GSA/GOVT-6, Federal Register: April 25, 2008 (Volume 73, Number 81) authorities: 41 U.S.C. 252a, 252b, 427, 428; E.O. 12931, and Section 639 of the Consolidated Appropriations Act, 2005 (Pub. L. 108-447).

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 Business Transformation Agency (BTA) Defense Agency Initiative (DAI) Records System is a Financial Management System that provides auditable accounting of DoD programs. Routine uses of this system of records will include Time and attendance using the Defense Civilian Payroll System (DCPS).

DAI systems provide for the reconciliation of human resources and payroll data within the systems, for

comparison and reconciliation with that of disbursing, accounting and other administrative systems/ subsystems/modules to ensure accuracy, completeness and data integrity.

BTA/DAI will ensure that the initiative is consistent with the requirements of the Business Enterprise Architecture (BEA) and Enterprise Transition Plan (ETP) developed pursuant to Section 2222, Title 10, U.S. C., the Standard Financial Information Structure (SFIS) of the Department of Defense; the Federal Financial Management Improvement Act of 1996 (FFMIA) and other applicable requirements of law and regulation.

In DCPDS, each civilian employee has a master record. The data base contains current, projected, and historical position and employee personnel management data, such as education level, work experience, current grade and step, awards history, projected training requirements and completed training, etc. The only data DCPDS sends DAI includes: name, SSN, city, state, zip code, country, gender, and birth date.

DCPS is the DoD Civilian Pay System. The system maintains pay and leave entitlement records, deductions and withholdings, time and attendance data and other pertinent employee data. DAI provides the source keeping documentation to support civilian payroll. The name, SSN, hours and type of hours are exchanged to record Government employee time and labor.

DTS: The Defense Travel System (DTS) facilitates Government travel from booking to claim to payment. DTS will contain the information needed to effect travel and payment. DAI will record the individual's name from DTS in the general ledger entry.

EFT, hereafter referred to as Contractor EFT (CEFT), serves as the DFAS system enabling the payment of employees directly into their respective bank accounts. In order to track employees, CEFT uses SSN. CEFT retains the data to facilitate follow-on payments. Employee data retained in DAI will be discussed later.

Purchase Card: The Purchase Card systems sends DAI transactions to be posted to the general ledger via an interface that provides the merchant information, credit card, description and amount. The individual purchase card (credit card) number is associated with the individual.

Claim for Reimbursement/Miscellaneous Pay: When a claim is submitted from a Government employee, certain data are needed to pay the individual. The data collected facilitate the construction of a new record, a purchase order (the claim), and a payment later made via CEFT.

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

Risk 1 - Access to PII: Access to DAI via CAC with PKI encryption limited to individuals who are properly screened and cleared on a role based/need to know basis in the performance of their duties. Procedures are in place to deter and detect browsing and unauthorized access. Vendors access their own data in the iSupplier module via user ID and password. A vendor may only access their own data.
Risk 2 - Unmasked PII: Currently, DAI masks the SSN, Date of Birth, and Gender of the individual. Other PII data noted in Section 3, para. a are being reviewed. When generating management reports, these data are not included. Reports typically include Project, Task, Expenditure Type and Pay period. Printed reports from Production containing PII are either destroyed (burn bag) or locked in filing cabinets. An example of this is an Employee report of persons that have not been entered or been certified during the pay period.
Risk 3 - Accidental Release of PII: DAI controls the data both at rest and in transit. The data at rest are all located on servers located at DISA Megacenters and protected by several layers of security and monitoring. DAI is also exploring the use of Oracle Advanced Security option to encrypt the data at rest. Data in transit between the DISA servers in the centers as well as between the DISA clusters and external systems are encrypted.

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. All BTA offices use DAI for time and attendance and Procure to Pay (vendor file).

☒ **Other DoD Components.**

Specify. The Defense Agencies and Field Activities authorized by OSD.

☒ **Other Federal Agencies.**

Specify. Via DCPDS and DCPS, in addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, these records or information contained therein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

DCPDS: http://www.defenselink.mil/privacy/notices/osd/DPR34.shtml

DCPS: http://www.defenselink.mil/privacy/notices/dfas/T7335.shtml

DTS: http://www.defenselink.mil/privacy/notices/dfas/T7334.shtml

CEFT: http://www.defenselink.mil/privacy/notices/dfas/T7320.shtml

DCPS, DCPDS, DTS and CEFT also report that data will be shared with the 'Blanket Routine Uses'. These can be found at:

Purchase Card: http://edocket.access.gpo.gov/2008/E8-8883.htm

☒ **State and Local Agencies.**

Specify. As identified above under Blanket Routine Uses Item numbers 2 and 7 of noted above.

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

Specify. Contractors/Vendors other than Systems Administrators will not have access to PII. In addition to the contract clauses noted below, Contractors sign a non-disclosure agreement before commencing work.

Contractors under DISA DITCO ENCORE support DAI. Each ENCORE contract contains the following clauses.

FAR Clause 52.224-1, Privacy Act Notification, APR 1984, and
FAR Clause 52.224-2, Privacy Act, APR 1984, (a).

Both clauses can be located at http://www.acquisition.gov/far/current/html/52_223_226.html.

☐ **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.

On hiring, an individual may object to the collection of PII by refusing to complete required application forms, but such objection would preclude the ability to entitle and disburse payroll to the perspective federal civilian employee.

(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.

Through the SORN Notices for DCPDS (DPR 34) and DCPS (T-7335) published in the Federal Register and the Privacy Act Statement provided at the time of data collection, DoD has informed individuals of the purpose of its collection. By providing the information, the individual concurs with the uses of the information as published in the Federal Register and this PIA. Individuals are not given the ability to determine individual uses for the information collected.

Manual Time-keeping: Non-DAI users from other Defense Agencies/Field Activities that employ time-keepers conducting time and attendance manually may not be aware that DAI exists, but these individuals understand that there is some system that will be used to create their paycheck or push their pay to their bank via EFT.

With the Privacy Act Information provided with the individual's job application for Federal Employment, the individual provides the activity with their PII, some of which may eventually be used by DAI.

(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.

Appropriate Privacy Act Statements are provided at the point of collection by the DoD and or other Federal Agencies.

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.