PRIVACY IMPACT ASSESSMENT (PIA)

For the

Defense Agencies Initiative (DAI)
Defense Logistics Agency (DLA)

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 and 16692
- ☐ 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: 007-000001686 and 007-000100114

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 GSA/GOV-6, DLA S340.10, DLA S890.11, DLA S900.50, DP

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.

S340.10 -5 U.S.C. Chapter 61, Hours of Work; Chapter 53, Pay Rates and Systems; Chapter 57, Travel, Transportation, and Subsistence; and Chapter 63, Leave; 5 U.S.C. 301, Departmental Regulations; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 31 U.S.C., Chapter 35, Accounting and Collection; and E.O. 9397 (SSN), as amended.

DLA S890.11-- 5 U.S.C. Chapter 61, Hours of Work; Chapter 53, Pay Rates and Systems; Chapter 57, Transportation, and Subsistence; and Chapter 63, Leave; 5 U.S.C. 301, Departmental Regulations; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 31 U.S.C., Chapter 35, Accounting and Collection; and E.O. 9397 (SSN), as amended.

S900.50—5 U.S.C. 301, Departmental Regulations; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 5 U.S.C. Chapter 61, Hours of Work; Chapter 53, Pay Rates and Systems; Chapter 57, Travel, Transportation, and Subsistence; and Chapter 63, Leave; 41 U.S.C. 405a, Uniform Federal Procurement Regulations and Procedures; and FAR Part 16.601(b)(1), Time-and-Materials, Labor-Hour, and Letter Contracts.

T7335 (March 13, 2014, 73 FR 75683), 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.

DPR 34 (November 15, 2010, 75 FR 69642), 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, and 99; 5 U.S.C. 7201, Anti-discrimination 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 CFR1614.601, EEO Group Statistics.

T7320 (January 14, 2010, 75 FR 2115), 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 78, 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. 0. 9397 (SSN) as amended in November 2008.

GSA/GOVT-6, Federal Register: (November 3, 2006, 71 FR 64707), 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 DAI application exchanges data with other Federal, DoD, and Agency systems as needed to support the DoD Business Enterprise Architecture (BEA) end-to-end business processes. Most data are financial or related to Time & Labor, which might contain personally identifiable information, in order to support the DoD Global Information Grid and to enable net-centric operations as would be needed for logistics support operations. Data collected include the following:

- Working hours, leave and overtime to track accounting information and workload,
- Project activity for analysis and reporting purposes,
- Statistical reporting on leave and overtime use/usage patterns, and
- Costing capabilities.

Information is provided through database feeds from the Defense Finance and Accounting Service (DFAS) for the purpose of issuing payroll to civilian employees. Civilian employee personally identifiable information (PII) maintained includes the individual's name, SSN, DoD ID, date of birth, pay rate, and leave balances.

The DAI system is a Financial Management System that provides auditable accounting of DoD programs. Routine uses of this system include time and attendance users on the Defense Civilian Pay System (DCPS).

The DAI system provides reconciliation of human resources and payroll data for comparison and reconciliation with disbursing, accounting, and other administrative systems, subsystems, or modules to ensure accuracy, completeness, and integrity of data.

DAI ensures 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 Defense Civilian Personnel Data System (DCPDS), each civilian employee has a master record. The database contains current, projected, and historical position and employee personnel management data, such as education level, work experience, pay grade and step, awards history, projected training requirements, completed training, and so on. DCPDS only sends DAI the following PII data: name, SSN, city, state, zip code, country, gender, and date of birth.

DCPS (distinct from DCPDS) maintains pay and leave entitlement records, deductions and withholdings, time and attendance data, and other pertinent employee data. DAI provides the source with documentation to support civilian payroll. The name, SSN, hours and type of hours are exchanged to record Government employee time and labor.

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.

Customer Electronic Funds Transfer (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.

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

Claim for Reimbursement or 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 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, Unauthorized Access to PII: Access to DAI via CAC with PKI encryption is limited to individuals who are properly screened and cleared either on a role or need-to to-know basis in the performance of their duties. Procedures are in place to detect and deter browsing and unauthorized access.

Risk 2, Unintentional exposure of PII: Currently, DAI masks the SSN, Date of Birth, and Gender of the individual. Other types of PII data are being reviewed for possible masking. When generating management reports, masked PII data are not included. Reports typically include Project, Task, Expenditure Type, and Pay period data. 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 certified during the pay period.

Risk 3, Accidental Release of PII: DAI controls the data both at rest and in transit. All data at rest are on servers located at DISA mega-centers and protected by several layers of security and monitoring. For data at rest, DAI uses Oracle Transparent Data Encryption (TDE). 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.

• Defense Logistics Agency (DLA) Defense Agency Initiative (DAI) program office employees
• DLA Transaction Services

☒ **Other DoD Components.**

Specify.

The DAI DoD data exchange partner agencies are as follows:
• Defense Advanced Research Projects Agency (DARPA)
• Defense Finance and Accounting Service (DFAS)
• Missile Defense Agency (MDA)
• Office of the Secretary of Defense (OSD) Defense Civilian Personnel Advisory Service (DCPAS)

☒ **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, 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:

- U.S. Treasury
- Internal Revenue Service
- Federal Reserve Bank
- Social Security Administration
- Office of Personnel Management
- General Services Administration Government Purchase Card (Access Online - AXOL) and System for Award Management (SAM)
- National Finance Center
- Office of Thrift Savings Plan
- Department of Veterans Affairs
- Department of Labor Division of Federal Employees' Compensation

☒ **State and Local Agencies.**

Specify.
- State revenue departments
- State employment agencies
- Bureaus of employment compensation
- City revenue departments

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

Specify. Contracts supporting the DAI contain, or will contain upon contract award or modification, the following clauses:

- FAR Clause 16.601 Time and Materials Contracts, (b)(1)
- FAR Clause 52.224-1, Privacy Act Notification, APR 1984
- FAR Clause 52.224-2, Privacy Act, APR 1984, (a)
- FAR Clause 52.239-1, Privacy or Security Safeguards

Above clauses can be located at the following location:

https://www.acquisition.gov/far/html/FARTOCP52.html

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

Specify.
- Consumer reporting agencies
- American Red Cross
- Banking establishments for the purpose of billing and expense data.
- Private entities providing travel services for individuals on official business
- Officials of labor unions

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.

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

The DAI application does not provide the option for users to object to the collection of their PII. DAI is not the original source of the data. Personal information is aggregated into this system from other sources. Individuals have an option to refuse to provide information during the original collection of the data.

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.

The DAI application does not provide the option for users to consent to the usage of their PII. DAI is not the original source of the data. Personal information is aggregated into this system from other sources. Individuals have an option to refuse to provide information during the original collection of the data.

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.

Privacy Act advisory will be provided on the DAI web application via Splash Screen, as described in section 2, (i) (2), within three months after the publication of this document.

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.