PRIVACY IMPACT ASSESSMENT (PIA)

For the

Business Enterprise Information Services - Reference Data Service (BEIS-RD)
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: 5215
- ☐ 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: 007-97-01-01-02-2907-00

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: T7320

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.

- Title 5 United States Code 301, Departmental Regulations; Public Law 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 18 NOV 2008 by E.O. 13478.

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 BEIS Family of Systems (FoS) Reference Data Service component, Corporate Electronic Funds Transfer (CEFT) and the associated Electronic Funds Transfer Records provides the DoD with a central repository for military and civilian remittance information, which is used to verify the validity of payee and financial institution accounts prior to issuing an electronic payment. CEFT data is consolidated in the DFAS Corporate Database (DCD) which formerly had it's own DITPR ID and is now part of the BEIS family of systems. The actual system containing the PII data has not physically relocated or changed and is under the direct control of DFAS. It is now logically part of BEIS.

Types of personal information:
Individual's Name, Social Security Number, home address, financial institution account number, account type, financial institution name, American Banking Association routing and transmittal number, lock box number, electronic funds transfer payment method, and electronic funds transfer waiver.

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

Privacy Risk:

Due to CEFT/EFT containing individual's name, SSN, address and financial information, the risk is high of financial fraud and identity theft in the event of inadvertent discloser to unauthorized personnel.

Privacy Risk Mitigation: Adherence to the DoDD and DODI 8500.1/8500.2 (Information Assurance Policy and Implementation Instruction) by implementing and executing an aggressive DoDI 8510.2 DIACAP IA monitoring strategy within the program based on data encryptions and stringent need-to-know justifications.

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. BTA - DAI

☒ **Other DoD Components.**

Specify. Armed Services, DFAS, Department of Veterans Affairs,

☒ **Other Federal Agencies.**

Specify. U.S. Treasury Department, Social Security Administration, IRS, Federal Reserve Banks

☐ **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. American Red Cross and military relief societies.

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.

The CEFT/EFT service provided by the Business Enterprise Information Service is considered a pass-through type of data processing service (No direct end user interface for input/retrieval). EFT data is provided to the BEIS Reference Data Service/CEFT by other government financial systems.

Individuals are provided with a Privacy Act Statement when they apply for Direct Deposit of payroll via standard form SF1199A. Electronic Fund Transfers (EFT) are required for all Federal Payments in accordance with Public Law 104-134 Section 3720C except when such compliance imposes a hardship. Individuals claiming hardship must submit a request for a waiver to their local finance and accounting office.

(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.

Individuals are presented with the uses of their PII as part of the Privacy Act Statement when providing their financial institution information via forms SF 1199A. This information is required under Public law 104-134 Section 3720C unless providing it imposes hardship. Individuals claiming hardship are required to submit a waiver request to their local finance and accounting office. Submitting form SF 1199A constitutes consent to the specific use of their PII.

(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 CEFT/EFT service provided by the Business Enterprise Information Service is considered a pass-through type of data processing service (No direct end user interface for input/retrieval). EFT data is provided to the BEIS Reference Data Service/CEFT by other government financial systems.

Privacy Act Statement
Section 6311 of title 5, United States Code, authorizes collection of this information. The primary use of this information is by management and your payroll office to approve and record your use of leave. Additional disclosures of the information may be: To the Department of Labor when processing a claim for compensation regarding a job connected injury or illness; to a State unemployment compensation office regarding a claim; to Federal Life Insurance or Health Benefits carriers regarding a claim; to a Federal, State, or local law enforcement agency when your agency becomes aware of a violation or possible violation of civil or criminal law; to a Federal agency when conducting an investigation for employment or security reasons; to the Office of Personnel Management or the General Accounting Office when the information is required for evaluation of leave administration; or the General Services Administration in connection with its responsibilities for records management.

Public Law 104-134 (April 26, 1996) requires that any person doing business with the Federal Government furnish a social security number or tax identification number. This is an amendment to title 31, Section 7701. Furnishing the social security number, as well as other data, is voluntary, but failure to do so may delay or prevent action on the application. If your agency uses the information furnished on this form for purposes other than those indicated above, it may provide you with an additional statement reflecting those purposes.

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.