PRIVACY IMPACT ASSESSMENT (PIA)

DoD Information System/Electronic Collection Name:

E-BIZ Business Management Redesign

DoD Component Name:

Defense Finance and Accounting Service

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 10

☐ 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** 007-97-01-34-02-6304-00

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** T7335b [as 'Electronic Business-Labor and Accounting Report (E-BIZ) Records']

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 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.

5 U.S.C. 301, Departmental Regulations, Defense Financial Management Regulation (DoDFMR)7000.14-R, Vol 8; 31 U.S.C. 3512, Executive agency accounting and other financial management reports and plans; 31 U.S.C. 3513, Financial reporting and accounting system and E.O. 9397(SSN).

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.

E-BIZ is used as a feeder system that has a suite of business processes that integrate resource, accounting, financial and other business functions into a comprehensive management information planning system. The data includes budget information, manpower data, performance measures, workload management, time and attendance, labor reporting, work counts, cost accounting, funds control, accounts payable and receivable, general ledger, and financial reporting. It is used to produce useful, timely and accurate management and financial data, allow users to do analysis and reconciliation to ensure data accuracy, provide decision and planning tools for management, and provide timely and accurate financial statements. User names and social security numbers are captured in the system.

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

The result of mishandling personal data may lead to lost, stolen or compromised PII which could be harmful to the individual in many ways (e.g., identity theft, damage to the individual's reputation and /or financial hardship). Such incidents could cast DFAS in an unfavorable light to the public. Hence, access is limited to persons authorized to service or to use the system in performance of their official duties (requires screening and approval for need to know). DFAS adheres to physical protections of PII as described in accordance with DFAS 5200.1-R. IA policy (DFAS 8400.1-R) prescribes protection requirements for sensitive data, to include PII, for all DFAS systems. Management responsibilities for protecting data are maintained in DFAS 8500.1-R.

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

PII data will be shared with the DCPS (Defense Civilian Payroll System) application that uses the PII data to match employees' records between the two systems. Data is also shared with DFAS supervisors who approve the employee's Time and Attendance (T&A), and a small group of users in Accounting Operations who work rejected payroll and travel documents (restricted access by designated security roles).

☒ **Other DoD Components.** Specify

Quarterly outbound file sent to the Joint Manpower Management System (JMMS) which is owned by the Defense Manpower Data Center (DMDC).

☐ **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.

Employee form is currently under review and revision for standardization and compliance to ensure the Privacy Act statement and signature blocks are present. Employee can object to the collection of PII by not signing form, however, a completed form is required for employee to submit T&A hours.

(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.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

Form is currently under revision for standardization and compliance to include the Privacy Act statement and signature blocks to consent to use.

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 E-Biz Employee Maintenance form which is required for user time and attendance system access contains a Privacy Act Advisory statement.

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.