

## 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:

Business Management Redesign (e-Biz)

### 2. DOD COMPONENT NAME:

Defense Finance and Accounting Service

### 3. PIA APPROVAL DATE:

08/04/21

### 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.

Business Management Redesign (e-Biz) is 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. e-Biz uses Personally Identifiable Information (PII) data such as birth date, DoD ID number, employment information, name(s), position/title, rank/grade, Social Security Number (SSN), work e-mail address, and Tax Identification Number (TIN) to produce useful, timely, and accurate management and financial data. e-Biz 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.

#### 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)

Verification and authentication – e-Biz uses the PII data to match with the Defense Civilian Pay System (DCPS) application to ensure proper posting of employee earnings. Mission-related use – e-Biz uses PII information as verification and authentication within e-Biz. e-Biz matches the PII data with the payroll application to ensure proper posting of employee earnings.

#### 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.

Employee Application Level Security (ALS) form represents standardization and compliance to ensure the Privacy Act statement and signature blocks are present. Employees can object to the collection of PII by not signing the form, however, a completed form is required for the employee to submit Time and Attendance (T&A) hours.

#### 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.

Employee ALS form represents 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 the form, however, a completed form is required for employee to submit T&A hours.

#### 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

This system contains Privacy Act Data

Authority: Executive Order (E.O.) 10450, 9397 as amended and Public Law 99-474, The Computer Fraud and Abuse Act.

Purpose of Use: To record names and Social Security Numbers for the purpose of validating the trustworthiness of individuals requesting access to Department of Defense (DoD) systems and information.

Routine Uses: Those generally permitted under 5 United States Code (U.S.C.) 522A(B) of the Privacy Act as required.

Disclosure: Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay, or prevent further processing of the request.

Note: Records may be maintained in both electronic and/or form.

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

☒ Within the DoD Component

Specify.

e-Biz shares PII data with the DCPS and Human Resources Business Intelligence Datamart (HRBID) application in which both applications use the PII data to match employee records between the two systems. e-Biz also shares data with Defense Finance and Accounting Service (DFAS) supervisors who approve employees' T&A, and a small group of users in Accounting Operations who work rejected payroll and travel documents (restricted access by designated security roles). e-Biz shares PII with internal DFAS organizations that demonstrate a need to know.

☐ Other DoD Components

Specify.

☐ Other Federal Agencies

Specify.

☐ State and Local Agencies

Specify.

☒ 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.

NOTE: Temporary access granted while contractor Client Global Insights (CGI) Federal implements Standard Financial Information Structure (SFIS)/Standard Line of Accounting (SLOA) functionality into the system. Contract language to safeguard is as follows:  
CONTRACTOR USE OF DATA: Performance of this contract may require the contractor to access and use data and information proprietary to a Government agency. Contractor and contractor personnel shall not divulge or release data or information developed or obtained in performance of this effort, until made public by the Government, except upon written approval of the Contracting Officer.  
SECURITY REQUIREMENTS, PRIVACY ACT, AND NON-DISCLOSURE REQUIREMENTS: See DFAS Clause 52.224-9000 "Information Assurance" (September 2014). The Contractor shall comply with established security procedures.  
SECURITY REQUIREMENTS AND PRIVACY ACT REQUIREMENTS - SECURE ENVIRONMENT: All work-performed relative to the tasking identified in the Statement of Work (SOW) are unclassified or carry a Privacy Act Classification. System security shall be in accordance with DoD directive 8500.1, Information Assurance.

☐ Other (e.g., commercial providers, colleges).

Specify.

**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           |   |

Individuals provide PII data directly on the e-Biz Employee Maintenance form, which is required for user T&A system access. Form represents standardization and compliance to ensure the Privacy Act statement and signature blocks are present. Existing DoD information systems, the DCPS, HRBID, DFAS Corporate Database (DCD), and Defense Travel System (DTS) applications also provide PII data used in matching employee records between systems.

**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 type="checkbox"/> Official Form (Enter Form Number(s) in the box below) |
| <input type="checkbox"/> Face-to-Face Contact                                     | <input type="checkbox"/> Paper   |
| <input type="checkbox"/> Fax  | <input 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) |  |

The e-Biz Security e-mail inbox receives new civilian and non-civilian timekeeping forms. System to system data connection such as DCPS, HRBID, DCD, and DTS have signed, documented interface agreements outlining the physical connection details.

**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.

**i. 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.

Cutoff for records is at the end of the payroll year. Records destruction takes place after audit or when 10 years old, whichever is sooner. Destruction methods include degaussing the electronic media and recycling hard-copy records. Destruction methods for recycled hard copies include shredding, burning, or pulping.

**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.

DoD 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) as amended.

**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.

This system does not require Office of Management and Budget (OMB) approval. Information collected is internal to DFAS and used to determine work hours and billing. Does not collect information on members of the public.