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)*

☒ Individuals

☒ Existing DoD Information Systems

☐ Other Federal Information Systems

☐ Databases

☐ Commercial 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)*

☒ E-mail

☐ Face-to-Face Contact

☐ Fax

☒ Information Sharing - System to System

☐ Other *(If Other, enter the information in the box below)*

☐ Official Form (*Enter Form Number(s) in the box below)*

☐ Paper

☐ Telephone Interview

☐ Website/E-Form

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 T7335b

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or http://dpcld.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.

l. 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. DFAS 5015.2-M Schedul

(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 statue 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.

SECTION 2: PII RISK REVIEW

a. What PII will be collected *(a data element alone or in combination that can uniquely identify an individual)? (Check all that apply)*

□ Biometrics	☒ Birth Date	□ Child Information
□ Citizenship	□ Disability Information	☒ DoD ID Number
□ Driver's License	□ Education Information	□ Emergency Contact
☒ Employment Information	□ Financial Information	□ Gender/Gender Identification
□ Home/Cell Phone	□ Law Enforcement Information	□ Legal Status
□ Mailing/Home Address	□ Marital Status	□ Medical Information
□ Military Records	□ Mother's Middle/Maiden Name	☒ Name(s)
□ Official Duty Address	□ Official Duty Telephone Phone	□ Other ID Number
□ Passport Information	□ Personal E-mail Address	□ Photo
□ Place of Birth	☒ Position/Title	□ Protected Health Information (PHI)[1]
□ Race/Ethnicity	☒ Rank/Grade	□ Religious Preference
□ Records	□ Security Information	☒ Social Security Number (SSN) *(Full or in any form)*
☒ Work E-mail Address	☒ If Other, enter the information in the box below	

Tax Identification Number (TIN)

If the SSN is collected, complete the following questions.

(DoD Instruction 1000.30 states that all DoD personnel shall reduce or eliminate the use of SSNs wherever possible. SSNs shall not be used in spreadsheets, hard copy lists, electronic reports, or collected in surveys unless they meet one or more of the acceptable use criteria.)

(1) Is there a current (dated within two (2) years) DPCLTD approved SSN Justification on Memo in place?

□ Yes ☒ No

If "Yes," provide the signatory and date approval. If "No," explain why there is no SSN Justification Memo.

The SSN and/or TIN Justification Memo – e-Biz is in the process of updating the current memo on file.

(2) Describe the approved acceptable use in accordance with DoD Instruction 1000.30 "Reduction of Social Security Number (SSN) Use within DoD".

Department of Defense Instruction (DoDI) 1000.30 under section 2 (7) Federal Taxpayer Identification Number. The application of Federal and State income tax programs rely on the use of the SSN. As such, systems that have any function that pertains to the collection, payment, or record keeping of this use case may contain the SSN.

(3) Describe the mitigation efforts to reduce the use including visibility and printing of SSN in accordance with DoD Instructoin 1000.30, "Reduction of Social Security Number (SSN) Use within DoD".

The application obfuscates the SSN which is only available to individuals on an approved need-to-know basis.

(4) Has a plan to eliminate the use of the SSN or mitigate its use and or visibility been identified in the approved SSN Justification request?

If "Yes," provide the unique identifier and when can it be eliminated?
If "No," explain.

□ Yes ☒ No

Justification for the use of the SSN and/or TIN does not constitute blanket permission to use such data. The e-Biz application supports payment, collection, and reporting for DoD components. e-Biz must continue to collect and store the SSN and TIN in order to disburse payments, process collections, and handle tax-reporting requirements established by the Internal Revenue Service. The system in question, e-Biz, has established user roles that safeguard the SSN and TIN.

b. What is the PII confidentiality impact level[2]? □ Low ☒ Moderate □ High

[1] The definition of PHI involves evaluating conditions listed in the HIPAA. Consult with General Counsel to make this determination.

[2] Guidance on determining the PII confidentiality impact level, see Section 2.5 “Categorization of PII Using NIST SP 800-122.” Use the identified PII confidentiality impact level to apply the appropriate Privacy Overlay low, moderate, or high. This activity may be conducted as part of the categorization exercise that occurs under the Risk Management Framework (RMF). Note that categorization under the RMF is typically conducted using the information types described in NIST Special Publication (SP) 800-60, which are not as granular as the PII data elements listed in the PIA table. Determining the PII confidentiality impact level is most effective when done in collaboration with the Information Owner, Information System Owner, Information System Security Manager, and representatives from the security and privacy organizations, such as the Information System Security Officer (ISSO) and Senior Component Official for Privacy (SCOP) or designees.

c. How will the PII be secured?

(1) Physical Controls. *(Check all that apply)*

☒ Cipher Locks
☒ Combination Locks
☒ Key Cards
☒ Security Guards
☒ Closed Circuit TV (CCTV)
☒ Identification Badges
□ Safes
☒ If Other, enter the information in the box below

e-Biz inherits all physical controls protecting Defense Information Systems Agency (DISA) hosting enclaves: Mechanicsburg, Pennsylvania for primary and Ogden, Utah as secondary. e-Biz and DISA employ additional protective measures such as personnel screening and use of visitor registers to protect data. Access to records is limited to properly screened, cleared, and authorized individuals on a need-to-know basis in the performance of their official duties.

(2) Administrative Controls. *(Check all that apply)*

☒ Backups Secured Off-site
□ Encryption of Backups
☒ Methods to Ensure Only Authorized Personnel Access to PII
☒ Periodic Security Audits
☒ Regular Monitoring of Users' Security Practices
☒ If Other, enter the information in the box below

All administrative controls required by DoDI 8500.2 or applicable National Institute of Standards and Technology (NIST) Special Publication 800-53 controls have been implemented and validated for this system. e-Biz tracks and works per the system, Plan of Action and Milestones (POA&M) for any non-compliant controls. Implementation will occur as soon as possible. DISA sites may not encrypt systems for operational reasons, but they are subject to layered protective measures including network and system hardening determined to be adequate for sensitive unclassified information.

(3) Technical Controls. *(Check all that apply)*

□ Biometrics
☒ Encryption of Data at Rest
☒ Firewall
☒ Role-Based Access Controls
☒ Virtual Private Network (VPN)
☒ Command Access Card (CAC)
☒ Encryption of Data in Transit
☒ Intrusion Detection System (IDS)
□ Used Only for Privileged (Elevated Roles)
□ If Other, enter the information in the box below
☒ DoD Public Key Infrastructure Certificates
□ External Certificate Authority Certificates
☒ Least Privilege Access
☒ User Identification and Password

d. What additional measures/safeguards have been put in place to address privacy risks for this information system or electronic collection?

The application obfuscates the SSN which is only available to administrators and those individuals on an approved need-to-know basis.

SECTION 3: RELATED COMPLIANCE INFORMATION

a. Is this DoD Information System registered in the DoD IT Portfolio Repository (DITPR) or the DoD Secret Internet Protocol Router Network (SIPRNET) Information Technology (IT) Registry or Risk Management Framework (RMF) tool[3]?

☒	Yes, DITPR	DITPR System Identification Number	10
□	Yes, SIPRNET	SIPRNET Identification Number	
☒	Yes, RMF tool	RMF tool Identification Number	42
□	No		

If "No," explain.

b. DoD information systems require assessment and authorization under the DoD Instruction 8510.01, "Risk Management Framework for DoD Information Technology".

Indicate the assessment and authorization status:

☒	Authorization to Operate (ATO)	Date Granted:	8/2/2024
□	ATO with Conditions	Date Granted:	
□	Denial of Authorization to Operate (DATO)	Date Granted:	
□	Interim Authorization to Test (IATT)	Date Granted:	

(1) If an assessment and authorization is pending, indicate the type and projected date of completion.

(2) If an assessment and authorization is not using RMF, indicate the projected transition date.

c. Does this DoD information system have an IT investment Unique Investment Identifier (UII), required by Office of Management and Budget (OMB) Circular A-11?

☒ Yes □ No

If "Yes," Enter UII 007-000006304 If unsure, consult the component IT Budget Point of Contact to obtain the UII

[3] Guidance on Risk Management Framework (RMF) tools (i.g., eMASS, Xacta, and RSA Archer) are found on the Knowledge Service (KS) at https://rmfks.osd.mil.