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 Continuity Planning System (BCPS)

2. DOD COMPONENT NAME:

Defense Finance and Accounting Service

3. PIA APPROVAL DATE:

10/23/19

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
- [x] 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
- [x] 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 Continuity Planning System (BCPS) consists of two Commercial-Off-The-Shelf (COTS) software tools: Business Continuity Planning Tool (BCPT) & an Alert Notification Tool (ANT). The BCPT utilizes the Enterprise Business Resiliency Planning (eBRP) COTS software suite. eBRP is a stand-alone, web-based application that is used as a repository for contingency planning and Continuity of Operations (COOP) plans to guide non-subject matter experts with software templates, planning processes, and identification of any necessary processes and strategies which will ensure continuation of critical functions/operations during an all hazards business interruption. eBRP Suite incorporates over 370 customizable standard Business Continuity reports. Business Continuity Planning administrators create continuity plans in eBRP in order to support organizational requirements. This software supports high-availability through load balancing, replication and/or active-passive hosting. This system can be available 24/7. The software incorporates the CommandCentre toolkit used for simulation, exercise, testing or real-time incident management. eBRP has the capability to fully integrate with three major Alert Notification Tools. ANT utilizes the COTS Cloud Service Provider (CSP) Software-as-a-Service (SaaS) suite Send Word Now (SWN), to provide emergency alert notifications to Defense Finance and Accounting System (DFAS) personnel.
The following information types are collected: EDIPI, Employee name, Work organization, Work location, Work email, Work phone, Personal home/mobile phone number.

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)*

The data is collected for identification & emergency/mission-related notification purposes.

e. Do individuals have the opportunity to object to the collection of their PII? [x] 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.

Individuals may choose not to provide PII voluntary. However, failure to provide the requested information may result in the individual(s) emergency points of contact, not being notified in the event of a disaster. For contractor personnel; failure to provide information may result in administrative termination of their support function. Disclosure is voluntary, but failure to provide requested information will prevent an individual from holding a key position within the Disaster Recovery Program.

f. Do individuals have the opportunity to consent to the specific uses of their PII? [x] 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.

Individuals are provided the opportunity to consent to the specific use of PII voluntarily. The data source is stored in the MyBiz application. This PII data is updated by the employee. They are not required to provide this information. It is strictly voluntary. MyBiz provides the PII banner and states the following:

Privacy Act Statement

The information you provide to the Defense Civilian Personnel Data System (DCPDS) is covered by the Privacy Act of 1974.For questions regarding your personal information please contact your local Human Resources Office.
Authorities: 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; 10USC 136; DoD Instruction 1400.25, volumes 1100 and 1401; 29 CFR 1614.601; and E.O.9397.
Principal Purposes: To allow civilian (appropriated fund and non-appropriated fund) employees in the Department ofDefense (DoD) to update personal information.
Routine Uses: None. The DoD 'Blanket Routine Uses' set forth at the beginning of OSD's compilation of systems of records notices apply to this system.
Disclosure: Voluntary. However, failure to provide or update your information may require manual HR processing for the absence of some information.

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

Privacy Act Statement

The information you provide to the Defense Civilian Personnel Data System (DCPDS) is covered by the Privacy Act of 1974.For questions regarding your personal information please contact your local Human Resources Office.
Authorities: 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; 10USC 136; DoD Instruction 1400.25, volumes 1100 and 1401; 29 CFR 1614.601; and E.O.9397.
Principal Purposes: To allow civilian (appropriated fund and non-appropriated fund) employees in the Department ofDefense (DoD) to update personal information.
Routine Uses: None. The DoD 'Blanket Routine Uses' set forth at the beginning of OSD's compilation of systems of records notices apply to this system.
Disclosure: Voluntary. However, failure to provide or update your information may require manual HR processing for the absence of some information.

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.	Defense Finance and Accounting Service
☐ 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.

Information from BCPS(eBRP) is used for the DFAS Alert notification system.
Contract language is as follows:
52.239-1 PRIVACY OR SECURITY SAFEGUARDS (AUG 1996)
(a) The Contractor shall not publish or disclose in any manner, without the Contracting Officer's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government.
(b) To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases.
(c) If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

☐ 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

DCPDS, DMDC

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

Other: Data files are received as attachments via email by the DFAS Office of Preparedness team. Data files are manually manipulated and entered into the eBRP system manually (by hand).
E-Form: DFAS Form 9385

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 T3020 - Living Disaster Recovery Plannin

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

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

Cut off upon verification of input or when no longer needed to support the reconstruction of, or serve as back-up to the database, whichever is later. Destroy/delete at cutoff.

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.

5 U.S.C. 301, Departmental Regulations; DFAS Regulation 3020.26, Corporate Contingency Plan; DoDD 1400.31, Mobilization Management of the DoD Civilian Work Force; DoDI 1400.32, DoD Civilian Work Force Contingency and Emergency Planning Guidelines and Procedures; DoDI 3020.37, Continuation of Essential DoD Contractor Services During Crises and E.O. 12656, Assignment of Emergency Preparedness Responsibilities.

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.

Paragraph 8b(11) Items Not Considered Public Information Collections: Collections of information from DoD civilian employees within the scope of their employment (includes all the tasks performed to accomplish the job they perform for the OSD or DoD Component), unless the results are to be used for general statistical purposes.